# Algebra

Unterlagen zu Vorlesungen von
Martin Goldstern und Reinhard Winkler
gehalten an der TU Wien

1. Juli 2022

# ALGEBRA

TU Wien

Dieser Text dient als Begleitmaterial (Skriptum) zu den entsprechend dem Studienplan zur Technischen Mathematik regelmäßig angebotenen, aufeinander aufbauenden Lehrveranstaltungen *Algebra I (= Algebra)* und *Algebra II* (jeweils Vorlesung und Übung). Kapitel 1 bis 6 begleiten die Vorlesung Algebra I, Kapitel 7 bis 10 die Vorlesung Algebra II. Der Anhang (= Kapitel 11) wird nicht als Teil der Vorlesung behandelt, sondern stellt mengentheoretische Grundlagen bereit, auf die in der Algebra gelegentlich zurückgegriffen wird. Eine systematische Behandlung der Inhalte des Anhangs muss Lehrveranstaltungen speziell über Logik, Mengenlehre und Grundlagen der Mathematik vorbehalten bleiben.

Die vorliegende Version des Skriptums zielt auf die Vorlesung Algebra I im Sommersemester 2021 ab. Gegenüber der Ausgabe von 2020 gab es keine nennenswerten Veränderungen, abgesehen von einige Korrekturen und zusätzlichen UE-Aufgaben.

Seit 2020 ist nur den Kapiteln und Abschnitten (erste und zweite Gliederungsebene), sondern auch jedem der Unterabschnitte (dritte Gliederungsebene) eine Einleitung mit dem jeweiligen „Inhalt in Kurzfassung“ vorangestellt. Dies soll helfen, das Wichtige mit einem kurzen Blick im Auge zu behalten und vom Beiläufigen zu unterscheiden.

Eine Mini-Version des Skriptums, die *nur* diese Kurzfassungen enthält, ist im tuwel-Kurs „104.998 Algebra (VO 3,5) 2021S“ verfügbar.

Da die letzten Ergänzungen nicht den Kernstoff betreffen, wird, wer aus früheren Jahren eine ältere Version des Skriptums besitzt, damit die wesentlichen Inhalte der Vorlesung Algebra I auch im Sommersemester 2021 abgedeckt finden. Zu bedenken ist jedoch, dass die Vorlesung von Übungen begleitet wird, zu denen das Skriptum die Angaben der Aufgaben enthält. Bei jeder Revision (zuletzt: Februar 2021) ändert sich die Nummerierung der Aufgaben. Die pdf-Datei der aktuellen Version wird mit Anfang des Sommersemesters in elektronischer Form über tuwel zur Verfügung gestellt.

Gebundene physische Exemplare können nach Beginn der Vorlesung beim TU-Verlag günstig erworben werden. Auch in Zukunft sind Revisionen zu erwarten. Wir haben die Absicht, diese gleichfalls wieder auch in elektronischer Form zur Verfügung zu stellen.

Zum Inhaltlichen: Mathematik lebt zu einem guten Teil von ihren reichhaltigen inneren Querverbindungen. Für die Algebra als stark strukturtheoretisch geprägter Disziplin gilt das ganz besonders. Aus diesem Grund hängt die Qualität einer Vorlesung über dieses Thema nicht zuletzt von einem ökonomischen Aufbau ab, in dem gleichzeitig die keineswegs nur linear verlaufenden Verbindungen sichtbar werden. In der Algebra noch mehr als in manch anderen Teilgebieten der Mathematik spielt dabei ein sorgfältiger begrifflicher Aufbau eine wesentliche Rolle. Ein profundes Verständnis für diesen Aufbau ist daher ein wichtiger Schlüssel zur Bewältigung des Großteils des Stoffes von Algebra I. Die technischen Komplikationen in den Beweisen sind in den meisten Fällen vergleichsweise gering. In der Algebra II, wo die meisten Begriffsbildungen bereits zur Verfügung stehen, verlagern sich die Gewichte dann hin zu subtileren Beweisen. Trotzdem ist es unser Ziel, die Inhalte möglichst organisch darzustellen; ausufernde technische Komplikationen, die stets die Gefahr bergen, dass Details den Blick auf die wesentlichen Ideen verdecken, versuchen wir nach Möglichkeit zu vermeiden (was aber nicht immer möglich ist).
Die Grobstruktur von Vorlesungen und Skriptum ist vorwiegend diesem Anliegen geschuldet. In den vergangenen Jahren haben wir diesbezüglich beträchtliche Verbesserungen vorgenommen, indem wir Teile älterer Versionen umstrukturiert, ergänzt und den inhaltlichen Aufbau ökonomischer gestaltet haben. Vereinzelte Fragmente stammen noch von anderen Autorinnen und Autoren, die für uns nicht mehr alle identifizierbar sind, denen aber durchwegs unser Dank gilt.
Durch die Reorganisation entstand gelegentlich Raum für zusätzliche interessante Inhalte. Leider hinkt die Anpassung der Feinstruktur bis hin zu Notation, Drucksatz etc. den großräumigen Veränderungen hinterher und ist noch bei weitem nicht abgeschlossen. Wir bitten deshalb um Nachsicht angesichts mancher Mängel wie auch gelegentlicher Redundanzen, die noch nicht vollständig aufgearbeitet sind. Immerhin sollte der vorliegende Text mittlerweile den gesamten Stoff der aktuellen Algebra-Lehrveranstaltungen enthalten.
An einigen Stellen geht das Skriptum auch über den Vorlesungsstoff hinaus. Vor allem beträchtliche Teile der Grundlagenkapitel, von denen vieles schon aus früheren Lehrveranstaltungen bekannt ist, werden in der Vorlesung nur überblicksartig behandelt. Auch von den späteren Kapiteln werden in der Vorlesung manche (Unter-)Abschnitte hintangestellt oder gar ausgelassen. Teile, die mit * gekennzeichnet sind, warten noch auf eine grundlegende Überarbeitung und sind gegenwärtig nicht Prüfungsstoff.

Empfehlung für Hörerinnen und Hörer, insbesondere von Algebra I: Jeder Student, jede Studentin, hat seinen oder ihren eigenen Lernstil; die einen lernen durch Zuhören, die anderen durch Lesen des Skriptums (oder auch aus Büchern, aus der Wikipedia oder von youtube-Videos – beachten Sie in diesem Fall aber, dass sich die Namen mancher Konzepte von Buch zu Buch unterschieden, und dass Definitionen in anderen Quellen zwar oft äquivalent zu unseren sind, aber dennoch ganz anders formuliert), wieder andere lernen, indem Sie anderen etwas erklären; am nachhaltigsten lernt man wohl, wenn man Lösungen und Sachverhalte selbst entdeckt.
Wir empfehlen allen, sich die Vorlesungen live anzuhören und/oder die aufgezeichneten Vorlesungen nachzuhören. Erstens merken Sie dadurch, welcher Stoff gemacht wurde und

wie dieser gewichtet wurde, zweitens haben Sie beim Zuhören des live-streams die Möglichkeit, Fragen zu stellen und so Unklarheiten gleich aufzuklären. Wenn Unklarheiten erst später entstehen, können diese oft im Repetitorium aufgeklärt werden.
Unerlässlich ist die Verwendung der Unterlagen für die begleitende LVA *Übungen*, weil dazu die Übungsaufgaben im Skriptum verwendet werden. Bedenken Sie, bevor Sie das Skriptum ausdrucken, dass beim TU-Verlag (Freihaus, Erdgeschoß) auch eine preisgünstige gebundene Version erhältlich sein wird.
Die allgemeine Empfehlung zur Prüfungsvorbereitung lautet: Setzen Sie auf Ihre eigene Urteilsfähigkeit hinsichtlich der Wichtigkeit mathematischer Inhalte, schätzen Sie Stoffteile diesbezüglich ein und setzen Sie beim Lernen entsprechende Prioritäten. Wenn Sie die zentralen Inhalte gut durchdringen, machen Sie sich flexibel auch für Prüfungsfragen, mit denen Sie in dieser Form nicht gerechnet haben. Das anzustreben ist eine empfehlenswerte Strategie bei der Aneignung von Mathematik generell wie besonders auch bei der Vorbereitung auf die Algebra-Prüfung.

Martin Goldstern
Reinhard Winkler Februar 2021

## Klassifikation der UE-Aufgaben

Jede Übungsaufgabe wird zu einem von mehreren Typen (gelegentlich auch zu mehr als einem) durch jeweils einen der Buchstaben A, B, D, E, F, V, W zugeordnet. Dies soll den Studierenden im Vorhinein darüber Information geben, welche Arbeit und welche Einsicht sie erwartet:

(A) (Alternative Sichtweise): Für einen bereits bekannten Inhalt soll durch einen alternativer Zugang das Verständnis erweitert werden.

(B) (Beispiel): Damit wird exemplarisch ein Beispiel behandelt, das charakteristisch ist für einen Begriff oder Sachverhalt aus der allgemeinen Theorie.Oder ein Gegenbeispiel, welches belegt, dass eine scheinbar harmlose Variante oder Umformulierung den Sinn einer Definition deutlich verändert, oder aus einem wahren und interessanten Satz einen falschen oder trivial gültigen Satz erzeugt.

(D) (Diskussion): Damit werden offene und möglicherweise vage Aufgabenstellung markiert, die eher zur Diskussion anregen sollen als ein ganz bestimmtes Ergebnis einzufordern.

(E) (Erweiterung): Damit wird der eigentliche Lehrstoff der Vorlesung verlassen. Der Lohn für den Aufwand, sich trotzdem mit der Aufgabe zu beschäftigen, besteht in einer Erweiterung des Horizonts und/oder Vertiefung des Verständnisses. Über diesen Umweg kann man davon eventuell auch in Hinblick auf die Prüfung profitieren. Oft ergibt sich dieser Effekt schon allein dadurch, dass man sich die Aufgabenstellung klar macht.

(F) (Fingerübung): Solche Aufgaben dienen vor allem der Kontrolle des Verständnisses der wesentlichen Konzepte, sind abgesehen davon aber in der Regel für sich genommen von geringerem Interesse. Diese Aufgaben können sehr kurz oder auch länger sein. Substanzielle, d.h. für die Theorie wichtige neue Ideen sind für die Bearbeitung nicht erforderlich. Fingerübungen, die dennoch irgendwelche Einsichten von allgemeinerem Interesse zeitigen, sind mit (F+) gekennzeichnet.

(V) (Vervollständigung): Hier steht das Anliegen im Vordergrund, Beweislücken im Haupttext des Skriptums zu schließen. Häufig handelt es sich um kleine, eher technische Ergänzungen, die zunächst ausgespart wurden, damit in einem Beweis die wesentlichen Gedanken nicht durch ausufernde technische Details verschleiert werden. Manchmal werden auch etwas längliche Beweise, die aber weder sehr schwierig noch besonders erhellend sind, in Übungsaufgaben von diesem Typ ausgelagert.

(W) (Wichtig, Wesentlich): In solchen Übungsaufgaben werden Aussagen bewiesen, die eine wichtige Rolle für das Verständnis der Hauptinhalte der Vorlesung spielen.

Selbstverständlich sind die Grenzen zwischen diesen Typen nicht scharf, und jede Übungsaufgabe trägt mehrere Aspekte in sich. Wir haben jeweils einen davon ausgewählt, den wir im Vordergrund sehen.

# Inhaltsverzeichnis


**1 Einführung in die algebraische Denkweise** **1**

1.1 Die natürlichen Zahlen . . . . . 1
1.1.1 Natürliche Zahlen als endliche Kardinalitäten . . . . . 2
1.1.2 Bemerkungen zu Induktionsbeweisen . . . . . 5
1.1.3 Axiomatisierung nach Peano . . . . . 7
1.1.4 Das von Neumannsche Modell . . . . . 11
1.1.5 Arithmetik und Ordnung der natürlichen Zahlen . . . . . 12
1.1.6 Zifferndarstellung und Normalform . . . . . 16
1.2 Zahlenbereichserweiterungen als Beispielgeber . . . . . 18
1.2.1 Die ganzen Zahlen . . . . . 18
1.2.2 Die rationalen Zahlen . . . . . 22
1.2.3 Die reellen Zahlen . . . . . 24
1.2.4 Die komplexen Zahlen . . . . . 28
1.3 Paradigmen aus der Linearen Algebra . . . . . 31
1.3.1 Lineare (Un-)Abhängigkeit . . . . . 32
1.3.2 Das Austauschlemma und seine Konsequenzen . . . . . 33
1.3.3 Die Klassifikation beliebiger Vektorräume durch ihre Dimension . 34
1.3.4 Die Klassifikation linearer Abbildungen . . . . . 35

**2 Grundbegriffe** **39**

2.1 Der logisch-modelltheoretische Rahmen der allgemeinen Algebra . . . . . 39
2.1.1 Notation und Terminologie . . . . . 39
2.1.2 Grundbegriffe der Ordnungstheorie . . . . . 45
2.1.3 Operationen und universelle Algebren . . . . . 49
2.1.4 Relationale Strukturen . . . . . 57
2.1.5 Homomorphismen zwischen Algebren . . . . . 61
2.1.6 Strukturverträgliche Abbildungen zwischen relationalen Strukturen 63
2.1.7 Klassifikation modulo Isomorphie als Paradigma . . . . . 65
2.1.8 Terme, Termalgebra, Gesetze und Varietäten . . . . . 67
2.1.9 Ein kurzer Exkurs in die mathematische Logik . . . . . 73
2.1.10 Klone . . . . . 78
2.2 Der kategorientheoretische Rahmen . . . . . 81
2.2.1 Kategorien . . . . . 82
2.2.2 Beispiele von Kategorien . . . . . 84
2.2.3 Universelle Objekte und ihre Eindeutigkeit . . . . . 86
2.2.4 Funktoren . . . . . 88
2.2.5 Kommutative Diagramme als Funktoren . . . . . 92

2.2.6 Natürliche Transformationen . . . . . 94
2.3 Elemente algebraischer Strukturanalyse . . . . . 97
2.3.1 Unteralgebren und Erzeugnisse . . . . . 97
2.3.2 Direkte Produkte . . . . . 106
2.3.3 Homomorphe Bilder, Kongruenzrelationen und Faktoralgebren . . 109
2.3.4 Direkte Limiten . . . . . 116
2.3.5 Triviale und nichttriviale Varietäten . . . . . 120
2.3.6 Isomorphiesätze . . . . . 121

**3 Elementare Strukturtheorien 125**
3.1 Halbgruppen und Monoide . . . . . 125
3.1.1 Potenzen und Inverse . . . . . 125
3.1.2 Wichtige Beispiele von Halbgruppen . . . . . 129
3.1.3 Algebraische Strukturanalyse auf $\mathbb{N}$ . . . . . 131
3.1.4 Quotienten- bzw. Differenzenmonoid . . . . . 137
3.2 Gruppen . . . . . 143
3.2.1 Nebenklassenzerlegung . . . . . 143
3.2.2 Faktorgruppen und Normalteiler . . . . . 146
3.2.3 Direkte und schwache Produkte von Gruppen . . . . . 152
3.2.4 Zyklische Gruppen . . . . . 157
3.2.5 Permutationsgruppen . . . . . 165
3.2.6 Symmetrie . . . . . 171
3.3 Moduln, insbesondere abelsche Gruppen . . . . . 172
3.3.1 Abelsche Gruppen als Moduln über $\mathbb{Z}$ und $\mathbb{Z}_m$ . . . . . 172
3.3.2 Unter- und Faktormoduln, Homomorphismen, Produkte und direkte Summen . . . . . 173
3.3.3 Zerlegung von Torsionsgruppen in ihre $p$-Anteile . . . . . 179
3.3.4 Endliche abelsche Gruppen . . . . . 182
3.4 Ringe . . . . . 185
3.4.1 Kongruenzrelationen und Ideale . . . . . 186
3.4.2 Ideale in kommutativen Ringen mit 1 . . . . . 189
3.4.3 Charakteristik . . . . . 192
3.4.4 Die binomische Formel . . . . . 193
3.4.5 Quotientenkörper . . . . . 194
3.4.6 Polynome und formale Potenzreihen . . . . . 199
3.4.7 Der Chinesische Restsatz . . . . . 206
3.4.8 Beispiele nichtkommutativer Ringe . . . . . 208
3.5 Geordnete Gruppen und Körper . . . . . 211
3.5.1 Grundlegende Definitionen . . . . . 211
3.5.2 Geordnete Gruppen . . . . . 212
3.5.3 Angeordnete Körper und nochmals $\mathbb{R}$ . . . . . 213
3.5.4 Modelltheoretische Bemerkungen . . . . . 219
3.6 Verbände und Boolesche Algebren . . . . . 220
3.6.1 Elementare Eigenschaften . . . . . 221

3.6.2 Unterverbände . . . 222
3.6.3 Kongruenzrelationen; Filter und Ideale . . . 222
3.6.4 Vollständige Verbände . . . 225
3.6.5 Distributive und modulare Verbände . . . 227
3.6.6 Boolesche Algebren und Boolesche Ringe . . . 233
3.6.7 Atome . . . 238
3.6.8 Der Darstellungssatz von Stone . . . 241

**4 Universelle Konstruktionen in Varietäten 247**
4.1 Freie Algebren und der Satz von Birkhoff . . . 247
4.1.1 Motivation . . . 247
4.1.2 Bekannte Beispiele und Definition einer freien Algebra . . . 248
4.1.3 Die freie Algebra als homomorphes Bild der Termalgebra . . . 253
4.1.4 Die freie Gruppe . . . 257
4.1.5 Die freie Boolesche Algebra . . . 260
4.1.6 Die freie Algebra als subdirektes Produkt . . . 262
4.1.7 Der Satz von Birkhoff . . . 264
4.2 Koprodukte und Polynomalgebren . . . 265
4.2.1 Bekannte Beispiele und Definition des Koproduktes . . . 265
4.2.2 Konstruktion des Koproduktes als freie Algebra . . . 267
4.2.3 Polynomalgebren . . . 269
4.2.4 Der Gruppenring und Monoidring . . . 273

**5 Teilbarkeit 277**
5.1 Elementare Teilbarkeitslehre . . . 277
5.1.1 Der Fundamentalsatz der Zahlentheorie als Paradigma . . . 277
5.1.2 Teilbarkeit als Quasiordnung auf kommutativen Monoiden . . . 278
5.1.3 Teilbarkeit in Integritätsbereichen . . . 280
5.1.4 Teilbarkeit und Hauptideale – prime und irreduzible Elemente . . . 282
5.2 Faktorielle, Hauptideal- und euklidische Ringe . . . 285
5.2.1 Faktorielle Ringe . . . 285
5.2.2 Hauptidealringe . . . 292
5.2.3 Euklidische Ringe . . . 294
5.3 Anwendungen und Ergänzungen . . . 298
5.3.1 Der Quotientenkörper eines faktoriellen Rings . . . 298
5.3.2 Polynomringe über faktoriellen Ringen sind faktoriell . . . 301
5.3.3 Faktorisierung von Polynomen . . . 304
5.3.4 Symmetrische Polynome . . . 307
5.3.5 Gebrochen rationale Funktionen und ihre Partialbruchzerlegung . . . 312
5.3.6 Interpolation nach Lagrange und nach Newton . . . 314

**6 Körper 317**
6.1 Prim-, Unter- und Erweiterungskörper . . . 317
6.1.1 Primkörper . . . 318

6.1.2 Das Vektorraumargument . . . 320
6.1.3 Algebraische und transzendente Elemente . . . 321
6.1.4 Algebraische Erweiterungen und endliche Dimension . . . 325
6.1.5 Transzendente Körpererweiterungen . . . 327
6.1.6 Anwendung: Konstruierbarkeit mit Zirkel und Lineal . . . 330
6.2 Adjunktion von Nullstellen von Polynomen . . . 334
6.2.1 Adjunktion einer Nullstelle . . . 334
6.2.2 Die Konstruktion von Zerfällungskörpern und algebraischem Abschluss . . . 336
6.2.3 Die Eindeutigkeit von Zerfällungskörpern und algebraischem Abschluss . . . 339
6.2.4 Mehrfache Nullstellen und formale Ableitung . . . 341
6.2.5 Einheitswurzeln und Kreisteilungspolynome . . . 343
6.2.6 Beispiele einfacher Erweiterungen . . . 345
6.3 Endliche Körper (Galoisfelder) . . . 347
6.3.1 Klassifikation endlicher Körper . . . 347
6.3.2 Die Unterkörper eines endlichen Körpers . . . 349
6.3.3 Irreduzible Polynome über endlichen Primkörpern . . . 351
6.3.4 Konstruktion endlicher Körper . . . 355
6.3.5 Der algebraische Abschluss eines endlichen Körpers . . . 358

**7 Vertiefung der Modultheorie 361**
7.1 Wichtige Beispiele: Prüfergruppen und $p$-adische Zahlen . . . 361
7.1.1 Prolog über topologische Algebren und insbesondere Gruppen . . . 362
7.1.2 Beispiel Prüfergruppe . . . 366
7.1.3 Beispiel $p$-adische Zahlen . . . 367
7.1.4 Pontrajaginsche Dualität . . . 372
7.1.5 Der kategorientheoretische Aspekt . . . 374
7.2 Grundbegriffe der Strukturtheorie der Moduln . . . 376
7.2.1 Freie Moduln, Basen und Dimension . . . 376
7.2.2 Dimensionsinvarianz . . . 379
7.2.3 Exakte Sequenzen . . . 381
7.3 Injektive und projektive Moduln . . . 386
7.3.1 Teilbare Gruppen . . . 386
7.3.2 Injektive Moduln . . . 390
7.3.3 Projektive Moduln . . . 391
7.4 Moduln über Hauptidealringen . . . 394
7.4.1 Notationen und Sprechweisen . . . 394
7.4.2 Untermoduln freier Moduln . . . 396
7.4.3 Formulierung des Hauptsatzes und Beweisstrategie . . . 398
7.4.4 Torsionsmoduln . . . 399
7.4.5 Abschluss des Beweises des Hauptsatzes . . . 402
7.4.6 Eine Anwendung des Hauptsatzes: Jordansche Normalformen . . . 403

7.5 Hom-Funktor und Dualität . . . 403
7.5.1 Die abelsche Gruppe $\mathrm{Hom}_R(A, B)$ und der Hom-Funktor . . . 404
7.5.2 Rechts-, Links- und Bimoduln . . . 408
7.5.3 Duale Moduln . . . 409
7.5.4 Das Tensorprodukt . . . 410
7.5.5 Algebren . . . 411

**8 Vertiefung der Gruppentheorie 413**
8.1 Gruppenaktionen und Sylowsätze . . . 413
8.1.1 Gruppenaktionen und allgemeine Klassengleichung . . . 413
8.1.2 Aktion durch Konjugation und spezielle Klassengleichung . . . 416
8.1.3 Folgerungen aus der Klassengleichung und der Satz von Cauchy . . . 417
8.1.4 Die drei Sylow-Sätze . . . 418
8.1.5 Eine Anwendung der Klassengleichung: Der Satz von Wedderburn 420
8.2 Einige konkrete Beispiele . . . 422
8.2.1 Die Beschreibung von Gruppen durch Erzeuger und Relationen . . . 422
8.2.2 Die Diedergruppen $D_n$ . . . 423
8.2.3 Die alternierenden Gruppen $A_n$ . . . 423
8.2.4 Die Quaternionengruppe $Q_8$ und dizyklische Gruppen . . . 424
8.2.5 Zwei weitere Strukturätze . . . 425
8.2.6 Bemerkungen zur Klassifikation endlicher Gruppen . . . 426
8.3 Nilpotenz, Auflösbarkeit und Subnormalreihen . . . 429
8.3.1 Nilpotente Gruppen . . . 429
8.3.2 Auflösbare Gruppen . . . 431
8.3.3 Subnormalreihen . . . 432
8.3.4 Die Sätze von Zassenhaus, Schreier und Jordan-Hölder . . . 433
8.4 Konstruktionen zur Erweiterung von Gruppen . . . 436
8.4.1 Allgemeine Gruppenerweiterungen . . . 437
8.4.2 Semidirekte Produkte . . . 438
8.4.3 Das Kranzprodukt . . . 441
8.5 Direkte Zerlegung: Der Satz von Krull-Schmidt . . . 442
8.5.1 Kettenbedingungen und Formulierung des Satzes . . . 443
8.5.2 Normale Endomorphismen . . . 445
8.5.3 Normale Endomorphismen induzieren direkte Zerlegungen . . . 446
8.5.4 Beweis der Eindeutigkeit . . . 448

**9 Galoistheorie 451**
9.1 Historie und allgemeine Grundkonzepte . . . 451
9.1.1 Historisches . . . 452
9.1.2 Die von einer Relation induzierte Galoiskorrespondenz . . . 453
9.1.3 Abstrakte Galoiskorrespondenzen . . . 454
9.1.4 Beispiele von Galoiskorrespondenzen . . . 456
9.2 Galoissche Körpererweiterungen . . . 459
9.2.1 Die klassische Galoiskorrespondenz . . . 459

9.2.2 Galoissch und algebraisch impliziert normal und separabel . . . . . 462
9.2.3 Normale Erweiterungen . . . . . 463
9.2.4 Separable Erweiterungen . . . . . 466
9.3 Der Hauptsatz der Galoistheorie . . . . . 469
9.3.1 Formulierung des Hauptsatzes für endlichdimensionale Erweiterungen . . . . . 470
9.3.2 Zwei Ungleichungen . . . . . 471
9.3.3 Beweis des Hauptsatzes für endlichdimensionale Erweiterungen . . 474
9.3.4 Der allgemeine Hauptsatz . . . . . 476
9.3.5 Zwei Folgerungen aus dem Hauptsatz . . . . . 479
9.4 Die Galoisgruppe eines Polynoms . . . . . 480
9.4.1 Galoisgruppen als endliche Permutationsgruppen . . . . . 481
9.4.2 Die quadratische Gleichung . . . . . 482
9.4.3 Die Diskriminante . . . . . 483
9.4.4 Die kubische Gleichung . . . . . 486
9.4.5 Die Gleichung vierten Grades . . . . . 488
9.4.6 Die symmetrische Gruppe $S_5$ als Galoisgruppe . . . . . 491
9.5 Auflösung von Gleichungen durch Radikale . . . . . 492
9.5.1 Problemanalyse . . . . . 493
9.5.2 Die Adjunktion reiner Wurzeln . . . . . 494
9.5.3 Radikale Erweiterungen haben auflösbare Galoisgruppen . . . . . 496
9.5.4 Norm und Spur * . . . . . 497
9.5.5 Zyklische und abelsche Erweiterungen * . . . . . 498
9.5.6 Die Rolle der primitiven Einheitswurzeln * . . . . . 500
9.5.7 Kreisteilungskörper und -polynome * . . . . . 501
9.5.8 Nochmals auflösbare Galoisgruppen * . . . . . 503
9.5.9 Auflösbare Galoisgruppen erzwingen Auflösbarkeit durch Radikale *505
9.5.10 Zusammenfassung: Der Satz von Galois . . . . . 506

**10 Kommutative Ringe und Nullstellensatz 507**
10.1 Noethersche Moduln und Ringe . . . . . 507
10.1.1 Kettenbedingungen für Moduln . . . . . 507
10.1.2 Kettenbedingungen für Ringe . . . . . 510
10.1.3 Der Basissatz . . . . . 510
10.1.4 Ein kurzer Einschub über Primideale . . . . . 512
10.1.5 Idealtheorie in Noetherschen Ringen . . . . . 513
10.2 Ganzheit in kommutativen Ringen . . . . . 514
10.2.1 Ganze Elemente und Ringerweiterungen . . . . . 515
10.2.2 Ganzer Abschluss . . . . . 516
10.2.3 Dedekindsche Ringe . . . . . 517
10.2.4 Ein Hauptidealring, der nicht euklidisch ist . . . . . 518
10.3 Der Hilbertsche Nullstellensatz . . . . . 520
10.3.1 Die Ausgangssituation in der algebraischen Geometrie . . . . . 521
10.3.2 Ganze Erweiterungen und Ideale . . . . . 522

10.3.3 Parametrisierung in Ringerweiterungen . . . . . 524
10.3.4 Der kleine Nullstellensatz . . . . . 525
10.3.5 Der volle Nullstellensatz . . . . . 527

**11 Anhang: Mengentheoretische Grundlagen A1**
11.1 Wohlordnungen . . . . . A1
11.1.1 Grundbegriffe . . . . . A1
11.1.2 Transfinite Induktion . . . . . A3
11.1.3 Die „Wohlordnung“ aller Wohlordnungen modulo $\cong$ . . . . . A5
11.2 Definition durch transfinite Rekursion . . . . . A6
11.2.1 Der Rekursionssatz . . . . . A6
11.2.2 Vollständige Induktion auf $\mathbb{N}$ . . . . . A6
11.3 Äquivalenzen des Auswahlaxioms . . . . . A7
11.3.1 Präliminarien . . . . . A7
11.3.2 Formulierung der Äquivalenzen . . . . . A8
11.3.3 Beweis der Äquivalenz der Aussagen in 11.3.2 . . . . . A9
11.3.4 Anwendungen des Auswahlaxioms . . . . . A11
11.4 Ordinal- und Kardinalzahlen . . . . . A12
11.4.1 Ordnungstypen . . . . . A12
11.4.2 Eigenschaften von Ordinalzahlen . . . . . A14
11.4.3 Größenvergleich von Mengen . . . . . A15
11.4.4 Kardinalzahlen . . . . . A16
11.4.5 Operationen für Ordinalzahlen . . . . . A17
11.4.6 Operationen auf Kardinalzahlen . . . . . A17
11.4.7 Von Neumanns Modell von $\mathbb{N}$ . . . . . A18
11.4.8 Unendliche Kardinalzahlarithmetik . . . . . A19
11.5 Axiomatische Mengenlehre . . . . . A22
11.5.1 Vorbemerkungen . . . . . A22
11.5.2 Die Axiome von ZFC . . . . . A23

# 1 Einführung in die algebraische Denkweise

Auf Kapitel 1 wird zwar später gelegentlich zurückgegriffen werden, doch folgt es selbst noch keinem strengen systematischen Aufbau. Dieser beginnt erst mit Kapitel 2. Vorerst sollen anhand möglichst bereits vertrauter Beispiele fundamentale und einfache, gelegentlich aber relativ abstrakte Begriffe, welche die Algebra nach modernem Verständnis durchziehen, ebenfalls vertraut gemacht werden. In Abschnitt 1.1 stehen mengentheoretische Grundlegungen von $\mathbb{N}$, dem System der natürlichen Zahlen im Mittelpunkt. Anhand der vertrauten Erweiterungen der Zahlenbereiche, ausgehend von $\mathbb{N}$ über $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ bis $\mathbb{C}$ wird in Abschnitt 1.2 ein sehr typisches Anliegen der Algebra vorgestellt: die Konstruktion von Strukturen mit gewissen gewünschten Eigenschaften. Dabei treten Homo- und Isomorphismen (strukturverträgliche Abbildungen) deutlich in den Vordergrund. Für den Fall von Vektorräumen ist vieles davon schon aus der Linearen Algebra bekannt und wird in Abschnitt 1.3 nochmals in neuem Lichte rekapituliert.

## 1.1 Die natürlichen Zahlen

Leopold Kronecker (1823–1891) meinte bekanntlich über die Herkunft mathematischer Begriffe, die ganzen Zahlen habe der liebe Gott gemacht, alles andere sei Menschenwerk. Doch gibt es gute Gründe, auch die ganzen und sogar die natürlichen Zahlen (welche Kronecker wohl meinte) genauer zu hinterfragen. Die moderne, stark von der Mengenlehre Georg Cantors (1845–1918) geprägte Mathematik gibt uns einen großzügigen Rahmen dafür. Interpretiert man Kronecker historisch und didaktisch, so kann man seinem berühmten Diktum durchaus Sinnvolles abgewinnen: In der Geschichte der Menschen – sowohl kollektiv als Jahrtausende alte Entwicklung unserer Zivilisation wie auch individuell als psychologisch-intellektuelle Entfaltung des heranwachsenden Menschen – erscheinen, wenn man die Stränge zurück verfolgt, immer wieder die natürlichen Zahlen zusammen mit den elementaren Operationen (Addition, Multiplikation etc.) als die erste und entscheidende Abstraktion und somit als Ausgangspunkt der Mathematik. Gleichzeitig ermöglichen sie einen reizvollen Einstieg in die Welt der Algebra. Ein solcher, selbst noch nicht der Algebra im engeren Sinne zuzuordnen, soll in diesem Abschnitt geboten werden.

In 1.1.1 stellen wir einen mengentheoretisch basierten Zugang zum System $\mathbb{N}$ der natürlichen Zahlen vor. Dabei orientieren wir uns möglichst eng an der Bedeutung natürlicher Zahlen als Kardinalitäten endlicher Mengen, d.h. als Invarianten bezüglich Bijektionen. 1.1.2 bringt einige Bemerkungen zur Induktion als Beweismethode. Die Axiomatisierung von $\mathbb{N}$ durch Giuseppe Peano ist Gegenstand von 1.1.3. In 1.1.4 behandeln wir das in der axiomatischen Mengenlehre zum Standard gewordene Modell von $\mathbb{N}$ nach John von Neumann. In 1.1.5 führen wir die Arithmetik auf $\mathbb{N}$ – ihrer ursprünglichen Bedeutung

entsprechend – auf mengentheoretische Operationen zurück. Damit wird auch der Beweis der grundlegenden Rechenregeln wie Assoziativgesetz etc. sehr einfach. Den Abschnitt beschließen in 1.1.6 einige Bemerkungen zur Darstellung mathematischer Objekte, insbesondere zur Zifferndarstellung natürlicher Zahlen.

### 1.1.1 Natürliche Zahlen als endliche Kardinalitäten

Inhalt in Kurzfassung: Jede natürliche Zahl entspricht einer Klasse untereinander gleichmächtiger endlicher Mengen. Dieser Grundgedanke wird nun mathematisch streng entwickelt.

Es gibt verschiedene Möglichkeiten, die natürlichen Zahlen zu beschreiben; wir beginnen hier mit einem Zugang, der die natürlichen Zahlen als „Größen“ von Mengen beschreibt. Wir verstehen diese Beschreibung der natürlichen Zahlen als „grundlagenorientiert“. Das Ziel ist es nicht, neue Fakten über die natürlichen Zahlen zu entdecken oder zu beweisen; im Gegenteil, wir beweisen hier Tatsachen, die wir eigentlich schon wissen. Ziel dabei ist es, die Rolle der Definitionen und Beweise besser zu verstehen.
Die folgende Definition ist für endliche wie auch für unendliche Mengen sinnvoll:

**Definition 1.1.1.1.** Wenn $A$ und $B$ beliebige Mengen sind, dann schreiben wir $A \approx B$ („$A$ und $B$ sind gleichmächtig“) als Abkürzung für „Es gibt eine bijektive Abbildung zwischen $A$ und $B$.“

$$A \approx B \;\Leftrightarrow\; \exists f\colon A \to B,\ f \text{ bijektiv}$$

Die Relation $\approx$ ist reflexiv, weil die identische Abildung auf jeder Menge bijektiv ist; symmetrisch, weil die Umkehrabbildung einer bijektiven Abbildung wieder bijektiv ist; und transitiv, weil die Verkettung bijektiver Abbildungen ebenfalls bijektiv ist. Also gilt:

**Proposition 1.1.1.2.** *Auf jeder Menge von Mengen ist die Relation $\approx$ eine Äquivalenzrelation.*

Wir konzentrieren uns nun auf die Teilmengen einer beliebigen festen Menge.

**Definition 1.1.1.3.** Sei $M$ eine beliebige Menge. Mit $\mathfrak{P}(M)$ bezeichnen wir die Potenzmenge von $M$, also die Menge aller[1] Teilmengen. Mit $\mathfrak{P}_{\text{fin}}(M)$ bezeichnen wir die Menge aller endlichen Teilmengen von $M$.

Wenn wir den Begriff „endlich“ auch formal (und nicht nur intuitiv und informell) behandeln wollen, kann $\mathfrak{P}_{\text{fin}}(M)$ so definiert werden:

**Definition 1.1.1.4.**

- Wir nennen eine Familie $\mathscr{A} \subseteq \mathfrak{P}(M)$ induktiv, wenn erstens $\emptyset \in \mathscr{A}$ gilt und zweitens für alle $B \in \mathscr{A}$ und alle $x \in M$ auch die Vereinigung $B \cup \{x\}$ in $\mathscr{A}$ liegt.

[1] Insbesondere ist die leere Menge, die wir mit $\emptyset$ oder $\{\}$ bezeichnen, jedenfalls ein Element von $\mathfrak{P}(M)$, ebenso wie die Menge $M$ selbst.

- Dann ist $\mathfrak{P}(M)$ eine induktive Menge, und $\mathfrak{P}_{\text{fin}}(M)$ ist als Durchschnitt aller induktiven Mengen definiert:

$$\mathfrak{P}_{\text{fin}}(M) := \bigcap \{\mathscr{A} \subseteq \mathfrak{P}(M) \mid \mathscr{A} \text{ induktiv}\}$$

  Anders formuliert gilt

$$X \in \mathfrak{P}_{\text{fin}}(M) \;\Leftrightarrow\; \forall \mathscr{A} \subseteq \mathfrak{P}(M) : (\mathscr{A} \text{ induktiv } \Rightarrow X \in \mathscr{A}).$$

- Die Menge $M$ heißt *endlich*, wenn $\mathfrak{P}(M) = \mathfrak{P}_{\text{fin}}(M)$ gilt, und *unendlich* sonst.

Ohne Schwierigkeit macht man sich klar:

**Proposition 1.1.1.5.** *1. Sei $M$ eine beliebige Menge, und $(\mathscr{A}_i : i \in I)$ eine Familie von induktiven Teilmengen von $\mathfrak{P}(M)$. Dann ist auch $\bigcap_i \mathscr{A}_i$ induktiv. Insbesondere ist $\mathfrak{P}_{\text{fin}}(M)$ induktiv.*

*2. Wenn $A \subseteq M$, dann gilt $\mathfrak{P}_{\text{fin}}(A) = \mathfrak{P}_{\text{fin}}(M) \cap \mathfrak{P}(A)$.*

*3. Die Familie $\mathfrak{P}_{\text{fin}}(M)$ besteht genau aus allen endlichen Teilmengen von $M$.*

*4. Hat die leere Menge $\emptyset$ eine gewisse Eigenschaft, die sich von jeder Menge $M$ auf jede Menge der Form $M \cup \{x\}$ ($x$ beliebig) vererbt, so hat jede endliche Menge diese Eigenschaft.*

*5. Sei $M$ eine beliebige Menge. Dann sind die folgenden Aussagen äquivalent:*[2]

- $\mathfrak{P}(M) = \mathfrak{P}_{\text{fin}}(M)$.
- $M \in \mathfrak{P}_{\text{fin}}(M)$.
- *Es gibt ein maximales Element in $\mathfrak{P}_{\text{fin}}(M)$, das heißt: Es gibt $A \in \mathfrak{P}_{\text{fin}}(M)$, sodass es keine echte Obermenge $B \supsetneq A$ in $\mathfrak{P}_{\text{fin}}(M)$ gibt.*
- *Jede nichtleere Teilmenge $\mathcal{E} \subseteq \mathfrak{P}(M)$ hat ein maximales Element.*

**UE 1 ▶ Übungsaufgabe 1.1.1.6.** (V) Beweisen Sie Proposition 1.1.1.5. **◀ UE 1**

**UE 2 ▶ Übungsaufgabe 1.1.1.7.** (B) Sei $E$ eine Eigenschaft, $M$ eine Menge. Um zu zeigen, dass alle Teilmengen $T \subseteq M$ die Eigenschaft $E$ haben, bietet sich folgende „induktive“ Vorgehensweise an: Man zeigt (a) und (b), und schließt daraus (c): **◀ UE 2**

(a) Die leere Menge hat die Eigenschaft $E$.

(b) Für alle $S \subseteq M$ und alle $m \in M$ gilt:
Wenn $S$ die Eigenschaft $E$ hat, dann auch $S \cup \{m\}$.

[2] In dieser wie in den folgenden Aufgaben kann Ihr bereits vorhandenes Wissen über die natürlichen Zahlen als Inspiration dienen; für den Beweis müssen Sie sich aber auf unsere Definition der Endlichkeit beziehen.

(c) Jede Menge $T \subseteq M$ hat die Eigenschaft $E$.

Ist der Schluss „Wenn (a) und (b), dann (c)“ korrekt? Für beliebige Mengen $M$ und beliebige Eigenschaften $E$? Zumindest für beliebige abzählbare Mengen $M$?
Wenn ja, beweisen Sie dies. Wenn nein, finden Sie ein Gegenbeispiel (also eine geeignete Eigenschaft $E$ und Menge $M$).

**Definition 1.1.1.8.** Sei $I$ eine beliebige Menge. Nach Proposition 1.1.1.2 induziert die Relation $\approx$ auf der Menge $\mathfrak{P}_{\text{fin}}(I)$ eine Äquivalenzrelation. Dadurch wird $\mathfrak{P}_{\text{fin}}(I)$ in Klassen gleichmächtiger Mengen partitioniert; die Äquivalenzklasse einer Menge $E \in \mathfrak{P}_{\text{fin}}(I)$ bezeichnen wir mit $[E]_{\approx} = [E]_{\approx,I} := \{D \in \mathfrak{P}_{\text{fin}}(I) : D \approx E\}$. Die Menge aller dieser Äquivalenzklassen bezeichnen wir mit

$$\mathbb{N}_I := \{[E]_{\approx,I} \mid E \in \mathfrak{P}_{\text{fin}}(I)\}.$$

**Lemma 1.1.1.9** (Induktionsprinzip für $\mathbb{N}_I$)**.** *Sei $A \subseteq \mathbb{N}_I$ mit*

- $[\emptyset]_{\approx} \in A$*;*
- *für alle $[B] \in A$ und alle $x \in I$ gilt auch $[B \cup \{x\}]_{\approx} \in A$.*

*Dann ist $A = \mathbb{N}_I$.*

*Beweis.* Die Menge $P := \{B : [B] \in A\}$ ist eine induktive Teilmenge von $\mathfrak{P}_{\text{fin}}(I)$, daher muss $P = \mathbb{N}_I$ gelten. □

**Definition 1.1.1.10.** Seien $I$ und $I'$ beliebige Mengen, $n \in \mathbb{N}_I$, $n' \in \mathbb{N}_{I'}$. Wir schreiben $n \sim n'$, wenn es $E \in n$, $E' \in n'$ mit $E \approx E'$ gibt. (Äquivalent: Wenn für alle $E \in n$ und alle $E' \in n'$ gilt: $E \approx E'$.)

**Lemma 1.1.1.11.** *Wenn $I$ und $I'$ unendlich sind, dann gibt es (genau) eine Bijektion $\iota\colon \mathbb{N}_I \to \mathbb{N}_{I'}$, die*

$$\forall n \in \mathbb{N}_I : \ \iota(n) \sim n$$

*erfüllt.*

**UE 3** ► **Übungsaufgabe 1.1.1.12.** (V) Beweisen Sie Lemma 1.1.1.11. (Zeigen Sie insbesondere, dass $\iota$ wohldefiniert, injektiv und surjektiv ist.) ◄ **UE 3**

Die Abbildung $\iota$ ordnet also jeder Äquivalenzklasse $n$ gleichmächtiger Teilmengen von $I$ die Äquivalenzklasse jener Teilmengen von $I'$ zu, die gleichmächtig mit den Elementen von $n$ sind. Zum Beispiel wird der Klasse aller 1-elementigen Teilmengen von $I$ die Klasse alle 1-elementigen Teilmengen von $I'$ zugeordnet.
Wir benötigen im Folgenden einige wichtige Eigenschaften von endlichen Mengen, die alle auf Grundlage der gerade gegebenen Definition beweisbar sind.

**Lemma 1.1.1.13.**

(1) *Wenn $E \subseteq F$ gilt, und $F$ endlich ist, dann auch $E$.*

(2) *Für $E \approx E'$ durch eine Bijektion $f\colon E \to E'$ bezeugt wird, dann induziert $f$ eine natürliche Bijektion zwischen $\mathfrak{P}(E)$ und $\mathfrak{P}(E')$; die Einschränkung dieser Bijektion auf $\mathfrak{P}_{\text{fin}}(E)$ liefert eine Bijektion $g$ zwischen $\mathfrak{P}_{\text{fin}}(E)$ und $\mathfrak{P}_{\text{fin}}(E')$, die überdies mit der Relation $\approx$ verträglich ist (das heißt: $A_1 \approx A_2$ impliziert $g(A_1) \approx g(A_2)$).*

(3) *Wenn $E$ endlich ist, dann ist auch $E \cup \{a\}$ endlich. (Wenn $a \in E$ gilt, dann ist das trivial, also ist diese Aussage nur für $a \notin E$ interessant.)*

(4) *Wenn $E$ und $E'$ endliche Mengen sind, dann ist auch die Vereinigungsmenge $E \cup E'$ endlich. (Sie dürfen ohne Beschränkung der Allgemeinheit annehmen, dass $E$ und $E'$ disjunkt sind. Warum?)*

(5) *Wenn $E$ und $E'$ endliche Mengen sind, dann ist auch die Produktmenge $E \times E'$ endlich.*

(6) *Zu beliebigen Mengen $A$, $B$ gibt es eine Menge $B'$, die zu $A$ disjunkt und zu $B$ gleichmächtig ist.*

**UE 4** ► **Übungsaufgabe 1.1.1.14.** (V) Beweisen Sie Lemma 1.1.1.13; verwenden Sie dabei unsere Definition 1.1.1.4. Für die meisten Aufgaben werden Sie Induktion verwenden müssen. Geben Sie jeweils explizit die Menge an, von der Sie zeigen, dass sie 0 enthält und unter der Nachfolgeroperation abgeschlossen ist. (Etwa in Punkt (4): Für jede endliche Menge $E$ sei $A_E$ die Menge aller $n \in \mathbb{N}$ mit der Eigenschaft „Für alle $E'$ mit $E' \approx n$ ist $E \cup E'$ endlich.“)
(Hinweis zu (6): Betrachten Sie die Menge $\{A\} \times B$. Kann sie ein Element von $A$ enthalten?) ◄ **UE 4**

### 1.1.2 Bemerkungen zu Induktionsbeweisen

Inhalt in Kurzfassung: Wir erläutern hier verschiedene Möglichkeiten, wie man das Induktionsprinzip in Beweisen einsetzen kann.

*Bemerkung* 1.1.2.1. Um eine Aussage $\forall x \in \mathbb{N} : \psi(x)$ zu beweisen, genügt es, zu zeigen, dass die Menge $M := \{n \in \mathbb{N} : \psi(n)\}$ erstens die Zahl 0 enthält und zweitens unter der Nachfolgeroperation $x \mapsto x + 1$ abgeschlossen ist.
Wenn eine Aussage $\forall x \in \mathbb{N}\ \forall y \in \mathbb{N} : \varphi(x, y)$ (wie etwa das Kommutativgesetz der Addition) mit Induktion zu beweisen ist, dann bieten sich verschiedene Möglichkeiten an:

- „Induktion mit Parameter“: Wir halten einen (beliebigen) Wert $b \in \mathbb{N}$ fest, und beweisen dann die Aussage $\forall x \in \mathbb{N} : \varphi(x, b)$ mit Induktion „nach $x$“. Das heißt, wir zeigen, dass für jedes $b \in \mathbb{N}$ die Menge

  $$M_b := \{x \in \mathbb{N} \mid \varphi(x, b)\}$$

  sowohl die Zahl 0 enthält als auch unter Nachfolgern abgeschlossen ist.

- „Simultane Induktion“: Wir setzen $\psi(x) := \forall y : \varphi(x, y)$, und beweisen die Formel $\forall x : \psi(x)$ mit Induktion „nach $x$“. Das heißt, wir zeigen, dass die Menge

$$M := \{x \in \mathbb{N} \mid \forall y : \varphi(x, y)\}$$

  sowohl die Zahl 0 enthält als auch unter Nachfolgern abgeschlossen ist.

- „Induktion nach dem Maximum“: Wir setzen $\psi(z) := \forall x \leq z\ \forall y \leq z : \varphi(x, y)$, und beweisen die Formel $\forall z : \psi(z)$ mit Induktion „nach $z$“. Das heißt, wir zeigen, dass die Menge

$$M := \{z \in \mathbb{N} \mid \forall x \leq z\ \forall y \leq z : \varphi(x, y)\}$$

  sowohl die Zahl 0 enthält als auch unter Nachfolgern abgeschlossen ist.

Diese Liste ist nicht vollständig. Man könnte zum Beispiel auch „Induktion nach der Summe“ betrachten.
Man beachte, dass man bei Parameter-Induktion im Induktionsschritt $\varphi(n, b) \Rightarrow \varphi(n + 1, b)$ nur die Voraussetzung $\varphi(n, b)$ verwenden darf; bei simultaner Induktion kann man hingegen für den Beweis von $\varphi(n + 1, y)$ bereits $\forall z\ \varphi(n, z)$ verwenden.

Es kommt gelegentlich vor, dass man sich den Induktionsschritt $\varphi(x) \Rightarrow \varphi(x+1)$ dadurch erleichtern kann, dass man $\varphi$ durch eine stärkere Aussage $\varphi'$ ersetzt. Die Implikation $\varphi'(x) \to \varphi'(x+1)$ könnte nämlich wegen der stärkeren Voraussetzung leichter zu beweisen sein.
Ein Spezialfall dieser Variante ist die „Verlaufsinduktion“:

**Lemma 1.1.2.2.** *Sei $\varphi(x)$ eine Formel. Wir setzen $\varphi_{\leq}(x) := \forall y \in \mathbb{N} : (y \leq x \Rightarrow \varphi(x))$ und $\varphi_{<}(x) := \forall y \in \mathbb{N} : (y < x \Rightarrow \varphi(x))$. Dann sind die folgenden Aussagen äquivalent:*

- $\forall x \in \mathbb{N} : \varphi(x)$.
- $\forall x \in \mathbb{N} : \varphi_{\leq}(x)$.
- $\forall x \in \mathbb{N} : \varphi_{<}(x)$.

*Bemerkung* 1.1.2.3. (1) Für einen Induktionsbeweis von $\forall x \in \mathbb{N} : \varphi_{<}(x)$ ist kein „Induktionsanfang“ notwendig, denn $\varphi_{<}(0)$ gilt trivialerweise.

(2) Im Induktionsschritt für die erste Aussage muss man

$$(*)_1 \qquad \varphi(x) \Rightarrow \varphi(x + 1)$$

beweisen. Für die zweite Aussage hingegen muss man

$$(*)_2 \qquad \varphi_{\leq}(x) \Rightarrow \varphi_{\leq}(x + 1)$$

beweisen, was leicht aus

$$(*)'_2 \qquad \varphi_{\leq}(x) \Rightarrow \varphi(x + 1)$$

folgt. Da die Voraussetzung in $(*)'_2$ stärker als die in $(*)_1$ ist, ist $(*)'_2$ oft leichter beweisbar als $(*)_1$.

**UE 5 ► Übungsaufgabe 1.1.2.4.** Für die Addition auf $\mathbb{N}$ gilt **◄ UE 5**

(1) $\forall x : x + 0 = x$.

(2) $\forall x, y : (x + y) + 1 = x + (y + 1)$.

Zeigen Sie (nur unter Verwendung dieser Axiome, plus Induktion):

(a) $\forall y : 0 + y = y$ (insbesondere gilt also $0 + 1 = 1$).

(b) $\forall x \forall y : x + y = y + x$.

Geben Sie bei jedem Induktionsbeweis an, von welcher Menge Sie zeigen, dass sie 0 enthält und unter Nachfolgern abgeschlossen ist.

### 1.1.3 Axiomatisierung nach Peano

Inhalt in Kurzfassung: Die wesentlichen Eigenschaften des (unendlichen) Systems $\mathbb{N}$ der natürlichen Zahlen lassen sich durch einige wenige Forderungen erfassen. Hier wird im Wesentlichen (nicht in der Formalisierung) der berühmte Zugang von Peano gewählt. Dass er das Gewünschte leistet, wird durch einen Eindeutigkeitssatz illustriert.

Wir nehmen im Folgenden an, dass es eine unendliche Menge $I$ gibt, und wir schreiben $\mathbb{N}_I$ für die Menge aller $\approx$-Äquivalenzklassen von $\mathfrak{P}_{\text{fin}}(I)$. Wegen Lemma 1.1.1.11 lassen wir aber den Index $I$ gelegentlich weg, da sich Aussagen über $\mathbb{N}_I$ für eine beliebige andere unendliche Menge $I'$ leicht in entsprechende Aussagen $\mathbb{N}_{I'}$ übersetzen lassen.
Wir schreiben 0 oder $0_I$ für die Äquivalenzklasse der leeren Menge, und 1 oder $1_I$ für die Äquivalenzklasse aller einelementigen Mengen $\{x\} \subseteq I$. Im Sinne der natürlichen Ordnung auf $\mathbb{N}_I$ (siehe Definition 1.1.5.11 und Lemma 1.1.5.15) ist 1 der Nachfolger von 0.
Allgemeiner kann man jeder Äquivalenzklasse $n = [C]_\approx$ ihren „Nachfolger“ $\nu(n)$ zuordnen, nämlich die Äquivalenzklasse

$$\nu([C]) := [C \cup \{d\}]_\approx$$

für beliebiges $d \in I \setminus C$. (Man sieht leicht, dass $\nu$ wohldefiniert ist, d.h., dass diese Definition nicht von der Wahl des Repräsentanten $C$ abhängt.)
Es gelten die folgenden Aussagen (wobei wir den Index $I$ unterdrücken):

**Lemma 1.1.3.1.**

(1) $0 \in \mathbb{N}$.

(2) *Für alle* $n \in \mathbb{N}$ *ist auch* $\nu(n) \in \mathbb{N}$.

(3) *Die Abbildung* $\nu\colon \mathbb{N} \to \mathbb{N}$ *ist injektiv: Aus* $\nu(n) = \nu(k)$ *folgt* $n = k$.

(4) *Für alle* $n \in \mathbb{N}$ *gilt:* $\nu(n) \neq 0$.

(5) *Für jede Teilmenge* $T \subseteq \mathbb{N}$ *gilt:*

*Wenn* $0 \in T$,
*und für alle* $n \in \mathbb{N}$ *die Implikation* $(n \in T \Rightarrow \nu(n) \in T)$ *gilt,*
*dann ist* $T = \mathbb{N}$.

*Beweis.* (3) Aus der Existenz einer Bijektion $f\colon C \cup \{c\} \to D \cup \{d\}$ (mit $c \notin C$, $d \notin D$) ist auf die Existenz einer Bijektion $g\colon C \to D$ zu schließen.
Wenn $f(c) = d$ gilt, dann ist die Einschränkung[3] $g := f\restriction C$ bereits die gewünschte Bijektion; andernfalls sei $d' = f(c)$ und $c' := f^{-1}(d)$. Dann gilt sicher $d' \neq d$, also $d' \in D$, analog $c' \in C$. Wir definieren $g(c') := d'$, und $g\restriction(C \setminus \{c'\}) = f\restriction(C \setminus \{c'\})$ und erhalten wieder eine Bijektion $g\colon C \to D$.

(5) Sei $T \subseteq \mathbb{N}$. Wir nehmen $0 \in T$ und $\forall n \in \mathbb{N} : (n \in T \to \nu(n) \in T)$ an und betrachten die Menge $M := \{C \in \mathfrak{P}_{\text{fin}}(I) : [C]_{\approx} \in T\}$. Dann ist $M$ induktiv. Daher muss $M = \mathfrak{P}_{\text{fin}}(I)$ gelten, woraus wir $T = \mathbb{N}$ folgern können.

□

**Definition 1.1.3.2.** Sei $M$ eine Menge, $0_M$ ein Element, $\nu_M$ eine Funktion mit Definitionsbereich $M$. Wir nennen $(M, 0_M, \nu_M)$ eine *Peano-Struktur*, wenn die sogenannten *Peano-Axiome* [4], das sind die (entsprechend umformulierten) Eigenschaften aus Lemma 1.1.3.1, erfüllt sind:

(1) $0_M \in M$.

(2) $\nu_M\colon M \to M$, d.h.: für alle $n \in M$ ist auch $\nu_M(n) \in M$.

(3) Die Abbildung $\nu_M$ ist injektiv: Aus $\nu_M(n) = \nu_M(k)$ folgt $n = k$.

(4) Für alle $n \in M$ gilt: $\nu_M(n) \neq 0_M$.

(5) Für jede Teilmenge[5] $T \subseteq M$ gilt:

Wenn $0 \in T$,
und für alle $n \in M$ die Implikation $(n \in T \Rightarrow \nu_M(n) \in T)$ gilt,
dann ist $T = M$.

[3] Wir verwenden sowohl die Schreibweise $f|_T$ als auch $f\restriction T$ für die Einschränkung $f \cap (T \times B)$ einer Funktion $f : A \to B$ auf die Teilmenge $T \subseteq A$.

[4] Giuseppe Peano formulierte diese Axiome 1889. In Peanos Version beginnen die natürlichen Zahlen allerdings mit 1, nicht mit 0. Dieser Unterschied ist für unsere Überlegungen aber nicht relevant.

Die Frage, ob 0 eine „natürliche“ Zahl ist, ist keine mathematische. Es ist offensichtlich, dass sowohl die Menge $\{0, 1, 2, \ldots\}$ der endlichen Kardinalzahlen also auch die Menge $\{1, 2, \ldots\}$ der beim Zählen verwendeten Zahlen in der Mathematik eine wichtige Rolle spielen; welche dieser Mengen das Prädikat „natürlich“ erhält, ist aus mathematischer Sicht egal. Dass wir 0 zu den natürlichen Zahlen rechnen, erweist sich erstens in der Algebra oft als zweckmäßig und stimmt zweitens mit internationalen und österreichischen Normen überein, siehe ÖNORM EN ISO 80000-2.

[5] Man beachte, dass diese letzte Forderung nicht über *Elemente* der betrachteten Struktur (also: über natürliche Zahlen) quantifiziert, sondern über *Teilmengen* der betrachteten Struktur, also über Mengen von natürlichen Zahlen. Die Sprache, in der dieses Axiom formuliert ist, nennt man daher „Logik zweiter Stufe“; in „Logik erster Stufe“ beziehen sich die Quantoren $\forall$ und $\exists$ immer nur auf Elemente einer Struktur.

Es gibt eine schwächere, erststufige Variante der Peano-Axiome, mit der wir uns hier aber nicht beschäftigen werden. Solche Axiome ließen Spielraum für so genannte *Nonstandardmodelle* der natürlichen Zahlen, die zu $\mathbb{N}$ nicht isomorph sind. Diesbezüglich Interessierte seien auf die mathematische Logik verwiesen.

Lemma 1.1.3.1 besagt, dass die Struktur $(\mathbb{N}_I, \nu_I, 0_I)$ eine Peano-Struktur ist. Tatsächlich aber enthalten die fünf Peano-Axiome in einem gewissen Sinn alle wesentliche Information über die natürlichen Zahlen. Diese noch etwas vage Behauptung wollen wir nun präzisieren.
In den Peano-Axiomen steckt sicherlich dann die wesentliche Information über die natürlichen Zahlen, wenn jede Peano-Struktur $(M, 0_M, \nu_M)$ im Sinne von Definition 1.1.3.2 zu $(\mathbb{N}, 0, \nu)$ strukturgleich ist. Dies wiederum bedeutet, dass die Elemente von $M$ in bijektiver und kanonischer Weise den natürlichen Zahlen entsprechen, in mathematischer Terminologie: Es gibt einen *Isomorphismus*, d.h. genauer eine bijektive Abbildung $\varphi\colon \mathbb{N} \to M$, mit

- $\varphi(0) = 0_M$, und
- $\varphi(\nu(n)) = \nu_M(\varphi(n))$ für alle $n \in \mathbb{N}$, also $\varphi \circ \nu = \nu_M \circ \varphi$.

$$\begin{array}{ccc} \mathbb{N} & \xrightarrow{\nu} & \mathbb{N} \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi} \\ M & \xrightarrow[\nu_M]{} & M \end{array}$$

In diesem Fall heißen $(\mathbb{N}, 0, \nu)$ und $(M, 0_M, \nu_M)$ *isomorph*, symbolisch

$$(\mathbb{N}, 0, \nu) \cong (M, 0_M, \nu_M).$$

Der Begriff des Isomorphismus ist zentral in der Algebra, muss aber natürlich an die jeweilige Situation angepasst werden. Im vorliegenden Fall geht es nur um die sogenannte *Verträglichkeit* mit Nullelement 0 und Nachfolgerfunktion $\nu$. Schon im vorliegenden einführenden Kapitel werden wir Isomorphismen in vielen anderen Varianten verwenden und davon ausgehen, dass aus dem Kontext klar ist, was genau jeweils damit gemeint ist. Systematisch werden wir in 2.1.5 darauf zurück kommen.

**UE 6** ► **Übungsaufgabe 1.1.3.3.** (F) Begründen Sie: Ist jedes Modell der Peano-Axiome isomorph zu $(\mathbb{N}, 0, \nu)$, so sind auch je zwei beliebige Modelle der Peano-Axiome zueinander isomorph. ◄ **UE 6**

Tatsächlich gilt die folgende Eindeutigkeitsaussage modulo Isomorphie, die uns berechtigt, irgendeine der so konstruierten Mengen $\mathbb{N}_I$ zur Definition der natürlichen Zahlen zu verwenden.

**Theorem 1.1.3.4.** Sei $(M, 0_M, \nu_M)$ eine beliebige Peano-Struktur, so gilt

$$(\mathbb{N}, 0, \nu) \cong (M, 0_M, \nu_M).$$

Der zugehörige Isomorphismus $\varphi\colon \mathbb{N} \to M$ ist eindeutig bestimmt.

Einsichtig ist dies sofort, weil die Rekursion $\varphi(0) = 0_M$, $\varphi(n+1) = \nu_M(\varphi(n))$ tatsächlich einen eindeutigen Isomorphismus $\varphi_M$ definiert. Streng genommen beruht dies auf dem *Rekursionssatz*. Eine sehr allgemeine Version kann man im Anhang (Kapitel 11, 11.2.1.2) nachschlagen. Hier genügt die klassische Formulierung:

**Theorem 1.1.3.5.** Sei $X$ eine Menge, $x_0 \in X$ und $f : X \to X$. Dann gibt es genau eine Abbildung $\varphi : \mathbb{N} \to X$ (so etwas nennt man bekanntlich eine *Folge* in $X$) mit der Eigenschaft $\varphi(0) = x_0$ und $\varphi(\nu(n)) = f(\varphi(n))$ für alle $n \in \mathbb{N}$.

**UE 7 ► Übungsaufgabe 1.1.3.6.** (W) Beweisen Sie Theorem 1.1.3.5, indem Sie folgende Sachverhalte überprüfen. **◄ UE 7**

1. Bezeichne $T$ die Menge aller $n \in \mathbb{N}$ mit der Eigenschaft, dass es eine eindeutige Abbildung $\varphi_n : \mathbb{N}_{<n} := \{k \in \mathbb{N} : k < n\} \to M$ mit folgenden Eigenschaften gibt:
   - Ist $0 \in \mathbb{N}_{<n}$, so gilt $\varphi_n(0) = 0_M$;
   - sind $k, k+1 \in \mathbb{N}_{<n}$, so gilt $\varphi_n(k+1) = \nu_M(\varphi_n(k))$.

   Zeigen Sie: $0 \in T$ und $n \in T$ impliziert $n+1 \in T$.

2. Aus dem Induktionsprinzip auf $\mathbb{N}$ folgt $T = \mathbb{N}$, also ist $\varphi_n$ für alle $n \in \mathbb{N}$ eindeutig definiert. Zeigen Sie, dass die Vereinigung $\varphi := \bigcup_{n\in\mathbb{N}} \varphi_n$ erstens eine Funktion ist, und zweitens der gesuchte Isomorphismus ist. (Hinweis: Zeigen Sie $k < n \Rightarrow \varphi_k \subseteq \varphi_n$.)

**UE 8 ► Übungsaufgabe 1.1.3.7.** (W) Verwenden Sie den Rekursionssatz 1.1.3.5, um die Eindeutigkeit von Peanostrukturen im Sinne von Theorem 1.1.3.4 zu beweisen. **◄ UE 8**

**UE 9 ► Übungsaufgabe 1.1.3.8.** (B) Illustrieren Sie für die Peano-Axiome[6] (3)-(5), dass nicht darauf verzichtet werden kann, ohne dadurch die Eindeutigkeit der beschriebenen Struktur zu verlieren. Finden Sie dazu für $j = 3, 4, 5$ eine Menge $M^{(j)}$, ein Element $0_{M^{(j)}}$ und eine Funktion $\nu_{M^{(j)}}$, so dass $(M^{(j)}, 0_{M^{(j)}}, \nu_{M^{(j)}})$ alle Peano-Axiome erfüllt außer $(j)$. **◄ UE 9**

Ein alternativer, stärker mengentheoretisch orientierter Zugang zu den natürlichen Zahlen stammt von Richard Dedekind (1831-1916): Sei $M$ eine Menge und $f : M \to M$ injektiv aber nicht surjektiv. Dann erhält man eine Peanostruktur wie folgt: Weil $f$ nicht surjektiv ist, gibt es ein $m_0 \in M \setminus f(M)$. Wir setzen $0_M := m_0$ und nennen eine Teilmenge $T \subseteq M$ Dedekind-induktiv, wenn $m_0 \in T$ und aus $m \in T$ stets $f(m) \in T$ folgt. Sei $\mathbb{N}_M$ der Schnitt aller Dedekind-induktiven Teilmengen von $M$, außerdem $\nu_M := f{\restriction}\mathbb{N}_M$ die Einschränkung von $f$ auf $\mathbb{N}_M$. Dann erweist sich $(\mathbb{N}_M, 0_M, \nu_M)$ als Peano-Struktur.

**UE 10 ► Übungsaufgabe 1.1.3.9.** (V) Führen Sie alle zugehörigen Überlegungen zum gerade beschriebenen Dedekindschen Zugang im Detail durch. **◄ UE 10**

[6] Die Axiome (1) und (2) besagen genau, dass eine Peano-Struktur stets eine Algebra im Sinne von Definition 2.1.3.2 ist, was wir auch in dieser Aufgabe jedenfalls fordern wollen.

### 1.1.4 Das von Neumannsche Modell

Inhalt in Kurzfassung: Ein mengentheoretisches Modell für die Peanoaxiome (siehe vorangegangener Unterabschnitt) wurde von John von Neumann angegeben. Es hat für sich reizvolle Eigenschaften, zeigt aber vor allem, dass die Mengenlehre mindestens so stark ist wie die Peanoarithmetik (in Wahrheit sogar stärker).

Die scheinbare Abhängigkeit der natürlichen Zahlen $\mathbb{N}_I$ von einem willkürlichen Parameter $I$ mag als ein ästhetischer Mangel unserer Definition erscheinen.
Warum beschränken wir uns etwa in der Definition der Zahl 1 auf jene Mengen $\{a\}$, für die $a \in I$ (mit festem $I$) gilt, bei der Definition der Zahl 2 auf jene Mengen $\{a, b\}$, die (neben $a \neq b$) auch $a, b \in I$ erfüllen, etc? Könnten wir nicht eine Menge $M$ als „induktiv“ definieren, wenn erstens $\emptyset \in M$ gilt, und zweitens für alle $C \in M$ und beliebiges $x \notin C$ auch $C \cup \{x\} \in M$? Der Durchschnitt aller induktiven Mengen wäre dann immer noch induktiv und würde (modulo der Relation $\approx$) auch ein Modell der natürlichen Zahlen liefern, wäre also insbesondere isomorph zu $\mathbb{N}_I$ und würde die Peano-Axiome erfüllen.
So eine Konstruktion lässt sich (auf Basis der mengentheoretischen Axiome ZFC, siehe Anhang) aber nicht durchführen, da so eine Menge $M$ insbesondere *alle* Singletons $\{a\}$ enthalten müsste, und damit, vereinfacht gesprochen, zu groß wäre. Man kann (aus den ZFC-Axiomen) sogar beweisen, dass es so eine Menge nicht geben kann.
Da wir aber ohnehin nach der Relation $\approx$ ausfaktorisieren, d.h. zur Menge der Äquivalenzklassen übergehen wollen, erweist es sich als gar nicht nötig, *alle* Repräsentanten einer Äquivalenzklasse (z.B. alle Singletons) in unserer gesuchten Menge unterzubringen.
Die folgende Konstruktion, die auf John von Neumann (1903–1957) zurückgeht, geht noch weiter und sucht in jeder Äquivalenzklasse (bezüglich $\approx$) einen *einzigen* Repräsentanten. In diesem System wird die Rolle der Zahl 0 von der leeren Menge übernommen:

$$0_{\mathrm{vN}} := \emptyset$$

Die Zahl 1 wird durch eine einzige Menge der Form $\{a\}$ repräsentiert; eine kanonische Wahl von $a$ ergibt sich durch[7] die Definition $a := 0_{\mathrm{vN}}$:

$$1_{\mathrm{vN}} := \{0_{\mathrm{vN}}\}$$

Ein Repräsentant der Zahl 2 ist eine Menge der Form $\{x, y\}$, wobei wir garantieren müssen, dass $x \neq y$ gilt; es bietet sich an, $x := 0_{\mathrm{vN}}$ und $y := 1_{\mathrm{vN}}$ zu wählen, etc.

$$2_{\mathrm{vN}} := \{0_{\mathrm{vN}}, 1_{\mathrm{vN}}\},\ 3_{\mathrm{vN}} := \{0_{\mathrm{vN}}, 1_{\mathrm{vN}}, 2_{\mathrm{vN}}\},\ \ldots$$

Um klarzustellen, was „. . . “ hier bedeutet, gehen wir so vor:

**Definition 1.1.4.1.** Ein System $S$ von Mengen mit $\emptyset \in S$ heißt vN-induktiv, falls zu jedem $s \in S$ auch $s' := s \cup \{s\}$ in $S$ liegt.

[7] Man beachte, dass die Menge $\emptyset$ zwar leer ist, die Menge $\{\emptyset\}$ aber nicht, weil sie definitionsgemäß ein Element enthält. Daraus folgt auch, dass die Mengen $\emptyset$ und $\{\emptyset\}$ verschieden sind.

Man sieht leicht, dass ein vN-induktives System $S$ jedenfalls die Elemente $0_{\text{vN}}, 1_{\text{vN}}, 2_{\text{vN}}, \ldots$ enthalten muss.
Das Unendlichkeitsaxiom der Mengenlehre (siehe Kapitel 11, insbesondere Abschnitt 11.5.2) garantiert die Existenz vN-induktiver Mengen. Die Menge $\mathbb{N}$ der natürlichen Zahlen (im Sinne der von Neumannschen Konstruktion) ist definiert als

$$\mathbb{N}_{\text{vN}} := \bigcap \{S : \ S \text{ ist vN-induktiv}\}.$$

**UE 11** ► **Übungsaufgabe 1.1.4.2.** (F+) Zeigen Sie, dass der Schnitt vN-induktiver Mengen (insbesondere also die Menge $\mathbb{N}_{\text{vN}}$) vN-induktiv ist. ◄ **UE 11**

**Theorem 1.1.4.3.** Die Struktur $(\mathbb{N}_{\text{vN}}, 0_{\text{vN}}, \nu_{\text{vN}})$ (genannt das *Modell von John von Neumann*) mit $\nu_{\text{vN}} \colon \mathbb{N}_{\text{vN}} \to \mathbb{N}_{\text{vN}}$, $n \mapsto n \cup \{n\}$, ist isomorph zu $(\mathbb{N}_I, 0_I, \nu_I)$ für jede unendliche Menge $I$ (und daher ein Modell der Peano-Axiome).

*Beweisskizze.* Nach dem Rekursionssatz 1.1.3.5 gibt es genau eine Abbildung $\varphi \colon N_I \to \mathbb{N}_{\text{vN}}$, die $\varphi(0_I) = 0_{\text{vN}}$ und
$\varphi(\nu_I(n)) = \nu_{\text{vN}}(\varphi(n))$ für alle $n \in \mathbb{N}_I$ erfüllt.
Mit Induktion zeigt man, dass $C \approx \varphi([C])$ für alle $C \in \mathfrak{P}_{\text{fin}}(I)$ gilt. Daraus folgt die Injektivität von $\varphi$.
Da die Bildmenge induktiv ist, muss $\varphi$ surjektiv sein. □

Zwar haben wir noch nicht über Axiomatisierungen der Mengenlehre, etwa durch das Axiomensystem ZFC (siehe Abschnitt 11.5 im Anhang) gesprochen, doch sei an dieser Stelle auf folgende Konsequenz von Theorem 1.1.4.3 hingewiesen: Ist eine Mengenlehre, in der das Modell der natürlichen Zahlen von John von Neumann konstruiert werden kann, widerspruchsfrei, so sind auch die Peanoaxiome widerspruchsfrei. Analoges gilt auch für die nun folgende Ausweitung um die arithmetischen Operationen zur Peano-Arithmetik.

### 1.1.5 Arithmetik und Ordnung der natürlichen Zahlen

Inhalt in Kurzfassung: In den bisher behandelten Peanoaxiomen war von einer Nachfolgerfunktion die Rede, nicht jedoch von Addition, Multiplikation und Ordnung auf $\mathbb{N}$. Diese Anreicherungen der Struktur sollen nun, wieder auf mengentheoretischer Grundlage, erfolgen. Außerdem werden die wichtigsten Rechenregeln für natürliche Zahlen hergeleitet.

**Satz 1.1.5.1.** *Sei $I$ unendlich, $n, k \in \mathbb{N}_I$. Dann gibt es*

- *disjunkte Mengen $A, B \in \mathfrak{P}_{\text{fin}}(I)$ mit $n = A/\!\approx$, $k = B/\!\approx$; für jede solche Wahl von $A$ und $B$ gilt dann auch $A \cup B \in \mathfrak{P}_{\text{fin}}(I)$.*
- *eine Menge $C \in \mathfrak{P}_{\text{fin}}(I)$ mit $C \approx A \times B$*

- *eine Menge $D \in \mathfrak{P}_{\text{fin}}(I)$ mit $D \approx B^A$. (Wir schreiben[8] $B^A$ für die Menge aller Funktionen von $A$ nach $B$.)*

**UE 12 ► Übungsaufgabe 1.1.5.2.** Beweisen Sie Satz 1.1.5.1. **◄ UE 12**

Dieser Satz erlaubt uns, arithmetische Operationen auf der Menge $\mathbb{N}_I$ zu definieren:

**Definition 1.1.5.3.** Sei $I$ eine unendliche Menge, $A, B \in \mathfrak{P}_{\text{fin}}(I)$.
Wir definieren

$$\begin{aligned} [A]_\approx + [B]_\approx &:= [A \cup B]_\approx \quad \text{(sofern } A \text{ und } B \text{ disjunkt sind)} \\ [A]_\approx \cdot [B]_\approx &:= [A \times B]_\approx \\ [B]_\approx^{[A]_\approx} &:= [B^A]_\approx \end{aligned}$$

Bei diesen Definitionen ist ein Aspekt, nämlich *Wohldefiniertheit*, entscheidend in einer Weise, die uns durch die ganze Algebra begleiten wird. Und zwar werden Operationen (oder allgemeiner Funktionen; hier sind es Addition, Multiplikation und Exponentiation) auf einer Menge von Klassen definiert, indem man mit ihren Elementen bereits bekannte Operationen (hier: die Konstruktion von Vereinigungen, kartesischen Produkte und Mengen von Funktionen) anwendet. A priori wäre es denkbar, dass verschiedene Elemente der Klassen zu verschiedenen Ergebnissen führen. Wohldefiniertheit bedeutet hier, dass genau das nicht eintreten kann. Beim in der Algebra besonders wichtigen Begriff der *Kongruenzrelation* (siehe Definition 2.3.3.1) spielt ebenfalls diese Art von Wohldefiniertheit die zentrale Rolle.

**UE 13 ► Übungsaufgabe 1.1.5.4.** (V) Zeigen Sie, dass $n + k$, $n \cdot k$ und $n^k$ wohldefiniert sind. **◄ UE 13**
(Bevor Sie den Beweis beginnen, geben Sie etwas ausführlicher an, was überhaupt zu zeigen ist, etwa in der Form „Zu zeigen ist: Für alle $X$ gilt: wenn ... dann ...“.)

Man kann leicht zeigen, dass die üblichen Rechengesetze für die Elemente von $\mathbb{N}_I$ gelten, zum Beispiel:

**Lemma 1.1.5.5.** *Die Addition ist eine kommutative Operation auf den natürlichen Zahlen.*

*Beweis.* Sei $k + l = j$. Das heißt, dass es disjunkte Mengen $K$ und $L$ gibt mit $[K]_\approx = k$, $[L]_\approx = l$, und mit $[K \cup L]_\approx = j$,
Dann ist aber $l+k$ definitionsgemäß die $\approx$-Äquivalenzklasse der Menge $L \cup K$: $[L \cup K]_\approx = l + k$. Wegen $L \cup K = K \cup L$ erhalten wir $l + k = [L \cup K]_\approx = [K \cup L]_\approx = k + l$ . □

[8] Wir identifizieren Funktionen mit ihren Graphen; eine Funktion von $A$ nach $B$ ist also eine Menge $f$, die erstens eine Teilmenge von $A \times B$ ist, und die zweitens die Eigenschaft hat, dass es für jedes $x \in A$ genau ein $y \in B$ gibt, welches $(x, y) \in f$ erfüllt. In 2.1.1 werden diese Grundlagenbegriffe nochmals systematisch zusammengestellt werden.

**UE 14 ► Übungsaufgabe 1.1.5.6.** (W) Beweisen Sie (auf Grundlage der obigen Definition 1.1.5.3) dass für alle natürlichen Zahlen $k, l, j$ die folgenden Gleichungen bzw. Implikationen gelten: **◄ UE 14**

(1) $k + l = l + k$. (Haben wir schon gezeigt.)
(2) $k \cdot l = l \cdot k$. (Hier ist eine geeignete Bijektion zu finden.)
(3) $(k + l) + j = k + (l + j)$ (Assoziativgesetz für Addition und Multiplikation)
(4) $k \cdot (l + j) = k \cdot l + k \cdot j$ (Distributivgesetz)
(5) $k + 0 = k$, $k + 1 = \nu(k)$
(6) $k \cdot 0 = 0$, $k \cdot 1 = k$.
(7) Aus $k + l = k' + l$ folgt $k = k'$. (Kürzungsregel für $+$.)
(8) Aus $k \cdot l = k' \cdot l$ und $l \neq 0$ folgt $k = k'$. (Kürzungsregel für $\cdot$.)

**UE 15 ► Übungsaufgabe 1.1.5.7.** (W) Beweisen Sie (auf Grundlage der obigen Definition 1.1.5.3) dass für alle natürlichen Zahlen $k, l, j$ die folgenden Gleichungen gelten: **◄ UE 15**

(1) $(k^j)^l = k^{j \cdot l}$.
(2) $(k^j) \cdot (k^l) = k^{j+l}$.

Hinweis: Für den ersten Beweis muss man eine Bijektion $b$ zwischen den Mengen $(K^J)^L$ und $K^{J \times L}$ finden. Beachten Sie, dass die Elemente der Definitions- wie auch die Wertemenge der Funktion $b$ selbst wiederum Funktionen sind.

**Satz 1.1.5.8.** (1) *Für alle $x, y \in \mathbb{N}$ gilt*

$$((+)) \qquad x + 0 = x \quad \textit{und} \quad x + \nu(y) = \nu(x + y).$$

(2) *Umgekehrt: Sei $f\colon N \times \mathbb{N} \to \mathbb{N}$ eine beliebige Funktion, die $f(x, 0) = x$ und $f(x, \nu(y)) = \nu(f(x, y))$ für alle $x, y \in \mathbb{N}$ erfüllt, dann muss $f(x, y) = x + y$ für alle $x, y \in \mathbb{N}$ gelten.*

*Kurz gesagt: Die Gleichungen $((+))$ charakterisieren die Additionsfunktion.*

*Beweis.* Wir skizzieren einen Beweis der Eindeutigkeit: Für beliebiges $x$ betrachten wir die Menge $T_x := \{y : f(x, y) = x + y\}$. Man sieht leicht, dass $T_x$ induktiv ist; daraus folgt die Behauptung. □

**UE 16 ► Übungsaufgabe 1.1.5.9.** (W) Zeigen Sie, dass die Gleichungen **◄ UE 16**

$$((\cdot)) \qquad \forall x, y : \; x \cdot 0 = 0 \text{ und } x \cdot \nu(y) = (x \cdot y) + x$$

die Multiplikationsfunktion charakterisieren.

**UE 17 ► Übungsaufgabe 1.1.5.10.** (W) Zeigen Sie, dass die Gleichungen **◄ UE 17**

$$((\uparrow)) \qquad \forall x, y: \ x^0 = 1 \text{ und } x^{\nu(y)} = (x^y) \cdot x$$

die Exponentiation charakterisieren.

**Definition 1.1.5.11.** Sei $I$ eine unendliche Menge. Auf der Menge $\mathbb{N}_I$ definieren wir die folgende Relation $\leq$:

$$[E] \leq [F] \ :\Leftrightarrow \ \exists E' : E \approx E' \subseteq F$$

Man sieht leicht, dass diese Relation wohldefiniert ist (d.h. nicht von der Wahl der Repräsentanten abhängt), sowie dass sie reflexiv und transitiv ist. Wir zeigen in Korollar 1.1.5.14 und Lemma 1.1.5.15, dass es sich um eine lineare Ordnung (siehe Definition 2.1.1.6) handelt.

**Lemma 1.1.5.12.** (1) *Für alle $n \in \mathbb{N}_I$ gilt $\nu(n) \neq n$.*
(2) *Für alle endlichen $E \subseteq I$ und alle $e \in I \setminus E$ gilt $E \cup \{e\} \not\approx E$.*

*Beweis.* Die zweite Behauptung ist äquivalent zur ersten.
Um die erste Behauptung zu zeigen, müssen wir nur überprüfen, ob die Menge $\{n \in \mathbb{N}_I : \nu(n) \neq n\}$ induktiv ist. Die Aussage $\nu(0) \neq 0$ ist offensichtlich wahr, da die leere Menge nicht bijektiv auf eine nichtleere Menge abgebildet werden kann; und die Implikation

$$\nu(\nu(n)) = \nu(n) \ \Rightarrow \ \nu(n) = n$$

bzw. die dazu äquivalente Aussage

$$\nu(n) \neq n \ \Rightarrow \ \nu(\nu(n)) \neq \nu(n)$$

ist nur ein Spezialfall der in Lemma 1.1.3.1(3) bewiesenen Injektivität von $\nu$. Daher ist die betrachtete Menge induktiv, umfasst also ganz $\mathbb{N}_I$. □

**Lemma 1.1.5.13.** *Seien $k, n \in \mathbb{N}_I$. Wenn $k \leq n$ und $k \neq n$, dann gilt $\nu(k) \leq n$.*

*Beweis.* Sei $k \leq n$, $k \neq n$. Wir können Mengen $K \subseteq I$ und $N \subseteq I$ finden, die $n = [N]$, $k = [K]$ und $K \subsetneq N$ erfüllen. Sei $k_0 \in N \setminus K$ beliebig, dann ist $\nu(k) = [K \cup \{k_0\}]_\approx$ und $K \cup \{k_0\} \subseteq N$, daher $\nu(k) \leq n$. □

**Korollar 1.1.5.14.** Die Relation $\leq$ ist antisymmetrisch auf $\mathbb{N}_I$.

*Beweis.* Die Ungleichung $k \leq \nu(k)$ ist leicht einzusehen. Wenn $n \leq k$ und $k \leq n$ gilt, aber nicht $k = n$, dann muss nach dem gerade bewiesenen Lemma die Ungleichung $\nu(n) \leq \nu(k) \leq n$ gelten, ein Widerspruch. □

**Lemma 1.1.5.15.** *Die Relation $\leq$ ist eine lineare Ordnung auf $\mathbb{N}_I$.*

*Beweis.* Zu zeigen ist noch, dass für alle $n$ und $k$ die Aussage

$$\forall n \forall k : n \leq k \ \vee \ k \leq n$$

gilt.
Sei also $n$ beliebig. Setze

$$T_n := \{k \in \mathbb{N}_I : n \leq k \text{ oder } k \leq n\}.$$

Wir zeigen, dass $T_n$ induktiv ist. Die Ungleichung $0 \leq n$ ist klar, daher gilt $0 \in T_n$.
Wenn nun $k \in T_n$ ist, dann betrachten wir 2 Fälle:

- $n \leq k$. Dann ist $n \leq k \leq \nu(k)$, also $\nu(k) \in T_n$.
- $k \leq n$. OBdA gilt $n \not\leq k$, also insbesondere $k \neq n$. Daher gilt nach Lemma 1.1.5.13 $\nu(k) \leq n$, daher $\nu(k) \in T_n$.

□

In Analogie zu den oben genannten Bedingungen $((+))$, $((*))$ und $((\uparrow))$, die Addition, Multiplikation und Exponentiation durch jeweils zwei Bedingungen charakterisieren – eine für die Zahl 0, die andere für Nachfolger – geben wir hier eine Charakterisierung der Relation $\leq$ an:

**Satz 1.1.5.16.** *Es gilt*

$$((\leq)) \qquad \forall x, y : \ (x \leq 0 \Leftrightarrow x = 0) \text{ und } (x \leq \nu(y) \Leftrightarrow x \leq y \text{ oder } x = \nu(y))$$

**UE 18** ► **Übungsaufgabe 1.1.5.17.** (A) Die Bedingung $((\leq))$ charakterisiert bereits die Relation $\leq$, das heißt: ◄ **UE 18**
Jede Relation $R \subseteq \mathbb{N} \times \mathbb{N}$, die $x \ R \ 0 \Leftrightarrow x = 0$ und

$$x \ R \ \nu(y) \ \Leftrightarrow \ x \ R \ y \text{ oder } x = \nu(y)$$

für alle $x, y$ erfüllt, muss die Relation $\leq$ sein.

### 1.1.6 Zifferndarstellung und Normalform

Inhalt in Kurzfassung: Für das Operieren mit konkreten Zahlen sind geeignete Formen der Repräsentation wie die übliche Zahlendarstellung zur Basis 10 unabdingbar. Es folgen dazu einige grundsätzliche Überlegungen.

Wegen der großen Bedeutung der Symbolsprache in der Mathematik ist die Unterscheidung zwischen einem mathematischen Objekt und seiner symbolischen Darstellung von großer Wichtigkeit. So bezeichnen etwa die Symbolketten *zwei*, *two*, 2 und $1 + 1$ dasselbe mathematische Objekt. Von Interesse sind daher Bezeichnungssysteme, die einer Bijektion zwischen der Menge der zu beschreibenden Objekte und ihren symbolischen

Repräsentationen entsprechen. Man spricht dann von einer *Normalform*. In der Mathematik spielen überdies Operationen wie etwa Addition und Multiplikation eine so wichtige Rolle, dass man Normalformen bevorzugt, wo diese Operationen einfach handhabbare Entsprechungen auf symbolischer Ebene haben.
Der Begriff des Algorithmus und erst recht seine systematische Analyse kommen ohne eine sorgfältige Behandlung all dieser Aspekte nicht aus. Das ist zwar nicht Hauptthema der Algebra. Wir wollen aber an geeigneten Stellen auf damit verbundene Aspekte und auch Schwierigkeiten hinweisen.
Bei den natürlichen Zahlen liegen die Dinge denkbar einfach. Denn die übliche Zifferndarstellung in einem Positionssystem zu einer Basis $b \in \mathbb{N}$ mit $b \geq 2$ (im dekadischen Fall ist $b = 10$) erfüllt alle Desiderata in geradezu idealtypischer Weise. Beruhend auf der Darstellung $n = \sum_{i \geq 0} a_i b^i$ mit $a_i \in \{0, 1 \ldots, b-1\}$ wird jedem $n \in \mathbb{N}$ eine eindeutige[9] endliche Folge von Ziffern $a_i$ zugeordnet, womit einfache Algorithmen für die Grundrechnungsarten formuliert werden können.

**UE 19** ► **Übungsaufgabe 1.1.6.1.** (V) Führen Sie dies genauer aus, indem Sie folgende Aufgaben behandeln. Als Basis dürfen Sie der Einfachheit halber $b = 2$ setzen (binäre Darstellung). ◄ **UE 19**

1. Beschreiben Sie präzise (etwa durch eine rekursive Definition) eine Bijektion, welche jeder natürlichen Zahl $n$ ihre symbolische Darstellung zuordnet.
2. Beweisen Sie, dass es sich tatsächlich um eine Bijektion handelt. (Geben Sie Definitions- und Wertemenge explizit an.)
3. Beschreiben Sie den Algorithmus für die Bildung des Nachfolgers einer natürlichen Zahl. (D.h.: Wie man aus der symbolischen Darstellung einer Zahl $n$ die symbolische Darstellung von $\nu(n)$ berechnet.)
4. Beschreiben Sie den Algorithmus für die Addition zweier natürlicher Zahlen.
5. Beweisen Sie, dass Ihr Additionsalgorithmus tatsächlich das Gewünschte leistet.
6. Beschreiben Sie den Algorithmus für die Multiplikation zweier natürlicher Zahlen.
7. Beweisen Sie, dass Ihr Multiplikationsalgorithmus tatsächlich das Gewünschte leistet.
8. Beschreiben Sie einen Algorithmus, der von zwei natürlichen Zahlen die größere bestimmt.

Etwas komplizierter als bei der Arithmetik natürlicher Zahlen können die Dinge liegen, wenn aus verschiedenen a priori in Frage kommenden Darstellungen für ein und dasselbe Objekt erst eine als Normalform ausgezeichnet werden muss. Beispiele: Zu jedem

[9] Für die Eindeutigkeit muss man noch verlangen, dass die führende Ziffer ungleich 0 ist – ausgenommen bei der Darstellung der Zahl 0, wo man die Darstellung durch die Ziffer 0 der Darstellung durch eine leere Summe bzw. durch die leere Folge vorzieht.

Bruch ganzer Zahlen kann eindeutig eine gekürzte Darstellung mit positivem Nenner als Normalform ausgewählt werden (warum?). Jede gebrochen rationale Funktion besitzt Darstellungen als Bruch von Polynomen, aus denen mit Hilfe einer Normierung (z.B. gekürzte Darstellung und höchster Koeffizient im Nenner gleich 1, siehe 5.3.1 und 5.3.5) eine als Normalform ausgewählt werden kann. Die Partialbruchzerlegung (siehe Abschnitt 5.3.5) gibt Anlass zu einer anderen Normalform. In Booleschen Algebren gibt es konjunktive und disjunktive Normalformen etc. Es gibt auch Beispiele, wo Normalformen nicht in algorithmisch befriedigender Weise ermittelt werden können (Schlagwort Wortproblem in Gruppen).

## 1.2 Zahlenbereichserweiterungen als Beispielgeber

In Abschnitt 1.1 über das System der natürlichen Zahlen war das Anliegen, sehr elementare mathematische Objekte nicht naiv, sondern begrifflich klar zu fassen. Nun wenden wir uns Systemen zu, die zwar immer noch wohlbekannt sind, deren Komplexität aber zunimmt. Dies geschieht im Zuge von Konstruktionen, die für die Algebra typisch und anhand der bekanntesten Beispiele besonders leicht zu fassen sind. Das sind vor allem die schrittweisen Zahlenbereichserweiterungen von $\mathbb{N}$ zu $\mathbb{Z}$ (1.2.1), von $\mathbb{Z}$ zu $\mathbb{Q}$ (1.2.2), von $\mathbb{Q}$ zu $\mathbb{R}$ (1.2.3) und von $\mathbb{R}$ zu $\mathbb{C}$ (1.2.4).
Aus didaktischen Gründen soll in diesem Abschnitt der Herausarbeitung des Exemplarischen der Vorzug gegeben werden gegenüber systematischer Vollständigkeit, die an späteren Stellen, vor allem in Kapitel 3, nachgeholt wird.

### 1.2.1 Die ganzen Zahlen

Inhalt in Kurzfassung: Die Konstruktion des Systems $\mathbb{Z}$ der ganzen Zahlen kann ausgehend von $\mathbb{N}$ mit rein mengentheoretischen Mitteln erfolgen. Diese Konstruktion ist typisch für die Denkweise in der Algebra und wird sich, bezogen auf die additive Struktur, später (z.B. in der Theorie der Halbgruppen) auch für Verallgemeinerungen eignen.

Die Kürzungsregel für die Addition natürlicher Zahlen (aus $a + b = a + c$ folgt $b = c$, siehe Übungsaufgabe 1.1.5.6 (7)) lässt sich in die Sprache der Gleichungen übersetzen: Eine Gleichung der Form $a + x = b$ besitzt in $\mathbb{N}$ höchstens eine Lösung für $x$, für die wir $x = b - a$ schreiben. Ist $a > b$, gibt es aber keine Lösung in $\mathbb{N}$. Dies führt zur Erweiterung der Menge $\mathbb{N}$ zu einer Menge $\mathbb{Z}$, die also mindestens alle Elemente $b-a$ mit $a, b \in \mathbb{N}$ enthalten soll. (In diesem Fall erweist sich das auch als ausreichend.) Um auf mengentheoretisch festem Boden zu stehen, schreiben wir anstatt des noch in der Luft hängenden formalen Ausdrucks $b - a$ das geordnete Paar[10] $(a, b)$ an[11]. Hier ergibt sich

[10] Das geordnete Paar, bestehend aus zwei beliebig vorgegebenen Komponenten $a, b$, wird nach Kuratowski meist als Menge $(a, b) := \{\{a\}, \{a, b\}\}$ definiert. Damit sind die gewünschten Eigenschaften erfüllt, insbesondere ist $(a, b) = (c, d)$ dann und nur dann, wenn sowohl $a = c$ als auch $b = d$.

[11] A posteriori stellt sich das Paar $(a, b)$ zwar tatsächlich als Differenz der natürlichen Zahlen $a$ und $b$ heraus (genauer: als ein Repräsentant dieser Differenz, die selbst eine Äquivalenzklasse ist); diese Differenz kann man aber erst bilden, wenn die Grundmenge feststeht.

aber die Notwendigkeit, verschiedene Paare als ein und dasselbe Objekt zu definieren, weil beispielsweise $(2,3)$ und $(3,4)$ dieselbe ganze Zahl $2-3=3-4=-1$ repräsentieren. Das allgemeine Problem behebt man, indem man eine geeignete Äquivalenzrelation[12] $\sim$ auf der Menge $\mathbb{N}^2 = \mathbb{N}\times\mathbb{N} = \{(a,b) : \ a,b\in\mathbb{N}\}$ definiert derart, dass $(a,b)\sim(c,d)$ genau dann gilt, wenn die Paare $(a,b)$ und $(c,d)$ im zu konstruierenden neuen Bereich demselben Objekt entsprechen sollen. In vorliegenden Fall soll das $a-b=c-d$ bedeuten, was sich zu $a+d=c+b$ umschreiben lässt, einer innerhalb $\mathbb{N}$ sinnvollen Beziehung, die wir als Definition für $(a,b)\sim(c,d)$ verwenden. Die Menge $\mathbb{Z}$ definieren wir daher als sogenannte Faktormenge

$$\mathbb{Z} := (\mathbb{N}\times\mathbb{N})/_\sim = \{[(a,b)]_\sim : \ a,b\in\mathbb{N}\},$$

d.h. als Menge aller Äquivalenzklassen

$$[(a,b)]_\sim := \{(c,d)\in\mathbb{N}\times\mathbb{N} : (c,d)\sim(a,b)\}$$

bezüglich $\sim$.
Für die Algebra ist diese Menge $\mathbb{Z}$ deshalb so interessant, weil auf ihr in natürlicher Weise wieder eine Addition definiert werden kann. Zunächst kann man für Paare definieren:

$$(a,b)+(c,d) := (a+c,b+d).$$

Weil also auf dem kartesischen Produkt $\mathbb{N}^2=\mathbb{N}\times\mathbb{N}$ die neue Operation durch *komponentenweise* Festsetzung entsteht, spricht man von einem *direkten Produkt* von zwei Kopien des kommutativen additiven Monoids $\mathbb{N}$. Klarerweise übertragen sich Assoziativität, Kommutativität und ähnliche Gesetze von $\mathbb{N}$ auf $\mathbb{N}\times\mathbb{N}$.
Noch interessanter aber ist, dass diese Definition der Addition *verträglich* ist mit $\sim$, genauer: Sind $p_1,p_2,q_1,q_2\in\mathbb{N}^2$ Paare mit $p_1\sim p_2$ und $q_1\sim q_2$, so folgt auch $p_1+q_1\sim p_2+q_2$. Man sagt, dass $\sim$ eine *Kongruenzrelation* bezüglich $+$ ist.
Ganz ähnliche Situationen werden uns noch häufig begegenen, und wir werden beizeiten eine Definition in noch allgemeinerem Kontext geben. Vorläufig ist es wichtig, sich klar zu machen, dass das Ergebnis der Definition

$$[p]_\sim + [q]_\sim := [p+q]_\sim$$

gerade wegen der Verträglichkeit mit $+$ (also wegen der Kongruenzeigenschaft von $\sim$ bezüglich $+$) nicht von den speziellen Vertretern $p$ und $q$ der Äquivalenzklassen abhängt.

[12] Zur Erinnerung: Eine binäre Relation $R$ (d.h. eine Teilmenge $R$ von $M\times M$) auf $M$ heißt Äquivalenzrelation, wenn sie — wie Halbordnungen — reflexiv und transitiv, darüber hinaus aber symmetrisch ist statt antisymmetrisch. Symmetrisch bedeutet, dass $(a,b)\in R$ genau dann, wenn $(b,a)\in R$. Zwischen den Äquivalenzrelationen und den Partitionen auf $M$ herrscht eine wohlbekannte bijektive Beziehung, auf die wir uns sehr häufig beziehen werden. Dabei wird einer Äquivalenzrelation als Partition die Menge aller Äquivalenzklassen zugeordnet.
Statt $(a,b)\in R$ verwendet man oft die Infixnotation $a\ R\ b$ — insbesondere dann, wenn man die Äquivalenzrelation nicht mit einem Buchstaben sondern mit einem Symbol wie $\sim$, $\equiv$, $\cong$ etc bezeichnet.
Die *Äquivalenzklasse* von $a\in M$ wird mit $[a]$, $[a]_R$ oder $a/R$ bezeichnet. Systematisch werden wir diese Grundbegriffe in 2.1.1 zusammenstellen.

Wie schon im Zusammenhang mit den entsprechenden Definitionen auf $\mathbb{N}$ spricht man von *Wohldefiniertheit* und sagt, die Operation auf der Menge der Äquivalenzklassen werde durch jene auf den Elementen *induziert*. Man kann den Übergang von einem Element $p = (a, b) \in \mathbb{N}^2$ zu seiner Äquivalenzklasse $[p]_\sim$ als eine Abbildung $\kappa : \mathbb{N}^2 \to \mathbb{Z}$, die sogenannte *kanonische Abbildung*, auffassen, die gerade wegen Wohldefiniertheit und Verträglichkeit mit $+$ die sogenannte *Homomorphiebedingung*

$$\kappa(p + q) = \kappa(p) + \kappa(q)$$

erfüllt. Deshalb heißt $\kappa$ auch der *kanonische Homomorphismus*. Beim Übergang von Paaren zu Äquivalenzklassen bleiben überdies Assoziativität, Kommutativität etc. erhalten. (Siehe auch die Fußnote auf Seite 112.)

Ein weiterer entscheidender Punkt bei der Zahlenbereichserweiterung von $\mathbb{N}$ auf $\mathbb{Z}$ liegt darin, dass $\mathbb{N}$ mit einer Teilmenge von $\mathbb{Z}$ identifiziert[13] werden kann. Damit ist Folgendes gemeint: Die Zuordnung $\iota\colon \mathbb{N} \to \mathbb{Z}$, $n \mapsto [(n, 0)]_\sim$ erweist sich als *isomorphe Einbettung*[14] (genannt die kanonische Einbettung): Unmittelbar sieht man $\iota(m + n) = \iota(m) + \iota(n)$. Außerdem ist $\iota$ injektiv, weil aus $[(m, 0)]_\sim = \iota(m) = \iota(n) = [(n, 0)]_\sim$ die Äquivalenz $(m, 0) \sim (n, 0)$, also $m = m + 0 = n + 0 = n$ folgt.

Diese Konstruktion liefert allerdings nicht die gewünschte Beziehung $\mathbb{N} \subseteq \mathbb{Z}$; um diese zu garantieren, modifizieren wir die eben konstruierte Menge zu einer Menge $\mathbb{Z}'$, indem wir sämtliche Elemente in $\mathbb{Z}$, die die Form $\iota(n) = [(n, 0)]_\sim$ haben, durch ihre $\iota$-Urbilder $n$ ersetzen. Schließlich vergessen wir die ursprünglich konstruierte Menge $\mathbb{Z}$ und benennen die neue Menge von $\mathbb{Z}'$ auf $\mathbb{Z}$ um.

So wie die bisherigen Konstruktionsschritte wird uns auch dieses sogenannte *Prinzip der isomorphen Einbettung* noch oft begegnen.

Was wir in $\mathbb{N}$ vermisst und weshalb wir die Erweiterung zu $\mathbb{Z}$ überhaupt durchgeführt haben, nämlich die uneingeschränkte Ausführbarkeit der Subtraktion, funktioniert tatsächlich in ganz $\mathbb{Z}$: Zunächst ist $\iota(0) = [(0, 0)]_\sim$ neutrales Element bezüglich $+$ in $\mathbb{Z}$. Für jedes Paar $(m, n) \in \mathbb{N}^2$ spielt deshalb das Paar $(n, m)$ wegen $(m, n) + (n, m) = (n, m) + (m, n) = (m + n, n + m) \sim (0, 0) = \iota(0)$ in $\mathbb{Z}$ die Rolle des inversen Elementes, also $-[(m, n)]_\sim = [(n, m)]_\sim$.[15] Deshalb haben beliebige Gleichungen der Form $k + x = l$ in $\mathbb{Z}$ die Lösung $x = l - k = l + (-k)$. Kurz formuliert: $\mathbb{Z}$ ist eine Gruppe.

Schließlich beachte man, dass wir für unsere Zwecke auf kein Element von $\mathbb{Z}$ verzichten können, d.h. dass $\mathbb{Z}$ in der obigen Konstruktion so sparsam wie möglich gewählt wurde. Das kommt zum Ausdruck in der dritten Aussage des folgenden Satzes.

---

[13] Wenn wir sagen, dass wir $X$ und $Y$ „identifizieren“, dann bedeutet dies Folgendes: $X$ und $Y$ haben gewisse gemeinsame Eigenschaften; solange es nur um diese Eigenschaften geht, ist es egal, ob wir von $X$ oder von $Y$ sprechen. Wir lassen es sogar zu, dass wir von $X$ sprechen, tatsächlich aber $Y$ meinen. Wenn wir zum Beispiel sagen, dass die Gruppe der ganzen Zahlen kommutativ ist, dann spielt es keine Rolle, ob wir von der Gruppe $(\mathbb{Z}, +)$ (vom Typ (2), d.h. mit einer binären Operation $+$; siehe Definition 2.1.3.2 für das Konzept des Typs) oder von der Gruppe $(\mathbb{Z}, +, 0, -)$ (vom Typ $(2, 0, 1)$) sprechen.

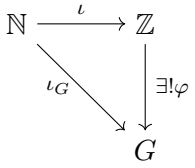
[14] Unter einer *isomorphen Einbettung* verstehen wir einen injektiven Homomorphismus, siehe Definition 2.1.5.1.

[15] Man beachte die Verwendung der Kommutativität $m + n = n + m$.

**Theorem 1.2.1.1.** (1) $\mathbb{Z}$ ist bezüglich der Addition eine Gruppe (mit obigen Neutralen und Inversen).

(2) Die oben beschriebene Abbildung $\iota\colon \mathbb{N} \to \mathbb{Z}$ ist eine isomorphe Einbettung der additiven Halbgruppe $\mathbb{N}$.

(3) Ist $G$ irgendeine Gruppe und $\iota_G\colon \mathbb{N} \to G$ eine isomorphe Einbettung der additiven Halbgruppe $\mathbb{N}$, so gibt es eine isomorphe Einbettung $\varphi\colon \mathbb{Z} \to G$ mit $\iota_G = \varphi \circ \iota$, die sogar eindeutig bestimmt ist.




**UE 20** ► **Übungsaufgabe 1.2.1.2.** (W) Beweisen Sie Theorem 1.2.1.1, indem Sie die folgenden noch ausständigen Schritte vollständig durchführen. Es gelten die Notationen des gesamten Unterabschnitts. ◄ **UE 20**

1. Die Relation $\sim$ ist eine Äquivalenzrelation auf $\mathbb{N}^2$. (Wo geht dabei die Kürzbarkeit der Addition in $\mathbb{N}$ ein?)

2. Es handelt sich bei $\sim$ sogar um eine Kongruenzrelation.

3. Geben Sie die Abbildung $\varphi$ an, prüfen Sie die behaupteten Eigenschaften nach und begründen Sie die Eindeutigkeit.

Die Eigenschaften in Theorem 1.2.1.1 zeichnen die ganzen Zahlen als (additive) Differenzengruppe von $\mathbb{N}$ aus. In 3.1.4 werden wir diese Konstruktion statt auf $\mathbb{N}$ auf beliebige kommutative kürzbare Monoide anwenden.
Wir kehren zurück zum System der ganzen Zahlen $\mathbb{Z}$. Bisher haben wir uns nur um die additive Struktur gekümmert. Doch auch die Multiplikation auf $\mathbb{N}$ lässt sich fortsetzen. Denn auch die Definition

$$[(a,b)]_\sim \cdot [(c,d)]_\sim := [(ac+bd, ad+bc)]_\sim$$

erweist sich als unabhängig von den Vertretern der Klassen, d.h. $\sim$ ist auch bezüglich $\cdot$ eine Kongruenzrelation. Daraus folgt:

**Proposition 1.2.1.3.** *$\mathbb{Z}$ ist bezüglich der Multiplikation ein kommutatives Monoid mit neutralem Element $\iota(1)$.*

**UE 21** ► **Übungsaufgabe 1.2.1.4.** (V) Beweisen Sie Proposition 1.2.1.3 in allen Einzelheiten. (Zeigen Sie insbesondere, dass $\sim$ eine Kongruenzrelation ist.) ◄ **UE 21**

Nun zur Ordnungsstruktur auf $\mathbb{Z}$: Sei $\iota\colon \mathbb{N} \to \mathbb{Z}$ die kanonische Einbettung. Wir nennen ein Element $\iota(n) \in \mathbb{Z}$ positiv, falls $n \in \mathbb{N} \setminus \{0\}$ (wohldefiniert wegen der Injektivität von $\iota$), und negativ, falls $-\iota(n)$ positiv ist. $\mathbb{Z}^+$ bezeichne die Menge der positiven, $\mathbb{Z}^-$ die der negativen Elemente. Dann bilden die drei Mengen $\mathbb{Z}^+, \mathbb{Z}^-, \{0\}$ eine disjunkte Zerlegung von $\mathbb{Z}$.

**UE 22** ► **Übungsaufgabe 1.2.1.5.** (F) Beweisen Sie, dass es sich tatsächlich um eine Partition der Menge $\mathbb{Z}$ handelt. ◄ **UE 22**

Außerdem setzen wir $a \leq b$, sofern $b - a$ positiv oder $a = b$ ist. Damit gilt:

**Satz 1.2.1.6.** *Die bisher auf $\mathbb{Z}$ definierten Strukturen haben folgende weitere Eigenschaften:*

1. *$\mathbb{Z}$ zusammen mit Addition und Multiplikation ist ein* Integritätsbereich*, das ist definitionsgemäß ein nullteilerfreier kommutativer Ring mit Einselement. (Ein Ring heißt* nullteilerfrei*, wenn aus $ab = 0$ stets $a = 0$ oder $b = 0$ folgt.)*
2. *Zieht man auch noch die Ordungsrelation heran, erhält man sogar einen angeordneten Ring. Damit ist gemeint, dass eine Totalordnung $\leq$ auf $\mathbb{Z}$ vorliegt, die folgende Monotoniegesetze erfüllt: Für $a, b, c \in \mathbb{Z}$ folgt aus $a \leq b$ stets $a + c \leq b + c$ und, sofern zusätzlich $c \geq 0$ gilt, $ac \leq bc$.*

**UE 23** ► **Übungsaufgabe 1.2.1.7.** (V) Beweisen Sie Satz 1.2.1.6. Verwenden Sie hier nur die als bekannt vorausgesetzten Rechenregeln in $\mathbb{N}$; die Rechenregeln für $\mathbb{Z}$ dürfen Sie nicht voraussetzen. ◄ **UE 23**

**UE 24** ► **Übungsaufgabe 1.2.1.8.** (B) ◄ **UE 24**

(1) Finden Sie alle Halbgruppenhomomorphismen $f : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$.

(2) Finden Sie alle Gruppenhomomorphismen $f : (\mathbb{Z}, +, 0, -) \to (\mathbb{Z}, +, 0, -)$.

(3) Finden Sie alle Ring-Homomorphismen $f : (\mathbb{Z}, +, 0, -, \cdot) \to (\mathbb{Z}, +, 0, -, \cdot)$.

(4) Finden Sie alle $\mathrm{Ring}_1$-Homomorphismen $f : (\mathbb{Z}, +, 0, -, \cdot, 1) \to (\mathbb{Z}, +, 0, -, \cdot, 1)$. (Also alle Abbildungen, die mit allen $\mathrm{Ring}_1$-Operationen verträglich sind: $f(x \cdot y) = f(x) \cdot f(y)$, $f(1) = 1$, etc.)

Hinweis: Die Reihenfolge ist so gewählt, dass die erste zu beschreibende Mengen von Homomorphismen die nachfolgenden umfasst etc. Wenn es Ihnen sympathischer ist, können Sie auch in anderer Reihenfolge vorgehen.

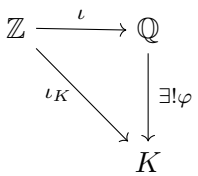
### 1.2.2 Die rationalen Zahlen

Inhalt in Kurzfassung: Die Konstruktion des Systems $\mathbb{Q}$ der rationalen Zahlen aus $\mathbb{Z}$ folgt jener von $\mathbb{Z}$ aus $\mathbb{N}$ aus dem vorangegangenen Abschnitt.

Der Übergang von $\mathbb{Z}$, dem System der ganzen Zahlen, zu $\mathbb{Q}$, dem der rationalen, erfolgt in weitgehender Analogie zu jenem von $\mathbb{N}$ zu $\mathbb{Z}$. Wir können uns entsprechend kurz fassen. Wegen der multiplikativen Kürzungsregel haben Gleichungen der Gestalt $ax = b$ für $a \neq 0$ in $\mathbb{Z}$ höchstens eine Lösung. Eine solche existiert genau dann, wenn $a$ ein Teiler von $b$ ist. Dies motiviert einerseits zur Untersuchung von Teilbarkeitseigenschaften in $\mathbb{Z}$ und verwandten Strukturen (siehe Kapitel 5), andererseits zur Erweiterung des Zahlenbereichs um Lösungen, die wir als Brüche $\frac{b}{a}$ anschreiben, zu einem Körper.
Eine ganz analoge Konstruktion wie in 1.2.1 auf $\mathbb{N} \times \mathbb{N}$ können wir auf die multiplikative Halbgruppe $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ anwenden und erhalten die Menge $\mathbb{Q}$ aller Äquivalenzklassen von Paaren $(a, b)$ mit $b \neq 0$. Wie gewohnt schreiben wir die Elemente von $\mathbb{Q}$ als Brüche an. Die Schreibweise $\frac{a}{b}$ steht also für die Äquivalenzklasse des Paares $(a, b)$. In Übereinstimmung mit den Rechenregeln für das Erweitern bzw. Kürzen von Brüchen ist $\frac{a}{b} = \frac{c}{d}$ genau dann, wenn $ad = cb$ in $\mathbb{Z}$ gilt. Neutrales Element ist $1 := [(1, 1)]_\sim$. Doch auch die additive Struktur von $\mathbb{Z}$ kann in bekannter Weise auf $\mathbb{Q}$ fortgesetzt werden. Wir fassen zusammen:

**Satz 1.2.2.1.** *Auf der Menge $M := \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ sei die Operation $(a, b) + (c, d) := (ad + cb, bd)$ definiert. Außerdem schreiben wir $(a, b) \sim (c, d)$ für $ad = cb$. Dann gilt:*

1. *$(M, +, (0, 1))$ ist ein kommutatives Monoid.*
2. *Die Relation $\sim$ ist eine Kongruenzrelation auf $M$ auch bezüglich $+$. Also ist die Addition $[(a, b)]_\sim + [(c, d)]_\sim := [(ad + cb, bd)]_\sim$ auf $\mathbb{Q}$ wohldefiniert.*
3. *Die Menge $\mathbb{Q} := M/\sim$ bildet bezüglich der induzierten Operation $+$ (siehe 2.) und dem neutralen Element $0 := [0, 1]_\sim$ nicht nur ein kommutatives Monoid, sondern (mit den Inversen $-[(a, b)]_\sim := [(-a, b)]_\sim$) sogar eine (abelsche) Gruppe.*
4. *$(\mathbb{Q}, +, 0, -, \cdot, 1)$ ist sogar ein Körper.*
5. *Die Abbildung $\iota \colon \mathbb{Z} \to \mathbb{Q}$, $k \mapsto [(k, 1)]_\sim$ ist eine isomorphe Einbettung des Integritätsbereichs $\mathbb{Z}$ in $\mathbb{Q}$.*
6. *Jeder Körper $K$, der vermittels einer Einbettung $\iota_K \colon \mathbb{Z} \to K$ eine isomorphe Kopie des Integritätsbereichs $\mathbb{Z}$ enthält, enthält auch eine isomorphe Kopie des Körpers $\mathbb{Q}$ vermittels einer durch die Bedingung $\iota_K = \varphi \circ \iota$ eindeutig bestimmten Einbettung $\varphi \colon \mathbb{Q} \to K$. (In diesem Sinne ist $\mathbb{Q}$ der kleinste Körper, der $\mathbb{Z}$ enthält.)*




7. *Die Ordungsrelation auf $\mathbb{Z}$ kann in eindeutiger Weise so auf $\mathbb{Q}$ fortgesetzt werden, dass gilt:*

*a) Die Ungleichung* $[(a,b)]_\sim > 0$ *gilt genau dann, wenn* $ab > 0$ *in* $\mathbb{Z}$.

*b) In* $(\mathbb{Q}, +, \cdot, \leq)$ *gelten die* Monotoniegesetze*: Aus* $q_1 \leq q_2$ *folgt stets* $q_1 + q_3 \leq q_2 + q_3$*, im Falle* $q_3 > 0$ *auch* $q_1 q_3 \leq q_2 q_3$.

**UE 25 ► Übungsaufgabe 1.2.2.2.** (W) Beweisen Sie Satz 1.2.2.1. Verwenden Sie dabei nur die als bekannt vorausgesetzten Rechenregeln in $\mathbb{Z}$; die Rechenregeln für $\mathbb{Q}$ dürfen Sie nicht voraussetzen. **◄ UE 25**

Die letzte Aussage in Satz 1.2.2.1 weist $\mathbb{Q}$ als einen *angeordneten Körper* aus, die anderen als *Quotientenkörper* von $\mathbb{Z}$. Auf die allgemeine Konstruktion des Quotientenkörpers eines Integritätsbereichs (und noch allgemeiner: eines Bruchrings) werden wir in 3.4.5 zurückkommen.

### 1.2.3 Die reellen Zahlen

Inhalt in Kurzfassung: Für die dritte große Zahlenbereichserweiterung, nämlich von $\mathbb{Q}$ zu $\mathbb{R}$, sind mehrere Zugänge möglich. In jedem Fall sind aber neue Ideen erforderlich. Hier beschreiten wir den Weg mittels Cauchyfolgen. (Eine alternative Konstruktion mittels Dedekindscher Schnitte wird in 3.5.3 zur Sprache kommen.) Trotz der nun stärker analytischen Aura treten im Zusammenhang mit den Cauchyfolgen aber wieder Aspekte von großem algebraischen Interesse auf (Idealeigenschaft).

Der Übergang von $\mathbb{Q}$ zu $\mathbb{R}$ unterscheidet sich stark von den bisherigen Zahlenbereichserweiterungen. Der Grund liegt darin, dass man sich diesmal keine algebraische Eigenschaft von der Erweiterung wünscht, sondern eine ordnungstheoretische bzw. eine topologisch-analytische. Das wird oft verschleiert, wenn an dieser Stelle der berühmte Beweis für die Irrationalität von $\sqrt{2}$ geführt wird, weil dadurch der Eindruck erweckt wird, dass es nur um die Ergänzung von Wurzeln gehe. Doch zeigt die imaginäre Wurzel $\sqrt{-1}$, dass es nicht primär darum geht. Der Unterschied besteht darin, dass $\sqrt{2}$ gewissermaßen einer Lücke in $\mathbb{Q}$, und zwar irgendwo zwischen $\frac{14}{10}$ und $\frac{15}{10}$ entspricht. Das ist bei $\sqrt{-1}$ nicht der Fall. Deshalb lohnt eine Übungsaufgabe, wo einige Lücken in $\mathbb{Q}$ auszumachen sind, auch solche, die keinen Wurzeln entsprechen, sondern anders motiviert sind.

**UE 26 ► Übungsaufgabe 1.2.3.1.** (B) In dieser Aufgabe dürfen Sie wichtige Eigenschaften natürlicher Zahlen ohne Beweis verwenden, sofern Sie diese sorgfältig formulieren. **◄ UE 26**

1. Zeigen Sie, dass es kein $\alpha \in \mathbb{Q}$ mit $\alpha^2 = 2$ gibt.
2. Wie in Teil 1 mit $\alpha^2 = 3$ statt $\alpha^2 = 2$.
3. Für welche $m, n \in \mathbb{N}$ gibt es ein $\alpha \in \mathbb{Q}$ mit $\alpha^m = n$? (Begründung)
4. Zeigen Sie, dass die Eulersche Zahl $e = \sum_{n=0}^{\infty} \frac{1}{n!}$ irrational ist. (Anleitung: Jede Partialsumme $s_n$ ist eine rationale Zahl der Form $\frac{p_n}{n!}$ mit $p_n \in \mathbb{N}$. Wäre $e = \frac{p}{q}$

rational mit $p, q \in \mathbb{N}$, so ließe sich die Differenz $d := e - s_q > 0$ auf gemeinsamen Nenner $q!$ bringen, erfüllte also $d \geq \frac{1}{q!}$. Daraus lässt sich ein Widerspruch ableiten. In dieser Aufgabe dürfen Sie die Theorie unendlicher Reihen aus der Analysis verwenden, insbesondere die Formel für die geometrische Reihe.)

5. Die Kreiszahl $\pi$ ist definiert als das Doppelte der kleinsten positiven Nullstelle des Cosinusfunktion $\cos x := \sum_{n=0}^{\infty}(-1)^n \frac{x^{2n}}{(2n)!}$. Was aus der reellen Analysis fließt bei der Wohldefiniertheit von $\pi$ ein?

6. Zeigen Sie $\pi \notin \mathbb{Q}$. (Sehr schwierig.)

Die Vertiefung der Theorie der reellen Zahlen im Sinne der reellen Analysis ist natürlich dort besser aufgehoben. Dennoch gibt es auch aus algebraischer Sicht manch Interessantes, das wir aus der Analysis rekapitulieren oder uns in einem neuen Licht vor Augen führen wollen. Auf die stark ordnungstheoretisch orientierte Konstruktion von $\mathbb{R}$ mittels Dedekindscher Schnitte werden wir noch an geeigneter Stelle (3.5.3) zu sprechen kommen. Um typisch algebraische Konzepte exemplarisch vorzustellen, hat die folgende alternative Konstruktion von $\mathbb{R}$, die auf Cantor zurückgeht, manche Vorzüge:
Wir betrachten die Menge CF aller Cauchyfolgen in $\mathbb{Q}$. Zur Erinnerung: Eine Folge $x = (x_n)_{n\in\mathbb{N}}$ (zunächst) rationaler Zahlen $x_n$ heißt *Cauchyfolge*, wenn es zu jedem $\varepsilon > 0$ ein $n_0 \in \mathbb{N}$ gibt derart, dass $|x_{n_1} - x_{n_2}| < \varepsilon$ für alle $n_1, n_2 \geq n_0$ gilt. Auf CF sind in natürlicher Weise Addition und Multiplikation definiert, nämlich durch

$$(x_n)_{n\in\mathbb{N}} + (y_n)_{n\in\mathbb{N}} := (x_n + y_n)_{n\in\mathbb{N}}$$

und

$$(x_n)_{n\in\mathbb{N}} \cdot (y_n)_{n\in\mathbb{N}} := (x_n \cdot y_n)_{n\in\mathbb{N}}.$$

**UE 27 ► Übungsaufgabe 1.2.3.2.** (V) Beweisen Sie, dass dabei die Folgen der $x_n + y_n$ und der $x_n \cdot y_n$ wieder Cauchyfolgen sind. **◄ UE 27**

Diese Definitionen sind wieder Beispiele eines direkten Produktes, hier nicht nur von zwei Strukturen, sondern von abzählbar vielen Kopien des Ringes $\mathbb{Q}$ der rationalen Zahlen, für jedes $n \in \mathbb{N}$ eine Kopie.
Klarerweise erfüllen die Operationen + und · auf CF alle Gesetze eines kommutativen Ringes, wobei die konstanten Folgen mit Wert 0 bzw. 1 Null- bzw. Einselement sind (für die wir wieder 0 und 1 schreiben). Allerdings können verschiedene rationale Folgen gegen dieselbe reelle Zahl konvergieren. Also identifizieren wir gemäß einer geeigneten Äquivalenzrelation $\sim$, nämlich:

$$x = (x_n)_{n\in\mathbb{N}} \quad \sim \quad y = (y_n)_{n\in\mathbb{N}}$$

genau dann, wenn $(x_n - y_n)_{n\in\mathbb{N}}$ eine Nullfolge ist. Nützlich ist auch eine Formulierung mit Hilfe der Menge

$$I := \{(x_n)_{n\in\mathbb{N}} : \ x_n \in \mathbb{Q}, \ \forall \varepsilon > 0 \, \exists n_0 \in \mathbb{N} \, \forall n \geq n_0 : \ |x_n| < \varepsilon\}$$

aller rationalen Nullfolgen.[16] Dann gilt $x = (x_n)_{n\in\mathbb{N}} \sim y = (y_n)_{n\in\mathbb{N}}$ genau dann, wenn $(x_n - y_n)_{n\in\mathbb{N}} \in I$.
Die Menge $I$ aller Nullfolgen in $\mathbb{Q}$ spielt nun eine zentrale Rolle. Weil $\sim$ vermittels $I$ definiert wurde, schreiben wir für die Menge CF $/_\sim$ aller $\sim$-Äquivalenzklassen auch CF $/I$.
Als entscheidend dafür, dass die nun folgende Konstruktion möglich ist, erweist sich, dass $I$ ein sogenanntes *Ideal* in CF ist. Das ist allgemein eine nichtleere Teilmenge $I \subseteq R$ eines Ringes $R$ mit folgenden beiden Eigenschaften:

1. Aus $a, b \in I$ folgt $a - b \in I$. ($I$ ist also eine additive Untergruppe von $R$.)
2. Aus $a \in I$ folgt $ab, ba \in I$ für beliebige $b \in R$. (Idealeigenschaft)

**UE 28** ► **Übungsaufgabe 1.2.3.3.** (V) Prüfen Sie nach: Die Menge $I$ aller Nullfolgen in $\mathbb{Q}$ bildet ein Ideal im Ring $R := \mathrm{CF}$. ◄ **UE 28**

Von sehr allgemeiner Bedeutung ist der folgende Zusammenhang:

**Proposition 1.2.3.4.** *Sei $R$ ein Ring.*

1. *Sei $I \subseteq R$ ein Ideal und die Relation $\sim_I$ auf $R$ definiert durch: $a \sim_I b$ genau dann, wenn $a - b \in I$. Dann ist $\sim_I$ eine Kongruenzrelation auf $R$.*
2. *Ist umgekehrt $\sim$ eine Kongruenzrelation auf einem Ring $R$, so bildet die Nullklasse $I_\sim := [0]_\sim$ ein Ideal.*
3. *Die Konstruktionen aus 1. und 2. sind invers zueinander, d.h. $I_{\sim_I} = I$ und $\sim_{I_\sim} = \sim$.*

**UE 29** ► **Übungsaufgabe 1.2.3.5.** (W) Beweisen Sie Proposition 1.2.3.4. ◄ **UE 29**

Deshalb sind auf $\mathbb{R} := \mathrm{CF}\,/I$ die Operationen

$$[(x_n)_{n\in\mathbb{N}}]_\sim + [(y_n)_{n\in\mathbb{N}}]_\sim := [(x_n + y_n)_{n\in\mathbb{N}}]_\sim$$

und

$$[(x_n)_{n\in\mathbb{N}}]_\sim \cdot [(y_n)_{n\in\mathbb{N}}]_\sim := [(x_n y_n)_{n\in\mathbb{N}}]_\sim$$

wohldefiniert. Sie machen $\mathbb{R}$ zu einem Ring mit Nullelement $0 := [(0)_{n\in\mathbb{N}}]_\sim$ und Einselement $1 := [(1)_{n\in\mathbb{N}}]_\sim$. (Dies folgt im Wesentlichen unmittelbar aus dem Bisherigen.)
Folglich besitzt die Menge $\mathbb{R} := \mathrm{CF}\,/I$ eine natürliche Ringstruktur. Auch die Ordungsstruktur kann in natürlicher Weise definiert werden. Zwar lässt sie sich als Totalordnung nicht direkt von $\mathbb{Q}$ auf das direkte Produkt fortsetzen, sehr wohl aber auf die Menge der $\sim$-Äquivalenzklassen.
$x = [(x_n)_{n\in\mathbb{N}}]_\sim \leq y = [(y_n)_{n\in\mathbb{N}}]_\sim$ genau dann, wenn es ein $n_0 \in \mathbb{N}$ gibt mit $x_n < y_n$ für alle $n \geq n_0$ oder wenn $x \sim y$.

[16] Die Variable $\varepsilon > 0$ wird meist für reelle Größen verwendet, die an dieser Stelle allerdings noch nicht zur Verfügung stehen. Doch auch wenn man nur rationale $\varepsilon$ zulässt – und so ist die Formel hier zu verstehen –, ändert das nichts an der Menge $I$.

**UE 30** ► **Übungsaufgabe 1.2.3.6.** (V) Zeigen Sie, dass die Relation $\leq$ auf $\mathbb{R}$ wohldefiniert und eine Totalordnung ist. ◄ **UE 30**

Auf diese Weise wird $\mathbb{R}$ ein angeordneter Körper, wie auch schon $\mathbb{Q}$. Darüber hinaus – und das ist die für die Analysis entscheidende Eigenschaft – ist $\mathbb{R}$ als solcher sogar *vollständig*. Das bedeutet explizit: Ist $T \subseteq \mathbb{R}$ nicht leer und nach oben beschränkt (d.h. es gibt eine obere Schranke von $T$, das ist ein $s \in \mathbb{R}$ mit $t \leq s$ für alle $t \in T$), so hat $T$ sogar ein sogenanntes *Supremum* (eine kleinste obere Schranke) $s_0 = \sup T$ in $\mathbb{R}$ (nicht notwendig in $T$ selbst), das also $s_0 \leq s$ für alle oberen Schranken $s$ von $T$ erfüllt. Wir können also sehr kurz zusammenfassen:

**Satz 1.2.3.7.** *$\mathbb{R}$ mit den Operationen und der Relation aus Aufgabe 1.2.3.6 ist ein vollständig angeordneter Körper.*

**UE 31** ► **Übungsaufgabe 1.2.3.8.** (W) Beweisen Sie Satz 1.2.3.7. Gehen Sie dabei wie folgt vor: ◄ **UE 31**

1. Listen Sie (möglichst übersichtlich gegliedert) alle Eigenschaften auf, die im Begriff des vollständig angeordneten Körper enthalten sind.
2. Markieren Sie, welche dieser Eigenschaften aus dem bisher Gesagten bereits unmittelbar abzulesen sind.
3. Formulieren Sie, was für die verbleibenden Eigenschaften zu zeigen ist.
4. Beweisen Sie die Vollständigkeit von $\mathbb{R}$.
5. Ergänzen Sie allfällige noch fehlende Beweisteile.

In 3.5.3 werden wir nochmals auf die reellen Zahlen zu sprechen kommen, indem wir eine alternative Konstruktion zur Vervollständigung von Halbordnungen, nämlich mittels Dedekindscher Schnitte, auf $\mathbb{Q}$ anwenden werden. Die folgenden Übungsaufgabe weist bereits in diese Richtung. Außerdem werden wir in 3.5.3 einen Blick auf die Struktur beliebiger (archimedisch) angeordneter Körper werfen und einen Eindeutigkeitssatz für $\mathbb{R}$ beweisen.

**UE 32** ► **Übungsaufgabe 1.2.3.9.** (A) (In dieser Aufgabe gehen wir davon aus, dass wir die rationalen Zahlen gut verstehen, ebenso wie die Grundrechnungsarten und die Ordnung auf den rationalen Zahlen. Fakten über die reellen Zahlen dürfen wir noch nicht ohne Beweis verwenden.) ◄ **UE 32**

- Wir betrachten die nach 1.2.3.5 definierte Äquivalenzrelation $\sim$ auf der Menge CF aller Cauchyfolgen in $\mathbb{Q}$. Für zwei verschiedene Äquivalenzklassen $[x]_\sim$, $[y]_\sim$ ($x \not\sim y$) definieren wir

$$[x]_\sim < [y]_\sim \qquad \Leftrightarrow \qquad \exists n_0 \; \forall n > n_0 \; (x_n < y_n)$$

- Es sei $D$ die Menge aller $A \subseteq \mathbb{Q}$ mit folgenden Eigenschaften: $A \neq \emptyset$, $A \neq \mathbb{Q}$, $\forall a \in A\ \forall q \in \mathbb{Q} : (q < a \Rightarrow q \in A)$, und $A$ hat kein größtes Element.

Geben Sie eine (natürliche) Bijektion $f : \mathrm{CF}/\!\sim \to D$ an, die $[x]_\sim < [y]_\sim \Leftrightarrow f([x]_\sim) \subsetneq f([y]_\sim)$ erfüllt.
Zeigen Sie, dass $D$ bzw $\mathrm{CF}/\!\sim$ durch $\subseteq$ bzw. durch (die oben definierte Relation) $\leq$ linear geordnet wird. (Hinweis zur Notation: Wie generell im Zusammenhang mit Halbordnungen steht $x \leq y$ für $x < y$ oder $x = y$ und $x < y$ für $x \leq y$ und $x \neq y$.)

### 1.2.4 Die komplexen Zahlen

Inhalt in Kurzfassung: Komplexe Zahlen können in vertrauter Weise als Paare mit Real- und Imaginärteil als Komponenten aufgefasst werden. Sie bilden einen Körper $\mathbb{C}$, für den ein Eindeutigkeitssatz gilt, außerdem der Fundamentalsatz der Algebra. Der hier skizzierte Beweis verlangt keine höheren Hilfsmittel, lediglich den Satz vom Maximum aus der reellen Analysis. Abschließend werden auch noch kurz die Hamiltonschen Quaternionen besprochen.

Bekanntlich entsteht das System $\mathbb{C}$ der komplexen Zahlen aus dem Bedürfnis, auch Gleichungen wie (als einfachsten Fall) $p(x) = x^2 + 1 = 0$, die keine reellen Lösungen besitzen, zu lösen. Ist $K$ irgendein Körper, der den Körper $\mathbb{R}$ enthält und $i \in K$ (imaginäre Einheit) so eine Lösung (d.h. es gelte $i^2+1 = 0$), so ist auch $-i$ eine Lösung. Offenbar können wir schreiben $p(x) = x^2 + 1 = (x - i)(x + i)$, woraus ersichtlich ist, dass $i$ und $-i$ die einzigen Lösungen von $p(x) = 0$ sind. Klarerweise muss $K$ als Körper auch alle Elemente der Form $a + ib$ mit $a, b \in \mathbb{R}$ enthalten. Wir fassen so ein Element als Paar $(a, b)$ auf und entsprechend den Körper $\mathbb{C}$ der komplexen Zahlen[17] in üblicher Weise als Menge $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ mit den Operationen $(a_1, b_1) + (a_2, b_2) := (a_1 + a_2, b_1 + b_2)$ (direktes Produkt der additiven Gruppe $\mathbb{R}$ mit sich selbst) und $(a_1, b_1) \cdot (a_2, b_2) := (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1)$.

[17] Die geometrische Interpretation als komplexe Zahlenebene sowie die Darstellung in Polarkoordinaten dürfte aus der Analysis bekannt sein. Die wichtigsten Fakten:

- Die Zahl $a - ib$ bzw. $(a, -b)$ nennen wir zu $a + ib = (a, b)$ *konjugiert*. Die zu $z = a + ib$ konjugierte Zahl $a - ib$ wird meist mit $\bar{z}$ bezeichnet. Die Zahl $z\bar{z} = (a + ib)(a - ib) = a^2 + b^2$ ist reell und nichtnegativ.
- Der *Absolutbetrag* der Zahl $a + ib$ $(a, b \in \mathbb{R})$ ist die reelle Zahl $|a + ib| := \sqrt{a^2 + b^2}$. Für reelle Zahlen stimmt dies mit dem üblichen Betrag überein.
- Die Gleichung $|z_1 \cdot z_2|^2 = |z_1|^2 \cdot |z_2|^2$ lässt sich leicht nachrechnen; daraus erhält man $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$.
- Jede Zahl $a + ib$ mit $|a + ib| = 1$ lässt sich eindeutig in der Form $\cos\varphi + i \sin\varphi = \exp(i\varphi) = e^{i\varphi}$ mit $\varphi \in (-\pi, \pi]$ schreiben (oder, je nach Geschmack, $\varphi \in [0, 2\pi)$).
- Damit ist jede Zahl $z \in \mathbb{C} \setminus \{0\}$ eindeutig als $z = r \cdot e^{i\varphi}$ darstellbar (mit $r \in \mathbb{R}$, $r > 0$, $\varphi \in [0, 2\pi)$).
- Multiplikation und Division lassen sich in dieser Darstellung besonders leicht ausführen: $re^{i\varphi} \cdot se^{i\psi} = rs \cdot e^{i(\varphi+\psi)}$ und ${}^{re^{i\varphi}}\!/_{se^{i\psi}} = \frac{r}{s} \cdot e^{i(\varphi-\psi)}$.

Um interessante Beispiele zu gewinnen, werden wir gelegentlich die Darstellung komplexer Zahlen mittels Polarkoordinaten verwenden. Für den systematischen Aufbau einer in sich geschlossenen algebraischen Theorie wäre das nicht nötig.

**UE 33 ► Übungsaufgabe 1.2.4.1.** (W) Zeigen Sie, dass $\mathbb{C}$ mit diesen Operationen wirklich einen Körper und dass die Menge $\{(a,0) : a \in \mathbb{R}\}$ einen zu $\mathbb{R}$ isomorphen Unterkörper bildet. **◄ UE 33**

**UE 34 ► Übungsaufgabe 1.2.4.2.** (F) **◄ UE 34**

(1) Finden Sie alle komplexen Zahlen $z = a + bi$, die $z \cdot z = i$ erfüllen.

(2) Finden Sie alle komplexen Zahlen $z = a + bi$, die $z^5 + 2 = 0$ erfüllen.

Wir werden in Zukunft die Menge $\{(a,0) : a \in \mathbb{R}\}$ mit $\mathbb{R}$ identifizieren, also (vermittels einer isomorphen Einbettung) die Menge $\mathbb{R}$ als Teilmenge von $\mathbb{C}$ auffassen. Weiters definieren wir $i := (0,1)$. Für dieses Element gilt $i^2 = (0,1) \cdot (0,1) = (-1,0) = -1$. Jedes Element $z \in \mathbb{C}$ lässt sich somit tatsächlich eindeutig in der Form $z = (a,b) = (a,0) + (0,b) = (a,0) + (0,1)(b,0) = a + ib$ schreiben.
Leicht identifiziert man auch eine isomorphe Kopie von $\mathbb{C}$ innerhalb eines beliebigen Körpers, wenn dieser sowohl $\mathbb{R}$ als auch eine Entsprechung von $i$ enthält. Genauer gilt:

**Satz 1.2.4.3.** *Sei $K$ ein Körper, $\varphi\colon \mathbb{R} \to K$ eine isomorphe Einbettung von $\mathbb{R}$ als Körper und $i_K$ ein Element von $K$ mit $i_K^2 = -1 \in K$. Dann gibt es genau zwei isomorphe Einbettungen $\psi\colon \mathbb{C} \to K$, die $\psi(a,0) = \varphi(a)$ für alle $a \in \mathbb{R}$ erfüllen. Diese sind gegeben durch $\psi_1(a,b) := \varphi(a) + i_K\varphi(b)$ und $\psi_2(a,b) := \varphi(a) - i_K\varphi(b)$. Insbesondere (wenn man nämlich $K = \mathbb{C}$ setzt) hat $\mathbb{C}$ genau zwei Körperautomorphismen, die $\mathbb{R}$, genauer: die Menge aller Paare $(a,0)$ mit $a \in \mathbb{R}$, punktweise fest lassen. Einer davon ist die Identität, der andere die Konjugation $(a,b) \mapsto (a,-b)$.*

**UE 35 ► Übungsaufgabe 1.2.4.4.** (V) Beweisen Sie Satz 1.2.4.3, indem Sie allfällige noch ausständige Punkte sorgfältig ausführen. Hinweis: Zeigen Sie, dass $\psi$ durch $\psi(0,1)$ eindeutig festgelegt ist und für diesen Wert nur $i_K$ und $-i_K$ in Frage kommen. **◄ UE 35**

Wie aus Satz 1.2.4.3 hervorgeht, muss man gewisse Eindeutigkeiten innerhalb der Bereiche $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ im Falle von $\mathbb{C}$ zu einer Zweideutigkeit abschwächen. Dennoch spricht man beispielsweise von *der* komplexen Zahl $2 + 3i$ (gemeint ist das Paar $(2,3)$), ohne auf die Problematik[18] einzugehen, dass durch die Forderung $i^2 = -1$ noch nicht ausgeschlossen ist, dass damit genauso $2 - 3i$ gemeint sein könnte (also das Paar $(2,-3)$). Selbstverständlich werden auch wir uns dieser etwas ungenauen aber praktischen und deshalb gebräuchlichen Ausdrucksweise bedienen.
Man beachte, dass im Zusammenhang mit $\mathbb{C}$ nur algebraische Gesichtspunkte im Spiel waren, keine ordnungstheoretischen. Der Grund:

[18] Um weitere potentielle Unklarheiten zu vermeiden, verwenden wir das Symbol $\sqrt{t}$ ausschließlich dann, wenn $t$ eine nichtnegative reelle Zahl ist; in diesem Fall bezeichnet $\sqrt{t}$ jene eindeutig bestimmte nichtnegative reelle Zahl $r$ mit $r^2 = t$.

**Satz 1.2.4.5.** *Es gibt keine Ordnungsrelation, die $\mathbb{C}$ zu einem angeordneten Körper macht.*

**UE 36 ▶ Übungsaufgabe 1.2.4.6.** (W) Beweisen Sie Satz 1.2.4.5. **◀ UE 36**

Es sei hervorgehoben, dass in Satz 1.2.4.3 auf die Forderung $\psi(a,0) = \varphi(a)$ nicht verzichtet werden kann. Auf den ersten Blick und angesichts von Aufgabe 3.5.3.13 mag das erstaunen. Der Körper $\mathbb{C}$ besitzt aber unüberschaubar viele[19] Automorphismen. Eine sorgfältige Konstruktion würde an dieser Stelle zu weit führen (nicht zuletzt deshalb, weil eine explizite Konstruktion ohne Verwendung des Auswahlaxioms bzw. des Zornschen Lemmas gar nicht möglich ist).
Die enorme Bedeutung der komplexen Zahlen für große Teile der Mathematik (insbesondere auch für die Analysis) liegt nicht nur, aber zu einem guten Teil daran, dass Körper der komplexen Zahlen *algebraisch abgeschlossen* ist.

**Definition 1.2.4.7.** Ein Körper $K$ heißt *algebraisch abgeschlossen*, wenn jedes Polynom

$$p(x) = \sum_{k=0}^{n} a_k x^k$$

mit $a_k \in K$, $n \geq 1$ und $a_n \neq 0$ mindestens eine Nullstelle in $K$ hat.

Dass der Körper $\mathbb{C}$ diese Eigenschaft hat, ist einer der großen Sätze der Mathematik:

**Satz 1.2.4.8** (Fundamentalsatz der Algebra, Fassung 1)**.** *Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.*

Trotz seines Namens ist der analytische Charakter des Fundamentalsatzes mindestens ebenso stark ausgeprägt wie der algebraische. Denn in der einen oder anderen Weise muss die Vollständigkeit der reellen Zahlen eingesetzt werden. Die ersten Beweise, die modernen Ansprüchen genügen, wurden von Carl Friedrich Gauß (1777–1855) erbracht. Mittlerweile gibt es zahlreiche Beweise. Auch wir werden mehrere kennen lernen, vorzugsweise solche mit starkem algebraischen Anteil. Andere Beweise betonen den topologischen Aspekt oder verwenden vergleichsweise starke Geschütze aus der komplexen Analysis. Ein relativ leicht zugänglicher ist vermutlich bereits aus der Analysis-Grundvorlesung bekannt: Man zeigt erstens, dass für ein Polynom $p$ die Funktion $|p|$, die jedem $z \in \mathbb{C}$ den Wert $|p(z)| \in \mathbb{R}_{\geq 0}$ zuordnet, ein (globales) Minimum haben muss, und zweitens, dass der Wert dieses Minimums nicht $> 0$ sein kann:

1. Sei also das komplexe Polynom $p(z) = \sum_{k=0}^{n} a_k z^k$ mit $a_k \in \mathbb{C}$, $n \geq 1$ und $a_n \neq 0$ vorgegeben. Für eine genügend große reelle Zahl $R$ gilt $\forall z \in \mathbb{C} : |z| \geq R \Rightarrow |p(z)| > |a_0| = |p(0)|$ (warum?). Auf der kompakten Kreisscheibe $D$ um 0 mit Radius $R$ nimmt $|p|$ als stetige Funktion an einem Punkt $z_0 \in D$ einen minimalen Wert an, der dann globales Minimum von $|p|$ auf ganz $\mathbb{C}$ sein muss (warum?).

[19] Zum Beispiel gibt es einen Automorphismus von ganz $\mathbb{C}$, der die drei Lösungen der Gleichung $x^3 - 2 = 0$ zyklisch vertauscht.

2. Ohne Beschränkung der Allgemeinheit ist $z_0 = 0$ (warum? Ersetze $p$ durch das Polynom $q(z) := p(z + z_0)$.) Wenn nun $z_0$ keine Nullstelle von $p$ wäre, dann hätte $p(z)$ ohne Beschränkung der Allgemeinheit die Form $p(z) = 1 + a_k z^k + \cdots + a_n z^n$ mit $k \geq 1$, $a_k \neq 0$ (warum?). Wähle $c \in \mathbb{C}$ so, dass $c^k = -1/a_k$ gilt, und betrachte $p(c\varepsilon)$ für kleines $\varepsilon > 0$, um einen Widerspruch herzuleiten.

**UE 37** ► **Übungsaufgabe 1.2.4.9.** (V) Führen Sie den oben skizzierten Beweis des Fundamentalsatzes genauer aus. ◄ **UE 37**

Der Fundamentalsatz lässt sich auch so lesen: Es gibt keine algebraischen und folglich (wie wir in 6.1.4 sehen werden) keine endlichdimensionalen Erweiterungen von $\mathbb{C}$ als Körper. Mit den komplexen Zahlen ist somit ein Abschluss der Zahlenbereichserweiterungen erreicht. Trotzdem sind Erweiterungen möglich: entweder sogenannte transzendente, also unendlichdimensionale (mehr hierüber insbesondere in 6.1.5) oder endlichdimensionale, bei denen aber gewisse Eigenschaften eines Körpers verloren gehen.
Verzichtet man lediglich auf die Kommutativität der Multiplikation, so gibt es den *Schiefkörper* $\mathbb{H}$ der sogenannten Hamiltonschen *Quaternionen*. Als Vektorraum über $\mathbb{R}$ ist er 4-dimensional. Eine Basis ist gegeben durch Elemente, die man traditionell mit $1, i, j, k$ bezeichnet. Dabei fasst man 1 und $i$ als die entsprechenden komplexen Zahlen auf, $j$ und $k$ als zusätzliche sogenannte imaginäre Einheiten, von denen jede dieselbe Rolle spielt wie $i$, d.h. $i^2 = j^2 = k^2 = -1$. Insbesondere hat jedes $z \in \mathbb{H}$ eine eindeutige Darstellung $z = r_1 1 + r_2 i + r_3 j + r_4 k$ mit $r_1, r_2, r_3, r_4 \in \mathbb{R}$. Weiterhin ist 1 neutrales Element bezüglich der Multiplikation. Außerdem gilt $ij = k = -ji$, $jk = i = -kj$ und $ki = j = -ik$, sowie $rz = zr$ für alle $z \in \mathbb{H}$ und alle $r \in \mathbb{R} \subseteq \mathbb{C} \subseteq \mathbb{H}$.

**UE 38** ► **Übungsaufgabe 1.2.4.10.** (B,E) Zeigen Sie: Es gibt tatsächlich einen sogar (bis auf Isomorphie) eindeutig bestimmten Schiefkörper $\mathbb{H}$ mit den angegebenen Eigenschaften. Anleitung für die Existenz eines solchen Schiefkörpers: Realisieren Sie $\mathbb{H}$ als eine vierparametrige Menge reeller $4 \times 4$-Matrizen $A(r_1, r_2, r_3, r_4)$. Gehen Sie dabei davon aus, dass die Multiplikation mit einer Quaternion $z = r_1 1 + r_2 i + r_3 j + r_4 k$ einer linearen Transformation des Raumes $\mathbb{R}^4$ entspricht, und ordnen Sie diesem $z$ die entsprechende Matrix zu. Überzeugen Sie sich, dass diese Zuordnung $z \mapsto A(r_1, r_2, r_3, r_4)$ eine isomorphe Einbettung ist. Überprüfen Sie, dass die Spaltenvektoren von $A(r_1, r_2, r_3, r_4)$ orthogonal (nicht notwendig normiert!) mit Determinante $\sqrt{r_1^2 + r_2^2 + r_3^2 + r_4^2}$ sind. Hieraus folgt leicht, dass es sich bei $\mathbb{H}$ nicht nur um einen Ring mit 1, sondern um einen Schiefkörper handelt. ◄ **UE 38**

Schwächt man die Forderungen an einen Körper, z.B. die Assoziativität der Multiplikation noch weiter ab, finden sich auch noch weitere Strukturen höherer Dimension.

## 1.3 Paradigmen aus der Linearen Algebra

In diesem Abschnitt rekapitulieren wir wichtige Begriffe und Resultate aus der Linearen Algebra, um erste Beispiele von Klassifikationssätzen zu erhalten: Mit Hilfe des Begriffs

der Linearen (Un-)Abhängigkeit (1.3.1) lässt sich das Austauschlemma formulieren und beweisen (1.3.2). Darauf fußt (wenigstens für endlich erzeugte Vektorräume) der Dimensionsbegriff, der eine vollständige Klassifikation aller Vektorräume über einem festen Körper ermöglicht (1.3.3). Daran anschließend lassen sich entsprechende Fragen auch für lineare Abbildungen (die zwischen Vektorräumen die interessanten sind) formulieren und beweisen (1.3.4).

### 1.3.1 Lineare (Un-)Abhängigkeit

Inhalt in Kurzfassung: Der Vollständigkeit halber werden einige Grundlagen aus der Linearen Algebra wiederholt. Besonders interessant in Hinblick auf spätere Verallgemeinerungen: der Fortsetzungssatz für lineare Abbildungen und die Existenz von Basen.

Aus der Linearen Algebra sind die folgenden Begriffe bekannt:

**Definition 1.3.1.1.** Sei $V$ ein Vektorraum über dem Körper (oder auch Schiefkörper) $K$. Für jede Teilmenge $T \subseteq V$ schreiben wir $[T]$ für die *lineare Hülle* von $T$, also für den Durchschnitt aller Untervektorräume $U \leq V$, die $T \subseteq U$ erfüllen. Eine Menge $T$ heißt *linear abhängig*, wenn es ein $t \in T$ gibt mit $t \in [T \setminus \{t\}]$. (Das heißt: $t$ lässt sich als $K$-Linearkombination von Vektoren in $T \setminus \{t\}$, genauer: von einer endlichen Teilmenge von $T \setminus \{t\}$, schreiben.)
Äquivalent: der Nullvektor lässt sich als nichttriviale Linearkombination (von endlich vielen Vektoren in $T$) darstellen.
Eine Menge $S$ von Vektoren heißt *linear unabhängig*, wenn sie nicht linear abhängig ist; äquivalent: wenn sich jeder Vektor in $[S]$ auf genau eine Weise als Linearkombination von Vektoren in $S$ schreiben lässt.
Ein *Erzeugendensystem* von $V$ ist eine Teilmenge $E$ mit $[E] = V$.
Eine Teilmenge $B$ von $V$ heißt *Basis* von $V$, wenn die folgenden (äquivalenten) Bedingungen erfüllt sind:

- $B$ ist minimales[20] Erzeugendensystem, das heißt: $[B] = V$ aber $[B'] \neq V$ für alle echten Teilmengen $B' \subsetneq B$.
- $B$ ist linear unabhängiges Erzeugendensystem.
- $B$ ist maximale[21] linear unabhängige Menge, das heißt: $B$ ist l.u., aber es gibt keine l.u. echte Obermenge $B' \supsetneq B$.

Man beachte, dass die leere Menge $\emptyset$ stets linear unabhängig ist, während eine Menge, die den Nullvektor $\vec{0}$ enthält, immer linear abhängig ist.
Aus der Definition ergibt sich leicht:

**Satz 1.3.1.2.** *Sei $B$ Basis von $V$, und sei $W$ ein beliebiger Vektorraum über dem Körper oder Schiefkörper $K$. Dann gibt es für jede Funktion $f\colon B \to W$ genau eine lineare Abbildung $\varphi\colon V \to W$, die $f$ fortsetzt.*

[20] Man beachtet, dass hier Minimalität in Bezug auf die partielle Ordnung $\subseteq$ gemeint ist, nicht Minimalität in Bezug auf „Größe“ im Sinne von Kardinalität.
[21] Auch hier geht es nicht um Maximalität im Sinne der Kardinalität.

Aus der linearen Unabhängigkeit $B$ folgt nämlich, dass die durch

$$\varphi\left(\sum_{b\in B} x_b b\right) := \sum_{b\in B} x_b f(b)$$

definierte Abbildung wohldefiniert ist. Weil $B$ Erzeugendensystem ist, ist $\varphi$ auf ganz $V$ definiert; die Linearität von $\varphi$ ergibt sich aus der Definition.
Mit Hilfe des Auswahlaxioms kann man zeigen, dass jeder Vektorraum eine Basis hat. Man kann sogar den folgenden stärkeren Satz zeigen:

**Satz 1.3.1.3.** *Sei $V$ Vektorraum, und sei $L \subseteq V$ eine linear unabhängige Menge. Dann gibt es eine Basis $B$ von $V$ mit $L \subseteq B$.*

## 1.3.2 Das Austauschlemma und seine Konsequenzen

Inhalt in Kurzfassung: Für endlich erzeugte Vektorräume hat das Austauschlemma zur Folge, dass je zwei Basen gleich viele Elemente haben. Auch dieses Motiv wird später Verallgemeinerungen ermöglichen (Schlagwort Transzendenzbasen; siehe Definition 6.1.5.1).

Die Sätze aus diesem Abschnitt sind aus der Linearen Algebra bereits bekannt. Wir führen sie deshalb nochmals explizit an, weil wir später (in Abschnitt 6.1.5) mit ganz ähnlichen Konzepten/Beweisen algebraische Unabhängigkeit statt linearer Unabhängigkeit untersuchen können.
Für jeden $K$-Vektorraum $V$ und jede Teilmenge $A \subseteq V$ schreiben wir $[A]$ für die $K$-lineare Hülle von $A$.

**Lemma 1.3.2.1** (Austauschlemma)**.** *Sei $V$ ein $K$-Vektorraum, $A \subseteq V$, $b, c \in V$. Wenn $c \in [A \cup \{b\}]$ aber $c \notin [A]$ gilt, dann ist $b \in [A \cup \{c\}]$.*

*Beweis.* Der Vektor $c$ lässt sich als Linearkombination $c = \lambda b + \sum_{i\in I} \lambda_i a_i$ schreiben, mit $I$ endlich, $\lambda, \lambda_i \in K$, $a_i \in V$. Es muss $\lambda \neq 0$ gelten, sonst wäre $c$ in $[A]$. Daher lässt sich $b$ als $\frac{1}{\lambda}(c - \sum_i \lambda_i a_a)$ schreiben, also $b \in [A \cup \{c\}]$. □

**Folgerung 1.3.2.2.** *Wenn $V$, $A$, $b$, $c$ die Voraussetzungen des Austauschlemmas erfüllen, dann gilt $[A \cup \{b\}] = [A \cup \{c\}]$.*
*Wenn $A$ überdies linear unabhängig war, dann sind auch $A \cup \{b\}$ und $A \cup \{c\}$ linear unabhängig.*

**Folgerung 1.3.2.3** (Austauschsatz von Steinitz[22])**.** *Wenn $B$ und $C$ Basen des $K$-Vektorraums $V$ sind, dann gibt es für jedes $b \in B$ ein $c \in C$, sodass $(B \setminus \{b\}) \cup \{c\}$ wiederum eine Basis ist.*

*Beweis.* Sei $b \in B$. Die Annahme $C \subseteq [B \setminus \{b\}]$ führt via $V = [C] \subseteq [[B \setminus \{b\}]] = [B \setminus \{b\}] \subsetneq V$ zu einem Widerspruch, daher gibt es ein $c$ mit $c \notin [B \setminus \{b\}]$. Nach dem Austauschlemma gilt $b \in [(B\setminus\{b\})\cup\{c\}]$. Daher ist $(B\setminus\{b\})\cup\{c\}$ ein Erzeugendensystem, und nach Korollar 1.3.2.2 sogar eine Basis. □

[22] Ernst Steinitz (1871-1928)

**Lemma 1.3.2.4.** *Sei $V$ Vektorraum mit einer endlichen Basis $B$. Dann gilt: Für jede Basis $C$ von $V$ gilt $|B| = |C|$, also: alle Basen von $V$ haben die gleiche (endliche) Kardinalität.*

*Beweis.* Sei $C_0 := C$. Wenn $B \neq C_0$ ist, sei $c \in C_0 \setminus B$ beliebig. (So ein $c$ gibt es, sonst wäre $C_0 \subsetneq B$, was für Basen unmöglich ist.)
Wir finden mit dem Austauschsatz von Steinitz (mit vertauschten Rollen von $B$ und $C$) ein $b \in B$, sodass $C_1 := (C_0 \setminus \{c\}) \cup \{b\}$ noch immer eine Basis ist, wobei $|C_0| = |C_1|$. Wir wissen $b \notin C_0$, denn sonst wäre ja $C_0 \setminus \{c\}$ eine Basis; weil $b$ ein neues Element von $B \cap C_1$ ist, gilt $|B \cap C_1| = |B \cap C_0| + 1$. Mit Induktion finden wir weitere Basen $C_2$, $C_3$, ... die alle gleich groß sind, aber immer größeren Schnitt mit $B$ haben. Nach höchstens $|B|$ Schritten müssen wir eine Basis $C_k$ erhalten, für die $C_k = B$ gilt. Wegen $|C_0| = |C_1| = \cdots = |C_k|$ erhalten wir $|C| = |B|$. □

### 1.3.3 Die Klassifikation beliebiger Vektorräume durch ihre Dimension

Inhalt in Kurzfassung: Da je zwei Basen eines Vektorraums gleich viele Elemente enthalten, kann deren Anzahl als Definition der Dimension dieses Vektorraums dienen. Es zeigt sich, dass die Vektorräume über einem gegebenen Körper mit dieser Zahl in folgendem Sinne klassifiziert werden können: Zwei Vektorräume sind genau dann isomorph, wenn sie dieselbe Dimension haben.

Die Eindeutigkeit der Kardinalität einer Basis (somit auch die Sinnhaftigkeit der Definition der Dimension) lässt sich für beliebige Vektorräume beweisen, unabhängig von der Größe ihrer Erzeugendensysteme.

**Lemma 1.3.3.1.** *Sei $V$ Vektorraum über $K$, sei $B \subseteq V$ Basis, und sei $C \subseteq V$, $|C| < |B|$. Dann ist $C$ kein Erzeugendensystem: $[C] \subsetneq V$.*

**Korollar 1.3.3.2.** Seien $B_1$, $B_2$ Basen von $V$. Dann gilt $B_1 \approx B_2$.

*Beweis von Lemma 1.3.3.1.* Ist $V$ endlichdimensional, so folgt die Behauptung aus Lemma 1.3.2.4.
Sei also $V$ nicht endlichdimensional. Dann müssen $B$ und $C$ unendlich sein.
Für jedes $c \in C$ gibt es eine endliche Menge $S_c \subseteq B$ mit $c \in [S_c]$. Da die Mengen $S_c$ alle endlich sind, kann die Menge $\bigcup_{c \in C} S_c$ höchstens die Kardinalität $|C| < |B|$ haben (siehe Anhang, genauer: 11.4.8), also ist die Menge $S := \bigcup_{c \in C} S_c$ eine echte Teilmenge von $B$. Nun war aber $B$ eine minimales Erzeugendensystem, daher gilt

$$[S] \subsetneq [B] = V.$$

Andererseits gilt $\forall c \in C : c \in [S_c] \subseteq [S]$, daher $C \subseteq [S]$ und somit

$$[C] \subseteq [S].$$

Also ist $C$ kein Erzeugendensystem von $V$. □

Zusammen mit Satz 1.3.1.3, wonach jeder Vektorraum eine Basis besitzt ($L = \emptyset$ setzen), können wir nun die Dimension eines Vektorraumes definieren.

**Definition 1.3.3.3.** Die *Dimension* $\dim_K V$ eines Vektoraumes $V$ über dem Körper $K$ ist definiert als die Kardinalität einer (und somit jeder beliebigen) Basis von $V$.

Zusammenfassend erhalten wir:

**Satz 1.3.3.4** (Klassifizierung der $K$-Vektorräume)**.** *Für zwei Vektorräume $V_1$ und $V_2$ über demselben Körper $K$ sind die folgenden beiden Aussagen äquivalent:*

(1) $V_1 \cong V_2$. *($V_1$ und $V_2$ sind isomorph, d.h. definitionsgemäß: Es gibt eine $K$-lineare Bijektion $f\colon V_1 \to V_2$, und die inverse Abbildung ist auch $K$-linear.)*

(2) $\dim_K V_1 = \dim_K V_2$. *(Je zwei Basen $B_1$ von $V_1$ und $B_2$ von $V_2$ sind gleichmächtig, d.h. definitionsgemäß: Es gibt eine Bijektion $g\colon B_1 \to B_2$.)*

*Kurz gesagt: $K$-Vektorräume sind durch ihre Dimension eindeutig (bis auf $K$-Isomorphie) bestimmt.*

**UE 39** ► **Übungsaufgabe 1.3.3.5.** (F) Wir nennen Unterräume $U_1, U_2$ eines Vektorraums $V$ äquivalent ($U_1 \sim U_2$), wenn es einen Automorphismus $f : V \to V$ gibt, der $f(U_1) = U_2$ erfüllt. ◄ **UE 39**

(1) Zeigen Sie, dass zwei Unterräume eines endlichdimensionalen Vektorraums genau dann äquivalent sind, wenn sie die gleiche Dimension haben.

(2) Zeigen Sie anhand eines Beispiels, dass dies für unendlichdimensionale Vektorräume nicht immer gilt.

(3) Finden Sie eine Charakterisierung der Relation $\sim$, die auch für unendlichdimensionale Vektorräume funktioniert. (Hinweis: Kodimension.)

### 1.3.4 Die Klassifikation linearer Abbildungen

Inhalt in Kurzfassung: Nicht nur Vektorräume können in kanonischer Weise – nämlich bezüglich Isomorphie durch die Dimension – klassifiziert werden, sondern auch lineare Abbildungen (Matrizen) – nämlich bezüglich Äquivalenz durch den Rang. Im Falle von Abbildungen von einem Vektorraum in sich über einem algebraisch abgeschlossenen Körper bietet sich auch noch eine zweite Klassifikation an – nämlich bezüglich Ähnlichkeit durch die Jordansche Normalform. All diese Konzepte sind Wiederholungen aus der Linearen Algebra unter Hervorhebung gewisser für die Algebra charakteristischer Aspekte.

Da wir Vektorräume bis auf lineare Isomorphie klassifiziert haben, bietet es sich an, auch die Isomorphien (und allgemeiner: die linearen Abbildungen) zwischen Vektorräumen zu klassifizieren.
Für jeden $K$-Vektorraum $V$ definieren wir $\mathrm{Aut}(V)$ als die Menge aller linearen Bijektionen $f\colon V \to V$.
Wir interessieren uns für die folgenden beiden Äquivalenzrelationen zwischen Abbildungen.

**Definition 1.3.4.1.** Sei $K$ ein Körper, und seien $V$ und $W$ Vektorräume über $K$.

1. Wir nennen zwei Abbildungen $f, g\colon V \to W$ *äquivalent*, wenn es Automorphismen $c \in \mathrm{Aut}(V)$ und $d \in \mathrm{Aut}(W)$ gibt mit $g \circ c = d \circ f$.

$$\begin{array}{ccc} V & \xrightarrow{c} & V \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} \\ W & \xrightarrow{d} & W \end{array}$$

2. Für Selbstabbildungen $f\colon V \to V$ passt der folgende Begriff besser:
   Wir nennen zwei Abbildungen $f, g\colon V \to V$ *ähnlich*, wenn es einen Automorphismus $c \in \mathrm{Aut}(V)$ gibt mit $c \circ f = g \circ c$.

$$\begin{array}{ccc} V & \xrightarrow{c} & V \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} \\ V & \xrightarrow{c} & V \end{array}$$

Für endlichdimensionale Vektorräume $V, W$ lassen sich die linearen Abbildungen $f\colon V \to W$ bis auf Äquivalenz durch ihren Rang klassifizieren.

**Definition 1.3.4.2.** Der *Rang* von $f\colon V \to W$ ist die Dimension des Bildes: $\mathrm{rang}(f) := \dim f(V)$.

**Satz 1.3.4.3.** *Seien $f, g\colon V \to W$ lineare Abbildungen zwischen Vektorräumen, und sei $\dim W < \infty$. Dann sind $f$ und $g$ genau dann äquivalent, wenn sie den gleichen Rang haben.*

**UE 40** ► **Übungsaufgabe 1.3.4.4.** (F) Wir betrachten Tripel $(V, f, W)$, wobei $V$ und $W$ endlichdimensionale Vektorräume über einem festen Körper $K$ sind, und $f\colon V \to W$ eine lineare Abbildung. Wir definieren eine Äquivalenzrelation $\sim$ auf der Klasse aller solchen Tripel: $(V, f, W) \sim (V', f', W')$ gilt genau dann, wenn es Isomorphismen $i\colon V \to V'$ und $j\colon W \to W'$ gibt, die $j \circ f = f' \circ i$ erfüllen. ◄ **UE 40**
Charakterisieren Sie die Äquivalenzklasse eines Tripels $(V_0, f_0, W_0)$ durch Dimensionsüberlegungen analog zu Satz 1.3.4.3:

$$[(V_0, f_0, W_0)]_\sim = \{(V, f, W) \mid \cdots ? \cdots\}$$

Für Selbstabbildungen eines endlichdimensionalen Vektorraums führen wir den folgenden Satz aus der Linearen Algebra ohne Beweis an.

**Definition 1.3.4.5.** Eine lineare Selbstabbildung $f$ eines endlichdimensionalen $K$-Vektorraums $V$ heißt *Jordan-Kästchen* bezüglich der Basis $b_1, \ldots, b_k$ wenn es ein $\lambda \in K$ gibt, sodass $f(b_1) = \lambda b_1$, $f(b_i) = b_{i-1} + \lambda b_i$ für alle $i \in \{2, \ldots, k\}$. Bezüglich dieser Basis entspricht der Abbildung $f$ dann die Matrix

$$\begin{pmatrix} \lambda & 1 & 0 & \ldots & \\ 0 & \lambda & 1 & \ldots & \\ & \ddots & \ddots & \ddots & \\ 0 & \ldots & 0 & \lambda & 1 \\ 0 & \ldots & \ldots & 0 & \lambda \end{pmatrix}$$

mit dem einzigen Eigenwert $\lambda$.
Eine lineare Abbildung $f\colon V \to V$ ist in Jordan-Normalform in Bezug auf eine Basis $B$, wenn es eine Partition $B = B_1 \cup \cdots \cup B_n$ gibt, sodass für alle $i$ die Abbildung $f$ die Beziehung $f([B_i]) \subseteq [B_i]$ erfüllt, und jede der Abbildungen $f{\restriction}[B_i]\colon [B_i] \to [B_i]$ ein Jordan-Kästchen bezüglich $B_i$ ist.

**Satz 1.3.4.6.** *Sei $V$ ein endlichdimensionaler Vektorraum über dem algebraisch abgeschlossenen Körper $K$. Dann gibt es zu jeder linearen Selbstabbildung $f\colon V \to V$ eine Basis $B$, sodass $f$ in Jordan-Normalform bezüglich $B$ ist. Überdies sind die Dimensionen der auftretenden Jordan-Kästchen sowie die zu den Jordan-Kästchen gehörenden Eigenwerte durch $f$ eindeutig bestimmt.*

# 2 Grundbegriffe

Hier beginnt der systematisch aufbauende Teil der Vorlesung. In den bisherigen Abschnitten wurden die (überwiegend bereits vertrauten) Zahlenbereichskonstruktionen unter algebraischen Gesichtspunkten rekapituliert. Nun geht es um einen gemeinsamen begrifflichen Rahmen für die Untersuchung der behandelten Strukturen und für natürliche Verallgemeinerungen. Ein erster solcher Rahmen, der auch dem Zugang in der mathematischen Logik, insbesondere der Modelltheorie entspricht, wird in Abschnitt 2.1 entwickelt. Dabei handelt es sich im Wesentlichen um die Sichtweise der sogenannten *Allgemeinen* oder auch *Universellen Algebra*. Noch abstrakter und in mancherlei Hinsicht dem strukturtheoretischen Denken der klassischen Algebra besser angepasst ist die Kategorientheorie, deren allererste Anfänge Inhalt von Abschnitt 2.2 sind. In Abschnitt 2.3 wird es dann wieder etwas konkreter, wenn es um Unteralgebren, direkte Produkte, homomorphe Bilder und Isomorphiesätze geht.

## 2.1 Der logisch-modelltheoretische Rahmen der allgemeinen Algebra

In diesem Abschnitt wird ein recht weiter begrifflicher Rahmen gesteckt, innerhalb dessen die meisten strukturtheoretischen Anliegen, die uns auch noch in weiterer Folge beschäftigen werden, einheitlich abgehandelt werden können. Entsprechend beginnen wir mit der Rekapitulation notationeller und terminologischer Konventionen (2.1.1) und Grundbegriffen der Ordnungstheorie (2.1.2), wo eine Menge durch gewisse Relationen Struktur erhält. Sind es statt Relationen Operationen, so liegt eine universelle Algebra vor (2.1.3). Die Synthese beider Strukturelemente nennt man auch eine Relationale Strukturen (2.1.4). Verbindendes Element von Strukturen sind Homomorphismen zwischen Algebren (2.1.5) bzw. strukturverträgliche Abbildungen zwischen relationalen Strukturen (2.1.6). In beiden Fällen kann die Klassifikation modulo Isomorphie als generelles Paradigma der Algebra verstanden werden (2.1.7). Weitere Themen, die in diesem Abschnitt angeschnitten werden, sind Terme, Termalgebra, Gesetze und Varietäten (2.1.8), die mathematische Logik in Form eines kurzen Exkurses (2.1.9) und Strukturen innerhalb derer Funktionen unterschiedlicher Stelligkeit eingesetzt werden können, sogenannte Klone (2.1.10).

### 2.1.1 Notation und Terminologie

Inhalt in Kurzfassung: Weitgehend bereits aus dem ersten Semester bekannte Grundbegriffe werden der Vollständigkeit halber zusammengestellt und in der Algebra wichtige Eigenschaften und Gesichtspunkte hervorgehoben. Beispiele solcher Grundbegriffe sind:

kartesisches Produkt, geordnetes Paar, Relation, Funktion/Abbildung, injektiv, surjektiv, bijektiv, Relationenprodukt mit der Verkettung von Abbildungen als Spezialfall, inverse Relation/Abbildung, (Halb-)Ordnungsrelation, Äquivalenzrelation und Quasiordnung.

Jahrtausendelang kam die Logik kaum über jene sogenannten *Syllogismen* hinaus, die Aristoteles schon im vierten Jahrhundert vor unserer Zeitrechnung formuliert hat. Dabei handelt es sich um Schlussfiguren wie jene nach dem berühmten Beispiel:

Alle Menschen sind sterblich. Sokrates ist ein Mensch. Also ist Sokrates sterblich.

Heute können wir dafür auch formal schreiben:

$$((\forall x : (m(x) \to s(x))) \wedge m(S)) \to s(S).$$

Dabei stehen die Symbole $m$ und $s$ für die Prädikate „ist Mensch“ bzw. „ist sterblich“, $S$ für Sokrates. Denkt man in diesem Zusammenhang an wichtige mathematische Konzepte wie etwa die Definition

$$\forall \varepsilon > 0 \; \exists n_0 = n_0(\varepsilon) \; \forall n \geq n_0 : \; |x_n - \alpha| < \varepsilon$$

für die Grenzwertbeziehung $\lim_{n\to\infty} x_n = \alpha$ einer Folge $(x_n)_{n\in\mathbb{N}}$, so beobachten wir: In den Formeln können Teilaussagen (im Beispiel: $|x_n - \alpha| < \varepsilon$) vorkommen, die nicht nur von einem Objekt abhängen (wie die Prädikate bei Aristoteles), sondern von mehreren (im Beispiel: vom Folgenindex $n$, der reellen Zahl $\alpha$ und der positiven reellen Zahl $\varepsilon$). Zur formalen Beschreibung sind also mehrstellige Prädikate erforderlich. In mengentheoretischer Terminologie entsprechen dem Teilmengen $n$-facher kartesischer Produkte, also Mengen von $n$-Tupeln. Kazimierz Kuratowski (1896–1980) folgend definieren wir daher:

**Definition 2.1.1.1.** Für beliebige Objekte (Mengen) $a, b$ ist das *geordnete Paar*[1] $(a, b)$ die Menge $\{\{a\}, \{a, b\}\}$. Das *kartesische Produkt* zweier beliebiger Mengen $A, B$ definieren wir durch $A \times B := \{(a, b) : \; a \in A, b \in B\}$. Rekursiv definieren wir für $n = 1, 2, \ldots$ und für Mengen $A_1, \ldots, A_n$ außerdem $A_1 \times \cdots \times A_n \times A_{n+1} := (A_1 \times A_2 \times \cdots \times A_n) \times A_{n+1}$, im Falle $A_1 = A_2 = \cdots = A$ entsprechend $A^1 := A$, $A^{n+1} := A^n \times A$. Wir schreiben für $a \in A = A^1$ gelegentlich auch $(a)$, für $((a_1, a_2), a_3) \in (A_1 \times A_2) \times A_3 = A_1 \times A_2 \times A_3$ meist $(a_1, a_2, a_3)$ etc. Schließlich vereinbaren wir $A^0 := \{\emptyset\}$.
Teilmengen $\rho$ von $A_1 \times \ldots \times A_n$ heißen auch *$n$-stellige Relationen* zwischen den Mengen $A_1, \ldots, A_n$. Im Fall $n = 2$, $A_1 = A_2 = A$ heißt $\rho$ auch eine *binäre Relation*[2] auf $A$. Für $(a, b) \in \rho$ schreiben wir auch $a\rho b$.

[1] Die wesentliche Eigenschaft dieses Paarbegriffs: $(a_1, b_1) = (a_2, b_2)$ genau dann, wenn $a_1 = a_2$ und $b_1 = b_2$. Es gibt auch andere formale Definitionen des geordneten Paares, welche unsere Zwecke gleich gut erfüllen wie die hier gewählte. Es soll nur verdeutlicht werden, dass der Begriff des geordneten Paares im Rahmen der Mengenlehre definiert werden kann und dafür neben den Mengen keine weitere Sorte von Ausgangsobjekten vonnöten ist.

[2] Man beachte, dass wir Relationen nicht nur als Aussagen oder Prädikate betrachten, sondern als *Objekte*. Die Formeln $3 < 4$ ist eine Aussage über die Zahlen 3 und 4, aber die Relation $<$ (auf den natürlichen Zahlen) ist ein Objekt, konkreter: eine Menge, nämlich eine Mengen von Paaren. Man kann also mit Relationen mengentheoretische Operationen ausführen (zum Beispiel den Durchschnitt zweier Relationen bilden).

Gibt es für eine Relation $\rho$ zwischen $A$ und $B$ zu jedem $a \in A$ genau ein $b \in B$ mit $(a, b) \in \rho$, so heißt $\rho$ auch *Funktion*[3] oder *Abbildung* von $A$ nach $B$, symbolisch

$$\rho\colon A \to B.$$

In diesem Fall schreiben wir $\rho(a)$ für jenes $b \in B$ mit $a\rho b$ oder auch $\rho : a \mapsto b$. Eine Abbildung $\rho\colon A \to B$ heißt *injektiv*[4] */surjektiv*[5]*/bijektiv*[6], falls es zu jedem $b \in B$ höchstens/mindestens/genau ein $a \in A$ gibt mit $f(a) = b$.[7]
Für eine Abbildung $f\colon A \to B$ sowie Teilmengen $A_0 \subseteq A$ und $B_0 \subseteq B$ sind die Schreibweisen $f(A_0) := \{f(a) : \ a \in A_0\}$ für das soganannte *Bild* der Menge $A_0$ und $f^{-1}(B_0) := \{a \in A : \ f(a) \in B_0\}$ für das *Urbild* der Menge $B_0$ unter $f$ gebräuchlich. Unter der *Einschränkung* $f\restriction A_0$ von $f$ auf $A_0$ versteht man die Menge $f \cap (A_0 \times B)$, die offensichtlich selbst eine Abbildung $f\restriction A_0\colon A_0 \to B$ ist.
Wir wenden uns auch der Komposition von Abbildungen und — allgemeiner — Relationen zu.

**Definition 2.1.1.2.** Seien $\rho_1 \subseteq A \times B$ und $\rho_2 \subseteq B \times C$ Relationen. Dann ist das *Relationenprodukt* (genannt auch Verkettung, Komposition, Verknüpfung oder Hintereinanderausführung von Relationen oder, gegebenenfalls, Funktionen) als die Menge

$$\{\, (a, c) \in A \times C \mid \exists b \in B : (a, b) \in \rho_1 \text{ und } (b, c) \in \rho_2 \,\}$$

definiert.
Für diese Operation auf Relationen gibt es zwei einander widersprechende Schreibweisen: Einerseits könnte man dieses Produkt $\rho_1 \circ \rho_2$ nennen, weil dann

$$a(\rho_1 \circ \rho_2)c \ \Leftrightarrow \ \exists b \in B : a \ \rho_1 \ b \ \rho_2 \ c$$

gilt, andererseits ist im Spezialfall, dass $\rho_1$ und $\rho_2$ Funktionen sind, die Schreibweise $\rho_2 \circ \rho_1$ üblich[8], weil dann

$$\rho_2(\rho_1(a)) = (\rho_2 \circ \rho_1)(a)$$

[3] Manche Lehrbücher verlangen, dass eine Funktion $F$ durch eine Relation $\rho$, eine Definitionsmenge $A$ und eine Zielmenge $B$ festgelegt wird, also etwa $F = (A, \rho, B)$, und bezeichnen $\rho$ als den „Graphen der Funktion $F$“. Wir identifizieren eine Funktion mit ihrem Graphen $\rho$; die Definitionsmenge ist durch $\rho$ eindeutig bestimmt als die Menge $\{a \mid \exists b : (a, b) \in \rho\}$; die Zielmenge kann irgendeine Menge sein, die $\{b \mid \exists a : (a, b) \in \rho\}$ enthält, und ergibt sich meist aus dem Kontext.
Beachten Sie, dass man die Injektivität einer Funktion aus ihrem Graphen ablesen kann; Surjektivität ist hingegen keine Eigenschaft der Funktion selbst, sondern eine Beziehung zwischen einer Funktion und einer Zielmenge. So ist zum Beispiel die Funktion $\{(x, x^2) : x \in \mathbb{R}\}$ surjektiv von $\mathbb{R}$ auf $\mathbb{R}_{\geq 0}$, aber nicht surjektiv von $\mathbb{R}$ auf $\mathbb{R}$.

[4] englisch: *injective* oder *one-to-one, 1-1*

[5] englisch: *surjective* oder *onto B*

[6] englisch: *bijective*

[7] Anmerkung zur Injektivität: Eine Abbildung $f\colon A \to B$ ist injektiv, wenn für alle $x_1, x_2 \in A$ die Implikation $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$ gilt. Äquivalent dazu ist die Implikation $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$; letztere Implikation ist oft leichter nachzuprüfen, weil wir mit Gleichungen besser umgehen können als mit Ungleichungen.

[8] Die Notation $f(x)$ für Funktionsanwendung geht auf Leonhard Euler (1707–1783) zurück. Grundsätzlich spräche aber nichts dagegen und manches dafür, das Objekt $g(f(x))$ in umgekehrter Reihenfolge zu notieren als $(x)(f \circ g) = ((x)f)g$ oder, noch einfacher, als $xfg$ oder $x_{fg}$. Tatsächlich findet sich diese Schreibweise in der Fachliteratur vereinzelt, besonders in der Gruppentheorie, wo sie mit der lateinischen Schrift, weil sie von links nach rechts verläuft, eindeutig besser harmoniert.

gilt. Bei Bedarf könnte man zwei Symbole $\rho_1 \underset{\rightarrow}{\circ} \rho_2$ und $\rho_2 \underset{\leftarrow}{\circ} \rho_1$ parallel für Relationsprodukte verwenden; wir entscheiden uns für die zweite Variante und nennen das oben beschriebene Produkt $\rho_2 \circ \rho_1$.

**Definition 2.1.1.3.** Die *inverse Relation* (auch *duale Relation*) $\rho^{-1} \subseteq B \times A$ einer Relation $\rho \subseteq A \times B$ ist definiert als Menge aller $(b, a) \in B \times A$ mit $(a, b) \in \rho$.

Folgende Eigenschaften sind leicht nachzuprüfen:

**Proposition 2.1.1.4.** *Für Relationen $\rho = \rho_1 \subseteq A \times B$, $\rho_2 \subseteq B \times C$ und $\rho_3 \subseteq C \times D$ gilt:*

1. *Das Relationenprodukt ist assoziativ:* $(\rho_3 \circ \rho_2) \circ \rho_1 = \rho_3 \circ (\rho_2 \circ \rho_1)$
2. *Für die identische Relation (Abbildung)* $\mathrm{id}_B := \{(b, b) \mid b \in B\}$ *auf $B$ gilt* $\rho_2 \circ \mathrm{id}_B = \rho_2$ *und* $\mathrm{id}_B \circ \rho_1 = \rho_1$.
3. *Sind $\rho_1$ und $\rho_2$ Funktionen, so auch $\rho_2 \circ \rho_1$.*
4. *Sind $\rho_1$ und $\rho_2$ injektive Funktionen, so auch $\rho_2 \circ \rho_1$.*
5. *Sind $\rho_1$ und $\rho_2$ surjektive Funktionen, so auch $\rho_2 \circ \rho_1$.*
6. *Sind $\rho_1$ und $\rho_2$ bijektive Funktionen, so auch $\rho_2 \circ \rho_1$.*
7. *Sei $\rho : A \to B$ eine Funktion. Die inverse Relation $\rho^{-1}$ ist genau dann eine Funktion, wenn $\rho$ eine injektive Funktion ist. In diesem Fall ist $\rho^{-1} \colon \rho(A) \to A$.*
8. *Genau dann ist sogar $\rho^{-1} \colon B \to A$, wenn $\rho \colon A \to B$ eine bijektive Funktion ist.*

**UE 41 ► Übungsaufgabe 2.1.1.5.** (V) Beweisen Sie Proposition 2.1.1.4. **◄ UE 41**

**Definition 2.1.1.6.** Eine binäre Relation $\rho$ auf $A$ heißt

- *reflexiv (auf $A$)*, falls $a \rho a$ für alle $a \in A$
- *antireflexiv (auch areflexiv oder irreflexiv)*, falls $(a, a) \notin \rho$ für alle $a \in A$
- *transitiv*, falls $a \rho b$ und $b \rho c$ stets (also für alle $a, b, c \in A$) $a \rho c$ impliziert
- *symmetrisch*, falls $a \rho b$ stets $b \rho a$ impliziert
- *antisymmetrisch*, falls $a \rho b$ und $b \rho a$ stets $a = b$ impliziert.

Die Elemente $a, b \in A$ heißen *vergleichbar* (bezüglich $\rho$), falls $a \rho b$ oder $b \rho a$ gilt. Die binäre Relation $\rho$ auf $A$ heißt

- *Halbordnung(srelation)*[9] auf $A$ und $(A, \rho)$ heißt *Halbordnung*[10] (oder *partielle Ordnung*), wenn $\rho$ reflexiv, transitiv und antisymmetrisch ist. Eine antireflexive transitive Relation heißt *strikte Halbordnung(srelation)*. Jeder Halbordnung $(M, R)$ kann man die strikte Halbordnung $(M, R')$ mit $R' = R \setminus \{(x, x) \mid x \in M\}$ zuordnen und umgekehrt. Offensichtlich ist dieser Zusammenhang zwischen Halbordnungen und strikten Halbordnungen ein bijektiver.[11]

- (*strikte*) *Totalordnung*[12] (alternativ auch *Kette*[13] oder *lineare Ordnung*) auf $A$, wenn $\rho$ eine (strikte) Halbordnung auf $A$ ist, in der je zwei Elemente $a \neq b \in A$ vergleichbar sind.

- (*strikte*) *Wohlordnung*, wenn $\rho$ eine (strikte) Totalordnung ist mit: Jede nichtleere Teilmenge $T \subseteq A$ hat ein kleinstes Element, d.h. es gibt ein $t_0 \in T$ mit $t_0 \rho t$ für alle $t \in T \setminus \{t_0\}$.

- *Äquivalenzrelation*, wenn $\rho$ reflexiv, transitiv und symmetrisch ist.

**UE 42** ► **Übungsaufgabe 2.1.1.7.** (F) Sei $M$ eine beliebige Menge. Ist jede symmetrische transitive Relation $\rho \subseteq M \times M$ auch reflexiv? ◄ **UE 42**

Bekanntlich stehen die Äquivalenzrelationen auf einer Menge $A$ in einem bijektiven Zusammenhang mit den *Partitionen* $\mathcal{P}$ von $A$. Das sind jene Teilmengen $\mathcal{P} \subseteq \mathfrak{P}(\mathcal{A})$ der sogenannten *Potenzmenge* $\mathfrak{P}(A) := \{K : \ K \subseteq A\}$ von $A$ (der Menge aller Teilmengen von $A$), für die gilt: Alle $K \in \mathcal{P}$ sind nicht leer, paarweise *disjunkt* (d.h. je zwei $K_1 \neq K_2 \in \mathcal{P}$ haben leeren Schnitt) und ihre Vereinigung ist ganz $A$. Es gilt nämlich:

**Proposition 2.1.1.8.** *Sei $A$ eine Menge.*
*Für jede Äquivalenzrelation $\sim$ auf $A$ und für jedes $a \in A$ sei $[a]_\sim := \{b \in A : \ a \sim b\}$, genannt die* Äquivalenzklasse *von $a$. Außerdem bezeichne $\mathcal{P}_\sim$ die Menge aller Äquivalenzklassen $[a]_\sim$ mit $a \in A$.*
*Umgekehrt sei für jede Partition $\mathcal{P}$ von $A$ die Relation $\sim_\mathcal{P}$ auf $A$ definiert durch: $a \sim_\mathcal{P} b$ genau dann, wenn es ein $K \in \mathcal{P}$ gibt mit $a, b \in K$.*
*Dann gilt:*

1. *Für jede Äquivalenzrelation $\sim$ auf $A$ ist $\mathcal{P}_\sim$ eine Partition von $A$.*

[9] englisch: *partial order*
[10] Achtung: manche Autoren kürzen *Halbordnung* durch *Ordnung* ab, andere verstehen unter *Ordnung* immer eine Totalordnung.
[11] Aus diesem Grund ist mit dem Wort „Ordnung“ oder „Halbordnung“ gelegentlich auch eine strikte Halbordnung gemeint. Ob es sich tatsächlich um eine Halbordnung in unserem Sinn oder um eine strikte Halbordnung handelt, lässt sich meist aus dem Kontext oder aus der Notation erschließen: Für Halbordnungen werden meist Symbole wie $\leq$, $\leqq$, $\subseteq$, $\preceq$, $\sqsubseteq$ etc verwendet, für strikte Halbordnungen $<$, $\subset$, $\prec$, $\sqsubset$, etc. Um die Antireflexivität einer Relation zu betonen, verwendet man auch gerne Symbole wie $\subsetneqq$.
[12] englisch: *total order*
[13] englisch: *chain*

2. *Für jede Partition $\mathcal{P}$ von $A$ ist $\sim_{\mathcal{P}}$ eine Äquivalenzrelation auf $A$.*

3. *Die Zuordnungen $\sim \mapsto \mathcal{P}_\sim$ und $\mathcal{P} \mapsto \sim_{\mathcal{P}}$ sind zueinander inverse Bijektionen zwischen der Menge aller Äquivalenzrelationen auf $A$ und der Menge aller Partitionen von $A$, d.h. explizit: Für jede Äquivalenzrelation $\sim$ auf $A$ stimmt die Äquivalenzrelation $\sim_{\mathcal{P}_\sim}$ wieder mit $\sim$ überein, und für jede Partition $\mathcal{P}$ von $A$ stimmt die Partition $\mathcal{P}_{\sim_{\mathcal{P}}} = \mathcal{P}$ wieder mit $\mathcal{P}$ überein.*

**UE 43 ▶ Übungsaufgabe 2.1.1.9.** (W) Beweisen Sie Proposition 2.1.1.8. **◀ UE 43**

Eine Verbindung zwischen Äquivalenzrelationen und Halbordnungen stellen die Quasiordnungen dar.

**Definition 2.1.1.10.** Eine binäre Relation auf $A$ heißt *Quasiordnung* oder auch *Präordnung*, wenn sie reflexiv und transitiv ist.

Im Gegensatz zu Halbordnungen wird also bei einer Quasiordnung keine Antisymmetrie vorausgesetzt. Das elementarste und gleichzeitig eines der wichtigsten Beispiele ist die Teilerrelation auf $\mathbb{Z}$ (oder, allgemeiner, auf einem Ring mit Eins). Sinnvollerweise identifiziert man in diesem Kontext die Zahlen $k$ und $-k$. Diesem naheliegenden Schritt entspricht der folgende allgemeine Sachverhalt.

**Satz 2.1.1.11.** *Sei $\leq_M$ eine Quasiordnung auf einer Menge $M$. Definiert man für $a, b \in M$ die Relation $a \sim b$ durch $a \sim b :\Leftrightarrow a \leq_M b$ und $b \leq_M a$, so erhält man eine Äquivalenzrelation $\sim$ auf $M$. Auf der Faktormenge $M/\sim$ (der Menge aller Äquivalenzklassen auf $M$) lässt sich durch $[a]_\sim \leq [b]_\sim :\Leftrightarrow a \leq_M b$ eine Halbordnungsrelation definieren.*

**UE 44 ▶ Übungsaufgabe 2.1.1.12.** (W) Beweisen Sie Satz 2.1.1.11. Vergessen Sie insbesondere nicht, auf die Wohldefiniertheit einzugehen. **◀ UE 44**

**Definition 2.1.1.13.** Mit den Bezeichnungen aus Satz 2.1.1.11 heißt $(M/\sim, \leq)$ die *der Quasiordnung $(M, \leq_M)$ zugehörige Halbordnung.*

**Anmerkung 2.1.1.14.** Der einfacheren Terminologie halber wollen wir auch dann von Äquivalenzrelationen etc. sprechen, wenn $A$ und $\rho$ keine Mengen sind, sondern Klassen. Intuitiv sind das mengenähnliche Objekte (insofern sie durch ihre Elemente eindeutig bestimmt sind), die aber so groß sind, dass man Widersprüche in Kauf nehmen müsste, wenn man alle Operationen, die für Mengen erlaubt sind, auch mit Klassen uneingeschränkt ausführte. Der wichtigste formale Unterschied besteht darin, dass nur Mengen selbst wieder als Elemente von Mengen oder auch Klassen auftreten können. Wichtige Beispiele echter Klassen: Klassen von Algebren wie etwa die Klasse aller Gruppen und die (wohlgeordnete) Klasse aller Ordinalzahlen, die Klasse aller zu einer gegebenen Menge gleichmächtigen Mengen etc.

### 2.1.2 Grundbegriffe der Ordnungstheorie

Inhalt in Kurzfassung: Von den zahlreichen Begriffen aus der Theorie der Halbordnungen, die im Folgenden eingeführt werden, werden später vor allem vollständige Verbände und die mit ihnen zusammenhängenden Aussagen immer wieder eine wichtige Rolle spielen. Nützlich für die Veranschaulichung von (endlichen) Halbordnungen sind Hassediagramme.

Wir erinnern daran, dass eine Halbordnung auf einer Menge $M$ eine zweistellige Relation $R$ ist, die antisymmetrisch, transitiv und auf $M$ reflexiv ist. (Siehe 2.1.1.6.)

*Bezeichnungen.* Statt $R$ werden meist Symbole wie „$\leq$“, „$\sqsubseteq$“, etc. geschrieben. Weiters sei:

$$x \geq y :\Leftrightarrow y \leq x,$$
$$x < y :\Leftrightarrow x \leq y,\ x \neq y,$$
$$x > y :\Leftrightarrow x \geq y,\ x \neq y.$$

Statt „$a \leq x$ und $b \leq x$“ schreiben wir meist abgekürzt „$a, b \leq x$“; analog ist $x \leq a, b$ zu verstehen. Statt „$a \leq b$ und $b \leq c$“ schreiben wir oft $a \leq b \leq c$.

**Beispiele 2.1.2.1.** (1) $(\mathbb{R}, \leq)$ ist eine Kette.

(2) $(\mathbb{N}, |)$ ist eine halbgeordnete Menge, aber keine Kette.

(3) $(\mathfrak{P}(M), \subseteq)$ ist halbgeordnete Menge, aber für $|M| \geq 2$ keine Kette.

(4) Ist $(M, \leq)$ eine halbgeordnete Menge und $N \subseteq M$, dann ist $(N, \leq_N)$ ebenfalls eine halbgeordnete Menge. Ist $(M, \leq)$ eine Kette, dann auch $(N, \leq_N)$. Dabei steht $\leq_N$ für die Menge aller Paare $(x, y)$ die sowohl $x \leq y$ als auch $x, y \in N$ erfüllen, also für $\leq \cap (N \times N)$.

**Definition 2.1.2.2.** Seien $(P, \leq)$ und $(Q, \sqsubseteq)$ partielle Ordnungen (und $<$ bzw. $\sqsubset$ die zugehörigen strikten Ordnungsrelationen). Eine Funktion $f : P \to Q$ heißt

- *(schwach) monoton*, wenn für alle $x, x' \in P$ die Implikation $x \leq x' \Rightarrow f(x) \sqsubseteq f(x')$ gilt;
- *strikt monoton*, wenn für alle $x, x' \in P$ die Implikation $x < x' \Rightarrow f(x) \sqsubset f(x')$ gilt.

**Definition 2.1.2.3.** Sei $(P, \leq)$ eine partielle Ordnung (und $(P, <)$ die zugehörige strikte partielle Ordnung), $A \subseteq P$, $p_0 \in P$. Dann heißt

- $p_0$ *untere Schranke* von $A$, wenn $p_0 \leq a$ für alle $a \in A$ gilt.
- $p_0$ *kleinstes Element* von $A$, wenn $p_0 \in A$ und $p_0 \leq a$ für alle $a \in A$ gilt; wir schreiben dann $p_0 = \min(A)$.
- $p_0$ *minimal*[14] in $A$, wenn $p_0 \in A$ und es kein $a \in A$ mit $a < p_0$ gibt (sehr wohl aber ist erlaubt, dass $a$ und $p_0$ unvergleichbar sind).

[14] Man beachte den Unterschied zwischen einem minimalen und einem (=**dem**) kleinsten Element. Die Aussage „$x$ ist minimal in $A$“ ist im Allgemeinen nicht äquivalent zu „$x = \min(A)$“!

- $p_0$ *Infimum* von $A$, wenn $p_0$ die größte untere Schranke von $A$ ist; wir schreiben dann $p_0 = \inf A$.
  (Wenn $A$ ein kleinstes Element $m$ hat, dann gilt $m = \inf A$. Wenn $A$ kein kleinstes Element hat, dann kann es dennoch ein Infimum geben; dieses liegt dann aber nicht in $A$.)

- Eine Teilmenge $A \subseteq P$ heißt *nach unten beschränkt*, wenn es in $P$ eine untere Schranke von $A$ gibt.

- Eine Teilmenge $A \subseteq P$ heißt *Antikette*, wenn je zwei verschiedene Elemente $a, b \in A$ unvergleichbar sind, d.h. wenn weder $a \leq b$ noch $b \leq a$ gilt.

Analog sind die Begriffe *obere Schranke*, *größtes Element*, *maximal*, *Supremum* und *nach oben beschränkt* definiert. Eine Teilmenge $A \subseteq P$ heißt (schlechthin) *beschränkt*, wenn $A$ sowohl nach unten als auch nach oben beschränkt ist.

Der Paarigkeit, mit der die meisten dieser Begriffe auftreten, liegt ein ziemlich offensichtliches *Dualitätsprinzip* für halbgeordnete Mengen zugrunde: Ist $(M, \leq)$ eine halbgeordnete Menge, dann auch $(M, \geq)$. Daraus ergeben sich die folgenden dualen Begriffe:

| $\leq$ | $\geq$ |
|---|---|
| kleinstes Element | größtes Element |
| maximales Element | minimales Element |

So gilt etwa: $m$ ist maximal in $(M, \leq) \Leftrightarrow m$ ist minimal in $(M, \geq)$.

**Beispiele 2.1.2.4.**
- In $(\mathbb{R}, \leq)$ entsprechen die eben definierten Begriffe den in der Analysis üblichen.
- In $(\mathbb{N}, |)$ gilt für $T \subseteq \mathbb{N}$ mit $T \neq \emptyset$: $\inf T = \mathrm{ggT}(T)$ und $\sup T = \mathrm{kgV}(T)$. Weiters ist $\inf \emptyset = 0$ und $\sup \emptyset = 1$.
- In $(\mathfrak{P}(M), \subseteq)$ gilt für $\mathfrak{S} \subseteq \mathfrak{P}(M)$: $\inf \mathfrak{S} = \bigcap \mathfrak{S} := \bigcap_{A \in \mathfrak{S}} A$ und $\sup \mathfrak{S} = \bigcup \mathfrak{S} := \bigcup_{A \in \mathfrak{S}} A$.

**Anmerkung 2.1.2.5.**
- Man beachte, dass die leere Menge zwar kein kleinstes oder minimales Element enthalten kann, dass aber jedes Element von $P$ sowohl obere wie auch untere Schranke der leeren Menge ist.
- Um zu zeigen, dass $p$ kleinstes Element der Menge $A$ ist, genügt es im Allgemeinen *nicht*, die Annahme $\exists a \in A : a < p$ auf einen Widerspruch zu führen. Damit zeigt man nämlich nur, dass $p$ *minimal* in $A$ ist.
- Man sieht leicht, dass eine partielle Ordnung höchstens ein kleinstes Element enthalten kann (möglicherweise aber mehrere minimale Elemente).
- Eine Halbordnung $(P, \leq)$ (aufgefasst als Teilmenge ihrer selbst) ist folglich genau dann nach unten/oben beschränkt, wenn sie ein kleinstes/größtes Element enthält. Insbesondere ist die einelementige Halbordnung beschränkt, nicht aber die leere Halbordnung.

**Definition 2.1.2.6.** Eine Halbordnung $(M, \leq)$ heißt eine *Noethersche Halbordnung*, wenn sie die aufsteigende Kettenbedingung ($ACC$ = ascending chain condition) erfüllt: Es gibt keine unendlich aufsteigenden Ketten, das heißt: keine streng monotone Abbildung $f\colon (\mathbb{N}, \leq) \to (M, \leq)$. Dual heißt $(M, \leq)$ eine *Artinsche Halbordnung*, wenn sie die absteigende Kettenbedingung ($DCC$ = descending chain condition) erfüllt: Es gibt keine unendlich absteigenden Ketten, das heißt: keine streng monotone Abbildung $f\colon (\mathbb{N}, \leq) \to (M, \geq)$.

**UE 45** ▶ **Übungsaufgabe 2.1.2.7.** (F) Man gebe Beispiele von Halbordnungen (oder sogar linearen Ordnungen), die zeigen, dass die Kettenbedingungen ACC und DCC unabhängig voneinander sind (d.h., dass keine die andere impliziert). ◀ **UE 45**

**UE 46** ▶ **Übungsaufgabe 2.1.2.8.** (E) Man zeige, dass eine Kette mit ACC und DCC endlich ist. ◀ **UE 46**

**UE 47** ▶ **Übungsaufgabe 2.1.2.9.** (B) Gilt obige Aussage für beliebige Halbordnungen, wenn man zusätzlich voraussetzt, dass es keine unendliche Antikette gibt? ◀ **UE 47**

**UE 48** ▶ **Übungsaufgabe 2.1.2.10.** (F) Geben Sie eine nichtleere partielle Ordnung an, die kein kleinstes Element hat. (Wenn möglich, finden Sie eine endliche partielle Ordnung mit dieser Eigenschaft.)
Geben Sie eine nichtleere partielle Ordnung an, die kein minimales Element hat. (Wenn möglich, finden Sie eine endliche partielle Ordnung mit dieser Eigenschaft.) ◀ **UE 48**

**UE 49** ▶ **Übungsaufgabe 2.1.2.11.** (F) Geben Sie eine nichtleere partielle Ordnung an, die genau ein minimales Element hat, aber kein kleinstes Element hat. (Wenn möglich, finden Sie eine endliche partielle Ordnung mit dieser Eigenschaft.) ◀ **UE 49**

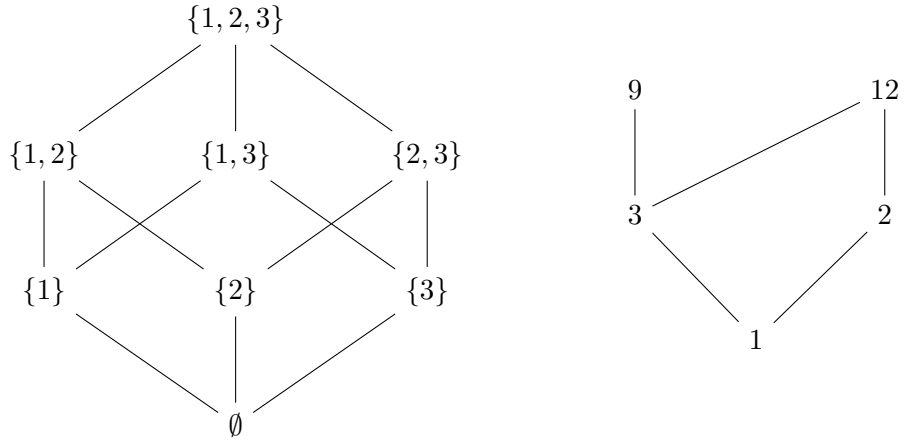
Oft sind die folgenden einfachen Charakterisierungen Noetherscher bzw. Artinscher Halbordnungen nützlich:

**Proposition 2.1.2.12.** *Eine Halbordnung $(M, \leq)$ ist genau dann Noethersch, wenn sie die sogenannte* Maximalbedingung *erfüllt: Jede nichtleere Teilmenge $T \subseteq M$ enthält ein maximales Element.*
*Eine Halbordnung $(M, \leq)$ ist genau dann Artinsch, wenn sie die sogenannte* Minimalbedingung *erfüllt: Jede nichtleere Teilmenge $T \subseteq M$ enthält ein minimales Element.*

*Beweis.* Wegen der Dualität genügt es, die erste der beiden Aussagen zu beweisen.
Sei also $(M, \leq)$ eine Noethersche Halbordnung und $T \subseteq M$ nicht leer. Wir nehmen indirekt an, dass $T$ kein maximales Element enthalte. Dann ist für jedes $t \in T$ die Menge $S_t := \{t' \in T \mid t' > t\}$ nicht leer. Laut Auswahlaxiom gibt es somit eine Funktion $f : T \to T$ mit $f(t) \in S_t$ für alle $t \in T$. Wir wählen irgendein $t_0 \in T$. Nach dem Rekursionssatz gibt es eine eindeutige Folge $(t_n)_{n\in\mathbb{N}}$ mit $t_{n+1} = f(t_n)$ für alle $n \in \mathbb{N}$. Nach Konstruktion ist $t_0 < t_1 < t_2 \ldots \in T \subseteq M$ eine unendlich echt aufsteigende Folge, im Widerspruch zur Voraussetzung, dass $(M, \leq)$ Noethersch ist, d.h. ACC erfüllt.
Zum Beweis der Umkehrung sei die Maximalbedingung an $(M, \leq)$ vorausgesetzt. Wäre $(M, \leq)$ nicht Noethersch, so gäbe es eine unendlich echt aufsteigende Folge von Elementen $t_0 < t_1 < \ldots \in M$. Dann hätte die Menge $T := \{t_n : \ldots n \in \mathbb{N}\} \subseteq M$ kein maximales Element, Widerspruch zur Voraussetzung. □

**Definition 2.1.2.13.** Sei $(P, \leq)$ eine Halbordnung und $(P, <)$ die zugehörige strikte Halbordnung. Für $p, q \in P$ sagen wir, dass $q$ ein (direkter) *Nachfolger* von $p$ ist, wenn $p < q$ gilt, es aber kein $r$ mit $p < r < q$ gibt. Gelegentlich schreibt man dies als $p \lessdot q$.
Das *Hasse-Diagramm* von $P$ ist ein gerichteter Graph, dessen Knotenmenge die Menge $P$ ist, und dessen Kanten die Paare $(p, q)$ mit $p \lessdot q$ sind. In graphischen Darstellungen eines Hassediagramms stellt man den Graphen üblicherweise so dar, dass die Kanten alle hinauf gerichtet sind und erspart sich damit das Einzeichnen von Pfeilen.

**Beispiel 2.1.2.14.** Die Potenzmenge $\mathfrak{P}(\{1, 2, 3\})$ der 3-elementigen Menge $\{1, 2, 3\}$ wird durch die Relation $\subseteq$ halbgeordnet, ebenso die Menge $\{1, 2, 3, 9, 12\}$ durch die Relation $x|y$ ($x$ teilt $y$). Die Hassediagramme dieser Relationen sehen so aus:




**UE 50 ► Übungsaufgabe 2.1.2.15.** (F) Sei $(P, <)$ eine endliche partielle Ordnung. Dann ist $<$ die *transitive Hülle* der Relation $\lessdot$, d.h.: die kleinste transitive Relation, die $\lessdot$ als Teilmenge enthält. **◄ UE 50**

**UE 51** ► **Übungsaufgabe 2.1.2.16.** (F) Geben Sie zwei verschiedene partielle Ordnungen $(P, <_1)$, $(P, <_2)$ auf derselben Grundmenge an, die die gleichen Hassediagramme (was genau bedeutet das?) haben.[15] ◄ **UE 51**

**Proposition 2.1.2.17.** *Sei $(P, \leq)$ eine Halbordnung, in der jede Teilmenge ein Infimum hat. Dann hat auch jede Teilmenge von $P$ ein Supremum. Insbesondere liegt ein* vollständiger Verband *vor (siehe auch Definition 2.1.4.3).*

**UE 52** ► **Übungsaufgabe 2.1.2.18.** (W) Beweisen Sie Proposition 2.1.2.17 und erläutern Sie, warum die Halbordnung $(\mathbb{N}, \leq)$ kein Gegenbeispiel ist. ◄ **UE 52**

Die häufigste Anwendung von Proposition 2.1.2.17 ist die folgende.

**Korollar 2.1.2.19.** Sei $X$ eine Menge und $\mathfrak{S}$ eine durchschnittsstabile Menge von Teilmengen von $X$. (Explizit bedeutet das: Für jedes $\mathfrak{T} \subseteq \mathfrak{S}$ liegt auch der Durchschnitt $\bigcap \mathfrak{T} = \bigcap_{T \in \mathfrak{T}} T$, also das Infimum von $\mathfrak{T}$ bezüglich $\subseteq$, wieder in $\mathfrak{S}$. Weil der Durchschnitt über die leere Menge vereinbarungsgemäß die gesamte Menge $X$ ist, heißt das für $\mathfrak{T} = \emptyset$ insbesondere $X \in \mathfrak{S}$.) Dann ist $\mathfrak{S}$ bezüglich der Inklusion $\subseteq$ sogar ein vollständiger Verband.

Für uns sehr wichtige Beispiele von solch durchschnittsstabilen Systemen $\mathfrak{S}$ werden sein: Die Menge $\mathrm{Sub}(\mathfrak{A})$ aller Unteralgebren und die Menge $\mathrm{Con}(\mathfrak{A})$ aller Kongruenzrelationen einer Algebra $\mathfrak{A}$ (und somit als Spezialfall auch die Menge aller Normalteiler einer Gruppe und die Menge aller Ideale eines Rings). Interessant ist meist die Frage, ob das Supremum in solchen Verbänden konkret beschrieben werden kann. Im Kontrast zum Infimum, das als mengentheoretischer Schnitt eine sehr einfache Interpretation hat, kann nämlich, wenn $\mathfrak{S}$ nicht die gesamte Potenzmenge von $X$ ist, als Supremum nicht einfach die Vereinigung genommen werden, sondern es muss im Allgemeinen ein mehr oder weniger komplizierter Erzeugungsprozess beschrieben werden.

### 2.1.3 Operationen und universelle Algebren

Inhalt in Kurzfassung: Im Zentrum der Algebra stehen algebraische Strukturen, die nun eingeführt werden sollen. Dabei handelt es sich um Mengen zusammen mit Operationen unterschiedlicher Stelligkeit. Interessante Eigenschaften solcher Operationen sind z.B Gesetze (wie etwa Assoziativ-, Kommutativ- oder Distributivgesetz), die Anlass geben zur Definition interessanter Klassen algebraischer Strukturen (wie etwa Gruppen, Ringe oder Körper). Dieser Unterabschnitt bringt einen systematischen Aufbau zahlreicher

[15] Aus der vorigen Übungsaufgabe ergibt sich, dass jede endliche partielle Ordnung durch ihre Grundmenge und ihr Hassediagramm eindeutig bestimmt ist. Da das Hassediagram übersichtlicher als die Ordnung selbst ist, werden kleine endliche partielle Ordnungen meist durch ihr Hassediagramm beschrieben. Für unendliche partielle Ordnungen ist das Hassediagramm aber im Allgemeinen wenig aussagekräftig; daher wird der Begriff „Hassediagramm“ oft überhaupt nur für endliche partielle Ordnungen definiert.

derartiger Begriffsbildungen.

Wir beschäftigen uns nun mit speziellen Funktionen, nämlich solchen, deren Definitionsbereich ein $n$-faches kartesisches Produkt des Zielbereichs ist, also mit der Situation $f : A^n \to A$, sogenannte $n$-stellige Operationen auf $A$.

**Definition 2.1.3.1.** Sind $A, B$ Mengen, so bezeichnet $A^B$ die Menge aller Abbildungen $f\colon B \to A$.

Im Fall $n = 0 = \emptyset$ steht $A^n = A^0$ also für die Menge aller Abbildungen $f\colon \emptyset \to A$, d.h. aller Mengen von geordneten Paaren $(a, b)$ mit $a \in \emptyset$, $b \in A$. Da es keine solchen Paare gibt, die Elemente von $f$ sein könnten, ist die leere Menge das einzige derartige $f$, d.h. $A^0 = \{\emptyset\}$. Eine 0-stellige Operation $\omega\colon A^0 \to A$ ist also eindeutig bestimmt durch $c := \omega(\emptyset) \in A$. Somit entsprechen die 0-stelligen Operationen auf $A$ genau den Elementen von $A$, die wir demnach als die Werte (notgedrungen konstanter) Funktionen $\omega\colon A^0 \to A$ auffassen können. Oft schreiben wir $c \in A$ für die 0-stellige Operation $\omega$ mit $\omega(\emptyset) = c$.
Diese Haarspalterei wirkt müßig, hat aber praktischen Nutzen. Denn auf diese Weise lässt sich beispielsweise das neutrale Element einer Gruppe als 0-stellige Operation auffassen, was zur Vereinheitlichung nicht nur der Notation, sondern auch der Konzepte beiträgt.
Eine weitere Besonderheit besteht darin, dass auf der leeren Menge $A = \emptyset$ keine 0-stellige Operation existiert, sehr wohl aber zu jedem $n \geq 1$ genau eine $n$-stellige Operation $\omega$, nämlich die leere Menge $\emptyset\colon \emptyset^n \to \emptyset$ selbst.
Weniger pathologisch sind Operationen höherer Stelligkeit. Dennoch erscheint eine formale Bemerkung angebracht: Die Notation $A^n$ kann man nämlich auf zwei Arten verstehen, entweder über die (rekursive) Definition $A^1 := A$, $A^{n+1} := A^n \times A$ aus 2.1.1.1 oder gemäß Definition 2.1.3.1 als Menge von Abbildungen $n \to A$. Besonders klar wird die Identifikation dieser formal verschiedenen Objekte, wenn wir das von Neumannsche Modell der natürlichen Zahlen zugrundelegen, also $n$ als Menge $\{0, 1, \ldots, n-1\}$ auffassen. Betrachten wir exemplarisch $n = 2$, so haben wir es also entweder mit der Menge von Paaren $(a, a')$ für $a, a' \in A$ oder mit der Menge von Abbildungen $2 = \{0, 1\} \to A$ zu tun. Identifizieren wir $(a, a')$ mit der Funktion $0 \mapsto a$, $1 \mapsto a'$, so wird klar, dass es egal ist, auf welche Art wir $A^2$ interpretieren.
Typische Beispiele für 1-stellige Operationen $\omega : A \to A$ sind die Inversenbildung, etwa $\omega : a \mapsto -a$ in einer abelschen Gruppe $A$, oder die Komplementbildung $\omega : b \mapsto b'$ in einer Booleschen Algebra $B$. In diesen beiden Fällen schreiben wir auch $-$ bzw. $'$ für $\omega$.
Die klassischen Beispiele $n$-ärer Operationen liegen im Fall $n = 2$ vor: Addition und Multiplikation, Schnitt und Vereinigung in Verbänden etc. Meist verwendet man für das Bild des Paares $(a, b)$, $a, b \in A$, unter einer binären Operation $\omega$ die Schreibweise $a\omega b$ statt $\omega(a, b)$ und ersetzt $\omega$ durch vertraute Operationssymbole wie $+, \cdot, \cup, \cap, \circ$ etc., also $a + b$ etc. oder, wenn über $\omega$ kein Zweifel herrscht, manchmal auch schlicht $ab$, wie bei der gewöhnlichen Multiplikation. Die Schreibweise $A_1A_2$ (wobei $A_1$ und $A_2$ Teilmengen von $A$ sind) steht dann für das sogenannte *Komplexprodukt* der Mengen $A_1$ und $A_2$, bestehend aus allen Elementen $a_1a_2$ mit $a_1 \in A_1$ und $a_2 \in A_2$.
Für $n \geq 3$ spielen $n$-stellige Operationen in der Praxis meist bestenfalls eine Rolle im Hintergrund. In den Fokus geraten sie vor allem in der Theorie der Klone, siehe Unterab-

schnitt 2.1.10. Zwecks Einheitlichkeit der Theorie ist es aber in jedem Fall von Vorteil, a priori Operationen mit variabler endlicher Stelligkeit zuzulassen. (Unendlichstellige Operationen sind zwar auch denkbar, werden aber hier nicht behandelt.)
Zwecks Zusammenfassung und Weiterentwicklung definieren wir:

**Definition 2.1.3.2.** Sei $A$ eine Menge[16] und $n \in \mathbb{N}$. Dann verstehen wir unter einer *$n$-stelligen* (auch *$n$-ären*) *Operation* auf $A$ eine Abbildung $\omega\colon A^n \to A$. Im Fall $n = 2$ heißt $\omega$ auch eine *binäre Operation*, im Fall $n = 1$ eine *unäre Operation*. Im Fall $n = 0$ spricht man auch von einer *Konstanten* oder einem (durch $\omega$) *ausgezeichneten Element* von $A$. Ist $\omega$ nur auf einer Teilmenge von $A^n$ definiert, spricht man von einer *partiellen Operation*.
Ist $I$ eine Indexmenge und für jedes $i \in I$ eine $n_i$-stellige Operation $\omega_i\colon A^{n_i} \to A$ auf der Menge $A$ gegeben, so heißt $\mathfrak{A} = (A, \Omega)$ mit $\Omega = (\omega_i)_{i\in I}$ eine *universelle* oder *allgemeine Algebra*. Dabei heißen $A$ die *Trägermenge*, $\tau = (n_i)_{i\in I}$ der *Typ* und $\omega_i$ die *(fundamentalen) Operationen* von $\mathfrak{A}$. Ist $I = \{1, 2, \ldots, k\}$ endlich, so identifizieren wir $\mathfrak{A} = (A, \Omega)$ oft auch mit $(A, \omega_1, \ldots, \omega_k)$ und schreiben für den Typ $\tau = (n_1, \ldots, n_k)$.

Interessante, häufig auftretende Eigenschaften von Operationen und Elementen sind die folgenden.

**Definition 2.1.3.3.** Auf der Menge $A$ seien 2-stellige Operationen $\circ, +, \cdot, \vee$ und $\wedge$, 1-stellige Operationen $-, ^{-1}$ und $'$ und 0-stellige Operationen (Konstante) $0, 1, e \in A$ gegeben.

1. Die Operation $\circ$ heißt *assoziativ*, wenn alle $a, b, c \in A$ das sogenannte *Assoziativgesetz* erfüllen: $(a \circ b) \circ c = a \circ (b \circ c)$

2. Die Operation $\circ$ heißt *kommutativ*, wenn alle $a, b \in A$ das sogenannte *Kommutativgesetz* erfüllen: $a \circ b = b \circ a$

3. Die Operation $\cdot$ heißt *distributiv* bezüglich $+$, wenn alle $a, b, c \in A$ die so genannten *Distributivgesetze* erfüllen: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ (*Linksdistributivität*) und $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ (*Rechtsdistributivität*). Wie üblich werden wir die Konvention *Punkt geht vor Strich* verwenden sowie die Multiplikation nicht immer eigens notieren. Entsprechend vereinfacht sich oben z.B. der Ausdruck $(b\cdot a)+(c\cdot a)$ zu $ba + ca$.

4. Das Element $e \in A$ heißt *linksneutrales Element* bezüglich $\circ$, wenn es $e \circ a = a$ für alle $a \in A$ erfüllt. Entsprechend heißt $e \in A$ *rechtsneutrales Element* bezüglich $\circ$, wenn es $a \circ e = a$ für alle $a \in A$ erfüllt. Ist $e$ sowohl links- als auch rechtsneutrales Element, so heißt $e$ *neutrales Element* bezüglich $\circ$. Ein neutrales Element bezüglich einer additiv notierten Operation $+$ nennt man meistens *Nullelement* (oder schlicht Null) und schreibt dafür $0_A$ oder schlicht 0, analog *Einselement* $1_A$ oder 1 für eine multiplikativ notierte Operation $\cdot$.

[16] $A$ kann eine endliche oder unendliche Menge sein. Auch die leere Menge ist a priori zugelassen. Meistens werden wir jedoch Algebren mit nullstelligen Operationen betrachten; solche Algebren sind niemals leer.

5. Sei $e$ ein neutrales Element bezüglich $\circ$, und $a \in A$. Wenn es $a^* \in A$ gibt mit $a^* \circ a = e$, dann heißt $a$ *linksinvertierbar*; analog heißt es *rechtsinvertierbar*, wenn es $a^* \in A$ gibt mit $a \circ a^* = e$. In diesen Fällen heißt $a^* \in A$ *Linksinverses* von $a$ bzw. *Rechtsinverses* von $a$. Wenn $a$ sowohl links- als auch rechtsinvertierbar ist, dann heißt $a$ *invertierbar*. Ein Element, das sowohl Links- als auch Rechtsinverses von $a$ ist, heißt schlicht *Inverses* oder *inverses Element* von $a$ und wird meist als $a^{-1}$ angeschrieben[17]. Wenn für jedes $a \in B \subseteq A$ (oft ist $B = A$) ein Inverses $a^{-1}$ existiert, so heißt die Abbildung $.^{-1} : B \to A$, $a \mapsto a^{-1}$ *Inversenbildung* (bezüglich $\circ$ und $e$) auf $B \subseteq A$. Für die Inversenbildung bezüglich einer additiv notierten Operation $+$ schreibt man meist $-$, also $-a$ für das inverse Element von $a$ (welches dann durch $a - a := a + (-a) = (-a) + a = 0$ charakterisiert ist).

6. Man sagt, $\vee$ und $\wedge$ erfüllen die *Verschmelzungsgesetze*[18], wenn für alle $a, b \in A$ die Gleichungen $a \wedge (a \vee b) = a$ und $a \vee (a \wedge b) = a$ gelten. (De facto treten diese nur für kommutative und assoziative Operationen $\vee$ und $\wedge$ auf.)

7. Ein Element 1 heißt *absorbierend* bezüglich $\vee$, wenn für alle $a \in A$ die Gleichung $a \vee 1 = 1 \vee a = 1$ gilt.

8. Sei 1 absorbierend bezüglich $\vee$ und neutral bezüglich $\wedge$, dual dazu 0 absorbierend bezüglich $\wedge$ und neutral bezüglich $\vee$. Dann heißen $a$ und $b$ *komplementär*, wenn $a \vee b = b \vee a = 1$ und $a \wedge b = b \wedge a = 0$ gilt. Wir sagen auch, dass $a$ ein *Komplement* von $b$ ist.

9. Bezüglich der Operation $\circ$ heißt $a \in A$ *linkskürzbar* (manchmal auch *linksregulär*) bzw. *rechtskürzbar* (*rechtsregulär*), wenn es zu jedem $b \in A$ höchstens ein $c \in A$ gibt mit $a \circ c = b$ oder, äquivalent, $a \circ c_1 = a \circ c_2$ impliziert $c_1 = c_2$ (bzw. $c_1 \circ a = c_2 \circ a$ impliziert $c_1 = c_2$). Man sagt, die Operation $\circ$ habe eine der genannten Eigenschaften, wenn alle $a \in A$ sie haben. Liegen sowohl Links- als auch Rechtskürzbarkeit vor, so spricht man von *Kürzbarkeit* schlechthin.

10. Ein Element $a$ heißt *idempotent* bezüglich einer binären Operation $\circ$ auf einer Menge $A$, wenn $a \circ a = a$. Die Operation $\circ$ heißt idempotent, wenn alle $a \in A$ idempotent bezüglich $\circ$ sind.

**UE 53** ► **Übungsaufgabe 2.1.3.4.** (F) Untersuchen Sie, unter welchen zusätzlichen Voraussetzungen aus der Existenz eines (Links-, Rechts-) Inversen von $a$ auf die (Links-,Rechts-) Kürzbarkeit von $a$ geschlossen werden kann. ◄ **UE 53**

[17] Man beachte, dass nach dieser Definition ein invertierbares Element nicht unbedingt ein Inverses haben muss, weil das Links- und Rechtsinverse verschieden sein können! Für eine (äußerst prominente und wichtige) Situation, in der invertierbare Elemente stets ein Inverses haben, sei auf Proposition 2.1.3.8 verwiesen.

[18] englisch: *absorption laws*

**UE 54** ► **Übungsaufgabe 2.1.3.5.** (V) Man zeige: Ist $\cdot$ eine assoziative Operation auf $H$, dann gilt für $a_1, \ldots, a_n \in H$, $n \geq 3$, und $r, s \in \mathbb{N}$, $0 \leq r < s \leq n$: ◄ **UE 54**

$$a_1 \cdots a_n = a_1 \cdots a_r (a_{r+1} \cdots a_s) a_{s+1} \cdots a_n.$$

Wo Klammern fehlen, sind die Operationen von links nach rechts auszuführen. Zum Beispiel ist $a_1a_2a_3(a_4a_5a_6)a_7a_8$ Abkürzung für den Ausdruck

$$[[((a_1a_2)a_3) \cdot ((a_4a_5)a_6)] \cdot a_7] \cdot a_8 \ .$$

Formulieren Sie Ihren Beweis als Induktionsbeweis, und erklären Sie insbesondere, was die Induktionsvoraussetzung ist. Hinweis: Zeigen Sie zunächst $b \cdot (c_1 \cdots c_n) = bc_1 \cdots c_n$ mit Induktion nach $n$, dann $a_1 \cdots a_s = a_1 \cdots a_r (a_{r+1} \cdots a_s)$.

Obwohl das Kommutativgesetz insofern einfacher anmutet als das Assoziativgesetz, als es nur zwei Variable involviert, ist Assoziativität jene Eigenschaft, auf die am seltensten verzichtet werden kann. Erstmals ist sie im Zusammenhang mit den mengentheoretischen Operationen Vereinigung $\cup$ aufgetreten. Von dort hat sie sich auf Addition $+$ auf den Zahlenbereichen $\mathbb{N}$ und in weiterer Folge auf $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ übertragen. Ähnliches gilt für das kartesische Produkt $\times$ und die ebenfalls assoziative Multiplikation. Die Wichtigkeit der Assoziativität auch ohne Kommutativität ergibt sich vor allem daraus, dass die Komposition (die Verknüpfung, die Hintereinanderausführung, das Produkt) $\circ$ von Relationen und vor allem Funktionen assoziativ ist. Das wurde in Proposition 2.1.1.4 festgehalten, aus der auch folgt, dass für eine beliebige Menge $A$ die Komposition $\circ$ eine binäre und assoziative Operation auf jeder der Mengen $R_A$, $M_A$ und $S_A$ ist. Dabei besteht $R_A$ aus allen binären Relationen auf $A$, $M_A$ aus allen Funktionen $f\colon A \to A$ und $S_A$ aus allen bijektiven $f \in M_A$. Außerdem liegt in allen diesen Mengen auch das bezüglich $\circ$ neutrale Element $\mathrm{id}_A$. Man nennt $(R_A, \circ, \mathrm{id}_A)$ das *Relationenmonoid* auf $A$ und $(M_A, \circ, \mathrm{id}_A)$ das *symmetrische Monoid* (manchmal auch die *symmetrische Halbgruppe*) auf $A$. In $S_A$ gibt es sogar zu jedem Element $f$ ein Inverses, nämlich die Umkehrfunktion $f^{-1}$. Man nennt $(S_A, \circ, \mathrm{id}_A, {}^{-1})$ die *symmetrische Gruppe* auf $A$. Im Fall $A = \{1, 2, \ldots, n\}$ (oder allgemeiner $|A| = n$) mit $n \in \mathbb{N}$ schreibt man $S_n$ für $S_A$. Tatsächlich handelt es sich dabei um Monoide bzw. um eine Gruppe, wie aus der folgenden Definition auch von einigen weiteren wichtigen Klassen von Algebren ersichtlich ist:

**Definition 2.1.3.6.** Sei $\mathfrak{A} = (A, \Omega)$, $\Omega = (\omega_i)_{i \in I}$, eine universelle Algebra vom Typ $\tau = (n_i)_{i \in I}$ (meist ist $I$ endlich und entsprechend $\tau = (n_1, \ldots, n_k)$).

1. Eine Algebra $\mathfrak{A} = (A, \circ)$ vom Typ (2) heißt *Halbgruppe*, wenn $\circ$ assoziativ ist.

2. Eine Algebra $\mathfrak{A} = (A, \circ, e)$ vom Typ $(2, 0)$ heißt *Monoid*, wenn $(A, \circ)$ eine Halbgruppe und $e$ neutrales Element bezüglich $\circ$ ist.

3. Eine Algebra $\mathfrak{A} = (A, \circ, e, {}^{-1})$ vom Typ $(2, 0, 1)$ heißt *Gruppe*, wenn $(A, \circ, e)$ ein Monoid und ${}^{-1}$ eine Inversenbildung bezüglich $\circ$ und $e$ ist.

4. Eine Algebra $\mathfrak{A} = (A, +, 0, \cdot)$ vom Typ $(2, 0, 2)$ heißt *Halbring*, wenn $(A, +, 0)$ ein kommutatives Monoid ist, $(A, \cdot)$ eine Halbgruppe und $\cdot$ distributiv bezüglich $+$. Der Halbring heißt *kommutativ*, wenn $\cdot$ kommutativ ist. Gibt es ein Einselement 1 bezüglich $\cdot$, so heißt die Algebra $(A, +, 0, \cdot, 1)$ vom Typ $(2, 0, 2, 1)$ *Halbring mit Einselement*.

5. Eine Algebra $\mathfrak{A} = (A, +, 0, -, \cdot)$ vom Typ $(2, 0, 1, 2)$ heißt *Ring*, wenn $(A, +, 0, \cdot)$ ein Halbring ist und $(A, +, 0, -)$ eine abelsche Gruppe. Ist 1 ein Einselement bezüglich $\cdot$, so heißt die Algebra $(A, +, 0, -, \cdot, 1)$ vom Typ $(2, 0, 1, 2, 0)$ ein *Ring mit Einselement*, kurz *Ring mit* 1. Ein Ring (mit oder ohne 1) heißt *kommutativ*, wenn er als Halbring kommutativ ist, d.h. wenn die Multiplikation kommutativ ist.

6. Ist $(A, +, 0, -, \cdot, 1)$ ein Ring, so heißt ein Element $a \in A$ *Linksnullteiler* (*Rechtsnullteiler*), wenn es ein $b \in A \setminus \{0\}$ gibt mit $ab = 0$ ($ba = 0$). In beiden Fällen heißt $a$ ein *Nullteiler*. Der Ring heißt *nullteilerfrei*, wenn 0 der einzige Nullteiler in $A$ ist.

7. Ist die Algebra $\mathfrak{A} = (A, +, 0, -, \cdot, 1)$ vom Typ $(2, 0, 1, 2, 0)$ ein kommutativer Ring mit Einselement, der überdies $1 \neq 0$ erfüllt und nullteilerfrei ist, so heißt $\mathfrak{A}$ *Integritätsbereich*[19]. Besitzen alle $a \in A \setminus \{0\}$ sogar ein Inverses $a^{-1}$, heißt $\mathfrak{A}$ ein *Körper*.[20] Ist $\mathfrak{A}$ ein (nicht notwendigerweise kommutativer) Ring mit $1 \neq 0$, in dem alle Elemente $\neq 0$ ein multiplikatives Inverses haben, spricht man von einem *Schiefkörper* oder *Divisionsring*.[21] Da 0 kein multiplikatives Inverses haben kann, können wir $^{-1}$ nicht als weitere Operation zum Typ hinzufügen – diese Tatsache wird uns noch wiederholt beschäftigen.

8. Sei $\mathfrak{R} = (R, +_R, 0_R, -_R, \cdot_R)$ ein Ring und $\mathfrak{A} = (A, +_A, 0_A, -_A)$ eine abelsche Gruppe. Weiters sei $\Omega = (\omega_r)_{r \in R}$ mit 1-stelligen Operationen $\omega_r$ auf $A$, wobei wir $ra := \omega_r(a)$ für $r \in R$ und $a \in A$ schreiben. Gelten für alle $r, s \in R$ und $a, b \in A$ das Assoziativgesetz $(rs)a = r(sa)$ und beide Distributivgesetze $r(a+b) = ra + rb$ und $(r+s)a = ra + sa$, so heißt die Algebra $\mathfrak{M} = (A, +_A, \Omega)$ vom Typ $(2, (1)_{r \in R})$ ein $\mathfrak{R}$-*Modul* (oder Modul über $\mathfrak{R}$). (Manchmal spricht man auch von einem *Links-Modul*, wobei entsprechend ein *Rechts-Modul* vorliegt, wenn man $ar$ statt $ra$ für $\omega_r(a)$ schreibt und die entsprechenden Gesetze fordert.) Gibt es überdies ein $1_R$, welches $\mathfrak{R}_1 = (R, +_R, 0_R, -_R, \cdot_R, 1_R)$ zu einem Ring mit Einselement macht, und gilt $1_R a = a$ für alle $a \in A$, so nennt man $\mathfrak{M}$ einen *unitären* $\mathfrak{R}$-*Modul*.

   Wir werden – obwohl formal nicht ganz korrekt – die Operationen $\omega_r$, $r \in R$, auch oft in einer einzigen Funktion $R \times A \to A$ zusammenfassen, um die Notation zu vereinfachen[22].

[19] englisch: *integral domain*

[20] englisch: *field*

[21] englisch: *skew field* oder *division ring*

[22] Als formale Definition („Ein $R$-Modul ist eine abelsche Gruppe $A$ zusammen mit einer Operation $R \times A \to A$ mit den Eigenschaften...“) ist dieser Ansatz unpraktisch, da er nicht in unseren begrifflichen Rahmen passt, in dem die Operationen stets Funktionen $A^n \to A$ sind.

Ist $\mathfrak{K} = \mathfrak{R}_1$ sogar ein Schiefkörper oder Körper, so heißt $\mathfrak{M}$ ein *Vektorraum*[23] über $\mathfrak{K}$ oder kurz ein $\mathfrak{K}$-*Vektorraum*.

9. Eine kommutative Halbgruppe $(A, \wedge)$ heißt *Halbverband*, wenn $\wedge$ idempotent ist.

10. Die Algebra $\mathfrak{A} = (A, \vee, \wedge)$ vom Typ $(2, 2)$ heißt *Verband*[24] (*im algebraischen Sinn*), wenn $(A, \vee)$ und $(A, \wedge)$ kommutative Halbgruppen sind und $\vee$ und $\wedge$ beide Verschmelzungsgesetze erfüllen. (Wir werden uns in Proposition 2.1.4.8 davon überzeugen, dass dann sowohl $(A, \vee)$ als auch $(A, \wedge)$ Halbverbände sind.) Gibt es überdies neutrale Elemente $0 \in A$ bezüglich $\vee$ und $1 \in A$ bezüglich $\wedge$, so heißt die Algebra $(A, \vee, \wedge, 0, 1)$ vom Typ $(2, 2, 0, 0)$ ein *beschränkter Verband*. Ein Verband heißt *distributiv*, wenn sowohl $\vee$ distributiv ist bezüglich $\wedge$ als auch $\wedge$ bezüglich $\vee$.

11. Ein *Boolescher Verband* ist ein beschränkter distributiver Verband $(A, \vee, \wedge, 0, 1)$, in dem es zu jedem Element ein Komplement gibt. ($\forall a \in A\ \exists b \in A : (a \vee b = 1,\ a \wedge b = 0)$.)

12. Eine *Boolesche Algebra* ist eine Struktur $(A, \vee, \wedge, 0, 1, ')$ vom Typ $(2, 2, 0, 0, 1)$ mit folgenden Eigenschaften: $(A, \vee, \wedge, 0, 1)$ ist beschränkter distributiver Verband, und für alle $a \in A$ sind $a$ und $a'$ komplementär zueinander.

**UE 55** ► **Übungsaufgabe 2.1.3.7.** (F) Sei $R$ ein beliebiger Ring, $r \in R$. Zeigen Sie, dass $r$ genau dann linkskürzbar (rechtskürzbar) ist, wenn $r$ kein Linksnullteiler (Rechtsnullteiler) ist. ◄ **UE 55**

Vor allem in späteren Kapiteln werden wir in der Notation zunehmend schlampig sein, nicht alle Operationen einzeln auflisten und eventuell nicht einmal zwischen Algebra und Trägermenge unterscheiden. Diese Lockerheit im Umgang entspricht den globalen Gepflogenheiten in den meisten Teilen der Mathematik inklusive Algebra und hat unterschiedliche Rechtfertigungen. Zum Beispiel sind das neutrale Element $e$ sowie Inverse bezüglich einer assoziativen binären Operation $\circ$ eindeutig bestimmt, bedürfen daher nicht unbedingt einer expliziten Hervorhebung als 0- bzw. 1-stellige Operationen. Genauer:

**Proposition 2.1.3.8.** *Sei $\circ$ eine binäre Operation auf der Menge $A$. Ist von (Links-, Rechts-) Inversen die Rede, so gebe es auch ein neutrales Element $e \in A$ bezüglich $\circ$. Die Begriffe neutral bzw. invers sind stets bezüglich $\circ$ zu verstehen.*

1. *Ist $e_l$ ein linksneutrales Element und $e_r$ ein rechtsneutrales Element, dann folgt $e_l = e_r$.*

2. *Es gibt höchstens ein neutrales Element.*

3. *Ist $\circ$ assoziativ und sind $a_l$ und $a_r$ links- bzw. rechtsinvers zu $a$, so gilt $a_l = a_r$.*

[23] englisch: *vector space*
[24] englisch: *lattice*

4. *Ist $\circ$ assoziativ, dann sind Inverse (sofern sie existieren) eindeutig bestimmt.*

5. *Ist $a_l$ ein Linksinverses zu $a$, so ist umgekehrt $a$ ein Rechtsinverses zu $a_l$. Analog gilt: Ist $a_r$ ein Rechtsinverses zu $a$, so ist umgekehrt $a$ ein Linksinverses zu $a_r$. Ist $a^{-1}$ ein Inverses von $a$, dann ist $a$ ein Inverses von $a^{-1}$.*

6. *Sei $\circ$ assoziativ. Hat $a \circ b$ ein Linksinverses, so hat $b$ ein Linksinverses. Analog gilt: Hat $a \circ b$ ein Rechtsinverses, so hat $a$ ein Rechtsinverses.*

7. *Sei $\circ$ assoziativ. Haben $a$ und $b$ Linksinverse $a_l$ bzw. $b_l$, so hat $a \circ b$ das Linksinverse $b_l a_l$. Analog gilt: Haben $a$ und $b$ Rechtsinverse $a_r$ bzw. $b_r$, so hat $a \circ b$ das Rechtsinverse $b_r a_r$.*

8. *Sei $\circ$ assoziativ und $e$ ein neutrales Element. Außerdem gebe zu jedem $a \in A$ (mindestens) ein linksinverses Element $a_l$. Dann ist $a_l = a^{-1}$ für alle $a$ sogar ein inverses Element und $(A, \circ, e, .^{-1})$ eine Gruppe.*

*Beweis.* 1. In $e_l = e_l \circ e_r = e_r$ gilt die erste Gleichheit, weil $e_l$ linksneutral, die zweite, weil $e_r$ rechtsneutral ist.

2. Sind $e$ und $e'$ neutrale Elemente, so ist $e$ linksneutral und $e'$ rechtneutral, nach Aussage 1 also $e = e'$.

3. Es gilt $a_l = a_l \circ e = a_l \circ (a \circ a_r) = (a_l \circ a) \circ a_r = e \circ a_r = a_r$.

4. Je zwei Inverse sind sowohl links- als auch rechtsinvers, müssen nach der dritten Aussage also übereinstimmen.

5. Die erste Behauptung ist aus $a_l \circ a = e$ unmittelbar ersichtlich, die zweite aus $a \circ a_r = e$, die dritte aus $a \circ a^{-1} = a^{-1} \circ a = e$.

6. Ist $c_l$ ein Linksinverses von $ab$, so folgt $(c_l a)b = c_l(ab) = e$, also ist $c_l a$ ein Linksinverses von $b$. Analog beweist man die zweite Aussage.

7. Die Rechnung $(b_l a_l)(ab) = b_l(a_l a)b = b_l e b = b_l b = e$ zeigt, die erste Behauptung, analog $(ab)(b_r a_r) = e$ die zweite.

8. Nach Voraussetzung gibt es sowohl ein Linksinverses $a_l$ für $a$, als auch ein Linksinverses $(a_l)_l$ für $a_l$. Damit gilt $a = e \circ a = ((a_l)_l \circ a_l) \circ a = (a_l)_l \circ (a_l \circ a) = (a_l)_l \circ e = (a_l)_l$, folglich $a \circ a_l = (a_l)_l \circ a_l = e$. Also ist $a_l$ auch rechtsinvers für $a$. Wegen der Eindeutigkeit der Inversen (Aussage 4) ist $a \mapsto a^{-1}$ eindeutig bestimmt, womit auch die letzte Behauptung bewiesen ist.

□

Man könnte Gruppen alternativ beispielsweise auch definieren als Algebren $(G, \circ)$ vom Typ (2), mit einer assoziativen Operation $\circ$, zu der es ein neutrales Element $e$ und zu allen $g \in G$ Inverse gibt. Denn wegen Proposition 2.1.3.8 sind sowohl $e$ als auch sämtliche Inverse eindeutig bestimmt. Somit gibt es eine und nur eine Möglichkeit, was

in der entsprechenden Gruppe $(G, \circ, e, ^{-1})$ im Sinn von Definition 2.1.3.6 die 0-stellige Operation $e$ und die 1-stellige Operation $^{-1}$ sein müssen. Wir werden Gruppen in den meisten Fällen als Algebren vom Typ $(2, 0, 1)$ auffassen und nicht als Algebren vom Typ $(2)$.
Ähnlich ist es oft bequemer, in Moduln oder Vektorräumen die Multiplikation Skalar mal Vektor als eine Abbildung $K \times A \to A$ aufzufassen, und nicht als eine Familie 1-stelliger Operationen. Um den begrifflichen Rahmen klar abzustecken, werden wir vorerst allerdings eher formale Strenge walten lassen.

### 2.1.4 Relationale Strukturen

Inhalt in Kurzfassung: Erlaubt man auf Strukturen, wie sie im vorangegangenen Unterabschnitt definiert wurden, zusätzlich Relationen auf der Trägermenge, so erhält man relationale Strukturen. Wichtige Beispiele sind (halb)geordnete (Halb-)Gruppen oder auch Verbände, die man sowohl in einem algebraischen als auch in einem ordnungstheoretischen Sinn auffassen kann.

Nicht alle wichtigen Strukturelemente aus den Zahlenbereichserweiterungen können innerhalb des bisherigen Rahmens für universelle Algebren wiedergegeben werden. Vor allem gilt das für die Ordnungsrelation. Um ähnliche Flexibilität wie bei den Operationen zu haben, ziehen wir Relationen beliebiger endlicher Stelligkeit in Betracht. (Die meisten betrachteten Relationen werden aber zweistellig sein.)
Relationale Strukturen ergeben sich nun als natürliche Verallgemeinerung universeller Algebren, indem wir zusätzlich zu den Operationen auch noch Relationen zulassen.

**Definition 2.1.4.1.** Seien $\omega_i$, $i \in I$, $n_i$-stellige Operationen auf $A$ und $\rho_j$, $j \in J$, $m_j$-stellige Relationen auf $A$. Zur Abkürzung schreiben wir $\Omega = (\omega_i)_{i\in I}$ und $R = (\rho_j)_{j\in J}$. Dann heißt $\mathfrak{A} = (A, \Omega, R)$ eine *relationale Struktur* vom *Typ* (oder auch von der *Signatur*) $(\tau, \sigma)$ mit *Trägermenge* $A$, wobei $\tau = (n_i)_{i\in I}$ und $\sigma = (m_j)_{j\in J}$. Ist $J = \emptyset$, so fassen wir $\mathfrak{A}$ als universelle Algebra $(A, \Omega)$ auf und nennen $\mathfrak{A}$ auch *rein algebraisch*. Ist $I = \emptyset$, so nennen wir $\mathfrak{A} = (A, R)$ auch *rein relational*.
Fassen wir in einer relationalen Struktur $(A, \Omega, R)$ jedes $\omega_i \colon A^{n_i} \to A$ als Teilmenge $\omega_i \subseteq A^{n_i} \times A = A^{n_i+1}$ auf, also als $(n_i + 1)$-stellige Relation auf $A$, so nennen wir die resultierende Struktur $(A, \Omega \cup R)$ die *zugehörige rein relationale Struktur*.

Wie schon bei universellen Algebren schreiben wir bei endlichen Indexmengen $I$ und $J$ alle $\omega_i$ und $\rho_j$ meist einzeln an, etwa $\mathfrak{A} = (\mathbb{R}, +, 0, -, \cdot, 1, \leq)$ im Fall des angeordneten Körpers der reellen Zahlen. Hier ist also $|I| = 5$ und $|J| = 1$. Die wichtigsten Typen relationaler Strukturen, die nicht auch schon universelle Algebren sind, sind tatsächlich von ähnlicher Art, wo sich nämlich eine oder mehrere algebraische Operationen mit einer (Halb-)Ordnungsrelation verbinden: (halb)geordnete Gruppen und, darauf aufbauend, geordnete Ringe und Körper. In 3.5 werden wir noch interessante Beispiele dazu betrachten. Hier begnügen wir uns mit der folgenden Definition.

**Definition 2.1.4.2.** Unter einer *halbgeordneten Halbgruppe* verstehen wir eine relationale Struktur $\mathcal{H} = (H, \circ, \leq)$, wobei $(H, \circ)$ eine Halbgruppe ist, $(H, \leq)$ eine Halbordnung

und zusätzlich das *Monotoniegesetz* gilt: Für $a, b, c \in H$ folgt aus $a \leq b$ stets $c \circ a \leq c \circ b$ und $a \circ c \leq b \circ c$. Ist $(H, \leq)$ zusätzlich eine Totalordnung, heißt $\mathcal{H}$ eine *geordnete Halbgruppe*.

$\mathcal{G} = (G, \circ, e, ^{-1}, \leq)$ heißt eine *(halb)geordnete Gruppe*, wenn $(G, \circ, e, ^{-1})$ eine Gruppe ist und $(G, \circ, \leq)$ eine (halb)geordnete Halbgruppe.

$\mathcal{K} = (K, +, 0, -, \cdot, 1, \leq)$ heißt ein *(an)geordneter Körper*, wenn $(K, +, 0, -, \cdot, 1)$ ein Körper ist, $(K, +, 0, -, \leq)$ eine geordnete Gruppe und wenn überdies auch das *Monotoniegesetz für die Multiplikation* gilt: Für alle $a, b, c \in K$ folgt aus $a \leq b$ und $c \geq 0$ auch $a \cdot c \leq b \cdot c$ und $c \cdot a \leq c \cdot b$[25].

Einen wichtigen Sonderfall stellen Halbverbände $(H, \vee)$ oder $(H, \wedge)$ und Verbände $(V, \vee, \wedge)$ dar. Sie tragen bereits per se eine Halbordnungsstruktur. Und umgekehrt lassen sich (Halb-)Verbände im ordnungstheoretischen Sinn auch algebraisch umdeuten.

**Definition 2.1.4.3.** Sei $(P, \leq)$ eine partielle Ordnung.

(1) $P$ (genauer: $(P, \leq)$) heißt *Vereinigungs-Halbverband im ordnungstheoretischen Sinn*, wenn jede 2-elementige Teilmenge $\{a, b\}$ eine kleinste obere Schranke $\sup\{a, b\}$ hat. Statt $\sup\{a, b\}$ schreibt man auch oft $a \vee b$.

(2) *Schnitt-Halbverbände im ordnungstheoretischen Sinn* sind analog definiert. Statt $\inf\{a, b\}$ schreibt man oft $a \wedge b$.

(3) $P$ heißt *Verband* oder *verbandsgeordnete Menge*, wenn $P$ sowohl Schnitt- als auch Vereinigungs-Halbverband ist.

(4) $P$ heißt *vollständig*, wenn jede Teilmenge von $P$ sowohl eine kleinste obere als auch eine größte untere Schranke hat. (Siehe dazu auch 2.1.2.17.)

(5) $P$ heißt *bedingt vollständig*[26], wenn jede *beschränkte* Teilmenge (d.h., jede Teilmenge, die sowohl eine obere als auch eine untere Schranke hat) sowohl eine kleinste obere als auch eine größte untere Schranke hat.

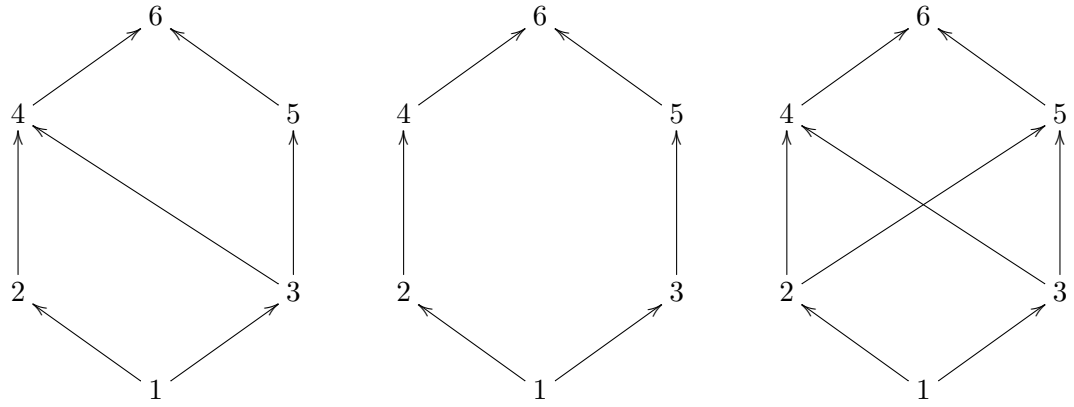
(6) Eine Halbordnung $P$ heißt *beschränkt*, wenn $P$ ein größtes und ein kleinstes Element hat.

**Beispiel 2.1.4.4.** Auf $M = \{1, 2, 3, 4, 5, 6\}$ seien drei Halbordnungsrelationen $\leq_a$, $\leq_b$

[25] Das zweite Monotoniegesetz folgt wegen der Kommutativität der Multiplikation aus dem ersten; der Vollständigkeit halber listen wir beide auf.

[26] Um schleppende Formulierungen zu vermeiden, werden bedingt vollständige lineare Ordnungen, die offensichtlich nicht beschränkt sind, oft einfach als vollständig bezeichnet, wie wir dies etwa bei vollständig angeordneten Körpern getan haben.

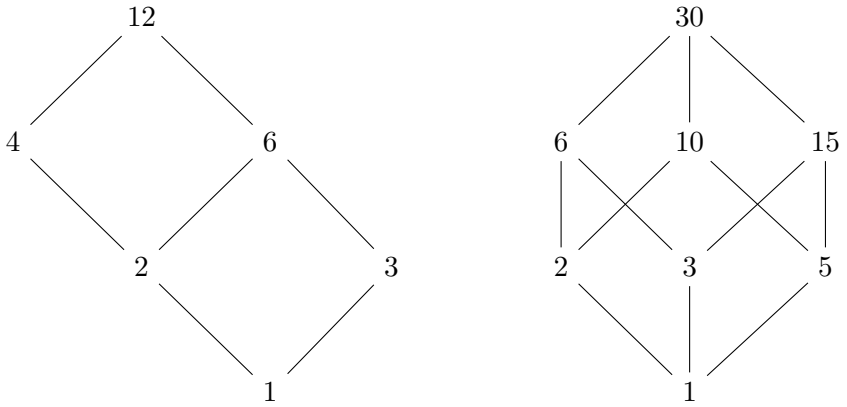
und $\leq_c$ definiert.




$(M, \leq_a)$ $(M, \leq_b)$ $(M, \leq_c)$

Die ersten beiden sind verbandsgeordnet, $(M, \leq_c)$ aber nicht. Zum Beispiel ist $\inf_a\{2,3\} = 1$ und $\sup_a\{2,3\} = 4$, und $\sup_b\{2,3\} = 6$. Hingegen ist $(M, \leq_c)$ *nicht* verbandsgeordnet: $\sup_c\{2,3\}$ existiert nicht, da die Menge $\{2,3\}$ die oberen Schranken 4, 5 und 6, also keine kleinste obere Schranke besitzt.

**Beispiel 2.1.4.5.** Teilerverbände $(T_n, \mathrm{ggT}, \mathrm{kgV})$ mit $T_n := \{t \in \mathbb{N}^+ \mid t \text{ teilt } n\}$, $n \in \mathbb{N}^+$. Hassediagramm von $T_{12}$ und von $T_{30}$:




**Anmerkung 2.1.4.6.** Die Operationen $\wedge$ und $\vee$ nennt man oft (in Analogie zu den Operationen $\cap$ und $\cup$ in $\mathfrak{P}(X)$) „Schnitt“ und „Vereinigung“[27].

Diese Bezeichnungen können aber gelegentlich missverstanden werden: Wenn wir etwa (Vorgriff auf 2.3.1.9) den Verband $\mathrm{Sub}(A)$ aller Unteralgebren einer Algebra $A$ betrachten, ist der verbandstheoretische Schnitt (d.h. das Infimum im Verband) zweier Unteralgebren zwar gleich dem mengentheoretischen Durchschnitt, die verbandstheoretische

[27] englisch: *meet, join*

Vereinigung (also das in Anmerkung 2.3.1.12 definierte Supremum $\mathfrak{U}_1 \vee \mathfrak{U}_2$) hat aber als Trägermenge im Allgemeinen eine echte Obermenge der mengentheoretischen Vereinigung $U_1 \cup U_2$.

**UE 56 ► Übungsaufgabe 2.1.4.7.** (F) $(P, \leq)$ ist genau dann ein Verband, wenn jede nichtleere endliche Teilmenge eine kleinste obere und eine größte untere Schranke hat. **◄ UE 56**

(Halb-)Verbände im ordnungstheoretischen können in solche im algebraischen Sinn übersetzt werden, weshalb man meist nur mehr von (Halb-)Verbänden spricht. Das beruht auf folgenden Aussagen.

**Proposition 2.1.4.8.** (1) *Sei $(P, \leq)$ ein Vereinigungs-Halbverband im ordnungstheoretischen Sinn, d.h. eine Halbordnung, in der zu je zwei Elementen $a, b \in P$ das Supremum $a \vee_{\leq} b := \sup\{a, b\}$ existiert. Dann ist $(P, \vee)$ ein Vereinigungs-Halbverband im algebraischen Sinn (siehe Definition 2.1.3.6).*

(2) *Sei umgekehrt $(P, \vee)$ ein Halbverband im algebraischen Sinn (d.h. eine idempotente kommutative Halbgruppe). Dann wird $(P, \leq_{\vee})$ zu einem Vereinigungshalbverband in ordnungstheoretischen Sinn, wenn man $a \leq_{\vee} b$ durch die Beziehung $a \vee b = b$ definiert.*

(3) *Für (Vereinigungs-)Halbverbände sind die beiden Zuordnungen $\leq \mapsto \vee_{\leq}$ und $\vee \mapsto \leq_{\vee}$ zueinander invers. (Halbverbände im algebraischen und ordnungstheoretischen Sinn sind also im Wesentlichen dieselben Objekte.)*

(4) *Sei $(P, \leq)$ ein Verband im ordnungstheoretischen Sinn. Dann ist $(P, \vee_{\leq}, \wedge_{\leq})$ ein Verband im algebraischen Sinn, wenn $\vee_{\leq}$ wie in Teil 1 als Supremum definiert ist und $\wedge_{\leq}$ als $\vee_{\geq}$, wobei $\geq$ die zu $\leq$ inverse Halbordnungsrelation ist. (Mit anderen Worten ist $a \wedge_{\leq} b := \inf\{a, b\}$.)*

(5) *Ist $(P, \vee, \wedge)$ ein Verband im algebraischen Sinn, dann sind $(P, \vee)$ und $(P, \wedge)$ Halbverbände im algebraischen Sinn.*

(6) *Sei $(P, \vee, \wedge)$ ein Verband im algebraischen Sinn. Dann stimmt die Halbordnung $\leq_{\vee}$ mit der zu $\leq_{\wedge}$ inversen Halbordnung überein, und $(P, \leq_{\vee})$ ist ein Verband im ordnungstheoretischen Sinn.*

(7) *Ist $(P, \vee, \wedge)$ ein Verband, so ist $\wedge$ durch $\vee$ eindeutig bestimmt und umgekehrt.*

(8) *Für Verbände sind die beiden Zuordnungen $\leq \mapsto (\vee_{\leq}, \wedge_{\leq})$ und $(\vee, \wedge) \mapsto \leq_{\vee}$ aus Teil 4 bzw. Teil 6 zueinander invers. (Verbände im algebraischen und ordnungstheoretischen Sinn sind also im Wesentlichen dieselben Objekte.)*

**UE 57 ► Übungsaufgabe 2.1.4.9.** (V) Beweisen Sie Proposition 2.1.4.8. **◄ UE 57**

In den allermeisten Fällen werden wir Proposition 2.1.4.8 in der folgenden wesentlich kürzeren Fassung verwenden:

**Folgerung 2.1.4.10.** *Auf einer Menge $V$ entsprechen Verbandsstrukturen im ordnungstheoretischen Sinn jenen im algebraischen Sinn auf kanonische bijektive Weise, indem*

*$(V, \leq)$ auf $(V, sup_{\leq}, \inf_{\leq})$ und umgekehrt $(V, \vee, \wedge)$ auf $(V, \leq_{\vee,\wedge})$ abgebildet wird. Dabei ist $a \leq_{\vee,\wedge} b$ genau dann, wenn $a \vee b = b$ oder, äquivalent, $a \wedge b = a$ gilt.*

*Beweis.* Umformulierung der letzten Aussage in Proposition 2.1.4.8. □

Bei Anwendungen von Folgerung 2.1.4.10 werden wir statt $\leq_{\vee,\wedge}$ meist nur $\leq$ und statt $\sup_{\leq}$ und $\inf_{\leq}$ meist $\vee$ bzw. $\wedge$ schreiben.

**UE 58** ► **Übungsaufgabe 2.1.4.11.** (B) Für jeden Verband $(V, \wedge, \vee)$ sind $(V, \wedge)$ und $(V, \vee)$ Halbverbände (vgl. Proposition 2.1.4.8, Aussage 5). Geben Sie ein Beispiel einer Struktur $(V, \wedge, \vee)$ an, die kein Verband ist, wo aber $(V, \wedge)$ und $(V, \vee)$ Halbverbände sind. (Hinweis: Es gibt eine endliche Struktur mit sehr wenigen Elementen, die diese Bedingungen erfüllt.) ◄ **UE 58**

**UE 59** ► **Übungsaufgabe 2.1.4.12.** (F) Sei $(V, \vee, \wedge)$ ein Verband, der $\forall x, y, z : (x \wedge z) \vee (y \wedge z) = (x \vee y) \wedge z$ erfüllt. Zeigen Sie, dass dann auch $\forall x, y, z : (x \vee z) \wedge (y \vee z) = (x \wedge y) \vee z$ gilt, d.h. dass $V$ distributiv ist. (Hinweis: Schreiben Sie $+$ für $\vee$ und $\cdot$ für $\wedge$.) ◄ **UE 59**

**UE 60** ► **Übungsaufgabe 2.1.4.13.** (F) Man bestimme die Hasse-Diagramme aller Verbände mit höchstens 6 Elementen (bis auf Isomorphie). (Es genügt nicht, alle solchen Verbände zu finden; Sie müssen auch beweisen, dass Ihre Liste vollständig ist, und dass keine zwei Verbände auf Ihrer Liste zueinander isomorph sind.)
Hinweis: Wenn Sie aus einem 6-elementigen Verband ein Element entfernen, ist die verbleibende Ordnung im Allgemeinen kein Verband.
Hinweis: Gehen Sie systematisch vor. Schaffen Sie Übersichtlichkeit, indem Sie Verbände nach irgendeinem unter Isomorphie invarianten Merkmal klassifizieren, zum Beispiel: Länge der längsten Kette. Größe der größten Antikette. Anzahl der oberen Nachbarn des kleinsten Elements. Etc. Wenn es zu viele Strukturen mit einem gemeinsamen Merkmal gibt, verwenden Sie ein weiteres Merkmal. ◄ **UE 60**

### 2.1.5 Homomorphismen zwischen Algebren

Inhalt in Kurzfassung: Verallgemeinert man den Begriff der linearen Abbildung zwischen Vektorräumen auf beliebige (universelle) Algebren, so stößt man auf jenen der Homomorphismen. Bei den meisten Abbildungen, die in der Algebra von Interesse sind, handelt es sich um solche.

Im Zuge der Zahlenbereichserweiterungen, vor allem der Eindeutigkeitssätze, haben wir exzessiv vom Begriff des Isomorphismus, der stärksten Form strukturverträglicher Abbildungen, Gebrauch gemacht. Nun sollen einige wichtige Varianten davon systematisch zusammengestellt werden. Wir beginnen mit jener Bedingung, die an die meisten in der Algebra vorkommenden Abbildungen gestellt wird, der Homomorphiebedingung.

**Definition 2.1.5.1.** Seien die Mengen $A, B$, die Abbildung $f\colon A \to B$ und zwei $n$-stellige Operationen $\omega_A$ und $\omega_B$ auf $A$ bzw. $B$ gegeben ($n \in \mathbb{N}$). Dann heißt $f$ *verträglich* mit $\omega_A$ und $\omega_B$ (oder auch $f$, $\omega_A$ und $\omega_B$ *miteinander verträglich*), wenn für alle $a_1, \ldots, a_n \in A$ die sogenannte *Homomorphiebedingung*

$$f(\,\omega_A(a_1, \ldots, a_n)\,) = \omega_B(\,f(a_1), \ldots, f(a_n)\,)$$

erfüllt ist. In diesem Fall heißt $f$ auch *Homomorphismus* bezüglich $\omega_A$ und $\omega_B$. Schreibt man $f^{[n]}$ für die Abbildung $f^{[n]}\colon A^n \to B^n$, $(a_1, \ldots, a_n) \mapsto (f(a_1), \ldots, f(a_n))$, so lässt sich die Homomorphiebedingung auch kurz schreiben als $f \circ \omega_A = \omega_B \circ f^{[n]}$.

$$\begin{array}{ccc} A^n & \xrightarrow{\omega_A} & A \\ {\scriptstyle f^{[n]}}\downarrow & & \downarrow{\scriptstyle f} \\ B^n & \xrightarrow{\omega_B} & B \end{array}$$

Seien $\mathfrak{A} = (A, \Omega_A)$ mit $\Omega_A = (\omega_{A,i})_{i\in I}$ und $\mathfrak{B} = (B, \Omega_B)$ mit $\Omega_B = (\omega_{B,i})_{i\in I}$ universelle Algebren vom selben Typ $\tau = (n_i)_{i\in I}$. Die Abbildung $f\colon A \to B$ sei für alle $i \in I$ verträglich bezüglich $\omega_{A,i}$ und $\omega_{B,i}$. Dann heißt $f$ auch *Homomorphismus* von $\mathfrak{A}$ nach $\mathfrak{B}$, symbolisch $f\colon \mathfrak{A} \to \mathfrak{B}$. So ein Homomorphismus $f$ heißt überdies:

- *Monomorphismus* von $\mathfrak{A}$ nach $\mathfrak{B}$ (oder auch eine isomorphe Einbettung von $\mathfrak{A}$ in $\mathfrak{B}$), wenn $f\colon A \to B$ injektiv ist.
- *Epimorphismus* von $\mathfrak{A}$ nach (auf) $\mathfrak{B}$, wenn $f\colon A \to B$ surjektiv ist.
- *Isomorphismus* von $\mathfrak{A}$ nach $\mathfrak{B}$ (oder auch zwischen $\mathfrak{A}$ und $\mathfrak{B}$), wenn $f\colon A \to B$ bijektiv ist. Gibt es einen Isomorphismus zwischen $\mathfrak{A}$ und $\mathfrak{B}$, so heißen $\mathfrak{A}$ und $\mathfrak{B}$ isomorph, und man schreibt $\mathfrak{A} \cong \mathfrak{B}$.
- *Endomorphismus* von $\mathfrak{A}$, wenn $\mathfrak{A} = \mathfrak{B}$ gilt.
- *Automorphismus* von $\mathfrak{A}$, wenn $f$ gleichzeitig Isomorphismus und Endomorphismus von $\mathfrak{A}$ ist.

Obwohl in der Bezeichnung *Isomorphismus* die Gleichheit der Struktur zum Ausdruck kommt, wurde in der Definition nicht eigens gefordert, dass die Umkehrabbildung $f^{-1}$ eines Isomorphismus $f$ auch ein Homomorphismus ist. Der Grund ist die dritte Behauptung in:

**Proposition 2.1.5.2.** (1) *Sind $f\colon \mathfrak{A} \to \mathfrak{B}$ und $g\colon \mathfrak{B} \to \mathfrak{C}$ Homomorphismen, so auch ihre Komposition $h := g \circ f\colon \mathfrak{A} \to \mathfrak{C}$, analog für Mono-, Epi-, Iso-, Endo- und Automorphismen.*

(2) *Die Identität $\mathrm{id}_A$ ist ein Automorphismus jeder Algebra $\mathfrak{A}$ mit Trägermenge $A$.*

(3) *Ist $f\colon A \to B$ bijektiv und strukturverträglich mit den $n$-stelligen Operationen $\omega_A$ auf $A$ und $\omega_B$ auf $B$, so ist die Umkehrfunktion $f^{-1}\colon B \to A$ strukturverträglich mit $\omega_B$ und $\omega_A$.*

(4) *Die Endomorphismen einer Algebra* $\mathfrak{A}$ *bilden (bezüglich der Komposition* $\circ$ *und dem neutralen Element* $\mathrm{id}_A$*) ein Monoid, das sogenannte* Endomorphismenmonoid $\mathrm{End}(\mathfrak{A})$ *von* $\mathfrak{A}$.

(5) *Die Automorphismen einer Algebra* $\mathfrak{A}$ *bilden (bezüglich der Komposition* $\circ$*) eine Gruppe, die sogenannte* Automorphismengruppe $\mathrm{Aut}(\mathfrak{A})$ *von* $\mathfrak{A}$.

**UE 61** ► **Übungsaufgabe 2.1.5.3.** (V) Beweisen Sie Proposition 2.1.5.2. ◄ **UE 61**

### 2.1.6 Strukturverträgliche Abbildungen zwischen relationalen Strukturen

Inhalt in Kurzfassung: Will man auch noch den Begriff des Homomorphismus verallgemeinern, nämlich von rein algebraischen auf relationale Strukturen, so bieten sich eine schwächere und eine stärkere Variante an (entspricht Monotonie in eine oder in beide Richtungen), die nun kurz zu besprechen sind.

Will man das Konzept des Homomorphismus von rein algebraischen Strukturen auf relationale übertragen, wird eine zusätzliche Unterscheidung nötig, weil die Entsprechung der dritten Aussage in Proposition 2.1.5.2 nicht mehr gilt. Ein einfaches Beispiel: Betrachten wir auf der Potenzmenge $A := \mathfrak{P}(M)$ der Menge $M$ einerseits die Relation $\subseteq$ und andererseits die Relation $\leq$, die durch $A \leq B$ für $|A| \leq |B|$ definiert sei. Dann ist die identische Abbildung $\mathrm{id}_A$ verträglich mit diesen Relationen in dem schwachen Sinn, dass aus $A \subseteq B$ stets $A \leq B$ folgt, nicht aber im starken Sinn, dass auch die Umkehrung gilt. Allgemein definiert man:

**Definition 2.1.6.1.** Seien zwei $n$-stellige Relationen $\rho_A$ und $\rho_B$ auf $A$ bzw. $B$ gegeben. Dann sagen wir, $f$ sei *schwach* bzw. *stark (struktur-) verträglich* mit $\rho_A$ und $\rho_B$, wenn für alle $a_1, \ldots, a_n \in A$ aus $(a_1, \ldots, a_n) \in \rho_A$ stets $(\, f(a_1), \ldots, f(a_n)\,) \in \rho_B$ folgt bzw. wenn diese beiden Aussagen sogar äquivalent sind.
Ist $n = 2$ und sind $\leq_A$ und $\leq_B$ Halbordnungsrelationen auf $A$ bzw. auf $B$ so nennt man schwach strukturverträgliche Abbildungen auch *monoton* oder *monoton wachsend*, bezüglich der inversen Ordnung $\geq_A$ von $\leq_A$ *antiton* oder *monoton fallend*.
Eine Abbildung, die mit den strikten Halbordnungsrelationen $<_A$ und $<_B$ schwach strukturverträglich ist, heißt auch strikt monoton.

**UE 62** ► **Übungsaufgabe 2.1.6.2.** (E) Interpretieren Sie für diese Aufgabe $n$-stellige Operationen $\omega_A, \omega_B$ als $n+1$-stellige Relationen $\rho_A, \rho_B$. Zeigen Sie: Die Homomorphiebedingung $f(\,\omega_A(a_1, \ldots, a_n)\,) = \omega_B(\, f(a_1), \ldots, f(a_n)\,)$ lässt sich als schwache Strukturverträglichkeit bezüglich $\rho_A$ und $\rho_B$ deuten (wenn $(a_1, \ldots, a_n, a) \in \rho_A$, dann $(\, f(a_1), \ldots, f(a_n), f(a)\,) \in \rho_B$), nicht aber als starke. Lediglich für injektives $f$ sind beide Aussagen äquivalent. ◄ **UE 62**

Offensichtlich gilt:

**Proposition 2.1.6.3.** *Ist $f\colon A \to B$ bijektiv und stark strukturverträglich mit den $n$-stelligen Relationen $\rho_A$ auf $A$ und $\rho_B$ auf $B$, so ist die Umkehrfunktion $f^{-1}\colon B \to A$ stark strukturverträglich mit $\rho_B$ und $\rho_A$.*

Im Hinblick auf Umkehrfunktionen ist bei Relationen also starke Strukturverträglichkeit das passende Konzept, während sich bei nicht notwendig bijektiven Homomorphismen von Algebren schwache Strukturverträglichkeit oft als angemessen erweist.

**UE 63** ► **Übungsaufgabe 2.1.6.4.** (F) Prüfen Sie für Abbildungen $f\colon A \to B$, $g\colon B \to C$, $n$-stellige Operationen $\omega_A, \omega_B, \omega_C$ und für $m$-stellige Relationen $\rho_A, \rho_B, \rho_C$ (jeweils auf $A$, $B$ bzw. $C$) nach: ◄ **UE 63**

1. Sind $f$ und $g$ schwach strukturverträglich bezüglich $\rho_A$ und $\rho_B$ bzw. $\rho_B$ und $\rho_C$, so ist $g \circ f$ schwach strukturverträglich bezüglich $\rho_A$ und $\rho_C$.
2. Sind $f$ und $g$ stark strukturverträglich bezüglich $\rho_A$ und $\rho_B$ bzw. $\rho_B$ und $\rho_C$, so ist $g \circ f$ stark strukturverträglich bezüglich $\rho_A$ und $\rho_C$.

Wegen der Notwendigkeit der Unterscheidung zwischen schwacher und starker Strukturverträglichkeit sind verschiedene Definitionen eines Homomorphismus zwischen relationalen Strukturen möglich. Um keinen überflüssigen terminologischen Ballast anzusammeln, wollen wir uns damit begnügen, zwischen relationalen Strukturen (in unserem Fall zwischen geordneten Gruppen und Körpern) nur *Isomorphismen*, und *isomorphe Einbettungen* (*Monomorphismen*) zu betrachten und dabei stets starke Strukturverträglichkeit zu verlangen. Wegen Aussage 3 in Proposition 2.1.5.2 führt diese Sprechweise zu keinen Mehrdeutigkeiten.

**UE 64** ► **Übungsaufgabe 2.1.6.5.** (F) Prüfen Sie für Abbildungen $f\colon A \to B$, $g\colon B \to C$ und relationale Strukturen $\mathfrak{A} = (A, \Omega_A, R_A)$, $\mathfrak{B} = (B, \Omega_B, R_B)$ und $\mathfrak{C} = (C, \Omega_C, R_C)$ nach: ◄ **UE 64**

1. Sind $f$ und $g$ beide schwach strukturverträglich, so auch $g \circ f\colon \mathfrak{A} \to \mathfrak{C}$.
2. Sind $f$ und $g$ beide stark strukturverträglich, so auch $g \circ f\colon \mathfrak{A} \to \mathfrak{C}$.
3. Die Automorphismen von $\mathfrak{A}$ bilden bezüglich $\circ$ eine Gruppe, genannt die Automorphismengruppe $\mathrm{Aut}(\mathfrak{A})$.

Bemerkung: Die Aufgaben 2.1.1.5 und 2.1.6.4 sollen verwendet und nicht nochmals bewiesen werden.

**UE 65** ► **Übungsaufgabe 2.1.6.6.** (B) Man zeige: Jede abzählbare dichte (zwischen je zwei Elementen liegen weitere) Kette ohne größtes und ohne kleinstes Element ist ordnungsisomorph zu den rationalen Zahlen mit der natürlichen Ordnung. ◄ **UE 65**
Hinweis: Verwenden Sie die Aufzählung $\mathbb{Q} = \{q_n \mid n \in \mathbb{N}\}$. Zeigen Sie zunächst, dass Sie jeden partiellen Isomorphismus $p$, das ist ein Isomorphismus $p : A \to B$ zwischen endlichen Teilmengen von $\mathbb{Q}$, zu einem partiellen Isomorphismus fortsetzen können, dessen Definitions- und Bildbereich echt größer ist.

### 2.1.7 Klassifikation modulo Isomorphie als Paradigma

Inhalt in Kurzfassung: Unter dem Gesichtspunkt der Algebra unterscheiden sich zwei isomorphe Strukturen nicht wesentlich. Dieser Gesichtspunkt lässt sogenannte Klassifikationssätze (schwächer: Darstellungssätze) besonders interessant erscheinen. Es geht nun darum, was genau darunter zu verstehen ist.

Eines der Hauptanliegen der Algebra besteht in der Klassifikation algebraischer oder sogar beliebiger relationaler Strukturen nach Isomorphie. In der Modelltheorie treten gewisse noch allgemeinere Aspekte in den Vordergrund, weshalb man die Modelltheorie sinnvollerweise als ein Teilgebiet der Logik ansieht und nicht mehr der Algebra, wo man sich an der aus der Linearen Algebra bekannten Klassifikation der Vektorräume mittels Dimension orientiert. Ausgangspunkt für uns ist die folgende einfache Beobachtung:

**Proposition 2.1.7.1.** *Auf jeder Klasse $\mathcal{K}$ von relationalen Strukturen desselben Typs ist $\cong$ eine Äquivalenzrelation.*

**UE 66 ► Übungsaufgabe 2.1.7.2.** (F) Folgern Sie Proposition 2.1.7.1 aus bereits Bekanntem. **◄ UE 66**

Ein Klassifikationssatz bezieht sich auf eine bestimmte Klasse $\mathcal{K}$ von relationalen Strukturen (Algebren), die typischerweise alle denselben Typ haben, und gibt an, wie man aus jeder Äquivalenzklasse bezüglich $\cong$ auf $\mathfrak{K}$ (siehe Proposition 2.1.7.1) einen (möglichst kanonischen) Vertreter erhält. Es folgen einige typische Beispiele für Klassen $\mathfrak{K}$ mit Klassifikationssätzen. Manche davon sind bereits bekannt, manche werden wir erst in späteren Kapiteln oder gar nicht in dieser Vorlesung kennen lernen.

- Mengen: Die Isomorphismen sind die bijektiven Abbildungen. Zwei Mengen sind also genau dann isomorph, wenn sie die gleiche Kardinalität (Mächtigkeit) $\kappa$ haben. Ein kanonisches Vertretersystem ist die Klasse der sogenannten Kardinalzahlen.

- Vektorräume $V$ über einem festen Körper $K$ (siehe 1.3.3): Die Isomorphismen sind die bijektiven linearen Abbildungen. Je zwei Vektorräume sind genau dann isomorph, wenn sie dieselbe Dimension haben. Also gibt es zu jeder Kardinalzahl $\kappa$ bis auf Isomorphie genau einen Vektorraum $V_\kappa$ über $K$ mit der Dimension $\kappa$. $V_\kappa$ kann als Menge aller $\kappa$-tupel mit Eintragungen aus $K$, von denen nur endlich viele $\neq 0$ sind, gewählt werden.

- zyklische Gruppen (siehe 3.2.4.8): Die Isomorphismen sind Gruppenisomorphismen. Je zwei zyklische Gruppen sind genau dann isomorph, wenn sie die gleiche Mächtigkeit haben. Als Mächtigkeiten treten genau $\aleph_0$ (abzählbar unendlich) und die natürlichen Zahlen $n = 1, 2, \ldots$ auf. Kanonische Vertreter sind die Gruppen $\mathbb{Z}$ und die Restklassengruppen[28] $C_n = \mathbb{Z}/n\mathbb{Z}$.

[28] Die Gruppe $\mathbb{Z}/n\mathbb{Z}$ wird oft auch mit $\mathbb{Z}_n$ bezeichnet; wir reservieren dieses Symbol aber für den Restklassen*ring* modulo $n$.

- endliche abelsche Gruppen (siehe 3.3.4.2): Bis auf Isomorphie treten genau die endlichen direkten Produkte von endlichen zyklischen Gruppen auf, wobei man Eindeutigkeit erzielt, wenn man nur jene von Primzahlpotenzordnung als Bausteine verwendet.

- endlich erzeugte abelsche Gruppen (siehe 7.4.3.2): Jede endlich erzeugte abelsche Gruppe ist endliches Produkt von zyklischen Gruppen, genauer: lässt sich eindeutig in der Form $\mathbb{Z}^n \times G$ darstellen, wobei $G$ endlich und zyklisch ist und $n \geq 0$.

- endliche einfache Gruppen: Der berühmte (und komplizierte) Klassifikationssatz sprengt den Rahmen der Vorlesung bei Weitem.

- Primkörper (siehe 6.1.1.8): Alle Primkörper (das sind definitionsgemäß Körper, die nur sich selbst als Unterkörper enthalten) sind bis auf Isomorphie gegeben durch die Restklassenkörper $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ mit einer Primzahl $p$ (Charakteristik $p$) und den Körper $\mathbb{Q}$ der rationalen Zahlen (Charakteristik 0).

- endliche Körper (siehe 6.3.1.2): Zu jeder Primzahlpotenz $p^n$, $p \in \mathbb{P}$, $n = 1, 2, \ldots$, gibt es bis auf Isomorphie genau einen Körper mit $p^n$ Elementen. Umgekehrt hat jeder endliche Körper als Kardinalität eine Primzahlpotenz $p^n > 1$. Wie genau all diese Körper erhalten werden können (nämlich als Zerfällungskörper des Polynoms $x^{p^n} - x$ über dem Primkörper mit $p$ Elementen), ist eines der wichtigen Resultate dieser Vorlesung.

- endliche Boolesche Algebren (siehe 3.6.7.6): Bis auf Isomorphie gibt es zu jeder Zweierpotenz $2^n$, $n \in \mathbb{N}$, genau eine Boolesche Algebra mit $2^n$ Elementen, z.B. die Potenzmengenalgebra einer $n$-elementigen Menge (kanonischer Vertreter: die Menge $n = \{0, 1, \ldots, n-1\}$). Umgekehrt hat jede endliche Boolesche Algebra als Kardinalität eine Zweierpotenz. Diesen Klassifikationssatz kann man als Spezialfall des Darstellungssatzes von Stone sehen, oder aus dem Hauptsatz über endliche abelsche Gruppen folgern.

Etwas schwächer sind sogenannte Darstellungssätze. Von ihnen verlangt man etwas weniger als von einem Klassifikationssatz. Und zwar genügt es, wenn für die Klasse $\mathfrak{K}$ von abstrakten Strukturen eine Teilklasse $\mathfrak{T}$ angegeben werden kann derart, dass es erstens zu jeder Struktur aus $\mathfrak{K}$ eine isomorphe aus $\mathfrak{T}$ gibt, und dass zweitens die Grundmengen, Operationen und Relationen der Strukturen in $\mathfrak{T}$ in konkreterer Weise als die in $\mathfrak{K}$ beschrieben werden können (statt abstrakten Gruppen in $\mathfrak{T}$ betrachtet man zB nur Gruppen von linearen Abbildungen auf Vektorräumen, wo die Multiplikation einfach die Verknüpfung von Abbildungen ist).
Wünschenswert ist auch die Angabe einer Strukturanalyse, mit Hilfe derer zu einer gegebenen Struktur aus $\mathfrak{K}$ eine isomorphe aus $\mathfrak{T}$ konstruiert werden kann. Im Gegensatz zu einem Klassifikationssatz ist es anhand eines Darstellungssatzes typischerweise jedoch nicht möglich, genau einen kanonischen Vertreter jedes Isomorphietyps anzugeben.
Wichtige Beispiele sind:

- Monoide und Gruppen: Der *Darstellungssatz von Cayley* für Monoide (siehe 3.1.2.5) besagt, dass jedes Monoid isomorph ist zu einem Untermonoid des symmetrischen Monoids, analog für Gruppen (siehe 3.2.5.1).

- Boolesche Algebren: Nach dem (allgemeinen) Darstellungssatz von Stone (siehe 3.6.8.13) ist jede Boolesche Algebra isomorph zu einer Mengenalgebra, also zu einer Unteralgebra einer Potenzmengenalgebra.

Der Beweis des Satzes von Cayley ist sehr leicht, der des Satzes von Stone deutlich anspruchsvoller. Sein Beweis zeigt zwar, wie man zu einer beliebig vorgegebenen Booleschen Algebra eine (in diesem Fall kanonische) isomorphe Mengenalgebra erhält. Isomorphe, aber verschiedene Boolesche Algebren können jedoch (anders wäre es bei einem echten Klassifikationssatz) zu nicht identischen (wenn auch natürlich isomorphen) Mengenalgebren führen.

### 2.1.8 Terme, Termalgebra, Gesetze und Varietäten

Inhalt in Kurzfassung: Ähnlich wie in der Logik ist es in der (universellen) Algebra unausweichlich, auch die formale Sprache zum Gegenstand zu machen. Dazu braucht es strenge Definitionen von scheinbar selbstverständlichen Begriffen wie Term etc. Von herausragendem Interesse ist in diesem Zusammenhang die Termalgebra (über gegebenen Mengen von Variablen und Operationssymbolen) sowie dass beliebige Variablenbelegungen mit Elementen einer Algebra des entsprechenden Typs zu einem eindeutigen Homomorphismus auf der Termalgebra, dem sogenannten Einsetzungshomomorphismus, fortgesetzt werden können.

Bisher haben wir Ausdrücke der Gestalt $x + y$ ausschließlich als Bezeichnung für ein Objekt verwendet, in diesem Fall die Summe von $x$ und $y$ unter der Annahme, dass $x$ und $y$ ebenso bekannt sind wie die Operation $+$. Nun sollen die Ausdrücke (die schriftlichen Zeichenreihen oder, noch genauer, die ihnen entsprechenden abstrakten mathematischen Objekte) selbst zum Gegenstand gemacht werden. Vorgegeben denken wir uns dabei Mengen von Symbolen, aus denen die *Variablen* $x$ und $y$ sowie das *Operationssymbol* $+$ entnommen sind. Das führt wie folgt zum Begriff des Terms.

**Definition 2.1.8.1.** Sei $(\tau)$ mit $\tau = (n_i)_{i\in I}$ ein Typ allgemeiner Algebren und $X$ eine unendliche Menge, deren Elemente wir *Variablen* nennen. Jedem $i \in I$ ordnen wir ein so genanntes *Operationssymbol* $\omega_i$ zu.[29] (Alle Symbole $x \in X$ und $\omega_i$, $i \in I$, seien paarweise verschieden und auch verschieden von allen später noch auftretenden syntaktischen Symbolen.) Jene $\omega_i$ mit $n_i = 0$ heißen auch *Konstantensymbole*, für die wir gelegentlich z.B. $c_i$ o.ä. schreiben. Die Menge $T = T(X, \tau)$ der *Terme* der zugeordneten Sprache ist definiert als Vereinigung $T := \bigcup_{k\in\mathbb{N}} T_k$ der Mengen $T_k$, $k \in \mathbb{N}$, die rekursiv wie folgt definiert sind:

[29] Wir können $\omega_i$ mit $i$ identifizieren, den Index $i$ also selbst als Operationssymbol verwenden. Weil dies aber zu sehr ungewohnten Schriftbildern führt, schreiben wir $\omega_i$, wenn wir die Rolle als Operationssymbol betonen wollen.

- $T_0 := X$.
- $T_{k+1} = T_k \cup S_k$, wobei $S_k$ als die Menge aller Symbolketten $\omega_i(t_1, \ldots, t_{n_i})$ mit $n_i \geq 0$ und $t_1, \ldots, t_{n_i} \in T_k$ definiert ist:

$$T_{k+1} := T_k \cup \{\omega_i(t_1, \ldots, t_{n_i}) \mid i \in I, t_1, \ldots, t_{n_i} \in T_k\}.$$

(Man beachte, dass insbesondere $\Omega_0 := \{\omega_i \in \Omega : \ n_i = 0\} \subseteq T_1$.)

Für $t \in T$ heißt $\min\{k \in \mathbb{N} : \ t \in T_k\}$ auch die *Stufe* von $t$.
Die $n_i$-stelligen Operationen $\omega_{T,i} : (t_1, \ldots, t_{n_i}) \mapsto \omega_i(t_1, \ldots, t_{n_i})$ auf $T$ machen $\mathfrak{T} = \mathfrak{T}(\tau, X) = (T, (\omega_{T,i})_{i \in I})$ zu einer Algebra vom Typ $\tau$, der so genannten *Termalgebra*, die von $\Omega, \tau$ und $X$ induziert wird.

Die Stufen der Terme – und vor allem die Tatsache, dass für $t = \omega_i(t_1, \ldots, t_{n_i})$ die Terme $t_i$ eine strikt niedrigere Stufe haben als $t$ – machen es möglich, Induktionsbeweise nach der Stufe $k$ eines Terms zu führen, wie wir das beispielsweise in 2.1.8.4 tun werden. Eine einfachere Anwendung ist die rekursive Definition der Menge $v(t)$ der Variablen, die – wie man sagt – *im Term $t$ vorkommen*: Ist $t = x \in X$ von der Stufe 0, so sei $v(t) := \{x\}$. Ist $t = \omega(t_1, \ldots, t_n)$ von der Stufe $k$ mit Termen $t_i$ der Stufen $k_i < k$, so sei $v(t) := v(t_1) \cup \ldots \cup v(t_n)$. Wir vereinbaren, dass die Schreibweise $t = t(x_1, \ldots, x_n)$ mit Variablen $x_1, \ldots, x_n \in X$ die Inklusion $v(t) \subseteq \{x_1, \ldots, x_n\}$ bedeute, dass also alle Variablen, die in $t$ vorkommen, unter den $x_i$, $i = 1, \ldots, n$ zu finden sind.

Es folgen nun einige Bemerkungen zur Codierung von Termen, die weniger aus algebraischer als aus informatischer Sicht von Interesse sind.
Die Symbolketten aus Definition 2.1.8.1 sind so aufgebaut, dass das Operationssymbol $\omega_i$ den Termen $t_1, \ldots, t_{n_i}$, auf die es angewendet wird, vorangestellt wird. Man spricht deshalb von *Präfixnotation*.[30] Für zweistellige Operationen ist es meist üblich, stattdessen, d.h. statt $\omega(x, y)$, die sogenannte *Infixnotation* $x\, \omega\, y$ zu verwenden, wo das Operationssymbol zwischen den Operanden steht; insbesondere dann, wenn das Operationssymbol $\omega$ nicht durch einen Buchstaben, sondern durch ein abstraktes Symbol wie $+$, $\circ$, $*$ etc dargestellt wird. In *Postfixnotation*[31] (wie sie etwa in der Programmiersprache FORTH oder der Seitenbeschreibungssprache PostScript verwendet wird) stellt man das Operationssymbol hinter die Operanden.

**Beispiel 2.1.8.2.** In der folgenden Tabelle stehen in jeder Zeile äquivalente Ausdrücke: zuerst in Präfixnotation, dann Infix, dann Postfix.

| Präfix | Infix | Postfix |
|---|---|---|
| $\sin(+(a, b))$ | $\sin(a + b)$ | $a, b, +, \sin$ |
| $+(\sin(a), b)$ | $\sin(a)+b$ | $a, \sin, b, +$ |
| $*(+(a, b), -(c, d))$ | $(a + b) * (c - d)$ | $a, b, +, c, d, -, *$ |

Die Präfixnotation in der ersten Zeile lässt sich von links nach rechts so lesen: „Sinus der Summe von $a$ und $b$.“ Die Postfixnotation kann man als Rezept oder Algorithmus

[30] auch: *polnische Notation*.
[31] auch: umgekehrte polnische Notation, reverse Polish notation, RPN

von links nach rechts so lesen: „Man nehme $a$ und $b$, addiere die beiden, und bilde von diesem Zwischenresultat den Sinus.“

In der Praxis wird meist eine gemischte Notation verwendet: Für einstellige Operationen wird meistens Präfixnotation verwendet ($\sin(x)$, $-x$), gelegentlich aber auch Postfixnotation ($x^{-1}$, $n!$). Die Komplementbildung von Mengen wird manchmal durch Präfixnotation ($-A$ oder $\sim A$) ausgedrückt, manchmal in Postfixnotation ($A'$ oder $A^c$). Binäre Operationssymbole werden meist in Infixnotation geschrieben, und in Präfixform wenn sie durch Buchstaben oder Buchstabenketten beschrieben werden: $x \wedge y$, aber $\min(x, y)$.

Die Unterscheidung zwischen Prä-, In- und Postfixnotation spielt beim praktischen Umgang mit formalen Sprachen eine Rolle, ist rein mathematisch aber von mäßigem Interesse. Bemerkenswert ist, dass sich bei ausschließlicher Verwendung der Postfixnotation (ebenso wie bei ausschließlicher Verwendung der Präfixnotation) keine Klammern notwendig sind: auch ohne Klammern lassen sich Terme eindeutig[32] decodieren. (Man spricht von *eindeutiger Lesbarkeit*.) Daher lässt man Klammern bei verschachtelten Funktionen gelegentlich weg, z.B. $fg(x)$ oder $fgx$ statt $f(g(x))$.

Oft ist es sinnvoll, sich Terme nicht als lineare Zeichenkette vorzustellen, sondern in Form eines *Baumdiagramms*: Ein Term $t$, der eine Summe darstellt (also $t_1 + t_2$, bzw $+(t_1, t_2)$ bzw $t_1\, t_2\, +$), wird in einen Baum (genauer: einen *planaren Wurzelbaum*[33]) transformiert, dessen Wurzel (die traditionell oben geschrieben wird) mit dem Symbol + markiert ist; von der Wurzel führt ein Zweig nach links und einer nach rechts; an diesen beiden Zweigen hängen die Bäume $T_1$ und $T_2$, die $t_1$ und $t_2$ repräsentieren:

$$+$$

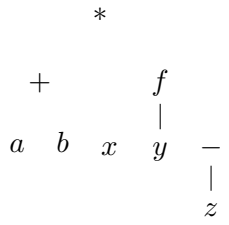
Der Term $(x * y) + (a * b)$ wird durch den Baum

$$\begin{array}{cccc} & & + & \\ & * & & * \\ x & & y & a & & b \end{array}$$

dargestellt, der Term $(a + b) * f(x, y, -z)$ durch den folgenden Baum:

[32] solange die Stelligkeit der Funktionssymbole bekannt ist. Wenn $f$ einstellig und $g$ zweistellig ist, dann ist mit $f\, g\, x\, y$ der Ausdruck $f(g(x, y))$ gemeint; wenn aber $f$ zweistellig und $g$ einstellig ist, dann ist $f(g(x), y)$ gemeint.

[33] Ein *Baum* ist ein zusammenhängender kreisfreier Graph. Ein *Wurzelbaum* ist ein Baum mit einem ausgezeichneten Knoten, der Wurzel. In einem Wurzelbaum hat jeder Knoten außer der Wurzel einen „Vorgänger“, nämlich den nächsten Knoten auf dem Weg zur Wurzel; die anderen Nachbarn des Knotens heißen Nachfolger. In einem planaren Baum sind die Nachfolger jedes Knotens linear geordnet.



Umgekehrt kann man aus der Baumdarstellung leicht Präfix-, Postfix- und Infixdarstellung ablesen. Wenn etwa der oben dargestellte Baum für $t_1 + t_2$ gegeben ist, übersetzt man zunächst (rekursiv) die Bäume $T_1$ und $T_2$ in Infixnotation $t_1$ und $t_2$; der Ausdruck $(t_1) + (t_2)$ ist dann die Infixnotation für den gesamten Baum.

**UE 67** ► **Übungsaufgabe 2.1.8.3.** (F) Ergänzen Sie die folgende Tabelle. Dabei seien $*$ und $+$ zweistellige Operationen, cos und sin einstellig, $i$ nullstellig und $a, b, c$ Variablen. ◄ **UE 67**

| Präfix | Infix | Postfix |
|---|---|---|
| $+\exp *a\,b\,c$ | | |
| | $\exp(-a * b)$ | |
| | $\exp(-a) * b$ | |
| | | $a\cos i\,b\,\sin *+$ |

Geben Sie für jeden dieser Ausdrücke auch ein Baumdiagramm an.

Wir kehren nun wieder zurück zu algebraisch wesentlichen Gesichtspunkten. Die bereits erwähnte Decodierbarkeit (eindeutige Lesbarkeit) des Baumes ist für die folgende, auf Kapitel 4 abzielende *universelle Eigenschaft* der Termalgebra entscheidend. Sie bringt eine höchst vertraute Tatsache zum Ausdruck: Jeder Term kann eindeutig ausgewertet werden, wenn man jede der in ihm auftretenden Variablen mit einem Wert belegt. Will man streng axiomatisch auf Basis beispielsweise der mengentheoretischen ZFC-Axiome vorgehen, so sind gewisse Feinheiten zu beachten. Dazu ein kurzer Exkurs.
Versteht man Terme als Symbolketten, so könnte man beispielsweise mit einem 2-stelligen Operationssymbol $\omega_2$ und zwei Variablen $x, y$ den Term $t = \omega_2(x, y)$ bilden. Fasst man diesen Term im Sinne der Präfixnotation als Kette der Symbole $\omega_2$, $x$ und $y$, und eine Kette als 3-Tupel auf, so wäre nach der rekursiven Definition 2.1.1.1 $t = (\omega_2, x, y) = ((\omega_2, x), y)$. Auf Basis des durch ZFC garantierten mengentheoretischen Universums ist jedes Objekt selbst wieder eine Menge. So könnte es ein einstelliges Operationssymbol $\omega_1$ geben, das zufällig jene Menge ist, die das geordnete Paar $(\omega_2, x)$ darstellt. Dann wäre $t = (\omega_2, x, y) = ((\omega_2, x), y) = (\omega_1, y)$. Somit hätte der Term $t$ neben der Interpretation als $\omega_2(x, y)$ auch jene als $\omega_1(y)$, und die eindeutige Lesbarkeit wäre verletzt. In der streng axiomatischen Mengentheorie hat man also Sorge zu tragen, dass solche ungewollten Koinzidenzen nicht auftreten können, indem man die Symbole, aus denen sich Terme aufbauen lassen, mit entsprechendem Vorbedacht wählt. Das ist möglich, wir wollen uns mit den technischen Details dazu aber nicht beschäftigen, sondern einfach darauf vertrauen, dass eindeutige Lesbarkeit garantiert ist. (Das ist zum Beispiel

der Fall, wenn man als Symbole sogenannte Urelemente ohne interne mengentheoretische Struktur zulässt.) Damit lässt sich der folgende für die Termalgebra zentrale Satz beweisen.

**Satz 2.1.8.4.** *Sei $X$ eine Variablenmenge, $\tau = (n_i)_{i\in I}$ ein Typ universeller Algebren, $\mathfrak{T} = \mathfrak{T}(X, \tau)$ die zugehörige Termalgebra und $\mathfrak{A}$ eine Algebra des Typs $\tau$ mit Trägermenge $A$.*
*Dann gibt es zu jeder Abbildung $\alpha\colon X \to A$ (*Variablenbelegung*) einen eindeutigen Homomorphismus $\bar{\alpha}\colon T \to A$, den von $\alpha$ induzierten* Einsetzungshomomorphismus *von der Termalgebra $\mathfrak{T}$ nach $\mathfrak{A}$, der $\alpha$ fortsetzt.*
*(In der Sprechweise von Kapitel 4 lässt sich sagen: Die Termalgebra $\mathfrak{T}$ ist frei über der Variablenmenge $X$ in der Klasse aller Algebren vom Typ $\tau$.)*

*Beweis.* Sei also $\alpha\colon X \to A$ vorgegeben. Wie in Definition 2.1.8.1 bezeichne $T_k$ die Menge der Terme der Stufe $k$ und $T$ ihre Vereinigung. Wir konstruieren rekursiv Abbildungen $\alpha_k\colon T_k \to A$ derart, dass $\bar{\alpha} := \bigcup_{k\in\mathbb{N}} \alpha_k$ die behauptete Eigenschaft hat. Und zwar setzen wir $\alpha_0(x) := \alpha(x)$ für $x \in X$. Damit ist $\alpha_0\colon T_0 \to A$ definiert. Für $k \geq 0$ sei nun $\alpha_k\colon T_k \to A$ bereits definiert. Wir setzen $\alpha_{k+1}(t) := \alpha_k(t)$ sofern $t \in T_k$. Andernfalls ist $t \in T_{k+1} \setminus T_k$, $t$ also von der Stufe $k+1$. Im Spezialfall $k = 0$ und $n_i = 0$ setzen wir $\alpha_1(\omega_i) := \omega_{i,\mathfrak{A}}$. Ansonsten hat $t$ die Gestalt $t = \omega_i(t_1, \ldots, t_{n_i})$ mit $i \in I$ und $t_1, \ldots, t_{n_i} \in T_k$. Dann setzen wir $\alpha_{k+1}(t) := \omega_{i,\mathfrak{A}}(\alpha_k(t_1), \ldots, \alpha_k(t_{n_i}))$. Auf diese Weise wird $\alpha_{k+1}$ eine wohldefinierte[34] Abbildung $T_{k+1} \to A$, die $\alpha_k\colon T_k \to A$ fortsetzt. Somit ist auch die Vereinigung $\bar{\alpha} := \bigcup_{k\in\mathbb{N}} \alpha_k : T \to A$ eine wohldefinierte Abbildung. Zu zeigen bleibt, dass $\bar{\alpha}\colon \mathfrak{T} \to \mathfrak{A}$ ein Homomorphismus und als solcher sowie als Fortsetzung von $\alpha$ eindeutig bestimmt ist.
Zur Homomorphiebedingung: Sei $i \in I$ beliebig und $t_1, \ldots, t_{n_i} \in T$. Wir betrachten den Term $t := \omega_i(t_1, \ldots, t_{n_i})$ von der Stufe $k+1$. Zu zeigen ist

$$\bar{\alpha}(t) = \bar{\alpha}(\omega_i(t_1, \ldots, t_{n_i})) = \omega_{i,\mathfrak{A}}(\bar{\alpha}(t_1), \ldots, \bar{\alpha}(t_{n_i})).$$

Ist $n_i = 0$, so gilt diese Beziehung aufgrund der speziellen Definition von $\alpha_1 \subseteq \bar{\alpha}$ für diesen Fall. Für $n_i > 0$ sei $k := \max\{k_1, \ldots, k_{n_i}\}$, wobei $k_j$ die Stufe von $t_j$ sei ($j = 1, \ldots, n_i$). Dann ist $t$ von der Stufe $k+1$. Nach Konstruktion gilt daher tatsächlich

$$\bar{\alpha}(t) = \alpha_{k+1}(t) = \omega_{i,\mathfrak{A}}(\alpha_k(t_1), \ldots, \alpha_k(t_{n_i}) = \omega_{i,\mathfrak{A}}(\bar{\alpha}(t_1), \ldots, \bar{\alpha}(t_{n_i})).$$

Zur Eindeutigkeit: Sei $\bar{\beta} : \mathfrak{T} \to \mathfrak{A}$ ein weiterer Homomorphismus mit $\bar{\beta}(x) = \bar{\alpha}(x) = \alpha(x) = \beta(x)$. Diese Voraussetzung besagt gerade, dass $\bar{\alpha}$ und $\bar{\beta}$ auf $T_0$ übereinstimmen. Mit Induktion nach $k$ folgt, dass dies auf allen $T_k$, $k \in \mathbb{N}$ gilt, woraus $\bar{\beta} = \bar{\alpha}$ folgt. Denn der Induktionsschritt ist eine unmittelbare Anwendung der Homomorphiebedingung: Gilt die Behauptung für ein beliebiges $k \in \mathbb{N}$ und ist $t := \omega_i(t_1, \ldots, t_{n_i})$ ein Term der Stufe $k+1$, dann folgt aus der Homomorphiebedingung

$$\bar{\beta}(t) = \bar{\beta}(\omega_i(t_1, \ldots, t_{n_i})) = \omega_{i,\mathfrak{A}}(\bar{\beta}(t_1), \ldots, \bar{\beta}(t_{n_i})),$$

[34] An dieser Stelle fließt die eindeutige Lesbarkeit ein. Streng genommen geht man auch hier mit Induktion vor: Aus dem Term $t$ sind sowohl $\omega_i$ (als erstes Symbol der Zeichenkette) als auch die $t_j$ (z.B. als Eintragungen eines $n_i$-tupels) ablesbar, und die $t_j$ sind nach Induktionsannahme eindeutig lesbar.

was nach Induktionsannahme tatsächlich mit

$$\omega_{i,\mathfrak{A}}(\bar{\alpha}_k(t_1),\ldots,\alpha_k(t_{n_i})) = \omega_{i,\mathfrak{A}}(\bar{\alpha}(t_1),\ldots,\bar{\alpha}(t_{n_i})) = \bar{\alpha}(t)$$

übereinstimmt. Man beachte, dass dies nach Konstruktion auch für $n_i = 0$ gilt: $\bar{\beta}(\omega_i) = \omega_{i,\mathfrak{A}} = \bar{\alpha}(\omega_i)$. □

Die obige rekursive Definition der Menge $v(t)$ aller Variablen, die im Term $t$ vorkommen, führt zu den folgenden interessanten Tatsachen: Mit Induktion nach der Stufe von $t$ zeigt man, dass $v(t)$ stets endlich ist. Bereits oben haben wir eingeführt, dass wir im Falle $v(t) \subseteq \{x_1,\ldots,x_n\}$ auch $t = t(x_1,\ldots,x_n)$ schreiben. Diese Notation ist gerechtfertigt, denn man sieht gleichfalls sehr leicht, dass für eine Variablenbelegung $\alpha\colon X \to A$ der Wert $\bar{\alpha}(t)$ nur von den $a_i := \alpha(x_i)$ für $i = 1,\ldots,n$ abhängt, d.h. von der Belegung nur für jene Variablen, die in $t$ vorkommen. Man schreibt dafür deshalb $t(a_1,\ldots,a_n) := \bar{\alpha}(t)$ für $\alpha : x_i \mapsto a_i$ und nennt es den *Wert* des Terms $t$.

**UE 68 ► Übungsaufgabe 2.1.8.5.** (V) Beweisen Sie die hier behaupteten Aussagen: **◄ UE 68**

1. In jedem Term $t$ kommen nur endlich viele Variablen vor.

2. Der Wert $\bar{\alpha}(t)$ eines Terms $t$ für eine Variablenbelegung $\alpha\colon X \to A$ hängt nur von den $\alpha(x)$ für jene $x \in X$ mit $x \in v(t)$ ab, also für die Variablen, die in $t$ vorkommen.

Mit Hilfe des Einsetzungshomomorphismus lässt sich zum Beispiel die Gültigkeit des Assoziativgesetzes $(xy)z = x(yz)$ in einer Algebra mit einer binären Operation so formulieren: Für jede Variablenbelegung $\alpha : X \to A$ mit $X = \{x,y,z\}$ liefert der $\alpha$ nach Satz 2.1.8.4 eindeutig fortsetzende Einsetzungshomomorphismus $\bar{\alpha}$ für die beiden Terme $t_1 = (xy)z$ und $t_2 = x(yz)$ denselben Wert $\bar{\alpha}(t_1) = \bar{\alpha}(t_2) \in A$. Dies in offensichtlicher Weise verallgemeinernd definieren wir:

**Definition 2.1.8.6.** Sei $\tau$ ein Typ von Algebren, $X$ eine Variablenmenge und $\mathfrak{T} = \mathfrak{T}(X,\tau)$ die dadurch induzierte Termalgebra mit Trägermenge $T$.
Ein *Gesetz* (oder auch eine *Gleichung*) $\gamma$ (für den Typ $\tau$) ist ein Paar $(t_1,t_2) \in T^2$, für das wir gelegentlich[35] auch $t_1 \approx t_2$ schreiben.
Ist überdies $\mathfrak{A}$ eine Algebra vom Typ $\tau$ mit Trägermenge $A$, so sagen wir, dass in $\mathfrak{A}$ das Gesetz $\gamma = (t_1,t_2)$ *gilt*, wenn für alle $\alpha\colon X \to A$ der induzierte Einsetzungshomomorphismus $\bar{\alpha}\colon \mathfrak{T} \to \mathfrak{A}$ (siehe 2.1.8.4) für $t_1$ und $t_2$ dasselbe Bild $\bar{\alpha}(t_1) = \bar{\alpha}(t_2) \in A$ liefert. Wir schreiben in diesem Fall $\mathfrak{A} \models t_1 \approx t_2$.
Ist $\Gamma \subseteq T^2$ eine Menge von Gesetzen, so heißt die Klasse $\mathcal{V}(\Gamma)$ aller Algebren vom Typ $\tau$, in denen alle Gesetze $\gamma \in \Gamma$ gelten, die durch $\Gamma$ bestimmte *Varietät*, und man nennt

[35] Wenn $x_1,\ldots,x_n$ eine Liste aller Variablen ist, die in $t_1$ und/oder $t_2$ vorkommen, dann könnte man das Gesetz $t_1 \approx t_2$ auch ausführlicher in der erststufigen Sprache der Prädikatenlogik in der Form $\forall x_1 \cdots \forall x_n : t_1 = t_2$ schreiben. Die Schreibweise mit dem Symbol $\approx$ soll darauf hinweisen, dass die Terme $t_1$ und $t_2$ nicht als formale Objekte gleich sind, sondern nur ihre Auswertungen an allen Elementen der betrachteten Algebra übereinstimmen.

$\tau$ auch den *Typ der Varietät*. Statt „Varietät“ sagt man auch[36,37,38] *gleichungsdefinierte Klasse*.

### 2.1.9 Ein kurzer Exkurs in die mathematische Logik

Inhalt in Kurzfassung: Viele Begriffsbildungen der universellen Algebra werden im Lichte der mathematischen Logik noch besser verständlich. Der vorliegende Unterabschnitt dient dem Zweck, die relevanten Verbindungen herzustellen.

Im Titel dieses Abschnitts ist von einem logisch-modelltheoretischen Rahmen der allgemeinen Algebra die Rede. Das verlangt noch einige Erklärungen.
Algebra und (mathematische) Logik gelten als zwei verschiedene und wichtige Teilgebiete der Mathematik. In der (klassischen) Algebra stehen Strukturen wie Gruppen, Ringe, Körper, Vektorräume etc. im Mittelpunkt. Ein Charakteristikum der Logik ist die (im Vergleich zur klassischen Algebra und erst recht im Vergleich zu vielen anderen mathematischen Disziplinen wie etwa der Analysis) wichtige Rolle der formalen Sprache, in der über ihre Objekte gesprochen wird. Traditionell gelten Beweistheorie, Rekursionstheorie, Mengenlehre und Modelltheorie als die vier Säulen der Logik:

- Die *Beweistheorie* beschäftigt sich mit der Frage, wie sich mathematisches Beweisen formalisieren lässt; sie betrachtet Beweise als mathematische Objekte und analysiert ihre Struktur.

- Die *Rekursionstheorie*, die man jetzt meist lieber *Berechenbarkeitstheorie* nennt, untersucht Beziehungen zwischen berechenbaren und nicht berechenbaren Funktionen, bzw. zwischen entscheidbaren und nicht entscheidbaren Mengen; sie steht der Theoretischen Informatik sehr nahe.

- Die *Mengenlehre* beschäftigt sich mit „dem“ mathematischen Universum der Mengen, bzw. mit Modellen der Mengenaxiome (etwa der ZFC-Axiome, siehe auch Anhang). Unendliche Kardinalitäten und Wohlordnungen sind sowohl wichtiges Hilfsmittel als auch Objekt der Untersuchungen.

- Die *Modelltheorie* schließlich steht anderen traditionsreichen Teilen der Mathematik, insbesondere der Algebra, am nächsten. Denn auch die Modelltheorie hat relationale Strukturen als zentralen Gegenstand, allerdings vor allem im Wechselspiel mit der formalen Sprache, mit der sich diese beschreiben lassen.

[36] Die Nomenklatur ist nicht immer eindeutig. Das Wort „Varietät“ wird manchmal für gleichungsdefinierte Klassen verwendet, manchmal für Klassen von Algebren, die unter $\mathsf{H}$, $\mathsf{S}$ und $\mathsf{P}$ abgeschlossen sind, siehe Definition 4.1.1.1. Wegen des Satzes von Birkhoff 4.1.7.1 liefern diese Definitionen aber äquivalente Begriffe.

[37] Achtung! In der algebraischen Geometrie wird das Wort „Varietät“ für einen völlig anderen Begriff verwendet, nämlich für die Menge aller Lösungen eines polynomialen Gleichungssystems, siehe Hilbertscher Nullstellensatz.

[38] englisch: *variety*

Es folgen einige Bemerkungen zur Modelltheorie, insbesondere zur Modelltheorie der *Prädikatenlogik erster Stufe*.
Die Strenge und Präzision der mathematischen Methode beruht wesentlich auf der klaren logischen Struktur ihrer Aussagen. Diese Struktur ergibt sich dadurch, dass einfache Aussagen mittels logischer Junktoren (und $\wedge$, oder $\vee$, Negation $\neg$, Implikation $\rightarrow$, Äquivalenz $\leftrightarrow$) und Quantoren (Allquantor $\forall$, Existenzquantor $\exists$) zu komplizierteren zusammengesetzt werden können. Quantoren sind nur in Verbindung mit Variablen sinnvoll, was spezielle Regeln für deren Verwendung erfordert, außerdem eventuell gewisse syntaktische Hilfszeichen wie Klammern, Punkte, Doppelpunkte etc. Es bleibt die Frage nach den elementarsten Aussagen, mit denen alles beginnt.
In jedem Fall fordert man ein Symbol für die Gleichheit, üblicherweise $=$. Zwischen welchen Objekten Gleichheit bzw. Ungleichheit behauptet werden kann, hängt nun von der Struktur ab, auf die wir uns beziehen wollen. Dargestellt werden ihre Elemente durch Terme, die sich aus Konstanten, Variablen und deren Verknüpfungen zusammensetzen. Die Verknüpfungen entsprechen den Operationen in universellen Algebren. Verbindet man zwei Terme $t_1$ und $t_2$, so wie wir das in Definition 2.1.8.6 getan haben, durch das Gleichheitssymbol $=$, so entsteht die elementare Aussage $t_1 = t_2$. Haben wir es mit einer relationalen Struktur zu tun, ist es überdies möglich, zusätzliche Relationen, die zwischen durch Terme dargestellten Objekten bestehen können, zum Ausdruck zu bringen. Aus diesen Gründen ist es sinnvoll, gewissen Klassen relationaler Strukturen eine formale Sprache zuzuordnen. Das soll nun skizziert werden.

Sei $(\tau, \sigma)$ mit $\tau = (n_i)_{i\in I}$ und $\sigma = (m_j)_{j\in J}$ ein Typ relationaler Strukturen und $X$ eine unendliche Variablenmenge. Wie schon bei den rein algebraischen Strukturen sei jedem $i \in I$ ein Operationensymbol $\omega_i$ zugeordnet. Die Menge $T = T(X, \tau)$ der Terme sei so definiert wie schon in 2.1.8.1. Darauf aufbauend wollen wir nun die Menge der Formeln definieren. Dabei treten neue Symbole auf: für jedes $j \in J$ ein Relationssymbol, das wir mit $j$ identifizieren dürfen, das wir aber aus Gewohnheit als $\rho_j$ anschreiben; außerdem Symbole für die logischen Junktoren und Quantoren. Genauer lautet die Definition wie folgt.

**Definition 2.1.9.1.** Unter den obigen Vereinbarungen bezeichnen wir Zeichenketten der Gestalt $t_1 = t_2$ (Gleichheit von Termen) und der Gestalt $\rho_j(t_1, \ldots, t_{m_j})$ mit Termen $t_i$ als *elementare Formeln* oder *Atomformeln*. (Für $m_j = 2$ schreiben wir oft auch $t_1\rho_j t_2$.) Beliebige Formeln ergeben sich rekursiv, nämlich als Zeichenketten, die in der kleinsten Menge $F = F(\Omega, R, \tau, \sigma, X)$ mit folgenden Eigenschaften liegen:

1. Alle elementaren Formeln sind Elemente von $F$.
2. Sind $f, f_1$ und $f_2$ Formeln in $F$, so auch die Zeichenketten $\neg f$, $f_1 \wedge f_2$ (eigentlich $(f_1) \wedge (f_2)$ etc.), $f_1 \vee f_2$, $f_1 \rightarrow f_2$ und $f_1 \leftrightarrow f_2$.
3. Ist $f$ eine Formel in $F$ und $x$ eine Variable, so sind auch die Formeln $\forall x : f$ (eigentlich $\forall x : (f)$) und $\exists x : f$ Formeln, also in $F$.

Damit ist die durch $\Omega, \tau, R, \sigma$ und $X$ induzierte *formale Sprache* gegeben.

Als *geschlossene Formeln* (oft auch *Aussagen*) bezeichnen wir Formeln ohne *freie*[39] *Variable.*

Gesetze im Sinn von Definition 2.1.8.6 lassen sich als elementare Formeln ohne Relationssymbole oder als spezielle geschlossene Formeln auffassen, nämlich solche, wo alle in einer Gleichung auftretenden Variablen durch einen Allquantor gebunden sind.
Hier wollen wir noch die *Interpretation von Formeln* besprechen. Bei gegebener Variablenbelegung $\alpha\colon X \to A$ steht ein Term $t$ für das Element $\bar{\alpha}(t)$ in $A$. Die Entsprechung von Termen in einer natürlichen Sprache sind also Nomen (d.h. Substantive und Pronomen). Im Gegensatz dazu steht eine Formel für eine Aussage über die von den involvierten Termen repräsentierten Objekte. In der Grammatik natürlicher Sprachen entspricht dem das Prädikat eines Satzes. Aussagen können wahr oder falsch sein, sie nehmen als Werte also keine Elemente der zu beschreibenden Struktur an, sondern einen von zwei möglichen Wahrheitswerten 1 (für *wahr*) und 0 (für *falsch*). Ähnliches wie für die Termbelegung $\bar{\alpha}$, die durch eine Variablenbelegung $\alpha$ eindeutig bestimmt ist, gilt auch für die Wahrheitswertebelegung von Formeln. Genauer wird dies, in Analogie zu Satz 2.1.8.4, in Proposition 2.1.9.3 beschrieben.
Zunächst brauchen wir noch eine Notation, die uns erlaubt, über Modifikationen von Variablenbelegungen zu sprechen:

**Definition 2.1.9.2.** Sei $\alpha\colon X \to A$ eine Variablenbelegung; sei $y \in X$ eine Variable, und sei $b \in A$. Mit $\alpha_{y/b}$ bezeichnen wir jene Variablenbelegung $\beta\colon X \to A$, die $\beta(y) = b$ erfüllt, aber an allen anderen Stellen mit $\alpha$ übereinstimmt: $\forall x \neq y : \beta(x) = \alpha(x)$.

**Proposition 2.1.9.3.** *Mit den Notationen von oben sei wieder $\alpha\colon X \to A$ eine Variablenbelegung in der relationalen Struktur $\mathfrak{A} = (A, \Omega_A, R_A)$ vom Typ $(\tau, \sigma)$ mit $\tau = (n_i)_{i\in I}$ und $\sigma = (m_j)_{j\in J}$. Sei weiters, gemäß Proposition 2.1.8.4, $\bar{\alpha}$ die zugehörige Termbelegung. Dann gibt es genau eine Abbildung $\hat{\alpha}\colon F \to \{0, 1\}$ mit folgenden Eigenschaften:*

1. *Eine elementare Formel der Gestalt $t_1 = t_2$, $t_1, t_2 \in T$, erhält unter $\hat{\alpha}$ genau dann den Wahrheitswert 1, wenn $\bar{\alpha}(t_1) = \bar{\alpha}(t_2)$.*

2. *Eine elementare Formel der Gestalt $\rho_j(t_1, \ldots, t_{m_j})$ erhält genau dann den Wahrheitswert 1, wenn $(\bar{\alpha}(t_1), \ldots, \bar{\alpha}(t_{m_j}) \in \rho_{A,j}$.*

3. *Eine Formel der Gestalt $\neg f$ mit $f \in F$ erhält genau dann den Wahrheitswert 1, wenn $f$ den Wahrheitswert 0 erhält.*

4. *Eine Formel der Gestalt $f_1 \wedge f_2$ mit $f_1, f_2 \in F$ erhält genau dann den Wahrheitswert 1, wenn sowohl $f_1$ als auch $f_2$ den Wahrheitswert 1 erhalten.*
   *Kurz gesagt: $\hat{\alpha}(f_1 \wedge f_2) = \min(\hat{\alpha}(f_1), \hat{\alpha}(f_2))$.*

[39] Die Menge $Fr(\varphi)$ der freien Variablen einer Formel $\varphi$ ist rekursiv definiert: Die freien Variablen einer elementaren Formel sind alle die in dieser Formel vorkommenden Variablen. $Fr(\varphi_1 \wedge \varphi_2)$ ist als die Vereinigung $Fr(\varphi_1) \cup Fr(\varphi_2)$ definiert, analog für die anderen Junktoren. Schließlich ist $Fr(\exists x\, \varphi) = Fr(\forall x\, \varphi) := Fr(\varphi) \setminus \{x\}$ definiert. Variable, die nicht frei sind, heißen (durch einen Quantor) gebunden.

5. *Eine Formel der Gestalt $f_1 \vee f_2$ mit $f_1, f_2 \in F$ erhält genau dann den Wahrheitswert* 1*, wenn wenigstens eine der Formeln $f_1$ oder $f_2$ den Wahrheitswert* 1 *erhält. Kurz gesagt: $\hat{\alpha}(f_1 \vee f_2) = \max(\hat{\alpha}(f_1), \hat{\alpha}(f_2))$.*

6. *Eine Formel der Gestalt $f_1 \to f_2$ mit $f_1, f_2 \in F$ erhält genau dann den Wahrheitswert* 1*, wenn $f_1$ den Wahrheitswert* 0 *oder $f_2$ den Wahrheitswert* 1 *erhält. Anders ausgedrückt: $\hat{\alpha}(f_1 \to f_2) = 0$ gilt genau dann, wenn $\hat{\alpha}(f_1) = 1$ aber $\hat{\alpha}(f_2) = 0$ ist.*

7. *Eine Formel der Gestalt $\forall y\, f_1$ erhält genau dann den Wahrheitswert 1 unter $\hat{\alpha}$, wenn für alle $b \in A$ die Gleichung $\widehat{\alpha_{y/b}}(f_1) = 1$ gilt.*
*Kurz gesagt: $\hat{\alpha}(\forall y\, f_1) = \min\{\widehat{\alpha_{y/b}}(f_1) : b \in A\}$.*

8. *Eine Formel der Gestalt $\exists y\, f_1$ erhält genau dann den Wahrheitswert 1 unter $\hat{\alpha}$, wenn es ein $b \in A$ gibt, sodass die Gleichung $\widehat{\alpha_{y/b}}(f_1) = 1$ gilt.*
*Kurz gesagt: $\hat{\alpha}(\exists y\, f_1) = \max\{\widehat{\alpha_{y/b}}(f_1) : b \in A\}$.*

*Erhält eine Formel $f \in F$ durch $\hat{\alpha}$ den Wahrheitswert* 1*, so sagen wir, „$f$ gilt für die Variablenbelegung $\alpha$“. Gilt das für alle Variablenbelegungen $X \to A$, so sagen wir, „$f$ gilt in $\mathfrak{A}$“.*

Damit ist die Bedeutung einer formalen Sprache skizziert, sofern man nur eine feste Struktur $\mathfrak{A}$ im Auge hat. Ist man dagegen an einer Theorie interessiert, die Gültigkeit für eine große Klasse von Strukturen hat, so stößt man auf *Axiomensysteme* und *axiomatische Theorien*. Dabei zeichnet man gewisse Formeln, die in allen betrachteten Strukturen gelten (sollen), als Axiome aus. Eine relationale Struktur $\mathfrak{A}$ vom der Sprache zugehörigen Typ $(\tau, \sigma)$ heißt *Modell* der Theorie (oder der Axiome), wenn jedes Axiom in $\mathfrak{A}$ gilt. Klarerweise zieht die Gültigkeit gewisser Formeln in einer Struktur die Gültigkeit vieler weiterer Formeln nach sich. Man sagt daher: Eine Formel $f$ *folgt* aus einer Menge $M$ anderer Formeln, wenn in jedem Modell für $M$ auch $f$ gilt. Das vielleicht wichtigste Ergebnis der mathematischen Logik, der *Vollständigkeitssatz* von Kurt Gödel (1906–1978), besagt, dass dieser Folgerungsbegriff auf der formalen Ebene der Zeichenketten, welche Formeln definitionsgemäß ja sind, nachvollzogen werden kann. Anders ausgedrückt: Logisches Schließen in diesem Sinne von Folgerung lässt sich automatisieren.
Wer meint, damit könne alle Mathematik den Computern überlassen werden, irrt allerdings in mehrfacher Hinsicht. Nur ein Aspekt sei hier hervorgehoben. Zur Illustration wählen wir etwa das Beispiel der angeordneten Körper $(K, +, 0, -, \cdot, 1, \leq)$. Man überlegt sich leicht, wie die zugehörige formale Sprache einer Theorie der angeordneten Körper und ihre Axiomatisierung aussehen kann.

**UE 69 ► Übungsaufgabe 2.1.9.4.** (F) **◄ UE 69**

(1) Verwenden Sie die Symbole $+, 0, -, \cdot, 1, \leq$ (mit den üblichen Stelligkeiten), sowie die üblichen logischen Symbole ($\vee, \wedge, \Rightarrow, \neg, \forall, \exists$ und Variable $x_1, x_2, \ldots$), und formulieren Sie in der auf diesem Alphabet aufbauenden Sprache ein Axiomensystem, das genau die angeordneten Körper beschreibt.

(2) Noch einmal das Gleiche, aber nun mit einer Sprache, wo es statt dem 2-stelligen Relationssymbol $\leq$ ein einstelliges Relationssymbol $P$ gibt, welches als „ist positiv“ interpretiert werden soll.

Es zeigt sich, dass die Menge der Formeln in einer solchen Sprache relativ klein ist, gemessen an dem, was uns beispielsweise schon in den reellen Zahlen interessiert. Versucht man etwa, die archimedische Eigenschaft (die Menge $\mathbb{N}_K$ der natürlichen Zahlen innerhalb eines angeordneten Körpers, siehe 3.5.3.7, ist in diesem unbeschränkt) mit den Mitteln dieser Sprache auszudrücken, wird man scheitern. Ein strenger Beweis, dass dies notgedrungen so sein muss, übersteigt zwar den Rahmen dieser Vorlesung.[40] Wer ein paar Minuten investiert, um der Frage nachzugehen, wird aber eine deutliche Intuition gewinnen, warum dies so ist.
Versucht man die auftretenden Probleme zu überwinden, kann man beispielsweise auf den Gedanken kommen, die Sprache dahingehend zu erweitern, dass wir uns gestatten, in Bezug auf eine relationale Struktur $\mathfrak{A} = (A, \Omega, R)$ nicht nur über Elemente von $A$ zu sprechen (sogenannte erststufige Theorien, genannt auch *Prädikatenlogik erster Stufe*), sondern auch über Teilmengen und allgemeiner Relationen auf $A$, also auch Teilmengen von $A^2$, $A^3$, etc. (*Prädikatenlogik zweiter Stufe*). Tatsächlich erweitert das die Ausdruckskraft der Sprache erheblich. Und zwar werden dadurch typischerweise viel mehr Aussagen formulierbar als innerhalb eines vernünftigen Axiomensystems beweisbar sind. Im Gegensatz zur Prädikatenlogik erster Stufe gilt nämlich auf der zweiten Stufe kein Vollständigkeitssatz.
Um keine Missverständnisse zu provozieren, noch eine Bemerkung zum berühmten *Unvollständigkeitssatz* von Gödel: Er besagt, dass es in der Theorie der Peano-Arithmetik (und auch in jeder umfassenderen Theorie, in der man über die natürlichen Zahlen sprechen kann, sofern nur eine sehr milde Bedingung an das Axiomensystem erfüllt ist) wahre Sätze gibt, die formulierbar aber nicht innerhalb des Axiomensystems beweisbar sind. Allerdings muss für diese Formulierung das Induktionsaxiom modifiziert werden. Indem es über beliebige Teilmengen von $\mathbb{N}$ spricht, gehört es in der Fassung von 1.1.3.2 nämlich einer Logik zweiter Stufe an, wo sowieso Vollständigkeit außer Reichweite ist. Man ersetzt das Induktionsprinzip daher durch ein so genanntes Axiomenschema der Form

$$(\varphi(0) \wedge \forall n : \ (\varphi(n) \to \varphi(n+1))) \to \forall n : \ \varphi(n).$$

Hierin darf man für $\varphi$ jede Formel ersetzen, die von einer Variablen $n$ abhängt und die der (erststufigen) Sprache der Peano-Arithmetik angehört. Der wesentliche Unterschied zum Induktionsprinzip in der mengentheoretischen Fassung wird deutlich, wenn man sich vor Augen hält, dass es überabzählbar viele Teilmengen $T$ von $\mathbb{N}$ gibt, aber nur abzählbar viele zugelassene Formeln $\varphi$ in einer Variablen (von denen jede eine Teilmenge von $\mathbb{N}$ beschreibt, nämlich $T_\varphi = \{n : \ \varphi(n)\}$).
Noch eine Bemerkung in Anschluss an Aufgabe 2.1.9.4: Man kann die Axiome eines angeordneten Körpers noch um Bedingungen ergänzen, die für die reellen Zahlen (via Zwischenwertsatz für stetige Funktionen) aus der Vollständigkeit folgen, nämlich dass

[40] Hinweis: Kompaktheitssatz der Prädikatenlogik erster Stufe.

jedes Polynom ungeraden Grades eine Nullstelle hat und jedes positive Element eine Quadratwurzel. Diese Bedingungen lassen sich in (erststufige) Formeln in der Sprache der angeordneten Körper übersetzen. Übernimmt man diese Formeln als Axiome, erhält man die *Theorie der reell abgeschlossenen Körper*. Diese Theorie erweist sich nicht nur als vollständig, sondern sogar als entscheidbar: Es gibt einen Algorithmus, der jede Frage, die sich in der Sprache der angeordneten Körper formulieren lässt, entscheidet; genauer: es gibt einen Algorithmus, der für jede geschlossene Formel $\varphi$, die in der erststufigen Sprache der angeordneten Körper formuliert ist, entweder einen Beweis dafür findet, dass $\varphi$ in allen reell abgeschlossenen Körpern (insbesondere auch in $\mathbb{R}$) gilt, oder einen Beweis dafür, dass $\varphi$ in keinem reell abgeschlossenen Körper gilt (also insbesondere nicht in $\mathbb{R}$) .
Die Theorie der reell abgeschlossenen Körper liefert also in Bezug auf erststufige Formeln eine vollständige Beschreibung der reellen Zahlen $\mathbb{R}$. Trotzdem gibt es auch zu $\mathbb{R}$ nicht isomorphe Modelle dieser Theorie: Einerseits sogenannte *Nonstandardmodelle* von $\mathbb{R}$ (die allesamt nicht archimedisch angeordnet sind), weiters aber auch gewisse Unterkörper von $\mathbb{R}$, darunter sogar viele abzählbare, wie zum Beispiel die Menge aller algebraischen reellen Zahlen.

### 2.1.10 Klone

Inhalt in Kurzfassung: Klone entsprechen der Idee, dass nicht nur einstellige Operationen (Funktionen auf einer Menge) durch Verkettung zu Halbgruppen zusammengesetzt werden können, sondern auch mehrstellige Operationen (Funktionen in mehreren Variablen) ineinander eingesetzt werden können. Die bezüglich dieser Operation abgeschlossenen Systeme (die außerdem die sogenannten Projektionen enthalten) nennt man Klone. Der folgende Unterabschnitt soll einen ersten bescheidenen Eindruck von der Theorie der Klone geben.

Etwas weiter von formalen Sprachen und Logik entfernt ist ein weiterer Gesichtspunkt, der in der Allgemeinen Algebra eine wichtige Rolle ist. Dabei geht es weniger darum, von welchen (fundamentalen) Operationen $\omega$ auf einer Menge $A$ wir ausgehen, sondern welche Operationen mit ihnen erzeugt werden können. In diesem Sinne wäre es beispielsweise unerheblich, ob wir in einer abelschen Gruppe neben der binären Operation $+$ die Inversenbildung wie bisher über eine (fundamentale) einstellige Operation $\omega_1 : a \mapsto -a$ oder vermittels einer binären Operation (Subtraktion) $\omega_2 : (a, b) \mapsto a - b$ ins Spiel bringen. Zusammen[41] mit $+$ lassen sich nämlich beide wechselseitig ausdrücken: $\omega_1(a) = \omega_2(\omega_2(a, a), a)$ beziehungsweise $\omega_2(a, b) = a + \omega_1(b)$. Offenbar interessieren also Mengen von Operationen, die bezüglich eines geeigneten Begriffs einer Komposition abgeschlossen sein. Der genaue Begriff lautet wie folgt.

**Definition 2.1.10.1.** Sei $A$ eine Menge. Für alle $n \in \mathbb{N} \setminus \{0\}$ seien die $n$-stelligen *Projektionen* $\pi_i^{(n)} \colon A^n \to A$ für $i = 1, \ldots, n$ definiert durch $\pi_i^{(n)}(a_1, \ldots, a_n) := a_i$. Weiters

[41] Überdies lässt sich auch die Operation $+$ durch die Operation $\omega_2$ ausdrücken, denn $a + b = a - (-b) = a - (0 - b) = \omega_2(a, \omega_2(\omega_2(b, b), b))$.

sei für $n$-stellige Operationen $f_i$, $i = 1, \ldots, k$, und eine $k$-stellige Operation $g$ auf $A$ die *Komposition* $h = g \circ_{n,k} (f_1, \ldots, f_k)$ definiert als die $n$-stellige Operation

$$h(\vec{a}) := g(\, f_1(\vec{a}), \ldots, f_k(\vec{a})\,) \quad \text{für alle } \vec{a} = (a_1, \ldots, n) \in A^n.$$

Statt $g \circ_{n,k} (f_1, \ldots, f_k)$ schreibt man oft auch kürzer $g(f_1, \ldots, f_k)$ (oder noch kürzer $g \circ \vec{f}$).
Unter einem *Klon* auf $A$ versteht man eine Menge $\Omega$ von Operationen mit Stelligkeiten $> 0$ auf $A$ mit folgenden Eigenschaften:

1. $\Omega$ enthält alle Projektionen $\pi_i^{(n)}$, $n = 1, 2, \ldots$, $1 \leq i \leq n$.

2. $\Omega$ ist abgeschlossen unter allen $\circ_{n,k}$, d.h.:

   Liegen die $n$-stelligen Operationen $f_1, \ldots, f_k$ und die $k$-stellige Operation $g$ auf $A$ in $\Omega$, so auch die Komposition $g \circ_{n,k} (f_1, \ldots, f_k)$.

Die Vereinigung aller $\circ_{n,k}$, $n, k \in \mathbb{N}$, bezeichnen wir mit $\circ$.

**Definition 2.1.10.2.** Ein „binärer (oder 2-stelliger) Klon“ auf einer Menge $A$ ist eine Menge von zweistelligen Funktionen $f : A^2 \to A$, die erstens die beiden Projektionen enthält und die zweitens unter $\circ_{2,2}$ abgeschlossen ist.
Analog werden ternäre (3-stellige) und höherstellige Klone definiert, sowie auch unäre Klone. Unäre Klone sind dann einfach Untermonoide des Transformationsmonoids $(A^A, \circ)$.

Jeder Klon $\Omega$ auf $A$ induziert in natürlicher Weise einen binären Klon $\Omega \cap (A^{A^2})$. Im Allgemeinen ist diese Abbildung $\Omega \mapsto \Omega \cap (A^{A^2})$ aber nicht injektiv.

**UE 70** ► **Übungsaufgabe 2.1.10.3.** (E) Finden Sie eine Menge $A$ und zwei Klone $C_1 \neq C_2$ auf $A$ mit $C_1 \cap A^{A^2} = C_2 \cap A^{A^2}$. ◄ **UE 70**
(Hinweis: Zum Beispiel $A := \{0, 1\}$. Als $C_1$ wähle man einen trivialen Klon, als $C_2$ den kleinsten Klon, der die „Mehrheitsfunktion“ $m(x_1, x_2, x_3) = 1 \Leftrightarrow |\{i : x_i = 1\}| \geq 2$ enthält.)

**UE 71** ► **Übungsaufgabe 2.1.10.4.** (E) Sei $k \geq 3$, $A := \{1, \ldots, k\}$. Mit $A^A$ bezeichnen wir die Menge aller einstelligen Operationen auf $A$ (also aller Funktionen von $A$ nach $A$). Finden Sie mindestens 3 Klone $C$ auf $A$, die $A^A \subseteq C$ erfüllen. ◄ **UE 71**
(Hinweis: Den kleinsten und den größten Klon mit der geforderten Eigenschaft findet man leicht. Um einen weiteren Klon zu finden, betrachten Sie die Menge aller nicht surjektiven Funktionen. Beachten Sie aber, dass jede Projektion surjektiv ist.)

**UE 72** ► **Übungsaufgabe 2.1.10.5.** (E) Sei $1 \leq k < n$, und sei $f\colon A^k \to A$. Sei $g\colon A^n \to A$ ◄ **UE 72** durch

$$g(a_1, \ldots, a_n) := f(a_1, \ldots, a_k)$$

definiert. Sei $\Omega$ ein Klon auf $A$.
Zeigen Sie: Dann gilt $f \in \Omega \Leftrightarrow g \in \Omega$.

**Anmerkung 2.1.10.6.** Warum haben wir in der Definition eines Klons keine nullstelligen Funktionen zugelassen? Wenn wir den Begriff „$_0$Klon“ analog zum Begriff „Klon“ definieren, aber auch nullstelligen Funktionen zulassen, dann könnte man die gerade bewiesene Eigenschaft auch für $k = 0$ formulieren, allerdings nicht beweisen. Mit anderen Worten: es gäbe dann einen $_0$Klon $\Omega$, der zwar eine konstante einstellige Funktion $g$ enthält (eine so genannte „virtuelle Konstante“), nicht aber die zugehörige tatsächliche Konstante, die nullstellige Funktion $f$.
Wenn man sich allerdings für die Unteralgebren von Klonen interessiert, ist es sinnvoll, zwischen virtuellen Konstanten (mit Stelligkeit $\geq 1$) und nullstelligen Funktionen zu unterscheiden. Die leere Menge ist genau dann Unteralgebra eines $_0$Klons (also: unter allen Funktionen des $_0$Klons abgeschlossen), wenn der $_0$Klon keine nullstelligen Funktionen enthält.

Im Kontext der Universellen Algebra sind die wichtigsten Beispiele erstens der von den fundamentalen Operationen einer Algebra erzeugte Klon (der Klon der *Termfunktionen*), und zweitens der von den fundamentalen Operationen zusammen mit allen Konstanten erzeugte Klon (der Klon der *Polynomfunktionen*, man unterscheide diesen Zugang über Klone von jenem in 4.2.2). Die Bezeichnung rührt daher, dass es sich dabei um genau jene Funktionen handelt, die durch Polynome auf der entsprechenden Algebra induziert werden (siehe Definition 4.2.3.1). Umgekehrt kann jeder Klon auf einer Menge $A$ als Menge der fundamentalen Operationen einer Algebra aufgefasst werden.
Ist $|A| \in \{0, 1\}$, so gibt es trivialerweise nur einen Klon auf $A$. Für $|A| = 2$ sind es immerhin (abzählbar) unendlich viele, für $|A| = 3$ schon überabzählbar viele. Dennoch versteht man die Menge aller Klone auf einer beliebigen endlichen Menge $A$ recht gut. Viel komplizierter ist die Situation bei unendlichem $A$. Die interessanten Fragen hängen stark mit unendlicher Kombinatorik zusammen.
Erwähnenswert im Zusammenhang mit Klonen ist folgender Satz:

**Theorem 2.1.10.7.** Sei $\Omega$ ein Klon auf der Menge $A$, der alle binären Operationen auf $A$ enthält. Dann ist $\Omega$ bereits der Klon aller Operationen (beliebiger Stelligkeit) auf $A$.

**UE 73** ► **Übungsaufgabe 2.1.10.8.** (E) Man beweise Satz 2.1.10.7 für: ◄ **UE 73**

1. endliches $A$. Anleitung: Orientieren Sie sich an der Lagrangeinterpolation über Körpern, siehe 5.3.6.

2. unendliches $A$. Anleitung: Verwenden Sie, dass jede unendliche Menge $A$ gleichmächtig mit $A \times A$ ist (siehe Anhang, Kapitel 11). Sei $p\colon A \times A \to A$ bijektiv.

Finde zunächst bijektive Abbildungen $p_n\colon A^n \to A$ in dem von $p$ erzeugten Klon und zeige dann, dass die Menge aller unären Operationen zusammen mit den $p_n$ alle Operationen erzeugt.

Dieses Ergebnis kann man als Erklärung dafür ansehen, dass in der klassischen Algebra explizit kaum Operationen mit einer Stelligkeit $n > 2$ auftreten.

**UE 74** ► **Übungsaufgabe 2.1.10.9.** (E) Sei $(P, \leq)$ eine Halbordnung. Auf $P^k$ definieren wir eine Halbordnung $\leq_k$ „punktweise“: $(x_1, \ldots, x_k) \leq_k (y_1, \ldots, y_k)$ genau dann, wenn $x_1 \leq y_1$, $\ldots$, $x_k \leq y_k$. Eine Funktion $f\colon P^k \to P$ heißt monoton, wenn $\vec{x} \leq_k \vec{y} \Rightarrow f(\vec{x}) \leq f(\vec{y})$ für alle $\vec{x}, \vec{y} \in P^k$ gilt. Zeigen Sie, dass die Menge ◄ **UE 74**

$$C_{\leq} := \bigcup_{n=1}^{\infty} \{f\colon P^n \to P \mid f \text{ monoton}\}$$

einen Klon bildet. Beschreiben Sie für jede mögliche Halbordnung $R$ auf der Menge $\{0, 1\}$ den Klon $C_R$. (Überlegen Sie insbesondere, ob $R \neq S \Rightarrow C_R \neq C_S$ gilt.)

**UE 75** ► **Übungsaufgabe 2.1.10.10.** (F) Sei $(P, \leq)$ eine Halbordnung. Auf $P^k$ definieren wir die „lexikographische“ Halbordnung $\leq_{k,\text{lex}}$ wie folgt: Für $\vec{x} := (x_1, \ldots, x_k) \neq \vec{y} := (y_1, \ldots, y_k)$ sei $i := i_{\vec{x},\vec{y}}$ minimal mit $x_i \neq y_i$. Wir setzen $\vec{x} <_{k,\text{lex}} \vec{y}$ genau dann, wenn $x_{i_{\vec{x},\vec{y}}} < y_{i_{\vec{x},\vec{y}}}$. Weiters sei $\vec{x} \leq_{k,\text{lex}} \vec{y}$ genau dann, wenn $\vec{x} <_{k,\text{lex}} \vec{y}$ oder $\vec{x} = \vec{y}$.
(Anmerkung: Wenn $(P, \leq)$ eine lineare Ordnung ist, dann auch $\leq_{k,\text{lex}}$.)
Wir nennen eine Funktion $f\colon P^k \to P$ lex-monoton, wenn $\vec{x} \leq_{k,\text{lex}} \vec{y} \Rightarrow f(\vec{x}) \leq f(\vec{y})$ für alle $\vec{x}, \vec{y} \in P^k$ gilt. Ist die Menge aller lex-monotonen Funktionen ein Klon? ◄ **UE 75**

**UE 76** ► **Übungsaufgabe 2.1.10.11.** (F) Zeigen Sie, dass die Menge $\mathcal{O}_A$ aller Klone auf einer Menge $A$ (geordnet durch die Relation $\subseteq$) einen vollständigen Verband bildet. ◄ **UE 76**

## 2.2 Der kategorientheoretische Rahmen

In mancherlei Hinsicht noch wesentlich weiter gefasst als die bisherigen Strukturen eines gewissen Typs ist der begriffliche Rahmen der *Kategorientheorie*. Er erlaubt es, neben algebraischen und relationalen Strukturen z.B. auch topologische, maßtheoretische und viele andere in geeignete Klassen zusammenzufassen. Dazu ist es nötig, nicht nur Mengen in Betracht zu ziehen, sondern auch echte *Klassen*, d.h. Klassen, die keine Mengen sind.[42]

[42] In der Mengenlehre, die durch die ZFC-Axiome (von Zermelo und Fraenkel) beschrieben wird, gibt es gar keine Klassen; wenn man aber doch von Klassen spricht, wie etwa der Klasse aller Gruppen, dann spricht man in Wirklichkeit über die *Eigenschaft*, eine Gruppe zu sein; man kann beweisen, dass es keine Menge gibt, die alle Gruppen als Elemente enthält. In anderen Formulierungen der Mengenlehre, etwa im System NBG, das auf von Neumann, Bernays und Gödel zurückgeht, gibt es

Unterabschnitt 2.2.1 bringt dazu die grundlegenden Definitionen, 2.2.2 einige typische Beispiele. In 2.2.3 findet sich jener (in wenigen Zeilen beweisbare) Satz, den wir an vielen Stellen gewinnbringend einsetzen werden: Universelle (d.h. initiale bzw. finale) Objekte sind bis auf Äquivalenz eindeutig bestimmt, was in unseren Anwendungsbeispielen insbesondere Isomorphie bedeutet. In vielen Situationen lohnt es auch das Konzept des Funktors (2.2.4) zu kennen. Es ist das kategorientheoretische Analogon zum Homomorphismus zwischen Algebren. Eine auf den ersten Blick überraschende, ebenfalls aber höchst praktische Anwendung dieses Begriffs sind kommutative Diagramme, der Gegenstand von 2.2.5. Einen etwas weiteren Ausblick eröffnen natürliche Transformationen (2.2.6).

### 2.2.1 Kategorien

Inhalt in Kurzfassung: Dem Begriff der Kategorie liegt die Idee zugrunde, dass es von Interesse ist, Strukturen gleicher Art (seien es algebraische, relationale, topologische etc.) als sogenannte Objekte zu einer Klasse zusammenzufassen und die strukturverträglichen Abbildungen (Morphismen) zwischen je zwei solchen Objekten zu betrachten. Die formale Definition einer Kategorie ist extrem allgemein und Gegenstand dieses Unterabschnitts.

Wir definieren den Begriff der „Kategorie“, sowie den der „konkreten Kategorie“.

**Definition 2.2.1.1.** Eine *Kategorie* $\mathcal{C}$ ist gegeben durch

(i) eine Klasse von *Objekten* $A, B, \ldots \in \mathrm{Ob}(\mathcal{C})$ zusammen

(ii) mit einer Klasse paarweise disjunkter Mengen[43] $\mathrm{Hom}(A,B) = \mathrm{Hom}_{\mathcal{C}}(A,B)$ von *Morphismen* $f$ (für alle $A, B \in \mathrm{Ob}(\mathcal{C})$);

(iii) und einer Klasse von *Kompositionen*, geschrieben $(g,f) \mapsto g \circ f$,

$$\mathrm{Hom}(B,C) \times \mathrm{Hom}(A,B) \to \mathrm{Hom}(A,C)$$

für alle $A, B, C \in \mathrm{Ob}(\mathcal{C})$,

die die untenstehenden Eigenschaften $(I)$ und $(II)$ erfüllen.
Statt $A \in \mathrm{Ob}(\mathcal{C})$ schreiben wir oft nur $A \in \mathcal{C}$. Statt $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ schreiben wir auch $f\colon A \to B$ oder $f\colon A \to^{\mathcal{C}} B$; wir nennen $A$ die *Quelle* und $B$ das *Ziel* von $f$.

neben den Mengen auch „echte Klassen“ oder „Unmengen“, die zwar (ebenso wie Mengen) dadurch bestimmt sind, welche Elemente sie enthalten, die aber selbst nicht als Elemente anderer Klassen oder Mengen auftreten können. Typischerweise kommt eine Klasse zustande durch Zusammenfassung aller Objekte mit einer bestimmen Eigenschaft, was ja ziemlich genau dem Inhalt der historisch ersten Mengendefinition von Cantor entspricht. Die Einschränkungen beim Umgang mit Klassen gegenüber dem mit Mengen sind nötig, um Paradoxien von der Art jener von Russell zu vermeiden.

[43] Statt $\mathrm{Hom}_{\mathcal{C}}(A,B)$ ist auch die Schreibweise $\mathcal{C}(A,B)$ üblich. Statt $\mathrm{Hom}_{\mathcal{T}op}(A,B)$ schreibt man dann $\mathcal{T}op(A,B)$, etc.

(I) *Assoziativgesetz*: $\forall A, B, C, D \in \mathrm{Ob}(\mathcal{C})\ \forall f\colon A \to B, g\colon B \to C, h\colon C \to D$ :

$$h \circ (g \circ f) = (h \circ g) \circ f$$

(II) *Identität*: Für jedes Objekt $B \in \mathrm{Ob}(\mathcal{C})$ gibt es einen ausgezeichneten Morphismus $1_B \in \mathrm{Hom}(B, B)$, genannt die Identität auf $B$, so dass für alle $A, C \in \mathrm{Ob}(\mathcal{C})$ und alle $f\colon A \to B$ sowie $g\colon B \to C$ gilt:

$$1_B \circ f = f$$
$$g \circ 1_B = g$$

Ein Morphismus $f\colon A \to B$ heißt *Äquivalenz*, falls es ein $g\colon B \to A$ gibt mit $g \circ f = 1_A$ und $f \circ g = 1_B$. $A$ und $B$ heißen dann *äquivalent*, i.Z. $A \cong B$.
Bilden die Objekte einer Kategorie $\mathcal{C}$ eine Menge, so spricht man auch von einer *kleinen Kategorie*.

Wir werden noch zahlreiche Beispiele von Kategorien kennen lernen. Sehr typisch ist etwa die Kategorie der Gruppen mit den Gruppenhomomorphismen als Morphismen und der üblichen Verkettung von Abbildungen als Komposition. Da die Gruppen keine Menge bilden (es gibt „zu viele“ davon), handelt es sich um keine kleine Kategorie. Wir wir noch sehen werden, bildet ein einzelner Graph oder eine einzelne partielle Ordnung ein Beispiel für eine kleine Kategorie.
Man beachte, dass weder die Objekte einer Kategorie mit einer bestimmten Trägermenge einhergehen müssen, noch Morphismen mit Abbildungen im herkömmlichen Sinn. Legt man jedoch auf diese Sichtweise Wert, kann man die Definition folgendermaßen ergänzen.

**Definition 2.2.1.2.** Gibt es zu einer Kategorie $\mathcal{C}$ zusätzlich eine Funktion[44][45] $\mathsf{U}$, die jedem $A \in \mathrm{Ob}(\mathcal{C})$ eine Menge (ein *Universum*) $\mathsf{U}(A)$ und jedem Morphismus $f\colon A \to B$ eine Abbildung $\mathsf{U}(f)\colon \mathsf{U}(A) \to \mathsf{U}(B)$ im herkömmlichen Sinne zuordnet, so dass gilt:

(i) $\mathsf{U}(1_A)$ ist die identische Abbildung auf $\mathsf{U}(A)$,

(ii) die Komposition in $\mathcal{C}$ entspricht der Abbildungskomposition (d.h. $\mathsf{U}(f \circ g) = \mathsf{U}(f) \circ \mathsf{U}(g)$, wobei die erste Komposition $\circ$ jene in der Kategorie $\mathcal{C}$ und $\circ$ die gewöhnliche Abbildungskomposition in $\mathcal{Sets}$ ist, siehe 2.2.2,

(iii) die Abbildung $\mathsf{U}$ ist auf jeder der Mengen $\mathrm{Hom}_{\mathcal{C}}(A, B)$, mit $A, B \in Ob(\mathcal{C})$ injektiv,

dann heißt $\mathcal{C}$ *konkrete Kategorie*.

[44] Eine *relationale Klasse* ist eine Klasse, deren Elemente Paare sind; eine *funktionale Klasse* ist eine relationale Klasse, die rechtseindeutig ist, d.h. niemals Paare $(a, b)$ und $(a, b')$ mit $b \neq b'$ enthält. Da der Definitionsbereich der hier betrachteten „Funktion“ $\mathsf{U}$ eine echte Klasse sein kann, ist im Allgemeinen auch $\mathsf{U}$ eine echte Klasse; der Ausdruck „Funktion“ ist dann als Abkürzung für „funktionale Klasse“ zu lesen.

[45] $\mathsf{U}$ ist der Buchstabe $U$, nicht das Symbol $\bigcup$ für die Vereinigung von Mengen.

Die Zuordnung $\mathsf{U}$, die in der Definition 2.2.1.2 einer konkreten Kategorie auftritt, ist ein erstes Beispiel eines Funktors, siehe Definition 2.2.4.1. Und zwar nennt man diesen Funktor $\mathsf{U}$ (wie auch ähnliche in vergleichbaren Situationen) auch den *Vergissfunktor*[46]. Denn wendet man ihn beispielsweise auf die Kategorie der Gruppen an, so „vergisst“ man beim Übergang von der Gruppe zur Trägermenge gewissermaßen die algebraische Struktur auf dieser Trägermenge.
In vielen Gebieten der Mathematik gibt es einen natürlichen Begriff von „Morphismus“ zwischen den Strukturen, die in diesem Gebiet betrachtet werden (Homomorphismus in der Algebra, stetige Funktion in der Topologie, maßerhaltende Funktion in der Maßtheorie, etc.); somit bilden diese Strukturen oft in natürlicher Weise eine konkrete Kategorie, wobei die Klasse aller betrachteten Strukturen oft eine echte Klasse und keine Menge ist – so wie für den Fall der Gruppen bereits erwähnt.

### 2.2.2 Beispiele von Kategorien

Inhalt in Kurzfassung: Varietäten sind wichtige Beispiele von Kategorien. Von anderer Art aber gleichfalls von Interesse ist, dass man auch Graphen als Kategorien auffassen kann. Grob gesagt sind die Knoten die Objekte der Kategorie, Kanten sind (gewisse) Morphismen.

Die für uns wichtigsten Beispiele von Kategorien sind Varietäten. Und zwar lässt sich jede Varietät $\mathcal{V}$ in natürlicher Weise als konkrete Kategorie auffassen:
$\mathrm{Ob}(\mathcal{V})$ ist die Klasse aller Algebren in $\mathcal{V}$ und die Morphismen sind die Homomorphismen. Aus technischen Gründen[47] kann man hier allerdings nicht die Graphen der Abbildungen verwenden. Für $A, B \in \mathcal{V}$ setzen wir stattdessen

$$\mathrm{Hom}(A, B) = \{(A, f, B) \mid f \text{ ist Homomorphismus von } A \text{ nach } B\}.$$

Die Komposition ist die Abbildungskomposition. Genauer: Für $F = (A, f, B) \in \mathrm{Hom}(A, B)$ und $G = (B, g, C) \in \mathrm{Hom}(B, C)$ ist $G \circ F := (A, g \circ f, C)$.
Weil die Komposition assoziativ ist und die identischen Abbildungen Homomorphismen sind, die als Einselemente im Sinne von Definition 2.2.1.1 fungieren, erhält man tatsächlich eine Kategorie.
Diese Kategorie wird zur konkreten Kategorie, indem man $\mathsf{U}$ jeder Algebra ihre Trägermenge und jedem Homomorphismus die entsprechende Abbildung zwischen Mengen zuordnen lässt. Denn offensichtlich sind alle drei Bedingungen in Definition 2.2.1.2 erfüllt.

[46] englisch: *forgetful functor*

[47] Wir haben verlangt, dass die Morphismenmengen paarweise disjunkt sind. Wenn nun $\mathfrak{A}$ und $\mathfrak{A}'$ verschiedene Algebren aus $\mathcal{V}$ mit derselben Trägermenge sind, $\mathfrak{B}$ eine weitere Algebra in $\mathcal{V}$, dann könnte die selbe Funktion $f$ sowohl Homomorphismus von $\mathfrak{A}$ als auch von $\mathfrak{A}'$ nach $\mathfrak{B}$ sein; wir führen daher eine künstliche Unterscheidung zwischen dem (konkreten) Homomorphismus $f$ und dem (abstrakten) Morphismus $(\mathfrak{A}, f, \mathfrak{B})$ bzw. $(\mathfrak{A}', f, \mathfrak{B})$ ein.

Auch in den folgenden Beispielen können wir die Morphismenmengen disjunkt machen, indem wir jede Funktion $f\colon A \to B$ durch das Tripel $(A, f, B)$ ersetzen. Wohlgemerkt muss man für $A$ und $B$ die Objekte der Kategorie nehmen, nicht schlicht die Trägermengen.

Äquivalenz im kategorientheoretischen Sinn entspricht hier der Isomorphie von Algebren.

Folgende Spezialfälle von Varietäten als Kategorien begegnen uns besonders häufig:
Sind sowohl der Typ $\tau$ als auch die $\mathcal{V}$ definierende Menge $\Gamma$ von Gesetzen mit $\mathcal{V} = \mathcal{V}(-)$ leer, so erhält man die Kategorie $\mathcal{Sets}$ der Mengen.
Ist $\tau = (0)$ einelementig mit einer nullstelligen Operation und weiterhin $\Gamma = \emptyset$, so entsteht die Kategorie $\mathcal{Sets}_*$ der *punktierten Mengen*, oder *Mengen mit einem ausgezeichneten Punkt*; diese Algebren haben eine einzige nullstellige Operation $*$; Morphismen sind Homomorphismen im Sinne der Algebra, das heißt also: Abbildungen $f$, die $f(*) = *$ erfüllen, ausgezeichnete Punkte also auf ausgezeichnete Punkte abbilden.
Von Interesse sind auch die Kategorien $\mathcal{Grp}$ und $\mathcal{Ab}$ der Gruppen bzw. der abelschen Gruppen, außerdem die Kategorien $\mathcal{Rng}$ der Ringe bzw. $\mathcal{Rng}_1$ der Ringe mit Einselement.
Keine Varietäten aber dennoch interessante konkrete Kategorien sind (jeweils: Angabe der Objekte mit den Morphismen): Körper mit Monomorphismen (injektive Homomorphismen als Ringe mit 1); die Kategorie $\mathcal{Top}$ der topologischen Räume mit stetigen Abbildungen; die Kategorie $\mathcal{Top}_*$ der topologischen Räume mit einem ausgezeichneten Punkt mit stetigen Abbildungen, die ausgezeichnete Punkte auf ausgezeichnete Punkte abbilden, analog zu $\mathcal{Sets}_*$. Wir werden auch noch einige interessante Beispiele komplizierterer Art kennen lernen.

Von anderer Art ist das folgende Beispiel einer Kategorie.

**Definition 2.2.2.1.** Sei $R$ eine reflexive und transitive Relation auf einer Menge $V$. Wir können $(V, R)$ in folgender Weise als Kategorie auffassen:

- Die Objekte der Kategorie $(V, R)$ sind die Elemente von $V$.
- Für alle $a, b \in V$ mit $(a, b) \in R$ sei $\mathrm{Hom}_{(V,R)}(a, b)$ die einelementige Menge $\{(a, b)\}$. (Insbesondere ist $\mathrm{Hom}_{(V,R)}(a, a) = \{(a, a)\}$.)
- Für alle $a, b \in V$ mit $(a, b) \notin R$ sei $\mathrm{Hom}_{(V,R)}(a, b)$ die leere Menge.
- Komposition ist in natürlicher Weise definiert: Wenn $a\ R\ b\ R\ c$ gilt, dann liefert die Komposition der Elemente von $\mathrm{Hom}_{(V,R)}(a, b)$ und $\mathrm{Hom}_{(V,R)}(b, c)$ das (einzige) Element von $\mathrm{Hom}_{(V,R)}(a, c)$: $(b, c) \circ (a, b) = (a, c)$.

Wenn $E$ eine beliebige binäre Relation auf eine Menge $V$ ist, bezeichnen wir mit $E^*$ die reflexive transitive Hülle von $E$, das ist die kleinste $E$ umfassende Relation, die reflexiv und transitiv ist. (Eine solche gibt es, weil die Relationen mit dieser Eigenschaft durchschnittsstabil sind und somit nach 2.1.2.19 einen vollständigen Verband bilden.) Dann können wir $(V, E)$ als die durch $(V, E^*)$ gegebene Kategorie auffassen.

Für Relationen $E$ auf kleinen endlichen Mengen $V$ stellt man $(V, E)$ oft so dar, dass man eine möglichst kleine Menge $E_0$ mit $E_0^* = E^*$ findet, und dann $(V, E_0)$ als gerichteten Graphen $\Gamma = (V, E_0)$ auffasst, mit Kantenmenge $E_0$.
Also induziert jeder gerichtete Graph $\Gamma = (V, E)$ eine (nicht konkrete) Kategorie, die wir auch mit $\mathcal{C}(\Gamma)$ bezeichnen. Etwas später, wenn wir auch noch den Begriff des Funktors zur Verfügung haben, werden wir damit definieren, was unter einem kommutativen Diagramm zu verstehen ist.

**UE 77** ► **Übungsaufgabe 2.2.2.2.** (B) Sei $\Gamma = (V, E)$ ein Graph. ($V$ ist eine Menge, ebenso auch $E \subseteq V \times V$.) ◄ **UE 77**

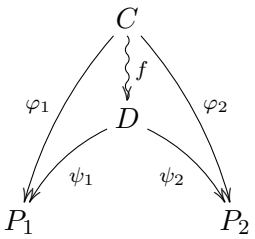
(1) Geben Sie ein $\mathsf{U}$ an, das die Kategorie $\mathcal{C}(\Gamma)$ zu einer konkreten Kategorie macht. (Beachten Sie, dass Sie $\mathsf{U}$ sowohl auf den Objekten als auch auf den Morphismen von $\mathcal{C}(\Gamma)$ definieren müssen.)

(2) Gibt es eine Kategorie $\mathcal{C}$, zu der es kein $\mathsf{U}$ gibt, das $\mathcal{C}$ zu einer konkreten Kategorie macht?

Typisch für die Konstruktion von neuen Kategorien aus einer bereits vorliegenden ist das folgende Beispiel.

**Beispiel 2.2.2.3.** Sei $\mathcal{C}$ eine Kategorie, und seien $P_1$ und $P_2$ Objekte in $\mathcal{C}$. Die Kategorie $\mathcal{C} \downarrow \{P_1, P_2\}$ ist so[48] definiert:

- Objekte von $\mathcal{C} \downarrow \{P_1, P_2\}$ sind Tripel $(C, \varphi_1, \varphi_2)$, wobei $C$ ein Objekt von $\mathcal{C}$ ist, und $\varphi_1$, $\varphi_2$ Morphismen von $C$ nach $P_1$ bzw. $P_2$.
- $\mathrm{Hom}_{\mathcal{C}\downarrow\{P_1,P_2\}}(\,(C, \varphi_1, \varphi_2),\, (D, \psi_1, \psi_2)\,)$ besteht aus allen Tripeln $(C, f, D)$ mit einem Morphismus $f \in \mathrm{Hom}_{\mathcal{C}}(C, D)$, der $\psi_i \circ f = \varphi_i$ für $i = 1, 2$ erfüllt.




- Die Komposition ist durch

$$(D, g, E) \circ (C, f, D) := (C, g \circ f, E)$$

gegeben, wobei $g \circ f$ die Komposition in $\mathcal{C}$ bezeichnet.

**UE 78** ► **Übungsaufgabe 2.2.2.4.** (F) Seien $\mathcal{C}$, $P_1$, $P_2$ wie in Beispiel 2.2.2.3. Dann ist $(C, \varphi_1, \varphi_2)$ genau dann ein terminales Objekt in $\mathcal{C} \downarrow (P_1, P_2)$, wenn ... (selbst vervollständigen und beweisen). ◄ **UE 78**

### 2.2.3 Universelle Objekte und ihre Eindeutigkeit

Inhalt in Kurzfassung: Der einzige rein kategorientheoretische Satz, den wir später verwenden werden (das dafür sehr häufig), besagt, dass universelle (genauer: initiale und

[48] Die Kategorie $\mathcal{C} \downarrow \{P_1, P_2\}$ ist ein spezielles Beispiel einer so genannten *Komma-Kategorie*.

terminale) Objekte einer Kategorie bis auf Äquivalenz eindeutig bestimmt sind. Die Definition all dieser Begriffe sowie der (kurze aber sehr typische) Beweis dieses Satzes sind die Hauptinhalte dieses Unterabschnitts.

**Definition 2.2.3.1.** Sei $\mathcal{C}$ eine Kategorie.

- $I \in Ob(\mathcal{C})$ heißt *initiales Objekt*, wenn es für alle $A \in Ob(\mathcal{C})$ einen *eindeutigen* Morphismus $f\colon I \to A$ gibt.
- $T \in Ob(\mathcal{C})$ heißt *terminales Objekt*, wenn es für alle $A \in Ob(\mathcal{C})$ einen *eindeutigen* Morphismus $f\colon A \to T$ gibt.

Initiale und terminale Objekte nennt man auch *universelle Objekte*. (Manchmal werden auch nur die initialen Objekte als universell bezeichnet und die terminalen als *kouniversell*.)

**Satz 2.2.3.2.** *Initiale Objekte einer Kategorie $\mathcal{C}$ sind, sofern es welche gibt, bis auf Äquivalenz eindeutig bestimmt; ebenso terminale Objekte.*

*Beweis.* Seien $I, J$ initiale Objekte von $\mathcal{C}$. Weil $I$ initial ist, existiert genau ein $f\colon I \to J$. Weil $J$ initial ist, existiert genau ein $g\colon J \to I$. Nun sind $g \circ f\colon I \to I$ und $f \circ g\colon J \to J$ Morphismen von $\mathcal{C}$, aber auch $1_I$ und $1_J$ sind Morphismen von $\mathcal{C}$. Da $I$ initial ist, gibt es genau einen Morphismus $I \to I$ (setze $A = I$ in der Definition). Daraus folgt $g \circ f = 1_I$. Analog ergibt sich $f \circ g = 1_J$, womit $I$ und $J$ äquivalent sind.
Genauso behandelt man den Fall terminaler Objekte. □

**UE 79** ► **Übungsaufgabe 2.2.3.3.** (F) Geben Sie initiale und terminale Objekte in folgenden Kategorien an (bzw. beweisen Sie, dass solche Objekte nicht existieren): $\mathcal{Sets}$, $\mathcal{Sets}_*$, $\mathcal{Grp}$, $\mathcal{Vec}_{\mathbb{Q}}$. (Hinweis: Vergessen Sie nicht, dass die leere Menge auch eine Menge ist.) ◄ **UE 79**

Wir werden zahlreiche Beispiele universeller Objekte von großem Interesse kennenlernen, z.B. Quotientenmonoide, -gruppen und -körper, Produkte, Koprodukte, freie Objekte und Polynomalgebren.

**UE 80** ► **Übungsaufgabe 2.2.3.4.** (F) Sei $\iota : \mathbb{N} \to \mathbb{Z}$ die Identität auf $\mathbb{N}$ (komplizierter gesagt: der eindeutig bestimmte Halbgruppenhomomorphismus, der 1 auf 1 abbildet). ◄ **UE 80**
Geben Sie eine Kategorie $\mathcal{D}$ an, sodass erstens gilt:

$$(*) \qquad (\mathbb{Z}, \iota) \text{ ist initial in } \mathcal{D},$$

und sodass zweitens die Aussage $(*)$ eine Umformulierung von Theorem 1.2.1.1(3) ist.

**UE 81** ► **Übungsaufgabe 2.2.3.5.** (D) Jeder der Zahlenbereiche $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ wurde so konstruiert, dass gewisse Mindestanforderungen auf minimale Weise erfüllt wurden. Die entsprechende Minimalität hatte jeweils einen Eindeutigkeitssatz zur Folge, der sich auch in eine universelle (initiale) Eigenschaft innerhalb einer geeigneten Kategorie übersetzen lässt. In der vorigen Übungsaufgabe haben wir dies für $\mathbb{Z}$ getan; finden Sie nun entsprechende Sätze für $\mathbb{N}$, $\mathbb{Q}$, $\mathbb{R}$ und/oder $\mathbb{C}$.
(Hinweis: Die Lösungen sind keineswegs eindeutig. Es kann durchaus sinnvoll und interessant sein, jeweils mehrere unterschiedliche Lösungen zu betrachten und miteinander zu vergleichen.) ◄ **UE 81**

### 2.2.4 Funktoren

Inhalt in Kurzfassung: Funktoren zwischen Kategorien spielen ziemlich genau die Rolle, die Homomorphismen zwischen Algebren desselben Typs spielen. Allerdings sind ko- von kontravarianten Funktoren zu unterscheiden. Wir werden wenig Gebrauch von Funktoren machen. Von zentraler Bedeutung sind sie in Gebieten wie etwa der Algebraischen Topologie. Da werden topologischen Räumen und stetigen Abbildungen durch Funktoren in verträglicher und sehr effektiver Weise gewisse algebraische Strukturen und Homomorphismen zugeordnet. Hier begnügen wir uns mit sehr einfachen Beispielen von Funktoren.

So wie algebraische Strukturen durch Homomorphismen zueinander in Beziehung gesetzt werden können, ist eine analoge Betrachtungsweise auch für Kategorien möglich. Diese führt zum Begriff des *Funktors*.

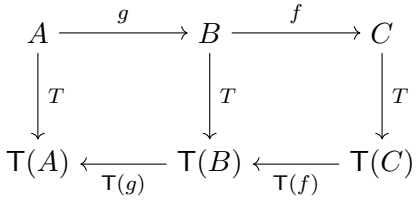
**Definition 2.2.4.1.** Seien $\mathcal{C}_1$ und $\mathcal{C}_2$ Kategorien. Wir betrachten Abbildungen $\mathsf{T}$ (als Abbildungen sind hier auch beliebige Klassen von Paaren zugelassen, nicht nur Mengen) folgender Art:
$\mathsf{T}$ ordnet jedem Objekt $A \in \mathcal{C}_1$ ein Objekt $\mathsf{T}(A) \in \mathcal{C}_2$ zu, außerdem jedem Morphismus $f\colon A \to B$ in $\mathcal{C}_1$ einen Morphismus $\mathsf{T}(f)$ in $\mathcal{C}_2$. Man nennt $\mathsf{T}$ einen *Funktor* von $\mathcal{C}_1$ nach $\mathcal{C}_2$, wenn erstens $\mathsf{T}(1_A) = 1_{\mathsf{T}(A)}$ (Funktoren bilden die Identität stets wieder auf die Identität ab) und zweitens eine der folgenden beiden Situationen vorliegt. Dabei spricht man im ersten Fall von einem *kovarianten*, im zweiten von einem *kontravarianten* Funktor.

**kovarianter Funktor** Für alle $A, B \in \mathcal{C}_1$ und für alle $f \in \mathrm{Hom}_{\mathcal{C}_1}(A, B)$ gilt $\mathsf{T}(f) \in \mathrm{Hom}_{\mathcal{C}_2}(\mathsf{T}(A), \mathsf{T}(B))$, kurz gesagt: Wenn $f\colon A \to B$, dann $\mathsf{T}(f)\colon \mathsf{T}(A) \to \mathsf{T}(B)$.

Weiters soll für alle $A, B, C \in \mathcal{C}_1$ und alle $g\colon A \to B$, $f\colon B \to C$ die Gleichung $\mathsf{T}(f \circ g) = \mathsf{T}(f) \circ \mathsf{T}(g)$ gelten.

$$\begin{array}{ccccc} A & \xrightarrow{\ g\ } & B & \xrightarrow{\ f\ } & C \\ \downarrow{\scriptstyle T} & & \downarrow{\scriptstyle T} & & \downarrow{\scriptstyle T} \\ \mathsf{T}(A) & \xrightarrow{\ \mathsf{T}(g)\ } & \mathsf{T}(B) & \xrightarrow{\ \mathsf{T}(f)\ } & \mathsf{T}(C) \end{array}$$

**kontravarianter Funktor** Hier drehen sich alle Richtungen um. Für $f\colon A \to B$ verlangen wir $\mathsf{T}(f)\colon \mathsf{T}(B) \to \mathsf{T}(A)$. Die Verträglichkeit mit der Komposition hat die Form $\mathsf{T}(f \circ g) = \mathsf{T}(g) \circ \mathsf{T}(f)$.




**UE 82** ► **Übungsaufgabe 2.2.4.2.** (F) Sei $\mathsf{T}$ ein Funktor von der Kategorie $\mathcal{C}_1$ in die Kategorie $\mathcal{C}_2$ und $A, B \in \mathcal{C}_1$. Zeigen Sie:
Sind $A, B$ äquivalent in $\mathcal{C}_1$, so auch $\mathsf{T}(A)$ und $\mathsf{T}(B)$ in $\mathcal{C}_2$. ◄ **UE 82**

Sehr wichtige Anwendungen finden Funktoren in der algebraischen Topologie. Zum Beispiel treten Funktoren von der Kategorie der topologischen Räume in die Kategorie der Gruppen auf. Einem topologischen Raum wird dabei beispielsweise seine Fundamentalgruppe, allgemeiner seine Homotopiegruppe oder auch seine Homologiegruppe zugeordnet. Übungsaufgabe 2.2.4.2 garantiert, dass topologische Räume mit nicht isomorphen Gruppen nicht homöomorph sein können. Nützlich ist das zum Beispiel deshalb, weil oft die Nichtisomorphie von Gruppen offensichtlich ist, während sich der direkte Nachweis der Nichthomöomorphie topologischer Räume als sehr schwierig erweist.
Wir betrachten nun einige einfache Beispiele von Funktoren.
Auf jeder konkreten Kategorie $\mathcal{C}$ ist die Abbildung $\mathsf{U}$, die jedem Objekt $A \in \mathcal{C}$ seine Trägermenge $\mathsf{U}(A)$ und jedem Morphismus $f\colon A \to B$ in $\mathcal{C}$ die zugehörige Mengenabbildung $\mathsf{U}(f)\colon \mathsf{U}(A) \to \mathsf{U}(B)$ gemäß Definition 2.2.1.2 zuordnet, ein kovarianter Funktor in die Kategorie $\mathcal{Sets}$ der Mengen. Man nennt $\mathsf{U}$ auch den *Vergissfunktor*, weil allfällige zusätzliche Struktur, welche die Mengen $\mathsf{U}(A)$ als Objekte $A$ von $\mathcal{C}$ tragen, nach Anwendung von $\mathsf{U}$ vergessen wird.
Die gleiche Sprechweise ist auch in allgemeineren Situationen üblich. Zum Beispiel kann man bei Ringen die multiplikative Struktur ignorieren (vergessen) und nur noch die additive Gruppe betrachten. Dies liefert einen Funktor von der Kategorie der Ringe in die Kategorie der abelschen Gruppen.
Wir wenden uns einem Beispiel zu, wo umgekehrt von Mengen ausgegangen wird, denen durch einen Funktor eine reichere Struktur zugeordnet wird.

**Beispiel 2.2.4.3.** Wir betrachten einen festen Körper $K$. Sei $\mathcal{Vec}_K$ die Kategorie alle $K$-Vektorräume, wobei wir als Morphismen alle $K$-linearen Abbildungen zulassen.

- Wir ordnen jeder Menge $X$ den Vektorraum $\mathsf{V}(X)$ aller Familien $(k_x)_{x\in X} \in K^X$ zu, in denen $k_x \neq 0$ nur für endlich viele $x \in X$ gilt. Die Vektorraumoperationen sind dabei die kanonischen: $(k_x)_{x\in X} + (l_x)_{x\in X} := (k_x + l_x)_{x\in X}$ und $\lambda(k_x)_{x\in X} := (\lambda k_x)_{x\in X}$.

Jedem $x_0 \in X$ können wir in natürlicher Weise ein Element $b(x_0) \in \mathsf{V}(X)$ (genauer: in der Menge $\mathsf{U}(\mathsf{V}(X))$) zuordnen, nämlich jenes Element $(k_x)_{x\in X}$ welches $k_{x_0} = 1$ und $k_x = 0$ für alle $x \neq x_0$ erfüllt.

Die Familie $(b(x))_{x\in X}$ ist offensichtlich eine Basis für $\mathsf{V}(X)$.

- Sei nun $f\colon X \to Y$ eine beliebige Mengenabbildung, also $f \in \mathrm{Hom}_{\mathcal{S}ets}(X, Y)$. Nach dem Fortsetzungssatz der linearen Algebra gibt es eine eindeutige lineare Abbildung $\mathsf{V}(f)\colon \mathsf{V}(X) \to \mathsf{V}(Y)$, die $\mathsf{V}(f)(b(x)) = b(f(x))$ für alle $x \in X$ erfüllt.

Der so definierte Funktor $\mathsf{V}$ von $\mathcal{S}ets$ nach $\mathcal{V}ec_K$ heißt auch der Freie Funktor (für $K$-Vektorräume).

**UE 83** ► **Übungsaufgabe 2.2.4.4.** (V) Erläutern Sie ausführlich, warum $\mathsf{V}$ tatsächlich ein kovarianter Funktor ist. ◄ **UE 83**

Zwei weitere sehr einfache Beispiele von Funktoren innerhalb der Kategorie der Mengen entstehen durch Bildung der Potenzmenge.

**Definition 2.2.4.5.** Der kovariante Potenzmengenfunktor $\mathfrak{P}$ von $\mathcal{S}ets$ nach $\mathcal{S}ets$ ist so definiert:

- $\mathfrak{P}(M)$ ist die Potenzmenge von $M$, für alle Objekte $M$ in $\mathcal{S}ets$.
- $\mathfrak{P}(f)\colon \mathfrak{P}(A) \to \mathfrak{P}(B)$ ist die Abbildung $S \mapsto \{f(x) : x \in S\} = f(S)$, für alle $f \in \mathrm{Hom}_{\mathcal{S}ets}(A, B)$.

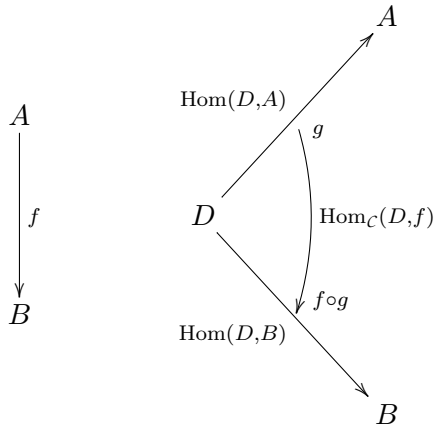
Der kontravariante Potenzmengenfunktor $\bar{\mathfrak{P}}$ von $\mathcal{S}ets$ nach $\mathcal{S}ets$ ist so definiert:

- $\bar{\mathfrak{P}}(M) := \mathfrak{P}(M)$.
- $\bar{\mathfrak{P}}(f)\colon \bar{\mathfrak{P}}(B) \to \bar{\mathfrak{P}}(A)$ ist die Abbildung $T \mapsto \{x \in A : f(x) \in T\} = f^{-1}(T)$, für alle $f \in \mathrm{Hom}_{\mathcal{S}ets}(A, B)$.

**UE 84** ► **Übungsaufgabe 2.2.4.6.** (F) Überprüfen Sie, dass die in 2.2.4.5 definierten Zuordnungen tatsächlich ko- bzw. kontravariante Funktoren sind. ◄ **UE 84**

Weitere einfach definierte Funktoren sind die Hom-Funktoren:

**Definition 2.2.4.7.** Sei $\mathcal{C}$ eine Kategorie, $D \in Ob(\mathcal{C})$.




Der *kovariante Hom-Funktor*, der oft mit $\mathrm{Hom}_{\mathcal{C}}(D,-)$ bezeichnet wird, geht von der Kategorie $\mathcal{C}$ in die Kategorie $\mathcal{Sets}$. Er

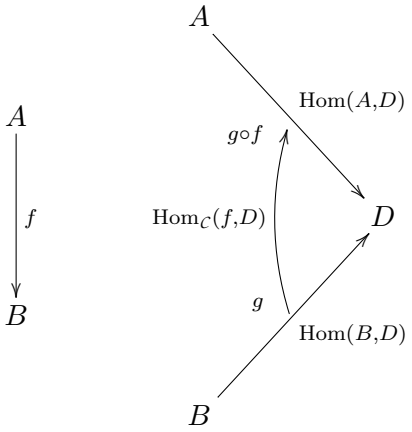
- ordnet jedem Objekt $A \in Ob(\mathcal{C})$ die Menge $\mathrm{Hom}_{\mathcal{C}}(D,A)$ zu;
- ordnet jedem Morphismus $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ die Abbildung $\mathrm{Hom}_{\mathcal{C}}(D,f)$ zu. Diese Abbildung geht von $\mathrm{Hom}_{\mathcal{C}}(D,A)$ nach $\mathrm{Hom}_{\mathcal{C}}(D,B)$, und ist durch die Vorschrift

$$\mathrm{Hom}_{\mathcal{C}}(D,f)(g) = f \circ_{\mathcal{C}} g$$

(für alle $g \in \mathrm{Hom}_{\mathcal{C}}(D,A)$) definiert.

Der *kontravariante Hom-Funktor*, der oft mit $\mathrm{Hom}_{\mathcal{C}}(-,D)$ bezeichnet wird, geht von der Kategorie $\mathcal{C}$ in die Kategorie $\mathcal{Sets}$. Er

- ordnet jedem Objekt $A \in Ob(\mathcal{C})$ die Menge $\mathrm{Hom}_{\mathcal{C}}(A,D)$ zu;
- ordnet jedem Morphismus $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ die Abbildung $\mathrm{Hom}_{\mathcal{C}}(f,D)\colon \mathrm{Hom}_{\mathcal{C}}(B,D) \to \mathrm{Hom}_{\mathcal{C}}(A,D)$ zu, die durch $\mathrm{Hom}_{\mathcal{C}}(f,D)(g) = g \circ_{\mathcal{C}} f$ (für alle $g \in \mathrm{Hom}_{\mathcal{C}}(B,D)$) definiert ist.




**UE 85** ► **Übungsaufgabe 2.2.4.8.** (V) Prüfen Sie alle behaupteten Eigenschaften des ko- und des kontravarianten Funktors $\mathrm{Hom}_{\mathcal{C}}(D,-)$ bzw. $\mathrm{Hom}_{\mathcal{C}}(-,D)$ nach. ◄ **UE 85**

**UE 86** ► **Übungsaufgabe 2.2.4.9.** (F) Zeigen Sie dass folgender Funktor (wir schreiben ihn als nachgestelltes Symbol $^*$) auf der Kategorie $\mathcal{Vec}_K$ der Vektorräume über dem Körper $K$ ein kontravarianter Funktor ist.
Dabei wird ◄ **UE 86**

- jedem $V \in \mathcal{Vec}_K$ sein Dualraum $V^*$ zugeordnet.
(Zur Erinnerung: $V^*$ ist der Raum aller linearen Abbildungen von $V$ nach $K$, genannt auch Funktionale, mit den punktweise definierten Operationen.)

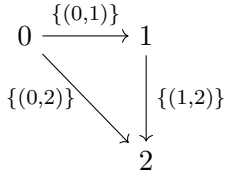
- Jedem Morphismus, d.h. jeder linearen Abbildung $f\colon V \to W$, wird ihre sogenannte *transponierte* Abbildung[49] $f^*\colon W^* \to V^*$ zugeordnet, die jedem Funktional $\ell \in W^*$ das Funktional $a \mapsto \ell(f(a))$ zuordnet.

Klarerweise ist die Zusammensetzung zweier kontravarianter Funktoren ein kovarianter Funktor. Insbesondere kann man den Funktor $^*$ aus Aufgabe 2.2.4.9 iterieren und erhält einen kovarianten Funktor $^{**}$ auf der Kategorie der Vektorräume über dem Körper $K$. Beschränkt man sich auf endlichdimensionale Vektorräume $V$, so ist bekanntlich der Dualraum $V^*$ isomorph zu $V$. Die Angabe eines Isomorphismus zwischen beiden ist aber willkürlich. Im Gegensatz dazu gibt es für jeden Vektorraum $V$ eine kanonische (natürliche) Abbildung $\alpha\colon V \to V^{**}$, gegeben durch $v \mapsto v^{**}$. Dabei ist $v^{**}\colon V^* \to K$ für ein beliebiges $\ell \in V^*$ definiert durch $v^{**}(\ell) := \ell(v)$. Aus der linearen Algebra wissen wir, dass $\alpha$ genau dann ein Isomorphismus ist, wenn $V$ endlichdimensional ist.
In der Funktionalanalysis betrachtet man normierte (oder allgemeiner: topologische) Vektorräume über dem Grundkörper $K = \mathbb{R}$ oder $K = \mathbb{C}$ und definiert den Dualraum $V'$ anders, nämlich als Menge der *stetigen* linearen Abbildungen von $V$ nach $K$.
Hier kann es auch bei unendlichdimensionalen Räumen vorkommen, dass die kanonische Abbildung $\alpha\colon V \to V''$ ein Isomorphismus ist; $V$ heißt in diesem Fall ein *reflexiver Raum*. Prominente reflexive Räume sind die Räume $\mathcal{L}_p(\mu)$ mit $1 < p < \infty$ über einem Maß $\mu$. Ihre Dualräume erhält man (bis auf isometrische Isomorphie) jeweils, wenn man $p$ durch jenes (so genannte konjugierte) $q$ ersetzt, welches durch $\frac{1}{p} + \frac{1}{q} = 1$ definiert ist.
Die Sprache der Kategorien und Funktoren ermöglicht es, ähnliche Situationen in einem sehr allgemeinen Kontext zu beschreiben. Hier wollen wir uns allerdings mit diesem sparsamen Hinweis begnügen.

### 2.2.5 Kommutative Diagramme als Funktoren

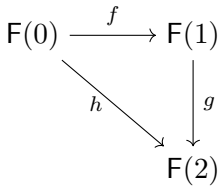
Inhalt in Kurzfassung: Kommutative Diagramme sind graphische Darstellungen dafür, dass verschiedene Verkettungen gewisser Abbildungen übereinstimmen. Situationen, wo es genau darum geht, sind in der Algebra ubiquitär. Sehr reizvoll ist die Einsicht, dass derartige Konstellationen auch in der Sprache der Kategorien und Funktoren, angewandt auf Kategorien von Graphen, ausgedrückt werden können.

**Beispiel 2.2.5.1.** Sei $V := \{0, 1, 2\}$, $E := \{(0, 1), (1, 2)\}$. Die transitive Hülle von $E$ ist dann $E^* = \{(0, 1), (1, 2), (0, 2)\}$. Durch $(V, E)$ bzw. durch $(V, E^*)$ wird (wie in 2.2.2.1 beschrieben) eine Kategorie *3* mit 3 Objekten definiert:



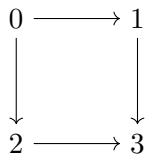

[49] oder auch *adjungierte* Abbildung

Sei nun $\mathcal{C}$ eine beliebige Kategorie. Dann wird ein kovarianter Funktor $\mathsf{F}\colon \mathcal{3} \to \mathcal{C}$ durch die 3 Objekte $\mathsf{F}(0)$, $\mathsf{F}(1)$, $\mathsf{F}(2)$ und durch die drei Morphismen[50] $f := \mathsf{F}(0,1)$, $g := \mathsf{F}(1,2)$ und $h := \mathsf{F}(0,2)$ beschrieben, wobei (wegen der Homomorphieeigenschaft von $\mathsf{F}$) die Bedingung $h = g \circ f$ gelten muss.

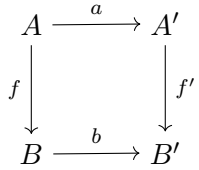



Ein Funktor $\mathsf{F}\colon \mathcal{3} \to \mathcal{C}$ ist also ein *kommutierendes* oder *kommutatives Dreieck* von $\mathcal{C}$-Morphismen.

**Beispiel 2.2.5.2.** Sei $V := \{0,1,2,3\}$, $E := \{(0,1),(0,2),(1,3),(2,3)\}$. Durch $(V,E)$ (bzw. durch $(V,E^*)$) wird eine Kategorie mit 4 Objekten und 5 Morphismen (sowie 4 identischen Morphismen) beschrieben, die wir $\square$ nennen. (Im folgenden Diagramm ist der Pfeil $(2,3)\circ(0,2) = (0,3) = (1,3)\circ(0,1)$ nicht eingezeichnet.)




Ein Funktor $\mathsf{F}\colon \square \to \mathcal{C}$ wird durch vier $\mathcal{C}$-Objekte $A = \mathsf{F}(0), A' = \mathsf{F}(1), B = \mathsf{F}(2), B' = \mathsf{F}(3)$ und vier Morphismen $f, f', a, b$ gegeben, die $f' \circ a = b \circ f$ erfüllen müssen, wodurch ein fünfter (diagonaler) Morphismus definiert wird.




So ein Funktor beschreibt also ein *kommutierendes* oder *kommutatives Quadrat* von $\mathcal{C}$-Morphismen.

**Definition 2.2.5.3.** Sei $V$ Menge, $E \subseteq V \times V$ eine Relation. Die Struktur $\Gamma = (V,E)$ bezeichnen wir als *gerichteten Graphen*. Die reflexive transitive Hülle $E^*$ von $E$ fassen wir wie in 2.2.2 als Kategorie auf, die wir auch mit $\Gamma$ bezeichnen.
Sei $\mathcal{C}$ eine Kategorie. Unter einem *kommutativen* $\Gamma$*-Diagramm in* $\mathcal{C}$ verstehen wir einen kovarianten Funktor von $\Gamma$ nach $\mathcal{C}$.

[50] Statt $f := \mathsf{F}(0,1)$ könnte man genauer $f := \mathsf{F}(\,(0,1)\,)$ schreiben, da ja $\mathsf{F}$ keine zweistellige Funktion ist, die zwei Argumente 0 und 1 erhält, sondern eine einstellige Funktion, die das Argument $(0,1)$ erhält. Dies wäre aber mühsamer zu lesen.

**Anmerkung 2.2.5.4.** Man könnte hier auch kontravariante Funktoren betrachten. Einen kontravarianten Funktor $(V, E) \to \mathcal{C}$ fassen wir aber lieber als kovarianten Funktor $(V, E^{op}) \to \mathcal{C}$ auf, wobei $E^{op} := \{(y, x) \mid (x, y) \in E\}$.

**Lemma 2.2.5.5.** *Sei $\Gamma = (V, E)$ ein Graph, $\mathcal{C}$ eine Kategorie.*
*Dann ist jedes kommutative $\Gamma$-Diagramm $\mathsf{F}$ (also: jeder Funktor $\mathsf{F}\colon \Gamma \to \mathcal{C}$) durch die Familie $(\mathsf{F}(e) : e \in E)$ eindeutig bestimmt.*
*Umgekehrt gilt: Sei $(f_e : e \in E)$ eine mit $E$ indizierte Familie von $\mathcal{C}$-Morphismen. Dann gibt es ein kommutatives $\Gamma$-Diagramm $\mathsf{F}$ mit $\mathsf{F}(e) = f_e$ für alle $e \in E$) genau dann, wenn*

- *erstens für alle $(x, y), (y, z) \in E$ gilt, dass das Ziel von $f_{(x,y)}$ gleich der Quelle von $f_{(y,z)}$ ist;*
- *zweitens für alle $(x, y) \in E^*$ und für beliebige Pfade $(x, z_1), (z_1, z_2), \ldots, (z_k, y)$ und $(x, z'_1), (z'_1, z'_2), \ldots, (z'_{k'}, y)$ die Gleichheit $f_{z_k,y} \circ \cdots \circ f_{x,z_1} = f_{z'_{k'},y} \circ \cdots \circ f_{x,z'_1}$ gilt. (Es genügt, dies für Pfade zu überprüfen, die nur die Endpunkte gemeinsam haben.)*

**UE 87 ▶ Übungsaufgabe 2.2.5.6.** (V) Beweisen Sie Lemma 2.2.5.5. **◀ UE 87**

## 2.2.6 Natürliche Transformationen

Inhalt in Kurzfassung: Stehen zwei Funktoren in einer Beziehung, die durch ein bestimmtes kommutatives Diagramm dargestellt werden kann, stößt man schnell auf den Begriff der natürlichen Transformation zwischen zwei Funktoren. Hier berühren wir diesen Themenkreis nur sehr oberflächlich, um die vorliegende Darstellung einiger Grundbegriffe der Kategorientheorie etwas abzurunden. Wir werden diese Konzepte später nicht mehr brauchen.

**Beispiel 2.2.6.1.** Wir betrachten die Menge $\mathbb{Z}$ mit der Relation $\{(n, n+1) : n \in \mathbb{Z}\}$.

$$\cdots \to -2 \to -1 \to 0 \to 1 \to 2 \to \cdots$$

Die transitive reflexive Hülle dieser Relation ist die wohlbekannte Relation $\leq$; wie in 2.2.2.1 wird $\mathbb{Z}$ dadurch zu einer Kategorie.
Sei $\mathcal{C}$ eine beliebige Kategorie. Ein kovarianter Funktor $\mathsf{F}\colon \mathbb{Z} \to \mathcal{C}$ wird dann durch eine Folge $(A_n : n \in \mathbb{Z})$ von $\mathcal{C}$-Objekten zusammen mit einer Folge $(f_n : n \in \mathbb{Z})$ von $\mathcal{C}$-Morphismen gegeben, wobei $f_n \in \mathrm{Hom}_{\mathcal{C}}(A_n, A_{n+1})$ gilt.
Seien die $\mathbb{Z}$-Diagramme $\mathsf{F}$ und $\mathsf{G}$ durch $(A_n, f_n : n \in \mathbb{Z})$ bzw. $(B_n, g_n : n \in \mathbb{Z})$ gegeben. Eine *natürliche Transformation* (oder ein *Morphismus von Diagrammen*) ist dann eine Familie $(\varphi_n : n \in \mathbb{Z})$ von Morphismen, $\varphi_n\colon A_n \to B_n$, wobei

$$\begin{array}{ccccccccc}
\ldots & \longrightarrow & A_{n-1} & \xrightarrow{f_{n-1}} & A_n & \xrightarrow{f_n} & A_{n+1} & \longrightarrow & \ldots \\
 & & \downarrow{\scriptstyle \varphi_{n-1}} & & \downarrow{\scriptstyle \varphi_n} & & \downarrow{\scriptstyle \varphi_{n+1}} & & \\
\ldots & \longrightarrow & B_{n-1} & \xrightarrow{g_{n-1}} & B_n & \xrightarrow{g_n} & B_{n+1} & \longrightarrow & \ldots
\end{array}$$

aus lauter kommutativen Quadraten besteht. Anders formuliert: Für alle $n$ gilt $\varphi_{n+1} \circ f_n = g_n \circ \varphi_n$.

$$\begin{array}{ccc} A_n & \xrightarrow{f_n} & A_{n+1} \\ {\scriptstyle\varphi_n}\downarrow & & \downarrow{\scriptstyle\varphi_{n+1}} \\ B_n & \xrightarrow{g_n} & B_{n+1} \end{array}$$

Dieses Konzept wird zum Beispiel in der Modultheorie im Zusammenhang mit (exakten) Sequenzen in 7.2.3 wichtige Anwendungen finden.

**Definition 2.2.6.2.** Seien $\mathcal{C}$ und $\mathcal{D}$ Kategorien, und seien $\mathsf{F}$ und $\mathsf{G}$ kovariante Funktoren von $\mathcal{C}$ nach $\mathcal{D}$. Eine *natürliche Transformation* $\tau$ von $\mathsf{F}$ nach $\mathsf{G}$ ist eine mit $Ob(\mathcal{C})$ indizierte Familie von Pfeilen in $\mathcal{D}$

$$(\tau_A : A \in Ob(\mathcal{C})) \qquad \text{mit} \qquad \forall A \in Ob(\mathcal{C}) : \tau_A \in \mathrm{Hom}_{\mathcal{D}}(\mathsf{F}(A), \mathsf{G}(A))$$

für die das unten stehende Quadrat kommutiert, d.h., dass für alle $A, B \in Ob(\mathcal{C})$ und alle $h \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ die Bedingung $\tau_B \circ \mathsf{F}(h) = \mathsf{G}(h) \circ \tau_A$ erfüllt ist.

$$\begin{array}{ccc} \mathsf{F}(A) & \xrightarrow{\mathsf{F}(h)} & \mathsf{F}(B) \\ {\scriptstyle\tau_A}\downarrow & & \downarrow{\scriptstyle\tau_B} \\ \mathsf{G}(A) & \xrightarrow{\mathsf{G}(h)} & \mathsf{G}(B) \end{array}$$

Wir kürzen den Sachverhalt „$\tau$ ist natürliche Transformation von $\mathsf{F}$ nach $\mathsf{G}$“ durch den Ausdruck $\tau\colon \mathsf{F} \to \mathsf{G}$ ab.

**Beispiel 2.2.6.3.** Sei $\mathfrak{P}\colon \mathcal{Sets} \to \mathcal{Sets}$ der kovariante Potenzmengenfunktor, und sei $I\colon \mathcal{Sets} \to \mathcal{Sets}$ der identische Funktor ($I(A) = A$, $I(f) = f$ für alle Objekte $A$ bzw. Pfeile $f$ in $\mathcal{Sets}$.)
Für jede Menge $A$ sei $\tau_A\colon A \to \mathfrak{P}(A)$ die durch $\tau_A(x) = \{x\}$ definierte Abbildung. Dann ist $\tau = (\tau_A : A \in \mathcal{Sets})$ eine natürliche Transformation von $I$ nach $\mathfrak{P}$.

**UE 88** ► **Übungsaufgabe 2.2.6.4.** (E) Für jede punktierte Menge $(A, a_0) \in Ob(\mathcal{Sets}_*)$ definieren wir $\mathfrak{P}^*(A, a_0) := (\{B \subseteq A : a_0 \in B\}, \{a_0\}) \in Ob(\mathcal{Sets}_*)$. ◄ **UE 88**
Sei $I\colon \mathcal{Sets}_* \to \mathcal{Sets}_*$ der Identitätsfunktor. Zeigen Sie, dass $\mathfrak{P}^*$ (bei geeigneter Definition auf den Morphismen) ein kovarianter Funktor von $\mathcal{Sets}_*$ nach $\mathcal{Sets}_*$ ist, und geben Sie eine natürliche Transformation von $\mathfrak{P}^*$ nach $I$ an.

**Lemma 2.2.6.5.** • *Seien* $\mathsf{F}, \mathsf{G}, \mathsf{H}$ *Funktoren von* $\mathcal{C}$ *nach* $\mathcal{D}$*, und seien* $\sigma\colon \mathsf{F} \to \mathsf{G}$ *und* $\tau\colon \mathsf{G} \to \mathsf{H}$ *natürliche Transformationen. Dann ist* $\tau \circ \sigma$*, definiert durch*

$$\forall A \in Ob(\mathcal{C}):\ (\tau \circ \sigma)_A\colon \mathsf{F}(A) \to \mathsf{H}(A), \quad (\tau \circ \sigma)_A := \tau_A \circ \sigma_A,$$

*eine natürliche Transformation von* $\mathsf{F}$ *nach* $\mathsf{H}$*.*

• *Die Familie* $id_{\mathsf{F}} := (\mathrm{id}_{\mathsf{F}(A)} : A \in Ob(\mathcal{C}))$ *ist eine natürliche Transformation von* $\mathsf{F}$ *nach* $\mathsf{F}$*.*

**UE 89** ► **Übungsaufgabe 2.2.6.6.** (V) Beweisen Sie Lemma 2.2.6.5. ◄ **UE 89**

Man kann Beispiel 2.2.6.1 verallgemeinern, indem man statt der Kategorie $\mathbb{Z}$ eine beliebige kleine Kategorie als „Indexmenge“ zulässt. Damit kann man die Klasse aller kovarianten Funktoren $\mathsf{F}\colon \mathcal{J} \to \mathcal{D}$ in natürlicherweise ebenfalls als Kategorie auffassen:

**Definition 2.2.6.7.** Sei $\mathcal{J}$ eine kleine Kategorie und $\mathcal{D}$ eine Kategorie. Die *Potenzkategorie* $\mathcal{D}^{\mathcal{J}}$ ist so definiert:

- $Ob(\mathcal{D}^{\mathcal{J}})$ ist die Klasse aller kovarianten Funktoren $\mathsf{F}\colon \mathcal{J} \to \mathcal{D}$.
- Für alle $\mathsf{F}, \mathsf{G}\colon \mathcal{J} \to \mathcal{D}$ ist $\mathrm{Hom}_{\mathcal{D}^{\mathcal{J}}}(\mathsf{F}, \mathsf{G})$ die Klasse aller natürlichen Transformationen $\tau\colon \mathsf{F} \to \mathsf{G}$.
- Komposition und Identität sind gemäß Lemma 2.2.6.5 definiert.

**UE 90** ► **Übungsaufgabe 2.2.6.8.** (E) Überprüfen Sie, dass $\mathcal{D}^{\mathcal{J}}$ tatsächlich eine Kategorie ist. ◄ **UE 90**

**UE 91** ► **Übungsaufgabe 2.2.6.9.** (E) Sei $K$ ein Körper. Sei $\mathsf{V} : \mathcal{Sets} \to \mathcal{Vec}_K$ der in Beispiel 2.2.4.3 definierte Funktor. Sei $\mathsf{U} : \mathcal{Vec}_K \to \mathcal{Sets}$ der Vergissfunktor, und sei $\mathsf{I} : \mathcal{Sets} \to \mathcal{Sets}$ der Identitätsfunktor. Geben Sie eine natürliche Transformation $\tau : \mathsf{I} \to \mathsf{U} \circ \mathsf{V}$ an. ◄ **UE 91**

**UE 92** ► **Übungsaufgabe 2.2.6.10.** (E) Seien $K$, $\mathsf{V} : \mathcal{Sets} \to \mathcal{Vec}_K$ und $\mathsf{U} : \mathcal{Vec}_K \to \mathcal{Sets}$ wie in der vorigen Aufgabe, und sei $\mathsf{I}' : \mathcal{Vec}_K \to \mathcal{Vec}_K$ der Identitätsfunktor. Geben Sie eine natürliche Transformation $\tau : \mathsf{V} \circ \mathsf{U} \to \mathsf{I}'$ an. (Bemühen Sie sich, eine interessante natürliche Transformation zu finden, und nicht einfach jene, wo jede Abbildung $\tau_A$ die Nullabbildung ist.) ◄ **UE 92**

## 2.3 Elemente algebraischer Strukturanalyse

Für eine, mehrere oder gar viele gegebene Algebren gibt es mehrere Methoden, um zu weiteren zu kommen. In diesem Abschnitt sollen die wichtigsten besprochen werden: Unteralgebren (Teilmengen, die selbst wieder Algebren bilden, 2.3.1), direkte Produkte (kartesische Produkte, die komponentenweise die gegebenen Strukturen erben, 2.3.2), Faktoralgebren (Partitionen, also Vergröberungen der ursprünglichen Algebra, nach Äquivalenzrelationen, auf die sich die ursprüngliche algebraische Struktur übertragen lässt; über den Homomorphiesatz gibt dies auch einen Überblick über die auf der gegebenen Algebra definierten Homomorphismen, 2.3.3), und direkte Limiten (2.3.4). Der kurze Unterabschnitt 2.3.5 beschäftigt sich mit der Frage der Kardinalitäten von Algebren in einer Varietät. Vermittels der sogenannten Isomorphiesätze (2.3.6) versteht man auch gewisse Kombinationen der in diesem Abschnitt eingeführten Konstruktionen sehr gut.

### 2.3.1 Unteralgebren und Erzeugnisse

Inhalt in Kurzfassung: In Verallgemeinerung des Begriffs des Unterraums eines Vektorraums sind Unteralgebren einer Algebra genau das, was man sich erwartet: Teilmengen, auf die eingeschränkt wieder eine Algebra desselben Typs vorliegt. Sehr schnell überzeugt man sich: Der Durchschnitt von Unteralgebren ist wieder eine Unteralgebra. Daraus folgt, dass sämtliche Unteralgebren einer gegebenen Algebra bezüglich der Inklusion einen vollständigen Verband bilden. Insbesondere gibt es zu jeder Teilmenge eine kleinste umfassende Unteralgebra, das sogenannte Erzeugnis dieser Teilmenge. Ein häufig verwendetes Ergebnis besagt, dass zwei Homomorphismen, die auf einer Teilmenge übereinstimmen, auch auf deren Erzeugnis übereinstimmen.

Aus der linearen Algebra kennen wir bereits die Begriffe der Untergruppe und des Untervektorraums; es handelt sich hier immer um Untermengen einer vorgegebenen Struktur (einer Gruppe, eines Vektorraums), die unter gewissen Operationen abgeschlossen sind. Hier besprechen wir das zugrunde liegende allgemeinere Konzept.

**Definition 2.3.1.1.** Ist $A$ eine Menge, $\omega : A^n \to A$ eine $n$-stellige Operation auf $A$ ($n \in \mathbb{N}$) und $U \subseteq A$, dann heißt $U$ *abgeschlossen* bezüglich $\omega$, wenn $\omega(U^n) \subseteq U$ gilt (d. h., wenn aus $u_1, \ldots, u_n \in U$ stets $\omega(u_1, \ldots, u_n) \in U$ folgt; im Fall $n = 0$ bedeutet das $\omega \in U$).
Ist $\mathfrak{A} = (A, (\omega_i)_{i\in I})$ eine Algebra vom Typ $(n_i)_{i\in I}$ und $U \subseteq A$, dann heißt $U$ *abgeschlossen* bezüglich $(\omega_i)_{i\in I}$, wenn $U$ abgeschlossen bezüglich $\omega_i$ für alle $i \in I$ ist. In diesem Fall wird durch $\omega_i^*(x_1, \ldots, x_{n_i}) := \omega_i(x_1, \ldots, x_{n_i})$, $(x_1, \ldots, x_{n_i}) \in U^{n_i}$, eine $n_i$-stellige Operation $\omega_i^*$ auf $U$ definiert: $\omega_i^* = \omega_i{\restriction}U^{n_i}$. Die Algebra $\mathfrak{U} := (U, (\omega_i^*)_{i\in I})$ (oft ungenau $U$ statt $\mathfrak{U}$) heißt dann eine *Unteralgebra* von $\mathfrak{A}$, symbolisch $U \leq \mathfrak{A}$ oder $\mathfrak{U} \leq \mathfrak{A}$. Meist schreiben wir $\omega_i$ für $\omega_i^*$, das heißt, wir identifizieren[51] die Operation $\omega_i$ mit ihrer Einschränkung $\omega_i^*$.

[51] Siehe Fußnote auf Seite 20.

**Anmerkung 2.3.1.2.** Bei Algebren ohne nullstellige Operationen ist es sinnvoll, auch die leere Menge als Unteralgebra zuzulassen, vor allem aus folgendem Grunde. Der Durchschnitt von Unteralgebren einer Algebra $(A, (\omega_i)_{i\in I})$ wird sich wiederum als Unteralgebra herausstellen und ist dann klarerweise die kleinste Unteralgebra von $A$. Wenn die Stelligkeit aller Operationen $> 0$ ist, dann kann das auch die leere[52] Menge sein; wenn es allerdings nullstellige Operationen gibt, dann enthält jede Unteralgebra alle nullstelligen Operationen (bzw. genauer: deren Werte).

Unteralgebren von Gruppen sind wieder Gruppen, die man *Untergruppen* nennt, ähnlich Unteralgebren von Ringen, die man *Unterringe* nennt etc. Generell sind Varietäten abgeschlossen bezüglich der Bildung von Unteralgebren:

**Proposition 2.3.1.3.** *Sei $\mathcal{V}$ eine Varietät (siehe 2.1.8.6), $\mathfrak{A} \in \mathcal{V}$ und $\mathfrak{U} \leq \mathfrak{A}$. Dann ist $\mathfrak{U} \in \mathcal{V}$.*

**UE 93 ► Übungsaufgabe 2.3.1.4.** (F) Beweisen Sie Proposition 2.3.1.3. **◄ UE 93**

Zur Illustration einige kunterbunte Beispiele:

- Sei $(H, \cdot)$ eine Halbgruppe. $U \subseteq H$ ist eine Unteralgebra von $(H, \cdot)$, wenn für $x, y \in U$ immer $xy \in U$. Es ist dann $\cdot = \cdot\restriction U \times U$ eine binäre Operation auf $U$, und $(U, \cdot)$ ist eine Halbgruppe, denn das Assoziativgesetz gilt in $H$ und damit erst recht in $T$. $(U, \cdot)$ heißt *Unterhalbgruppe* von $(H, \cdot)$.
- Ist $(G, \cdot)$ eine Gruppe vom Typ (2) und $(U, \cdot)$ Unterhalbgruppe von $(G, \cdot)$, so ist im allgemeinen $(U, \cdot)$ *keine* Gruppe. Beispiel: $(G, \cdot) = (\mathbb{Z}, +)$, $(U, \cdot) = (\mathbb{N}, +)$.
- Hingegen: Sei $(G, \cdot, e, {}^{-1})$ eine Gruppe vom Typ $(2, 0, 1)$. $U \subseteq G$ ist eine Unteralgebra, wenn

$$\begin{aligned} \forall x, y \in U : xy &\in U \\ e &\in U \\ \forall x \in U : x^{-1} &\in U \end{aligned}$$

  gilt. Bekanntermaßen ist das äquivalent zu

$$\begin{aligned} U &\neq \emptyset \\ \forall x, y \in U : xy^{-1} &\in U \end{aligned}$$

  Da die definierenden Gesetze einer Gruppe vom Typ $(2, 0, 1)$ in $G$ und damit auch in $U$ gelten, ist die Unteralgebra $(U, \cdot, e, {}^{-1})$ wieder eine Gruppe, genannt *Untergruppe* von $(G, \cdot, e, {}^{-1})$.

[52] Siehe Fußnote auf Seite 51.

- Ist $(R, +, 0, -, \cdot)$ ein Ring vom Typ $(2, 0, 1, 2)$, dann ist jede Unteralgebra $(U, +, 0, -, \cdot)$ wieder ein Ring, genannt *Unterring* von $(R, +, 0, -, \cdot)$. Dies gilt nicht für Ringe vom Typ $(2, 2)$. Beispiel: $(\mathbb{N}, +, \cdot)$ ist Unter*algebra* von $(\mathbb{Z}, +, \cdot)$, aber nicht Unter*ring*.

- Wichtig ist folgende analoge Situation: Sei $(K, +, 0, -, \cdot, 1)$ ein Körper vom Typ $(2, 0, 1, 2, 0)$ und $(U, +, 0, -, \cdot, 1)$ eine Unteralgebra (d. h. ein Unterring mit demselben Einselement). Ist $(U, +, 0, -, \cdot, 1)$ selbst ein Körper, so heißt dieser ein *Unterkörper* von $(K, +, 0, -, \cdot, 1)$. Es gilt: $U$ ist ein Unterkörper genau dann, wenn

$$\begin{aligned} \forall x, y \in U : x + y &\in U \\ 0 &\in U \\ \forall x \in U : -x &\in U \\ \forall x, y \in U : xy &\in U \\ 1 &\in U \\ \forall x \in U : (x \neq 0 \Rightarrow x^{-1} &\in U). \end{aligned}$$

  Beispiel: $(\mathbb{R}, +, 0, -, \cdot, 1)$ ist Unterkörper von $(\mathbb{C}, +, 0, -, \cdot, 1)$, aber $(\mathbb{Z}, +, 0, -, \cdot, 1)$ ist *kein* Unterkörper.

- Sei $(V, +, 0, -, (\omega_\lambda)_{\lambda \in K})$ ein Vektorraum über $K$ und $(U, +, 0, -, (\omega_\lambda)_{\lambda \in K})$ eine Unteralgebra, d. h.,

$$\begin{aligned} \forall x, y \in U : x + y &\in U \\ 0 &\in U \\ \forall x \in U : -x &\in U \\ \forall \lambda \in K, x \in U : \omega_\lambda(x) = \lambda x &\in U. \end{aligned}$$

  Dann ist auch $(U, +, 0, -, (\omega_\lambda)_{\lambda \in K})$ ein Vektorraum über $K$, genannt ein *Unterraum*.

- Betrachten wir das Monoid $M = (\{0, 1\}, \cdot, 1)$. Jede Teilmenge von $\{0, 1\}$ (insbesondere also auch die leere Menge) ist eine Unterhalbgruppe der Halbgruppe $(\{0, 1\}, \cdot)$. Die Algebren $(\{0\}, \cdot, 0)$, $(\{1\}, \cdot, 1)$ und natürlich $(\{0, 1\}, \cdot, 1)$ sind überdies Monoide. Allerdings sind nur $(\{1\}, \cdot, 1)$ und $(\{0, 1\}, \cdot, 1)$ *Untermonoide*, weil nur diese das neutrale Element 1 von $M$ haben – wir verstehen ein Monoid als Algebra vom Typ $(2, 0)$.

**UE 94** ► **Übungsaufgabe 2.3.1.5.** (F) Man zeige: $S := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ ist ein Unterkörper von $\mathbb{R}$ (mit den Standardoperationen). ◄ **UE 94**

**UE 95** ► **Übungsaufgabe 2.3.1.6.** (F) Sei $K = (K, +, 0, -, \cdot, 1)$ ein Körper mit Charakteristik 0. Zeigen Sie, dass es einen Unterkörper $K_0$ von $K$ gibt, der zu $\mathbb{Q}$ isomorph ist.
(Anmerkung: durch $f(0_{\mathbb{N}}) := 0_K$, $f((n+1)_{\mathbb{N}}) := f(n)+1_K$ wird eine Funktion $f : \mathbb{N} \to K$ definiert; statt $f(n)$ schreibt man meist $n*1$. „Charakteristik 0“ bedeutet: Für alle $n > 0$ gilt $f(n) \neq 0_K$.) ◄ **UE 95**

**Proposition 2.3.1.7.** *Sei $(A, \Omega)$ eine Algebra und $(T_j)_{j\in J}$ eine Familie von Unteralgebren. Dann ist $T := \bigcap_{j\in J} T_j$ ebenfalls eine Unteralgebra. Ist $(A, \Omega)$ ein Körper, und sind die $T_j$ Unterkörper, so auch $T$.*

**Anmerkung 2.3.1.8.** Für die leere Indexmenge $J = \emptyset$ ist der in Proposition 2.3.1.7 auftretende allgemeine Durchschnitt $\bigcap_{j\in J} T_j := \{ x \in A \mid \forall j \in J : x \in T_j \}$ als $\bigcap_{j\in J} T_j := A$ definiert.

*Beweis (von Proposition 2.3.1.7).* Der Fall $J = \emptyset$ ist klar, sodass wir im Folgenden $J \neq \emptyset$ annehmen. Ist $\omega \in \Omega$ eine $n$-stellige Operation und sind $a_1, \ldots, a_n \in T$ beliebig, so gilt $\omega(a_1, \ldots, a_n) \in T_j$ für alle $j \in J$, da $T_j$ eine Unteralgebra ist. Also gilt $\omega(a_1, \ldots, a_n) \in T$. Den Körperfall beweist man analog. □

Zusammen mit Korollar 2.1.2.19 folgt, wie bereits dort angekündigt:

**Folgerung 2.3.1.9.** *Ist $\mathfrak{A} = (A, (\omega_i)_{i\in I})$ eine Algebra, so bildet die Menge* $\mathrm{Sub}(\mathfrak{A})$ *aller Unteralgebren von $\mathfrak{A}$ mit der mengentheoretischen Inklusion eine vollständig verbandsgeordnete Menge, wobei das Infimum der mengentheoretische Durchschnitt ist.*

Wir interessieren uns nicht nur für das Infimum (= mengentheoretischer Schnitt), sondern auch für das Supremum in $\mathrm{Sub}(A)$. Man überzeugt sich sehr schnell, dass diese Verträglichkeit von Unteralgebren mit dem mengentheoretischen Durchschnitt für die Vereinigung nicht in gleicher Weise gilt:

**UE 96** ► **Übungsaufgabe 2.3.1.10.** (F) ◄ **UE 96**

(a) Zeigen Sie anhand eines Beispiels, dass für zwei Unteralgebren $\mathfrak{U}_1, \mathfrak{U}_2$ einer Algebra $\mathfrak{A}$ mit Trägermengen $U_1, U_2$ die Vereinigung $U := U_1 \cup U_2$ nicht Trägermenge einer Unteralgebra von $\mathfrak{A}$ sein muss.

(b) Zeigen Sie, dass die Vereinigung beliebig vieler Trägermengen von Unteralgebren, die bezüglich $\subseteq$ eine Kette bilden, sehr wohl stets eine Unteralgebra ist.

Für $S \subseteq A$ ist

$$\langle S \rangle = \langle S \rangle_{\mathfrak{A}} := \bigcap \{T \mid T \supseteq S \text{ und } T \text{ ist Unteralgebra von } (A, \Omega)\}$$

die *kleinste* Unteralgebra von $(A, \Omega)$, die $S$ enthält. Entsprechend definiert man:

**Definition 2.3.1.11.** $\langle S \rangle$ heißt die *von $S$ erzeugte Unteralgebra* von $(A, \Omega)$. $S$ heißt ein *Erzeugendensystem* von $\langle S \rangle$. Wenn $S$ endlich ist, sagen wir $S = \{s_1, \ldots, s_n\}$, dann schreiben wir statt $\langle \{s_1, \ldots, s_n\} \rangle$ abkürzend $\langle s_1, \ldots, s_n \rangle$.

**Anmerkung 2.3.1.12.** Nach Definition ist das Supremum in $\mathrm{Sub}(\mathfrak{A})$ von zwei Unteralgebren $\mathfrak{U}_1, \mathfrak{U}_2 \in \mathrm{Sub}(\mathfrak{A})$ gegeben durch die kleinste Unteralgebra, die die Trägermengen $U_1, U_2$ umfasst. Dies ist genau die von $U_1 \cup U_2$ erzeugte Unteralgebra, d.h. $U_1 \vee U_2 = \langle U_1 \cup U_2 \rangle \leq \mathfrak{A}$.

Die von $S$ erzeugte Algebra $\langle S \rangle$ kann auch so konstruiert werden: Sei $S_0 := S$. Induktiv definieren wir nun eine aufsteigende Folge von Mengen gemäß

$$S_{k+1} := S_k \cup \{\omega(b_1, \ldots, b_n) \mid b_1, \ldots, b_n \in S_k, \omega \in \Omega\}$$

und setzen $S_\infty := \bigcup_{k=0}^{\infty} S_k$. Wir zeigen als Nächstes, dass $S_\infty = \langle S \rangle$ gilt, und stellen eine Verbindung zu Termen her:

**Proposition 2.3.1.13.** *Seien $\mathfrak{A} = (A, \Omega)$ eine Algebra, $S \subseteq A$ und $S_k$, $k \in \mathbb{N}$, sowie $S_\infty$ definiert wie oben. Sei außerdem $T$ die Menge der Terme (siehe Definition 2.1.8.1) über der Variablenmenge $S$ und den Operationen[53] $\Omega$. Dann gilt:*

1. *$S_\infty = \langle S \rangle$.*
2. *$\langle S \rangle$ ist genau die Menge aller Werte von Termen, wenn wir für die Variablen aus $S$ ihren „Wert“ in $A$ einsetzen. Formal: Sei $\alpha : S \to A$ die identische Abbildung $s \mapsto s$. Für den von $\alpha$ induzierten Einsetzungshomomorphismus $\bar{\alpha} : T \to A$ gilt $\langle S \rangle = \bar{\alpha}(T)$. Insbesondere kann man die Kardinalität von $\langle S \rangle$ abschätzen durch $|\langle S \rangle| \leq \max\{|\mathbb{N}|, |S|, |\Omega|\}$.*

*Beweis.* 1. Mit Induktion nach $k$ zeigt man unmittelbar, dass für alle $k \in \mathbb{N}$ die Inklusion $S_k \subseteq \langle S \rangle$ gilt. Da jedenfalls $S = S_0 \subseteq S_\infty$ gilt, genügt es für die umgekehrte Inklusion nachzuweisen, dass $S_\infty$ unter den Operationen aus $\Omega$ abgeschlossen ist. Sei dazu $\omega \in \Omega$ $n$-stellig und seien $b_1, \ldots, b_n \in S_\infty$. Für jedes $i = 1, \ldots, n$ gibt es $k_i \in \mathbb{N}$ mit $b_i \in S_{k_i}$. Setzen wir $k := \max(k_1, \ldots, k_n)$, so gilt also $b_1, \ldots, b_n \in S_k$. Nach Definition von $S_{k+1}$ folgt $\omega(b_1, \ldots, b_n) \in S_{k+1} \subseteq S_\infty$.

2. Wir beweisen zunächst mit Induktion nach $k$, dass $S_k$ genau die Menge aller Werte von höchstens $k$-stufigen Termen ist, formal $S_k = \bar{\alpha}(T_k)$, wobei $T_k$ die Menge der höchstens $k$-stufigen Terme bezeichnet. (Noch formaler: Wir beweisen, dass die Menge $\{k \in \mathbb{N} \mid S_k = \bar{\alpha}(T_k)\}$ induktiv ist.)

   Der Induktionsanfang $k = 0$ folgt direkt aus den Definitionen: $S_0 = S$ (als Werte), $T_0 = S$ (als Variablen) und $\bar{\alpha}(S) = S$. Unter der Annahme $S_k = \bar{\alpha}(T_k)$ gilt

$$\begin{aligned} b \in S_{k+1} &\Leftrightarrow b \in \underbrace{S_k}_{=\bar{\alpha}(T_k)} \text{ oder } \exists \omega \in \Omega\, \exists b_1, \ldots, b_n \in \underbrace{S_k}_{=\bar{\alpha}(T_k)} : b = \omega(b_1, \ldots, b_n) \\ &\Leftrightarrow b \in \bar{\alpha}(T_k) \text{ oder } \exists \omega \in \Omega\, \exists p_1, \ldots, p_n \in T_k : b = \underbrace{\omega(\bar{\alpha}(p_1), \ldots, \bar{\alpha}(p_n))}_{=\bar{\alpha}(\omega(p_1, \ldots, p_n))} \\ &\Leftrightarrow b \in \bar{\alpha}(T_{k+1}), \end{aligned}$$

[53] Genauer: der Sprache, die wir der Operationenmenge $\Omega$ zuordnen

also $S_{k+1} = \bar{\alpha}(T_{k+1})$ wie gewünscht.

Unter Berücksichtigung von $S_\infty = \bigcup_{k=0}^{\infty} s_k$ und 1. sowie $T = \bigcup_{k=0}^{\infty} T_k$ ergibt sich daraus unmittelbar die Aussage.

Für die Kardinalitätsabschätzung zeigt man $|T_k| \leq \max(|\mathbb{N}|, |S|, |\Omega|)$ mit Induktion nach $k$ unter Berücksichtigung von $|T_k^n \times \Omega| \leq \max(|\mathbb{N}|, |T_k|, |\Omega|)$ für festes $n$ und weiter $|\bigcup_{n\in\mathbb{N}} T_k^n \times \Omega| \leq \max(|\mathbb{N}|, |T_k|, |\Omega|)$ (siehe Anhang, Unterabschnitt 11.4.8). □

Besondere Erwähnung verdient der Fall von Körpern. Unter einem *Unterkörper* $K$ eines Körpers $E$ (*Erweiterungskörper*) versteht man einen Unterring mit 1, der selbst Körper ist, der also zu jedem $\alpha \in K \setminus \{0\}$ auch das multiplikative Inverse $\alpha^{-1}$ enthält. Da wir die multiplikative Inversenbildung wegen des Problems mit der 0 nicht als fundamentale Operation auffassen können, ist der Begriff des Unterkörpers nicht ein Spezialfall des allgemeinen Begriffs einer Unteralgebra gemäß Definition 2.3.1.1. Beispielsweise ist $\mathbb{Z}$ eine Unteralgebra von $\mathbb{R}$ als Ring mit 1, nicht aber Unterkörper. Dennoch lassen sich die meisten Konzepte und Sachverhalte, die Algebren und Unteralgebren betreffen, in offensichtlicher Weise auf Körper und Unterkörper übertragen, wenn man die Bildung multiplikativer Inverse sinngemäß mit einbezieht. Wenn wir eine Teilmenge $S$ eines Körpers $K$ betrachten, ist mit $\langle S\rangle$ also nicht der Durchschnitt aller Unteralgebren von $K$ gemeint, die $S$ enthalten, sondern der Durchschnitt aller Unter*körper*, die $S$ enthalten.

**UE 97** ► **Übungsaufgabe 2.3.1.14.** Formulieren und beweisen Sie eine Variante von Proposition 2.3.1.13 für Körper. ◄ **UE 97**

**Anmerkung 2.3.1.15.** Die Beschreibung der erzeugten Algebra $\langle S\rangle$ „von unten“ als Vereinigung der Mengen $S_k$ ist für viele leichter zu verstehen, weil sie algorithmischen Charakter hat und die Elemente des Abschlusses explizit beschreibt. Sind $S$ und $\Omega$ höchstens abzählbar, so kann man auch $\langle S\rangle$ explizit abzählen.
Die Beschreibung des Abschlusses „von oben“ als Durchschnitt aller abgeschlossenen Mengen ist abstrakter und scheint auch komplizierter zu sein, weil es typischerweise sehr viele (oft überabzählbar viele) abgeschlossene Mengen gibt, deren Durchschnitt man bilden muss. Oft ist diese Charakterisierung aber leichter anwendbar, weil man sich dadurch ein mühsames Induktionsargument („Nach Induktion über $k$ zeigen wir, dass für alle $S_k$ gilt: ...“) ersparen kann.

Als Anwendung dazu lässt sich die wichtige Tatsache deuten, dass Homomorphismen durch ihre Werte auf einem Erzeugendensystem eindeutig bestimmt sind:

**Proposition 2.3.1.16.** *Seien $\mathfrak{A}$, $\mathfrak{B}$ Algebren, $\varphi\colon \mathfrak{A} \to \mathfrak{B}$ und $\varphi'\colon \mathfrak{A} \to \mathfrak{B}$ Homomorphismen. Sei $A_0 \subseteq A$. Wenn $\mathfrak{A} = \langle A_0\rangle$ und $\varphi(a) = \varphi'(a)$ für alle $a \in A_0$, dann ist $\varphi = \varphi'$.*

**UE 98** ► **Übungsaufgabe 2.3.1.17.** (W) Zeigen Sie Proposition 2.3.1.16. (Anmerkung: Es gibt zwei Möglichkeiten, dies zu beweisen: „von oben“ und „von unten“.) Diskutieren Sie auch die entsprechende Modifikation dieser Aussage für Körper. ◄ **UE 98**

Mit derselben Idee wie die erste Aussage von Proposition 2.3.1.13 beweist man:

**Proposition 2.3.1.18.** *Sei $\mathfrak{A} = (A, \Omega)$ eine Algebra oder ein Körper und sei $S \subseteq A$. Dann gilt*

$$\langle S \rangle = \bigcup_{S' \subseteq S \text{ endlich}} \langle S' \rangle.$$

**UE 99 ▶ Übungsaufgabe 2.3.1.19.** (V) Zeigen Sie Proposition 2.3.1.18. **◀ UE 99**

**UE 100 ▶ Übungsaufgabe 2.3.1.20.** (F) Zeigen Sie: **◀ UE 100**

1. In Vektorräumen gilt[54]:

$$\langle \{x_1, \ldots, x_n\} \rangle = \left\{ \sum_{1 \leq i \leq n} \lambda_i x_i \mid \lambda_1, \ldots, \lambda_n \in K \right\}.$$

2. Ist $(G, \cdot, e, ^{-1})$ eine *abelsche* Gruppe, dann gilt:

$$\langle \{x_1, \ldots, x_n\} \rangle = \{\, x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n} \mid k_1, \ldots, k_n \in \mathbb{Z} \,\}.$$

   Schreibt man die abelsche Gruppe in der Form $(G, +, 0, -)$, dann gilt:

$$\langle \{x_1, \ldots, x_n\} \rangle = \{k_1 x_1 + k_2 x_2 + \cdots + k_n x_n \mid k_1, \ldots, k_n \in \mathbb{Z}\}.$$

   (Man beachte aber, dass diese Darstellung im Allgemeinen nicht eindeutig ist; im Allgemeinen kann man nicht einmal aus der Gleichung $k_1 x_1 = k_1' x_1$ (in $G$) die Gleichheit $k_1 = k_1'$ (in $\mathbb{Z}$) folgern.)

   In diesem Unterpunkt (und allen folgenden) dürfen (und sollen) Sie einerseits die Tatsache, dass in Produkten beliebig umgeklammert werden kann (siehe Übungsaufgabe 2.1.3.5), und andererseits die – wohlvertraute – Rechenregel $a^{m+n} = a^m a^n$ für Potenzen verwenden (siehe Proposition 3.1.1.10 und Übungsaufgabe 3.1.1.11); für eine präzise Formulierung der Potenzen sei ebenfalls auf Abschnitt 3.1.1 verwiesen.

3. In beliebigen (nichtabelschen) Gruppen gilt:

$$\langle \{x_1, x_2\} \rangle = \{x_1^{k_{11}} x_2^{k_{12}} x_1^{k_{21}} x_2^{k_{22}} \cdots x_1^{k_{n1}} x_2^{k_{n2}} \mid n \in \mathbb{N},\, k_{ij} \in \mathbb{Z}\}.$$

[54] Die leere Summe $\sum_{i \in \emptyset} x_i$ definieren wir als 0. Dadurch gilt erstens die Gleichung $\sum_{i \in A \cup B} x_i = \sum_{i \in A} x_i + \sum_{j \in B} x_j$ für alle disjunkten Mengen $A, B$, und zweitens passt dann die angeführte Formel zur Tatsache, dass der von der leeren Menge erzeugte Vektorraum genau aus dem Nullvektor besteht: $\langle \emptyset \rangle = \{0\}$.

4. Ist $R$ ein kommutativer Unterring mit 1 von $S$ und $\alpha \in S$, so gilt:

$$\langle R \cup \{\alpha\}\rangle = \{p(\alpha) \mid p \in R[x]\}.$$

Dabei bezeichnet $R[x]$ die Menge aller Polynome $\sum_{k=0}^{n} a_k x^k$ mit $n \in \mathbb{N}$ und $a_i \in R$, $p(\alpha)$ den Wert des Polynoms $p$, wenn man für die „Unbestimmte“ $x$ das Element $\alpha$ einsetzt.

5. Ist $K$ ein Unterkörper von $E$ und $\alpha \in E$, so gilt:

$$\langle K \cup \{\alpha\}\rangle = \left\{ \frac{p(\alpha)}{q(\alpha)} \mid p, q \in K[x], q(\alpha) \neq 0 \right\}.$$

**UE 101** ► **Übungsaufgabe 2.3.1.21.** (W) Sei $K_1$ der Durchschnitt aller Unterkörper von $\mathbb{R}$, die $\sqrt{5}$ enthalten, und sei $K_2$ der Durchschnitt aller Unterkörper von $\mathbb{R}$, die $\pi$ enthalten. ◄ **UE 101**

(1) Beschreiben Sie $K_1$, und geben Sie einen Gruppenisomorphismus zwischen $(K_1, +, 0, -)$ und der additiven Gruppe $\mathbb{Q} \times \mathbb{Q}$ an.
(Hinweis: Siehe Übungsaufgabe 2.3.1.5.)

(2) Beschreiben Sie $K_2$, und geben Sie eine möglichst explizite surjektive Abbildung von $\mathbb{Q}^{<\infty} \times \mathbb{Q}^{<\infty}$ auf $K_2$ an. (Mit $X^{<\infty}$ bezeichnen wir die Menge $\bigcup_{n\in\mathbb{N}} X^n$ aller endlichen Folgen mit Elementen aus $X$.)
(Hinweis: Übungsaufgabe 2.3.1.20).

In beiden Unteraufgaben ist zu beweisen, dass die von Ihnen beschriebene Menge tatsächlich ein Körper ist, und dass die von Ihnen beschriebene Abbildung ein Isomorphismus bzw. surjektiv ist.

**UE 102** ► **Übungsaufgabe 2.3.1.22.** (1) (F) Gegeben sei folgende Menge $E$ von Teilmengen der Menge $\{0, 1, 2, 3\}$: ◄ **UE 102**

$$E := \{\, \{0\},\, \{0,1\},\, \{0,2\},\, \{0,2,3\},\, \{0,1,2,3\} \,\}$$

Geben Sie eine Algebra $\mathfrak{A}$ auf der Menge $A = \{0, 1, 2, 3\}$ an, deren Unteralgebren genau die Elemente von $E$ sind.

(2) (F) Ist Teil (1) für beliebige Mengen $E \subseteq \mathfrak{P}(A)$ lösbar?

(3) (F) Geben Sie ein effektives Kriterium (d.h., einen Algorithmus) an, das Ihnen für jede endliche Menge $A$ erlaubt, von jeder vorgelegten Menge $E \subseteq \mathfrak{P}(A)$ zu entscheiden, ob es eine Algebra $\mathfrak{A}$ auf der Grundmenge $A$ gibt, sodass $\mathrm{Sub}(\mathfrak{A}) = E$.

(4) (E) Inwiefern kann Ihr Kriterium auf unendliche Mengen verallgemeinert werden?

So wie in der Linearen Algebra endlichdimensionale Vektorräume viele interessante Eigenschaften haben, die nicht für beliebige Vektorräume gelten, spielt die entsprechende Verallgemeinerung dieses Konzeptes in sehr vielen einzelnen Strukturtheorien eine entscheidende Rolle.

**Definition 2.3.1.23.** Eine Algebra $\mathfrak{A}$ mit Trägermenge $A$ heißt *endlich erzeugt* beziehungsweise *abzählbar erzeugt*, wenn es eine endliche bzw. höchstens abzählbar unendliche Menge $E \subseteq A$ gibt mit $A = \langle E \rangle_{\mathfrak{A}}$.

Es besteht der folgende Zusammenhang zu Noetherschen Halbordungen:

**Proposition 2.3.1.24.** *Der Unteralgebrenverband* $(\mathrm{Sub}(\mathfrak{A}), \subseteq)$ *einer Algebra* $\mathfrak{A}$ *ist genau dann Noethersch, wenn jede Unteralgebra von* $\mathfrak{A}$ *endlich erzeugt ist.*

*Beweis.* Sei $(\mathrm{Sub}(\mathfrak{A}), \subseteq)$ Noethersch. Wir nehmen indirekt an, dass es eine Unteralgebra $\mathfrak{U} \leq \mathfrak{A}$ mit Trägermenge $U$ gebe, die nicht endlich erzeugt ist. Dann ist zu jeder endlichen Teilmenge $E \subseteq U$ die Menge $C_E := U \setminus \langle E \rangle_{\mathfrak{A}}$ nicht leer. Laut Auswahlaxiom gibt es eine Abbildung $f : \mathcal{E} \to U$ von der Menge $\mathcal{E}$ aller endlichen $E \subseteq U$ nach $U$ mit $f(E) \in C_E$ für alle $E \in \mathcal{E}$. Nach dem Rekursionssatz gibt es eine eindeutige Folge von $u_n \in U$ mit $u_0 = f(\emptyset)$ und $u_{n+1} := f(\{u_0, \ldots, u_n\})$ für alle $n \in \mathbb{N}$. Nach Konstruktion bilden dann die $\mathfrak{U}_n := \langle \{u_0, \ldots, u_n\} \rangle_{\mathfrak{A}} \leq \mathfrak{A}$, $n \in \mathbb{N}$, eine unendliche echt aufsteigende Folge in $\mathrm{Sub}(\mathfrak{A})$, Widerspruch zu Noethersch.
Sei nun umgekehrt jede Unteralgebra $\mathfrak{U} \leq \mathfrak{A}$ endlich erzeugt. Der Beweis ist erbracht, wenn wir zu einer beliebig vorgegebenen unendlichen (nicht notwendig echt) aufsteigenden Folge von Unteralgebren $\mathfrak{U}_0 \leq \mathfrak{U}_1 \leq \ldots \leq \mathfrak{A}$ ein $n_0 \in \mathbb{N}$ finden, so dass $\mathfrak{U}_n = \mathfrak{U}_{n_0}$ für alle $n \geq n_0$ gilt. Für $n \in \mathbb{N}$ bezeichne dazu $U_n$ die Trägermengen von $\mathfrak{U}_n$ . Die Vereinigung $U := \bigcup_{n \in \mathbb{N}} U_n$ ist laut Übungsaufgabe 2.3.1.10 die Trägermenge einer Unteralgebra $\mathfrak{U}$. Nach Voraussetzung wird $\mathfrak{U}$ von endlich vielen Elementen $u_1, \ldots, u_m \in U$ erzeugt. Zu jedem $i = 1, \ldots, m$ gibt es einen Index $k_i \in \mathbb{N}$ mit $u_i \in U_{k_i}$. Weil die $U_n$ eine Kette bezüglich $\subseteq$ bilden, gilt $u_i \in U_{n_0}$ für $i = 1, \ldots, m$ und $n_0 := \max\{k_1, \ldots, k_m\}$. Folglich gilt

$$\mathfrak{U} = \langle \{u_1, \ldots, u_m\} \rangle_{\mathfrak{A}} \leq \mathfrak{U}_{n_0} \leq \mathfrak{U}_n \leq \mathfrak{U},$$

also $\mathfrak{U}_n = \mathfrak{U}_{n_0}$ für alle $n \geq n_0$, womit der Satz bewiesen ist. □

**UE 103** ► **Übungsaufgabe 2.3.1.25.** (A) Geben Sie unter Verwendung von Proposition 2.1.2.12 ◄ **UE 103** einen alternativen Beweis der Implikation „Noethersch ⇒ endlich erzeugt“ in Satz 2.3.1.24:

> Sei $\mathfrak{A}$ Noethersch, und sei $\mathfrak{U}$ eine Unteralgebra mit Trägermenge $U$. Um zu zeigen, dass $\mathfrak{U}$ endlich erzeugt ist, betrachten wir die Familie aller endlich erzeugten Unteralgebren von $\mathfrak{U}$; diese hat ein maximales Element...

Als Abschluss des Unterabschnitts über Unteralgebren heben wir noch ihre Verträglichkeit mit Homomorphismen hervor, sowohl Bilder als auch Urbilder betreffend. Sei dazu $f\colon G \to H$ ein Homomorphismus zwischen zwei Algebren desselben Typs $(n_i)_{i \in I}$ mit entsprechenden Operationen $\omega_{G,i}$ und $\omega_{H,i}$. Dann ist die Menge $f(G)$ der Bilder $f(g)$, $g \in G$, eine Unteralgebra von $H$. Sind nämlich $g_1, \ldots, g_{n_i}$ für irgendein $i \in I$ beliebige Elemente aus $G$, so ist wegen der Homomorphiebedingung

$$\omega_{H,i}(f(g_1), \ldots, f(g_{n_i})) = f(\omega_{G,i}(g_1, \ldots, g_{n_i}))$$

die Menge $f(G)$ abgeschlossen bezüglich $\omega_{H,i}$. Dasselbe Argument lässt sich auf Unteralgebren von $G$ statt auf $G$ selbst anwenden: Liegen die $f(g_i)$ in einer Unteralgebra $U$ von $H$, so, wegen der Abgeschlossenheit von $U$ bezüglich $\omega_{H,i}$, auch $f(\omega_{G,i}(g_1, \ldots, g_{n_i}) = \omega_{H,i}(f(g_1), \ldots, f(g_{n_i}))$. Außerdem zeigt ein sehr ähnliches Argument die analoge Aussage für Urbilder statt Bilder unter Homomorphismen.

**Proposition 2.3.1.26.** *Bilder wie auch Urbilder von Unteralgebren unter Homomorphismen sind wieder Unteralgebren.*

**UE 104** ► **Übungsaufgabe 2.3.1.27.** (F+) Beweisen Sie die Aussage über Urbilder aus Proposition 2.3.1.26. ◄ **UE 104**

### 2.3.2 Direkte Produkte

Inhalt in Kurzfassung: Liegt eine Familie von Algebren des gleichen Typs vor, so trägt das kartesische Produkt ihrer Trägermengen eine natürliche algebraische Struktur desselben Typs. Man spricht vom direkten Produkt der Algebren. Direkte Produkte zeichnen sich durch eine universelle Eigenschaft aus, in der die sogenannten Projektionen vom direkten Produkt in die einzelnen Komponenten eine zentrale Rolle spielen.

Wir erinnern uns an die Konstruktion ganzer Zahlen $k = [(n_1, n_2)]_\sim$ als Äquivalenzklassen von Paaren natürlicher Zahlen $n_1, n_2$ oder reeller Zahlen $r = [(a_n)_{n\in\mathbb{N}}]_\sim$ als Äquivalenzklassen von Cauchyfolgen rationaler Zahlen $a_n$. In beiden Fällen trägt die Menge der Paare bzw. Folgen selbst eine algebraische Struktur, die sich aus der komponentenweisen Anwendung von Operationen ergibt, z.B.: $(m_1, m_2) + (n_1, n_2) = (m_1 + n_1, m_2, n_2)$ bzw. $(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} = (a_n + b_n)_{n\in\mathbb{N}}$. Das ist charakteristisch für die allgemeine Konstruktion *direkter Produkte* aus zwei oder mehreren (eventuell auch unendlich vielen) Strukturen gleicher Art zu einer weiteren, „größeren“ Struktur dieser Art. In unseren Beispielen sind es zwei bzw. abzählbar unendlich viele Kopien der additiven Strukturen auf $\mathbb{N}$ bzw. $\mathbb{Q}$. Darüber hinaus gibt es natürliche Epimorphismen vom direkten Produkt auf jede der Komponenten, nämlich die Projektionen. Diese Beobachtung lässt sich zur Definition 2.3.2.3 präzisieren, die wir vorbereiten, indem wir zunächst lediglich die Trägermengen behandeln:

**Definition 2.3.2.1.** Sei $K$ eine Indexmenge und $A_k$, $k \in K$, Mengen. Das *kartesische Produkt* $\prod_{k\in K} A_k$ ist die Menge aller Funktionen $f$ mit Definitionsbereich $K$, die

$$\forall k \in K : f(k) \in A_k$$

erfüllen (die Funktionen $f$ gehen also von $K$ in die Menge $\bigcup_{k\in K} A_k$).
Die Elemente von $A := \prod_{k\in K} A_k$ heißen *$K$-Tupel*; wir bezeichnen Elemente von $A$ auch manchmal als Vektoren $\vec{a} = (a_k : k \in K)$. Statt $(a_k : k \in K)$ ist auch die Schreibweise $(a_k)_{k\in K}$ üblich.
Für $j \in K$ heißt die Abbildung $p_j \colon \prod_k A_k \to A_j$, die durch $p_j(f) = f(j)$ definiert ist, die $j$-te *Projektion*.

Eine Bemerkung zum Fall $K = \{1, 2\}$ ist am Platze. In diesem Fall besteht das kartesische Produkt aus allen Abbildungen $1 \mapsto a_1 \in A_1, 2 \mapsto a_2 \in A_2$. Notiert man so eine Abbildung als $(a_k)_{k\in K} = (a_k)_{k=1,2}$, so liegt es nahe, sie mit dem geordneten Paar $(a_1, a_2)$ zu identifizieren. Dann wäre die Menge $\prod_{k\in K} A_k = \prod_{k=1,2} A_k$ als Menge aller Paare $(a_1, a_2)$ mit $a_1 \in A_1$ und $a_2 \in A_2$ schlicht das gewöhnliche kartesische Produkt zweier Mengen gemäß Definition 2.1.1.1, daher die Bezeichnungsweise. Ein typisches Element von $\prod_{k=1,2} A_k$ hat präzise gesprochen jedoch die Form $\{(1, a_1), (2, a_2)\}$ und nicht $(a_1, a_2)$. Obwohl die beiden Mengen rein formal also verschieden sind, bezeichnet man beide als „kartesische Produkte“ $A_1 \times A_2$ und identifiziert sie oft in der beschriebenen Weise (siehe auch die Bemerkungen nach Definition 2.1.3.1).
Ein Sonderfall, der aus anderen Gründen gesonderte Erwähnung verdient, ist $K = \emptyset$. Dann gibt es genau eine Familie $(A_k : k \in K)$ von Mengen, und das Produkt dieser „leeren“ Familie enthält ein einziges Tupel, nämlich die leere Menge, symbolisch: $\prod_{k\in\emptyset} A_k = \{\emptyset\}$.

**UE 105** ► **Übungsaufgabe 2.3.2.2.** (F+) Seien $A_k$, $k \in K$, Mengen, $A := \prod_{k\in K} A_k$ deren Produkt, und für alle $j \in K$ sei $p_j \colon A \to A_j$ die $j$-te Projektion. Sei $B$ eine beliebige Menge, und seien $q_j \colon B \to A_j$ beliebige Abbildungen.
Dann gibt es genau eine Abbildung $h \colon B \to A$, die $p_j \circ h = q_j$ für alle $j$ erfüllt. ◄ **UE 105**

Analoges gilt für algebraische Strukturen. Die Präzisierung gelingt mit folgender Definition, die Definition 2.3.2.1 als Spezialfall (mit $I = \emptyset$) enthält.

**Definition 2.3.2.3.** Seien $\mathfrak{A}_k = (A_k, (\omega_{i,k})_{i\in I})$, $k \in K$, Algebren vom selben Typ $(n_i)_{i\in I}$ und sei $A := \prod_{k\in K} A_k$ das Produkt aller Mengen $A_k$. Für alle $i \in I$ sei die Operation $\omega_i$ auf $A$ komponentenweise definiert:

$$\omega_i((a_{k,1})_{k\in K}, \ldots, (a_{k,n_i})_{k\in K}) := (\omega_{i,k}(a_{k,1}, \ldots, a_{k,n_i}))_{k\in K}$$

Die Algebra $\mathfrak{A} := (A, (\omega_i)_{i\in I})$ heißt das *direkte Produkt* der Algebren $\mathfrak{A}_k$ und wird mit $\prod_{k\in K} \mathfrak{A}_k$ bezeichnet. Ist $K$ endlich mit $m$ Elementen, so schreibt man für das direkte Produkt $\mathfrak{A}$ häufig auch $\mathfrak{A}_1 \times \ldots \times \mathfrak{A}_m$.

In unmittelbarer Verallgemeinerung von Aufgabe 2.3.2.2 ergibt sich:

**Proposition 2.3.2.4.** *Sei $(\mathfrak{A}_k : k \in K)$ eine Familie von Algebren desselben Typs, und sei $\mathfrak{A} := \prod_k \mathfrak{A}_k$ deren Produkt. Für alle $j \in K$ sei $p_j \colon \mathfrak{A} \to \mathfrak{A}_j$ die $j$-te Projektion. Sei $\mathfrak{B}$ eine beliebige Algebra vom selben Typ wie die $\mathfrak{A}_k$, und seien $q_j \colon \mathfrak{B} \to \mathfrak{A}_j$ beliebige Homomorphismen.*
*Dann sind die Abbildungen $p_j$ Homomorphismen, und es gibt genau einen Homomorphismus $h : \mathfrak{B} \to \mathfrak{A}$, der $p_j \circ h = q_j$ für alle $j$ erfüllt.*

**UE 106** ► **Übungsaufgabe 2.3.2.5.** (W) Beweisen Sie Proposition 2.3.2.4. ◄ **UE 106**

In der Sprache der Kategorientheorie besagt Proposition 2.3.2.4, dass Produkte als universelle Objekte in einer geeigneten Kategorie aufgefasst werden können. Die allgemeine Definition dazu:

**Definition 2.3.2.6.** Sei $\mathcal{C}$ eine Kategorie, $A_k, k \in K$, Objekte in $\mathcal{C}$. Dann heißt ein Objekt $P$ aus $\mathcal{C}$ zusammen mit einer Familie $(p_k)_{k\in K}$ von Morphismen $p_k\colon P \to A_k$ ein *Produkt* der $A_k$ in $\mathcal{C}$, symbolisch $P = \prod_{k\in K} A_k$, wenn es ein terminales Objekt in folgender Kategorie $\mathcal{C}^* = \mathcal{C}^*((A_k, p_k)_{k\in K})$ ist:

- Die Objekte von $\mathcal{C}^*$ sind Tupel $(A, (\varphi_k)_{k\in K})$, wobei $A \in Ob(\mathcal{C})$ und $\varphi_k\colon A \to A_k$ Morphismen aus $\mathcal{C}$ sind.
- Die Morphismen in $\mathcal{C}^*$ von einem Objekt $((A, (\varphi_k)_{k\in K})$ nach $(B, (\psi_k)_{k\in K})$ sind gegeben durch sämtliche Tripel $(A, f, B)$, wobei $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ ist mit $\varphi_k = \psi_k \circ f$ für alle $k \in K$.
- Die Komposition $\circ$ folgt der Regel $(B, g, C) \circ (A, f, B) := (A, g \circ f, C)$ mit der Komposition $g \circ f$ in $\mathcal{C}$.

Ist $\mathcal{C}$ zusammen mit $\mathsf{U}$ eine konkrete Kategorie, so ist auch $\mathcal{C}^*$ eine konkrete Kategorie mit $\mathsf{U}((A, (\varphi_i)_{i\in I}) = \mathsf{U}(A)$.

**UE 107** ► **Übungsaufgabe 2.3.2.7.** (V) Überzeugen Sie sich davon, dass es sich bei $\mathcal{C}^*$ aus Definition 2.3.2.6 tatsächlich wieder um eine Kategorie handelt, und dass direkte Produkte in Varietäten auch solche im kategorientheoretischen Sinn sind. ◄ **UE 107**

Unmittelbar einsichtig ist:

**Proposition 2.3.2.8.** *Seien $\mathfrak{A}_k$, $k \in K$, Algebren desselben Typs $\tau$ mit Trägermengen $A_k$, und sei $t = t(x_1, \ldots, x_n)$, $x_i \in X$, ein Term aus der Termalgebra $\mathfrak{T}(\tau, X)$. Weiters seien für alle $k \in K$ Elemente $a_{1,k}, \ldots, a_{n,k} \in A_k$ gegeben. Dann gilt in der Produktalgebra $\mathfrak{A} := \prod_{k\in K} \mathfrak{A}_k$:*

1. $t\left((a_{1,k})_{k\in K}, \ldots, (a_{n,k})_{k\in K}\right) = \left(t(a_{1,k}, \ldots, a_{n,k})\right)_{k\in K}$
2. *Gilt in allen $\mathfrak{A}_k$, $k \in K$ ein Gesetz der Form $t_1 \approx t_2$ mit $t_1, t_2 \in \mathfrak{T}(\tau, X)$, so auch in $\mathfrak{A}$.*

**UE 108** ► **Übungsaufgabe 2.3.2.9.** (V) Beweisen Sie Proposition 2.3.2.8. Anleitung für den ersten Teil: Induktion nach der Stufe des Terms $t$. ◄ **UE 108**

Daraus folgt unmittelbar:

**Folgerung 2.3.2.10.** *Ist $\mathcal{V}$ eine Varietät mit $\mathfrak{A}_k \in \mathcal{V}$ für alle $k \in K$, so liegt auch das direkte Produkt $\prod_{k\in K} \mathfrak{A}_k$ in $\mathcal{V}$.*

Insbesondere gilt: Direkte Produkte von Halbgruppen (bzw. Gruppen, Vektorräumen über dem selben Körper $K$, Ringen, Booleschen Algebren) sind wieder Halbgruppen (bzw. Gruppen, Vektorräume über $K$, Ringe, Boolesche Algebren).

Achtung! Das direkte Produkt von mindestens zwei Integritätsbereichen ist *nie* ein Integritätsbereich, denn $(0,1)\cdot(1,0)=(0,0)$. (Beachte: $0\neq 1$.)

**UE 109 ► Übungsaufgabe 2.3.2.11.** (F) Man kann Produkte „zusammenfassen“. Wenn die Indexmenge $I$ eine disjunkte Vereinigung $I=\dot{\bigcup}_{k\in K} J_k$ ist, dann ist das Produkt über $I$ kanonisch isomorph zu einem Produkt (über der Indexmenge $K$) von Produkten: **◄ UE 109**

$$\prod_{i\in I}\mathfrak{A}_i \cong \prod_{k\in K}\mathfrak{B}_k \quad \text{mit } \mathfrak{B}_k := \prod_{j\in J_k}\mathfrak{A}_j.$$

(Geben Sie den Isomorphismus explizit an.)

In direkten Produkten von Monoiden, Gruppen, Ringen etc. haben die ursprünglichen Komponenten isomorphe Kopien in den ihnen entsprechenden Komponenten des Produktes; für Gruppen $G$, $H$ gilt nämlich $G\cong G\times\{e_H\}\leq G\times H$. Man beachte aber, dass dies allgemein *nicht* gilt. Ein einfaches Beispiel, das diese Situation illustriert, erhält man in der Klasse aller Algebren vom Typ (1), d.h. mit einer einzigen einstelligen Operation. Dazu betrachten wir je eine zwei- und dreielementige Trägermenge $A=\{a_1,a_2\}$ und $B=\{b_1,b_2,b_3\}$ zusammen mit den zyklischen Permutationen $f_A: a_1\mapsto a_2\mapsto a_1$ und $f_B: b_1\mapsto b_2\mapsto b_3\mapsto b_1$. Die Operation $f_C$ auf dem direkten Produkt auf $C:=A\times B$ ist dann ebenfalls eine zyklische Permutation, diemals auf einer sechselementigen Menge. Dann hat $(C,f_C)$ nur die trivialen Unteralgebren, insbesondere also keine isomorphen Kopien von $(A,f_A)$ und $(B,f_B)$.

**UE 110 ► Übungsaufgabe 2.3.2.12.** (B) Führen Sie diese Überlegung in allen Details aus. **◄ UE 110**

### 2.3.3 Homomorphe Bilder, Kongruenzrelationen und Faktoralgebren

Inhalt in Kurzfassung: So wie dem Konzept der Teilmenge einer Menge in der Algebra das Konzept der Unteralgebra entspricht, dem des kartesischen Produktes das direkte Produkt, so entsprechen den Konzepten Äquivalenzrelation und Partition in der Algebra jene von Kongruenzrelation bzw. Faktoralgebra. Eine wichtige Rolle spielen dabei auch Homomorphismen, insbesondere der kanonische Homomorphismus. Dies kommt im Homomorphiesatz zum Ausdruck. Sämtliche Kongruenzrelationen einer gegebenen Algebra bilden einen vollständigen Verband (sehr ähnlich wie auch die Unteralgebren). Die klassischen Beispiele sind die Kongruenzen ganzer Zahlen modulo einer natürlichen Zahl mit den Restklassenringen als Faktoralgebren. Zwei Partitionen induzieren immer auch Faktoralgebren: die einelementige Partition und jene aus ausschließlich einelementigen Klassen. Entsprechend sind die zugehörigen Äquivalenzrelationen stets auch Kongruenzrelationen, die sogenannten trivialen. Eine Algebra, die außer den trivialen Kongruenzrelationen keine weiteren besitzt, heißt einfach.

In diesem Unterabschnitt geht es um drei Konzepte, die sich ineinander übersetzen lassen. Als Ausgangspunkt wählen wir strukturerhaltende Abbildungen zwischen Algebren, also Homomorphismen. Jede Abbildung induziert eine Äquivalenzrelation bzw. Partition auf ihrem Definitionsbereich, indem man Elemente mit demselben Bild als äquivalent auffasst. Handelt es sich zusätzlich um einen Homomorphismus, ist die Äquivalenzrelation automatisch verträglich mit den Operationen, was sie zu einer sogenannten Kongruenzrelation macht. Dadurch wird auf der Partition eine natürliche Definition von Operationen möglich, wodurch eine sogenannte Faktoralgebra entsteht. Die Situation wird durch den Homomorphiesatz beschrieben. Nun zur Ausführung dieses Programms im Detail.
Wie jede Abbildung induziert auch ein Homomorphismus $f\colon G \to H$ zwischen Gruppen oder auch irgendwelchen Algebren $G$ und $H$ desselben Typs in natürlicher Weise eine Äquivalenzrelation

$$x \sim y \;:\Leftrightarrow\; f(x) = f(y)$$

auf $G$. Diese Äquivalenzrelation nennt man auch den *Kern* von $f$, symbolisch $\ker f$. (In manchen Fällen, die später eine wichtige Rolle spielen werden – nämlich wenn es sich bei den beiden Algebren z.B. um Gruppen, Ringe, Moduln, Vektorräume oder Boolesche Algebren handelt – ist $\ker f$ durch eine einzige Klasse, nämlich das Urbild der 0, eindeutig bestimmt, weshalb man auch diese Klasse als Kern bezeichnet.) Diese Äquivalenzrelation $\ker f$ hat die besondere Eigenschaft, mit allen Operationen von $G$ in folgendem Sinn *verträglich* zu sein: wenn etwa + eine zweistellige Operation ist, dann gilt

$$\begin{aligned} g_1 \sim \tilde{g}_1 \text{ und } g_2 \sim \tilde{g}_2 &\Rightarrow f(g_1) = f(\tilde{g}_1) \text{ und } f(g_2) = f(\tilde{g}_2) \\ &\Rightarrow f(g_1 + g_2) = f(g_1) + f(g_2) = f(\tilde{g}_1) + f(\tilde{g}_2) = f(\tilde{g}_1 + \tilde{g}_2) \\ &\Rightarrow g_1 + g_2 \sim \tilde{g}_1 + \tilde{g}_2. \end{aligned}$$

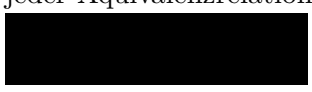
(Analoges gilt für alle Stelligkeiten.)
Im Homomorphiesatz 2.3.3.16 wird diese Überlegung noch mit Faktoralgebren in Verbindung gebracht. Dazu heben wir Relationen, die in der oben beschriebenen Weise mit Operationen verträglich sind, durch folgende Definition hervor.

**Definition 2.3.3.1.** Ist $f : A^n \to B$ eine Abbildung und $\sim$ eine Äquivalenzrelation auf $A$, so heißen $f$ und $\sim$ verträglich, wenn gilt: Für alle $a_1, \ldots, a_n, b_1, \ldots, b_n \in A$ mit $a_k \sim b_k$ für $k = 1, \ldots, n$, gilt $f(a_1, \ldots, a_n) \sim f(b_1, \ldots, b_n)$.
Sei nun $\mathfrak{A} = (A, (\omega_i)_{i\in I})$ eine Algebra vom Typ $(n_i)_{i\in I}$ und $\sim$ eine Äquivalenzrelation auf $A$. Dann heißt $\sim$ *Kongruenz(relation)* auf $\mathfrak{A}$, wenn $\sim$ mit allen $\omega_i$ *verträglich* ist, wenn also für alle $i \in I$ und $a_1, \ldots, a_{n_i}, b_1, \ldots, b_{n_i} \in A$ gilt:

$$a_1 \sim b_1, \ldots, a_{n_i} \sim b_{n_i} \Rightarrow \omega_i(a_1 \ldots a_{n_i}) \sim \omega_i(b_1 \ldots b_{n_i}).$$

Wir bezeichnen die Menge aller Kongruenzrelationen auf $\mathfrak{A}$ mit $\mathrm{Con}(\mathfrak{A})$.

Man beachte, dass für $n_i = 0$ die Verträglichkeitsbedingung in Definition 2.3.3.1 von jeder Äquivalenzrelation erfüllt wird (Reflexivität von $\sim$).



**UE 111** ► **Übungsaufgabe 2.3.3.2.** (B) Sei $A = \{1, 2, 3, 4, 5, 6, 7\}$ eine 7-elementige Menge und $\sim$ die durch die Partition $\{\{1, 2\}, \{3, 4, 5\}, \{6, 7\}\}$ induzierte Äquivalenzrelation. Geben Sie eine Algebra $\mathfrak{A} = (A, \omega_1, \ldots, \omega_k)$ an, sodass $\sim$ die einzige nichttriviale Kongruenzrelation (siehe Notation 2.3.3.13) dieser Algebra ist. (Hinweis: Man kommt mit unären Funktionen aus.) ◄ **UE 111**

**UE 112** ► **Übungsaufgabe 2.3.3.3.** (E) (Fortsetzung der vorigen Aufgabe.) ◄ **UE 112**

(1) Kommt man ganz allgemein immer mit unären Operationen aus? Genauer lautet die Frage: Angenommen, zu einer Familie $F$ von Äquivalenzrelationen auf einer Menge $A$ gibt es eine Menge von Operationen $\omega_i$ auf $A$ derart, dass die Elemente von $F$ genau die Kongruenzrelationen von $(A, (\omega_i)_{i\in I})$ sind. Gibt es dann immer eine Familie von einstelligen Operationen mit derselben Eigenschaft?

(2) Seien $A$, $\sim$, $\mathfrak{A}$ wie in Aufgabe 2.3.3.2. Sei $\mathcal{B}$ eine beliebige Algebra gleichen Typs, und sei $\varphi : \mathfrak{A}/\sim \to \mathfrak{B}$ ein beliebiger Homomorphismus. Zeigen Sie, dass $\varphi$ entweder konstant oder injektiv sein muss.

Das System $\mathrm{Con}(\mathfrak{A})$ aller Kongruenzrelationen einer Algebra $\mathfrak{A}$ verhält sich sehr ähnlich wie $\mathrm{Sub}(\mathfrak{A})$, jenes aller Unteralgebren. Entsprechend gehen wir analog vor wie in 2.3.1.7 und 2.3.1.9:

**Proposition 2.3.3.4.** *Seien $\mathfrak{A} = (A, \Omega)$ eine Algebra und $\sim_j$ für $j \in J$ Kongruenzrelationen. Dann ist auch der mengentheoretische Schnitt $\sim$ aller $\sim_j$, $j \in J$, (für $J = \emptyset$ ist für $\sim$ die Allrelation $\nabla_A = A \times A$ zu setzen) eine Kongruenzrelation auf $\mathfrak{A}$.*

Zusammen mit Korollar 2.1.2.19 folgt, wie bereits dort angekündigt:

**Folgerung 2.3.3.5.** *Ist $\mathfrak{A} = (A, (\omega_i)_{i\in I})$ eine Algebra, so ist $(\mathrm{Con}(\mathfrak{A}), \subseteq)$ ein vollständiger Verband (im ordnungstheoretischen Sinn) mit dem mengentheoretischen Durchschnitt als Infimum.*

**UE 113** ► **Übungsaufgabe 2.3.3.6.** (E) Sei $\mathfrak{A}$ eine Algebra mit Trägermenge $A$. ◄ **UE 113**

(1) Zeigen Sie $\mathrm{Con}(\mathfrak{A}) = \mathrm{Sub}(\mathfrak{A} \times \mathfrak{A}) \cap \mathrm{Eq}(A)$, wobei $\mathrm{Eq}(A)$ die Menge der Äquivalenzrelationen auf $A$ bezeichne.

(2) Finden Sie eine Algebra $\mathfrak{B}$ auf der Menge $B := A \times A$, sodass $\mathrm{Con}(\mathfrak{A}) = \mathrm{Sub}(\mathfrak{B})$.

**UE 114** ► **Übungsaufgabe 2.3.3.7.** (F+) Beweisen Sie Proposition 2.3.3.4 und Folgerung 2.3.3.5. ◄ **UE 114**

Auch das Supremum in $\mathrm{Con}(\mathfrak{A})$ lässt sich ähnlich beschreiben wie in $\mathrm{Sub}(\mathfrak{A})$: Ist $\mathfrak{A} = (A, (\omega_i)_{i\in I})$ eine Algebra und $M \subseteq A \times A$, so ist der Schnitt $\sim$ aller Kongruenzrelationen auf $\mathfrak{A}$, die $M$ als Teilmenge enthalten, die von $M$ erzeugte Kongruenzrelation auf $\mathfrak{A}$. Insbesondere gilt das, wenn $M$ die Vereinigung einer Familie von Kongruenzrelationen

$\sim_j$, $j \in J$, auf $\mathfrak{A}$ ist. Das ist die Beschreibung des Supremums im vollständigen Verband $(\mathrm{Con}(\mathfrak{A}), \subseteq)$ *von oben*. So wie bei Unteralgebren lässt sich $\sim$ auch durch einen Erzeugungsprozess *von unten* beschreiben:

**UE 115** ► **Übungsaufgabe 2.3.3.8.** (E) Sei $\mathcal{A}$ eine Algebra, $\theta_1, \theta_2 \in \mathrm{Con}(\mathcal{A})$. Wir definieren $\psi$ als die Menge aller Paare $(a, b) \in A \times A$, für die es ein $n \geq 0$ und eine Folge $(a_0, \ldots, a_n)$ gibt, sodass $a_0 = a$, $a_n = b$ gilt, sowie für alle $i \in \{0, \ldots, n-1\} : (a_i, a_{i+1}) \in \theta_1 \cup \theta_2$.
Zeigen Sie, dass $\psi$ eine Kongruenzrelation ist, und weiters, dass $\psi$ in $(\mathrm{Con}(\mathcal{A}), \subseteq)$ die kleinste obere Schranke von $\theta_1$ und $\theta_2$ ist.
(Wenn es Ihnen die Notation erleichtert, nehmen Sie an, dass $\mathcal{A}$ eine Algebra vom Typ $(2, 2, 0)$ ist.) ◄ **UE 115**

**UE 116** ► **Übungsaufgabe 2.3.3.9.** (E) Sei $\mathfrak{M}$ eine Algebra, sei $(\sim_j : j \in J)$ eine Familie von Kongruenzrelationen, und sei $M \subseteq A \times A$ die Vereinigung der Relationen $\sim_j$.
Beschreiben Sie das Supremum der Relationen $\sim_j$ (äquivalent die von $M$ erzeugte Kongruenzrelation — was heißt das?) im Kongruenzverband durch einen Erzeugungsprozess von unten, indem Sie definieren, wie man $M_{n+1}$ aus $M_n$ erhält derart, dass gilt: Setzt man $M_0 := M$ und nimmt man als $\sim$ die Vereinigung $\bigcup_{n \in \mathbb{N}} M_n$, so ist $\sim$ die von $M$ erzeugte Kongruenzrelation. ◄ **UE 116**

Die große Bedeutung von Kongruenzrelationen ergibt sich daraus, dass genau sie die Konstruktion von Faktoralgebren ermöglichen:

**Proposition 2.3.3.10.** *Sei $\mathfrak{A} = (A, (\omega_i)_{i \in I})$ eine Algebra vom Typ $\tau = (n_i)_{i \in I}$ und $\sim$ eine Äquivalenzrelation auf $\mathfrak{A}$. Dann sind folgende beiden Aussagen äquivalent:*

1. *Die Relation $\sim$ ist sogar eine Kongruenzrelation auf $\mathfrak{A}$.*
2. *Auf der Menge $A/_\sim$ aller Äquivalenzklassen bezüglich $\sim$ gibt es eine Familie von $n_i$-stelligen Operationen $\omega_i^*$ mit:*

$$\omega_i^*([a_1]_\sim, \ldots, [a_{n_i}]_\sim) = [\omega_i(a_1, \ldots, a_{n_i})]_\sim$$

*für alle $i \in I$ und $a_1, \ldots, a_{n_i} \in A$.*

**Definition 2.3.3.11.** Sind die beiden äquivalenten Bedingungen aus Proposition 2.3.3.10 erfüllt, so heißt die Algebra $\mathfrak{A}/_\sim := (A/_\sim, (\omega_i^*)_{i \in I})$ die *Faktoralgebra* von $\mathfrak{A}$ nach (oder bezüglich) der Kongruenzrelation $\sim$. (Oft schreiben wir nur $\omega_i$ statt $\omega_i^*$.)

**UE 117** ► **Übungsaufgabe 2.3.3.12.** (W) Beweisen Sie Proposition 2.3.3.10. Hinweis: Fasst man die zweite Bedingung als Definition der Operationen $\omega_i^*$ auf, so ist vor allem Wohldefiniertheit[55] zu zeigen. ◄ **UE 117**

[55] Was heißt es, dass eine Funktion wohldefiniert ist? Wenn wir eine Funktion $f$ auf einer Menge $X$

**Definition 2.3.3.13.** Auf einer beliebigen Algebra $\mathfrak{A}$ mit Trägermenge $A$ sind die *Gleichheitsrelation*[56] $\Delta_A = \Delta = \{(x, x) \mid x \in A\}$, genannt auch *Identität*, und die *Allrelation* $\nabla_A = \nabla = A \times A$ stets Kongruenzen, genannt die *trivialen Kongruenzen* auf $\mathfrak{A}$. $\mathfrak{A}/\Delta$ und $\mathfrak{A}/\nabla$ sind die *trivialen Faktoralgebren*. Eine Algebra, auf der es außer den trivialen Kongruenzen keine weiteren gibt, heißt *einfach*.

Es gilt $\mathfrak{A}/\Delta \cong \mathfrak{A}$ und $|\mathfrak{A}/\nabla| \leq 1$. Aus dem Homomorphiesatz 2.3.3.16 wird folgen, dass eine Algebra $\mathfrak{A}$ genau dann einfach ist, wenn sie nur *triviale* homomorphe Bilder hat (d. h., jeder Homomorphismus $h\colon A \to B$ ist entweder konstant oder injektiv).

**UE 118** ► **Übungsaufgabe 2.3.3.14.** Wie viele triviale Äquivalenzrelationen und wie viele nicht-triviale Äquivalenzrelationen gibt es ◄ **UE 118**

1. auf einer 3-elementigen Menge?
2. auf einer 2-elementigen Menge?
3. auf einer 1-elementigen Menge?
4. auf der leeren Menge?

Nachdem wir den Zusammenhang zwischen Kongruenzrelationen und Faktoralgebren geklärt haben, sei auch noch hervorgehoben, wie diese einen Homomorphismus induzieren:

---

durch eine Rechenvorschrift (etwa einen Term) $t$ definieren, also $f(x) := t(x)$ setzen, dann bedeutet das Wort „wohldefiniert“ nur soviel, dass die Rechenvorschrift $t$ für jede Eingabe $x$ im gewünschten Definitionbereich der Funktion tatsächlich ein Resultat $t(x)$ ausgibt. (Man muss etwa darauf achten, dass nicht durch 0 dividiert wird, dass eventuell auftretende Wurzeln wirklich definiert sind, etc.)
Wenn wir aber $f$ durch eine Formel

$$(*) \qquad f(H(s)) := t(s) \text{ für alle } s \in S$$

definieren, wobei $H$ eine bereits definierte Funktion ist, die $S$ surjektiv auf $X$ abbildet (zum Beispiel könnte $H(s) := [s]_\sim$ für eine vorgegebene Äquivalenzrelation $\sim$ sein), dann enthält diese „Definition“ implizit die Behauptung, dass es tatsächlich eine Funktion gibt, die jedem Element der Form $H(s)$ das Element $t(s)$ zuordnet. Wenn es nämlich Objekte $s_1$, $s_2$ gibt, die zwar $H(s_1) = H(s_2)$ aber $t(s_1) \neq t(s_2)$ erfüllen, dann ist die „Definition“ $(*)$ nicht sinnvoll, da sie nicht erklärt, ob der Wert $f$ an der Stelle $H(s_1)$ nun $t(s_1)$ oder $t(s_2)$ sein soll.

Mit anderen Worten: Durch die Definition $(*)$ wird zunächst nur die Relation $\{(H(s), t(s)) : s \in S\}$ definiert; zu überprüfen ist noch, ob diese Relation tatsächlich eine Funktion ist.

Notwendig und hinreichend für die Gültigkeit der genannten Behauptung ist die Implikation

$$(**) \qquad \forall s, s' \; (H(s) = H(s') \Rightarrow t(s) = t(s')).$$

Wenn wir also eine Funktion $f$ durch eine Vorschrift $(*)$ definieren, müssen wir uns immer erst vergewissern, dass $(**)$ erfüllt ist.

Bevor man überprüft hat, ob $f$ tatsächlich wohldefiniert ist, empfiehlt es sich, den Ausdruck $f(\cdots)$ nicht zu verwenden, da ja noch nicht klar ist, was damit überhaupt gemeint ist.

Ein Spezialfall liegt vor, wenn $H$ injektiv ist. Dann ist Wohldefiniertheit kein Problem, weil die Vorschrift $(*)$ in diesem Fall äquivalent zu folgender Forderung ist: $f(x) = t(H^{-1}(x))$ für alle $y$.

[56] Auch andere Notationen sind üblich. Statt $\Delta_A$ schreibt man auch $id_A$ oder $=_A$ oder $\iota_A$, statt $\nabla_A$ auch $\omega_A$ oder einfach $A^2$.

**Proposition 2.3.3.15.** *Sei $\mathfrak{A} = (A, (\omega_i)_{i\in I})$ eine Algebra und $\sim$ eine Kongruenzrelation auf $\mathfrak{A}$. Dann ist die Abbildung*

$$\nu : \begin{cases} A \to A/_\sim \\ a \mapsto [a]_\sim \end{cases}$$

*ein surjektiver Homomorphismus von $\mathfrak{A}$ auf die Faktoralgebra $\mathfrak{A}/_\sim$, der so genannte* natürliche *oder auch* kanonische Homomorphismus*.*

*Beweis.* Ist $\tau = (n_i)_{i\in I}$ der Typ von $\mathfrak{A}$, so folgt die Behauptung aus (Notation wie in 2.3.3.10)

$$\nu(\omega_i(a_1, \ldots, a_{n_i})) = [\omega_i(a_1, \ldots, a_{n_i})]_\sim = \omega_i^*([a_1]_\sim, \ldots, [a_{n_i}]_\sim) = \omega_i^*(\nu(a_1), \ldots, \nu(a_{n_i})).$$

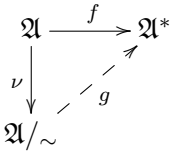
Die Surjektivität folgt daraus, dass jedes Element $\gamma$ von $\mathfrak{A}/_\sim$ per definitionem die Gestalt $\gamma = [a]_\sim = \nu(a)$ für ein $a \in A$ hat. □

Gewissermaßen als Umkehrung kommen wir nun zum bereits angekündigten Homomorphiesatz, der die Beziehung zwischen Homomorphismen, Kongruenzrelationen und Faktoralgebren zusammenfasst:

**Satz 2.3.3.16** (Homomorphiesatz)**.** *Seien $\mathfrak{A} = (A, (\omega_i)_{i\in I})$ und $\mathfrak{A}^* = (A^*, (\omega_i^*)_{i\in I})$ Algebren vom selben Typ $(n_i)_{i\in I}$ und $f\colon A \to A^*$ ein Homomorphismus. Dann ist der sogenannte* Kern

$$\sim := \{(x, y) \mid f(x) = f(y)\}$$

*von $f$ eine Kongruenz auf $\mathfrak{A}$, und es gibt genau eine Abbildung $g$ von $\mathfrak{A}/_\sim$ nach $\mathfrak{A}^*$ mit $f = g \circ \nu$ ($\nu$ ist die natürliche Abbildung $a \mapsto [a]_\sim$). Dieses $g$ ist ein injektiver Homomorphismus $g\colon \mathfrak{A}/_\sim \to \mathfrak{A}^*$ und genau dann sogar ein Isomorphismus, wenn $f$ surjektiv ist.*




*Beweis.* Wir beweisen zunächst jene Behauptungen, die für beliebige Abbildungen unabhängig von einer zugrunde liegenden algebraischen Struktur gelten: Dass die Relation $\sim$ eine Äquivalenzrelation ist, gilt für beliebige Abbildungen und überträgt sich unmittelbar von den entsprechenden Eigenschaften der Gleichheitsrelation (Reflexivität, Symmetrie und Transitivität). Wegen der Bedingung $f = g \circ \nu$ ist $g([a]_\sim) := f(a)$ die einzig mögliche Definition von $g$ mit den geforderten Eigenschaften. Aus $[a]_\sim = [b]_\sim$ folgt nach Definition von $\sim$ die Gleichheit $f(a) = f(b)$, weshalb $g$ durch diese Festlegung tatsächlich wohldefiniert ist. Weil die kanonische Abbildung $\nu : A \to A/_\sim$ surjektiv ist, stimmen die Bilder von $g$ und $g \circ \nu = f$ überein. Somit ist $g$ surjektiv genau dann, wenn $f$ surjektiv ist.
Es verbleibt der Beweis der algebraischen Aussagen des Homomorphiesatzes, nämlich, dass $\sim$ mit den Operationen verträglich, also eine Kongruenzrelation, und dass $g$ ein

Homomorphismus ist. Für $n_i = 0$ ist die Verträglichkeit von $\omega_i$ mit $\sim$ trivial und mit $g$ aus der Beziehung $g(\omega_i) = g([\omega_i]_\sim) = f(\omega_i) = \omega_i^*$ ersichtlich. Sei daher ab nun $n_i > 0$. Wir haben:

$$\left.\begin{array}{c} a_1 \sim b_1 \\ \vdots \\ a_{n_i} \sim b_{n_i} \end{array}\right\} \Rightarrow \left\{\begin{array}{c} f(a_1) = f(b_1) \\ \vdots \\ f(a_{n_i}) = f(b_{n_i}) \end{array}\right\} \Rightarrow \omega_i^*(f(a_1), \ldots, f(a_{n_i})) = \omega_i^*(f(b_1), \ldots, f(b_{n_i}))$$

Weil $f$ ein Homomorphismus ist, folgt daraus $f(\omega_i(a_1, \ldots, a_{n_i})) = f(\omega_i(b_1, \ldots, b_{n_i}))$ und somit

$$\omega_i(a_1, \ldots, a_{n_i}) \sim \omega_i(b_1, \ldots, b_{n_i}),$$

d.h. die Verträglichkeit von $\sim$ mit $\omega_i$. Die Verträglichkeit von $\sim$ mit $g$ (Homomorphieeigenschaft von $g$) liest man aus

$$\begin{aligned} g(\,\omega_i([a_1]_\sim, \ldots, [a_{n_i}]_\sim)\,) &= g(\,[\omega_i(a_1, \ldots, a_{n_i})]_\sim\,) = f(\omega_i(a_1, \ldots, a_{n_i})) \\ &= \omega_i^*(\,f(a_1), \ldots, f(a_{n_i})\,) = \omega_i^*(\,g([a_1]_\sim), \ldots, g([a_{n_i}]_\sim)\,) \end{aligned}$$

ab. □

**Folgerung 2.3.3.17.** *Für die Unteralgebra $(f(A), (\omega_i^*)_{i\in I})$ (im surjektiven Fall also $\mathfrak{A}^*$ selbst) von $\mathfrak{A}^*$ gilt $(f(A), (\omega_i^*)_{i\in I}) \cong \mathfrak{A}/_\sim$, also ist jedes homomorphe Bild einer Algebra isomorph zu einer Faktoralgebra.*

**Anmerkung 2.3.3.18.** Im Homomorphiesatz 2.3.3.16 beachte man insbesondere den Fall, dass $I = \emptyset$ leer ist, wo die Aussage in den entsprechenden Sachverhalt betreffend beliebige Abbildungen übergeht. Diese einfachere Aussage war Gegenstand des ersten Teils im Beweis.

**UE 119** ► **Übungsaufgabe 2.3.3.19.** Mit $C_2$ bezeichnen wir die (bis auf Isomorphie einzige) 2-elementige Gruppe. Finden Sie alle Kongruenzrelationen auf der 4-elementigen Gruppe Gruppe $C_2 \times C_2$; geben Sie für jede dieser Kongruenzrelationen $\theta$ eine surjektiven Homomorphismus an, der $\theta$ induziert. ◄ **UE 119**

Das klassische Beispiel einer Kongruenzrelation ist Kongruenz modulo $m$, symbolisch $\equiv_m$, auf $\mathbb{Z}$, definiert durch: $a \equiv_m b$ genau dann, wenn $m$ ein Teiler von $b - a$ ist, symbolisch $m|(b-a)$, wenn es also ein $d \in \mathbb{Z}$ mit $b - a = dm$ gibt. Diese Relation ist nicht nur eine Äquivalenzrelation, sondern auch verträglich mit Addition, Multiplikation und additiver Inversenbildung auf $\mathbb{Z}$ und folglich eine Kongruenzrelation auf dem (kommutativen) Ring $\mathbb{Z}$ (mit 1). Das ermöglicht die Konstruktion der Faktoralgebra $\mathbb{Z}_m := \mathbb{Z}/_{\equiv_m}$, des sogenannten *Restklassenrings* modulo $m$. In Abschnitt 3.4 über Ringe werden wir darauf zurückkommen.
Wie wir aus 2.3.1.3 und 2.3.2.10 wissen, vererben sich Gesetze, wie sie für die Definition von Varietäten verwendet werden, auf Unteralgebren und auf direkte Produkte. Analoges gilt für homomorphe Bilder und Faktoralgebren. Im Wesentlichen liegt das an:

**Proposition 2.3.3.20.** *Seien $\mathfrak{A} = (A, (\omega_{i,\mathfrak{A}})_{i\in I})$ und $\mathfrak{B} = (B, (\omega_{i,\mathfrak{B}})_{i\in I})$ Algebren desselben Typs $\tau = (n_i)_{i\in I}$ und $\varphi\colon \mathfrak{A} \to \mathfrak{B}$ ein Homomorphismus. Dann gilt für jeden Term $t = t(x_1, \ldots, x_n)$ und alle $a_1, \ldots, a_n \in A$ die Gleichung*

$$\varphi(t(a_1, \ldots, a_n)) = t(\varphi(a_1), \ldots, \varphi(a_n)).$$

Hieraus folgt fast unmittelbar:

**Folgerung 2.3.3.21.** *Sei $\mathcal{V}$ eine Varietät mit $\mathfrak{A} \in \mathcal{V}$.*

1. *Ist $\mathfrak{B}$ eine Algebra desselben Typs wie $\mathfrak{A}$ und $\varphi\colon \mathfrak{A} \to \mathfrak{B}$ ein surjektiver Homomorphismus, dann folgt $\mathfrak{B} \in \mathcal{V}$.*
2. *Ist $\sim$ eine Kongruenzrelation auf $\mathfrak{A}$, dann folgt $\mathfrak{A}/_\sim \in \mathcal{V}$.*

UE 120 ► **Übungsaufgabe 2.3.3.22.** (W) Beweisen Sie Proposition 2.3.3.20 (Induktion nach der Stufe von $t$) und folgern Sie daraus 2.3.3.21. Hinweis: Verwenden Sie den kanonischen Homomorphismus um die zweite Behauptung von 2.3.3.21 aus der ersten zu gewinnen. ◄ UE 120

Insbesondere sind folgende Klassen abgeschlossen bezüglich homomorpher Bilder und der Bildung von Faktoralgebren: Halbgruppen, (abelsche) Gruppen, Vektorräume über einem festen Körper, (kommutative) Ringe (mit 1), Verbände und Boolesche Algebren. Nicht gilt das jedoch für Integritätsbereiche und Körper:
Jede Algebra hat, faktorisiert nach der Allrelation, eine einelementige Algebra als Faktoralgebra. Diese ist definitionsgemäß weder Körper noch Integritätsbereich, also gilt 2.3.3.21 nicht, wenn man statt einer Varietät $\mathcal{V}$ die Klasse der Körper oder die Klasse der Integritätsbereiche nimmt. Ein nicht einelementiges Beispiel liefert der Integritätsbereich $\mathbb{Z}$ faktorisiert nach $\equiv_m$ für eine zusammengesetzte Zahl (d.h. Nicht-Primzahl) $m$. Denn auch dann ist, wie wir später noch ausführlicher besprechen werden, der Restklassenring $\mathbb{Z}_m = \mathbb{Z}/_{\equiv_m}$ kein Integritätsbereich.

## 2.3.4 Direkte Limiten

Inhalt in Kurzfassung: Zu jeder Familie von Mengen gibt es die Vereinigungsmenge. Hat man es jedoch mit algebraischen Strukturen zu tun, so bildet die Vereinigung in der Regel keine natürliche algebraische Struktur. Sehr wohl lässt sich eine solche aber unter zusätzlichen Voraussetzungen definieren, zum Beispiel in Varietäten, sofern die Algebren in einer verträglichen Weise ineinander eingebettet sind. Die resultierende Struktur zeichnet sich durch eine universelle Eigenschaft aus.

**Beispiel 2.3.4.1.** Sei $(\mathcal{R}_n : n \in \mathbb{N})$ eine aufsteigende Familie von Ringen mit Einselement. Das heißt:

- Für $n \in \mathbb{N}$ ist $\mathcal{R}_n = (R_n, +_n, 0_n, -_n, \cdot_n, 1_n)$ ein Ring.

- Für alle $n$ ist $\mathcal{R}_n$ Unterring von $\mathcal{R}_{n+1}$; es gilt also $0_n = 0_{n+1}$, $1_n = 1_{n+1}$, und die Operationen $+_n$, $-_n$, $\cdot_n$ sind die Einschränkungen der Operationen $+_{n+1}$, $-_{n+1}$, $\cdot_{n+1}$ auf $\mathcal{R}_n$ bzw. auf $\mathcal{R}_n \times \mathcal{R}_n$.

(Mit anderen Worten: Jede Identitätsabbildung $\mathrm{id}_n \colon R_n \to R_{n+1}$ ist ein Homomorphismus von Ringen mit 1.)
Dann gibt es genau einen Ring $\mathcal{R}_\infty$ mit Eins mit folgenden Eigenschaften:
Alle $\mathcal{R}_n$ sind Unterringe mit 1 von $\mathcal{R}$, und für jeden Ring $\mathcal{S}$ mit Eins und jede Familie von einander fortsetzenden Homomorphismen $\varphi_n \colon \mathcal{R}_n \to \mathcal{S}$ von Ringen mit 1 gibt es genau einen Homomorphismus $\varphi \colon \mathcal{R} \to \mathcal{S}$ von Ringen mit 1, der alle $\varphi_n$ fortsetzt.

*Beweis.* Auf der Menge $R_\infty := \bigcup_n R_n$ lassen sich in natürlicher Weise Ringoperationen definieren. Wenn etwa $x \in R_n$, $y \in R_m$ mit $k := \max(m, n)$ ist, können wir $x +_R y := x +_k y$ setzen, ähnlich für die anderen Operationen.
Man überprüft leicht, dass diese Operationen wohldefiniert sind und dass die Struktur $\mathcal{R}_\infty = (R_\infty, +_\infty, 0_\infty, -_\infty, \cdot_\infty, 1_\infty)$ dadurch zu einen Ring mit Einselement wird. Die Eindeutigkeitsaussage ist ebenfalls leicht zu verifizieren. □

Ein analoger Satz gilt auch für andere algebraische Strukturen:

**Satz 2.3.4.2.** *Sei $\mathcal{K}$ eine Varietät (siehe Definition 2.1.8.6) von Algebren, oder die Klasse aller Körper. Sei $(\mathfrak{A}_n)_{n\in\mathbb{N}}$ eine Familie von Algebren in $\mathcal{K}$, wobei für alle $n$ die Unteralgebrenbeziehung $\mathfrak{A}_n \leq \mathfrak{A}_{n+1}$ gilt. Dann gibt es eine eindeutig bestimmte Algebra $\mathfrak{A}_\infty \in \mathcal{K}$ mit folgenden Eigenschaften:*

- *Für alle $n$ gilt: $\mathfrak{A}_n$ ist eine Unteralgebra von $\mathfrak{A}_\infty$.*
- *$A_\infty$, die Trägermenge von $\mathfrak{A}_\infty$, ist die Vereinigung $A_\infty = \bigcup_n A_n$.*
- *(Daher:) Für jede Algebra $\mathfrak{B} \in \mathcal{K}$ und jede Familie $(\varphi_n : n \in \mathbb{N})$ von einander fortsetzenden Homomorphismen $\varphi_n \colon \mathfrak{A}_n \to \mathfrak{B}$ gibt es genau einen Homomorphismus $\varphi \colon \mathfrak{A}_\infty \to \mathfrak{B}$, der alle $\varphi_n$ fortsetzt.*

Eine Verallgemeinerung dieser Konstruktion werden wir in Definition 7.1.5.3 kennen lernen.

**UE 121** ► **Übungsaufgabe 2.3.4.3.** (V) Beweisen Sie Satz 2.3.4.2. Überlegen Sie insbesondere, warum die von Ihnen gefundenen Operationen wohldefiniert sind, und warum $\mathfrak{A}_\infty \in \mathcal{K}$ gilt. ◄ **UE 121**

Die folgende Darstellung von $\mathcal{A}_\infty$ als homomorphes Bild einer Unteralgebra von $\prod_n \mathcal{A}_n$ wird in Satz 2.3.4.5 zu einer Verallgemeinerung dieser Konstruktion führen.

**Satz 2.3.4.4.** *Sei $(\mathfrak{A}_i)_{i\in\mathbb{N}}$ eine aufsteigende Familie von nichtleeren[57] Algebren mit Vereinigung $\mathfrak{A}_\infty$ wie in Satz 2.3.4.2. Dann ist $\mathfrak{A}_\infty$ homomorphes Bild einer geeigneten Unteralgebra von $\prod_{i\in\mathbb{N}} \mathfrak{A}_i$. (Insbesondere vererben sich alle Gesetze, die in allen $\mathfrak{A}_i$ gelten, auf $\mathfrak{A}_\infty$.)*

[57] Der Fall $\forall i : A_i = \emptyset$ ist trivial, und im Fall $\exists j : A_j = \emptyset \ \wedge \ \exists j : A_j \neq \emptyset$ muss man beim Produkt der $A_i$ die leeren Faktoren weglassen.

*Beweis.* Sei $B$ als die Menge aller Tupel $\bar{a} = (a_i)_{i\in\mathbb{N}}$ definiert, die $\exists i_0 \in \mathbb{N}\ \forall i \geq i_0 : a_i = a_{i_0}$ erfüllen. Wir definieren $\lim \bar{a} = \lim(a_i)_{i\in\mathbb{N}} := a_{i_0}$. Wenn wir $A$ als topologischen Raum mit der diskreten Topologie betrachten, dann ist $\lim \bar{a}$ tatsächlich der Grenzwert der Folge $\bar{a}$ in diesem Raum. Es ist klar, dass alle Operationen stetig sind; wenn etwa $+$ eine zweistellige Operation ist, dann gilt $\lim(\bar{a} + \bar{b}) = \lim \bar{a} + \lim \bar{b}$.
Auf $B$ definieren wir eine Äquivalenzrelation $\sim$ durch: $(a_i)_{i\in\mathbb{N}} \sim (b_i)_{i\in\mathbb{N}}$ genau dann, wenn es ein $i_1 \in \mathbb{N}$ gibt mit $\forall i \geq i_1 : a_i = b_i$), wenn also die beiden Tupel „schließlich“ übereinstimmen. Anders formuliert gilt $(a_i)_{i\in\mathbb{N}} \sim (b_i)_{i\in\mathbb{N}}$ genau dann, wenn $\lim \bar{a} = \lim \bar{b}$.
Sei $C := B/\!\sim$. Dann gilt:

- $B$ ist Trägermenge einer Unteralgebra $\mathfrak{B}$ von $\prod_{i\in\mathbb{N}} \mathfrak{A}_i$.
  [Wenn $\omega$ eine $k$-stellige Operation ist, und $\bar{b}_1, \ldots, \bar{b}_k \in B$, dann wollen wir zeigen, dass auch $\bar{c} := \omega(\bar{b}_1, \ldots, \bar{b}_k)$ in $B$ liegt.
  Für jedes $j = 1, \ldots, k$ finden wir $i_j \in \mathbb{N}$ sodass die Folge (oder das $\mathbb{N}$-Tupel) $\bar{b}_j$ ab dem $i_j$-ten Eintrag konstant mit Wert $b(j) = \lim \bar{b}_j$ ist. Wenn wir $i^* := \max(i_1, \ldots, i_k)$ setzen, dann gilt für $j = 1, \ldots, k$, dass alle Folgen $\bar{b}_1, \ldots, \bar{b}_k$ ab dem $i^*$-ten Eintrag gemeinsam konstant sind, d.h. $(b_j)_{i^*} = (b_j)_{i^*+1} = \cdots = b(j)$. Daher ist auch $\bar{c}$ ab dem $i^*$-ten Eintrag konstant, nämlich mit Wert $\omega(b(1), \ldots, b(k))$. Somit liegt $\bar{c}$ in $B$.]
- $\sim$ ist Kongruenzrelation auf $B$, also trägt auch $C$ eine algebraische Struktur vom Typ $\tau$, wird also zu einer Faktoralgebra $\mathfrak{C}$.
  [Das folgt aus der oben bereits erwähnten Stetigkeit der Operationen bezüglich der diskreten Topologie auf $A$, die man leicht nachrechnet.]
- $\mathfrak{C} \simeq \mathfrak{A}_\infty$.
  [Man prüft nach, dass die Abbildung $\lim\colon C \to A_\infty$ ein Isomorphismus ist. Um die Surjektivität zu zeigen, muss man für jedes $a \in A_\infty$ eine Folge $\bar{b}$ mit Grenzwert $a$ finden. Wenn $a \in A_i$ gilt, dann können wir eine Folge $\bar{b} = (b_0, b_1, \ldots)$ finden, deren Werte $b_0 \in A_0$, …, $b_{i-1} \in A_{i-1}$ beliebig sind, und die ab $i$ den konstanten Wert $b_i = b_{i+1} = \cdots = a$ hat.]

□

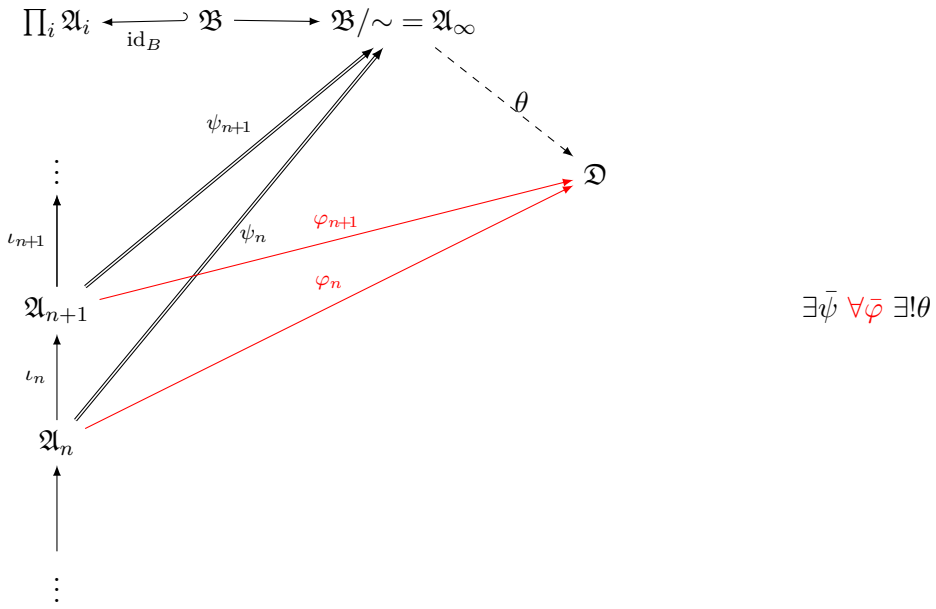
Man überlegt leicht, dass die Sätze 2.3.4.2 und 2.3.4.4 auch dann gelten, wenn man die Indexmenge $\mathbb{N}$ durch eine beliebige lineare[58] Ordnung $L$ ersetzt. In den Beweisen muss man nur überall $\mathbb{N}$ durch $L$ ersetzen. In $L$ gilt ebenso wie in $\mathbb{N}$, dass jede endliche nichtleere Teilmenge eine obere Schranke hat.
In Satz 2.3.4.2 haben wir eine aufsteigende Familie von Algebren betrachtet; wenn man statt $\mathcal{R}_n \leq \mathcal{R}_{n+1}$ verlangt, dass es einen injektiven Homomorphismus $\iota_n : \mathcal{R}_n \to \mathcal{R}_{n+1}$ gibt, so erhält man eine ganz ähnliche Situation, die man durch Umbenennung (oder Identifikation von Elementen mit ihren $\iota$-Bildern) auf Satz 2.3.4.2 zurückführen kann.
Die folgenden Konstruktion ist eine interessante Verallgemeinerung, wo man nicht mehr die Injektivität der Abbildungen $\iota_n$ verlangt. Im Spezialfall $\mathcal{R}_n \leq \mathcal{R}_{n+1}$ und $\iota_n = \mathrm{id}_{A_n}$ ergibt sich einfach Satz 2.3.4.2.

[58] Noch allgemeiner: eine nach oben gerichtete Menge

**Satz 2.3.4.5.** *Sei $\mathcal{K}$ eine Varietät (siehe Definition 2.1.8.6) von Algebren, oder die Klasse aller Körper. Sei $(\mathfrak{A}_n)_{n\in\mathbb{N}}$ eine Familie von Algebren in $\mathcal{K}$, und seien die Abbildungen $\iota_n\colon \mathfrak{A}_n \to \mathfrak{A}_{n+1}$ Homomorphismen.*
*Dann gibt es eine Algebra $\mathfrak{A}_\infty \in \mathcal{K}$ sowie Abbildungen $\psi_n$ mit folgenden Eigenschaften:*

- *Für alle $n$ ist $\psi_n\colon \mathfrak{A}_n \to \mathfrak{A}_\infty$ ein Homomorphismus.*
- *Für alle $n$ ist $\psi_n = \psi_{n+1} \circ \iota_n$.*
- *Für jede Algebra $\mathfrak{D} \in \mathcal{K}$ und jede Familie $(\varphi_n : n \in \mathbb{N})$ von Homomorphismen $\varphi_n\colon \mathfrak{A}_n \to \mathfrak{D}$, die $\forall n : \varphi_n = \varphi_{n+1} \circ \iota_n$ erfüllen, gibt es genau einen Homomorphismus $\theta\colon \mathfrak{A}_\infty \to \mathfrak{D}$, der $\forall n : \theta \circ \psi_n = \varphi_n$ erfüllt.*

*Überdies kann man die Algebra $\mathfrak{A}_\infty$ als homomorphes Bild einer Unteralgebra von $\prod_n \mathfrak{A}_n$ erhalten.*




*Beweis.* Der Beweis entsteht durch eine geringfügige Modifikation des Beweises von Satz 2.3.4.2.
Sei $B$ als die Menge aller Tupel $\bar{a} = (a_i)_{i\in\mathbb{N}}$ definiert, die $\exists i_0 \in \mathbb{N}\ \forall i \geq i_0 : a_{i+1} = \iota_i(a_i)$ erfüllen.
Auf $B$ definieren wir wiederum eine Äquivalenzrelation $\sim$ durch $\bar{a} \sim \bar{b}$ genau dann, wenn es ein $i_1 \in \mathbb{N}$ gibt mit $\forall i \geq i_1 : a_i = b_i$, wenn also die beiden Tupel „schließlich“ übereinstimmen.
Sei $A_\infty := B/\sim$. Dann gilt:

- $B$ ist Trägermenge einer Unteralgebra $\mathfrak{B}$ von $\prod_{i\in\mathbb{N}} \mathfrak{A}_i$.
- $\sim$ ist eine Kongruenzrelation auf $\mathfrak{B}$, also trägt auch $A_\infty$ eine algebraische Struktur, wird also zu einer Faktoralgebra $\mathfrak{A}_\infty$.

- Wir definieren $\psi_n : \mathfrak{A}_n \to \mathfrak{A}_\infty$ in natürlicher Weise: Für jedes $a \in \mathfrak{A}_n$ wählen wir eine Folge $\bar{b} = (b_i)_{i\in\mathbb{N}}$ in $\prod_i \mathfrak{A}_i$ mit den folgenden Eigenschaften:
  - Für $i < n$ sei $b_i \in R_i$ beliebig.
  - $b_n = a$.
  - $b_{n+1} = \iota_n(b_n)$, und weiter $b_{m+1} = \iota_m(b_m)$ für alle $m \geq n$.

  Dann ist $\bar{b}$ in der Algebra $B$. (Durch diese Eigenschaften ist zwar $\bar{b}$ nicht eindeutig bestimmt, wohl aber die $\sim$-Äquivalenzklasse von $\bar{b}$.)

  Sei $\psi_n(a)$ die $\sim$-Äquivalenzklasse von $\bar{b}$.
- $A_\infty$ ist die Vereinigung der Bilder $\psi_n(A_n)$: Für $[(b_i)_{i\in\mathbb{N}}] \in A_\infty$ gibt es $i_0 \in \mathbb{N}$ mit $\forall i \geq i_0 : b_{i+1} = \iota_i(b_i)$. Dann gilt $[(b_i)_{i\in\mathbb{N}}] = \psi_{i_0}(b_{i_0})$ und wir erhalten tatsächlich $A_\infty = \bigcup_{n\in\mathbb{N}} \psi_n(A_n)$.
- Wenn $\mathfrak{D} \in \mathcal{K}$, und $(\varphi_n : n \in \mathbb{N})$ Homomorphismen $\varphi_n \colon \mathfrak{A}_n \to \mathfrak{D}$ sind, die $\forall n : \varphi_n = \varphi_{n+1} \circ \iota_n$ erfüllen, dann gibt es genau einen Homomorphismus $\theta \colon \mathfrak{A}_\infty \to \mathfrak{D}$, der $\forall n : \varphi \circ \psi_n = \varphi_n$ erfüllt:

  Ist $[(b_i)_{i\in\mathbb{N}}]_\sim \in A_\infty$ gegeben, so gibt es $i_0 \in \mathbb{N}$ mit $\forall i \geq i_0 : b_{i+1} = \iota_i(b_i)$. Dann gilt für alle $i \geq i_0$, dass $\varphi_i(b_i) = \varphi_{i+1}(\iota_i(b_i)) = \varphi_{i+1}(b_{i+1})$. Wir definieren $\theta([(b_i)_{i\in\mathbb{N}}]_\sim) := \varphi_i(b_i)$ für irgendein $i \geq i_0$ (nach dem gerade Gezeigten stimmen diese Werte für alle $i \geq i_0$ überein) und bemerken, dass die Definition wohldefiniert ist, d.h. nicht vom gewählten $\sim$-Repräsentanten abhängt. Man rechnet leicht nach, dass $\theta$ ein Homomorphismus ist, der $\forall n : \theta \circ \psi_n = \varphi_n$ erfüllt.

  Wegen $\forall n : \theta \circ \psi_n = \varphi_n$ ist die Einschränkung von $\theta$ auf $\psi_n(A_n)$ bereits festgelegt; aus $A_\infty = \bigcup_{n\in\mathbb{N}} \psi_n(A_n)$ folgt damit die Eindeutigkeit von $\theta$ auf ganz $A_\infty$.

□

### 2.3.5 Triviale und nichttriviale Varietäten

Inhalt in Kurzfassung: Für Varietäten gilt eine bemerkenswerte Dichotomie. Und zwar enthält eine Varietät entweder nur höchstens einelementige Algebren und eventuell die leere Algebra (trivialer Fall) oder Algebren beliebig großer Kardinalität.

Gilt in einer Varietät $\mathcal{V}$ eines Typs $\tau$ das Gesetz $x \approx y$, so müssen in jeder Algebra $\mathfrak{A} \in \mathcal{V}$ je zwei Elemente gleich sein. Folglich enthält $\mathcal{V}$ nur einelementige Algebren (von denen je zwei zueinander isomorph sind) und, wenn im Typ $\tau$ keine 0-stelligen Operationen vorkommen, die leere Algebra. In diesem Fall heißt $\mathcal{V}$ die *triviale Varietät* (oder: ausgeartete Varietät) (zum Typ $\tau$). Gilt das Gesetz $x \approx y$ in $\mathcal{V}$ hingegen nicht, so gibt es zumindest ein $\mathfrak{A} \in \mathcal{V}$ mit mehr als einem Element. Wegen Proposition 4.1.1.2 liegen dann auch alle Potenzen $\mathfrak{A}^M = \prod_{m\in M} \mathfrak{A}_m$ (wobei für jedes $m \in M$ die Algebra $\mathfrak{A}_m$ gleich der Algebra $\mathfrak{A}$ ist) in $\mathcal{V}$, also Algebren von beliebig großer Kardinalität. Also:

**Proposition 2.3.5.1.** *Für eine Varietät $\mathcal{V}$ zum Typ $\tau = (n_i)_{i\in I}$ gilt genau einer der folgenden beiden Fälle:*

1. *$\mathcal{V}$ ist die triviale Varietät und enthält ausschließlich einelementige Algebren und, falls $n_i \neq 0$ für alle $i \in I$, die leere Algebra.*
2. *$\mathcal{V}$ ist nichttrivial und enthält zu jeder vorgegebenen Kardinalität $\kappa$ eine Algebra mit einer Trägermenge $A$, die $|A| \geq \kappa$ erfüllt.*

Gelegentlich werden wir „ohne Beschränkung der Allgemeinheit“ triviale Varietäten von unseren Überlegungen ausschließen, oder genauer: nur nichttriviale Varietäten betrachten, und den (meist uninteressanten) Fall der trivialen Varietäten dem Leser[59] überlassen.

### 2.3.6 Isomorphiesätze

Inhalt in Kurzfassung: In den beiden Isomorphiesätzen geht es vor allem darum, dass verschiedene Konstruktionen zu isomorphen Strukturen führen. Im ersten wird die Reihenfolge der Bildung einer Unter- und einer Faktoralgebra vertauscht; im zweiten werden zwei Faktorisierungen durch eine einzige ersetzt. Der zweite besagt darüber hinaus die Isomorphie des Kongruenzverbandes der ersten Faktoralgebra mit einem Teilintervall des Kongruenzverbandes der ursprünglichen Algebra.

Die beiden Sätze, die nun behandelt werden, machen Aussagen darüber, wie sich gewisse der bisher behandelten Konstruktionen miteinander vertragen. Der sogenannte erste Isomorphiesatz geht von einer Algebra mit Unteralgebra und Kongruenzrelation aus und besagt im Wesentlichen, dass man isomorphe Strukturen erhält, egal in welcher Reihenfolge man die Übergänge zu Unter- bzw. Faktoralgebra durchführt. Der sogenannte zweite Isomorphiesatz besagt grob gesagt, dass man die Iteration zweier Faktorisierungen durch eine einzige ersetzen kann.

**Lemma 2.3.6.1.** *Sei $\mathfrak{A}$ eine Algebra, $\theta$ eine Kongruenzrelation und $\mathfrak{B}$ eine Unteralgebra von $\mathfrak{A}$. Dann ist $[B]_\theta := \bigcup_{b\in B}[b]_\theta$ unter den Operationen von $\mathfrak{A}$ abgeschlossen, also eine Unteralgebra von $\mathfrak{A}$.*

*Beweis.* Sei $\omega$ eine $n$-stellige Operation von $\mathfrak{A}$ und seien $a_1, \ldots, a_n \in [B]_\theta$. Letzteres bedeutet gerade, dass es $b_1, \ldots, b_n \in B$ gibt mit $a_i \; \theta \; b_i$. Es folgt $\omega(a_1 \ldots a_n) \; \theta \; \omega(b_1 \ldots b_n)$. Weil $\mathfrak{B}$ eine Unteralgebra ist, gilt $\omega(b_1 \ldots b_n) \in B$ und daher $\omega(a_1 \ldots a_n) \in [B]_\theta$. □

**Notation 2.3.6.2.** Sei $\theta$ eine Äquivalenzrelation auf einer Menge $A \supseteq B$. Dann ist $\theta{\restriction_B} := \theta \cap (B \times B)$ eine Äquivalenzrelation auf $B$. Um die Notation zu vereinfachen, schreiben wir in so einem Fall oft auch $B/\theta$ statt $B/(\theta{\restriction_B})$.

**Satz 2.3.6.3** (Erster Isomorphiesatz)**.** *(Saloppe Formulierung: Faktorisierung und Übergang zu einer Unteralgebra sind miteinander verträglich.) Seien $\mathfrak{A}$, $\mathfrak{B}$, $\theta$ und $[B]_\theta$ wie in Lemma 2.3.6.1. Dann gilt*

$$B/\theta \cong [B]_\theta/\theta.$$

*Ein Isomorphismus ist gegeben durch $[b]_{\theta{\restriction_B}} \mapsto [b]_{\theta{\restriction_{[B]_\theta}}}$.*

[59] Selbstverständlich: allen, die diesen Test lesen – Lesern, Leserinnen, Leser:innen, und small furry creatures from Alpha Centauri.

*Beweis.* Sei $\varphi\colon A \to C$ ein Homomorphismus, der $\theta$ induziert, also $\theta = \ker(\varphi)$, und sei $D := \varphi(B)$. Dann ist $\theta{\restriction}_B = \ker(\varphi{\restriction}B)$, nach dem Homomorphiesatz 2.3.3.16 also $B/\theta \cong D$ via $g_1 : [b]_{\theta{\restriction}_B} \mapsto \varphi(b)$.
Weiters ist $[B]_\theta = \varphi^{-1}(D)$, und $\varphi([B]_\theta) = D$. Ähnlich wie vorhin ist $\theta{\restriction}_{[B]_\theta} = \ker(\varphi{\restriction}[B]_\theta)$, daher wiederum $[B]_\theta/\theta \cong D$ via $g_2 : [b]_{\theta{\restriction}_{[B]_\theta}} \mapsto \varphi(b)$.
Insgesamt ergibt sich $B/\theta \cong [B]_\theta/\theta$ via $g_2^{-1} \circ g_1 : [b]_{\theta{\restriction}_B} \mapsto [b]_{\theta{\restriction}_{[B]_\theta}}$. □

**UE 122** ► **Übungsaufgabe 2.3.6.4.** (F) Auf der Menge $M = \{1,2,3,4,5\}$ betrachten wir die Äquivalenzrelation $\theta$, die durch die Partition $\{\{1,2\},\{3,4\},\{5\}\}$ gegeben ist, sowie die Untermenge $U := \{4,5\}$. Definieren Sie auf der Menge $M$ eine Algebra $\mathfrak{M}$, sodass $\theta$ Kongruenz ist, $U$ Unteralgebra, und geben Sie explizit den Isomorphismus an, der im ersten Isomorphiesatz beschrieben wird. Um eine triviale Lösung zu vermeiden, verlangen wir zusätzlich, dass es neben der Allrelation keine Kongruenz $\sim$ mit $2 \sim 3$ gibt. ◄ **UE 122**

Mit der folgenden Aussage steuern wir auf den zweiten Isomorphiesatz zu:

**Lemma 2.3.6.5.** *Es seien $\theta_1$ und $\theta_2$ Kongruenzrelationen auf einer Algebra $\mathfrak{A}$ mit $\theta_1 \subseteq \theta_2$. Dann ist die Relation*

$$\theta_2/\theta_1 := \{([a]_{\theta_1}, [b]_{\theta_1}) \mid (a,b) \in \theta_2\}$$

*eine Kongruenzrelation auf $\mathfrak{A}/\theta_1$.*

*Beweis.* Die Reflexivität und Symmetrie von $\theta_2/\theta_1$ folgen unmittelbar aus den entsprechenden Eigenschaften von $\theta_2$ (siehe auch 2.3.6.6), womit $\theta_2/\theta_1$ eine Äquivalenzrelation ist. Außerdem gilt

$$\forall x, y \in A : ([x]_{\theta_1}, [y]_{\theta_2}) \in \theta_2/\theta_1 \Leftrightarrow (x,y) \in \theta_2$$

(und nicht nur die direkt aus der Definition folgende Richtung $\Leftarrow$). Daraus folgt dann auch die Transitivität von $\theta_2/\theta_1$. Den Beweis dieser Tatsachen überlassen wir der Leserin[60] in Übungsaufgabe 2.3.6.6.
Sei nun $\omega$ eine beliebige $n$-stellige Operation von $\mathfrak{A}$ (und damit auch von $\mathfrak{A}/\theta_1$) sowie $([a_1]_{\theta_1}, [b_1]_{\theta_1}), \ldots, ([a_n]_{\theta_1}, [b_n]_{\theta_1}) \in \theta_2/\theta_1$. Dies bedeutet, dass $(a_i, b_i) \in \theta_2$ für $1 \leq i \leq n$. Weil $\theta_2$ eine Kongruenz ist, folgt daraus auch

$$(\omega(a_1, \ldots, a_n), \omega(b_1, \ldots, b_n)) \in \theta_2$$

also $([\omega(a_1, \ldots, a_n)]_{\theta_1}, [\omega(b_1, \ldots, b_n)]_{\theta_1}) \in \theta_2/\theta_1$. Zusammen mit $\omega([a_1]_{\theta_1}, \ldots, [a_n]_{\theta_1}) = [\omega(a_1, \ldots, a_n)]_{\theta_1}$ und der entsprechenden Gleichheit für die $b_i$ erhalten wir

$$(\omega([a_1]_{\theta_1}, \ldots, [a_n]_{\theta_1}), \omega([b_1]_{\theta_1}, \ldots, [b_n]_{\theta_1})) \in \theta_2/\theta_1.$$

Wir haben damit gezeigt, dass $\theta_2/\theta_1$ mit der Operation $\omega$ verträglich ist. Da $\omega$ beliebig war, ist $\theta_2/\theta_1$ somit eine Kongruenz. □

[60] Siehe Fußnote auf Seite 121.

**UE 123** ► **Übungsaufgabe 2.3.6.6.** (F) Seien $A$ eine Menge, $\theta_1, \theta_2$ Äquivalenzrelationen auf $A$ ◄ **UE 123** und $\theta_2/\theta_1$ wie in Lemma 2.3.6.5 definiert.

1. Zeigen Sie: Wenn zusätzlich $\theta_1 \subseteq \theta_2$, dann gilt für alle $x, y \in A$ genau dann $([x]_{\theta_1}, [y]_{\theta_1}) \in \theta_2/\theta_1$, wenn $(x, y) \in \theta_2$. Außerdem ist $\theta_2/\theta_1$ eine Äquivalenzrelation.
2. Geben Sie ein Beispiel von einer Menge $A$ und Äquivalenzrelationen $\theta_1, \theta_2$ sowie von Elementen $x, y \in A$ an derart, dass die Aussagen $([x]_{\theta_1}, [y]_{\theta_1}) \in \theta_2/\theta_1$ und $(x, y) \in \theta_2$ nicht äquivalent sind.
3. Zeigen Sie: Wenn die Aussagen $([x]_{\theta_1}, [y]_{\theta_1}) \in \theta_2/\theta_1$ und $(x, y) \in \theta_2$ für alle $x, y \in A$ äquivalent sind, dann gilt schon $\theta_1 \subseteq \theta_2$.

**Satz 2.3.6.7** (Zweiter Isomorphiesatz)**.** *(Saloppe verbale Formulierung: Iterierte Faktorisierung lässt sich durch eine einzige ersetzen.) Sei $\mathfrak{A}$ eine Algebra und seien $\theta_1 \subseteq \theta_2$ Kongruenzen auf $\mathfrak{A}$ und $\theta_2/\theta_1 := \{([a]_{\theta_1}, [b]_{\theta_1}) \mid (a, b) \in \theta_2\}$ (d.h. wie in Lemma 2.3.6.5 und somit Kongruenz auf $\mathfrak{A}/\theta_1$). Dann gilt*

$$(\mathfrak{A}/\theta_1)/(\theta_2/\theta_1) \cong \mathfrak{A}/\theta_2$$

*vermittels des Isomorphismus*

$$f\colon (\mathfrak{A}/\theta_1)/(\theta_2/\theta_1) \to \mathfrak{A}/\theta_2, \quad [[a]_{\theta_1}]_{\theta_2/\theta_1} \mapsto [a]_{\theta_2}.$$

*Überdies gilt für jede Kongruenzrelation $\theta \in \mathrm{Con}(\mathfrak{A})$: Das Intervall*

$$[\theta, \nabla] := \{\psi \in \mathrm{Con}(\mathfrak{A}) \mid \theta \subseteq \psi\}$$

*im Kongruenzverband $\mathrm{Con}(\mathfrak{A})$ ist ein Unterverband von $\mathrm{Con}(\mathfrak{A})$ und isomorph zum Kongruenzverband $\mathrm{Con}(\mathfrak{A}/\theta)$ der Faktoralgebra. Ein Verbandsisomorphismus ist gegeben durch*

$$k\colon [\theta, \nabla] \to \mathrm{Con}(\mathfrak{A}/\theta) \quad k(\psi) := \psi/\theta.$$

*Beweis.* Wir betrachten zunächst die Abbildung $g : [a]_{\theta_1} \mapsto [a]_{\theta_2}$. Sie ist als Abbildung $g : A/\theta_1 \to A/\theta_2$ wohldefiniert. Sind nämlich $a, b \in A$ mit $[a]_{\theta_1} = [b]_{\theta_1}$, so gilt wegen $\theta_1 \subseteq \theta_2$ auch $[a]_{\theta_2} = [b]_{\theta_2}$, also ist die Definition $g([a]_{\theta_1}) := [a]_{\theta_2}$ unabhängig von der Wahl des Repräsentanten $a$ der Klasse $[a]_{\theta_1}$. Die Surjektivität von $g$ ist offensichtlich. Die Homomorphiebedingung gilt, weil für eine beliebige $n$-stellige Operation $\omega$ von $\mathfrak{A}$ (und damit auch von beiden Faktoralgebren) sowie für $a_1, \ldots, a_n \in A$

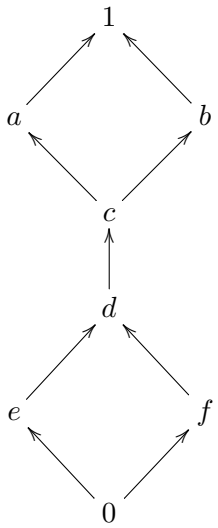
$$\begin{aligned} g(\omega([a_1]_{\theta_1}, \ldots, [a_n]_{\theta_1})) &= g([\omega(a_1, \ldots, a_n)]_{\theta_1}) = [\omega(a_1, \ldots, a_n)]_{\theta_2} = \\ &= \omega([a_1]_{\theta_2}, \ldots, [a_n]_{\theta_2}) = \omega(g([a_1]_{\theta_1}), \ldots, g([a_n]_{\theta_1})). \end{aligned}$$

gilt. Insgesamt ist $g$ also ein surjektiver Homomorphismus mit Kern $\ker g = \theta_2/\theta_1 \in \mathrm{Con}(\mathfrak{A}/\theta_1)$. Nach dem Homomorphiesatz 2.3.3.16 folgt daher, dass $f$ wie in der Aussage des Satzes tatsächlich ein Isomorphismus für $(\mathfrak{A}/\theta_1)/(\ker g) = (\mathfrak{A}/\theta_1)/(\theta_2/\theta_1) \cong \mathfrak{A}/\theta_2$ ist.

Nun zur Abbildung $k$: Die bisherigen Überlegungen zeigen $k\colon [\theta, \nabla] \to \mathrm{Con}(\mathfrak{A}/\theta)$. Klarerweise ist $k$ mit $\subseteq$ verträglich, denn für $\theta \subseteq \psi_1, \psi_2$ gilt $\psi_1 \subseteq \psi_2$ genau dann, wenn $k(\psi_1) \subseteq k(\psi_2)$. Schließlich gibt es zu jedem $\Psi \in \mathrm{Con}(\mathfrak{A}/\theta)$ offenbar genau ein $\psi \in [\theta, \nabla] \subseteq \mathrm{Con}(\mathfrak{A})$ mit $k(\psi) = \Psi$, nämlich $\psi = \{(a, b) \in A^2 : \ ([a]_\theta, [b]_\theta) \in \Psi\}$. Folglich ist $k$ bijektiv, somit ein Isomorphismus zwischen den $\subseteq$-Halbordnungen $[\theta, \nabla] \subseteq \mathrm{Con}(\mathfrak{A})$ und $\mathrm{Con}(\mathfrak{A}/\theta)$. Da beides Verbände sind, handelt es sich bei $k$ sogar um einen Verbandsisomorphismus. □

**UE 124 ► Übungsaufgabe 2.3.6.8.** **◄ UE 124**

Sei $V$ der durch das nebenstehende Hasse-Diagramm gegebene Verband, aufgefasst als Algebra.




(1) Begründen Sie, dass diese partielle Ordnung tatsächlich einen Verband definiert.

(2) Finden Sie zwei nichttriviale Kongruenzrelationen $\varphi$ und $\theta$ mit $\theta \subsetneqq \varphi$.

(3) Geben Sie $V/\varphi$, $V/\theta$, $\varphi/\theta$ und $(V/\theta)/(\varphi/\theta)$ an.

(4) Sei $\Theta = \{(0,0), (e,e), (f,f)\} \cup (V \setminus \{0, e, f\})^2$. Finden Sie einen Verband $V'$ und einen Homomorphismus $\varphi\colon V \to V'$ (im Sinne der Algebra), der die Kongruenzrelation $\Theta$ induziert.

(5) Seien $V$ und $\Theta$ wie bisher und $B = \{0, 1\}$. Geben Sie $\Theta{\restriction_B}$, $[B]_\Theta$, $\Theta{\restriction_{[B]_\Theta}}$, $B/\Theta{\restriction_B}$, und $[B]_\Theta/\left(\Theta{\restriction_{[B]_\Theta}}\right)$ an.

**UE 125 ► Übungsaufgabe 2.3.6.9.** (B) Sei $M = \{1, 2, 3, 4, 5\}$. Auf $M$ betrachten wir die Äquivalenzrelationen, die durch die Partitionen $\{\{1,2\}, \{3\}, \{4\}, \{5\}\}$ und $\{\{1,2\}, \{3,4,5\}\}$ gegeben sind. Definieren Sie auf der Menge $M$ eine Algebra $\mathfrak{M}$, sodass diese beiden Relationen die einzigen nichttrivialen Kongruenzen von $\mathfrak{M}$ sind, und geben Sie explizit den Isomorphismus an, der im zweiten Isomorphiesatz beschrieben wird. **◄ UE 125**

# 3 Elementare Strukturtheorien

Nachdem wir im vorigen Kapitel einen allgemeinen begrifflichen Rahmen zur algebraischen Strukturanalyse aufgebaut haben, sollen nun, sowohl zur Illustration wie auch um für das Weitere wichtige Beispiele kennen zu lernen, Ansätze allgemeiner Strukturtheorien für Halbgruppen und Monoide (3.1), Gruppen (3.2), Moduln und abelsche Gruppen (3.3), Ringe (3.4), geordnete Gruppen und Körper (3.5) sowie für Verbände und Boolesche Algebren (3.6) entwickelt werden. Viel davon wird in späteren Kapiteln noch vertieft werden.

## 3.1 Halbgruppen und Monoide

In diesem Abschnitt geht es durchwegs um Strukturen mit einer binären Operation. Diese Operation schreiben wir aber nur dann an, wenn es zur Unterscheidung vorteilhaft erscheint. Das Produkt zweier Elemente $a$ und $b$ wird also statt der Infixnotation $a \cdot b$ schlicht als $ab$ notiert. Sehr bald werden wir uns auf assoziative Operationen, also auf Halbgruppen und dann weiter auf Monoide, also Halbgruppen mit Einselement, konzentrieren. Zu Beginn (3.1.1) geht es um Potenzen von Elementen und ihre Rechenregeln, 3.1.2 bringt wichtige Beispiele (freies und symmetrisches Monoid), in 3.1.3 wird die eindeutige Primfaktorzerlegung in $\mathbb{N}$ unter algebraischen Gesichtspunkten behandelt und in 3.1.4 behandeln wir die Erweiterung von Monoiden um inverse Elemente in Richtung Gruppe.

### 3.1.1 Potenzen und Inverse

Inhalt in Kurzfassung: Wir beginnen die Halbgruppentheorie mit einfachen Konzepten, die weitgehend aus der elementaren Arithmetik in den Zahlbereichen vertraut sind. Die Tatsache, dass Inverse nicht zu allen Elementen eines Monoids existieren, führt zum Begriff der Einheiten, die stets eine Untergruppe bilden und auch in späteren Kapiteln eine wichtige Rolle spielen werden. Die üblichen Rechenregeln für Potenzen gelten allgemeiner in Halbgruppen bzw. in kommutativen Halbgruppen und zeigen überdies, dass sich jede abelsche Gruppe in natürlicher Weise auch als $\mathbb{Z}$-Modul auffassen lässt.

Die übliche rekursive Definition von *Produkten* auch von mehr als nur zwei Elementen $a_i$ einer Halbgruppe ist offenbar ganz allgemein für binäre Operationen $\cdot$ auf einer Menge $A$ sinnvoll:

$$a_1 \dots a_{n+1} := (a_1 \dots a_n)a_{n+1}.$$

Entsprechend setzt man für *Potenzen*

$$a^1 := a \quad a^{n+1} := a^n \cdot a \quad \text{für } a \in A \text{ und } n \in \mathbb{N}^+ = \mathbb{N} \setminus \{0\}.$$

Gibt es ein bezüglich $\cdot$ neutrales Element $e \in A$, so ergänzt man diese rekursive Definition durch

$$a^0 := e.$$

Existiert überdies ein Inverses $a^*$ zu $a \in A$, setzt man

$$a^{-n} := (a^*)^n.$$

Ist die binäre Operation nicht assoziativ, kann man diese Festsetzung jedoch als willkürlich ansehen, weil Klammerung z.B. von rechts statt von links zu anderen Ergebnissen führen könnte.

**UE 126** ► **Übungsaufgabe 3.1.1.1.** (F) Geben Sie eine Menge $A$ und eine binäre Operation $\cdot$ auf $A$ an, wo $a^3 \neq a \cdot (a \cdot a)$ für ein $a \in A$. ◄ **UE 126**

Für assoziative Operationen jedoch ist das Anschreiben von Klammern bei Produkten von drei oder mehr Elementen nicht erforderlich, wie wir aus Übungsaufgabe 2.1.3.5 ersehen. Explizit gilt also: Ist $H$ eine Halbgruppe und sind $a_1, \ldots, a_n \in H$, so definiert das *Produkt* $a_1 a_2 \ldots a_n$ ein eindeutiges Element, unabhängig davon, wie die Klammern gesetzt werden.
Wir erinnern an Proposition 2.1.3.8. Aus ihr folgt insbesondere, dass in einer Halbgruppe $(H, \cdot)$ mit einem Element $e \in H$, welches $ae = ea = a$ für alle $a \in H$ erfüllt, dieses eindeutig bestimmt ist, d.h. es gibt nur ein Element, für das $(H, \cdot, e)$ sogar ein Monoid ist. In diesem Fall ist dann auch für jedes $a \in H$ ein Inverses $a^{-1}$, sofern es existiert, eindeutig bestimmt. Gibt es in einem Monoid $(M, \cdot, e)$ für alle $a \in M$ ein $a^{-1}$, so liegt demnach eine eindeutige unäre Operation $.^{-1} : M \to M$, $a \mapsto a^{-1}$ vor, die $(M, \cdot, e, .^{-1})$ zu einer Gruppe macht. Haben nicht alle $a \in M$ ein Inverses, so liegt die folgende Begriffsbildung nahe.

**Definition 3.1.1.2.** Ist $\mathfrak{M} = (M, \cdot, e)$ ein Monoid, so nennt man ein Element $a \in M$, zu dem es in $M$ ein Inverses $a^{-1}$ (also ein Element mit $aa^{-1} = a^{-1}a = e$) gibt, eine *Einheit*. Die Menge $E = E(\mathfrak{M})$ aller Einheiten heißt die *Einheitengruppe* von $\mathfrak{M}$.

Diese Terminologie ist berechtigt:

**Proposition 3.1.1.3.** *Die Einheitengruppe eines Monoids ist eine Gruppe.*

**UE 127** ► **Übungsaufgabe 3.1.1.4.** (F+) Beweisen Sie Proposition 3.1.1.3. ◄ **UE 127**

Im Zusammenhang mit Homomorphismen sind folgende einfache Beobachtungen nützlich:

**Proposition 3.1.1.5.** *Seien $H$ und $H'$ Halbgruppen und $\varphi : H \to H'$ ein Homomorphismus.*

1. *Ist $e$ links- bzw. rechtsneutral in $H$, so ist $\varphi(e)$ links- bzw. rechtsneutral in $\varphi(H)$.*

2. *Ist $e \in H$ neutral in $H$ und $e' \in H'$ neutral ein $H'$, so folgt i.A.* nicht $\varphi(e) = e'$.

3. *Seien $(H, \cdot, e)$ und $(H', \cdot, e')$ sogar Monoide und $\varphi\colon H \to H'$ ein Monoidhomomorphismus. Ist $a_l$ ein Linksinverses von $a$, dann ist $\varphi(a_l)$ ein Linksinverses von $\varphi(a)$. Analog gilt dann auch: Ist $a_r$ ein Rechtsinverses von $a$, dann ist $\varphi(a_r)$ ein Rechtsinverses von $\varphi(a)$. Inbesondere gilt: Wenn $a$ ein Inverses hat, dann auch $\varphi(a)$, wobei $\varphi(a)^{-1} = \varphi(a^{-1})$.*

4. *Seien $(H, \cdot, e, ^{-1})$ und $(H', \cdot, e', ^{-1})$ sogar Gruppen und $\varphi\colon H \to H'$ ein Monoidhomomorphismus. Dann ist $\varphi$ automatisch ein Gruppenhomomorphismus.*

**UE 128** ▶ **Übungsaufgabe 3.1.1.6.** (V) Beweisen Sie Proposition 3.1.1.5. ◀ **UE 128**

Die letzte Aussage der vorangehenden Proposition liefert die Verträglichkeit von Inversen mit Homomorphismen. Ein weiteres einfaches Verträglichkeitsresultat lässt sich für Inverse und Kommutativität beweisen.

**Lemma 3.1.1.7.** *Sei $H$ eine Halbgruppe und seien $a, b \in H$ mit $ab = ba$. Wenn $a$ ein Inverses $a^{-1}$ hat, dann gilt $a^{-1}b = ba^{-1}$. Hat $b$ ebenfalls ein Inverses $b^{-1}$, dann gilt auch $a^{-1}b^{-1} = b^{-1}a^{-1}$.*

**UE 129** ▶ **Übungsaufgabe 3.1.1.8.** Beweisen Sie Proposition 3.1.1.7. Geben Sie explizit an, wo und wie Sie das Assoziativgesetz verwenden. („Wie“ bedeutet: Geben Sie an, für welche $A$, $B$, $C$ Sie $(AB)C = A(BC)$ verwenden.) ◀ **UE 129**

Unabhängig davon, ob es in einer Halbgruppe bereits ein neutrales Element gibt, kann ein neues Element hinzugefügt werden, das diese Rolle übernimmt. Man rechnet leicht nach:

**Proposition 3.1.1.9.** *Ist $H$ eine Halbgruppe und $e \notin H$, so wird $M := H \cup \{e\}$ zum Monoid mit Einselement $e$, wenn man die binäre Operation auf $H$ auf $M$ fortsetzt durch $eh = he := h$ für alle $h \in M$.*

Sehr häufig werden wir statt von Halbgruppen gleich von Monoiden ausgehen, insbesondere wenn wir uns damit lästige Fallunterscheidungen oder Sonderfälle ersparen können. Dank Proposition 3.1.1.9 bedeutet das keine schwerwiegende Einschränkung. Zu beachten ist eventuell, dass durch die in 3.1.1.9 beschriebene Konstruktion ein in $H$ möglicherweise bereits existierendes Einselement $e_H$ wegen $e_H e = e e_H = e_H \neq e$ in $M = H \cup \{e\}$ diesen Status an $e$ abgeben muss.

Wir kehren zurück zu Potenzen in Halbgruppen, Monoiden und Gruppen. Offenbar gelten die folgenden von den klassischen Zahlenbereichen vertrauten Rechenregeln auch in unserem allgemeineren Kontext:

**Proposition 3.1.1.10.** *In Halbgruppen $H$ gelten folgende Rechenregeln:*

1. $a^{m+n} = a^m a^n$
2. $(a^m)^n = a^{mn}$
3. $(ab)^n = a^n b^n$, *sofern* $ab = ba$, *insbesondere also wenn die binäre Operation kommutativ ist,*

*für alle* $a, b \in H$ *und* $m, n \in \mathbb{N}^+$. *Ist* $H$ *ein Monoid, so sind auch* $m = 0$ *und/oder* $n = 0$ *zugelassen, im Fall der Existenz von Inversen* $a^{-1}$ *von* $a$ *und* $b^{-1}$ *von* $b$ *auch beliebige* $m, n \in \mathbb{Z}$.

**UE 130** ▶ **Übungsaufgabe 3.1.1.11.** (F+) Beweisen Sie Proposition 3.1.1.10. Gehen Sie dabei von der induktiven Definition von $a^n$ aus: $a^0$ ist das neutrale Element, $a^1 := a$, $a^{n+1} := a^n \cdot a$ für $n \geq 0$, $a^{-1}$ ist invers zu $a$, $a^{-n} := (a^{-1})^n$ für $n \geq 2$. Verwenden Sie vollständige Induktion, und geben Sie explizit an, auf welche Teilmenge von $\mathbb{N}$ Sie das Induktionsprinzip anwenden. Achtung: Gelegentlich sind Fallunterscheidungen wie $n \geq 0$, $n < 0$ notwendig. Geben Sie explizit an, wo und wie Sie das Assoziativgesetz verwenden. („Wie“ bedeutet: Geben Sie an, für welche $A$, $B$, $C$ Sie $(AB)C = A(BC)$ verwenden.) ◀ **UE 130**

Die Rechenregel $a^m a^n = a^{m+n}$ spielt im Beweis der folgenden Aussage die entscheidende Rolle. In Kapitel 4 werden wir die dabei auftretenden abstrakten Gesichtspunkte noch in allgemeinerem Zusammenhang vertiefen.

**Proposition 3.1.1.12.** *Ist* $H$ *eine Halbgruppe und* $a \in H$, *so gibt es genau einen Halbgruppenhomomorphismus* $\varphi\colon \mathbb{N}^+ \to H$ *von der additiven Halbgruppe* $\mathbb{N}^+$ *nach* $H$ *mit* $\varphi(1) = a$, *nämlich* $\varphi : n \mapsto a^n$. *Der Bildbereich von* $\varphi$ *ist die von* $a$ *erzeugte Halbgruppe* $\langle a \rangle$. *Ist* $H$ *sogar ein Monoid mit Einselement* $e$, *so lässt sich* $\varphi$ *durch* $\varphi(0) := e$ *sogar zu einem ebenfalls eindeutigen Monoidhomomorphismus* $\mathbb{N} \to H$ *fortsetzen.*

**UE 131** ▶ **Übungsaufgabe 3.1.1.13.** (W) Beweisen Sie Proposition 3.1.1.12 und deuten Sie diese Aussage als universelle Eigenschaft in einer geeigneten Kategorie. Bereits früher bewiesene Tatsachen dürfen und sollen Sie möglichst verwenden. ◀ **UE 131**

Als Verallgemeinerung davon lässt sich die folgende Tatsache auffassen:

**Proposition 3.1.1.14.** *Sei* $H$ *eine Halbgruppe und* $X \subseteq H$. *Die von* $X$ *erzeugte Unterhalbgruppe* $\langle X \rangle$ *ist die Menge* $M$ *aller Produkte* $x_1 x_2 \dots x_n$ *(wie in der Definition zu Beginn linksgeklammert zu denken) mit* $n \in \mathbb{N}^+$ *und* $x_i \in X$ *für* $i = 1, \dots, n$.

**UE 132** ▶ **Übungsaufgabe 3.1.1.15.** (F) Beweisen Sie Proposition 3.1.1.14 unter Verwendung von Proposition 2.3.1.13. Finden Sie außerdem ein Beispiel einer Algebra $(H, \cdot)$ vom Typ (2) und einer Teilmenge $X \subseteq H$, wo $H \neq \langle X \rangle$ gilt. Welche Inklusion muss aber jedenfalls gelten? ◀ **UE 132**

Fast selbsterklärend ist die Schreibweise für Komplexprodukte.

**Definition 3.1.1.16.** Ist $H$ eine Halbgruppe, $n \in \mathbb{N}$, und sind $A_1, \ldots, A_n \subseteq H$ Teilmengen von $H$, so heißt die Teilmenge

$$A_1 \cdots A_n := \{a_1 \ldots a_n : \ a_i \in A_i \text{ für } i = 1, \ldots, n\}$$

*Komplexprodukt* von $A_1, \ldots, A_n$.[1]
Falls mindestens eine der Mengen $A_1$, ..., $A_n$ leer ist, so ist auch das Komplexprodukt $A_1 \cdots A_n$ leer.

## 3.1.2 Wichtige Beispiele von Halbgruppen

Inhalt in Kurzfassung: Als wichtigste Beispiele von Halbgruppen bzw. Monoiden werden das freie und das symmetrische Monoid samt Darstellungssatz von Cayley ausführlicher besprochen.

Die wichtigste Halbgruppe, die wir bisher behandelt haben, ist $\mathbb{N}$ bezüglich $+$. Ihre Bedeutung liegt primär an der Rolle der natürlichen Zahlen als Kardinalitäten endlicher Mengen (siehe Abschnitt 1.1.1), kommt aber auch unter abstrakt algebraischen Gesichtspunkten in Proposition 3.1.1.12 zum Ausdruck. In Verallgemeinerung davon könnte man nach einer Halbgruppe $F = F(X)$ (oder einem Monoid) mit der Eigenschaft suchen, dass jede Abbildung $j : X \to H$ in eine Halbgruppe (oder in ein Monoid) $H$ zu einem eindeutigen Homomorphismus $F(X) \to H$ fortgesetzt werden kann. Der Buchstabe $F$ steht für *frei*, weil so eine Struktur eine *freie Halbgruppe* (oder ein *freies Monoid*) heißt. Der Hintergrund wird im allgemeineren Kontext von Abschnitt 4.1 deutlich werden.
Die Konstruktion eines solchen $F(X)$ ist ziemlich einfach. Als Trägermenge hat man lediglich die Menge aller endlichen (Zeichen-)Folgen (Strings, Wörter über $X$) $x_1 \ldots x_n$ mit $n \in \mathbb{N}^\times$ und $x_i \in X$ für $i = 1, \ldots, n$ zu nehmen, als Operation die *Konkatenation*

$$(x_1 \ldots x_n) \cdot (y_1 \ldots y_m) := x_1 \ldots x_n y_1 \ldots y_m.$$

Wem die Arbeit mit mathematisch etwas vagen Objekten wie „Zeichenketten“ $x_1 \ldots x_n$ missfällt, kann stattdessen Tupel $(x_1, \ldots, x_n)$ verwenden und formal etwas korrekter definieren: $(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_m) := (z_1, \ldots, z_{n+m})$ mit $z_i := x_i$ für $i = 1, \ldots, n$ und $z_{n+j} := y_j$ für $j = 1, \ldots, m$. Will man analog ein freies Monoid statt einer freien Halbgruppe, so erweitert man die Menge aller endlichen Zeichenketten zur Menge $X^*$, die auch das sogenannte *leere Wort* enthält, das wir oft mit dem Buchstaben $\varepsilon$ bezeichnen. Formal kann man es als Folge der Länge 0 auffassen, also als Funktion mit leerem Definitionsbereich. Das leere Wort ist das neutrale Element bezüglich der Konkatenation.

[1] Die naheliegende Schreibweise $A^n$ für den Fall $A_1 = \ldots = A_n$ ist problematisch, weil sie sehr leicht zur Verwechslung mit dem kartesischen Produkt $A \times A \times \ldots \times A$ führen kann, außerdem mit der Menge $\{a^n : \ a \in A\}$.

**UE 133** ▶ **Übungsaufgabe 3.1.2.1.** (V) Begründen Sie, dass die oben beschriebene Struktur tatsächlich die oben formulierte Eigenschaft einer freien Halbgruppe bzw. eines freien Monoids hat: Jede Abbildung $j : X \to H$ in eine Halbgruppe bzw. in ein Monoid $H$ kann zu einem eindeutigen Homomorphismus $X^* \to H$ fortgesetzt werden kann. Deuten Sie die Situation auch als universelle Eigenschaft in einer geeigneten Kategorie. ◀ **UE 133**

Freie Halbgruppen und Monoide über Alphabeten spielen eine wichtige Rolle in der Theorie der formalen Sprachen und somit in der theoretischen Informatik.
Hätten wir uns auf abelsche Halbgruppen/Monoide beschränkt, so würde sich die Konstruktion vereinfachen, weil es nicht auf die Reihenfolge der $x_i$ in einer Zeichenkette ankommt, sondern nur auf die Anzahl $n_x \in \mathbb{N}$ der Vorkommnisse jedes $x \in X$. Ein typisches Element des freien abelschen Monoids $A_X$ ist daher gegeben durch eine Familie $(n_x)_{x\in X} \in \mathbb{N}^X$, wobei $n_x \neq 0$ allerdings nur für endlich viele $x \in X$ gelten darf, auch wenn $X$ unendlich sein sollte. Für die freie abelsche Halbgruppe (statt Monoid) ist im Unterschied dazu lediglich die Familie mit $n_x = 0$ für alle $x \in X$ (die ja dem leeren Wort entspricht) auszuschließen.

**UE 134** ▶ **Übungsaufgabe 3.1.2.2.** (V) Analog 3.1.2.1, nur für abelsche statt für beliebige Halbgruppen bzw. Monoide. ◀ **UE 134**

Aus dem Bisherigen ist ersichtlich, dass freie Monoide (analog freie Halbgruppen, abelsche Monoide, abelsche Halbgruppen) insofern *universell* unter allen Monoiden sind, als jedes beliebige Monoid $M$ homomorphes Bild eines freien Monoids ist, nämlich z.B. mit der Trägermenge von $M$ als $X$: Es gibt einen surjektiven Homomorphismus $\alpha : M^* \to M$.

**UE 135** ▶ **Übungsaufgabe 3.1.2.3.** (F) Beweisen Sie diese Behauptung. ◀ **UE 135**

In gewissem Sinn dual wäre die Eigenschaft, dass jedes beliebige Monoid in ein geeignetes Monoid aus einer bestimmten Teilklasse von Monoiden isomorph eingebettet werden kann. Das ist tatsächlich möglich, wenn man als Teilklasse die symmetrischen Halbgruppen nimmt.

**Definition 3.1.2.4.** Sei $X$ eine beliebige Menge und $M_X$ (oder auch $X^X$) die Menge aller Abbildungen $f\colon X \to X$. Die Abbildungsmultiplikation $\circ$ als binäre Operation zusammen mit der identischen Abbildung $\mathrm{id}_X : x \mapsto x$ als neutralem Element macht $M_X$ zu einem Monoid, dem sogenannten *symmetrischen Monoid* auf $X$.

Mit dieser Definition gilt der *Darstellungssatz von Cayley für Monoide*:

**Satz 3.1.2.5.** *Jedes Monoid $M$ lässt sich vermittels der Einbettung $\iota : a \mapsto f_a$, $f_a(x) := ax$ für $a, x \in M$ isomorph in das symmetrische Monoid $M_X$ einbetten, wenn man für $X$ die Trägermenge von $M$ wählt.*

*Beweis.* Klarerweise ist $\iota\colon M \to M_X$ wohldefiniert mit Definitionsbereich $M$ und Werten in $M_X$. Weiters ist $\iota$ injektiv, denn $\iota(a) = \iota(b)$ bedeutet $f_a = f_b$ und somit speziell

$a = ae = f_a(e) = f_b(e) = be = b$, wenn $e$ das neutrale Element in $M$ bezeichnet. Wegen $f_e(x) = ex = x$ bildet $\iota$ das neutrale Element $e$ in $M$ auf $\iota(e) = f_e = \mathrm{id}_X$, das neutrale Element in $M_X$, ab. Schließlich ist auch die Homomorphiebedingung für die binäre Operation erfüllt:

$$f_{ab}(x) = (ab)x = a(bx) = f_a(bx) = f_a(f_b(x)) = (f_a \circ f_b)(x)$$

(Erst jetzt haben wir die Assoziativität verwendet.) für alle $x \in X$, also $\iota(ab) = f_{ab} = f_a \circ f_b = \iota(a) \circ \iota(b)$. □

Die Einbettung $\iota$ aus Satz 3.1.2.5 nennt man die *reguläre Darstellung* des Monoids $M$. Sie wird auch im ganz analogen und noch wichtigeren Darstellungssatz von Cayley für Gruppen (siehe 3.2.5) verwendet. Bedenkt man die Möglichkeit, beliebige Halbgruppen zu Monoiden zu ergänzen (siehe 3.1.1.9), so zeigen die Cayleyschen Sätze, dass die Komposition von Abbildungen die allgemeinste assoziative Operation repräsentieren kann.

**UE 136 ► Übungsaufgabe 3.1.2.6.** (F) In dieser Aufgabe beschäftigen wir uns mit einem zum Darstellungssatz von Cayley ähnlichen Satz für Halbgruppen statt für Monoide. **◄ UE 136**

1. Sei $H$ eine Halbgruppe. Finden Sie eine Menge $S$ und eine isomorphe Einbettung $\iota : H \to S^S$. Hinweis: Proposition 3.1.1.9
2. Finden Sie eine Halbgruppe $H$, sodass die Abbildung $\varphi : H \to H^H$, $a \mapsto f_a$, wobei $f_a(x) := ax$, nicht injektiv ist.

Wichtige Halbgruppen ganz anderer Art treten in der Maßtheorie, Fourieranalysis und Wahrscheinlichkeitstheorie mit der Faltung $*$ von Funktionen oder von Maßen als assoziativer Operation auf. Und zwar ist für zwei Wahrscheinlichkeitsmaße $\mu$ und $\nu$ ihre Faltung $\mu * \nu$ so definiert, dass sie die Verteilung der Summe $X + Y$ zweier unabhängiger Zufallsgrößen $X$ und $Y$ mit Verteilungen $\mu$ bzw. $\nu$ ist. So bildet die Menge aller Normalverteilungen $\nu_{m,v}$ auf $\mathbb{R}$ mit Mittelwert $m \in \mathbb{R}$ und Varianz $v \geq 0$ bezüglich der Faltung ein Monoid, das der Rechenregel $\nu_{m_1,v_1} * \nu_{m_2,v_2} = \nu_{m_1+m_2,v_1+v_2}$ genügt, folglich isomorph ist zum (additiven) Monoid $\mathbb{R} \times \mathbb{R}_0^+$.
Hier verzichten wir auf eine Vertiefung solcher Beispiele, weil wir dafür zu weit in die Maßtheorie ausholen müssten. An die Faltung wird uns an späterer Stelle das gleichfalls aus der Analysis vertraute Cauchyprodukt von Potenzreihen (in der Algebra: von formalen Potenzreihen, siehe 3.4.6) erinnern, aber auch die Konstruktion des Gruppenrings (siehe 4.2.4).

### 3.1.3 Algebraische Strukturanalyse auf $\mathbb{N}$

Inhalt in Kurzfassung: Wir geben einen ersten Beweis von der Eindeutigkeit der Primfaktorzerlegung natürlicher Zahlen und deuten diesen als Struktursatz: Das multiplikative Monoid auf $\mathbb{N}^+$ ist isomorph zur direkten Summe abzählbar unendlich vieler Kopien des additiven Monoids auf $\mathbb{N}$. Ein damit verwandter Struktursatz beschreibt den vollständigen Verband, der durch die Teilerrelation auf $\mathbb{N}$ gegeben ist. Für spätere Zwecke wird

auch die Division mit Rest auf $\mathbb{N}$ und $\mathbb{Z}$ bereitgestellt.

Wir wollen wieder mit der Menge $\mathbb{N}$ der natürlichen Zahlen beginnen und wählen ihre sehr einfache additive Struktur zum Bezugspunkt für die Analyse der multiplikativen Struktur. Dabei ist es keine wesentliche Einschränkung, wenn wir uns der einfacheren Notation halber auf das kommutative Monoid (Halbgruppe mit Einselement) $(\mathbb{N}^+, \cdot)$ mit $\mathbb{N}^+ := \mathbb{N}\setminus\{0\}$ konzentrieren. Eine sehr befriedigende Beschreibung liefert der sogenannte *Fundamentalsatz der Arithmetik* oder auch der *Zahlentheorie*. Zur Erinnerung die wichtigsten Definitionen. Dabei ist es manchmal vorteilhaft, statt $\mathbb{N}$ die gesamte Menge $\mathbb{Z}$ heranzuziehen.

**Definition 3.1.3.1.** Eine ganze Zahl $a \in \mathbb{Z}$ heißt *Teiler* von $b \in \mathbb{Z}$, falls es ein $c \in \mathbb{Z}$ gibt mit $b = ac$, symbolisch $a|b$ (*a teilt b*). Man sagt in diesem Fall auch, $b$ ist ein *Vielfaches* von $a$. Eine Zahl $p \in \mathbb{N}$ heißt *Primzahl*, falls $p$ innerhalb $\mathbb{N}$ genau die beiden Teiler 1 und $p \neq 1$ hat.[2] Die Menge aller Primzahlen bezeichnen wir mit $\mathbb{P}$.

**Satz 3.1.3.2** (*Fundamentalsatz der Arithmetik*)**.** *Jede natürliche Zahl $n > 0$ hat eine (bis auf die Reihenfolge der Faktoren) eindeutige Darstellung als Produkt von Primzahlen, genannt* Primfaktorzerlegung *(1 fassen wir als leeres Produkt auf), genauer: Zu jedem $n \in \mathbb{N}$ gibt es genau eine Familie $(e_p)_{p\in\mathbb{P}}$ von Exponenten $e_p \in \mathbb{N}$ mit $n = \prod_{p\in\mathbb{P}} p^{e_p}$. Dabei sind nur endlich viele $e_p$ von 0 verschieden, weshalb das Produkt, weil nur endlich viele Faktoren von 1 verschieden sind, wohldefiniert ist.*

*Beweis.* Die Behauptung lässt sich in eine Existenz und eine Eindeutigkeitsaussage aufspalten.
Zunächst zur Existenz so einer Darstellung: Gäbe es, indirekt, eine positive natürliche Zahl ohne Primfaktorzerlegung, so auch eine kleinste, die wir $n$ nennen. Diese Zahl $n$ ist weder 1 (leeres Produkt) noch eine Primzahl (Produkt aus einem Faktor), hat also einen von 1 und $n$ verschiedenen Teiler $a \in \mathbb{N}$. Also gibt es ein $b \in \mathbb{N}$ mit $n = ab$. Offenbar gilt $1 < a, b < n$. Da $n$ minimal gewählt war, müssen $a$ und $b$ Primfaktorzerlegungen haben, deren Produkt aber eine Primfaktorzerlegung von $n$ ist, Widerspruch.
Noch interessanter ist die Eindeutigkeitsaussage: Wieder gehen wir indirekt von einem kleinsten $n$ mit mehr als einer Primfaktorzerlegung aus:

$$n = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s$$

mit $p_i, q_j \in \mathbb{P}$ für $1 \leq i \leq r, 1 \leq j \leq s$. Wäre $p_i = q_j$ für gewisse Indizes $i, j$, so ließe sich durch diese Zahl durchdividieren, und auch $\frac{n}{p_i} < n$ hätte mehr als eine Primfaktorzerlegung, Widerspruch. Also gilt $p_i \neq q_j$ für alle $i, j$. Insbesondere ist $p_1 \neq q_1$, oBdA $p_1 < q_1$. Wir betrachten die Zahl

$$n' := (q_1 - p_1)q_2 \cdot \ldots \cdot q_s = n - p_1(q_2 \cdot \ldots \cdot q_s) = p_1(p_2 \cdot \ldots \cdot p_r - q_2 \cdot \ldots \cdot q_s) = p_1 m$$

mit $m := p_2 \cdot \ldots \cdot p_r - q_2 \cdot \ldots \cdot q_s$. Wegen $n' > 0$ ist auch $m > 0$. Einerseits gilt nun: Indem man $m$ in Primfaktoren zerlegt, erhält man aus der Gleichung $n' = p_1 m$ eine

[2] 1 selbst ist also definitionsgemäß keine Primzahl.

Primfaktorzerlegung von $n'$ mit mindestens einem Primfaktor $p_1$. Andererseits überlegen wir, dass $p_1$ kein Teiler von $q_1 - p_1$ sein kann, weil es sonst auch ein Teiler der Primzahl $q_1 > p_1$ wäre, was unmöglich ist. Deshalb erhält man, wenn man in der Gleichung $n' = (q_1 - p_1) \cdot q_2 \cdot \ldots \cdot q_2$ auch noch eine Primfaktorzerlegung von $q_1 - p_1$ einsetzt, eine weitere Primfaktorzerlegung von $n'$, die $p_1$ sicher nicht enthält.
Wir haben also zwei verschiedene Primfaktorzerlegungen für $n'$ gefunden, was wegen $n' < n$ im Widerspruch steht zur Minimalität von $n$. □

Wir verwenden

$$\prod_{p\in\mathbb{P}}^{w} \mathbb{N} = \{(e_p)_{p\in\mathbb{P}} : e_p \in \mathbb{N}, e_p \neq 0 \text{ für nur endlich viele } p\},$$

das schwache Produkt (siehe Definition 3.2.3.9) abzählbar unendlich vieler (hier mit $p \in \mathbb{P}$ indizierter) Kopien von $\mathbb{N}$. Es enthält jene Elemente des vollen kartesischen Produktes, die nur endlich viele von 0 verschiedene Eintragungen haben. Mit dieser Notation lässt sich Satz 3.1.3.2 auch so formulieren:
Die Abbildung

$$\varphi\colon \prod_{p\in\mathbb{P}}^{w} \mathbb{N} \to \mathbb{N}^+, \quad (e_p)_{p\in\mathbb{P}} \mapsto \prod_{p\in\mathbb{P}} p^{e_p}$$

ist bijektiv.
Doch $\varphi$ ist nicht nur bijektiv. Für $x = (e_p)_{p\in\mathbb{P}}, y = (f_p)_{p\in\mathbb{P}} \in \prod_{p\in\mathbb{P}}^{w} \mathbb{N}$ ist, wenn wir komponentenweise addieren, wegen

$$\begin{aligned}\varphi(x+y) = \varphi((e_p)_{p\in\mathbb{P}} + (f_p)_{p\in\mathbb{P}}) &= \prod_{p\in\mathbb{P}} p^{e_p+f_p} = \prod_{p\in\mathbb{P}} p^{e_p} \cdot \prod_{p\in\mathbb{P}} p^{f_p} = \\ &= \varphi((e_p)_{p\in\mathbb{P}}) \cdot \varphi((f_p)_{p\in\mathbb{P}}) = \varphi(x) \cdot \varphi(y)\end{aligned}$$

offenbar auch die Homomorphiebedingung erfüllt. In algebraische Sprache übersetzt, haben wir bewiesen:

**Satz 3.1.3.3.** *Das multiplikative Monoid* $(\mathbb{N}^+, \cdot, 1)$ *der positiven natürlichen Zahlen ist isomorph zum schwachen Produkt abzählbar vieler Kopien des additiven Monoids* $(\mathbb{N}, +, 0)$ *aller natürlichen Zahlen (inklusive* 0*). Ein Isomorphismus* $\varphi\colon \prod_{p\in\mathbb{P}}^{w}(\mathbb{N}, +, 0) \to (\mathbb{N}^+, \cdot, 1)$ *ist gegeben durch*

$$(e_p)_{p\in\mathbb{P}} \mapsto \prod_{p\in\mathbb{P}} p^{e_p}.$$

Die Macht dieses Satzes wird offensichtlich, wenn man sich folgende Zusammenhänge klar macht. Schreiben wir $(e_p(n))_{p\in\mathbb{P}} := \varphi^{-1}(n)$ mit dem Isomorphismus $\varphi$ aus Satz 3.1.3.3, so lesen wir für $a, b \in \mathbb{N}^+$ ab, dass Teilbarkeit $a|b$ genau dann gilt, wenn $e_p(a) \leq e_p(b)$ für alle $p \in \mathbb{P}$ gilt. Die relationale Struktur $(\mathbb{N}, |)$ ist also isomorph zu einer relationalen Struktur, die sich in naheliegender Weise als Unterstruktur eines direkten Produktes deuten lässt. Und zwar ist $(\mathbb{N}, \leq)$ als Totalordnung verbandsgeordnet im ordnungstheoretischen Sinn. Der zugeordnete Verband $(\mathbb{N}, \max, \min)$ im algebraischen Sinn ist sogar distributiv. Weil die distributiven Verbände als gleichungsdefinierte Klasse (Varietät) abgeschlossen sind

bezüglich der Bildung direkter Produkte, ist auch $\prod_{p\in\mathbb{P}}(\mathbb{N}, \max, \min)$ ein distributiver Verband, wobei die Operationen max und min komponentenweise auszuführen sind. $\prod^w_{p\in\mathbb{P}} \mathbb{N}$ ist eine (Trägermenge einer) Unteralgebra dieses Verbandes, somit selbst ein distributiver Verband. Aufgrund der obigen Überlegungen ist $\varphi$ ein Isomorphismus der zugeordneten Halbordnungen $(\mathbb{N}^+, |)$ und $(\prod^w_{p\in\mathbb{P}} \mathbb{N}, \leq)$, wenn man $\leq$ komponentenweise auffasst. Leicht überlegt man sich, dass der Verband $(\mathbb{N}^+, |)$ distributiv bleibt, wenn man das Element 0 mit $n|0$ für alle $n \in \mathbb{N}$, d.h. als größtes Element, hinzufügt. Wie man sich ebenfalls schnell klar macht, wird der Verband dadurch sogar vollständig. Damit ist ein Beweis für folgenden Satz angedeutet:

**Satz 3.1.3.4.** *Die Menge* $\mathbb{N}$ *der natürlichen Zahlen bildet bezüglich Teilbarkeit einen distributiven, vollständigen Verband. Kleinstes Element ist* 1*, größtes Element ist* 0*. Supremum ist das* kleinste gemeinsame Vielfache*, abgekürzt kgV. Infimum ist der* größte gemeinsamer Teiler*, abgekürzt ggT. Sowohl kgV als auch ggT einer Teilmenge* $T \subseteq \mathbb{N}$ *lassen sich aus der Primfaktorzerlegung gewinnen, indem man für jedes* $p \in \mathbb{P}$ *als Exponenten* $e_p$ *(Notation wie oben) das Maximum bzw. das Minimum (sofern vorhanden) aller* $e_p(t)$ *mit* $t \in T$ *nimmt, allerdings mit folgenden Ausnahmen: Für unendliches* $T$ *sowie im Falle* $0 \in T$ *ist* $kgV(T) = 0$*, und für* $T \subseteq \{0\}$ *ist* $ggT(T) = 0$*.*

**UE 137 ▶ Übungsaufgabe 3.1.3.5.** (V) Vervollständigen Sie den Beweis von Satz 3.1.3.4. **◀ UE 137**

**UE 138 ▶ Übungsaufgabe 3.1.3.6.** (E) In den Überlegungen zu Satz 3.1.3.4 hat man sich nicht nur für die algebraische Struktur auf Produkten interessiert, sondern auch für Halbordnungen darauf. Gehen Sie dem nach, indem Sie folgende Schritte ausführen: **◀ UE 138**

1. Definieren Sie eine Ihnen für das Folgende sinnvoll erscheinende Kategorie $\mathcal{C}$, deren Objekte alle Halbordnungen sind.
2. Begründen Sie Ihre Wahl der Morphismen in $\mathcal{C}$.
3. Gibt es in $\mathcal{C}$ uneingeschränkt Produkte?
4. Schränken Sie $\mathcal{C}$ auf jene Halbordnungen ein, die verbandsgeordnet sind. Wie verhält sich die resultierende Kategorie zur Kategorie der Verbände im algebraischen Sinn, aufgefasst als Varietät?

Auf der Hand liegen Satz 3.1.3.4 entsprechende Aussagen über die multiplikative Struktur von $\mathbb{Z}$. Zu beachten ist lediglich, dass $m|n$ und $n|m$ dann nicht $n = m$ impliziert, sondern lediglich $n = m$ oder $n = -m$. Entsprechend sind ggT und kgV dann nur bis aufs Vorzeichen eindeutig bestimmt etc. Wir werden davon schon ab jetzt Gebrauch machen. In allgemeinerem Kontext und systematisch wird das Gegenstand der Teilbarkeitslehre in Kapitel 5 sein. Die multiplikative Halbgruppe lässt sich in ziemlich offensichtlicher Weise als direktes Produkt von zwei Faktoren beschreiben.

**UE 139 ► Übungsaufgabe 3.1.3.7.** (F) Beschreiben Sie, wie und warum die Halbgruppe $(\mathbb{Z} \setminus \{0\}, \cdot)$ isomorph ist zum direkten Produkt von $(\mathbb{N}^+, \cdot)$ und einer zweiten Halbgruppe. Welcher? ◄ **UE 139**

Zur Erinnerung: Auf einer beliebigen Menge $A$ sind die *Gleichheitsrelation* $\Delta_A := \{(x, x) \mid x \in A\}$ (auch genannt *Identität*), und die *Allrelation* $\nabla_A = A \times A$ stets Äquivalenzrelationen, genannt die *trivialen Äquivalenzrelationen* auf $A$. Alle anderen Äquivalenzrelationen heißen „nichttrivial“.

**UE 140 ► Übungsaufgabe 3.1.3.8.** (F) Finden Sie nichttriviale Kongruenzrelationen $R$ und $S$ auf der Struktur $(\mathbb{N}, +)$ mit folgenden Eigenschaften: ◄ **UE 140**

- $(3, 14) \in R$
- Es gibt mindestens zwei $R$-Äquivalenzklassen, die 1-elementig sind, und mindestens zwei, die nicht einelementig sind.
- $(3, 14) \in S$
- Keine $S$-Äquivalenzklasse ist 1-elementig.

**UE 141 ► Übungsaufgabe 3.1.3.9.** (F+) Finden Sie alle Kongruenzrelationen auf $(\mathbb{N}, +)$. Erklären Sie auch, warum Ihre Liste vollständig ist. ◄ **UE 141**

**UE 142 ► Übungsaufgabe 3.1.3.10.** (D) In dieser Übungsaufgabe interessieren wir uns für Unteralgebren und Kongruenzrelationen auf $\mathbb{N}$ bezüglich additiver und/oder multiplikativer Struktur. Versuchen Sie jeweils alle Objekte der angegebenen Art zu beschreiben. Wenn Ihnen das zu schwierig erscheint (was in der Mehrzahl der Fälle wahrscheinlich ist), ermitteln Sie, wieviele es davon gibt. Unterscheiden Sie dabei verschiedene unendliche Kardinalitäten, insbesondere $|\mathbb{N}|$ und $|\mathbb{R}|$. ◄ **UE 142**

1. Unteralgebren von $(\mathbb{N}, +, 0)$
2. Kongruenzrelationen von $(\mathbb{N}, +, 0)$
3. Unteralgebren von $(\mathbb{N}, \cdot, 1)$
4. Kongruenzrelationen von $(\mathbb{N}, \cdot, 1)$
5. Unteralgebren von $(\mathbb{N}, +, 0, \cdot, 1)$
6. Kongruenzrelationen von $(\mathbb{N}, +, 0, \cdot, 1)$

Dabei soll „möglichst alle“ heißen, dass Sie, wenn eine vollständige Beschreibung aller gesuchten Objekte zu schwierig ist, wenigstens nach gewissen Merkmalen unterscheiden und begründen, ob es jeweils ein oder mehrere Objekte mit diesen Merkmalen gibt.

Der folgende einfache Sachverhalt verbindet Addition mit Multiplikation und wird sich vielfach als äußerst wichtig erweisen.

**Satz 3.1.3.11** (Division mit Rest)**.** *Sei $m > 0$ eine positive ganze Zahl, $b$ eine beliebige ganze Zahl. Dann gibt es genau ein Paar $(q, r)$ von ganzen Zahlen mit folgenden Eigenschaften:*

- $b = qm + r$
- $0 \leq r < m$

*$q$ heißt der* Quotient*, $r$ der* Rest *der Division. Genau dann ist $r = 0$, wenn $b$ durch $m$ teilbar ist. (Man beachte, dass $b - r$ jedenfalls durch $m$ teilbar ist. ) Genau für $b \in \mathbb{N}$ ist auch $q \in \mathbb{N}$.*

*Beweis.* Existenz: Wir setzen $q := \lfloor \frac{b}{m} \rfloor$ (die größte ganze Zahl $\leq \frac{b}{m}$) und $r := b - qm$. Aus $q \leq \frac{b}{m} < q + 1$ erhalten wir $qm \leq b < qm + m$, also $0 \leq r < m$.
Eindeutigkeit: Wenn $b = qm + r = q'm + r'$ mit $0 \leq r \leq r' < m$ ist, dann gilt $0 \leq qm - q'm = r' - r < m$. Die Zahl $r' - r$ ist also durch $m$ teilbar; da alle Vielfachen von $m$ entweder $\leq 0$ oder $\geq m$ sind, und $r' - r$ im halboffenen Intervall $[0, m)$ liegt, muss $r' - r = 0$, also $r' = r$ gelten, somit auch $q = q'$.
Ist $b \geq 0$, so zeigt der Beweis der Existenz auch $q \geq 0$. Die Umkehrung ist aus $b = qm + r \geq qm$ und $m > 0$ ersichtlich. □

In der folgenden Übungsaufgabe wird dieser Satz auf beliebige $m \neq 0$ verallgemeinert.

**UE 143** ► **Übungsaufgabe 3.1.3.12.** (F) Sei $m \neq 0$ eine ganze Zahl, $b$ eine beliebige ganze Zahl. ◄ **UE 143**
Dann gibt es genau ein Paar $(q, r)$ von ganzen Zahlen mit folgenden Eigenschaften:

- $b = qm + r$
- $0 \leq r < |m|$

**Anmerkung 3.1.3.13.** Wenn $m$ und $b$ ganze Zahlen mit $b, m \neq 0$ sind, dann gibt es

- genau ein Paar $(q_1, r_1)$ von ganzen Zahlen mit $b = mq_1 + r_1$ und $0 \leq |r_1| < |m|$ und $r_1 \geq 0$
- genau ein Paar $(q_2, r_2)$ von ganzen Zahlen mit $b = mq_2 + r_2$ und $0 \leq |r_2| < |m|$ und $\mathrm{sgn}(r_2) = \mathrm{sgn}(b)$
- genau ein Paar $(q_3, r_3)$ von ganzen Zahlen mit $b = mq_3 + r_3$ und $0 \leq |r_3| < |m|$ und $\mathrm{sgn}(r_3) = \mathrm{sgn}(m)$

Sowohl die Zahl $r_1$ (die nicht negativ ist) als auch die Zahl $r_2$ (die das gleiche Vorzeichen wie $b$ hat) als auch die Zahl $r_3$ könnte man als „Rest bei Division von $b$ durch $m$“ bezeichnen, und mit $b \bmod m$ oder $b \,\%\, m$ abkürzen. Wenn Sie also diese Sprechweise oder Notation verwenden, dann stellen Sie zunächst klar, welche Definition Sie verwenden.

**Anmerkung 3.1.3.14.** Gelegentlich (etwa beim euklidischen Algorithmus) ist die folgende Variante praktischer:
Sei $m \neq 0$ eine ganze Zahl, $b$ eine beliebige ganze Zahl. Dann gibt es ein Paar $(q, r)$ von ganzen Zahlen mit folgenden Eigenschaften:

- $b = qm + r$
- $|r| \leq q/2$.

### 3.1.4 Quotienten- bzw. Differenzenmonoid

Inhalt in Kurzfassung: Hat man die Konstruktion der additiven Gruppe $\mathbb{Z}$ aus der Halbgruppe $\mathbb{N}$ vor Augen, so stellt sich die Frage, unter welchen Bedingungen sich diese Konstruktion von $\mathbb{N}$ auf beliebige Halbgruppen bzw. Monoide $M$ verallgemeinern lässt. Wie man sich schnell überzeugt, ist für die Existenz von Inversen eines Halbgruppenelements dessen Kürzbarkeit notwendig. Ist diese für alle Elemente gegeben, so ist Kommutativität hinreichend (nicht notwendig) für die Existenz einer Erweiterung zu einer Gruppe, der sogenannten Quotienten- oder (bei additiver Notation) Differenzengruppe. Varianten dieser Konstruktion betreffen die Möglichkeit, Inverse nicht für alle Elemente, sondern nur für jene aus einem kürzbaren Untermonoid zu fordern. Die resultierenden Strukturen lassen sich auch durch eine universelle Eigenschaft charakterisieren, nämlich als initiale Objekte in einer geeigneten Kategorie.

Wir erinnern uns an den Übergang von $\mathbb{N}$ zu $\mathbb{Z}$, wo ein Monoid zu einer Gruppe erweitert wurde. Dabei müssen also zumindest Inverse hinzugefügt werden. Unser Interesse wird vor allem hinreichenden Bedingungen an ein zunächst beliebiges Monoid $M$ gelten, die garantieren, dass eine analoge Konstruktion möglich ist. In Hinblick auf allgemeinere Situationen ziehen wir in Betracht, dass nur gewisse Elemente aus $M$, nämlich jene aus einer Teilmenge $K \subseteq M$, Inverse bekommen müssen. Gesucht ist zunächst also eine isomorphe Einbettung $\iota : M \to Q$ in ein Monoid $Q$, in dem sämtliche $\iota(k)$ mit $k \in K$ ein Inverses besitzen. So ein $k$ muss jedenfalls kürzbar sein: Aus $xk = yk$ folgt

$$\iota(x) = \iota(x)\iota(k)\iota(k)^{-1} = \iota(xk)\iota(k)^{-1} = \iota(yk)\iota(k)^{-1} = \iota(y)\iota(k)\iota(k)^{-1} = \iota(y),$$

wegen der Injektivität einer isomorphen Einbettung also $x = y$. Also ist $k$ rechtskürzbar, analog linkskürzbar, insgesamt also tatsächlich kürzbar. Mit $K(M)$ bezeichnen wir die Menge aller kürzbaren Elemente in $M$. Es ist eine leichte Übungsaufgabe nachzuprüfen, dass $K(M)$ stets ein Untermonoid von $M$ ist.

**UE 144** ► **Übungsaufgabe 3.1.4.1.** (F) Zeigen Sie: Sowohl die Menge $K_l(M)$ aller links- als auch die Menge $K_r(M)$ aller rechtskürzbaren Elemente in einem Monoid $M$ bilden Untermonoide. Also ist auch $K(M) = K_l(M) \cap K_r(M)$ ein Untermonoid von $M$. ◄ **UE 144**

Nach der vorangegangenen Überlegung kann es eine isomorphe Einbettung eines Monoids $M$ in eine Gruppe $G$ (so wie $\mathbb{N}$ in $\mathbb{Z}$) nur geben, wenn $M$ kürzbar ist. Dennoch wollen wir mit unseren Untersuchungen weiterhin auch allgemeinere Situationen erfassen. Zum Beispiel erweist es sich als interessant, statt isomorphen Einbettungen $\iota : M \to G$ auch beliebige Monoidhomomorphismen $\varphi : M \to Q$ zuzulassen. Wir definieren entsprechend:

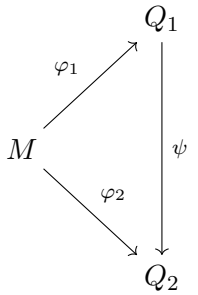
**Definition 3.1.4.2.** Seien $M$ und $Q$ Monoide und $\varphi : M \to Q$ ein Homomorphismus. Wir sagen, $(Q, \varphi)$ ist ein *Quotientenmonoid im weiteren Sinn* (*Quotientenmonoid iwS*)

bezüglich $K \subseteq M$, wenn $\varphi(k)$ für alle $k \in K$ ein Inverses $\varphi(k)^{-1}$ in $Q$ hat. Das von $\varphi(M)$ und allen $\varphi(k)^{-1}$, $k \in K$, erzeugte Untermonoid von $Q$ bezeichnen wir mit $Q_{(M,\varphi)}$.
Für gegebenes $\varphi : M \to Q$ bezeichnen wir mit $K(Q, \varphi)$ die Menge aller $k \in M$, für die $\varphi(k)$ ein Inverses in $Q$ hat.

Sehr leicht sieht man ein:

**UE 145** ► **Übungsaufgabe 3.1.4.3.** (F) Mit den Notationen aus Definition 3.1.4.2 gilt $K(Q, \varphi) \leq M$. Ist $\varphi$ überdies eine isomorphe Einbettung, so gilt auch $K(Q, \varphi) \leq K(M)$. ◄ **UE 145**

Sucht man zu vorgegebenem $K \subseteq M$ ein $(Q, \varphi)$ mit $K \subseteq K(Q, \varphi)$, so kann man sich folglich auf jene $K$ beschränken, die Untermonoide $K \leq M$ sind. Für gegebenes $K \subseteq M$ definieren wir die folgende Kategorie $\mathcal{C}(M, K)$.
Die Objekte in $\mathcal{C}(M, K)$ seien von der Gestalt $(Q, \varphi)$, wobei $\varphi\colon M \to Q$ ein Monoidhomomorphismus ist derart, dass jedes $\varphi(k)$ mit $k \in K$ in $Q$ ein Inverses besitzt. Die Morphismen bezüglich $\mathcal{C}(M, K)$ von einem Objekt $(Q_1, \varphi_1)$ in ein Objekt $(Q_2, \varphi_2)$ seien jene Monoidhomomorphismen $\psi\colon Q_1 \to Q_2$, für die $\varphi_2 = \psi \circ \varphi_1$ gilt.




Die Komposition in $\mathcal{C}(M, K)$ sei die übliche Komposition von Abbildungen.

**UE 146** ► **Übungsaufgabe 3.1.4.4.** (V) Überzeugen Sie sich davon, dass $\mathcal{C}(M, K)$ tatsächlich eine Kategorie ist. Darin sind zwei Objekte $(Q_1, \varphi_1)$ und $(Q_2, \varphi_2)$ genau dann äquivalent, wenn es einen Monoidisomorphismus $\psi : Q_1 \to Q_2$ gibt mit $\varphi_2 = \psi \circ \varphi_1$. Insbesondere sind in diesem Fall $Q_1$ und $Q_2$ als Monoide isomorph. ◄ **UE 146**

Wir erinnern uns nochmals an die Situation $M = K = \mathbb{N}$ und $Q = \mathbb{Z}$. Die Inklusionsabbildung $\iota : \mathbb{N} \to \mathbb{Z}$ hat nach Satz 1.2.1.1 die Eigenschaft, dass es zu jeder isomorphen Einbettung $\iota' : \mathbb{N} \to G$ des additiven Monoids $\mathbb{N}$ in eine Gruppe $G$ eine eindeutige isomorphe Gruppeneinbettung $\psi : \mathbb{Z} \to G$ mit $\iota' = \psi \circ \iota$ gibt. Hätten wir in der Definition der Kategorie $\mathcal{C}(M, Q)$ als Morphismen nicht beliebige Monoidhomomorphismen zugelassen, sondern nur isomorphe Einbettungen, so würde diese Eigenschaft $(\mathbb{Z}, \iota)$ als ein initiales Objekt auszeichnen. Zur Anpassung an unsere Situation fühlen wir uns zu folgender Definition motiviert:

**Definition 3.1.4.5.** Sei $\varphi\colon M \to Q$ ein Monoidhomomorphismus und $K \leq M$ ein Untermonoid von $M$. Ist $(Q, \varphi)$ eine initiales Objekt in der Kategorie $\mathcal{C}(M, K)$, so heißt $Q$ zusammen mit $\varphi$ (formal: das Paar $(Q, \varphi)$) ein *Quotientenmonoid im eigentlichen Sinn* (Quotientenmonoid ieS) oder schlicht *Quotientenmonoid* von $M$ bezüglich $K$. Ist außerdem $K = M$, so heißt $Q$ zusammen mit $\varphi$ eine *Quotientengruppe* des Monoids $M$. Wenn $M$ kommutativ ist und die Verknüpfung additiv geschrieben wird, dann spricht man statt von einem Quotientenmonoid bzw. einer Quotientengruppe vorzugsweise von einem *Differenzenmonoid* bzw. einer *Differenzengruppe*.

Nach Satz 2.2.3.2 sind initiale Objekte in einer Kategorie eindeutig bis auf Äquivalenz. Somit sind zu gegebenem $M$ und $K$ sämtliche Quotienten- bzw. Differenzenmonoide von $M$ bezüglich $K$ zueinander äquivalent, insbesondere als Monoide isomorph.
Der allgemeinen Konstruktion für den kommutativen kürzbaren Fall vorgreifend sei schon an dieser Stelle empfohlen, sich zur Übung davon zu überzeugen, dass $\mathbb{Z}$ zusammen mit der Inklusionsabbildung $\iota : \mathbb{N} \to \mathbb{Z}$ eine Differenzengruppe des additiven Monoids $\mathbb{N}$ auch im Sinn von Definition 3.1.4.5 ist.

**UE 147** ► **Übungsaufgabe 3.1.4.6.** (V) Beweisen Sie diese Behauptung. (Beachten Sie, dass in Definition 3.1.4.5 im Gegensatz zu Theorem 1.2.1.1 beliebige Homomorphismen und nicht nur isomorphe Einbettungen zugelassen sind.) ◄ **UE 147**

Zur Illustration des konträren Phänomens betrachte man auch das folgende Beispiel. Auf der zweielementigen Menge $H := \{0, 1\}$ definiert $xy := x$ eine nichtkommutative Halbgruppenoperation. Adjunktion eines neutralen Elementes $e$ ergibt nach Proposition 3.1.1.9 ein Monoid $M = \{e, 0, 1\}$. Das einelementige Monoid $\{e\}$ zusammen mit der konstanten Abbildung $M \to \{e\}$ erweist sich als Quotientenmonoid von $M$ (Übung). Es liegt also ein Beispiel eines Monoids vor, das erstens nicht isomorph in sein Quotientenmonoid eingebettet wird, und zweitens ein (in diesem Fall auf triviale Weise) kommutatives Quotientenmonoid hat, obwohl es selbst nicht kommutativ ist.

**UE 148** ► **Übungsaufgabe 3.1.4.7.** (V) Verifizieren Sie die Behauptungen aus dem vorangegangenen Absatz. ◄ **UE 148**

Dass wir uns bei der Definition von Quotientenmonoiden nicht auf isomorphe Einbettungen beschränkt haben, hat seine Motivation in Satz 3.1.4.8, wonach Quotientenmonoide im Sinne von Definition 3.1.4.5 uneingeschränkt existieren. Die Frage, wann man sogar isomorphe Einbettungen garantieren kann, wird uns danach beschäftigen. Der Beweis von Satz 3.1.4.8 verwendet eine Methode, die auf ähnliche Weise in vielen verwandten Situationen angewendet werden kann, etwa bei der Konstruktion von Quotientenringen und -körpern in 3.4.5. Auch bei der zweiten Konstruktion einer freien Algebra in 4.1.6 werden wir ganz ähnlich vorgehen, und im Beweis des Darstellungssatzes für Boolesche Algebren 3.6.8.13 klingen ebenfalls verwandte Ideen an. Und zwar wird ein sogenanntes *subdirektes Produkt*, das heißt eine Unteralgebra eines (großen) direkten Produktes, konstruiert, die zusammen mit einem sich zwanglos ergebenden Homomorphismus die gewünschten Eigenschaften hat.

**Satz 3.1.4.8.** *Sei $M$ ein Monoid und $K \subseteq M$. Dann gibt es ein Quotientenmonoid von $M$ bezüglich $K$.*

*Beweis.* Sei $\mathcal{C} = \mathcal{C}(M, K)$ die Kategorie aus Definition 3.1.4.5, in der wir ein initiales Objekt $(Q_0, \varphi_0)$ finden müssen.
Wir beginnen mit folgender Beobachtung: Ist $X$ eine unendliche Menge mit $|M| \leq |X|$, so lassen sich alle Objekte $(Q, \varphi)$ aus $\mathcal{C}$ im Wesentlichen auf Teilmengen von $X$ realisieren. Damit ist Folgendes gemeint: Für gegebenes $(Q, \varphi)$ bezeichne $Q_{(M,\varphi)}$ wieder das von $T := \varphi(M) \cup \{\varphi(k)^{-1} : \ k \in K\}$ erzeugte Untermonoid von $Q$. Ist $M$ endlich, so auch $T$, womit $Q_{(M,\varphi)}$ wegen Proposition 2.3.1.13 höchstens abzählbar unendlich ist, also $|Q_M| \leq |X|$. Für unendliches $M$ gilt $|T| = |M|$ (siehe 11.4.8 im Anhang), wieder nach 2.3.1.13 also ebenfalls $|Q_{(M,\varphi)}| = |T| = |M| \leq |X|$. Daher gibt es eine Injektion $f : Q_{(M,\varphi)} \to X$. Definieren wir[3] $f(q) \cdot f(q') := f(q \cdot q')$ für $q, q' \in Q_{(M,\varphi)}$, sowie $e_Y := f(e_{Q_{(M,\varphi)}})$, so erhalten wir wohldefinierte Operationen auf $Y := f(Q_{(M,\varphi)}) \subseteq X$, mit denen $Y$ zu einem zu $Q_{(M,\varphi)}$ isomorphen Monoid wird.
Sei nun $X$ eine Menge wie in der Beobachtung oben, d.h. mit $|M| \leq |X|$. Wir schränken die Kategorie $\mathcal{C}$ ein auf die Unterkategorie $\mathcal{C}_X$, deren Objekte nur jene Objekte $(Q, \varphi)$ von $\mathcal{C}$ sind, für die $Q \subseteq X$ gilt. Morphismen und Komposition zwischen Objekten in $\mathcal{C}_X$ seien jene aus $\mathcal{C}$. Die Objekte $(Q, \varphi)$ von $\mathcal{C}_X$ bilden sogar eine Menge[4] $\mathcal{Q}$. Wegen $1 \leq |M| \leq |X|$ ist $X$ nicht leer. Somit enthält auch $\mathcal{Q}$ wenigstens ein Element $(Q, \varphi)$, wobei $Q$ ein einelementiges Monoid und $\varphi : M \to Q$ der konstante Homomorphismus ist. Wir betrachten das direkte Produkt

$$P := \prod_{(Q,\varphi)\in\mathcal{Q}} Q$$

und den Homomorphismus

$$\varphi_0 : M \to P, \quad m \mapsto (\varphi(m))_{(Q,\varphi)\in\mathcal{Q}}.$$

Wir behaupten, dass $(Q_0, \varphi_0)$ mit $Q_0 := \varphi_0(M) \leq P$ (subdirektes Produkt) die gewünschten Eigenschaften hat, d.h. ein initiales Objekt in $\mathcal{C}$ ist.
Sei dazu $(Q, \varphi)$ irgendein Objekt in $\mathcal{C}$, also $\varphi : M \to Q$ ein Monoidhomomorphismus derart, dass alle $\varphi(k)$, $k \in K$, ein Inverses in $Q$ haben. Wie weiter oben bezeichne $Q_{(M,\varphi)}$ das von diesen Inversen und $\varphi(M)$ erzeugte Untermonoid von $Q$. Nach dem obigen Argument gibt es ein Monoid $Y \subseteq X$, das vermöge einer Abbildung $f : Q_{(M,\varphi)} \to Y$ isomorph zu $Q_{(M,\varphi)}$ ist. Dann ist $(Y, f \circ \varphi) \in \mathcal{Q}$, entspricht also einer Komponente im Produkt $P$. Bezeichne $\pi : Q_0 \to Y$ die Projektion auf diese Komponente. Nach Konstruktion ist $f^{-1} \circ \pi : Q_0 \to Q_{(M,\varphi)} \subseteq Q$ ein Homomorphismus, der $\varphi = (f^{-1} \circ \pi) \circ \varphi_0$ erfüllt und durch diese Eigenschaft sogar eindeutig bestimmt ist. Genau das war zu beweisen. □

[3] Die Wohldefiniertheit folgt aus der Injektivität von $f$.
[4] Das liegt daran, dass wir es mit Teilmengen einer festen Menge zu tun haben, womit – salopp formuliert – es nicht zu viele Objekte gibt.

**UE 149** ► **Übungsaufgabe 3.1.4.9.** (F) Zeigen Sie: Ist $(Q, \varphi)$ ein Quotientenmonoid von $M$ bezüglich $K$, dann wird $Q$ als Monoid von der Menge $\varphi(M) \cup \{\varphi^{-1}(k) : k \in K\}$ erzeugt, es gilt also $Q = Q_{(M,\varphi)}$ (Bezeichnungsweise wie in Definition 3.1.4.2). ◄ **UE 149**

Nach Satz 3.1.4.8 existieren Quotientenmonoide $(Q, \varphi)$ im Sinne von Definition 3.1.4.5 also stets, d.h. für ein beliebig gegebenes Monoid $M$ und Untermonoid $K \leq M$. Wir haben aber bereits gesehen, dass es sich keineswegs immer um isomorphe Einbettungen (wie von $\mathbb{N}$ in $\mathbb{Z}$) handeln muss. Insbesondere ist dafür notwendig, dass $K$ kürzbar ist, was wir in Satz 3.1.4.8 nicht voraussetzen mussten. Eine Untersuchung der einzelnen Schritte in der Konstruktion von $\mathbb{Z}$ aus $\mathbb{N}$, wie sie in 1.2.1 behandelt wurde, zeigt sehr schnell, dass auch von der Kommutativität der Addition auf $\mathbb{N}$ Gebrauch gemacht wurde. Sie ist zwar nicht immer notwendig für die Möglichkeit einer Erweiterung eines Monoids $M$ zu einer Gruppe (beispielsweise könnte $M$ selbst bereits eine nichtabelsche Gruppe sein). Dass wir Sie ab nun voraussetzen werden, liegt jedoch nicht an unserer Wahl der Konstruktion in Satz 3.1.4.11: Es gäbe ohne diese Voraussetzung (wenn auch recht komplizierte) Gegenbeispiele.
Wir kommen nun zu der angekündigten alternativen Konstruktion des Quotientenmonoids unter der Voraussetzung, dass das gegebene Monoid $M$ abelsch und das Untermonoid $K \leq M$ kürzbar ist. Im Vergleich zur allgemeineren Konstruktion aus Satz 3.1.4.8 entspricht diese Konstruktion derjenigen von $\mathbb{Z}$ aus $\mathbb{N}$ und ist somit wesentlich konkreter fasslich. Eine technische Komplikation wird sich daraus ergeben, dass Quotientenmonoide im weiteren Sinne im Allgemeinen nicht abelsch sind. Die folgende Übungsaufgabe zeigt allerdings, dass der „wesentliche“ Teil eines Quotientenmonoids im weiteren Sinne sehr wohl abelsch ist, wenn wir von einem abelschen Monoid ausgehen.

**UE 150** ► **Übungsaufgabe 3.1.4.10.** (F) Sei $M$ ein Monoid, $K \leq M$ und $(Q, \varphi)$ ein Quotientenmonoid im weiteren Sinn von $M$ bezüglich $K$ und $Q_{(M,\varphi)}$ wie in Definition 3.1.4.2. Zeigen Sie: Ist $M$ abelsch, dann auch $Q_{(M,\varphi)}$. ◄ **UE 150**

**Satz 3.1.4.11.** *Sei $M$ ein abelsches Monoid und $K \leq M$ ein kürzbares Untermonoid. Dann wird auf dem direkten Produkt $S := M \times K$ durch*

$$(m_1, k_1) \sim (m_2, k_2) :\Leftrightarrow m_1 k_2 = m_2 k_1, \quad m_1, m_2 \in M,\ k_1, k_2 \in K,$$

*eine Kongruenzrelation definiert. Die Abbildung $\iota\colon M \to Q := S/_\sim$, $m \mapsto [(m, 1)]_\sim$, ist eine isomorphe Einbettung des Monoids $M$ in $Q$. Das Faktormonoid $Q := S/_\sim$ bildet zusammen mit $\iota$ ein Quotientenmonoid von $Q$ bezüglich $K$.*

*Beweis.* Die Relation $\sim$ ist auf $S$ klarerweise reflexiv und symmetrisch. Die Transitivität ergibt sich so: $(m_1, k_1) \sim (m_2, k_2)$ und $(m_2, k_2) \sim (m_3, k_3)$ bedeutet $m_1 k_2 = m_2 k_1$ und $m_2 k_3 = m_3 k_2$. Daraus folgt (u.a. wegen der Kommutativität) $m_1 k_2 k_3 = m_2 k_1 k_3 = m_3 k_1 k_2$. Die Kürzbarkeit von $k_2$ liefert $m_1 k_3 = m_3 k_1$ also $(m_1, k_1) \sim (m_3, k_3)$. Also ist $\sim$ transitiv und somit eine Äquivalenzrelation.
Um die Verträglichkeit von $\sim$ mit der binären Operation nachzuweisen, seien $(m_1, k_1) \sim (m_1', k_1')$ (also $m_1 k_1' = m_1' k_1$) und $(m_2, k_2) \sim (m_2', k_2')$ (also $m_2 k_2' = m_2' k_2$). Zu zeigen ist

$(m_1m_2, k_1k_2) \sim (m_1'm_2', k_1'k_2')$. Das folgt unter abermaliger Verwendung der Kommutativität tatsächlich aus $m_1m_2k_1'k_2' = (m_1k_1')(m_2k_2') = (m_1'k_1)(m_2'k_2) = m_1'm_2'k_1k_2$. Somit ist $\sim$ eine Kongruenzrelation.
Also dürfen wir das Faktormonoid $Q := S/_\sim$ bilden und darin gemäß der Rechenregel $[(m_1, k_1)]_\sim \cdot [(m_2, k_2)]_\sim = [(m_1m_2, k_1k_2)]_\sim$ rechnen. Für $k_1 = k_2 = 1$ folgt daraus speziell die Homomorphiebedingung

$$\iota(m_1m_2) = [(m_1m_2, 1)]_\sim = [(m_1, 1)]_\sim \cdot [(m_2, 1)]_\sim = \iota(m_1) \cdot \iota(m_2).$$

Klarerweise bildet $\iota$ das Einselement $1 \in M$ auf das Einselement $[(1, 1)]_\sim \in Q$ ab.
Die Injektivität von $\iota$ ergibt sich so: Aus $\iota(m_1) = \iota(m_2)$ folgt $[(m_1, 1)]_\sim = [(m_1, 1)]_\sim$, d.h. $(m_1, 1) \sim (m_2, 1)$ oder $m_1 = m_11 = 1m_2 = m_2$. Damit ist gezeigt, dass $\iota : M \to Q$ eine isomorphe Einbettung ist.
Für $k \in K$ gilt

$$\iota(k) \cdot [(1, k)]_\sim = [(k, 1)] \cdot [(1, k)]_\sim = [(k, k)]_\sim = [(1, 1)]_\sim.$$

Also hat $\iota(k)$ in $Q$ das Inverse $[(1, k)]_\sim$. Somit ist $(Q, \iota)$ Quotientenmonoid im weiteren Sinne, also ein Objekt der Kategorie $\mathcal{C}(M, K)$ aus Definition 3.1.4.5.
Zu zeigen bleibt, dass $(Q, \iota)$ in $\mathcal{C}(M, K)$ sogar ein initiales Objekt ist. Sei dazu $(Q', \varphi)$ irgendein anderes Quotientenmonoid im weiteren Sinne. Wir müssen zeigen, dass es einen eindeutigen Homomorphismus $\psi : Q \to Q'$ gibt mit $\varphi = \psi \circ \iota$.
Ein beliebiges Element in $Q$ ist von der Gestalt $[(m, k)]_\sim$ mit $m \in M$ und $k \in K$. Nach Definition von $\mathcal{C}(M, K)$ hat $\varphi(k)$ ein Inverses in $Q'$. Wir setzen daher

$$\psi : [(m, k)]_\sim \mapsto \varphi(m)\varphi(k)^{-1}.$$

Der Beweis des Satzes ist erbracht, wenn wir Wohldefiniertheit, Homomorphieeigenschaft und Eindeutigkeit von $\psi$ zeigen.
Zur Wohldefiniertheit von $\psi$: Zu zeigen ist, dass aus $[(m_1, k_1)]_\sim = [(m_2, k_2)]_\sim$ stets $\varphi(m_1)\varphi(k_1)^{-1} = \varphi(m_2)\varphi(k_2)^{-1}$ folgt. Tatsächlich bedeutet $[(m_1, k_1)]_\sim = [(m_2, k_2)]_\sim$ nichts anderes als $m_1k_2 = m_2k_1$. Wir wenden $\varphi$ an und erhalten

$$\varphi(m_1)\varphi(k_2) = \varphi(m_1k_2) = \varphi(m_2k_1) = \varphi(m_2)\varphi(k_1).$$

Wir müssen also durch $\varphi(k_1)$ und $\varphi(k_2)$ kürzen – dazu beachten wir, dass die Elemente $\varphi(m_1), \varphi(m_2), \varphi(k_1)^{-1} \in M_{(Q,\varphi)}$ nach Übungsaufgabe 3.1.4.10 miteinander kommutieren, und multiplizieren obige Gleichung von links mit $\varphi(k_1)^{-1}$ und von rechts mit $\varphi(k_2)^{-1}$, um

$$\begin{aligned}\varphi(m_1)\varphi(k_1)^{-1} = \varphi(k_1)^{-1}\varphi(m_1) &= \varphi(k_1)^{-1}\varphi(m_2)\varphi(k_1)\varphi(k_2)^{-1} \\ &= \varphi(m_2)\varphi(k_1)^{-1}\varphi(k_1)\varphi(k_2)^{-1} = \varphi(m_2)\varphi(k_2)^{-1}\end{aligned}$$

zu erhalten.

Zur Homomorphieeigenschaft von $\psi$: Mit Hilfe der Wohldefiniertheit von $\psi$ und der Homomorphieeigenschaft von $\iota'$ ergibt sich auch jene von $\psi$:

$$\begin{aligned}\psi([(m_1,k_1)]_\sim\cdot[(m_2,k_2)]_\sim) &= \psi([(m_1m_2,k_1k_2]_\sim) = \varphi(m_1m_2)\varphi(k_1k_2)^{-1} = \\ &= \varphi(m_1m_2)\Big(\varphi(k_1)\varphi(k_2)\Big)^{-1} = \varphi(m_1m_2)\varphi(k_2)^{-1}\varphi(k_1)^{-1} \\ &= \varphi(m_1)\varphi(m_2)\varphi(k_1)^{-1}\varphi(k_2)^{-1} = \varphi(m_1)\varphi(k_1)^{-1}\varphi(m_2)\varphi(k_2)^{-1} \\ &= \psi([(m_1,k_1)]_\sim\cdot\psi([(m_2,k_2)]_\sim\end{aligned}$$

Die hier verwendeten Kommutativitäten ergeben sich wieder aus Übungsaufgabe 3.1.4.10. Abschließend zur Eindeutigkeit von $\psi$: Jedes Element $q \in Q$ ist von der Gestalt $q = [(m,k)]_\sim = m_Q k_Q^{-1}$ mit $m_Q := \iota(m)$ und $k_Q := \iota(k)$. Wenn $\varphi = \tilde{\psi} \circ \iota$ gilt, bedeutet das zunächst, dass $\tilde{\psi}(m_Q) = \tilde{\psi}(\iota(m)) = \varphi(m) = \psi(\iota(m)) = \psi(m_Q)$ gilt; analog auch $\tilde{\psi}(k_Q) = \psi(k_Q)$. Wir erhalten unter Verwendung von $\tilde{\psi}(k_Q^{-1}) = \tilde{\psi}(k_Q)^{-1}$ sowie der analogen Tatsache für $\psi$ (siehe Proposition 3.1.1.5)

$$\tilde{\psi}(q) = \tilde{\psi}(m_Q k_Q^{-1}) = \tilde{\psi}(m_Q)\tilde{\psi}(k_Q)^{-1} = \psi(m_Q)\psi(k_Q)^{-1} = \psi(m_Q k_Q^{-1}) = \psi(q),$$

also die Eindeutigkeit von $\psi$ bei vorgegebenem $\varphi$. □

Die Eindeutigkeit initialer Objekte modulo Äquivalenz nehmen wir als Rechtfertigung dafür, einfach von *dem* Quotientenmonoid zu sprechen. Seine Elemente schreibt man oft als Brüche $\frac{m}{k} = mk^{-1} = [(m,k)]_\sim$ mit der Notation aus Satz 3.1.4.11.

## 3.2 Gruppen

Eine der wichtigsten, wenn nicht die wichtigste Klasse algebraischer Strukturen ist die der Gruppen. In diesem Abschnitt beschäftigen wir uns zunächst mit den gruppentheoretischen Spezifika der in Abschnitt 2.3 in allgemeinem Rahmen behandelten Konzepte algebraischer Strukturanalyse: Unterstrukturen in 3.2.1, Faktorisierung in 3.2.2 und direkte Produkte in 3.2.3. Sodann untersuchen wir einige wichtige und in gewisser Hinsicht sehr repräsentative, konkrete Beispiele: Die additive Gruppe $\mathbb{Z}$ (3.2.4), Permutationsgruppen (3.2.5) und Gruppen, die unterschiedlichen Strukturtheorien entstammen (3.2.6).

### 3.2.1 Nebenklassenzerlegung

Inhalt in Kurzfassung: Jede Untergruppe induziert zwei Partitionen der Gruppe, nämlich in Links- und in Rechtsnebenklassen, von denen jeweils eine die Untergruppe selbst ist. Alle Nebenklassen haben die gleiche Mächtigkeit wie die Untergruppe, und es gibt gleich viele Links- wie Rechtsnebenklassen. Deren Anzahl nennt man den Index der Untergruppe in der Gruppe. Offensichtlich folgt: Die Ordnung (= Kardinalität) der Gruppe ist das Produkt aus der Ordnung der Untergruppe und dem Index. Daraus ergibt sich für endliche Gruppen der Satz von Lagrange: Die Ordnung einer Untergruppe ist Teiler der Ordnung der Gruppe.

Wir beginnen mit der Ordnung einer Gruppe und ihrer Elemente sowie daran anknüpfenden Begriffen.

**Definition 3.2.1.1.** Sei $G$ eine Gruppe. Dann nennt man die Kardinalität $|G|$ die *Ordnung* von $G$. Unter der *Ordnung eines Elements* $g \in G$ versteht man die Ordnung $|\langle g\rangle|$ der von $g$ erzeugten Untergruppe. Wir schreiben dafür $\mathrm{ord}(g)$. Offenbar kommen für $\mathrm{ord}(g)$ genau die Kardinalitäten aus $\mathbb{N}^+$ sowie $\aleph_0$ in Frage. Statt $\mathrm{ord}(g) = \aleph_0$ schreibt man vorzugsweise $\mathrm{ord}(g) = \infty$. Ist $\mathrm{ord}(g) < \infty$ endlich, so heißt $g \in G$ ein *Torsionselement*. Gilt sogar $\mathrm{ord}(g) = p^n$ mit $p \in \mathbb{P}$ und $n \in \mathbb{N}$, so heißt $g$ ein *$p$-Element*. $G$ heißt eine *$p$-Gruppe*, wenn jedes $g \in G$ ein $p$-Element ist. $G$ heißt eine *Torsionsgruppe*, wenn jedes $g \in G$ ein Torsionselement ist. $G$ heißt *zyklisch*, wenn es ein $g \in G$ (ein sogenanntes *erzeugendes Element* von $G$) gibt mit $G = \langle g\rangle$.

Gemäß der allgemeinen Definition 2.3.1.1 von Unteralgebren ist eine Teilmenge $U \subseteq G$ einer Gruppe $G$ genau dann eine Untergruppe, wenn sie abgeschlossen ist bezüglich aller drei Operationen, der binären Gruppenoperation (wenn also aus $a, b \in U$ stets $ab \in U$ folgt), der nullstelligen (wenn also das neutrale Element $1_G \in G$ auch in $U$ liegt) und der unären (wenn also mit jedem $a \in U$ auch das Inverse $a^{-1}$ in $U$ liegt). Ein Spezifikum der Gruppen mit sehr interessanten Konsequenzen besteht darin, dass jede Untergruppe $U \leq G$ in natürlicher Weise Zerlegungen von $G$ in gleich große Teile induziert, von denen einer $U$ selbst ist.

**Definition 3.2.1.2.** Sei $G$ eine Gruppe und $U \leq G$ eine Untergruppe von $G$. Für jedes Element $g \in G$ nennen wir

$$gU := \{gu : u \in U\}$$

die *Linksnebenklasse* von $g$ (modulo $U$, nach $U$, bzgl. $U$ u.ä.). Analog definieren wir die *Rechtsnebenklasse* $Ug := \{ug : u \in U\}$.

**Proposition 3.2.1.3.** *(*Nebenklassenzerlegung einer Gruppe nach einer Untergruppe*) Seien $G$ eine Gruppe und $U \leq G$, $g_1, g_2 \in G$. Für die Linksnebenklassen nach $U$ gilt entweder $g_1U = g_2U$ (nämlich genau dann, wenn $g_1^{-1}g_2 \in U$) oder $g_1U \cap g_2U = \emptyset$. Die Linksnebenklassen nach $U$ bilden eine Partition von $G$. Analoges gilt für die Rechtsnebenklassen, wobei $Ug_1 = Ug_2$ genau dann gilt, wenn $g_1g_2^{-1} \in U$.*

*Beweis.* Wir zeigen die Aussage für Linksnebenklassen. Die Nebenklassen $g_1U$ und $g_2U$ haben genau dann nichtleeren Schnitt, wenn es $u_1, u_2 \in U$ gibt zu $g_1u_1 = g_2u_2$. Für beliebiges $u_3 \in U$ folgt daraus

$$g_2u_3 = g_2u_2u_2^{-1}u_3 = g_1u_1u_2^{-1}u_3 \in g_1U.$$

Also gilt $g_2U \subseteq g_1U$, aus Symmetriegründen $g_1U \subseteq g_2U$, also $g_1U = g_2U$. Somit sind verschiedenen Linksnebenklassen zueinander disjunkt. Wegen $g \in gU$ für alle $g \in G$ ist die Vereinigung aller Linksnebenklassen ganz $G$, und es liegt tatsächlich eine Partition von $G$ vor. Mit der Beobachtung, dass $g_1U = g_2U$ äquivalent ist mit $U = g_1^{-1}g_2U$ und somit $g_1^{-1}g_2 \in U$, ist der Beweis der Aussage für Linksnebenklassen erbracht. Der für Rechtsnebenklassen verläuft völlig analog. □

**Satz 3.2.1.4** (Satz von Lagrange)**.** *Sei $G$ eine Gruppe und $U \leq G$.*

1. *Die durch $x \sim y \;:\Leftrightarrow\; xU = yU \;\Leftrightarrow\; x^{-1}y \in U$ definierte Relation ist eine Äquivalenzrelation auf $G$. Die Klasse von $g \in G$ ist genau die Linksnebenklasse $gU$. Die analoge Aussage gilt für Rechtsnebenklassen.*

2. *Für alle Links- und Rechtsnebenklassen gilt $|gU| = |U| = |Ug|$.*

3. *Ist $G$ endlich und $U \leq G$, so ist $|U|$ ein Teiler von $|G|$. („Untergruppenordnung teilt Gruppenordnung“)*

4. *Ist $G$ endlich und $g \in G$, so ist $\operatorname{ord}(g) = |\langle g\rangle|$ ein Teiler von $|G|$. („Elementordnung teilt Gruppenordnung“)*

*Beweis.* 1. Proposition 3.2.1.3.

2. Für jede Linksnebenklasse $gU$ ist die Abbildung $x \mapsto gx$ eine Bijektion zwischen $U$ und $gU$, weil sie mit $x \mapsto g^{-1}x$ eine Inverse besitzt. Folglich sind alle Linksnebenklassen $gU$, $g \in G$, zu $U$ und somit auch zueinander gleichmächtig. Analoges gilt für Rechtsnebenklassen, also auch $|g_1U| = |U| = |Ug_2|$ für beliebige $g_1, g_2 \in G$.

3. Folgt aus den vorigen Punkten: Sei $|U| = n$ und $k$ die Anzahl der Äquivalenzklassen. Wegen 2. haben alle Klassen die Kardinalität $n$, folglich ist $|G| = nk$.

4. Aussage 3 auf die von $g$ erzeugte Untergruppe $U := \langle g\rangle$ anwenden. □

Ist $G$ nicht abelsch, so müssen Links- und Rechtsnebenklassen nicht übereinstimmen. Man findet aber sehr leicht eine Bijektion:

**UE 151** ► **Übungsaufgabe 3.2.1.5.** (F) Zeigen Sie, dass es zu gegebenem $U \leq G$ ($G$ Gruppe) gleich viele Links- wie auch Rechtsnebenklassen gibt. (Beachten Sie, dass Ihr Beweis auch im unendlichen Fall gelten soll. Hinweis: Die Abbildung $aU \mapsto Ua^{-1}$ ist wohldefiniert und eine Bijektion.) ◄ **UE 151**

Deshalb gibt es in $G$ gleich viele Links- wie Rechtsnebenklassen von $U \leq G$.

**Definition 3.2.1.6.** Ist $G$ eine Gruppe und $U \leq G$, so nennt man diese Kardinalität (nämlich der Menge aller Linksnebenklassen oder, äquivalent, aller Rechtsnebenklassen) den *Index* von $U$ in $G$. Man schreibt dafür $[G : U]$.

Wegen der zweiten Aussage in Satz 3.2.1.4 gilt[5] $|G| = |U| \cdot [G : U]$. Ist $G$ endlich, so folgt daraus $[G : U] = \frac{|G|}{|U|}$.

[5] Wir setzen $n \cdot \infty = \infty \cdot n := \infty$.

### 3.2.2 Faktorgruppen und Normalteiler

Inhalt in Kurzfassung: Im Zusammenhang mit Kongruenzrelationen und Faktoralgebren ist bei Gruppen eine Beobachtung zentral: Kennt man die Kongruenzklasse des neutralen Elementes, so kennt man die gesamte Partition (Kongruenzrelation). Deshalb spielen jene Teilmengen von Gruppen eine besondere Rolle, die als Kongruenzklassen des neutralen Elements auftreten. Sie heißen Normalteiler und sind dadurch charakterisiert, dass es sich bei ihnen um Untergruppen handelt, für die überdies Links- und Rechtsnebenklassenzerlegung übereinstimmen oder, äquivalent, die invariant bezüglich sämtlicher innerer Automorphismen sind. Zahlreiche interessante Sachverhalte lassen sich mit Hilfe von Normalteilern einfach formulieren. Wichtige Beispiele dafür sind die Isomorphiesätze. Der vorliegende Unterabschnitt bringt aber auch einige andere einfache Sachverhalte, die in der Gruppentheorie immer wieder nützlich sind.

Aufgrund des Homomorphiesatzes hängen in beliebigen universellen Algebren Homomorphismen aufs Engste mit Kongruenzrelationen und somit mit Faktoralgebren zusammen. Für die Klasse der Gruppen treten auch diesbezüglich zahlreiche Besonderheiten auf, mit denen wir uns nun beschäftigen wollen. Erste einfache, aber immer wieder hilfreiche Beobachtungen sind die folgenden.

**Proposition 3.2.2.1.** *Seien $G, H$ Gruppen, $\sim$ eine Äquivalenzrelation auf $G$ und $f\colon G \to H$ eine Abbildung.*

1. *Ist $f$ ein Homomorphismus bezüglich der binären Operation auf $G$, dann sogar schon Gruppenhomomorphismus.*
2. *Ist $\sim$ eine Kongruenzrelation auf $G$ bezüglich der binären Operation, dann sogar bezüglich der Gruppenstruktur.*

*Beweis.* Die erste Behauptung folgt aus der dritten Aussage in Proposition 3.1.1.5. Die zweite ist eine einfache Übungsaufgabe. □

**UE 152 ▶ Übungsaufgabe 3.2.2.2.** (F+) Beweisen Sie die zweite Behauptung in 3.2.2.1. **◀ UE 152**

Wir beginnen unser Studium von Kongruenzrelationen. Ähnlich wie bei Ringen, für die wir die analoge Frage schon im Einleitungskapitel diskutiert haben (siehe Proposition 1.2.3.4), lässt sich die Situation bei Gruppen besonders einfach beschreiben, nämlich durch die Äquivalenzklasse des neutralen Elements. Zuvor die zugehörige Definition:

**Definition 3.2.2.3.** Eine Teilmenge $N$ der Gruppe $G$ heißt *Normalteiler* von $G$, symbolisch $N \lhd G$, wenn eine und damit alle der zueinander äquivalenten Bedingungen im folgenden Satz 3.2.2.4 erfüllt sind.[6]

**Satz 3.2.2.4.** *Sei $(G, \cdot, 1, ^{-1})$ eine Gruppe und $N \subseteq G$. Dann sind die folgenden Aussagen äquivalent:*

[6] Achtung: die Relation $\lhd$ ist reflexiv, dennoch schreibt man üblicherweise $\lhd$ und nicht $\trianglelefteq$.

(1) *Es gibt genau eine Kongruenzrelation* $\sim$ *auf* $G$ *mit* $N = [1]_\sim$.

(1′) *Es gibt eine Kongruenzrelation* $\sim$ *auf* $G$ *mit* $N = [1]_\sim$.

(2) *Es gibt eine Gruppe* $H$ *und einen Homomorphismus* $\varphi\colon G \to H$ *mit* $N = \varphi^{-1}(\{1_H\})$.

(2′) *Es gibt eine Gruppe* $H$ *und einen surjektiven Homomorphismus* $\varphi\colon G \to H$ *mit* $N = \varphi^{-1}(\{1_H\})$.

(3) $N$ *ist eine Untergruppe von* $G$ *mit* $xNx^{-1} = N$ *für alle* $x \in G$.

(3′) $N$ *ist eine Untergruppe von* $G$ *mit* $xNx^{-1} \subseteq N$ *für alle* $x \in G$.

(4) $N$ *ist eine Untergruppe von* $G$ *mit* $xN = Nx$ *für alle* $x \in G$.

(4′) $N$ *ist eine Untergruppe von* $G$ *mit* $xN \subseteq Nx$ *für alle* $x \in G$.

*Beweis.* Wir führen den Beweis der Äquivalenz zyklisch:
(1) $\Rightarrow$ (1′): Trivial.
(1′) $\Rightarrow$ (2): Folgt direkt aus dem Homomorphiesatz 2.3.3.16.
(2) $\Rightarrow$ (2′): Man ersetze $H$ durch $\varphi(G)$.
(2′) $\Rightarrow$ (3′): Das Urbild $N = \varphi^{-1}(\{1_H\})$ der einelementigen Untergruppe von $H$ ist eine Untergruppe von $G$ (2.3.1.26). Außerdem gilt für ein beliebiges Element $y = xnx^{-1} \in xNx^{-1}$ mit $n \in N$, also $\varphi(n) = 1_H$, auch

$$\varphi(y) = \varphi(xnx^{-1}) = \varphi(x)\varphi(n)\varphi(x^{-1}) = \varphi(x)\varphi(x)^{-1} = 1_H.$$

Also ist $y \in N$ und somit $xNx^{-1} \subseteq N$.
(3′) $\Rightarrow$ (3): Sei $xNx^{-1} \subseteq N$ für alle $x \in G$. Zu vorgegebenem $x \in G$ verwenden wir die Voraussetzung (3′) speziell für $x^{-1}$ anstelle von $x$, also $x^{-1}Nx \subseteq N$. Daraus folgt $N = xx^{-1}Nxx^{-1} \subseteq xNx^{-1}$. Insgesamt gilt also $xNx^{-1} = N$ für alle $x \in G$.
(3) $\Rightarrow$ (4): Multipliziert man $xNx^{-1} = N$ von rechts mit $x$, erhält man $xN = Nx$.
(4) $\Rightarrow$ (4′): Trivial.
(4′) $\Rightarrow$ (1): Sei also $N$ eine Untergruppe mit $xN \subseteq Nx$ für alle $x \in G$. Multiplikation mit $x^{-1}$ von rechts liefert $xNx^{-1} \subseteq N$, woraus wegen (3) $\Rightarrow$ (3′) sogar $xNx^{-1} = N$ folgt. Wenn es überhaupt eine Kongruenzrelation $\sim$ mit $N = [1]_\sim$ gibt, dann gilt sicher die Äquivalenz $x \sim y \;\Leftrightarrow\; 1 \sim x^{-1}y \;\Leftrightarrow\; x^{-1}y \in N$. Es gibt also höchstens eine Kongruenzrelation $\sim$ mit $N = [1]_\sim$, nämlich die durch

$$x \sim y \;:\Leftrightarrow\; x^{-1}y \in N$$

definierte Relation. Wir müssen nur noch überprüfen, dass dies tatsächlich eine Kongruenzrelation ist.
Nach Definition ist $x \sim y$ zu $x^{-1}y \in N$ äquivalent, also auch zu $y \in xN$. Das bedeutet, dass $y$ in der Linksnebenklasse von $N$ liegt. Weil $N$ nach Voraussetzung eine Untergruppe ist, bilden nach 2.3.1.26 die Linksnebenklassen von $N$ eine Partition der Gruppe $G$. Folglich ist $\sim$ eine Äquivalenzrelation.
Zu zeigen ist weiters die Verträglichkeit von $\sim$ mit den Operationen. Wegen 3.2.2.1 genügt es die mit der binären Operation nachzuweisen. Tatsächlich folgt aus $x \sim x'$ und $y \sim y'$ die Gleichung $(xy)^{-1}(x'y') = y^{-1}(x^{-1}x')y \in y^{-1}Ny \subseteq N$, also $xy \sim x'y'$. Daher ist $\sim$ eine Kongruenzrelation. Nach Definition ist schließlich auch

$$[1]_\sim = \{x : 1 \sim x\} = \{x : 1^{-1}x \in N\} = N.$$

□

**Anmerkung 3.2.2.5.** Alle vier Paare von Bedingungen aus Satz 3.2.2.4 lassen sich auch sehr ansprechend verbal fassen:
(1) und (1') beschreiben den bijektiven Zusammenhang Kongruenzrelation – Normalteiler, den wir im Anschluss noch ausführlicher diskutieren werden.
(2) und (2') übersetzen diese Korrespondenz im Sinne des Homomorphiesatzes. Die Normalteiler treten also genau als die *Kerne* von Gruppenhomomorphismen, d.h. als homomorphe Urbilder von neutralen Elementen auf. (Man beachte den Unterschied zum allgemeineren Begriff des Kerns einer Abbildung als induzierte Äquivalenzrelation, d.h. als Menge von Paaren. Die Sprechweise in der Gruppentheorie – ebenso bei Ringen, Moduln etc. – entspricht also der in der Linearen Algebra üblichen.)
(4) und äquivalent (4') besagen, dass die Zerlegungen in Links- bzw. in Rechtsnebenklassen genau dann identisch sind, wenn die Untergruppe sogar ein Normalteiler ist.
(3) und (3') schließlich bedeuten, dass Normalteiler invariant sind unter allen Abbildungen $\pi_x : g \mapsto xgx^{-1}$, $x \in G$, den sogenannten *inneren Automorphismen*, mit denen wir uns in 3.2.5 noch intensiver beschäftigen werden. Schon hier sei festgehalten, dass es sich dabei wegen $\pi_x(gh) = xghx^{-1} = xgx^{-1}xhx^{-1} = \pi_x(g)\pi_x(h)$ um Endomorphismen von $G$ handelt. Wegen $\pi_x \circ \pi_y : g \mapsto x(ygy^{-1})x^{-1} = (xy)g(xy)^{-1}$, also $\pi_x \circ \pi_y = \pi_{xy}$, gilt auch $\pi_x \circ \pi_{x^{-1}} = \pi_{x^{-1}} \circ \pi_x = \pi_{e_G} = \mathrm{id}_G$. Also sind die $\pi_x$ auch bijektiv, mithin tatsächlich Automorphismen von $G$.

Hervorzuheben ist der Fall abelscher Gruppen, da dann die Aussage $xN = Nx$ in Bedingung (4) aus Satz 3.2.2.4 automatisch erfüllt ist. Wir erhalten:

**Folgerung 3.2.2.6.** *Sei $(G, +, 0, -)$ eine abelsche Gruppe und $N \subseteq G$. Dann ist $N$ genau dann ein Normalteiler, wenn $N$ eine Untergruppe ist.*

Zurück zur bijektiven Korrespondenz $\Phi$ zwischen den Kongruenzrelationen $\sim$ und den Normalteilern $N$ auf einer Gruppe $G$, die sich durch (1) aus Satz 3.2.2.4 ergibt. Und zwar ordnet $\Phi$ jeder Kongruenzrelation $\sim$ auf $G$ die Klasse $[1]_\sim$ des neutralen Elements 1 in $G$ bezüglich $\sim$ zu, und $\Phi^{-1}$ jedem Normalteiler $N \lhd G$ die Äquivalenzrelation $\sim_N$ definiert durch $x \sim_N y :\Leftrightarrow y \in xN$. Hieraus ist auch ersichtlich, dass die zu einer Kongruenzrelation $\sim$ auf einer Gruppe $G$ gehörige Partition gerade die (Links- = Rechts-) Nebenklassenzerlegung nach dem zu $\sim$ gehörigen Normalteiler ist. Die Bijektion $\Phi$ ist offenbar auch mit der mengentheoretischen Inklusion $\subseteq$ verträglich: $\sim_1 \subseteq \sim_2$ genau dann, wenn $\Phi(\sim_1) \subseteq \Phi(\sim_2)$. Weil jeder Kongruenzverband vollständig ist, ergibt sich daraus:

**Folgerung 3.2.2.7.** *Die Normalteiler einer Gruppe $G$ bilden bezüglich der Inklusion $\subseteq$ als Halbordnungsrelation einen vollständigen Verband, den* Normalteilerverband*. Dieser ist isomorph zum Kongruenzverband $(\mathrm{Con}(G), \subseteq)$ von $G$. Der kanonische Isomorphismus $\Phi$ ordnet jeder Kongruenzrelation $\sim$ den Normalteiler $[1_G]_\sim$ zu.*

Das Infimum im Kongruenz- wie auch im Normalteilerverband ist der mengentheoretische Schnitt. Im Vergleich zum komplizierten Erzeugungsprozess von Untergruppen lässt

sich das Supremum von Normalteilern recht handlich als Komplexprodukt beschreiben. Für die folgende Zusammenstellung einiger in diesem Zusammenhang nützlicher Tatsachen sei an die Schreibweise $AB := \{ab : \ a \in A, b \in B\}$ sowie $A_1A_2 \dots A_nA_{n+1} := (A_1A_2 \dots A_n)A_{n+1}$ für Komplexprodukte von Teilmengen $A, B \subseteq G$ von Gruppen erinnert.

**Proposition 3.2.2.8.** *Seien $G$ eine Gruppe und $A, B \subseteq G$ Teilmengen.*

1. *Aus $A, B \leq G$ folgt im Allgemeinen nicht $AB \leq G$.*
2. *Aus $A \lhd G$ und $B \leq G$ folgt $AB = BA \leq G$.*
3. *Aus $A, B \lhd G$ folgt $AB \lhd G$.*
4. *Im Normalteilerverband ist das Supremum zweier oder, allgemeiner, endlich vieler Normalteiler $N_1, \dots, N_k \lhd G$ gegeben durch das Komplexprodukt $N_1N_2 \dots N_k$.*
5. *Sind $N_i \lhd G$, $i \in I \neq \emptyset$, Normalteiler der Gruppe $G$, so ist ihr Supremum $N := \sup_{i \in I} N_i$ im Verband aller Normalteiler gegeben durch die Vereinigung aller endlichen Komplexprodukte $N_{i_1} \dots N_{i_n}$, $n \in \mathbb{N}$ und $i_1, \dots i_n \in I$.*

**UE 153 ► Übungsaufgabe 3.2.2.9.** (W) Beweisen Sie Proposition 3.2.2.8. **◄ UE 153**

Für die Faktorgruppe $G/\sim$ nach einer Kongruenzrelation $\sim$ schreiben wir im Folgenden meistens $G/N$, wenn $N$ und $\sim$ einander in der Korrespondenz $\Phi$ aus Folgerung 3.2.2.7 entsprechen, d.h. wenn $N = \Phi(\sim) = [1_G]_\sim$ ist. Die Elemente der Faktorgruppe sind Nebenklassen $gN = Ng = [g]_\sim$, mit denen man offenbar nach den Regeln $(gN)(hN) = (gh)N$ und $(gN)^{-1} = g^{-1}N$ rechnet. Neutrales Element in $G/N$ ist $N = 1_GN = N1_G$ selbst.

Nach dem allgemeinen Homomorphiesatz 2.3.3.16 induziert jeder Gruppenhomomorphismus $f\colon G \to H$ eine Kongruenzrelation $\sim$. Nach obigen Überlegungen ist $\sim$ bereits durch die eine Klasse $N := [1_G]_\sim = f^{-1}(1_H) \lhd G$ eindeutig bestimmt, und zwar als Nebenklassenzerlegung nach $N$.
Folgerung 3.2.2.7 zeigt insbesondere, dass es in jeder Gruppe $G$ einen kleinsten und einen größten Normalteiler gibt. Klarerweise sind das $\{1_G\}$ und $G$, genannt die *trivialen Normalteiler*. Sie entsprechen den trivialen Kongruenzrelationen, der identischen Kongruenzrelation (Diagonale), wo $a \sim b$ nur für $a = b$, und der Allrelation, wo $a \sim b$ für alle $a, b \in G$. Über den Homomorphiesatz gehören dazu im ersten Fall injektive Homomorphismen, im zweiten konstante. Weil die Urbilder eines Elements Nebenklassen nach dem Kern sind, bedeutet das:

**Folgerung 3.2.2.10.** *Ein Gruppenhomomorphismus $f\colon G \to H$ ist genau dann injektiv, wenn* $\ker f = \{1_G\}$.

Die allgemeine Definition 2.3.3.13 einer einfachen Algebra führt im Fall von Gruppen zu:

**Folgerung 3.2.2.11.** *Eine Gruppe $G$ ist einfach genau dann, wenn $N = \{1_G\}$ und $N = G$ die einzigen Normalteiler von $G$ sind.*

Achtung, die Relation $\lhd$ ist nicht transitiv (siehe Übungsaufgabe 3.2.5.14).

Die Isomorphiesätze werden für Gruppen üblicherweise mit Normalteilern statt mit Kongruenzrelationen formuliert. Das folgende Lemma hilft bei der Übersetzung.

**Lemma 3.2.2.12.** *Sei $G$ Gruppe, $U \leq G$ und $N \lhd G$ mit zugehöriger Kongruenzrelation $\sim$. Dann ist $[U]_\sim := \bigcup_{u\in U}[u]_\sim = UN = NU$.*
*Die Einschränkung von $\sim$ auf $U$ (formal ist das die Schnittmenge von $\sim$ und $U \times U$) ist Kongruenz auf $U$ und entspricht dem Normalteiler[7] $N \cap U \lhd U$.*

*Beweis.* Wenn $x \in UN$, dann gibt es $u \in U$, $n \in N$ mit $x = un$. Daher ist $u^{-1}x \in N$, also $u \sim x$. Das zeigt $UN \subseteq [U]_\sim$. Ist umgekehrt $x \in [U]_\sim$, so folgt $u \sim x$ mit einem $u \in U$, also $u^{-1}x \in N$, und es gibt ein $n \in N$ mit $u^{-1}x = n$, daher $x = un$. Das zeigt $[U]_\sim \subseteq UN$, insgesamt also $[U]_\sim = UN$. Die Gleichung $UN = NU$ folgt schließlich aus Satz 3.2.2.4(4). Die zweite Aussage ist offensichtlich. □

**Folgerung 3.2.2.13** (Isomorphiesätze für Gruppen)**.** *Sei $G$ eine Gruppe.*

1. *Für $U \leq G$ und $N \lhd G$ ist $NU = UN \leq G$ eine Untergruppe von $G$, $N \cap U \lhd U$ ein Normalteiler von $U$, und es gilt die Isomorphie*

$$U/(N \cap U) \simeq UN/N.$$

   *Ein Isomorphismus ist gegeben durch*

$$u(N \cap U) \mapsto uN, \quad u \in U.$$

2. *Für Normalteiler $N_1, N_2 \lhd G$ mit $N_1 \subseteq N_2$ ist auch $N_1 \lhd N_2$ Normalteiler in $N_2$ und $N_2/N_1 := \{xN_1 : x \in N_2\} \lhd G/N_1$ Normalteiler in der Faktorgruppe, und es gilt die Isomorphie*

$$(G/N_1)/(N_2/N_1) \simeq G/N_2.$$

   *Ein Isomorphismus ist gegeben durch*

$$(gN_1)(N_2/N_1) \mapsto gN_2.$$

**UE 154** ► **Übungsaufgabe 3.2.2.14.** (W) Beweisen Sie die Isomorphiesätze für Gruppen (3.2.2.13) unter Verwendung von 2.3.6.3, 2.3.6.7 und 3.2.2.12. ◄ **UE 154**

[7] Achtung: $N \cap U$ ist Normalteiler von $U$, aber im Allgemeinen ist $N \cap U$ kein Normalteiler von $G$.

Eine Illustration dazu folgt etwas später in 3.2.5, wenn wir mehr interessante Beispiele zur Verfügung haben.

Wir schließen mit einem immer wieder nützlichen Beispiel einer Faktorisierung, das gleichzeitig eine gute Illustration einer recht allgemeinen Vorgangsweise ist. Oft ist es möglich, aus einer algebraischen Struktur gewisse unliebsame Eigenschaften zu eliminieren oder – wie man gerne sagt – wegzufaktorisieren. So kann man aus einer beliebigen, i.A. nicht abelschen Gruppe $G$ durch Faktorisierung nach einem Normalteiler $N \lhd G$ eine abelsche Gruppe $G/N$ machen. Auf triviale Weise ist das mit $N = G$ der Fall, weil die einelementige Gruppe $G/G$ natürlich abelsch ist. Das ist aber nicht sehr befriedigend, weil man möglichst viel von der Struktur von $G$ erhalten möchte und deshalb wenig vergröbernde Faktorisierungen (d.h. mit kleinen Normalteilern $N$) bevorzugt. Eine etwas feinere Analyse zeigt: Sollen für $a, b \in G$ die Nebenklassen kommutieren, soll also $abN = baN$ gelten, so lässt sich das mit den Regeln für das Rechnen in Faktorgruppen zu $[a, b] := aba^{-1}b^{-1} = ab(ba)^{-1} \in N$ umschreiben und vice versa. Notwendig und hinreichend für die Kommutativität von $G/N$ ist also, dass $N$ sämtliche sogenannte *Kommutatoren* $[a, b]$, $a, b \in G$, und somit den von diesen erzeugten Normalteiler enthält, die sogenannte *Kommutatorgruppe* $G'$ (manchmal auch die *abgeleitete Gruppe* genannt). Die Situation wird durch folgenden Satz beschrieben:

**Satz 3.2.2.15.** *Sei $G$ eine Gruppe und bezeichne $G'$ die von allen Kommutatoren $[a, b] = aba^{-1}b^{-1}$, $a, b \in G$, erzeugte Untergruppe. Dann gilt:*

1. *$G' \lhd G$ ist sogar ein Normalteiler.*
2. *$G/G'$ (die sogenannte* Abelisierung *von $G$) ist abelsch.*
3. *Für einen beliebigen Normalteiler $N \lhd G$ ist $G/N$ genau dann abelsch, wenn $G' \subseteq N$.*

*Beweis.* Die dritte Aussage geht aus der oben durchgeführten Überlegung hervor. Die zweite Aussage folgt unmittelbar aus der ersten und dritten. Folglich bleibt nur noch die erste zu zeigen. Wegen Anmerkung 3.2.2.5 genügt dafür wiederum der Nachweis, dass jeder innere Automorphismus von $G$ nicht aus der Untergruppe $G'$ hinausführt. Doch sogar durch einen beliebigen Endomorphismus $f$ von $G$ wird ein Kommutator $[a, b]$ auf den entsprechenden Kommutator

$$f([a, b]) = f(aba^{-1}b^{-1}) = f(a)f(b)f(a)^{-1}f(b)^{-1} = [f(a), f(b)],$$

also wieder auf ein Element von $G'$, abgebildet. Damit ist auch das Erzeugnis $G'$ der Kommutatoren unter inneren Automorphismen invariant, also $G' \lhd G$, und der Beweis von Satz 3.2.2.15 komplett. □

In Algebra II (genauer in Abschnitt 8.3.2 über auflösbare Gruppen) wird die Konstruktion der Untergruppe $G'$ aus $G$ nochmals aufgegriffen werden. Führt die Iteration nach endlich vielen Schritten zur einelementigen Gruppe, nennt man $G$ *auflösbar*, siehe Definition 8.3.2.1.

Wir schließen mit einer einfachen, beim Umgang mit konkreten Beispielen von Gruppen aber häufig nützlichen Beobachtung:

**Proposition 3.2.2.16.** *Jede Untergruppe $U$ einer Gruppe $G$ vom Index $[G:U]=2$ ist sogar ein Normalteiler von $G$.*

**UE 155 ► Übungsaufgabe 3.2.2.17.** (F+) Beweisen Sie Proposition 3.2.2.16. **◄ UE 155**

### 3.2.3 Direkte und schwache Produkte von Gruppen

Inhalt in Kurzfassung: Im Gegensatz zum allgemeinen Fall direkter Produkte treten bei Gruppen die einzelnen Faktoren nicht nur als homomorphe Bilder, sondern auch als Unterstrukturen auf. Somit ergibt sich umgekehrt die Frage, ob eine gegebene Gruppe als direktes Produkt gewisser Untergruppen gedeutet werden kann. Die Ergebnisse dieses Unterabschnitts beschäftigen sich mit dieser und ähnlichen Fragen, zunächst für den Fall endlich vieler Faktoren. Anschließend betrachten wir auch die Situation für beliebig viele Faktoren, was uns auf den Begriff des schwachen Produkts führt.

Wie bereits in 2.3.2 angeklungen, treten, wenn man die allgemeine Konstruktion direkter Produkte von Algebren auf Gruppen $G_i$, $i \in I$, spezialisiert, zusätzliche Aspekte auf. Denn neben den *kanonischen Projektionen*

$$\pi_{i_0}\colon \prod_{i\in I} G_i \to G_{i_0}, \quad (g_i)_{i\in I} \mapsto g_{i_0}$$

gibt es noch eine zweite Familie natürlicher Abbildungen in die umgekehrte Richtung, nämlich, gleichfalls für alle $i_0 \in I$, die *kanonischen Einbettungen*

$$\iota_{i_0}\colon G_{i_0} \to \prod_{i\in I} G_i, \quad g \mapsto (g_i)_{i\in I}$$

mit $g_{i_0} := g$ und $g_i = e_i$ (Einselement in $G_i$). Somit treten im direkten Produkt $G := \prod_{i\in I} G_i$ die Faktoren $G_i$ auch in natürlicher Weise als Untergruppen auf, nämlich in Form ihrer isomorphen Kopien $\tilde{G}_{i_0} := \iota_{i_0}(G_{i_0}) \leq G$. Bei der Strukturanalyse einer gegebenen Gruppe $G$ liegt es daher nahe, nach Untergruppen zu suchen, die als solche $\tilde{G}_{i_0}$ interpretiert werden können. Die wichtigsten Aspekte treten bereits bei zwei Faktoren auf. Diesen Fall wollen wir sorgfältig studieren, die offensichtlichen Verallgemeinerungen auf endlich viele Faktoren verbleiben als Übungsaufgabe.
Die Gruppe $G$ habe zwei Untergruppen $U_1, U_2 \leq G$ derart, dass die Abbildung $\varphi : U_1 \times U_2 \to G$, $(u_1, u_2) \mapsto u_1u_2$, vom direkten Produkt von $U_1$ und $U_2$ nach $G$ ein Isomorphismus ist. In diesem Fall nennen wir $G$ das *innere direkte Produkt* seiner Untergruppen $U_1$ und $U_2$ und schreiben $G = U_1 \odot U_2$. Die Projektionen $\pi_i : (u_1, u_2) \mapsto u_i$, $i = 1, 2$ sind Homomorphismen, ebenso wie die Abbildungen $\pi_i \circ \varphi^{-1}$, $i = 1, 2$, deren Kern $U_2$ bzw. $U_1$ ist. Also handelt es sich um Normalteiler. Klarerweise müssen $U_1$ und $U_2$ wegen der Injektivität von $\varphi$ trivialen Schnitt $U_1 \cap U_2 = \{e_G\}$ haben. Wegen der Surjektivität von

$\varphi$ schließlich muss $U_1U_2 = G$ gelten. Diese drei notwendigen Bedingungen erweisen sich gemeinsam aber auch als hinreichend. Um das einzusehen, beweisen wir zunächst das folgende Lemma.

**Lemma 3.2.3.1.** *Sei $G$ eine Gruppe mit neutralem Element $e_G$ und $U, V \lhd G$ Normalteiler von $G$ mit $U \cap V = \{e_G\}$. Dann gilt $uv = vu$ für alle $u \in U$ und $v \in V$.*

*Beweis.* Die zu beweisende Gleichheit $uv = vu$ gilt genau dann, wenn der Kommutator $k := [u, v] = uvu^{-1}v^{-1}$ von $u$ und $v$ das neutrale Element $e_G$ ist. Das ist tatsächlich der Fall, denn $k$ lässt sich auf zwei Weisen klammern:

$$k = uvu^{-1}v^{-1} = (uvu^{-1})v^{-1} = u(vu^{-1}v^{-1})$$

Wegen $V \lhd G$ ist $uvu^{-1} \in uVu^{-1} = V$, also auch $k = (uvu^{-1})v^{-1} \in V$. Analog zeigt die zweite Klammerung $k \in U$. Also gilt $k \in U \cap V = \{e_G\}$, mit anderen Worten $k = e_G$, was zu zeigen war. □

**Proposition 3.2.3.2.** *Seien $G$ eine Gruppe mit neutralem Element $e_G$ und $U, V \leq G$ Untergruppen. Genau dann ist $G$ das innere direkte Produkt von $U$ und $V$, wenn folgende drei Bedingungen erfüllt sind:*

(1) $U, V \lhd G$
(2) $U \cap V = \{e_G\}$
(3) $G = UV$

*Beweis.* Die vorangegangene Diskussion zeigt, dass alle drei Bedingungen notwendig sind. Für den Beweis genügt es daher zu zeigen, dass die Abbildung $\varphi : U \times V \to G$, $(u, v) \mapsto uv$ ein Isomorphismus ist.
Die Surjektivität von $\varphi$ folgt unmittelbar aus der dritten Bedingung.
Um die Injektivität von $\varphi$ nachzuprüfen, ist von einer Relation $u_1v_1 = u_2v_2$ mit $u_1, u_2 \in U$ und $v_1, v_2 \in V$ auszugehen. Wir formen um zu $u_2^{-1}u_1 = v_2v_1^{-1}$. Da die linke Seite in $U$ und die rechte in $V$ liegt, müssen wegen der zweiten Bedingung $U \cap V = \{e_G\}$ beide Ausdrücke das neutrale Element darstellen. Die Relation $u_2^{-1}u_1 = e_G = v_2v_1^{-1}$ bedeutet aber nichts anderes als $u_1 = u_2$ und $v_1 = v_2$, was zu zeigen war.
Die Homomorphiebedingung folgt aus

$$\varphi((u_1, v_1)(u_2, v_2)) = \varphi(u_1u_2, v_1v_2) = u_1u_2v_1v_2 \overset{(*)}{=} u_1v_1u_2v_2 = \varphi(u_1, v_1)\varphi(u_2, v_2),$$

wobei wir in $(*)$ die Gleichung $u_2v_1 = v_1u_2$ für $u_1, u_2 \in U$ und $v_1, v_2 \in V$ verwenden, was wegen Lemma 3.2.3.1 erlaubt ist. □

Ein rekapitulierender Blick auf den Beweis von Proposition 3.2.3.2 zeigt sehr deutlich die Rolle der drei Bedingungen in Hinblick auf die Zerlegung $g = uv$ eines Elementes $g \in G$ in zwei Faktoren $u \in U$ und $v \in V$: (3) garantiert, dass so eine Zerlegung möglich ist, (2) die Eindeutigkeit derselben und (1) die Verträglichkeit der Zerlegung mit der Gruppenoperation.

**UE 156** ► **Übungsaufgabe 3.2.3.3.** (F) Die Gruppe $G = U \odot V$ sei das innere direkte Produkt der Untergruppen $U, V$. Man zeige mit Hilfe des Homomorphiesatzes, dass $G/U \cong V$ und $G/V \cong U$. ◄ **UE 156**

Die Verallgemeinerung von zwei auf endlich viele Faktoren liegt auf der Hand:

**Definition 3.2.3.4.** Sei $G$ eine Gruppe mit Untergruppen $U_1, \ldots, U_n \leq G$. Dann heißt $G$ *inneres direktes Produkt* von $U_1, \ldots, U_n$, wenn die Abbildung

$$\varphi_{U_1,\ldots,U_n} = \varphi : \begin{cases} U_1 \times \cdots \times U_n & \to G \\ (u_1, \ldots, u_n) & \mapsto u_1 \cdots u_n \end{cases}$$

ein Isomorphismus zwischen dem direkten Produkt $\prod_{i=1}^n U_i = U_1 \times \cdots \times U_n$ der Gruppen $U_i$ einerseits und $G$ andererseits ist. In diesem Fall schreibt man oft auch $G = U_1 \odot \ldots \odot U_n$.

Will man direkte Produkte von Gruppen im Sinne von Definition 2.3.2.3 von inneren direkten Produkten im Sinne von Definition 3.2.3.4 unterscheiden, so spricht man bei ersteren auch von *äußeren* direkten Produkten. Offenbar gilt:

**Proposition 3.2.3.5.** *Das äußere direkte Produkt $G := \prod_{i=1}^n G_i$ endlich vieler Gruppen $G_i$ ist das innere direkte Produkt der Untergruppen $\tilde{G}_i := \iota_i(G_i)$ mit den kanonischen Einbettungen $\iota_i$.*

**UE 157** ► **Übungsaufgabe 3.2.3.6.** (F) Prüfen Sie Proposition 3.2.3.5 nach. ◄ **UE 157**

Der folgende Satz ist die natürliche Verallgemeinerung von Proposition 3.2.3.2 und liefert einige nützliche Kriterien zur Überprüfung, ob eine Gruppe $G$ ein direktes Produkt von Untergruppen ist.

**Satz 3.2.3.7.** *Seien $G$ eine Gruppe und $U_1, \ldots, U_n \leq G$ Untergruppen. Wir betrachten folgende Bedingungen:*

*(A) Die Abbildung $\varphi$ aus Definition 3.2.3.4 ist surjektiv.*

*(B) Für alle $i \neq j$ und alle $x \in U_i$, $y \in U_j$ gilt $xy = yx$.*

*(B') $U_i \lhd G$ für alle $i = 1, \ldots, n$.*

*(C) Für $i = 1, \ldots, n$ sei $V_i$ das Komplexprodukt aller $U_j$ mit Ausnahme von $U_i$, also: $V_1 := U_2 \cdots U_n$, $V_2 := U_1 U_3 \cdots U_n$, etc. Dann ist $U_i \cap V_i = \{e_G\}$ für $i = 1, \ldots, n$.*

*(C') Für $i = 1, \ldots, n-1$ gilt $(U_1 \cdots U_i) \cap U_{i+1} = \{e_G\}$.*

*Dann sind folgende Aussagen äquivalent:*

*(1) $G$ ist das innere direkte Produkt von $U_1, \ldots, U_n$.*

*(2) Es gelten die Bedingungen (A), (B) und (C).*

*(3) Es gelten die Bedingungen (A), (B) und (C').*

*(4) Es gelten die Bedingungen (A), (B') und (C).*

*(5) Es gelten die Bedingungen (A), (B') und (C').*

Der Beweis ergibt sich aus der folgenden Übungsaufgabe.

**UE 158** ► **Übungsaufgabe 3.2.3.8.** (W) Beweisen Sie Satz 3.2.3.7. (Hinweis: Verwenden Sie für $n = 2$ Proposition 3.2.3.2 und gehen Sie dann mittels Induktion nach $n$ vor.) ◄ **UE 158**

Wir wollen uns nun dem allgemeinen Fall eines direkten Produkts $G := \prod_{i\in I} G_i$ von Gruppen zuwenden, die mit einer beliebigen Indexmenge indiziert sind. Betrachten wir die Gruppe $G$ „von innen", so entspricht dem eine unendliche Familie $(U_i : i \in I)$ von Untergruppen, nämlich $U_{i_0} = \iota_{i_0}(G_{i_0})$ für die kanonischen Einbettungen $\iota_{i_0} : G_{i_0} \to \prod_{i\in I} G_i$. Der Versuch, Definition 3.2.3.4 unmittelbar zu verallgemeinern, indem man eine Abbildung

$$\varphi : \prod_{i\in I} U_i \to G$$

definiert und die Isomorphismuseigenschaft fordert, schlägt fehl: Wir müssten ein Tupel $(u_i)_{i\in I}$ so nach $G$ abbilden, dass der endliche Fall umfasst wird. Dies würde auf das unendliche Produkt $\prod_{i\in I} u_i$ von Elemente hinauslaufen, das aber nicht definiert ist[8]. Ein weiteres Indiz dafür, dass das volle direkte Produkt zu groß sein kann, liefert die Beobachtung, dass – anders als im endlichen Fall – alle isomorphen Kopien $\iota_{i_0}(G_{i_0})$ zusammen das direkte Produkt nicht erzeugen: Mit (endlichen!) Produkten von Elementen dieser Kopien erhält man nämlich nur Elemente $(g_i)_{i\in I} \in \prod_{i\in I} G_i$, die nur an endlich vielen Stellen einen vom neutralen Element verschiedenen Eintrag haben. Beide Tatsachen zusammen geben Anlass für die folgende Definition:

**Definition 3.2.3.9.** Seien $G_i$, $i \in I$, Gruppen mit Einselementen $e_i \in G_i$. Die Untergruppe (siehe Übungsaufgabe 3.2.3.10)

$$\prod_{i\in I}^{w} G_i := \left\{ (g_i)_{i\in I} \in \prod_{i\in I} G_i \mid g_i \neq e_i \text{ nur für endlich viele } i \in I \right\} \leq \prod_{i\in I} G_i$$

des direkten Produkts $\prod_{i\in I} G_i$ heißt *schwaches Produkt* der $G_i$ („w" steht für englisch „weak"). Wenn $I$ endlich ist, dann stimmen das schwache und das direkte Produkt überein.
Ist $g = (g_i)_{i\in I}$, so heißt die Menge $\mathrm{supp}(g) := \{i \in I \mid g_i \neq e_i\}$ der *Träger*[9] von $g$.

[8] Man beachte, dass wir im Allgemeinen keine Topologie auf $G$ zur Verfügung haben, sodass auch eine Definition als Grenzwert nicht sinnvoll ist.

[9] englisch: *support*

**UE 159** ► **Übungsaufgabe 3.2.3.10.** Zeigen Sie, dass das schwache Produkt $\prod_{i\in I}^{w} G_i$ eine Untergruppe des direkten Produkts $\prod_{i\in I} G_i$ ist. Zeigen Sie außerdem, dass die kanonischen Abbildungen $\iota_{i_0} : G_{i_0} \to \prod_{i\in I} G_i$ sogar in das schwache Produkt abbilden. ◄ **UE 159**

Das schwache Produkt ist tatsächlich die geeignete Definitionsmenge der Abbildung $\varphi$ in der Verallgemeinerung des inneren direkten Produkts auf beliebige Indexmengen.

**Definition 3.2.3.11.** Sei $G$ eine Gruppe und seien $U_i \leq G$, $i \in I$, Untergruppen. Dann heißt $G$ *inneres direktes Produkt* der $U_i$, $i \in I$, wenn die Abbildung

$$\varphi_{(U_i:i\in I)} = \varphi : \begin{cases} \prod_{i\in I}^{w} U_i & \to G \\ (u_i)_{i\in I} & \mapsto \prod_{i\in I} u_i \end{cases}$$

ein Isomorphismus zwischen dem schwachen Produkt $\prod_{i\in I}^{w} U_i$ der Gruppen $U_i$ einerseits und $G$ andererseits ist. In diesem Fall schreiben man auch oft $G = \bigodot_{i\in I} U_i$.

Die Abbildung $\varphi$ ist wohldefiniert, da für $u = (u_i)_{i\in I} \in \prod_{i\in I}^{w} U_i$ das Produkt $\prod_{i\in I} u_i$ tatsächlich ein endliches Produkt (nämlich über $i \in \operatorname{supp}(u)$) ist.
Genauso wie im Fall endlich vieler Gruppen (siehe Proposition 3.2.3.5) gilt:

**Proposition 3.2.3.12.** *Das schwache Produkt $G := \prod_{i\in I}^{w} G_i$ von Gruppen $G_i$ ist das innere direkte Produkt der Untergruppen $\tilde{G}_i := \iota_i(G_i)$ mit den kanonischen Einbettungen $\iota_i$.*

Um eine Satz 3.2.3.7 verallgemeinernde Charakterisierung zu zeigen, führen wir die allgemeine Situation mit dem folgenden Lemma auf den endlichen Fall zurück.

**Lemma 3.2.3.13.** *Sei $G$ eine Gruppe und seien $U_i \leq G$, $i \in I$, Untergruppen. Dann sind die folgenden Aussagen äquivalent:*

(1) *$G$ ist das innere direkte Produkt der $U_i$, $i \in I$.*

(2) *(a) Die Abbildung $\varphi$ aus Definition 3.2.3.11 ist surjektiv UND*

*(b) Für alle endlichen Teilmengen $F = \{i_1, \ldots, i_n\} \subseteq I$ ist $\langle \bigcup_{j=1}^{n} U_{i_j} \rangle$ die innere direkte Summe der Gruppen $U_{i_j}$, $j = 1, \ldots, n$.*

*Beweis.* Sei zunächst (1) angenommen. Aussage (2)(a) gilt trivialerweise, also ist nur (2)(b) zu zeigen. Sei dazu $F = \{i_1, \ldots, i_n\} \subseteq I$ endlich. Die Abbildung $\psi_F : \prod_{j=1}^{n} U_{i_j} \to \prod_{i\in I}^{w} U_i$, $(u_{i_1}, \ldots, u_{i_n}) \mapsto (\tilde{u}_i)_{i\in I}$, wobei $\tilde{u}_{i_j} := u_{i_j}$ für $j = 1, \ldots, n$ und $\tilde{u}_i := e_G$ für $i \in I \setminus F$, ist eine isomorphe Einbettung. Daher ist die Verkettung $\varphi \circ \psi_F$ ein Isomorphismus von $\prod_{j=1}^{n} U_{i_j}$ auf $M$, das Bild von $\varphi\circ\psi_F$. Da die Verkettung $\varphi\circ\psi_F$ nichts anderes als die Abbildung $(u_{i_1}, \ldots, u_{i_n}) \mapsto \prod_{j=1}^{n} u_{i_j}$ ist, also $\varphi \circ \psi_F = \varphi_{U_{i_1},\ldots,U_{i_n}}$, haben wir nur $M = \langle \bigcup_{j=1}^{n} U_{i_j} \rangle$ zu zeigen. Da alle Elemente $\prod_{j=1}^{n} u_{i_j}$ in $\langle \bigcup_{j=1}^{n} U_{i_j} \rangle$ enthalten sind, gilt jedenfalls $M \subseteq \langle \bigcup_{j=1}^{n} U_{i_j} \rangle$. Umgekehrt ist ein beliebiges $U_{i_1} \ni u_{i_1} = \varphi\circ\psi_F(u_{i_1}, e_G, \ldots, e_G)$ in $M$ enthalten; analog gilt $U_{i_j} \subseteq M$ für alle $j = 1, \ldots, n$. Da $M$ als Bild eines Homomorphismus eine Untergruppe ist, folgt $\langle \bigcup_{j=1}^{n} U_{i_j} \rangle \subseteq M$ wie behauptet.
Sei jetzt (2) angenommen. Es ist nur zu zeigen, dass $\varphi$ injektiv und ein Homomorphismus ist. Angenommen, $\varphi(u) = e_G$ für ein $u = (u_i)_{i\in I} \in \prod_{i\in I}^{w} U_i$, $u \neq (e_G)_{i\in I}$. Setzen wir $F = \{i_1, \ldots, i_n\} := \operatorname{supp}(u)$, so gilt

$$\varphi_{U_{i_1},\ldots,U_{i_n}}(u_{i_1}, \ldots, u_{i_n}) = \varphi \circ \psi_F(u_{i_1}, \ldots, u_{i_n}) = \varphi(u) = e_G,$$

im Widerspruch dazu, dass $\varphi_{U_{i_1},\dots,U_{i_n}}$ injektiv ist, da $\langle \bigcup_{j=1}^{n} U_{i_j} \rangle$ ein inneres direktes Produkt von $U_{i_1}, \dots, U_{i_n}$ ist. Angenommen, $\varphi$ ist kein Homomorphismus, also $\varphi(uv) \neq \varphi(u)\varphi(v)$ für $u = (u_i)_{i\in I}, v = (v_i)_{i\in I} \in \prod_{i\in I}^{w} U_i$. Setzen wir $F = \{i_1, \dots, i_n\} := \operatorname{supp}(u) \cup \operatorname{supp}(v)$, so gilt analog zu oben

$$\begin{aligned}\varphi_{U_{i_1},\dots,U_{i_n}}(u_{i_1}v_{i_1}, \dots, u_{i_n}v_{i_n}) = \varphi(uv) &\neq \varphi(u)\varphi(v) \\ &= \varphi_{U_{i_1},\dots,U_{i_n}}(u_{i_1}, \dots, u_{i_n})\varphi_{U_{i_1},\dots,U_{i_n}}(v_{i_1}, \dots, v_{i_n}),\end{aligned}$$

was erneut der Voraussetzung, dass $\langle \bigcup_{j=1}^{n} U_{i_j} \rangle$ ein inneres direktes Produkt von $U_{i_1}, \dots, U_{i_n}$ ist, widerspricht. □

Setzen wir Bedingung (2)(b) die Charakterisierung aus Satz 3.2.3.7 ein, so erhalten wir die gesuchte allgemeine Charakterisierung:

**Satz 3.2.3.14.** *Sei $G$ eine Gruppe und seien $U_i \leq G$, $i \in I$, Untergruppen. Wir betrachten folgende Bedingungen:*

*(A) Die Abbildung $\varphi$ aus Definition 3.2.3.11 ist surjektiv.*

*(B) Für alle $i \neq j$ und alle $x \in U_i$, $y \in U_j$ gilt $xy = yx$.*

*(B') $U_i \lhd G$ für alle $i \in I$.*

*(C) Ist $i \in I$ und verschieden von $i_1, \dots, i_n \in I$ und bezeichnet $V$ das Komplexprodukt aller $U_{i_j}$, also $V = U_{i_1} \cdots U_{i_n}$, so ist $U_i \cap V = \{e_G\}$.*

*Dann sind folgende Aussagen äquivalent:*

*(1) $G$ ist das innere direkte Produkt der $U_i$, $i \in I$.*

*(2) Es gelten die Bedingungen (A), (B) und (C).*

*(3) Es gelten die Bedingungen (A), (B') und (C).*

### 3.2.4 Zyklische Gruppen

Inhalt in Kurzfassung: Eine Gruppe heißt zyklisch, wenn sie von einem Element erzeugt wird. Die additive Gruppe $\mathbb{Z}$ der ganzen Zahlen ist bis auf Isomorphie die einzige unendliche zyklische Gruppe. Darüber hinaus gibt es zu jedem positiven $n \in \mathbb{N}$ bis auf Isomorphie genau eine zyklische Gruppe dieser Ordnung und keine weiteren. Jede zyklische Gruppe lässt sich als homomorphes Bild von $\mathbb{Z}$ realisieren (Restklassengruppen modulo $n$). Im vorliegenden Unterabschnitt werden diese und einige weitere Strukturaussagen über zyklische Gruppen hergeleitet. Eine Folgerung, die auch in anderem Zusammenhang immer wieder eine Rolle spielen wird, betrifft ganzzahlige Linearkombinationen zweier ganzer Zahlen: Ihre Werte sind genau die Vielfachen des größten gemeinsamen Teilers dieser Zahlen.

Die additive Gruppe $\mathbb{Z}$ der ganzen Zahlen spielt eine besonders wichtige Rolle. Wir wollen uns deshalb einen Überblick über ihre Untergruppen und homomorphen Bilder machen. Damit erfassen wir die Klasse der zyklischen Gruppen.
Zunächst einige Wiederholungen (z.B. aus Definition 3.2.1.1): Eine Gruppe heißt *zyklisch*, wenn es ein $g \in G$ gibt (ein sogenanntes *erzeugendes Element*), von dem $G$ erzeugt wird.
Ist $G$ eine Gruppe, so verwenden wir wie bei Halbgruppen die Schreibweise $g^n$ (bei additiver Notation $ng$) für Potenzen von Gruppenelementen $g \in G$, wobei nun der Exponent $n$ ohne Einschränkungen alle ganzen Zahlen durchlaufen kann.
Bevor wir die Struktur beliebiger zyklischer Gruppen analysieren, betrachten wir, wie oben angekündigt, zunächst die additive Gruppe $\mathbb{Z}$ und verschaffen uns einen Überblick über alle Untergruppen.

**Proposition 3.2.4.1.** *Für jedes $m \in \mathbb{Z}$ bezeichne $U_m := \langle m\rangle = m\mathbb{Z} = \{km : \ k \in \mathbb{Z}\}$ die von $m$ erzeugte Untergruppe der additiven Gruppe $\mathbb{Z}$.*

1. *$\mathbb{Z}$ und alle $U_m$ sind zyklisch.*
2. *Sämtliche Untergruppen von $\mathbb{Z}$ sind selbst zyklisch, also gegeben durch alle $U_m$, $m \in \mathbb{Z}$.*
3. *Für $m, n \in \mathbb{Z}$ gilt $U_m \subseteq U_n$ genau dann, wenn $n|m$. (Achtung! Die (absolut) kleinere Zahl erzeugt eine größere Gruppe.)*
4. *Für $m, n \in \mathbb{Z}$ gilt $U_m = U_n$ genau dann, wenn $n = m$ oder $n = -m$.*
5. *Die Abbildung $\kappa : \mathbb{N} \to \mathrm{Sub}(\mathbb{Z})$, $m \mapsto U_m = \langle m\rangle$ ist ein Isomorphismus zwischen dem Teilerverband $(\mathbb{N}, |)$ und dem Halbgruppenverband $(\mathrm{Sub}(\mathbb{Z}), \supseteq)$ bezüglich der Obermengenrelation.*
6. *Für $T \subseteq \mathbb{Z}$ gilt*

$$U := \langle T\rangle = \left\{ \sum_{i=1}^{n} k_i t_i : \ n \in \mathbb{N},\ k_1, \ldots, k_n \in \mathbb{Z},\ t_1, \ldots, t_n \in T \right\} = U_{\mathrm{ggT}(T)}.$$

*Beweis.* 1. $\mathbb{Z} = \langle 1\rangle = \langle -1\rangle$ und $U_m = \langle m\rangle = \langle -m\rangle$.

2. Sei $U \leq \mathbb{Z}$.
   $U = \{0\}$ (1.Fall) ist wegen $U = \langle 0\rangle$ zyklisch.
   Für $U \neq \{0\}$ (2.Fall) gibt es ein $m \in U \subseteq \mathbb{Z}$ mit $m \neq 0$. Ist $m < 0$, so ist das Inverse $-m > 0$ und auch in $U$. In jedem Fall gibt es also ein positives $m \in U$. Wir wählen das kleinste solche $m$ und behaupten $U = \langle m\rangle$.

   Die Inklusion $\supseteq$ ist klar, weil die von $m$ erzeugte Untergruppe von jeder anderen Untergruppe, die $m$ enthält, umfasst wird. Sei daher umgekehrt $u \in U$ beliebig. Wir müssen $u \in \langle m\rangle = \{km : \ k \in \mathbb{Z}\}$ zeigen. Laut 3.1.3.11 (Division mit Rest) gibt es ein $q \in \mathbb{Z}$ und ein $r \in \{0, 1, \ldots, m-1\}$ mit $u = qm + r$. Wegen $qm \in \langle m\rangle \subseteq U$ liegt auch $r = u - qm \in U$. Weil $m$ das kleinste positive Element in $U$ ist, folgt $r = 0$, also $u = qm \in \langle m\rangle$.

3. Ist $U_m \subseteq U_n$, so gilt insbesondere $m \in U_n = \{kn : \ k \in \mathbb{Z}\}$. Also gibt es ein $k \in \mathbb{Z}$ mit $m = kn$, was $n|m$ bedeutet. Gilt umgekehrt $n|m$, also $m = kn$ mit einem $k \in Z$, so liegt mit $m \in U_n$ auch die von $m$ erzeugte Untergruppe $U_m$ in $U_n$, also $U_m \subseteq U_n$.

4. Folgt aus 3. Aus $m|n$ und $n|m$ folgt nämlich $|m| \mid |n|$ und $|n| \mid |m|$, daher $|m| = |n|$, also $m = n$ oder $m = -n$. (Umgekehrt folgt aus $m = -n$ natürlich $U_m = U_n$.)

5. Folgt aus 3. und 4.

6. Nach Satz 3.1.3.4 ist $(\mathbb{N}, |)$ ein vollständiger Verband mit ggT als Infimum. Via $\kappa$ aus dem letzten Punkt entspricht dem das Infimum in $(\mathrm{Sub}(\mathbb{Z}), \supseteq)$, also das Supremum in $(\mathrm{Sub}(\mathbb{Z}), \subseteq)$ – das ist nichts anderes als die erzeugte Untergruppe. Offenbar ist die von einer Teilmenge $T \subseteq \mathbb{Z}$ erzeugte Untergruppe die Menge aller Linearkombinationen der Form $\sum_{i=1}^{n} k_i t_i$, welche folglich mit $U_{\mathrm{ggT}(T)}$ übereinstimmt. □

Eine nützliche Folgerung aus Aussage 6. ist die Folgende:

**Folgerung 3.2.4.2.** *Sei $T \subseteq \mathbb{Z}$ eine Menge ganzer Zahlen. Dann lässt sich eine ganze Zahl $n \in \mathbb{Z}$ genau dann als Linearkombination von Elementen aus $T$ mit ganzzahligen Koeffizienten darstellen, wenn* $\mathrm{ggT}(T)|n$ *gilt.*

**UE 160 ▶ Übungsaufgabe 3.2.4.3.** (W) Beweisen Sie Folgerung 3.2.4.2. **◀ UE 160**

In einem zweiten Schritt zeigen wir einige wichtige Strukturaussagen über allgemeine zyklische Gruppen, die bereits den Weg zum Klassifikationssatz, Satz 3.2.4.8, weisen.

**Proposition 3.2.4.4.** *1. Eine Gruppe $G$ ist genau dann zyklisch, wenn $G$ ein homomorphes Bild von $\mathbb{Z}$ ist.*

*2. Jede zyklische Gruppe ist abelsch.*

*3. Homomorphe Bilder zyklischer Gruppen sind zyklisch.*

*4. Untergruppen zyklischer Gruppen sind selbst zyklisch.*

*Beweis.* 1. Sei $G$ zyklisch mit erzeugendem Element $g$. Die Abbildung $\varphi : \mathbb{Z} \mapsto G$, $k \mapsto g^k$ ist nach der ersten Aussage aus Proposition 3.1.1.10 ein Gruppenhomomorphismus, der wegen $G = \{g^n \mid n \in \mathbb{Z}\}$ surjektiv ist.

Ist umgekehrt $G = \varphi(\mathbb{Z})$ mit irgendeinem Homomorphismus $\varphi : \mathbb{Z} \mapsto G$, so ist $G = \langle \varphi(1) \rangle$ zyklisch.

2. $\mathbb{Z}$ ist abelsch, wegen Proposition 4.1.1.2 folglich auch alle homomorphen Bilder von $\mathbb{Z}$, womit die Behauptung aus 1. folgt.

3. Sei $G = \varphi(C)$ das Bild der zyklischen Gruppe $C$ unter dem Homomorphismus $\varphi$. Nach 1. ist $C = \psi(\mathbb{Z})$ homomorphes Bild von $\mathbb{Z}$ unter einem Homomorphismus $\psi$. Also ist $G = \varphi \circ \psi(\mathbb{Z})$ homomorphes Bild von $\mathbb{Z}$ unter dem Homomorphismus $\varphi \circ \psi$, wieder nach 1. daher zyklisch.

4. Sei $G$ eine zyklische Gruppe und $H \leq G$. Nach 1. gibt es einen surjektiven Homomorphismus $\varphi\colon \mathbb{Z} \to G$. Das Urbild $U := \varphi^{-1}(H)$ von $U \leq G$ ist nach 2.3.1.26 eine Untergruppe von $\mathbb{Z}$, laut Aussage 2. in Proposition 3.2.4.1 also zyklisch. Nach 1. ist das homomorphe Bild $H = \varphi(U)$ von $U$ ebenfalls zyklisch. □

**UE 161** ► **Übungsaufgabe 3.2.4.5.** (F) Man zeige: Ist $(G, \cdot, e, ^{-1})$ eine Gruppe, dann ist jede endliche nichtleere Unterhalbgruppe $H$ von $(G, \cdot)$ eine Untergruppe. (Hinweis: betrachten Sie für jedes $x \in H$ die von $x$ erzeugte Halbgruppe $\langle x \rangle_{\text{Halbgruppe}}$, und zeigen Sie, dass diese das Element $e$ enthält.) ◄ **UE 161**

Wenn wir die Struktur beliebiger zyklischer Gruppen verstehen wollen, genügt es nach der ersten Aussage von Proposition 3.2.4.4, die homomorphen Bilder von $\mathbb{Z}$ zu betrachten. Mithilfe des Homomorphiesatzes ist das (bis auf Isomorphie) gleichbedeutend damit, die Normalteiler von $\mathbb{Z}$ zu studieren. Das soll nun geschehen.

**Definition 3.2.4.6.** Für $m \in \mathbb{Z}$ betrachten wir wieder $U_m = m\mathbb{Z} := \{mk \mid k \in \mathbb{Z}\}$. Die Äquivalenzrelation zur zugehörigen Nebenklassenzerlegung bezeichnen wir mit $\equiv_m$:

$$a \equiv_m b \;\Leftrightarrow\; a - b \in m\mathbb{Z} \;\Leftrightarrow\; m|(a-b)$$

Statt $a \equiv_m b$ schreibt man oft auch $a \equiv b \pmod m$, in Worten: *$a$ ist kongruent zu $b$ modulo $m$.*

Insbesondere gilt $a \equiv_0 b$ genau dann, wenn $a = b$. Weiters gilt $a \equiv_1 b$ für alle $a, b \in \mathbb{Z}$.

**Anmerkung 3.2.4.7.** Mit der ersten in Anmerkung 3.1.3.13 erwähnten Notation gilt

$$a \equiv b \pmod m \quad \Leftrightarrow \quad a \bmod m = b \bmod m,$$

also: $a$ und $b$ sind kongruent modulo $m$ genau dann, wenn sie bei Division durch $m$ den gleichen nichtnegativen Rest lassen.
Man beachte den notationellen Unterschied zwischen

$$a \equiv b \pmod m \quad \text{und} \quad a = (b \bmod m).$$

Zum Beispiel gilt $13 \equiv 8 \pmod 5$ (also: „$13 - 8$ ist ohne Rest durch 5 teilbar“), aber nicht $13 = (8 \bmod 5)$, weil mit $8 \bmod 5$ die Zahl 3 gemeint ist.

Aus Folgerung 3.2.2.6 erkennen wir, dass in der abelschen Gruppe $\mathbb{Z}$ die Normalteiler genau die Untergruppen sind. In Proposition 3.2.4.1 haben wir alle Untergruppen von $G = \mathbb{Z}$ bestimmt – und zwar sind es genau die (paarweise verschiedenen) Gruppen $U_m = m\mathbb{Z} = \subseteq \mathbb{Z}$ mit $m \in \mathbb{N}$. Nach dem Homomorphiesatz sind damit alle homomorphen Bilder von $\mathbb{Z}$ bis auf Isomorphie gegeben durch die Gruppen $C_m := \mathbb{Z}/m\mathbb{Z}$. (Diese zyklische Gruppe $C_m$ ist zu unterscheiden vom Restklassenring $\mathbb{Z}_m$ auf derselben Trägermenge, mit $C_m$ als additiver Gruppe, den wir erst später betrachten werden.) Wegen Proposition

3.2.4.4 sind das bis auf Isomorphie gleichzeitig genau die zyklischen Gruppen. Man nennt $C_m$ auch die *Restklassengruppe* modulo $m$.
Der kanonische Homomorphismus $\kappa_m\colon \mathbb{Z} \to C_m$ ordnet jedem $k \in \mathbb{Z}$ die Klasse $k+m\mathbb{Z} = \{\ldots, k-3m, k-2m, k-m, k, k+m, k+2m, k+3m, \ldots\} \in C_m$ zu, genannt die *Restklasse* von $k$ modulo $m$. Für gegebenes $m$ bezeichnet man $k + m\mathbb{Z}$ oft auch mit $\overline{k}$.[10]
Offenbar gilt $|C_m| = m$ für $m \in \mathbb{N}^+$. Im Fall $m = 0$ sind die Kongruenzklassen einelementig, der kanonische Homomorphismus daher ein Isomorphismus $C_0 \cong \mathbb{Z}$. Somit unterscheiden sich alle $C_m$, $m \in \mathbb{N}$, schon hinsichtlich ihrer Kardinalität und können erst recht nicht isomorph sein. Somit haben wir einen ersten, wenn auch noch nicht besonders tiefen Klassifikationssatz bewiesen:

**Satz 3.2.4.8.** *Sämtliche zyklische Gruppen sind bis auf Isomorphie gegeben durch die Restklassengruppen $C_m$, $m \in \mathbb{N}$. Dabei ist $C_0 \cong \mathbb{Z}$ die einzige unendliche zyklische Gruppe. Alle diese Gruppen sind paarweise nichtisomorph.*

Ist $G$ irgendeine Gruppe mit $|G| = p \in \mathbb{P}$ und $g \in G\backslash\{e\}$, so kommt wegen des Satzes von Lagrange (3.2.1.4) als Ordnung $\mathrm{ord}(g)$ nur $p$ in Frage. Die von $g$ erzeugte Untergruppe ist also bereits ganz $G$. Also:

**Proposition 3.2.4.9.** *Jede Gruppe $G$ von Primzahlordnung $|G| = p \in \mathbb{P}$ ist zyklisch, also $G \cong C_p$. Jedes $g \in G \setminus \{e\}$ ist ein erzeugendes Element.*

Für den nächsten Satz brauchen wir ein einfaches zahlentheoretisches Lemma:

**Lemma 3.2.4.10.** *Wir betrachten Teilbarkeit in den natürlichen Zahlen.*

1. *Für alle $a, b, c \in \mathbb{N} \setminus \{0\}$ gilt: $ab|ac \Leftrightarrow b|c$.*
2. *Wenn $a$ und $c$ teilerfremd sind ($\mathrm{ggT}(a, c) = 1$), dann gilt $a|bc \Leftrightarrow a|b$.*
3. *Für alle $a, b, c \in \mathbb{N} \setminus \{0\}$ gilt: $ab|c \Leftrightarrow b|\frac{c}{\mathrm{ggT}(a,c)}$.*

*Beweis.* 1. $abx = ac \Leftrightarrow bx = c$.

2. Die Implikation $\Leftarrow$ ist klar. Wir zeigen $\Rightarrow$.

   Sei $a|bc$. Wenn $p$ ein beliebiger Primfaktor von $a$ ist, und $a = p * a'$, dann muss wegen $\mathrm{ggT}(a, c) = 1$ die Primzahl $p$ ein Faktor von $b$ sein, sagen wir $b = p * b'$. Aus $pa'|pb'c$ folgt nun wegen (1) die Beziehung $a'|b'c$.

   Mit vollständiger Induktion nach der Anzahl der Primfaktoren (gerechnet mit ihrer Vielfachheit, so gibt es z.B. drei Primfaktoren von 12) von $a$ führt die Überlegung im vorigen Absatz zu $a|c$.

3. Sei $d := \mathrm{ggT}(a, c)$, und $a'd = a$, $c'd = c$. Dann gilt nach Punkt (1)

$$ab|c \Leftrightarrow a'db|c'd \Leftrightarrow a'b|c'$$

   Weil $a', c'$ teilerfremd sind, folgt aus Punkt (2) die Äquivalenz mit $b|c'$. □

[10] Wenn wir etwa $m := 8$ setzen, gilt $3 + 7 \equiv 2 \pmod 8$, gleichbedeutend mit $\overline{3} + \overline{7} = \overline{2}$. Das erste Additionssymbol bezeichnet die Addition von natürlichen Zahlen, das zweite die Addition in $C_m$.

Wir können eine weitere interessante Aussage herleiten, wenn wir uns vor Augen führen, dass wir die zu einer beliebigen zyklischen Gruppe $G = \langle g \rangle \cong C_m$ gehörige Zahl $m$ auf zwei Arten verstehen können, falls $m$ endlich ist: Einerseits ist $m = |C_m| = |G|$ die Kardinalität von $G$, somit nach Definition 3.2.1.1 die Ordnung von $g$. Andererseits haben wir $m$ konstruiert als erzeugendes Element des Kerns von $\varphi : \mathbb{Z} \to G$, $n \mapsto g^n$, woraus wir für $n \in \mathbb{Z}$ die Äquivalenz $g^n = e \;\Leftrightarrow\; m|n$ erhalten. Insbesondere gilt[11] $\operatorname{ord}(g) = \min\{n \in \mathbb{N}^+ \mid g^n = e\}$. Diese Tatsache können wir auch in beliebigen Gruppen $G$ nutzbringend einsetzen, wenn wir sie nämlich für die von $g$ erzeugte Untergruppe von $G$ anwenden. Damit erhalten wir die erste Aussage des folgenden Resultats über Teilbarkeitsaussagen von Ordnungen:

**Proposition 3.2.4.11.** *Seien $G$ eine Gruppe und die Ordnungen von $g, h \in G$ endlich. Dann gilt:*

1. *Für $n \in \mathbb{Z}$ ist $g^n = e$ äquivalent zu $\operatorname{ord}(g)|n$.*
   *Insbesondere gilt $\operatorname{ord}(g) = \min\{n \in \mathbb{N}^+ \mid g^n = e\}$.*

2. *Für $k \in \mathbb{Z}$ gilt $\operatorname{ord}(g^k) = \frac{\operatorname{ord}(g)}{t}$ mit $t := \operatorname{ggT}(\operatorname{ord}(g), k) > 0$.*

3. *Aus $gh = hg$ folgt $\operatorname{ord}(gh) | \operatorname{kgV}(\operatorname{ord}(g), \operatorname{ord}(h))$. (Insbesondere gilt das in abelschen Gruppen uneingeschränkt.)*

4. *Gilt zusätzlich $\langle g \rangle \cap \langle h \rangle = \{e\}$ (äquivalent: ist $\langle g, h \rangle$ ein inneres direktes Produkt von $\langle g \rangle$ und $\langle h \rangle$), dann folgt sogar $\operatorname{ord}(gh) = \operatorname{kgV}(\operatorname{ord}(g), \operatorname{ord}(h))$. Das ist insbesondere dann der Fall, wenn $\operatorname{ord}(g)$ und $\operatorname{ord}(h)$ teilerfremd sind.*

*Beweis.* 1. Folgt aus den obigen Bemerkungen.

2. Nach 1. und wegen $(g^k)^l = g^{kl}$ gilt

$$\operatorname{ord}(g^k)|\ell \;\Leftrightarrow\; (g^k)^\ell = e \;\Leftrightarrow\; k\ell | \operatorname{ord}(g) \;\Leftrightarrow\; \ell | \frac{\operatorname{ord}(g)}{\operatorname{ggT}(\operatorname{ord}(g), k)},$$

   wobei die letzte Äquivalenz aus Lemma 3.2.4.10(3) folgt.
   Daher gilt $\operatorname{ord}(g^k)|\ell \Leftrightarrow \ell | \frac{\operatorname{ord}(g)}{t}$, woraus die Aussage folgt.

3. Nach 1. müssen wir nur $(gh)^{\operatorname{kgV}(\operatorname{ord}(g),\operatorname{ord}(h))} = e$ nachrechnen. Nach der Voraussetzung $gh = hg$ gilt $(gh)^k = g^k h^k$, und wir erhalten

$$(gh)^{\operatorname{kgV}(\operatorname{ord}(g),\operatorname{ord}(h))} = g^{\operatorname{kgV}(\operatorname{ord}(g),\operatorname{ord}(h))} h^{\operatorname{kgV}(\operatorname{ord}(g),\operatorname{ord}(h))} = e.$$

4. Wegen 3. genügt es, $\operatorname{ord}(g) | \operatorname{ord}(gh)$ und $\operatorname{ord}(h) | \operatorname{ord}(gh)$ zu zeigen. Dafür reicht es wiederum nach 1., aus $e = (gh)^k$ die Folgerungen $\operatorname{ord}(g)|k$ und $\operatorname{ord}(h)|k$ zu ziehen. Tatsächlich schließen wir aus $e = (gh)^k = g^k h^k$, dass die Potenzen $h^k = g^{-k}$

[11] Setzen wir $\inf \emptyset := \infty$, so gilt die ähnliche Gleichung $\operatorname{ord}(g) = \inf\{n \in \mathbb{N}^+ \mid g^n = e\}$ auch für $g$ von unendlicher Ordnung.

übereinstimmen. Nach Voraussetzung ist dies nur möglich, wenn $h^k = g^{-k} = e$ gilt. Wegen 1. liefert dies das Gewünschte.

Seien nun $\mathrm{ord}(g)$ und $\mathrm{ord}(h)$ teilerfremd und sei $x := h^k = g^\ell$. Nach 2. ist die Ordnung von $x$ ein Teiler von sowohl $\mathrm{ord}(g)$ als auch $\mathrm{ord}(h)$, also muss $\mathrm{ord}(x) = 1$ bzw. $x = e$ gelten. □

**Anmerkung 3.2.4.12.** Einige Autoren definieren die Ordnung eines Elements $g$ als $\inf\{n \in \mathbb{N}^+ \mid g^n = e\}$. Nach dem letzten Resultat ist diese Definition zu unserer äquivalent.

Im abelschen Fall, in dem man sich über die Zusatzvoraussetzung $gh = hg$ keine Gedanken machen muss, werden wir das letzte Resultat in Lemma 3.3.3.1 noch etwas ausbauen. Wir haben in Proposition 3.2.4.1 bereits den Untergruppenverband von $\mathbb{Z}$ analysiert. Mit dem Bisherigen lässt sich auch der Untergruppenverband einer endlichen zyklischen Gruppe beschreiben.

**Satz 3.2.4.13.** *Sei $G = \langle g\rangle$ eine zyklische Gruppe und $T$ die Menge der Teiler von $m$, wobei $m := \mathrm{ord}(g)$ im Fall einer endlichen Ordnung und $m = 0$ für $\mathrm{ord}(g) = \infty$ zu setzen ist. Für den Untergruppenverband sowie Kongruenzverband von $G$ gilt dann die Isomorphie*

$$(T, |) \cong (\mathrm{Sub}(G), \supseteq) \cong (\mathrm{Con}(G), \supseteq).$$

*Ein Isomorphismus für die erste Beziehung ist gegeben durch*

$$\kappa : T \to \mathrm{Sub}(G), \quad t \mapsto \langle g^t\rangle,$$

*für die zweite (wie in jeder abelschen Gruppe) durch*

$$\psi : \mathrm{Sub}(G) \to \mathrm{Con}(G), \quad U \mapsto \sim_U,$$

*mit $a \sim_U b$ genau dann, wenn $ab^{-1} \in U$.*

*Beweis.* Den Fall $m = 0$ haben wir in Aussage 5. von Proposition 3.2.4.1 bereits bewiesen. Sei also $m = \mathrm{ord}(g)$ endlich.
Wir verwenden die Darstellung $G = \varphi(\mathbb{Z})$ als Bild von $\mathbb{Z}$ unter dem Homomorphismus $\varphi : n \mapsto g^n$. Für jede Untergruppe $U \leq G$ gilt $U = \varphi(U')$ mit $U' := \varphi^{-1}(U) \leq \mathbb{Z}$. Nach Aussage 2. von Proposition 3.2.4.1 ist $U' = U_t = t\mathbb{Z}$ für ein $t \in \mathbb{Z}$, wobei wir nach Aussage 4. derselben Proposition $t \in \mathbb{N}$ wählen dürfen. Jedenfalls gilt $\varphi(m) = g^m = e \in U$, also $m \in U_t$ und somit $t|m$. Außerdem gilt $U = \varphi(U_t) = \langle g^t\rangle$. Umgekehrt ist für jeden nichtnegativen Teiler $t$ von $m$ eine Untergruppe $\varphi(t\mathbb{Z})$ gegeben. Sobald wir gezeigt haben, dass für zwei Teiler $t_1, t_2$ von $m$ die Relation $\varphi(t_1\mathbb{Z}) \subseteq \varphi(t_2\mathbb{Z})$ genau dann gilt, wenn $t_2|t_1$, ist der Beweis abgeschlossen.
Aus $t_2|t_1$ folgt $t_1\mathbb{Z} \subseteq t_2\mathbb{Z}$ und daher auch $\varphi(t_1\mathbb{Z}) \subseteq \varphi(t_2\mathbb{Z})$. Gilt umgekehrt $\varphi(t_1\mathbb{Z}) \subseteq \varphi(t_2\mathbb{Z})$, so haben wir $t_2|t_1$ zu zeigen. Für $t_1 = m$ ist das klar, sodass wir von $t_1 < m$ ausgehen. Nach Annahme gilt $\varphi(t_1) \in \varphi(t_2\mathbb{Z}) = \langle g^{t_2}\rangle$. Die Elemente von $\langle g^{t_2}\rangle$ sind genau $(g^{t_2})^k$ für $k = 0, \ldots, \mathrm{ord}(g^{t_2}) - 1$. Nach Aussage 2. in Proposition 3.2.4.11 gilt

$\mathrm{ord}(g^{t_2}) = \frac{\mathrm{ord}(g)}{\mathrm{ggT}(\mathrm{ord}(g),t_2)} = \frac{\mathrm{ord}(g)}{t_2}$. Insgesamt erhalten wir also $g^{t_1} = \varphi(t_1) = (g^{t_2})^k = g^{t_2 k}$ für ein $k \in \{0, \ldots, \frac{\mathrm{ord}(g)}{t_2} - 1\}$. Daraus folgt $g^{t_1 - t_2 k} = e$ bzw. $\mathrm{ord}(g) | t_1 - t_2 k$. Wegen $0 < t_1, t_2 k < m = \mathrm{ord}(g)$, somit $|t_1 - t_2 k| < m$, ist das nur für $t_1 - t_2 k = 0$ möglich, was $t_2 | t_1$ impliziert. □

**Anmerkung 3.2.4.14.** A priori sind mit der Notation des letzten Beweises alle Bilder $\varphi(t\mathbb{Z})$ für beliebige $t$ und nicht nur für $t|m$ Untergruppen von $G$. Allerdings sind diese Untergruppen nicht alle verschieden: Setzen wir beispielsweise $m = 4$, so gilt $\varphi(3\mathbb{Z}) = \langle g^3 \rangle = \{g^3, g^2, g, e\} = \langle g \rangle$. Im letzten Teil des Beweises geht es faktisch darum, zu beweisen, dass man keine Untergruppe mehr doppelt erhält, sobald man sich auf die Teiler von $m$ einschränkt.

Als Folgerung lässt sich eine Formel über eine wichtige zahlentheoretische Funktion gewinnen, die *Eulersche $\varphi$-Funktion*. Diese Funktion zählt für $n \in \mathbb{N}$ die sogenannten *primen Restklassen* modulo $n$. Es gibt mehrere Möglichkeiten, diese zu definieren, die aber alle äquivalent sind.

**UE 162 ► Übungsaufgabe 3.2.4.15.** (F) Sei $n \in \mathbb{N}^+$. **◄ UE 162**

(a) Zeigen Sie, dass für jedes $k$ die folgenden Aussagen äquivalent sind:

(1) $\mathrm{ggT}(k, n) = 1$

(2) Für alle $\ell \in k + n\mathbb{Z}$ gilt $\mathrm{ggT}(\ell, n) = 1$.

(3) Es gibt ein $\ell \in k + n\mathbb{Z}$ mit $\mathrm{ggT}(\ell, n) = 1$.

(b) Zeigen Sie, dass die folgenden Mengen gleichmächtig sind:

(1) $A := \{k + n\mathbb{Z} \mid k \in \mathbb{Z} \wedge \mathrm{ggT}(n, k) = 1\}$

(2) $B := \{k + n\mathbb{Z} \mid k \in \{0, \ldots, n-1\} \ \wedge \ \mathrm{ggT}(n, k) = 1\}$

(3) $C := \{k \mid k \in \{0, \ldots, n-1\} \ \wedge \ \mathrm{ggT}(n, k) = 1\}$

**Definition 3.2.4.16.**

- Für $n \in \mathbb{N}^+$ heißt $k + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ eine *prime Restklasse* modulo $n$ oder auch *teilerfremde Restklasse* modulo $n$, wenn eine der äquivalenten Bedingungen (1)−(3) aus Übungsaufgabe 3.2.4.15(a) gilt, in Worten:
  - $k$ ist zu $n$ teilfremd.
  - Alle Repräsentanten von $k + n\mathbb{Z}$ sind zu $n$ teilerfremd.
  - Irgendein Repräsentant von $k + n\mathbb{Z}$ ist zu $n$ teilerfremd.
- Für $n \in \mathbb{N}^+$ ist $\varphi(n)$ definiert als die Anzahl der primen Restklassen modulo $n$, also als die gemeinsame Mächtigkeit der drei Mengen $A$,$B$,$C$ aus Übungsaufgabe 3.2.4.15(b):

$$\begin{aligned}\varphi(n) &= |\{k + n\mathbb{Z} \mid k \in \mathbb{Z} \wedge \mathrm{ggT}(n, k) = 1\}| \\ &= |\{k + n\mathbb{Z} \mid k \in \{0, \ldots, n-1\} \ \wedge \ \mathrm{ggT}(n, k) = 1\}| \\ &= |\{k \mid k \in \{0, \ldots, n-1\} \ \wedge \ \mathrm{ggT}(n, k) = 1\}|.\end{aligned}$$

Die dadurch definierte Funktion $\varphi$ heißt *Eulersche $\varphi$-Funktion*.

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | ... |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\varphi(n)$ | 1 | 1 | 2 | 2 | 4 | 2 | 6 | 4 | 6 | 4 | 10 | 4 | 12 | 6 | 8 | 8 | ... |

**Folgerung 3.2.4.17.** *Für die Eulersche $\varphi$-Funktion und $n \in \mathbb{N}^+$ gilt: $n = \sum_{t|n} \varphi(t)$.*

**UE 163** ► **Übungsaufgabe 3.2.4.18.** (F) Folgern Sie 3.2.4.17 aus Satz 3.2.4.13 und Proposition 3.2.4.11. ◄ **UE 163**

Eine explizite Formel für die Eulersche $\varphi$-Funktion werden wir mit Hilfe des Chinesischen Restsatzes erhalten, siehe Satz 3.4.7.3.

### 3.2.5 Permutationsgruppen

Inhalt in Kurzfassung: Die große Bedeutung von Permutationsgruppen für die gesamte Gruppentheorie ergibt sich aus dem Darstellungssatz von Cayley: Jede Gruppe ist isomorph zu einer Untergruppe der symmetrischen Gruppe auf ihrer Trägermenge, also zu einer Gruppe von Permutationen (= Permutationsgruppe). Dies allein rechtfertigt ein etwas ausführlicheres Studium von Permutationsgruppen, es ergeben sich aber darüber hinaus einige weitere reizvolle Aspekte. Einiges aus diesem Unterabschnitt dürfte schon aus dem Kapitel über Determinanten aus der Linearen Algebra bekannt sein, insbesondere die Unterscheidung zwischen geraden und ungeraden Permutationen.

Wir rufen uns den Darstellungssatz von Cayley für Monoide (3.1.2.5) in Erinnerung. Ihm zufolge lässt sich jedes Monoid $M$ vermittels der regulären Darstellung $\iota : a \mapsto f_a$, $f_a(x) := ax$ für $a, x \in M$ isomorph in das symmetrische Monoid auf der Menge $M$ einbetten. Wendet man diese Konstruktion auf eine Gruppe $G$ an, so sind alle $f_g$, $g \in G$, sogar Permutationen, d.h. Bijektionen von $G$ nach $G$: Für vorgegebenes $y \in G$ ist $f_a(x) = ax = y$ genau dann, wenn $x = a^{-1}y$ gilt. Also hat $y$ genau ein Urbild unter $f_a$, was Bijektivität von $f_a$ zeigt. Folglich ist die laut 3.1.2.5 isomorphe Einbettung $\iota$ von $G$ als Monoid sogar eine isomorphe (Monoid-)Einbettung der Gruppe $G$ in die symmetrische Gruppe auf der Trägermenge $G$ (die Gruppe aller Permutationen von $G$ bezüglich der Komposition, siehe letzter Punkt in 2.1.1.4). Nach Proposition 3.1.1.5 liegt tatsächlich eine isomorphe Gruppen-Einbettung vor. Somit gilt der *Darstellungssatz von Cayley für Gruppen*:

**Satz 3.2.5.1.** *Jede Gruppe $G$ lässt sich vermittels der Einbettung $\iota : a \mapsto f_a$, $f_a(x) := ax$ für $a, x \in G$ isomorph in die symmetrische Gruppe $S_G$ auf der Trägermenge $G$ einbetten.*

Nennt man, wie üblich, jede Untergruppe einer symmetrischen Gruppe $S_X$ (auf irgendeiner Menge $X$) eine *Permutationsgruppe*, so lautet der Darstellungssatz von Cayley für Gruppen: Jede Gruppe $G$ ist isomorph zu einer Permutationsgruppe auf der Trägermenge von $G$.

Dieser Sachverhalt legt es nahe, verschiedenste Aspekte der Gruppentheorie insbesondere für Permutationsgruppen zu untersuchen. Als Beispiel wählen wir den Themenkreis *innere Automorphismen* (siehe auch schon Anmerkung 3.2.2.5) und *Konjugation*, was speziell bei endlichen Permutationsgruppen zu reizvollen Einsichten führt.

**Definition 3.2.5.2.** Seien $X$ und $Y$ Mengen, $\phi\colon X \to Y$ bijektiv und $f\colon X \to X$. Dann heißt $f_\phi := \phi \circ f \circ \phi^{-1}\colon Y \to Y$ die bezüglich $\phi$ *Konjugierte* von $f$. Die Zuordnung $\Phi : f \mapsto f_\phi$ heißt *Konjugation*.[12]

**Proposition 3.2.5.3.** *Mit der Notation aus Definition 3.2.5.2 ist die Konjugation $\Phi$ ein Isomorphismus zwischen dem symmetrischen Monoid $M_X$ und dem symmetrischen Monoid $M_Y$. Die Einschränkung von $\Phi$ auf die symmetrische Gruppe $S_X$ ist ein Gruppenisomorphismus zwischen der symmetrischen Gruppe $S_X$ und der symmetrischen Gruppe $S_Y$.*

**UE 164 ▶ Übungsaufgabe 3.2.5.4.** (F) Beweisen Sie Proposition 3.2.5.3. **◀ UE 164**

Den Darstellungssatz von Cayley im Hinterkopf untersuchen wir nun eine ähnliche Situation für den Fall, dass $X = Y = G$ eine Gruppe ist. Zunächst aber eine Definition, die auch in anderem Zusammenhang von Interesse ist.

**Definition 3.2.5.5.** Ist $G$ eine Gruppe, so heißt

$$Z(G) := \{g \in G :\ \forall h \in G :\ gh = hg\} \lhd G$$

das *Zentrum* von $G$.

Die folgenden Aussagen knüpfen an Anmerkung 3.2.2.5 an.

**Proposition 3.2.5.6.** *Sei $G$ eine Gruppe. Für alle $g \in G$ definieren wir $\pi_g\colon G \to G$ $x \mapsto gxg^{-1}$ und betrachten die Abbildung $\Phi : g \mapsto \pi_g$. Dann gilt:*

1. *Für $g, h \in G$ gilt $\pi_g \circ \pi_h = \pi_{gh}$. Somit ist $\Phi$ ein Homomorphismus von $G$ in die Automorphismengruppe* $\mathrm{Aut}(G)$.
2. *Für alle $g \in G$ ist $\pi_g$ ein Automorphismus (genannt der durch* Konjugation *mit $g$ induzierte* innere Automorphismus *von $G$).*
3. *Für den Kern von $\Phi$ gilt*

$$\ker(\Phi) = Z(G) = \{g \in G :\ \forall h \in G :\ gh = hg\}.$$

*Insbesondere ist das Zentrum ein Normalteiler. Außerdem ist $\Phi\colon G \to \mathrm{Aut}(G)$ eine isomorphe Einbettung genau dann, wenn das Einselement $e \in G$ das einzige ist, das mit allen $g \in G$ vertauscht.*

[12] Dieser Begriff von Konjugation und Konjugierten ist von anderen zu unterscheiden, die ebenfalls mit ähnlichen Vokabeln bezeichnet werden. Man denke vor allem an die Wurzeln eines irreduziblen Polynoms im Zerfällungskörper, von denen komplex konjugierte Zahlen ein Spezialfall sind.

*4. Die inneren Automorphismen bilden einen Normalteiler* $\Phi(G) \lhd \mathrm{Aut}(G)$ *der Automorphismengruppe von* $G$*. (Die Faktorgruppe* $\mathrm{Aut}(G)/\Phi(G)$ *nennt man auch die* äußere Automorphismengruppe *von* $G$*.)*

**UE 165 ► Übungsaufgabe 3.2.5.7.** (W) Beweisen Sie Proposition 3.2.5.6. **◄ UE 165**

Eigenschaft (4) in Satz 3.2.2.4 zeigt:

**Folgerung 3.2.5.8.** *Eine Untergruppe* $N \leq G$ *ist genau dann Normalteiler, wenn sie invariant ist unter allen inneren Automorphismen, d.h. wenn* $\pi_g(N) = N$ *für alle* $g \in G$ *gilt.*

Interessant ist der Spezialfall, dass $G$ eine symmetrische Gruppe ist. Dazu erweist sich die *Zyklenschreibweise* von Permutationen als sehr nützlich. Zunächst sei daran erinnert, dass wegen Proposition 3.2.5.3 die Struktur der symmetrischen Gruppe $S_X$ auf der Menge $X$ nur von der Kardinalität $|X|$ abhängt. Im endlichen Fall $|X| = n \in \mathbb{N}$ schreiben wir $S_n$ für $S_X$, wobei wir oBdA meist $X = \{1, 2, \ldots, n\}$ annehmen. Jede Permutation $\pi \in S_n$ lässt sich auf ein beliebiges $a = a_1 \in X$ iteriert anwenden. Weil $X$ endlich ist, muss es irgendwann zu einer Wiederholung kommen, genauer: Es gibt ein minimales $k \in \mathbb{N}$ derart, dass alle $a_1 = \pi^0(a_1), a_2 := \pi^1(a_1), \ldots, a_k := \pi^{k-1}(a_1)$ paarweise verschieden sind, $a_{k+1} := \pi^k(a_1)$ jedoch mit einem $a_i$ mit $1 \leq i \leq n$ übereinstimmt. Weil $\pi$ injektiv ist, folgt daraus $a_{k+1} = a_1$ (andernfalls hätte $a_{k+1}$ neben $a_k$ noch ein zweites Urbild unter $\pi$), also $i = 1$. Lässt $\pi$ alle anderen Elemente fest, so spricht man von einer *zyklischen Permutation*, einem *k-Zyklus* oder auch von einem Zyklus der Länge $k$. Diesen Zyklus schreibt man in sogenannter Zyklenschreibweise als $\pi = (a_1 a_2 \ldots a_k)$ an. Ist bereits $X = \{a_1, a_2, \ldots, a_k\}$, so ist $\pi = (a_1 a_2 \ldots a_k)$. Andernfalls gibt jedes $b \in X \setminus \{a_1, a_2, \ldots, a_k\}$ Anlass zu einem weiteren Zyklus $(b_1 b_2 \ldots b_l)$, wobei die $b_j$ nicht unter den $a_i$ vorkommen. Weil $X$ endlich ist, bricht dieser Prozess ab, und man kann $\pi$ allgemein als Produkt paarweise elementfremder Zyklen schreiben:

$$\pi = (a_{1,1} a_{1,2} \ldots a_{1,k_1})(a_{2,1} a_{2,2} \ldots a_{2,k_2}) \ldots (a_{m,1} a_{m,2} \ldots a_{m,k_m})$$

Ein Zyklus $(a)$ der Länge 1 bedeutet, dass $a = \pi(a)$ Fixpunkt von $\pi$ ist. Zur Vereinfachung der Notation vereinbart man, dass solche Zyklen nicht angeschrieben werden müssen. Zyklen der Länge 2 nennt man auch *Transpositionen*.
Man beachte, dass erstens alle zyklischen Vertauschungen

$$(a_1 a_2 \ldots a_{k-1} a_k), (a_2 a_3 \ldots a_k a_1), \ldots, (a_k a_1 \ldots a_{k-2} a_{k-1})$$

denselben Zyklus darstellen. Zweitens haben Vertauschungen von elementfremden Zyklen keinen Einfluss auf die dargestellte Permutation. Dabei unterstellen wir, was ganz allgemein vereinbart sein soll: Sind $z_1, z_2, \ldots, z_m$ Zyklen (aufgefasst als Symbolketten), die Permutationen $\pi_1, \pi_2, \ldots, \pi_m \in S_n$ darstellen, so möge die *Juxtaposition* (die durch schlichte Aneinanderreihung entstehende Zeichenkette) $z_1 z_2 \ldots z_m$ die Komposition $\pi_1 \circ \pi_2 \circ \ldots \circ \pi_m$ bezeichnen, wobei wir das Symbol $\circ$ allerdings meist weglassen werden. Zu

beachten ist, dass wegen der Assoziativität von $\circ$ beliebige Klammernsetzungen dasselbe Ergebnis liefern und somit auf weitere Klammern verzichtet werden kann.
Ist $X$ unendlich, so kann die Zyklenschreibweise offenbar auch verwendet werden, allerdings nur für jene $\pi \in S_X$ mit endlichem Träger $\{a \in X : \pi(x) \neq x\}$.
Wir fassen die wichtigsten Tatsachen über endliche Permutationsgruppen und ihre Zyklenschreibweise zusammen:

**Proposition 3.2.5.9.** *1. Die Ordnung von $S_n$ ist gegeben durch $|S_n| = n!$.*

2. *Jedes $\pi \in S_n$ hat eine Darstellung als Produkt paarweise elementfremder Zyklen. Diese Darstellung ist eindeutig bis auf a) Weglassen und Hinzufügen von 1-Zyklen, b) die Reihenfolge der Zyklen und c) zyklische Vertauschungen innerhalb der Zyklen.*

3. *Jedes $\pi \in S_n$ hat eine Darstellung als Produkt von (i.a. nicht paarweise elementfremden) Transpositionen.*

4. *Ist für $\pi \in S_n$ die Zahl*

$$f(\pi) := |\{(i,j) : 1 \leq i < j \leq n \text{ und } \pi(i) > \pi(j)\}|$$

*der sogenannten* Fehlstände *von $\pi$ gerade, so ist in jeder Darstellung von $\pi \in S_n$ als Produkt von Transpositionen deren Anzahl gerade. So ein $\pi$ heißt eine* gerade Permutation.

*Ist hingegen $f(\pi)$ ungerade, so ist in jeder Darstellung von $\pi \in S_n$ als Produkt von Transpositionen deren Anzahl ungerade. So ein $\pi$ heißt eine* ungerade Permutation.

5. *Die sogenannte* Signumfunktion $\operatorname{sgn}\colon S_n \to \{-1, 1\}$, *die geraden Permutationen den Wert 1 und ungeraden den Wert $-1$ zuweist, ist ein Gruppenhomomorphismus von $S_n$ in die multiplikative Gruppe $\{-1, 1\}$.*

6. *Die geraden Permutationen $\pi \in S_n$ bilden einen Normalteiler von $S_n$, die sogenannte* alternierende Gruppe *$A_n$ der Ordnung $|A_n| = \frac{n!}{2}$ für $n \geq 2$ bzw. $|A_1| = 1$.*

7. *Ein Zyklus der Länge $k$ ist gerade (ungerade) genau dann, wenn $k$ ungerade (gerade) ist.*

*Beweis.* 1. Für $k \leq n \in \mathbb{N}$ sei $A(k,n)$ die Anzahl der injektiven Abbildungen von einer $k$- in eine $n$-elementige Menge. Dann ist $A(0,n) = 1$, $A(1,n) = n$, $A(2,n) = n(n-1)$, allgemein (Induktion nach $k$) $A(k,n) = \frac{n!}{(n-k)!}$, insbesondere also $|S_n| = A(n,n) = n!$.

2. Folgt aus den Bemerkungen vor dieser Proposition.

3. Wegen $(a_1 a_2 \dots a_k) = (a_1 a_2)(a_2 a_3) \dots (a_{k-1} a_k)$ gilt die Behauptung für Zyklen, und wegen Aussage 2 überträgt sie sich von Zyklen auf beliebige $\pi \in S_n$.

4. Offenbar hat die identische Permutation id keinen Fehlstand, also ist $f(\mathrm{id}) = 0$ gerade. Weil sich nach Aussage 2 jedes beliebige $\pi \in S_n$ als Produkt von Transpositionen schreiben lässt, genügt es zu zeigen, dass sich durch Multiplikation mit einer einzigen Transposition die Parität der Anzahl der Fehlstände (gerade oder ungerade, Anzahl modulo 2) ändert, was aus Übungsaufgabe 3.2.5.10 folgt.

5. Mittels 4. überzeugt man sich unmittelbar, dass für jeden der vier Fälle (gerade/gerade, gerade/ungerade, ungerade/gerade, ungerade/ungerade) die Homomorphiebedingung $\mathrm{sgn}(\pi\sigma) = \mathrm{sgn}(\pi)\,\mathrm{sgn}(\sigma)$ erfüllt ist.

6. Wegen 5. ist die Menge $A_n$ der geraden Permutationen der Kern des Homomorphismus sgn und als solcher ein Normalteiler. Für $n \geq 2$ gibt es mindestens eine Transposition $\tau \in S_n$. Die Nebenklasse $\tau A_n$ besteht genau aus den ungeraden Permutationen und hat gleich viele Elemente wie $A_n$, woraus $|A_n| = \frac{n!}{2}$ folgt. Die Behauptung $|A_1| = 1$ schließlich ist trivial.

7. In der Produktdarstellung $(a_1 a_2 \dots a_k) = (a_1 a_2)(a_2 a_3) \dots (a_{k-1} a_k)$ ist die Anzahl der Transpositionen $k - 1$, woraus mit 4. die Behauptung folgt. □

**UE 166** ► **Übungsaufgabe 3.2.5.10.** (F) Zeigen Sie: Ist $\pi \in S_n$ und $\tau$ eine Transposition, so gilt entweder $|\tau \circ \pi| = |\pi| + 1$ oder $|\tau \circ \pi| = |\pi| - 1$. (Bezeichnungsweisen wie in Aussage 4 von 3.2.5.9.) ◄ **UE 166**

Mit Hilfe der Zyklenschreibweise wiederholen wir bzw. sieht man sehr leicht:

**Proposition 3.2.5.11.** *1. Die Permutationen $\pi, \pi' \in S_n$ mögen die Darstellungen $\pi = \zeta_1 \zeta_2 \dots \zeta_k$ und $\pi' = \zeta'_1 \zeta'_2 \dots \zeta'_{k'}$ als Produkte von Zyklen $\zeta_i$ bzw. $\zeta'_i$ haben. Sind alle $\zeta_i$ zu allen $\zeta'_j$ elementfremd, so vertauschen $\pi$ und $\pi'$, d.h. $\pi\pi' = \pi'\pi$.*

*2. Sei $\pi = \zeta_1 \zeta_2 \dots \zeta_k$ eine Darstellung der Permutation $\pi \in S_n$ als Produkt paarweise elementfremder Zyklen der Längen $l_1, l_2, \dots, l_k$. Dann ist die Ordnung von $\pi$ gegeben durch* $\mathrm{ord}(\pi) = \mathrm{kgV}(l_1, l_2, \dots, l_k)$.

*3. Sei*

$$\pi = (a_{1,1} a_{1,2} \dots a_{1,l_1}) \dots (a_{k,1} a_{k,2} \dots a_{k,l_k})$$

*eine Darstellung der Permutation $\pi \in S_n$ als Produkt von Zyklen und $\sigma \in S_n$ beliebig. Dann erhält man eine Darstellung der zu $\pi$ bezüglich $\sigma$ konjugierten Permutation $\sigma\pi\sigma^{-1}$, indem man in der Zyklendarstellung von $\pi$ jedes $a_{i,j}$ durch $\sigma(a_{i,j})$ ersetzt, also:*

$$\sigma\pi\sigma^{-1} = (\sigma(a_{1,1})\sigma(a_{1,2}) \dots \sigma(a_{1,l_1})) \dots (\sigma(a_{k,1})\sigma(a_{k,2}) \dots \sigma(a_{k,l_k}))$$

*4. Eine Untergruppe $N \leq S_n$ ist genau dann Normalteiler $N \lhd S_n$ von $S_n$, wenn sie von jedem Permutationstyp entweder kein oder alle $\pi \in S_n$ dieses Typs enthält. Unter dem Permutationstyp von $\pi \in S_n$ sei dabei die Familie $(v_k(\pi))_{k \in \mathbb{N}}$ verstanden, wobei $v_k(\pi)$ die Anzahl der Zyklen der Länge $k$ in einer (und damit in jeder beliebigen) Darstellung von $\pi$ als Produkt elementfremder Zyklen ist.*

*Beweis.* 1. Haben wir schon verwendet.

2. Ein Zyklus der Länge $\ell$ hat offenbar die Ordnung $\ell$. Sind $\pi = \zeta_1\zeta_2\dots\zeta_k$ und $\pi' = \zeta'_1\zeta'_2\dots\zeta'_{k'}$ zwei Produkte paarweise elementfreier Zyklen, wobei zusätzlich auch $\zeta_i$ und $\zeta'_j$ kein Element gemeinsam haben, so gilt $\langle\pi\rangle \cap \langle\pi'\rangle = \{\mathrm{id}\}$: Jede Permutation in $\langle\pi\rangle$ hält alle Elemente fest, die in der Zyklendarstellung von $\pi$ nicht vorkommen. Dieselbe Aussage gilt für $\pi'$. Somit muss eine Permutation $\sigma \in \langle\pi\rangle \cap \langle\pi'\rangle$ jedes Element festhalten, das nicht in beiden Zyklendarstellungen vorkommt. Nach Annahme kann kein Element in beiden Zyklendarstellungen vorkommen, womit $\sigma$ alle Elemente festhalten muss, also $\sigma = \mathrm{id}$. Mit dieser Tatsache folgt die Aussage aus der ersten Aussage zusammen mit Aussage 4. aus 3.2.4.11 mittels Induktion nach $k$.

3. Ergibt sich unmittelbar aus $\sigma\pi\sigma^{-1}(\sigma(a)) = \sigma\pi(a)$.

4. Laut Folgerung 3.2.5.8 ist eine Untergruppe genau dann Normalteiler, wenn sie bezüglich innerer Automorphismen, d.h. bezüglich allen Konjugationen abgeschlossen ist. Das wiederum ist laut 3. genau dann der Fall, wenn sie mit jedem $\pi$ eines gewissen Permutationstyps alle Permutationen dieses Typs enthält. □

Die Nützlichkeit all dieser Erkenntnisse zeigt sich zum Beispiel im Folgenden.

**Proposition 3.2.5.12.** *Sei $G := S_X$ die symmetrische Gruppe auf der Menge $X$.*

1. *Für $|X| \geq 3$ ist das Zentrum von $G$ trivial: $Z(S_X) = \{\mathrm{id}_X\}$. Folglich ist in diesem Fall der Homomorphismus $\Phi\colon G \to \mathrm{Aut}(G)$ aus 3.2.5.6 eine isomorphe Einbettung.*

2. *Ist $|X| \geq 3$ und $|X| \neq 6$, so ist jeder Automorphismus von $G = S_X$ ein innerer Automorphismus. Folglich ist $\Phi\colon G \to \mathrm{Aut}(G)$ sogar ein Isomorphismus.*

3. *Für $|X| = 6$ gibt es Automorphismen von $G = S_X$, die keine inneren Isomorphismen sind.*

**UE 167** ► **Übungsaufgabe 3.2.5.13.** (E) Beweisen Sie Proposition 3.2.5.12. Zur Orientierung: Die erste Aussage ist relativ leicht. Die zweite braucht vor allem kombinatorische Überlegungen. Die dritte ist sehr anspruchsvoll. ◄ **UE 167**

**UE 168** ► **Übungsaufgabe 3.2.5.14.** (F) Geben Sie eine Gruppe $G$ mit zwei Untergruppen $H$ und $J$ mit $J \subseteq H \subseteq G$ an, so dass $J \lhd H$ und $H \lhd G$, nicht aber $J \lhd G$. (Hinweis: Sei $G$ z.B. die alternierende Gruppe $A_4$ oder die Gruppe aller Drehungen und Spiegelungen, die ein festes Quadrat auf sich abbilden.) ◄ **UE 168**

Zum Abschluss noch ein Beispiel, wo anhand der symmetrischen Gruppe $S_4$ der erste Isomorphiesatz für Gruppen (3.2.2.13, erste Aussage) illustriert wird.

**UE 169** ► **Übungsaufgabe 3.2.5.15.** (F) Sei $G := S_4$. Wir geben die Elemente von $G$ in Zyklenschreibweise an. Sei $U$ die vom Element (1234) erzeugte Untergruppe und $N = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$. Begründen Sie, warum $N \lhd S_4$ ein Normalteiler ist. Bestimmen Sie die Gruppen $NU$, $N \cap U$, $NU/N$, $U/(N \cap U)$ und geben Sie den kanonischen Isomorphismus zwischen $NU/N$ und $U/(N \cap U)$ explizit an. ◄ **UE 169**

**UE 170** ► **Übungsaufgabe 3.2.5.16.** (F) Sei $N_i \lhd G_i$ für $i = 1, 2$, $N_1 \cong N_2$ und $G_1/N_1 \cong G_2/N_2$. Folgt daraus $G_1 \cong G_2$? ◄ **UE 170**

### 3.2.6 Symmetrie

Inhalt in Kurzfassung: Der Begriff der Symmetrie hat eindeutig geometrischen Ursprung. Die adäquate mathematische Fassung dieses Phänomens fußt jedoch auf dem Gruppenbegriff. Im vorliegenden, letzten Unterabschnitt zur elementaren Gruppentheorie wird das ausblicksartig beleuchtet, vorwiegend unter historischen Gesichtspunkten und völlig ohne neue Resultate.

Der Begriff der Gruppe hat die Entwicklung der Mathematik im Laufe des 19. Jahrhunderts in ähnlicher Weise vorangetrieben wie der des Grenzwertes. Beim Grenzwert ging es vor allem um die Exaktifikation eines intuitiv recht eingängigen Konzeptes, das schon seit etwa 200 Jahren im Zentrum vieler Bestrebungen stand. Doch erst mit dem Begriff der Gruppe begann jene Tendenz zur Abstraktion, die wesentliche Teile der modernen Mathematik durchzieht, insbesondere die Algebra.
Historischer Ausgangspunkt war die Galoistheorie[13], siehe Kapitel 9 (Algebra II). In heutiger Sprechweise spielen darin Gruppen von Automorphismen von Körpern eine zentrale Rolle. Die Struktur dieser Gruppen ermöglicht entscheidende Rückschlüsse auf die ursprünglich gegebenen Objekte (der Körper, in denen Lösungen von algebraischen Gleichungen liegen). Ähnliche Motivationen veranlassten Felix Klein (1849 – 1925) im Jahr 1872, sein berühmtes *Erlanger Programm* zu formulieren, das – sehr verkürzt formuliert – darin besteht, geometrische Eigenschaften als Invarianten unter gewissen Transformationen zu begreifen, die eine Gruppe bilden. Beiden Situationen gemeinsam ist das Bestreben, eine Struktur über ihre inhärenten abstrakten Symmetrien zu verstehen. Diesem ersten Abstraktionsschritt von elementaren Objekten hin zu ihren Symmetriegruppen sind in der neueren Entwicklung der Mathematik noch zahlreiche ähnliche gefolgt. Kleine Kostproben davon haben wir schon kennengelernt, indem wir zunächst von arithmetischen Gesetzen zu Strukturen übergingen, in denen solche Gesetze gelten, und dann weiter zu Klassen (Varietäten, Kategorien) solcher Strukturen.
Unter speziell gruppentheoretischem Gesichtspunkt seien als Beispiele hier lediglich lineare Gruppen erwähnt. Geht man von einem Vektorraum $V$ über einem Körper $K$ aus, so bietet sich die Automorphismengruppe $\mathrm{Aut}(V)$ an, die man auch *allgemeine lineare Gruppe* nennt. Ist $V$ von endlicher Dimension $n$, so lässt sich diese Gruppe identifizieren

[13] benannt nach dem französischen Mathematiker Évariste Galois (1811-1832)

mit der multiplikativen Gruppe aller regulären $n \times n$-Matrizen über $K$. Man schreibt für diese Gruppe auch $\mathrm{GL}(n, K)$ (für *General Linear Group*). Darin liegt als Untergruppe die sogenannte *spezielle lineare Gruppe* $\mathrm{SL}(n, K)$, die nur die Matrizen mit Determinante 1 enthält. Faktorisiert man die allgemeine lineare Gruppe nach $K \setminus \{0\}$, so erhält man die ebenfalls wichtige *projektive lineare Gruppe* $\mathrm{PLG}(n, K)$. Weitere sehr interessante Gruppen linearer Transformationen sind die *orthogonale Gruppe* $\mathrm{O}(n)$ (über $\mathbb{R}$), und die *unitäre Gruppe* $\mathrm{U}(H)$ (über einem komplexen Hilbertraum $H$).
Die Strukturanalyse der linearen Gruppen ist so weit fortgeschritten, dass man versucht, beliebige Gruppen mit linearen Gruppen in Verbindung zu bringen. Insbesondere ist das der Zugang der sogenannten *Darstellungstheorie*, wo man versucht für eine Gruppe $G$ sämtliche Homomorphismen von $G$ in eine lineare Gruppe (sogenannte *lineare Darstellungen* von $G$) zu verstehen und damit von diesen auf $G$ rückzuschließen.

## 3.3 Moduln, insbesondere abelsche Gruppen

Moduln interessieren uns an dieser Stelle vor allem deshalb, weil abelsche Gruppen stets auch unitäre Moduln über dem Ring $\mathbb{Z}$ und in gewissen Fällen auch über $\mathbb{Z}_m$ sind (3.3.1). Das ergibt einen klareren Blick auf ihre Struktur. Aufgrund dieser Fokussierung benötigen wir – obwohl der Ringbegriff im Modulbegriff vorkommt – in diesem Abschnitt keine tieferen Kenntnisse über Ringe, wie wir sie in 3.4 entwickeln werden.
In 3.3.2 befassen wir uns mit den grundlegenden Konstruktionen, bevor in 3.3.3 und 3.3.4 als Hauptergebnis dieses Abschnitts die Struktur endlicher abelscher Gruppen geklärt wird. Eine vertiefende Fortsetzung des Themas, insbesondere die Analyse von Auswirkungen gewisser Eigenschaften des zugrundeliegenden Rings, ist Inhalt von Kapitel 7.

### 3.3.1 Abelsche Gruppen als Moduln über $\mathbb{Z}$ und $\mathbb{Z}_m$

Inhalt in Kurzfassung: Die übliche Notation für additive Potenzen zusammen mit den elementaren Potenzrechenregeln aus 3.1.1 zeigt unmittelbar, dass jede abelsche Gruppe in natürlicher Weise auch ein Modul über dem Ring $\mathbb{Z}$ ist. In diesem Zusammenhang werden für abelsche Gruppen auch Begriffe wie Torsionselement, Torsionsanteil, $p$-Element ($p \in \mathbb{P}$), Exponent u.ä. definiert.

Im Folgenden schreiben wir abelsche Gruppen stets in additiver Notation $(A, +, 0, -)$ und verwenden folgende Notationen und Sprechweisen:

**Definition 3.3.1.1.** Sei $A$ eine abelsche Gruppe. Dann heißt jedes $a \in A$ mit endlicher Ordnung $\mathrm{ord}(a)$ *Torsionselement*. Gilt stärker $\mathrm{ord}(a) = p^e$ mit $p \in \mathbb{P}$ und $e \in \mathbb{N}$, so heißt $a$ auch *$p$-Element*. Die Menge aller Torsionselemente von $A$ heißt der *Torsionsanteil*. Wir bezeichnen ihn mit $A_t$. Die Menge aller $p$-Elemente von $A$ heißt der *$p$-Anteil* von $A$. Wir bezeichnen ihn mit $A_p$. Gibt es ein $m \in \mathbb{N}^+$ mit $ma = 0$ für alle $a \in A$, so heißt das kleinste unter diesen $m$ auch der *Exponent* der abelschen Gruppe $A$. Dieser wird auch mit $\exp(A)$ bezeichnet.

Schreiben wir die Potenzrechenregeln aus Proposition 3.1.1.10 für abelsche Gruppen in additiver Schreibweise an, so erhalten wir[14]

1. $(m+n)a = ma + na$
2. $m(na) = (mn)a$
3. $n(a+b) = na + nb$

für alle $a, b \in A$ und alle $m, n \in \mathbb{Z}$. Gemeinsam mit der nach Definition geltenden Gleichung $1a = a$ (für alle $a \in A$) sind das genau die definierenden Gesetze eines unitären $\mathbb{Z}$-Moduls, siehe Definition 2.1.3.6.
Nehmen wir ferner an, es gibt ein $m \in \mathbb{N}^+$ mit $ma = 0$ für alle $a \in A$. Das bedeutet, dass $m$ ein Vielfaches aller additiven Ordnungen von Elementen $a \in A$ und somit des Exponenten von $A$ ist. In diesem Fall ist $A$ sogar ein $\mathbb{Z}_m$-Modul, weil dann $ka$ von $k$ nur über die Restklasse von $k$ modulo $m$ abhängt, genauer: Aus $k_1 \equiv k_2 \mod m$ folgt $k_2 = k_1 + nm$ mit $n \in \mathbb{Z}$, also $k_2 a = (k_1 + nm)a = k_1 a + n(ma) = k_1 a$. Somit ist in diesem Fall durch $(k + m\mathbb{Z})a := ka$, $k \in \mathbb{Z}$ und $a \in A$, eine Struktur auf $A$ wohldefiniert. Die Gesetze für einen unitären $\mathbb{Z}_m$-Modul vererben sich direkt von denen eines unitären $\mathbb{Z}$-Moduls. Wir erhalten also:

**Proposition 3.3.1.2.** *Jede abelsche Gruppe $A$ ist ein unitärer $\mathbb{Z}$-Modul vermittels $(k, a) \mapsto ka$, $k \in \mathbb{Z}$ und $a \in A$. Im Fall $\exp(A)|m$ mit positivem $m \in \mathbb{N}$ ist $A$ auch ein unitärer $\mathbb{Z}_m$-Modul vermittels $(k + m\mathbb{Z}, a) \mapsto ka$, $k \in \mathbb{Z}$ und $a \in A$.*

Über den Begriff der Ordnung bzw. des Exponenten erscheint klar, dass das Studium von Elementen $ka$ mit $k \in \mathbb{Z}$ und $a \in A$ lohnend ist. In Proposition 3.2.4.11 klingen bereits zwei wichtige Tatsachen an: Einerseits spielen Teilbarkeitsüberlegungen (zu den ganzen Zahlen $k$) eine wesentliche Rolle, andererseits gelten manche Aussagen nur unter einer zusätzlichen Kommutativitätsvoraussetzung. Daher entwickelt dieser Ansatz seine volle Stärke erst im Fall abelscher Gruppen; tatsächlich bilden derartige Teilbarkeitsüberlegungen das Rückgrat der Strukturanalyse abelscher Gruppen, wie wir sie in diesem Abschnitt anstellen wollen. Aus diesem Grund ist es erhellend, die Operationen $a \mapsto ka$ für festes $k \in Z$ bzw. $\mathbb{Z}_m$ als Teil der Struktur der abelschen Gruppe zu sehen – genau das leistet der Begriff des Moduls.

### 3.3.2 Unter- und Faktormoduln, Homomorphismen, Produkte und direkte Summen

Inhalt in Kurzfassung: Die grundlegenden Konstruktionen für Moduln verlaufen weitgehend analog zur Situation bei Gruppen bzw. bei Vektorräumen aus der Linearen Algebra. Wegen der Kommutativität der additiven Gruppe eines Moduls vereinfacht sich die Situation bei inneren direkten Produkten/Summen im Vergleich zu beliebigen Gruppen.

[14] Es sei explizit betont, dass die Kommutativität der Gruppenoperation dabei nur beim Distributivgesetz von rechts $n(a+b) = na + nb$ eingeht; die anderen Aussagen würden auch ohne diese Voraussetzung gelten.

Sei $A$ ein $R$-Modul, d.h. ein Modul über einem Ring $R$. Eine Teilmenge $U \subseteq A$ ist genau dann ein Untermodul $U \leq A$, wenn $U \leq A$ als (abelsche) Gruppe und zusätzlich $ru \in U$ für alle $r \in R$ und $u \in U$. Das ist genau dann der Fall, wenn $U$ abgeschlossen ist bezüglich der Bildung von *Linearkombinationen*, d.h. wenn für alle $r_1, \ldots, r_n \in R$ und $a_1, \ldots, a_n \in U$ auch

$$\sum_{i=1}^{n} r_i a_i \in U.$$

Entsprechend dienen Linearkombinationen auch zur Charakterisierung von $R$-Modul-Homomorphismen, den sogenannten *$R$-linearen Abbildungen*. Nach der allgemeinen Definition von Homomorphismen muss ein $R$-Modul-Homomorphismus $f\colon A \to B$ zwischen zwei $R$-Moduln $A$ und $B$ verträglich sein mit den fundamentalen Operationen: Addition, Nullelement, additives Inverses und Multiplikation mit $r$ für alle $r \in R$. Offenbar ist das genau dann der Fall, wenn für alle $r_1, \ldots, r_n \in R$ und $a_1, \ldots, a_n \in A$

$$f\left(\sum_{i=1}^{n} r_i a_i\right) = \sum_{i=1}^{n} r_i f(a_i)$$

gilt, wenn also $f$ verträglich mit allen Linearkombinationen ist.
Wie bei Gruppen nennt man

$$\ker(f) := \{a \in A :\ f(a) = 0\}$$

den *Kern* von $f$. Weil $f$ auch ein Homomorphismus von Gruppen ist, kommen als Kerne nur Normalteiler von $A$ in Frage, also additive Untergruppen von $A$. Diese stehen mit den Kongruenzrelationen $\sim$ auf $A$ durch die Bedingung $K = [0]_\sim$ in einer bijektiven Beziehung. $\ker(f)$ hat noch die zusätzliche Eigenschaft, ein Untermodul zu sein: $r \in R$ und $a \in \ker(f)$ impliziert $f(a) = 0$ und somit auch $f(ra) = rf(a) = r0 = 0$,[15] also $ra \in \ker(f)$. Kerne sind also stets Untermoduln. Umgekehrt definiert jeder Untermodul $U \leq A$ eine Kongruenzrelation $\sim$, indem man definiert: $a \sim b$ genau dann, wenn $a - b \in U$. Die Verträglichkeit von $\sim$ mit der Gruppenstruktur wissen wir schon von den Gruppen, und für die Multiplikation mit einem Ringelement $r \in R$ gilt: Aus $a \sim b$ folgt $a - b \in U$, wegen der Untermoduleigenschaft von $U$ weiter $ra - rb = r(a-b) \in U$ und somit $ra \sim rb$. Also:

**Proposition 3.3.2.1.** *Ist $A$ ein Modul über dem Ring $R$, so stehen die Kongruenzrelationen $\sim$ auf $A$ und die Untermoduln $U \leq A$ durch die Bedingung*

$$\forall a, b \in A :\ a \sim b \quad \textit{genau dann wenn} \quad a - b \in U$$

*in einer bijektiven Beziehung zueinander.*

Schreiben wir $A/U$ für den Faktormodul $A/_\sim$, wenn $U \leq A$ und die Kongruenzrelation $\sim$ gemäß 3.3.2.1 zusammengehören, so bedeutet das: Sämtliche Faktormoduln eines $R$-Moduls $A$ sind gegeben durch sämtliche $A/U$ mit $U \leq A$. Die Elemente von $A/U$ sind wie

[15] Es gilt $r0 = 0$ für alle $r \in R$: Wir rechnen nämlich $r0 = r(0+0) = r0 + r0$, woraus durch Kürzen (Addition von $-r0$) $r0 = 0$ folgt. Analog sieht man $0a = 0$ für alle $a \in A$.

bei Faktorgruppen Nebenklassen $a+U$ und gehorchen den Operationen $r(a+U) = ra+U$, $(a_1+U)+(a_2+U) = (a_1+a_2)+U$ und $-(a+U) = -a+U$. Das Nullelement in $A/U$ ist $0+U = U$.
Unter Verwendung des Homomorphiesatzes 2.3.3.16 ergibt das auch eine Beschreibung sämtlicher Homomorphismen auf $A$: Ist $f\colon A \to B$ irgendein oBdA surjektiver Modulhomomorphismus, dann ist $U := \ker(f) \leq A$ mit $A/U \cong B$ vermittels des Isomorphismus $a+U \mapsto f(a)$.

Wir wenden uns nun direkten Produkten zu. Sei $I$ eine (im Allgemeinen unendliche) Indexmenge und für jedes $i \in I$ ein $R$-Modul $A_i$ gegeben. Wie im Fall von Gruppen enthält das direkte Produkt $A := \prod_{i\in I} A_i$ der $A_i$ den Untermodul

$$\bigoplus_{i\in I} A_i := \left\{ (a_i)_{i\in I} \in \prod_{i\in I} A_i : \ a_i \neq 0 \text{ nur für endlich viele } i \in I \right\},$$

den wir im Kontext von Moduln und (additiv geschriebenen) abelschen Gruppen nur selten als schwaches Produkt sondern meistens als *(äußere) direkte Summe* der $A_i$ bezeichnen und mit dem Symbol $\bigoplus$ statt $\prod^w$ anschreiben. Die kanonischen Einbettungen $\iota_{i_0} : A_{i_0} \to \prod_{i\in I} A_i$ bilden in die direkte Summe $\bigoplus_{i\in I} A_i$ ab. Ist $I$ endlich, so stimmen direktes Produkt und direkte Summe wieder überein.
Eine der wichtigsten Eigenschaften der direkten Summe von Moduln bzw. abelschen Gruppen ist die folgende Beobachtung.

**Proposition 3.3.2.2.** *Seien $A_i$, $i \in I$, $R$-Moduln, sei $B$ ein weiterer $R$-Modul und seien $f_i : A_i \to B$ Modulhomomorphismen. Bezeichnet $\iota_{i_0} : A_{i_0} \to \prod_{i\in I} A_i$ die kanonischen Einbettungen, dann gibt es einen eindeutigen Homomorphismus $h : \bigoplus_{i\in I} A_i \to B$, der $h \circ \iota_{i_0} = f_{i_0}$ für alle $i_0 \in I$ erfüllt.*

**UE 171 ► Übungsaufgabe 3.3.2.3.** (V) Beweisen Sie Proposition 3.3.2.2. **◄ UE 171**

In Proposition 3.3.2.2 kommt eine Dualität zu Proposition 2.3.2.4 zum Ausdruck, die in Abschnitt 4.2.1 Anlass zur Definition sogenannter *Koprodukte* geben wird. Man beachte, dass wir dabei auf Moduln, somit abelschen Gruppen, arbeiten müssen. Für beliebige Gruppen ist die Proposition tatsächlich falsch. Der in diesem Zusammenhang entscheidende Unterschied zwischen abelschen und allgemeinen Gruppen bzw. die dahinterstehende Problematik kommt bereits in der folgenden Übungsaufgabe zum Ausdruck:

**UE 172 ► Übungsaufgabe 3.3.2.4.** (F) Wir betrachten die Gruppe $\mathbb{Z}\times\mathbb{Z}$ mit der punktweisen Addition. Sei $b_1 := (1,0)$, $b_2 := (0,1)$. Welche der folgenden Aussagen ist wahr? (Beweis bzw. Gegenbeispiel.) **◄ UE 172**

(1) Für alle Gruppen $H$ und alle $h_1, h_2 \in H$ gibt es einen eindeutig bestimmten Homomorphismus $\varphi\colon \mathbb{Z}\times\mathbb{Z} \to H$ mit $\varphi(b_1) = h_1$, $\varphi(b_2) = h_2$.

(2) Für alle abelschen Gruppen $H$ und alle $h_1, h_2 \in H$ gibt es einen eindeutig bestimmten Homomorphismus $\varphi\colon \mathbb{Z}\times\mathbb{Z} \to H$ mit $\varphi(b_1) = h_1$, $\varphi(b_2) = h_2$.

Wie in Gruppen unterscheidet man von dieser *äußeren* direkten Summe die *innere* direkte Summe:

**Definition 3.3.2.5.** Ein $R$-Modul $A$ heißt *innere direkte Summe* seiner Untermoduln $U_i \leq A$, wenn die Abbildung

$$\varphi\colon \bigoplus_{i\in I} U_i \to A, \quad (u_i)_{i\in I} \mapsto \sum_{i\in I} u_i$$

ein Isomorphismus von $R$-Moduln ist. Man schreibt in diesem Fall auch oft $A = \bigoplus_{i\in I} U_i$ oder im Fall von $|I| = 2$, sagen wir $I = \{1, 2\}$, auch $A = U_1 \oplus U_2$.

Man beachte, dass die Abbildung $\varphi$ aus Definition wieder deshalb wohldefiniert ist, weil die Summe, wenn man alle Summanden mit $a_i = 0$ weglässt, zur endlichen Summe wird.

*Bemerkung* 3.3.2.6. Ganz analog zu Gruppen (vgl. Proposition 3.2.3.12) ist eine äußere direkte Summe von Moduln immer auch eine innere direkte Summe der Bilder dieser Moduln unter den kanonischen Einbettungen. Umgekehrt ist jede innere direkte Summe nach Definition isomorph zur äußeren direkten Summe derselben Objekte. Daher kann man Resultate über äußere direkte Summen auf innere direkte Summen übertragen – besonders hervorgehoben sei das an dieser Stelle für Proposition 3.3.2.2.
Diese Übertragbarkeit bzw. Isomorphie rechtfertigt auch, wieso wir das Symbol $\oplus$ sowohl für äußere als auch für innere direkte Summen verwenden.

Wie bei Gruppen gibt es sehr nützliche Charakterisierungen, wann ein Modul bzw. eine abelsche Gruppe die innere direkte Summe von gegebenen Untermoduln bzw. Untergruppen ist. Wir konzentrieren uns in der Herleitung auf abelsche Gruppen, da sich hier die Resultate direkt durch Spezialisierung der entsprechenden Charakterisierungen für Gruppen (Proposition 3.2.3.2, Satz 3.2.3.7 und Satz 3.2.3.14) ergeben. Geht man die Beweise der Ergebnisse für Gruppen durch, so stellt man fest, dass die Beweise genauso auch für Moduln funktionieren,[16] sodass wir die Charakterisierungen für Moduln formulieren werden.
Bevor wir dazu kommen, müssen wir noch eine formale Frage klären. Fasst man abelsche Grupen als $\mathbb{Z}$-Moduln auf, so können wir die grundlegenden Konstruktionen im Kontext abelscher Gruppen auf zwei Arten durchführen – einmal als Spezialisierung von beliebigen Gruppen und einmal als Spezialisierung von Moduln. Es macht dabei keinen Unterschied, welche dieser Varianten man wählt, wie die folgende Übungsaufgabe zeigt. Diese Tatsache rechtfertigt einmal mehr unser Vorgehen, abelsche Gruppen als $\mathbb{Z}$-Moduln zu betrachten.

**Proposition 3.3.2.7.** *Seien $A$ und $B$ abelsche Gruppen, $U, U_i \leq A$, $i \in I$, Untergruppen von $A$ und $m$ eine positive natürliche Zahl. Dann gilt:*

1. *$U \leq A$ ist auch ein Unter-$\mathbb{Z}$-Modul von $A$. Im Fall $\exp(A)|m$ ist $U$ überdies ein Unter-$\mathbb{Z}_m$-Modul von $A$.*

[16] Der entscheidende Grund ist, dass im Modulfall die Abbildung $\varphi\colon \bigoplus_{i\in I} U_i \to A, \quad (u_i)_{i\in I} \mapsto \sum_{i\in I} u_i$ wegen der Distributivgesetze automatisch mit der Multiplikation mit Ringelementen verträglich ist, unabhängig von besonderen Eigenschaften der Untermoduln $U_i$.

2. *Jeder Gruppenhomorphismus $\varphi : A \to B$ ist auch ein $\mathbb{Z}$-Modulhomomorphismus, im Fall $\exp(A)|m$ überdies ein $\mathbb{Z}_m$-Modulhomomorphismus.*

3. *Ist $A$ die innere direkte Summe der $U_i$ als (abelsche) Gruppe (gemäß Definition 3.2.3.11), so auch als $\mathbb{Z}$-Modul (gemäß Definition 3.3.2.5), im Fall $\exp(A)|m$ überdies als $\mathbb{Z}_m$-Modul (ebenfalls gemäß Definition 3.3.2.5).*

**UE 173 ► Übungsaufgabe 3.3.2.8.** (V) Beweisen Sie Proposition 3.3.2.7. **◄ UE 173**

Die entscheidende Beobachtung bei der Spezialisierung der Charakterisierungen auf abelsche Gruppen ist, dass jede Untergruppe automatisch ein Normalteiler ist und dass für $x \in U_i$ und $y \in U_j$ automatisch $xy = yx$ gilt. Somit sind die Bedingungen (2) in Proposition 3.2.3.2 und (B) sowie (B') in Satz 3.2.3.7 und Satz 3.2.3.14) stets erfüllt und daher überflüssig. Wir erhalten also:

**Proposition 3.3.2.9.** *Ein $R$-Modul $A$ ist genau dann die innere direkte Summe von Untermoduln $U, V \leq A$, wenn sowohl $U \cap V = \{0\}$ als auch $A = U + V$ gilt.*

**Folgerung 3.3.2.10.** *Ein $R$-Modul $A$ ist genau dann die innere direkte Summe von Untermoduln $U_1, \ldots, U_n$, wenn folgende zwei Bedingungen erfüllt sind:*

1. *$A = U_1 + U_2 + \ldots + U_n$*

2. *Für alle $i = 1, \ldots, n$ gilt $U_i \cap (U_1 + U_2 + \ldots U_{i-1} + U_{i+1} + \ldots + U_n) = \{0\}$.*

**Satz 3.3.2.11.** *Ein $R$-Modul $A$ ist genau dann die innere direkte Summe von Untermoduln $U_i \leq A$, $i \in I$, wenn die folgenden beiden Bedingungen erfüllt sind:*

1. *Zu jedem $a \in A$ gibt es endlich viele $i_1, \ldots, i_n \in I$, $u_1 \in U_{i_1}, \ldots, u_n \in U_{i_n}$ mit $a = \sum_{i=1}^{n} u_i$.*

2. *Ist $i \in I$ und verschieden von allen $i_1, \ldots, i_n \in I$, so ist $U_i \cap (U_{i_1} + \ldots + U_{i_n}) = \{0\}$.*

*Bemerkung* 3.3.2.12. Sei $A$ sogar ein unitärer $R$-Modul, d.h. $R$ habe ein Einselement $1_R$, für das $1_R a = a$ für alle $a \in A$ gilt. Beachtet man, dass die $U_i$ stets Untermoduln sind und daher $ru \in U_i$ für alle $r \in R$ und $u \in U_i$ gilt, so ist die erste Bedingung aus Satz 3.3.2.11 äquivalent zur folgenden Bedingung (um aus untenstehender Bedingung die Bedingung aus dem Satz zu folgern, wählt man $r_i = 1_R$):

> Zu jedem $a \in A$ gibt es endlich viele $i_1, \ldots, i_n \in I$, $u_1 \in U_{i_1}, \ldots, u_n \in U_{i_n}$ und $r_1, \ldots, r_n \in R$ mit $a = \sum_{i=1}^{n} r_i u_i$.

Mit anderen Worten ist diese Bedingung also äquivalent dazu, dass $A$ von den $U_i$ erzeugt wird, siehe auch Proposition 2.3.1.18.

Wir werden in den nächsten beiden Unterabschnitten sehen, dass sich aus den zyklischen Gruppen sämtliche endlichen abelschen Gruppen ergeben; siehe Satz 3.3.4.2 (in Algebra II, vgl. Satz 7.4.3.1, werden wir dasselbe sogar für endlich *erzeugte* abelsche Gruppen zeigen). Die folgende Übungsaufgabe kann sowohl als Vorbereitung darauf als auch als Gruppenversion (der klassischen Fassung) des chinesischen Restsatzes (siehe Satz 3.4.7.2) betrachtet werden.

**UE 174 ► Übungsaufgabe 3.3.2.13.** (W) **◄ UE 174**

(1) $C_n \times C_m$ ist genau dann zyklisch, wenn $n$ und $m$ keinen gemeinsamen Teiler $d > 1$ haben. (Hinweis: finden Sie einen expliziten Isomorphismus $f : C_{mn} \to C_m \times C_n$, indem Sie zuerst einen Wert für $f(1)$ vorschreiben.)

(2) Zeigen Sie (äußere direkte Summe)

$$C_n \cong \bigoplus_{p \in \mathbb{P}} C_{p^{e_p}}$$

für die zyklische Gruppe $C_n$ der Ordnung $n = \prod_{p \in \mathbb{P}} p^{e_p}$.

*Bemerkung* 3.3.2.14. Die (innere) direkte Summe von Moduln spielt (in der Spezialisierung auf Vektorräume) schon in der linearen Algebra eine Rolle. Auch Proposition 3.3.2.2 wird zumindest implizit in der linearen Algebra verwendet, nämlich bei *Blockdiagonalmatrizen*: Beispielhaft betrachten wir für einen Körper $K$ den Vektorraum $K^5$ mit der kanonischen Basis $\{e_1, e_2, e_3, e_4, e_5\}$. Eine $5 \times 5$-Matrix über $K$, sagen wir

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} \\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45} \\ a_{51} & a_{52} & a_{53} & a_{54} & a_{55} \end{pmatrix} \in K^{5 \times 5},$$

induziert gemäß $x = (x_i)_{i=1,\dots,5} \mapsto Ax = (\sum_{j=1}^{5} a_{ij} x_j)_{i=1,\dots,5}$ eine lineare Abbildung $K^5 \to K^5$, die für größere Dimensionen (anstelle von 5) zumindest aus numerischer Sicht immer komplexer werden – man denke nur an die Bestimmung der Eigenwerte oder an die Lösung von linearen Gleichungssystemen. Wenn die Matrix hingegen Blockdiagonalform hat, d.h.

$$A = \begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix}$$

für beispielsweise $B \in K^{3 \times 3}$ und $C \in K^{2 \times 2}$, dann lässt sich das Verhalten der linearen Abbildung zu $A$ auf das Verhalten der niedrigerdimensionalen Abbildungen zu $B$ und $C$ zurückführen. Aus abstrakter Sicht betrachtet man dabei die Unterräume $U_1 := \langle e_1, e_2, e_3 \rangle$ sowie $U_2 := \langle e_4, e_5 \rangle$, die nach Proposition 3.3.2.9 eine innere direkte Summe von $K^5$ bilden. Sind $f_1 : U_1 \to K^5$ bzw. $f_2 : U_2 \to K^5$ die von $B$ bzw. $C$ induzierten linearen Abbildungen auf $U_1$ bzw. $U_2$ (betrachtet als Abbildungen nach $K^5$ anstatt nach $U_i$), so gibt es nach Proposition 3.3.2.2 bzw. Bemerkung 3.3.2.6 eine eindeutige lineare Abbildung $h : K^5 \to K^5$, die $f_1$ und $f_2$ fortsetzt – dies ist genau die von $A$ induzierte lineare Abbildung, die wir somit durch $f_1$ und $f_2$ beschrieben haben.

Zum Abschluss des Unterabschnitts führen wir ein weiteres Beispiel direkter Summen von Vektorräumen an.

**UE 175 ► Übungsaufgabe 3.3.2.15.** (F) Sei $K$ eine beliebige Indexmenge. Für $k \in K$ sei $V_k := \mathbb{R}$. $V_k$ ist nicht nur eine Gruppe sondern auch ein Vektorraum über $\mathbb{R}$. Lösen Sie zwei der folgenden drei Aufgaben: **◄ UE 175**

(1) Was ist die Dimension von $V_k$?
(2) Geben Sie eine Basis für $\bigoplus_{k\in K} V_k$ an.
(3) Geben Sie eine Basis für $\prod_k V_k$ an.

### 3.3.3 Zerlegung von Torsionsgruppen in ihre $p$-Anteile

Inhalt in Kurzfassung: Technische Vorüberlegungen zur Ordnung von Elementen in abelschen Gruppen zielen auf das Hauptergebnis dieses Unterabschnitts ab: Jede Torsionsgruppe ist die direkte Summe ihrer $p$-Komponenten. Abschließend wird dieser Satz auf die universelle Prüfergruppe und ihre $p$-Anteile, die $p$-Prüfergruppen, angewendet.

Wie bereits angekündigt verfeinern wir nun Proposition 3.2.4.11 für den abelschen Fall.

**Lemma 3.3.3.1.** *Sei $A$ eine abelsche Gruppe und $a_i \in A$ Torsionselemente. Dann gilt:*

*1.*
$$\operatorname{ord}\left(\sum_{i=1}^{n} a_i\right) \mid \prod_{i=1}^{n} \operatorname{ord}(a_i).$$

*2. Sind die* $\operatorname{ord}(a_i)$, $i = 1, \ldots, n$ *paarweise teilerfremd, so gilt sogar Gleichheit:*
$$\operatorname{ord}\left(\sum_{i=1}^{n} a_i\right) = \prod_{i=1}^{n} \operatorname{ord}(a_i)$$

*3. Es gibt ein Element $a \in A$ mit*
$$\operatorname{ord}(a) = \operatorname{kgV}(\operatorname{ord}(a_1), \ldots, \operatorname{ord}(a_n)).$$

*Beweis.* Die erste bzw. zweite Aussage folgt mit Induktion aus der dritten bzw. vierten Aussage von Proposition 3.2.4.11 – man beachte, dass je zwei Elemente stets kommutieren.
Für die dritte Aussage sei $p$ eine Primzahl mit $p|\operatorname{ord}(a_i)$ für ein $a_i$. Die Menge $P$ solcher $p \in \mathbb{P}$ ist endlich. Für jedes sei $a(p)$ eines der $a_i$, sodass die Primfaktorzerlegung der Ordnung einen maximalen Exponenten $e_p$ zu $p$ hat. Dann ist $\operatorname{ord}(a(p)) = p^{e_p} k_p$ mit einem zu $p$ teilerfremden $k_p$. Das Element $b_p := k_p a(p)$ hat die Ordnung $p^{e_p}$, und die Summe $a := \sum_{p\in P} b_p$ nach Teil 2 die Ordnung $\operatorname{ord}(a) = \prod_p p^{e_p} = \operatorname{kgV}(\operatorname{ord}(a_1), \operatorname{ord}(a_2), \ldots, \operatorname{ord}(a_k))$. □

**Folgerung 3.3.3.2.** *Hat die abelsche Gruppe $A$ endlichen Exponenten $m$, so gibt es ein $a \in A$ mit* $\operatorname{ord}(a) = m$.

*Beweis.* Für alle $a \in A$ ist $\operatorname{ord}(a)|m$. Insbesondere kommen unter sämtlichen $\operatorname{ord}(a)$, $a \in A$, nur endlich viele natürliche Zahlen $o_i$, $i = 1, \ldots, k$, mit $k \in \mathbb{N}$ vor. Zu jedem $i$ gibt es ein $a_i \in A$ mit $o_i = \operatorname{ord}(a_i)$. Laut Aussage 3 in Lemma 3.3.3.1 gibt es ein $a \in A$ mit $\operatorname{ord}(a) = \operatorname{kgV}(o_1, \ldots, o_k)$. Das ist nur für $\operatorname{ord}(a) = m$ möglich. □

Für die weitere Strukturanalyse sehr wichtig ist die folgende Aussage:

**Proposition 3.3.3.3.** *Sei $A$ eine abelsche Gruppe. Dann sind sowohl die Menge $A_t$ aller Torsionselemente von $A$ als auch für jede Primzahl $p \in \mathbb{P}$ die Menge $A_p$ aller $p$-Elemente (der* $p$-Anteil *oder die* $p$-Komponente *von $A$) Untergruppen von $A$:*

$$A_p \leq A_t \leq A$$

*Beweis.* $A_t$ und $A_p$ enthalten wegen $\operatorname{ord}(0) = 1 = p^0$ das Nullelement und sind wegen $\operatorname{ord}(a) = \operatorname{ord}(-a)$ abgeschlossen bezüglich additiver Inversenbildung. Sind $\operatorname{ord}(a)$ und $\operatorname{ord}(b)$ endlich, so wegen Lemma 3.3.3.1 auch $\operatorname{ord}(a+b) | \operatorname{ord}(a) \operatorname{ord}(b)$. Also ist $A_t$ abgeschlossen bezüglich $+$. Auch $A_p$ hat diese Eigenschaft, weil aus $a, b \in A_p$ folgt, dass $\operatorname{ord}(a) = p^{e_a}$ und $\operatorname{ord}(b) = p^{e_b}$ mit $e_a, e_b \in \mathbb{N}$. Wieder wegen Lemma 3.3.3.1 gilt dann $\operatorname{ord}(a+b) | \operatorname{ord}(a) \operatorname{ord}(b) = p^{e_a + e_b}$, was nur für $\operatorname{ord}(a+b) = p^e$ mit einem $e \in \mathbb{N}$ möglich ist. □

Klarerweise haben die $A_p$ für verschiedene $p$ nur 0 gemeinsam. Aus Lemma 3.3.3.1 folgt sogar:

**Lemma 3.3.3.4.** *Sei $A$ eine abelsche Gruppe, und seien $p, p_1, \ldots, p_n$ paarweise verschiedene Primzahlen. Dann gilt*

$$A_p \cap (A_{p_1} + \ldots + A_{p_n}) = \{0\}.$$

*Beweis.* Für $a \in A_p$ gilt $\operatorname{ord}(a) = p^e$ mit $e \in \mathbb{N}$. Für $a \in A_{p_1} + \ldots + A_{p_n}$ gibt es Elemente $a_i \in A_{p_i}$ mit $a = a_1 + \ldots + a_n$ sowie $\operatorname{ord}(a_i) = p_i^{e_i}$ und $e_i \in \mathbb{N}$. Laut Lemma 3.3.3.1 folgt daraus $\operatorname{ord}(a) | \prod_{i=1}^n p_i^{e_i}$. Beides ist nur für $\operatorname{ord}(a) = 1$ möglich, also $a = 0$. □

Verwenden wir die Charakterisierung 3.3.2.11 zudirekter Summen von Moduln für den Spezialfall abelscher Gruppen zusammen mit Bemerkung 3.3.2.12, so zeigt Lemma 3.3.3.4, dass die von den $p$-Komponenten $A_p$, $p \in \mathbb{P}$, erzeugte Untergruppe $U$ einer abelschen Gruppe $A$ sogar die (innere) direkte Summe der $A_p$ ist. Jedes Element von $U$ ist eine endliche Summe von Elementen gewisser $A_p$, insbesondere von Torsionselementen, folglich in $A_t$. Es gilt aber auch umgekehrt:

**Lemma 3.3.3.5.** *Sei $A$ eine abelsche Gruppe und $a \in A_t$. Für die Ordnung von $a$ gelte $\operatorname{ord}(a) = \prod_{i=1}^n p_i^{e_i}$ mit paarweise verschiedenen $p_i \in \mathbb{P}$ und $e_i \in \mathbb{N}^+$. Dann gilt $a \in A_{p_1} + \ldots + A_{p_n}$.*

*Beweis.* Wir betrachten die Komplementärteiler $t_i := \frac{\operatorname{ord}(a)}{p_i^{e_i}}$ der $p_i^{e_i}$ von $\operatorname{ord}(a)$. Für die Elemente $a_i := t_i a$ gilt dann $\operatorname{ord}(a_i) = p_i^{e_i}$, also $a_i \in A_{p_i}$. Wegen $1 = \operatorname{ggT}(t_1, \ldots, t_n)$ gibt es laut Aussage 6 in 3.2.4.1 ganze Zahlen $x_1, \ldots, x_n$ mit $1 = \sum_{i=1}^n x_i t_i$. Es folgt

$$a = 1a = \left( \sum_{i=1}^n x_i t_i \right) a = \sum_{i=1}^n x_i (t_i a) = \sum_{i=1}^n x_i a_i \in A_{p_1} + \ldots + A_{p_n}.$$

□

Wir fassen zusammen:

**Satz 3.3.3.6.** *Ist $A$ eine abelsche Gruppe, so gilt für ihren Torsionsanteil $A_t$ die direkte Zerlegung (Darstellung als innere direkte Summe):*

$$A_t = \bigoplus_{p\in\mathbb{P}} A_p$$

*Insbesondere ist jede abelsche Torsionsgruppe direkte Summe ihrer $p$-Komponenten.*

*Beweis.* Die beiden Bedingungen aus 3.3.2.11 dafür, dass die behauptete Darstellung gilt, sind laut Lemmata 3.3.3.4 und 3.3.3.5 erfüllt. □

Als Anwendungsbeispiel der Zerlegung in $p$-Komponenten wollen wir nun die sogenannten *Prüfergruppen* kennenlernen. Die einfachste Beschreibung gelingt als Gruppe komplexer Einheitswurzeln, alternativ als direkte Limiten endlicher zyklischer Gruppen.

**Satz 3.3.3.7.** *Mit $p$ seien stets Primzahlen bezeichnet.*

1. *Für jedes $p \in \mathbb{P}$ bildet die Menge $C_{p^\infty}$ aller $z \in \mathbb{C}$, für die es ein $n \in \mathbb{N}$ gibt mit $z^{p^n} = 1$, eine multiplikative Untergruppe von $\mathbb{C}$, die sogenannte* $p$-Prüfergruppe.

2. *Alle echten Untergruppen $U$ von $C_{p^\infty}$ sind endlich und isomorph zu einer zyklischen Gruppe $C_{p^n}$ für ein $n \in \mathbb{N}$. Umgekehrt gibt es zu jedem $n \in \mathbb{N}$ genau ein $U \leq C_{p^\infty}$ mit $|U| = p^n$, das wir mit $U_{p^n}$ bezeichnen. $U_{p^n}$ ist zyklisch und wird für $n > 0$ von der komplexen Zahl $\zeta_k := e^{\frac{2\pi i}{k}}$ mit $k = p^n$ erzeugt. Die Inklusion $U_{p^m} \subseteq U_{p^n}$ gilt genau dann, wenn $m \leq n$.*

3. *Die $p$-Prüfergruppe $C_{p^\infty}$ lässt sich in natürlicher Weise als direkter Limes der zyklischen Gruppen $C_{p^n}$, $n \in \mathbb{N}$, auffassen.*

4. *Die von allen $C_{p^\infty}$, $p \in \mathbb{P}$, erzeugte multiplikative Untergruppe $C_\infty$ von $\mathbb{C}$ (genannt die* universelle Prüfergruppe*) besteht genau aus allen komplexen Einheitswurzeln, d.h. aus allen $z \in \mathbb{C}$, zu denen es ein $n \in \mathbb{N}^+$ gibt mit $z^n = 1$.*

5. *Die universelle Prüfergruppe ist (in additiver Notation) die direkte Summe aller $p$-Prüfergruppen:*

$$C_\infty \cong \bigoplus_{p\in\mathbb{P}} C_{p^\infty}$$

6. *Jede Untergruppe $U$ von $C_{p^\infty}$ ist (wieder in additiver Notation) die innere direkte Summe von Untergruppen der $p$-Prüfergruppen:*

$$U \cong \bigoplus_{p\in\mathbb{P}} U_{p^{n(p)}}.$$

   *Dabei sind die $n(p) \in \mathbb{N} \cup \{\infty\}$ durch $U$ eindeutig bestimmt.*

**UE 176 ► Übungsaufgabe 3.3.3.8.** (B) Beweisen Sie Satz 3.3.3.7. **◄ UE 176**

**UE 177 ► Übungsaufgabe 3.3.3.9.** (B) **◄ UE 177**

1. Geben Sie ein Beispiel einer Gruppe $G$ an, in der die Menge der Torsionselemente keine Untergruppe von $G$ ist.
   Hinweis: Betrachten Sie zum Beispiel die Permutation $\pi_3 : \mathbb{Z} \to \mathbb{Z}$, die durch $\pi_3(x) = 3 - x$ definiert ist.
2. Geben Sie ein Beispiel einer nichtabelschen Gruppe an, in der die Menge der Torsionselemente eine nichttriviale Untergruppe von $G$ ist.

### 3.3.4 Endliche abelsche Gruppen

Inhalt in Kurzfassung: Im Falle endlicher abelscher Gruppen führt die Zerlegung in ihre $p$-Anteile zum Hauptsatz, wonach eine direkte Zerlegung in zyklische Gruppen möglich ist. Allerdings muss man zuvor die entsprechende Aussage für Gruppen von Primzahlpotenzordnung beweisen.

Im Fall einer endlichen abelschen Gruppe $A$ können wir die Zerlegung aus Satz 3.3.3.6 noch weiter treiben. Denn dann lassen sich auch noch die $p$-Komponenten in direkte Summen zyklischer Gruppen zerlegen. Entscheidend ist der folgende Hilfssatz, der auch für unendliches $A$ gilt.

**Lemma 3.3.4.1.** *Sei $A$ eine abelsche $p$-Gruppe, $p \in \mathbb{P}$, $a \in A$ ein Element maximaler Ordnung* $\operatorname{ord}(a) = p^n$. *Bezeichne $\langle b\rangle$ für beliebige $b \in A$ wie üblich die von $b$ erzeugte zyklische Untergruppe von $A$. Dann gilt:*

1. *Ist $\langle a\rangle \neq A$, dann gibt es ein $b \in A \setminus \{0\}$ mit $\langle a\rangle \cap \langle b\rangle = \{0\}$.*
2. *Es gibt ein $U \leq A$ mit $A = U \oplus \langle a\rangle$.*

*Beweis.* 1. Unter der Annahme $\langle a\rangle \neq A$ sei $c \in A \setminus \langle a\rangle$. Mit Hilfe dieses Elements werden wir ein $b$ der Ordnung $p$ konstruieren, das nicht in $\langle a\rangle$ liegt, woraus automatisch $\langle a\rangle \cap \langle b\rangle = \{0\}$ folgt. Wegen $p^n \cdot c = 0 \in \langle a\rangle$ gibt es ein minimales $j > 0$ mit $p^j c \in \langle a\rangle$, also $p^j c = m_1 a$, wobei $m_1 = p^k m$ mit $k \in \mathbb{N}$, $m \in \mathbb{Z}$ und $\operatorname{ggT}(p, m) = 1$ sei. Es folgt

$$0 = p^n c = p^{n-j}(p^j c) = p^{n-j} m_1 a = p^{n-j}(mp^k)a = p^{n-j+k} ma.$$

Wegen $p^{n-1}a \neq 0$ und $\operatorname{ggT}(p, m) = 1$ muss $n - j + k \geq n$ sein, also $k \geq j > 0$. Wir wählen

$$b := \underbrace{p^{j-1}c}_{\notin\langle a\rangle} - \underbrace{mp^{k-1}a}_{\in\langle a\rangle} \notin \langle a\rangle.$$

Wegen $pb = p^j c - mp^k a = p^j c - m_1 a = 0$ hat dieses $b$ die gewünschten Eigenschaften.

2. Sei $U \leq A$ maximal mit $U \cap \langle a \rangle = \{0\}$. Die Existenz eines solchen $U$ folgt in der üblichen Weise aus dem Lemma von Zorn. Sei $A_0 := U + \langle a \rangle$. Nach 3.3.2.9 ist $A_0 = U \oplus \langle a \rangle$. Somit bleibt lediglich $A_0 = A$ zu zeigen.

   Angenommen, es wäre $A_0 \neq A$. Dann ist die von $a + U$ in der Faktorgruppe $A/U$ erzeugte zyklische Untergruppe nicht ganz $A/U$. Außerdem hat $a + U$ in $A/U$ die Ordnung $p^n$, was in $A/U$ sicher maximal ist. Nach Teil 1 (angewendet auf $A/U$ statt $A$ und $a+U$ statt $a$) gibt es folglich ein $b \in A \setminus U$ mit $\langle a+U \rangle \cap \langle b+U \rangle = \{U\}$. Damit wäre die Untergruppe $U' := U + \langle b \rangle \leq A$ eine echte Obermenge von $U$ mit $U' \cap \langle a \rangle = \{0\}$, im Widerspruch zur Maximalität von $U$. □

Damit wird es leicht, den *Hauptsatz über endliche abelsche Gruppen* zu beweisen:

**Satz 3.3.4.2.** *Jede endliche abelsche Gruppe $A$ ist direkte Summe von zyklischen Gruppen von Primzahlpotenzordnung:*

$$A \cong \bigoplus_{p \in \mathbb{P}} \bigoplus_{n=1}^{\infty} C_{p^n}^{e_{p,n}},$$

*mit Vielfachheiten $e_{p,n} \in \mathbb{N}$, von denen nur endlich viele $\neq 0$ sind. Alle $e_{p,n}$ sind durch $A$ eindeutig bestimmt.*

*Beweis.* Zunächst zur Existenz einer Darstellung wie behauptet. Wegen Satz 3.3.3.6 genügt es, den Satz für festes $p \in \mathbb{P}$ und eine endliche abelsche $p$-Gruppe $A$ zu beweisen. Wir gehen mittels Induktion nach $|A|$ vor. Die einelementige Gruppe ist zyklisch von der Ordnung $p^0$, also ist die Aussage des Satzes für $|A| = 1$ mit $e_{p,n} = 0$ für alle $p$ und $n$ trivialerweise erfüllt. Angenommen $|A| > 1$ und die Aussage gelte für alle $p$-Gruppen der Ordnung $< |A|$. In diesem Fall ist die maximale Ordnung eines Elements $a \in A$ und somit die Ordnung der von diesem $a$ erzeugten zyklischen Gruppe $\langle a \rangle$ größer als 1. Nach Lemma 3.3.4.1 gibt es ein $U \leq A$ mit $A = U \oplus \langle a \rangle$. Wegen $n = |A| = |U| \cdot |\langle a \rangle| > |U|$ ist auf $U$ die Induktionsvoraussetzung anwendbar. Also ist $U$ inneres direktes Produkt zyklischer $p$-Gruppen, somit auch $A = U \oplus \langle a \rangle$. Folglich ist $A$ isomorph zu einer äußeren direkten Summe der kanonischen zyklischen $p$-Gruppen $C_{p^n}$.
Nun zur Eindeutigkeit: Die $p$-Komponenten $A_p$ sind durch $A$ eindeutig bestimmt. Wieder dürfen wir uns deshalb auf $p$-Gruppen für ein festes $p$ beschränken. Wir führen Induktion nach der maximalen $p$-Potenz, die unter der Ordnungen der Elemente von $A$ vorkommt. Wieder ist der Induktionsanfang (für die einelementige Gruppe) trivialerweise erfüllt. Sei also $A$ eine endliche $p$-Gruppe. In einer Darstellung

$$A \cong \bigoplus_{n=1}^{\infty} C_{p^n}^{e_{p,n}}$$

sei $n_0$ das größte $n$ mit $e_{p,n} > 0$. Es ist durch $A$ deshalb eindeutig bestimmt, weil $p^{n_0}$ die maximale Ordnung von Elementen $a \in A$ ist. Sei $U \leq A$ die von allen $a \in A$ mit maximaler Ordnung erzeugte Untergruppe. Aus obiger Darstellung liest man $|U| = (p^{n_0})^{e_{p,n_0}} = p^{n_0 e_{p,n_0}}$ ab. Wegen $n_0 > 0$ ist dadurch auch $e_{p,n_0}$ eindeutig bestimmt. Die

maximale $p$-Potenz von Elementen in $A/U$ ist $< n_0$, also ist die Induktionsvoraussetzung auf diese Faktorgruppe

$$A/U \cong \bigoplus_{n=1}^{n_0-1} C_{p^n}^{e_{p,n}}$$

anwendbar, weshalb auch alle $e_{p,n}$ mit $n < n_0$ durch $A$ eindeutig bestimmt sind. □

Es gilt ein analoger Satz unter allgemeineren Bedingungen: Schwächt man die Voraussetzung *endlich* an $A$ ab zu *endlich erzeugt*, so tritt neben den endlichen zyklischen Gruppen auch noch die unendliche zyklische Gruppe $\mathbb{Z}$ als möglicher direkter Summand auf. Statt abelscher Gruppen, das heißt statt unitärer $\mathbb{Z}$-Moduln, kann man den gleichen Beweis auch für endlich erzeugte Moduln über beliebigen Hauptidealringen führen. Das werden wir in 7.4 tun.

**UE 178 ► Übungsaufgabe 3.3.4.3.** (F) Begründen Sie: **◄ UE 178**

1. Die Gruppe $C_{50}$ ist isomorph zum Produkt $C_{25} \times C_2$.
2. Die Gruppe $C_2 \times C_{10}$ (Darstellung wie in 3.3.4.4) ist isomorph zu $C_2 \times C_2 \times C_5$ (Darstellung wie in 3.3.4.4).
3. Das Produkt $C_2^2 \times C_4^2 \times C_7^3$ (Darstellung wie in 3.3.4.4) ist isomorph zu $C_2 \times (C_2 \times C_7) \times (C_4 \times C_7) \times (C_4 \times C_7) \simeq C_2 \times C_{14} \times C_{28} \times C_{28}$.

**UE 179 ► Übungsaufgabe 3.3.4.4.** (E) Beweisen Sie folgende Variante des Hauptsatzes 3.3.4.2: Jede endliche abelsche Gruppe $A$ ist direkte Summe zyklischer Gruppen $C_{m_i}$, $i = 1, \ldots, n$, deren Ordnungen $m_i > 1$ eine Teilerkette $m_1|m_2|\ldots|m_n$ bilden. Die $m_i$ sind durch $A$ eindeutig bestimmt. Hinweis: Aus Lemma 3.3.3.1 folgt leicht, dass direkte Summen zyklischer Gruppen mit teilerfremden Ordnungen wieder zyklisch sind. Damit lässt sich die hier zu beweisende Variante ohne große Mühe aus dem Hauptsatz in der Version von ableiten. **◄ UE 179**

**UE 180 ► Übungsaufgabe 3.3.4.5.** (F) Geben Sie bis auf Isomorphie alle abelschen Gruppen an, deren Ordnung ein Teiler von 75 ist. (Das heißt: Geben Sie eine Liste von paarweise nichtisomorphen Gruppen an, sodass erstens die Ordnung jeder Gruppe Ihrer Liste ein Teiler von 75 ist, und dass zweitens jede Gruppe, deren Ordnung ein Teiler von 75 ist, zu einer Gruppe auf Ihrer Liste isomorph ist. Anmerkung: Die Teiler von 75 sind 1, 3, 5, 15, 25, 75.) **◄ UE 180**

**UE 181 ► Übungsaufgabe 3.3.4.6.** (F) Sei $p$ eine Primzahl. **◄ UE 181**

1. Wie viele Untergruppen hat $C_p \times C_p$?

2. Wie viele Untergruppen hat $C_{p^2}$?

(Hinweis: Überlegen Sie sich zuerst, dass alle nichttrivialen Untergruppen zyklisch sein müssen.)

**UE 182** ► **Übungsaufgabe 3.3.4.7.** (F) Finden Sie zwei zueinander nicht isomorphe abelsche Gruppen der Ordnung 75, und bestimmen Sie für beide Gruppen und für jedes $d \in \{1, 3, 5, 15, 25, 75\}$ ◄ **UE 182**

1. die Anzahl aller zyklischen Untergruppen der Ordnung $d$.
2. die Anzahl aller nicht-zyklischen Untergruppen der Ordnung $d$.

(Hinweis: Es kann hilfreich sein, die Anzahl aller Elemente der Ordnung $d$ zu bestimmen. In $C_{15}$ gibt es 8 Elemente der Ordnung 15, in $C_{75}$ gibt es 40 Elemente der Ordnung 75.)

**UE 183** ► **Übungsaufgabe 3.3.4.8.** (A) Sei $p$ eine Primzahl. Wie viele Automorphismen hat $C_p \times C_p$? (Hinweis: Verwenden Sie Ihr Wissen aus der Linearen Algebra.) ◄ **UE 183**

## 3.4 Ringe

Grundsätzlich verfolgen wir im Abschnitt über Ringe ein ähnliches Programm wie im Abschnitt 3.2 über Gruppen: Wir wollen erstens die allgemeinen Konzepte algebraischer Strukturanalyse aus 2.3 von beliebigen universellen Algebren so auf die speziellere Klasse der Ringe übertragen, dass schärfere Aussagen möglich werden, und zweitens diese an wichtigen Beispielen illustrieren. Neben starken Analogien (wie etwa jener zwischen Normalteilern und Idealen) verschieben sich allerdings bei manchen Aspekten die Gewichtungen, was sich auf die Struktur des Abschnitts auswirkt. Die meisten Ringe, mit denen wir uns beschäftigen werden, sind Ringe mit 1. Häufig spielt auch Kommutativität eine entscheidende Rolle.
Wir beginnen mit dem Studium von Kongruenzrelationen und den ihnen (analog zu den Normalteilern bei Gruppen) entsprechenden Idealen (3.4.1 für den allgemeinen und 3.4.2 für den kommutativen Fall mit 1). Wie schon bei den Gruppen spielt $\mathbb{Z}$ auch in der Kategorie der Ringe eine besondere Rolle. Sie hängt mit dem Konzept der Charakteristik eines Ringes mit 1 zusammen (siehe 3.4.3), zeigt sich aber auch an der wohlbekannten binomischen Formel (3.4.4). In 3.4.5 beschäftigen wir uns mit der (uneingeschränkt nur im Fall von Integritätsbereichen bestehenden) Möglichkeit, kommutative Ringe zu Körpern zu erweitern. Die neben $\mathbb{Z}$ und den darauf aufbauenden Zahlenbereichen wichtigsten Beispiele kommutativer Ringe werden von Polynomen und (formalen) Potenzreihen gebildet (3.4.6). Direkte Produkte spielen bei Ringen eine geringere Rolle als bei Gruppen. Von Bedeutung ist immerhin der Chinesische Restsatz (3.4.7). Als wichtigste Beispiele nichtkommutativer Ringe (3.4.8) schließlich sind Matrizenringe und Endomorphismenringe abelscher Gruppen und Moduln wenigstens zu erwähnen; insbesondere weil sie zu natürlichen Beispielen natürlicher Moduln über nichtkommutativen Ringen führen, nämlich abelschen Gruppen über ihren Endomorphismenringen.

### 3.4.1 Kongruenzrelationen und Ideale

Inhalt in Kurzfassung: Ideale spielen in der Ringtheorie die völlig analoge Rolle zu Normalteilern in der Gruppentheorie. Entsprechend folgt der vorliegende Unterabschnitt auch ganz analogen Gesichtspunkten wie jener aus der Gruppentheorie über Normalteiler (3.2.2). Betrachtet man einen Ring als Links- bzw. Rechtsmodul über sich selbst, so stößt man analog auf Links- bzw. Rechtsideale.

Obwohl wir schon in 1.2.3 zwangsläufig auf den Begriff des Ideals gestoßen sind, wollen wir das Thema Kongruenzrelationen und Homomorphismen auf Ringen nochmals systematisch aufrollen und unter den zusätzlichen, teils allgemeineren Gesichtspunkten beleuchten, die mit denen wir nunmehr vertraut sind. Dabei ist es zielführend, sich am Beispiel der Gruppen zu orientieren (siehe 3.2.2). Denn jede Kongruenzrelation $\sim$ auf einem Ring $R$ ist insbesondere auch eine Kongruenzrelation auf der additiven Gruppe von $R$, wird also eindeutig durch die Klasse $[0]_\sim$ von $0 \in R$ bestimmt. Folglich muss $\sim$ erst recht als Kongruenzrelation des Ringes durch $I := [0]_\sim$ eindeutig bestimmt sein. Die Klasse eines beliebigen Elements $x \in R$ ist von der Form $[x]_\sim = x + I$.

**Definition 3.4.1.1.** Eine Teilmenge $I$ eines Ringes $R$ heißt *Ideal* von $R$, symbolisch $I \lhd R$, wenn es eine Kongruenzrelation $\sim$ auf $R$ gibt mit $I := [0]_\sim$ (was nach dem allgemeinen Homomorphiesatz 2.3.3.16 gleichbedeutend damit ist, dass es einen Ringhomomorphismus gibt, dessen Kern $I$ ist).
Die Kongruenzklasse $[x]_\sim = x + I$ von $x \in R$ heißt auch *Nebenklasse* von $x$ modulo $I$. Im Fall $x + I = y + I$ (d.h. $x \sim y$) schreibt man auch $x \equiv y \bmod I$.

Die Ideale in Ringen spielen folglich eine völlig analoge Rolle zu den Normalteilern in Gruppen:

**Proposition 3.4.1.2.** *Zwischen der Menge der Kongruenzrelationen $\sim$ eines Ringes $R$ und der Menge der Ideale $I$ von $R$ wird durch die Relation $I = [0]_\sim$ eine Bijektion hergestellt. Dabei handelt es sich sogar um einen Isomorphismus zwischen den jeweils durch $\subseteq$ geordneten Verbänden aller Kongruenzrelationen bzw. aller Ideale von $R$.*

Wie bei Gruppen schreiben wir $R/I$ für den Faktorring $R/\sim$, wenn $\sim$ die Kongruenzrelation mit $I = [0]_\sim$ ist. Den trivialen Kongruenzrelationen auf $R$ entsprechen dabei die *trivialen Ideale*: $R$ (für die Allrelation) und $\{0\}$ (für die identische Relation). Der Ring $R/R$ hat nur ein Element, während $R/\{0\}$ zu $R$ isomorph ist (der kanonische Homomorphismus ist ein Isomorphismus). Weiter analog zu den Gruppen führt die allgemeine Definition 2.3.3.13 einer einfachen Algebra bei Ringen zu:

**Folgerung 3.4.1.3.** *Ein Ring $R$ ist genau dann einfach, wenn $R$ und $\{0\}$ die einzigen Ideale von $R$ sind.*

Jedes Ideal $I$ ist ein Normalteiler der additiven Gruppe von $R$, was wegen der Kommutativität von $+$ gleichbedeutend damit ist, dass $I$ eine additive Untergruppe von $R$ ist. Weil diese Bedingung keinerlei Rücksicht auf die multiplikative Struktur von $R$ nimmt,

dürfen wir nicht erwarten, dass umgekehrt jede additive Untergruppe von $R$ schon einer Kongruenzrelation der Ringes entspricht. Tatsächlich muss, anders als für beliebige additive Untergruppen, für alle $r \in R$ zum Beispiel $rI \subseteq I$ und $Ir \subseteq I$ gelten: Denn für die $I$ entsprechende Kongruenzrelation $\sim$ und $i \in I$ gilt ja $ri \sim r0 = 0$, also $ri \in I$ und analog $ir \in I$.[17] Bemerkenswert ist, dass diese zusätzliche Eigenschaft bereits ausreicht, um Ideale zu charakterisieren. Bevor wir das beweisen, fassen wir zusammen:

**Satz 3.4.1.4.** *Sei $R$ ein Ring und $I \subseteq R$. Dann sind die folgenden Aussagen äquivalent:*

(1) *$I$ ist ein Ideal. (Definitionsgemäß heißt das, dass es eine Kongruenzrelation $\sim$ auf $R$ mit $I = [0]_\sim$ gibt.)*

(1′) *Es gibt genau eine Kongruenzrelation $\sim$ auf $R$ mit $I = [0]_\sim$.*

(2) *Es gibt einen Ring $S$ und einen (surjektiven) Homomorphismus $\varphi\colon R \to S$ mit $I = \varphi^{-1}(\{0_S\})$.*

(3) *$I$ ist eine additive Untergruppe von $R$ mit $rI, Ir \subseteq I$ für alle $r \in R$ (folglich $RI, IR \subseteq I$).*

*Beweis.* Die Äquivalenz von (1) und (2) folgt unmittelbar aus der Spezialisierung des Homomorphiesatzes 2.3.3.16 auf Ringe. Aufgrund der vorangegangenen Überlegungen dürfen wir uns deshalb auf den Nachweis der einzig noch ausstehenden Implikation beschränken, nämlich auf den Schritt von (3) nach (1):
Wenn $I$ die Bedingung (3) erfüllt, dann definieren wir eine Relation $\sim_I$ durch $x \sim_I y \ :\Leftrightarrow\ x - y \in I$. Weil $I$ als Untergruppe auch ein Normalteiler der kommutativen additiven Gruppe auf $R$, ist $\sim_I$ auf dieser eine Kongruenzrelation. Wie folgende Schlusskette zeigt, ist $\sim_I$ aber auch mit der Multiplikation verträglich:

$$\begin{aligned} x \sim_I x',\, y \sim_I y' &\Rightarrow (x - x'),\, (y - y') \in I \\ &\Rightarrow (x - x')y',\, x(y - y') \in I \\ &\Rightarrow xy - x'y' = x(y - y') + (x - x')y' \in I \\ &\Rightarrow xy \sim_I x'y'. \end{aligned}$$

Also ist $\sim_I$ eine Kongruenzrelation. Aus $x \sim_I 0 \Leftrightarrow x - 0 \in I$ folgt $I = [0]_\sim$. □

**UE 184** ▶ **Übungsaufgabe 3.4.1.5.** (F) Geben Sie ein Beispiel eines kommutativen Rings $R$ und eines Unterrings $U \leq R$ an, der *kein* Ideal ist. ◀ **UE 184**

Analog zu den Normalteilern einer Gruppe (siehe Folgerung 3.2.2.7) bilden auch die Ideale eines Ringes wegen Proposition 3.4.1.2 einen vollständigen Verband mit dem mengentheoretischen Schnitt als Infimum. Auch das Supremum einer Menge von Idealen (definitionsgemäß der Schnitt aller diese umfassenden Ideale) lässt sich recht leicht beschreiben:

[17] In beliebigen Ringen $R$ gilt $r0 = 0r = 0$ für alle $r \in R$: Aus $r0 = r(0 + 0) = r0 + r0$ folgt nach Addition von $-r0$ sofort $r0 = 0$, analog $0r = 0$; siehe auch die Fußnote auf Seite 174.

**Proposition 3.4.1.6.** *Sei $R$ ein Ring mit* 1 *und $A \subseteq R$. Bezeichne $I$ den Schnitt aller Ideale $J \lhd R$ mit $A \subseteq J$. (I ist also das kleinste $A$ umfassende Ideal in $R$, genannt das von $A$* erzeugte Ideal*, symbolisch $I = (A)$, im Fall $A = \{a_1, \ldots, a_n\}$ auch $I = (a_1, \ldots, a_n)$.) Dann gilt:*

(1) *$I$ ist die Menge aller*

$$\sum_{i=1}^{n} r_i a_i s_i + \sum_{j=1}^{m'} r'_j b_j + \sum_{k=1}^{n'} c_k s'_k + \sum_{l=1}^{m} d_l$$

*mit $n, m', n', k \in \mathbb{N}$, $a_i, b_j, c_k, d_l \in A$ und $r_i, s_i, r'_j, s'_k \in R$.*

(2) *Hat $R$ ein Einselement, so ist $I$ auch darstellbar als die Menge aller*

$$\sum_{i=1}^{n} r_i a_i s_i$$

*mit $n \in \mathbb{N}$, $a_i \in A$ und $r_i, s_i \in R$.*

(3) *Ist $R$ kommutativ mit* 1*, so ist $I$ darstellbar als die Menge aller Summen (Linearkombinationen)*

$$\sum_{i=1}^{n} r_i a_i$$

*mit $n \in \mathbb{N}$, $a_i \in A$ und $r_i \in R$. Ist außerdem $A = \{a\}$, einelementig, so ist*

$$I = (a) = \{ra : \ r \in R\}.$$

**UE 185 ► Übungsaufgabe 3.4.1.7.** (V) Beweisen Sie Proposition 3.4.1.6. **◄ UE 185**

Die Idealbedingung $rI \subseteq I$ ist eine Verschärfung der Abgeschlossenheit von $I$ bezüglich der Multiplikation. Ideale sind also insbesondere Unterringe. Diese Sichtweise ist allerdings deshalb problematisch, weil sie falsch wird, wenn man Ringe $R$ mit 1 als 0-stelliger Operation betrachtet. Denn jede Unteralgebra eines Ringes mit 1 muss selbst 1 enthalten, was im Falle eines Ideals $I$ mit $1 \in I$ wegen $R = R1 \subseteq RI \subseteq I \subseteq R$ nur für das triviale Ideal $I = R$ möglich ist. Also:

**Proposition 3.4.1.8.** *Ist $R$ ein Ring mit* 1 *und $I \lhd R$, so gilt $1 \in I$ genau dann, wenn $I = R$.*

Unteralgebren sind Ideale $I$ allerdings dann, wenn man $R$ als Links- bzw. Rechts-Modul über sich selbst auffasst (mit den Operationen $\omega_r(a) := ra$ bzw. $\tilde{\omega}_r(a) := ar$ für $r \in R$). Über nichtkommutativen Ringen ist dafür nicht die volle Idealeigenschaft erforderlich. Deshalb spielen dort auch Links- und Rechtsideale eine wichtige Rolle.

**Definition 3.4.1.9.** Eine Teilmenge $I$ eines Rings $R$ heißt *Linksideal*, wenn $I$ additive Untergruppe von $R$ ist und abgeschlossen ist bezüglich der Multiplikation mit beliebigen Ringelementen von links: $rI \subseteq I$ für alle $r \in R$. *Rechtsideale* sind analog definiert mit Multiplikation von rechts ($Ir \subseteq I$ für alle $r \in R$) statt von links.

**UE 186** ► **Übungsaufgabe 3.4.1.10.** (B) Geben Sie ein Beispiel eines Rings und eines Linksideals $I$ an, sodass $I$ kein Ideal ist. (Hinweis: Matrizen.) ◄ **UE 186**

Sehr leicht überprüft man:

**Proposition 3.4.1.11.** *Sind $I, J \lhd R$ Ideale von $R$, dann auch die Komplexsumme $I + J := \{i + j : \ i \in I, j \in J\}$.*

**UE 187** ► **Übungsaufgabe 3.4.1.12.** (F) Beweisen Sie Proposition 3.4.1.11. ◄ **UE 187**

**Definition 3.4.1.13.** Ein Ideal $I \lhd R$ eines Ringes $R$ heißt *Hauptideal*[18], wenn $I$ von einem Element erzeugt wird, d.h. $\exists a \in I : I = (a)$.
Ein Integritätsbereich, dessen sämtliche Ideale Hauptideale sind, heißt *Hauptidealring*.

Das Paradebeispiel eines Hauptidealringes ist $\mathbb{Z}$: Als Ideale kommen nur die uns bereits aus 3.2.4.1 bekannten additiven Untergruppen $m\mathbb{Z} = \{mz \mid z \in \mathbb{Z}\}$ in Frage. Offenbar sind diese Mengen auch bezüglich der Multiplikation mit beliebigen ganzen Zahlen abgeschlossen, sind also Ideale. Jede dieser Mengen $m\mathbb{Z}$ wird von einem einzigen Element erzeugt, nämlich von $m$ (oder auch von $-m$).

**Proposition 3.4.1.14.** *Sämtliche Faktorringe (und somit bis auf Isomorphie auch alle homomorphen Bilder) von $\mathbb{Z}$ sind gegeben durch die sogenannten* Restklassenringe *modulo $m$, symbolisch $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$, $m \in \mathbb{N}$.*

**UE 188** ► **Übungsaufgabe 3.4.1.15.** (F) Zeigen Sie: Ist $R$ ein Hauptidealring und $J \lhd R/I$, so ist $J$ ein Hauptideal. Trotzdem muss $R/I$ kein Hauptidealring sein. ◄ **UE 188**

Hauptidealringe werden uns im Rahmen der Teilbarkeitslehre noch intensiv beschäftigen. Die Ringe $\mathbb{Z}_m$ entsprechen für $m > 0$ dem Rechnen modulo $m$, wobei die additive Struktur die uns bereits bekannte zyklische Gruppe $C_m$ ist. Weil alle Untergruppen (sprich Normalteiler) von $\mathbb{Z}$ Ideale sind, entspricht der Kongruenz- (= Ideal-) Verband auch des Ringes $\mathbb{Z}$ der umgekehrten Teilbarkeitsrelation auf $\mathbb{N}$, siehe Satz 3.2.4.13.
Im Vergleich zu beliebigen Ringen rücken bei kommutativen Ringen mit 1 zahlreiche weitere Besonderheiten ins Zentrum des Interesses.

### 3.4.2 Ideale in kommutativen Ringen mit 1

Inhalt in Kurzfassung: Unter den kommutativen Ringen mit 1 spielen die Integritätsbereiche und Körper eine besondere Rolle, die sich durch Faktorisierung nach Prim- bzw. maximalen Idealen ergeben. Im endlichen Fall ist jeder Integritätsbereich sogar ein Körper. Generell sind Körper unter den kommutativen Ringen mit 1 genau die einfachen

[18] englisch: *principal ideal*

(die also nur die trivialen Ideale enthalten).

Sei $R$ ein kommutativer Ring mit 1 und $I \lhd R$ ein Ideal. Wir fragen uns, unter welchen Bedingungen $R/I$ ein Integritätsbereich oder gar ein Körper ist. Nicht überraschend lässt sich das durch Eigenschaften von $I$ charakterisieren. Doch zunächst eine einfache Beobachtung.

**Satz 3.4.2.1.** *Jeder endliche Integritätsbereich ist ein Körper.*

*Beweis.* Sei $R$ ein Integritätsbereich und $r \in R \setminus \{0_R\}$. Wir betrachten die Abbildung $m_r \colon R \to R$, $x \mapsto rx$. Aus $rx = ry$ folgt wegen der Kürzungsregel in Integritätsbereichen $x = y$. Also ist $m_r$ injektiv. Weil $R$ endlich ist, muss $m_r$ auch surjektiv sein. Somit gibt es ein $x_r \in R$ mit $rx_r = m_r(x_r) = 1_R$, und $x_r$ ist ein multiplikatives Inverses von $r$. □

In Hinblick auf unsere Ausgangsfrage betreffend Körper ist die folgende Beobachtung nützlich.

**Proposition 3.4.2.2.** *Ein kommutativer Ring $R$ mit $1_R \neq 0_R$ ist genau dann ein Körper, wenn er einfach ist (d.h., definitionsgemäß, wenn $R$ nur die trivialen Kongruenzrelationen und somit nur die trivialen Ideale hat).*

*Beweis.* Sei zunächst $R$ ein Körper und $I \lhd R$ ein Ideal mit $I \neq \{0_R\}$, d.h. $i \in I$ für ein $i \neq 0_R$. Es genügt zu zeigen, dass daraus $R \subseteq I$ folgt. Sei also $r \in R$ beliebig. Weil $R$ ein Körper ist, hat $i$ ein Inverses $i^{-1} \in R$. Weil $I$ ein Ideal ist, liegt somit auch das Element $1_R = i^{-1}i$ in $I$ und die Aussage folgt aus Proposition 3.4.1.8.
Sei nun umgekehrt $R$ einfach. Zu einem beliebigem $r \in R \setminus \{0_R\}$ müssen wir ein multiplikatives Inverses in $R$ finden. Weil $R$ einfach ist, muss jedes Ideal $I$, in dem das Element $r$ liegt, schon ganz $R$ sein. Insbesondere muss das von $r$ erzeugte Ideal $I_r = \{sr : \ s \in R\}$ (Proposition 3.4.1.6) das Einselement $1_R$ enthalten. Also gibt es ein $s \in R$ mit $1_R = sr$. Dieses $s \in R$ ist das gesuchte Inverse von $r$. □

Wir gehen nun von irgendeinem kommutativen Ring $R$ mit Einselement und einem Ideal $I \lhd R$ aus. Nach dem zweiten Isomorphiesatz 2.3.6.7 ist der Kongruenz- und somit der Idealverband von $R/I$ isomorph zum Verband der Ideale $J \lhd R$ mit $I \subseteq J$. Gemäß Proposition 3.4.2.2 ist $R/I$ also genau dann ein Körper, wenn es zwischen $I$ und $R$ keine weiteren Ideale gibt. Solche Ideale nennt man *maximal*.
Ähnlich einfach zu verstehen ist, wann $R/I$ ein Integritätsbereich ist. Denn die Integritätsbereiche definierende Nullteilerfreiheit liegt im Faktorring $R/I$ genau dann vor, wenn das Produkt $(a+I)(b+I) = ab+I$ zweier Nebenklassen $a+I$ und $b+I$ nur dann wieder $I$ ist, wenn schon $a+I = I$ oder $b+I = I$ gilt. Anders ausgedrückt: Wenn aus $ab \in I$ folgt, dass $a \in I$ oder $b \in I$. Ein Ideal $I$ mit diesen Eigenschaften nennt man ein *Primideal*.
Die allgemeinen Definitionen lauten also:

**Definition 3.4.2.3.** Sei $R$ ein Ring und $I \lhd R$ ein Ideal in $R$. Dann sagt man:

1. $I$ ist ein *echtes Ideal*, wenn $I \neq R$.

2. $I$ ist ein *maximales Ideal*, wenn $I$ ein echtes Ideal ist und jedes Ideal $J \lhd R$ mit $I \subseteq J$ entweder $J = I$ oder $J = R$ erfüllt. (Mit anderen Worten: Wenn $I$ ein maximales Element in der partiellen Ordnung aller echten Ideale ist; Ideale sind hier durch die Inklusionsrelation $\subseteq$ partiell geordnet.)

3. $I$ ist ein *Primideal*, wenn $I$ ein echtes Ideal ist und für $a, b \in R$ aus $ab \in I$ stets $a \in I$ oder $b \in I$ folgt.

Wir fassen unsere obigen Überlegungen zusammen und ergänzen sie zu folgendem Satz:

**Satz 3.4.2.4.** *Sei $R$ ein kommutativer Ring mit Einselement $1_R \in R$ und $I \lhd R$ ein Ideal. Dann gilt:*

1. *$I$ ist genau dann ein echtes Ideal, wenn $1_R \notin I$.*

2. *$R/I$ ist genau dann ein Körper, wenn $I$ ein maximales Ideal ist.*

3. *$R/I$ ist genau dann ein Integritätsbereich, wenn $I$ ein Primideal ist.*

4. *Jedes maximale Ideal ist ein Primideal.*

5. *Ist $I$ ein echtes Ideal, so gibt es ein maximales (und somit Prim-) Ideal $J \lhd R$ mit $I \subseteq J$.*

6. *Ist $R \neq \{0_R\}$, so gibt es ein maximales Ideal in $R$.*

*Beweis.* Die erste Aussage ist eine Umformulierung von Proposition 3.4.1.8, hier für kommutative Ringe. Die zweite und dritte Behauptung ergeben sich aus den Überlegungen, die Definition 3.4.2.3 vorangegangen sind. Die vierte Behauptung folgt aus der zweiten und dritten, weil jeder Körper ein Integritätsbereich ist.
Der Beweis der fünften Behauptung erfolgt in typischer Weise mit Hilfe das Lemmas von Zorn (siehe Anhang, 11.3.2.4). Das System $\mathcal{S}$ aller echten Ideale $J \lhd R$ mit $I \subseteq J$ ist wegen $I \in \mathcal{S}$ nicht leer und bezüglich $\subseteq$ halbgeordnet. Man überzeugt sich unmittelbar davon, dass die Vereinigung $V$ einer $\subseteq$-Kette von Idealen wieder ein Ideal ist. Weil alle $J \in \mathcal{S}$ echte Ideale sind, enthält (erste Behauptung) keines davon $1_R$, also auch $1_R \notin V$. Somit sind die Voraussetzungen des Lemmas von Zorn erfüllt. Folglich gibt es ein $\subseteq$-maximales Element $J \in \mathcal{S}$. Dieses ist offenbar ein maximales Ideal mit $I \subseteq J$, wie behauptet.
Besteht $R$ nicht nur aus $0_R$, so ist $I := \{0_R\}$ ein echtes Ideal, auf das die fünfte Aussage angewendet werden kann. Damit ist auch die sechste Aussage bewiesen. □

Nicht jedes Primideal ist maximal, wie man in der folgenden Übungsaufgabe sieht.

**UE 189** ► **Übungsaufgabe 3.4.2.5.** (B) Geben Sie einen kommutativen Ring $R$ mit 1 an, sowie ein Primideal $I \neq \{0\}$ in $R$, welches nicht maximal ist. ◄ **UE 189**
Hinweis: Beachten Sie Satz 3.4.2.4, und finden Sie zunächst einen Integritätsbereich, der kein Körper ist.

### 3.4.3 Charakteristik

Inhalt in Kurzfassung: So wie $\mathbb{Z}$ haben auch alle endlichen zyklische Gruppen mit Ordnungen $n \in \mathbb{N}^+$ neben der additiven auch eine multiplikative Struktur, die sie zu kommutativen Ringen mit 1 machen. Jeder kommutative Ring mit 1 enthält die Kopie genau eines dieser Ringe als Unteralgebra. Ist dies $\mathbb{Z}$, so definiert man die Charakteristik des Ringes als 0, sonst als das entsprechende $n$. Dies drückt sich auch dadurch aus, dass $\mathbb{Z}$ ein initiales Objekt in der Kategorie der kommutativen Ringe mit 1 ist. Die Charakteristik eines Integritätsbereichs ist stets entweder 0 oder eine Primzahl.

In 3.2.4 haben wir gesehen, dass für jedes Element $g$ einer Gruppe $G$ die Abbildung $\varphi : k \mapsto kg$ (additive Notation) ein Gruppenhomomorphismus $\varphi\colon \mathbb{Z} \to G$ ist. Ersetzen wir $G$ durch einen Ring mit 1 und betrachten $g = 1$, so gilt, wie man leicht überprüft, sogar:

**Proposition 3.4.3.1.** *Sei $R$ ein Ring mit Einselement $1_R$. Dann ist die Abbildung*

$$\varphi\colon \mathbb{Z} \to R, \quad k \mapsto k_R := k1_R$$

*ein Ringhomomorphismus. $\mathbb{Z}$ ist sogar ein initiales Objekt in der Kategorie der Ringe mit* 1.

**UE 190 ▶ Übungsaufgabe 3.4.3.2.** (V) Beweisen Sie Proposition 3.4.3.1. **◀ UE 190**

Der Kern von $\varphi$ aus 3.4.3.1 ist ein Ideal von $\mathbb{Z}$, also nach 3.4.1.14 gleich $m\mathbb{Z}$ für ein $m \in \mathbb{N}$. Das Bild $\varphi(\mathbb{Z})$ ist offenbar der kleinste Unterring von $R$ mit 1 und nach dem Homomorphiesatz isomorph zu $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$. Jeder Ring mit 1 enthält als kleinsten Unterring folglich eine isomorphe Kopie entweder von $\mathbb{Z}$ (falls $m = 0$) oder vom Restklassenring $\mathbb{Z}_m$. Die Zahl $m$ heißt auch die *Charakteristik* von $R$, symbolisch $\operatorname{char} R$. Ist $m > 0$, so stimmt $m$ mit der additiven Ordnung von $1_R$ überein. Klarerweise ist $\operatorname{char} \mathbb{Z}_m = m$ $(m \in \mathbb{N})$ und $\operatorname{char} \mathbb{Z} = \operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{R} = \operatorname{char} \mathbb{C} = 0$.
Wir ziehen nun Satz 3.4.2.4 zu Rate, wonach (u.a.) $\mathbb{Z}_m$ genau dann ein Körper ist, wenn $m\mathbb{Z}$ ein maximales Ideal von $\mathbb{Z}$ ist. Weil $m\mathbb{Z} \subseteq n\mathbb{Z}$ genau für $n|m$ gilt, ist folglich $\mathbb{Z}_m$ genau dann ein Körper, wenn $m$ außer 1 keine echten Teiler in $\mathbb{N}$ hat, wenn also $m = p$ eine Primzahl ist. Ist $m \in \mathbb{N}$ hingegen keine Primzahl, so sind drei Möglichkeiten zu unterscheiden: $\mathbb{Z}_0 = \mathbb{Z}/0\mathbb{Z} = \mathbb{Z}/\{0\} \cong \mathbb{Z}$ ist ein Integritätsbereich, $\mathbb{Z}_1 = \mathbb{Z}/\mathbb{Z} \cong \{0\}$ ist einelementig. Ist jedoch $m = ab$ mit $1 < a, b < m$ zusammengesetzt, so sind $a_R \neq 0_R \neq b_R$ wegen $a_R b_R = m_R = \varphi(m) = 0_R$ Nullteiler. Wir fassen zusammen:

**Satz 3.4.3.3.** *Für die Restklassenringe $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$, $m \in \mathbb{N}$, sind folgende vier Fälle zu unterscheiden:*

1. *Für $m = p \in \mathbb{P}$ ist $\mathbb{Z}_m = \mathbb{Z}_p$ ein endlicher Körper.*
2. *Für eine zusammengesetzte Zahl $m > 1$ ist $\mathbb{Z}_m$ ein endlicher Ring mit Nullteilern (also weder Integritätsbereich noch Körper).*

3. *Für $m = 0$ ist $\mathbb{Z}_m = \mathbb{Z}_0 \cong \mathbb{Z}$ ein Integritätsbereich, aber kein Körper.*

4. *Für $m = 1$ ist $\mathbb{Z}_m = \mathbb{Z}_1 \cong \{0\}$ ein trivialer, einelementiger Ring (also weder Integritätsbereich noch Körper).*

**Schreibweise 3.4.3.4.** Oft werden wir in der Notation weniger genau sein: Für das Element $n_R := n{\cdot}1_R = n1_R \in R$ schreiben wir meistens nur $n$. Der Kontext[19] entscheidet, ob etwa mit „3“ die natürliche Zahl 3 gemeint ist, oder das Ringelement $3_R := 1_R + 1_R + 1_R$. Man beachte, dass die natürliche Zahl 3 verschieden von der Zahl 0 ist, aber das Ringelement $3_R$ durchaus gleich dem Nullelement $0_R \in R$ sein kann, nämlich wenn $\operatorname{char} R = 3$.

### 3.4.4 Die binomische Formel

Inhalt in Kurzfassung: Die aus der elementaren Arithmetik bekannte binomische Formel für die Potenz einer Summe gilt allgemeiner in beliebigen kommutativen Ringen mit 1. Besonders einfache Gestalt nimmt diese Formel an, wenn die Charakteristik des Ringes eine Primzahl ist und der Exponent eine Potenz dieser Primzahl. In diesem Fall ist das Potenzieren nämlich ein Homomorphismus nicht nur bezüglich der Multiplikation, sondern auch bezüglich der Addition. Die wird in der Theorie endlicher Körper noch eine wichtige Rolle spielen.

Vor allem bei Körpern ist der Unterschied zwischen Charakteristik 0 und Primzahlcharakteristik sehr häufig gravierend. Ein Beispiel dafür bereiten wir mit dem schon aus der Elementarmathematik bekannten und auch für die Analysis wichtigen[20] *binomischen Lehrsatz* (oder auch *binomische Formel*) vor:

**Satz 3.4.4.1.** *Sei $R$ ein Ring mit 1, $a, b \in R$, $ab = ba$ und $n \in \mathbb{N}$. Dann gilt*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}.$$

*Dabei sind die sogenannten* Binomialkoeffizienten $\binom{n}{i} := \frac{n!}{i!(n-i)!}$ *(mit durch $0! := 1$, $(n+1)! := (n+1)n!$ rekursiv definierten Zahlen $n!$, sprich $n$* faktorielle *oder $n$* Fakultät*) stets natürliche Zahlen, weshalb die Summe rechts ein wohldefiniertes Element in $R$ darstellt.*

[19] Achtung! Der Exponent der Unbestimmten in einem Polynom wird immer als natürliche Zahl interpretiert. So ist etwa im Polynom $2x^3$ die Zahl 2 Abkürzung für $1_R + 1_R$ („+“ ist hier die Ringaddition), während mit „3“ tatsächlich die natürliche Zahl gemeint ist. Formal ist dieses Polynom ja eine Potenzreihe $0 + 0x + 0x^2 + 2x^3 + 0x^4 + \cdots$, also ganz formal die Folge $(0_R, 0_R, 0_R, 2_R, 0_R, \ldots)$; die Zahl 3 kommt hier nur als Index des Elements $2_R = 1_R + 1_R$ vor, also sicher nicht als Ringelement.
Daher: Wenn zum Beispiel $\operatorname{char}(R) = 2$ ist, dann gilt zwar $2_R x = x + x = (1_R + 1_R)x = 0$, aber $x \cdot x = x^2 \neq x^0 = 1_R$.

[20] Man denke beispielsweise an die Herleitung von $\exp(a+b) = \exp(a)\exp(b)$ über das Cauchyprodukt zweier Exponentialreihen.

**UE 191** ► **Übungsaufgabe 3.4.4.2.** (W) Beweisen Sie den binomischen Lehrsatz auf zwei Arten: ◄ **UE 191**

1. Mittels Induktion nach $n$. Hinweis: Dazu ist eine Identität für Binomialkoeffizienten erforderlich, die Sie gleichfalls beweisen müssen.
2. Durch kombinatorische Deutung. (Welche Objekte zählt ein Binomialkoeffizient?)

Damit ergibt sich leicht:

**Satz 3.4.4.3.** *Sei $(R, +, 0, -, \cdot, 1)$ ein kommutativer Ring mit 1 und sei* $\operatorname{char} R = p \in \mathbb{P}$. *Dann ist die Abbildung $\varphi : R \to R$, $\varphi(x) := x^p$ ein Homomorphismus, d.h. es gilt*

$$(a+b)^p = a^p + b^p$$

*für alle $a, b \in R$. Allgemeiner sind für $k \in \mathbb{N}$ die Abbildungen $\varphi_k : R \to R$, $\varphi_k(x) := x^{p^k}$ Homomorphismen, d.h. es gilt*

$$(a+b)^{p^k} = a^{p^k} + b^{p^k}$$

*für alle $a, b \in R$.*

*Beweis.* Wir betrachten zunächst $\varphi = \varphi_1$. In 3.4.4.1 hat man lediglich zu beachten, dass für $0 < i < p$ der Binomialkoeffizient $\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{1\cdot 2\cdots i} \in \mathbb{Z}$ nicht nur ganzzahlig ist, sondern einen Faktor $p$ im Zähler, nicht aber im Nenner hat, also durch $p$ teilbar ist (hier geht ein, dass $p$ prim ist). Wegen $\operatorname{char} R = p$ fallen deshalb die Summanden für diese $i$ weg. Für $i = 0$ und $i = p$ ist hingegen $\binom{p}{i} = 1$, weshalb nur die Summanden $b^p$ und $a^p$ übrig bleiben. Damit ist die Behauptung, für diesen Fall bewiesen.
Für die zweite Behauptung ist nur mit Induktion nach $k$ zu beweisen, dass $\varphi_k = \varphi^k$ gilt ($k$-fache Anwendung von $\varphi$ hintereinander, d.h. $\varphi_k = \underbrace{\varphi \circ \cdots \circ \varphi}_{k}$). □

Zum Abschluss des Unterabschnitts ein Ausblick auf endliche Körper:

**UE 192** ► **Übungsaufgabe 3.4.4.4.** (F+) Man zeige: Ist $K$ ein endlicher Körper der Charakteristik $p \in \mathbb{P}$, dann sind die Abbildungen $\varphi_k$ aus der Formulierung von Satz 3.4.4.3 Automorphismen von $K$, die sogenannten *Frobenius-Automorphismen* (siehe auch Satz 6.3.3.6). ◄ **UE 192**

### 3.4.5 Quotientenkörper

Inhalt in Kurzfassung: Wendet man die Konstruktion der Quotientengruppe aus einem Monoid (siehe 3.1.4) auf die multiplikative Struktur eines Integritätsbereich an, so entspricht dies dem Übergang von ganzen Zahlen zu Brüchen. So wie dort (d.h. beim elementaren Bruchrechnen) kann auch im allgemeinen Fall die additive Struktur ebenfalls ausgedehnt werden. Wir konzentrieren uns hauptsächlich auf kommutative Ringe mit 1 und erhalten einen Körper (den Quotientenkörper). Auch die Beschränkung auf kürzbare multiplikative Teilmengen als zugelassene „Nenner“ ist möglich. Die abstrakte Definition der resultierenden Objekts erfolgt als initiales Objekt in einer geeigneten Kategorie, legt die Struktur daher bis auf Äquivalenz (insbesondere also bis auf Isomorphie) eindeutig

fest.

In Analogie zur bzw. gestützt auf die Konstruktion des Quotientenmonoids eines Monoids bezüglich eines Untermonoids (siehe 3.1.4) wollen wir nun einen Ring $R$ mit 1 so erweitern, dass gewisse Elemente multiplikative Inverse bekommen. Sofern sich dies als möglich erweist, ist der Weg durch die Konstruktion des Quotientenmonoids aus 3.1.4, angewendet auf die multiplikative Halbgruppe des Ringes, vorgezeichnet. Wir verzichten darauf einen allgemeinen Satz analog zu 3.1.4.8 ausführlich zu beweisen, da wir nicht auf maximale Allgemeinheit abzielen, sondern auf isomorphe Einbettbarkeit wie in Satz 3.1.4.11.

Die multiplikative Struktur muss also ein abelsches Monoid sein, d.h. wir beschäftigen uns mit kommutativen Ringen mit 1, auf deren multiplikative Halbgruppen wir Satz 3.1.4.11 anwenden wollen. Dieser Ansatz wird tatsächlich zum Erfolg führen, weil sich die bei der Konstruktion auftretende Faktorisierung auch mit der additiven Struktur verträgt.

Um das Programm im Detail durchzuführen, analysieren wir zunächst die erforderliche multiplikative Kürzbarkeit im Kontext der Ringstruktur. Um langweilige Fallunterscheidungen zu vermeiden, setzen wir $1 \neq 0$ voraus, was äquivalent ist zu $|R| \geq 2$. Soll $r \in R$ in einer Erweiterung von $R$ ein Inverses $r^{-1}$ haben, so kann $r$ kein *Nullteiler* sein, weil aus $rs = 0$ sofort $s = 1s = (r^{-1}r)s = r^{-1}(rs) = r^{-1}0 = 0$ folgt. Umgekehrt sind Nichtnullteiler $r$ stets kürzbar: Aus $xr = yr$ folgt $(x - y)r = 0$, also $x - y = 0$, d.h. $x = y$. Wir müssen unsere Ambitionen also auf Nichtnullteiler beschränken; wünschen wir uns, dass jedes Element des Rings ungleich 0 ein Inverses bekommt, so müssen wir von einem Integritätsbereich ausgehen. In diesem Fall werden wir einen Körper (den Quotientenkörper) erhalten. Präziser (und allgemeiner) sind wir interessiert an Quotientenringen im Sinne der folgenden Definition.

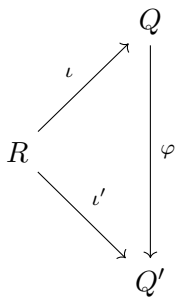
**Definition 3.4.5.1.** Sei $R$ ein kommutativer Ring mit 1 und $K$ ein kürzbares multiplikatives Untermonoid von $R$. Dann heißt $Q$ zusammen mit $\iota\colon R \to Q$ ein *Quotientenring* oder auch *Bruchring* von $R$ bezüglich $K$, wenn folgendes gilt:

1. $Q$ ist ein kommutativer Ring mit 1.

2. Die Abbildung $\iota\colon R \to Q$ ist eine isomorphe Einbettung von $R$ als Ring mit 1 in $Q$.

3. Jedes Element $\iota(r)$ mit $r \in K$ hat in $Q$ ein multiplikatives Inverses.

4. Ist $Q'$ irgendein anderer kommutativer Ring mit Einselement mit einer isomorphen Einbettung $\iota'\colon R \to Q'$ derart, dass jedes $\iota'(r)$ mit $r \in K$ ein multiplikatives Inverses in $Q'$ hat, so gibt es eine eindeutige isomorphe Einbettung $\varphi\colon Q \to Q'$ von $Q$ als Ring mit Einselement in $Q'$, so dass $\iota' = \varphi \circ \iota$.




Ist $R$ ein Integritätsbereich und $K = R^* = R \setminus \{0\}$, so heißt der Quotientenkörper von $R$ bezüglich $K$ zusammen mit $\iota$ auch *Quotientenkörper* von $R$.

Statt wie in Definition 3.4.5.1 lässt sich ein Quotientenring bzw. -körper bei vorgegebenem $R$ und $K$ auch als initiales Objekt in einer geeigneten Kategorie $\mathcal{C} = \mathcal{C}(R, K)$ definieren. Die Objekte sind alle kommutativen Ringe zusammen mit Einbettungen $\iota$ mit den ersten drei Eigenschaften aus 3.4.5.1. Die Morphismen sind Abbildungen $\varphi$ wie in der vierten Eigenschaft. Dann folgt aus Satz 2.2.3.2:

**Folgerung 3.4.5.2.** *Quotientenringe (insbesondere auch Quotientenkörper) sind bis auf Isomorphie eindeutig bestimmt.*

**UE 193 ► Übungsaufgabe 3.4.5.3.** (F) Führen Sie die Begründung von Folgerung3.4.5.2 im Detail aus. **◄ UE 193**

Wir wollen zeigen, dass ein Quotientenring stets existiert. Die Konstruktion des Quotientenmonoids des multiplikativen Monoids von $R$ bezüglich eines kürzbaren multiplikativen Untermonoid $K$ von $R$ gelingt gemäß Satz 3.1.4.11 durch Betrachten des Faktormonoids von $R \times K$ nach der Kongruenzrelation $\sim$. Dabei ist $\sim$ definiert durch $(r, r_0) \sim (s, s_0)$ genau dann, wenn $rs_0 = sr_0$. Die Elemente der so konstruierten Struktur sind $\sim$-Kongruenzklassen $[(r, r_0)]_\sim$. Entscheidend für die Erweiterung der Konstruktion von Monoiden auf Ringe ist, dass $\sim$ nicht nur mit der Multiplikation verträglich ist (was wir aus 3.1.4 wissen), sondern auch mit der Addition auf $R \times K$, die der elementaren Bruchrechnung nachgebildet ist:

**Lemma 3.4.5.4.** *Ist $R$ ein kommutativer Ring mit 1 und $K$ ein kürzbares multiplikatives Untermonoid von $R$, so wird auf $R \times K$ durch die Addition*

$$(r, r_0) + (s, s_0) := (rs_0 + sr_0, r_0 s_0)$$

*eine binäre Gruppenoperation mit neutralem Element $(0, 1)$ und Inversen $-(r, r_0) := (-r, r_0)$ definiert.*

**UE 194 ► Übungsaufgabe 3.4.5.5.** (F) Beweisen Sie Lemma 3.4.5.4. **◄ UE 194**

Für die weitere Konstruktion entscheidend ist:

**Lemma 3.4.5.6.** *Die Relation $\sim$ ist eine Kongruenzrelation auf der Gruppe aus Lemma 3.4.5.4.*

*Beweis.* Wegen Proposition 3.2.2.1 genügt es die Verträglichkeit von $\sim$ mit der Addition zu überprüfen. Seien also $(r, r_0) \sim (r', r'_0)$, d.h. $rr'_0 = r'r_0$, und $(s, s_0) \sim (s', s'_0)$, d.h. $ss'_0 = s's_0$. Zu zeigen ist

$$(rs_0 + sr_0, r_0s_0) = (r, r_0) + (s, s_0) \quad \sim \quad (r', r'_0) + (s', s'_0) = (r's'_0 + s'r'_0, r'_0s'_0),$$

was sich aus der Rechnung

$$(rs_0 + sr_0)(r'_0s'_0) = rr'_0s_0s'_0 + ss'_0r_0r'_0 = r'r_0s_0s'_0 + s's_0r_0r'_0 = (r's'_0 + s'r'_0)(r_0s_0)$$

ergibt. □

Da die Verträglichkeit von $\sim$ mit den nullstelligen Operationen 0 und 1 trivial ist, ist die Faktorstruktur $Q := (R \times K)/_\sim$ vom Typ $(2, 0, 1, 2, 0)$ wohldefiniert.

**Satz 3.4.5.7.** *Sei $R$ ein kommutativer Ring mit 1 und $K$ ein kürzbares multiplikatives Untermonoid von $R$. Dann ist die oben definierte Algebra $Q := (R \times K)/_\sim$ zusammen mit $\iota\colon R \to Q$, $r \mapsto [(r, 1)]_\sim$ ein Quotientenring von $R$ bezüglich $K$. Ist $R$ ein Integritätsbereich und $K = R \setminus \{0\}$, so liegt sogar ein Quotientenkörper vor.*

*Beweis.* Wir beweisen die vier Bedingungen aus Definition 3.4.5.1:

1. $Q$ ist ein kommutativer Ring mit 1: Alle Aussagen über die multiplikative Struktur von $Q$ (kommutatives Monoid) folgen aus den entsprechenden Konstruktionen für Quotientenmonoide, insbesondere aus Satz 3.1.4.11. $R \times K$ ist nach Lemma 3.4.5.4 eine kommutative Gruppe, was sich bei Faktorisierung bezüglich $\sim$ auf $Q = (R \times K)/_\sim$ überträgt. Distributivität gilt zwar nicht auf $R \times K$, man rechnet aber leicht

   $$(r, r_0)((s, s_0) + (s', s'_0)) \sim (r, r_0)(s, s_0) + (r, r_0)(s', s'_0)$$

   nach (Übung), was für die zu beweisende Distributivität auf $Q$ ausreicht.

2. $\iota$ ist eine isomorphe Einbettung von $R$ als Ring mit 1: Von der Konstruktion des Quotientenmonoids ist bekannt, dass $\iota$ eine isomorphe Einbettung des multiplikativen Monoids von $R$ in $Q$ ist. Die Verträglichkeit von $+$ (und folglich von $-$) ergibt sich so:

   $$\iota(r + s) = [(r + s, 1)]_\sim = [(r \cdot 1 + s \cdot 1, 1 \cdot 1)]_\sim = [(r, 1)]_\sim + [(s, 1)]_\sim = \iota(r) + \iota(s)$$

3. Das folgt wieder aus der Konstruktion des Quotientnemonoids.

4. Sei $Q'$ irgendein anderer kommutativer Ring mit Einselement mit einer isomorphen Einbettung $\iota' \colon R \to Q'$ derart, dass alle $\iota(r)$ mit $r \in K$ ein multiplikatives Inverses in $Q'$ haben. Weil $Q$ ein Quotientenmonoid des multiplikativen Monoids $R$ bezüglich des kürzbaren Untermonoids $K$ ist, gibt es eine eindeutige isomorphe Einbettung $\varphi \colon Q \to Q'$ des multiplikativen Monoids $Q$ in $Q'$ mit $\iota' = \varphi \circ \iota$. Somit muss erst recht jede Einbettung $\varphi$ von $Q$ in $Q'$ als Ring mit 1 eindeutig sein, nämlich, wie aus dem Beweis von 3.1.4.11 ersichtlich ist, $\varphi([(r, r_0)]_\sim) = \iota'(r)\iota'(r_0)^{-1}$. Weil die Verträglichkeit von $\varphi$ mit der multiplikativen Struktur gleichfalls schon aus 3.1.4.11 bekannt ist, bleibt einzig die mit der Addition zu zeigen. Es ist also lediglich nachzurechnen (Übung), dass

$$\varphi([(r, r_0)]_\sim + [(s, s_0)]_\sim) = \varphi([(r, r_0)]_\sim) + \varphi([(s, s_0)]_\sim)$$

gilt.

□

Wie schon bei Quotientenmonoiden schreibt man meistens $\frac{r}{r_0}$ für $[(r, r_0)]$.

**UE 195 ► Übungsaufgabe 3.4.5.8.** (V) Tragen Sie die im ersten und vierten Teil des Beweises von Satz 3.4.5.7 nicht durchgeführten Rechnungen nach. **◄ UE 195**

Quotientenringe und -körper existieren also unter sehr allgemeinen Voraussetzungen. Darüber hinaus geben die folgenden Aussagen nützliche Illustrationen zu diesen Begriffen. Die Beweise sind nicht schwierig und Gegenstand der darauf folgenden Übungsaufgabe.

**Proposition 3.4.5.9.** *1. Sei $R$ ein Unterring mit 1 eines Körpers $K$. Dann ist*

$$K' := \left\{ \frac{p}{q} : \ p, q \in R, q \neq 0 \right\}$$

*ein Unterkörper von $K$.*

*2. Der Körper $K'$ aus dem ersten Teil ist der kleinste Unterkörper von $K$, der $R$ enthält, symbolisch $K' = \langle R \rangle_{Körper}$. Explizit bedeutet das: Jeder Unterkörper $K''$ von $K$ mit $R \subseteq K''$ umfasst $K'$.*

*3. In derselben Situation ist $K$ (zusammen mit der Inklusionsabbildung) genau dann ein Quotientenkörper von $R$, wenn $K = K'$ gilt.*

*4. Ist $\iota \colon R \to K$ eine isomorphe Einbettung des Integritätsbereichs $R$ in einen Körper $K$ und $Q$ der von $\iota(R)$ erzeugte Unterkörper von $K$, so ist $Q$ zusammen mit $\iota$ ein Quotientenkörper von $R$.*

**UE 196 ► Übungsaufgabe 3.4.5.10.** (W) Beweisen Sie Proposition 3.4.5.9. **◄ UE 196**

Man sieht unmittelbar ein: Der Quotientenkörper des Integritätsbereiches $\mathbb{Z}$ ist der Körper $\mathbb{Q}$ der rationalen Zahlen. Der Quotientenkörper eines Körpers $K$ ist zu $K$ isomorph bzw. nach dem Prinzip der isomorphen Einbettung $K$ selbst. Von besonderem Interesse wird später auch der Quotientenkörper eines Polynomrings sein, der sogenannte *Körper der gebrochen rationalen Funktionen.*

**UE 197** ► **Übungsaufgabe 3.4.5.11.** (F) Beschreiben Sie Quotientenkörper von $R := \{a+b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ und von $S := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ auf möglichst einfache Weise und ohne auf die Konstruktion, auf die sich Satz 3.4.5.7 bezieht, zurückzugreifen. ◄ **UE 197**

Aus der Konstruktion des Quotientenringes geht hervor, dass sich die Darstellung rationaler Zahlen als Brüche auf allgemeinere Strukturen übertragen lässt. In $\mathbb{Q}$ gibt es unter den verschiedenen Darstellungen immer eine als gekürzter Bruch, etwa $\frac{16}{12} = \frac{4}{3}$. Der Grund ist offenbar die Existenz eines größten gemeinsamen Teilers von Zähler und Nenner in $\mathbb{Z}$, durch den gekürzt werden kann. Diese Möglichkeit besteht nicht immer, wenn man von $\mathbb{Z}$ zu beliebigen Intrgritätsbereichen übergeht. Im Kapitel 5 über Teilbarkeitslehre werden wir solche Aspekte nochmals behandeln.
Doch hat die Darstellung rationaler Zahlen als Brüche auch Nachteile. Dies wird deutlich, wenn wir an Größenvergleiche denken. Hier erweist es sich als vorteilhaft, rationale Zahlen als reelle Zahlen mit eventuell unendlicher Dezimaldarstellung aufzufassen. Denn aus dieser Darstellung lässt sich unmittelbar ablesen, welche von zwei Zahlen die kleinere ist und welche die größere.

**UE 198** ► **Übungsaufgabe 3.4.5.12.** (E) Zeigen Sie: Unter den reellen Zahlen sind die rationalen genau jene mit schließlich periodischer Dezimaldarstellung. Die gleiche Aussage gilt auch für die Darstellung bezüglich jeder anderen Basis $b = 2, 3, \ldots$ anstelle von 10. ◄ **UE 198**

### 3.4.6 Polynome und formale Potenzreihen

Inhalt in Kurzfassung: Formale Potenzreihen über einem kommutativen Ring $R$ mit 1 (d.h. mit Koeffizienten aus $R$) sind durch die Folge ihrer Koeffizienten gegeben, können daher als eben diese Folgen definiert werden. In üblicher Weise kann die Menge $R[[x]]$ aller formalen Potenzreihen sowohl mit einer additiven als auch mit einer multiplikativen Struktur (gliedweise bzw. Cauchyprodukt) ausgestattet werden. Offenbar enthält $R[[x]]$ auch den Ring $R[x]$ aller Polynome über $R$ (nur endlich viele Koeffizienten $\neq 0$). Ist $R$ ein Integritätsbereich, so auch $R[[x]]$ und $R[x]$, und es kann der Quotientenkörper von $R[[x]]$ gebildet werden. Dieser lässt sich als Ring $R[[[x]]]$ der formalen Laurentreihen auffassen, die auch endlich viele Glieder mit negativen Potenzen enthalten dürfen. Durch Iteration des Übergangs von $R$ zu $R[x]$ lassen sich auch Polynomringe in mehreren Variablen bilden. Polynomringe zeichnen sich durch eine universelle Eigenschaft aus, die in 4.2.3 noch näher beleuchtet werden wird.

In der naiven Auffassung wird der Polynomring $R[x]$ über einem kommutativen Ring $R$ mit 1 beschrieben als Menge aller formalen Summen

$$p(x) = \sum_{k=0}^{n} a_k x^k.$$

Da der Begriff einer *formalen Summe* (noch) auf unklarem begrifflichen Fundament steht, machen wir uns zur Präzisierung zunutze, dass $p$ allein durch die $a_k$ eindeutig bestimmt ist, also mit der Folge $(a_k)_{k\in\mathbb{N}}$ identifiziert werden kann.

**Definition 3.4.6.1.** Sei $R$ kommutativer Ring mit 1. Die Menge $R[[x]]$ der *formalen Potenzreihen* ist definiert als die Menge aller Folgen $(a_n)_{n\in\mathbb{N}}$ mit $a_n \in R$ für alle $n \in \mathbb{N}$. Statt $(a_n)_{n\in\mathbb{N}}$ schreiben wir für eine Potenzreihe allerdings meist $\sum_n a_n x^n$; den $n$-ten Eintrag $a_n$ der Folge $(a_n)_{n\in\mathbb{N}}$ nennen wir *Koeffizienten* von $x^n$ oder auch den *$n$-ten Koeffizienten* der Potenzreihe.
Auf $R[[x]]$ ist durch

$$(a_k)_{k\in\mathbb{N}} + (b_k)_{k\in\mathbb{N}} := (a_k + b_k)_{k\in\mathbb{N}}$$

eine Addition definiert und durch

$$(a_k)_{k\in\mathbb{N}} \cdot (b_k)_{k\in\mathbb{N}} := (c_k)_{k\in\mathbb{N}} \quad \text{mit} \quad c_k := \sum_{i=0}^{k} a_i b_{k-i}$$

eine Multiplikation (*Cauchyprodukt*), die den üblichen Produkten von Polynomen bzw. Potenzreihen entspricht.
Jedes Element $a \in R$ identifizieren wir mit der Potenzreihe $\sum a_n x^n$ mit $a_0 = a$, $a_n = 0$ für $n > 0$. Insbesondere schreiben wir 0 für die konstante Folge $(0)_{n\in\mathbb{N}}$ (also $a_n = 0$ für alle $n \in \mathbb{N}$, das neutrale Element in $R[[x]]$ bezüglich der Addition) und 1 für die Folge $(a_n)_{n\in\mathbb{N}}$ mit $a_0 = 1$ und $a_n = 0$ für $n > 0$ (das neutrale Element bezüglich der Multiplikation).
Die Potenzreihe $\sum a_n x^n$, die $a_0 = 0 = a_n$ für $n > 1$ und $a_1 = 1$ erfüllt, bezeichnen wir mit $x$.

**Definition 3.4.6.2.** Die Menge der *Polynome* über $R$, geschrieben $R[x]$, ist die Menge aller Potenzreihen $\sum_{n\in\mathbb{N}} a_n x^n \in R[[x]]$, für die es ein $m$ gibt mit $a_n = 0$ für alle $n > m$. Statt $\sum_{n\in\mathbb{N}} a_n x^n$ schreiben wir dann auch $\sum_{n=0}^{m} a_n x^n$ oder $a_m x^m + a_{m-1} x^{m-1} + \ldots + a_1 x + a_0$.

**Proposition 3.4.6.3.**
1. *$R[[x]]$ mit den soeben definierten Operationen[21] ist ein kommutativer Ring mit* 1*, genannt der* Ring der formalen Potenzreihen über *$R$.*
2. *$R[x]$ ist Unterstruktur von $R[[x]]$ (betrachtet als Ring mit* 1*), genannt der* Polynomring über *$R$.*

[21] Tatsächlich gibt es eine sehr natürliche Topologie auf $R[[x]]$ (nämlich die Produkttopologie auf $R[[x]] = \prod_{n\in\mathbb{N}} R$, wobei wir $R$ mit der diskreten Topologie ausstatten), bezüglich der diese Operationen die einzigen stetigen Fortsetzungen der Operationen auf $R[x]$ sind.

**UE 199 ► Übungsaufgabe 3.4.6.4.** (V) Beweisen Sie die beiden Behauptungen aus Proposition 3.4.6.3. **◄ UE 199**

Jedes $a \in R$ lässt sich nach Definition 3.4.6.1 als Potenzreihe $p(x) = \sum_{n=0}^{\infty} a_n x^n$ mit $a_0 = a$ und $a_n = 0$ für alle $n > 0$ auffassen, die sogar ein Polynom ist. Weil es sich bei dieser Identifikation sogar um eine isomorphe Einbettung handelt, gilt für diese kommutativen Ringe mit 1 die Unteralgebrenbeziehung $R \leq R[x] \leq R[[x]]$.
Ist $p \in R[[x]] \setminus \{0\}$, so gibt es Koeffizienten $a_n \neq 0$. Insbesondere gibt es ein kleinstes derartiges $n$, genannt die *Ordnung* von $p$, symbolisch

$$\operatorname{ord}(p) := \min\{n \in \mathbb{N} : \ a_n \neq 0\}.$$

Einen größten Index gibt es genau dann, wenn $p \in R[x] \setminus \{0\}$. Dieser Index heißt der *Grad* von $p$, symbolisch

$$\operatorname{grad}(p) := \max\{n \in \mathbb{N} : \ a_n \neq 0\}.$$

Um manch mühsame Fallunterscheidung zu vermeiden, vereinbaren wir außerdem

$$\operatorname{grad}(0) = -\infty \quad \text{und} \quad \operatorname{ord}(0) = \infty$$

und, sofern $p \in R[[x]] \setminus R[x]$, $\operatorname{grad}(p) = \infty$; außerdem für alle $k \in \mathbb{Z}$ die Beziehungen $-\infty < k < \infty$, $k + \infty = \infty$ und $k + (-\infty) = -\infty$.
Ziemlich leicht zu beweisen sind folgende Aussagen:

**Proposition 3.4.6.5.** *Sei $R$ ein kommutativer Ring mit 1, außerdem $p, q \in R[[x]]$ mit $p(x) = \sum_{n=0}^{\infty} a_n x^n$ und $q(x) = \sum_{n=0}^{\infty} b_n x^n$. Mit $R^*$, $R[[x]]^*$ und $R[x]^*$ seien die Einheitengruppen der Ringe $R$, $R[[x]]$ bzw. $R[x]$ bezeichnet. Dann gilt:*

1. $\operatorname{ord}(p+q) \geq \min\{\operatorname{ord}(p), \operatorname{ord}(q)\}$
2. $\operatorname{grad}(p+q) \leq \max\{\operatorname{grad}(p), \operatorname{grad}(q)\}$
3. $\operatorname{ord}(pq) \geq \operatorname{ord}(p) + \operatorname{ord}(q)$. *Ist $R$ ein Integritätsbereich, so gilt sogar Gleichheit.*
4. $\operatorname{grad}(pq) \leq \operatorname{grad}(p) + \operatorname{grad}(q)$. *Ist $R$ ein Integritätsbereich, so gilt sogar Gleichheit.*
5. *Ist $R$ ein Integritätsbereich, so auch $R[[x]]$ und $R[x]$.*
6. *Genau dann ist $p \in R[[x]]^*$, wenn $a_0 \in R^*$. Ist $q = p^{-1}$ das multiplikative Inverse von $p$, dann erfüllen die Koeffizienten $b_0 = a_0^{-1}$ und für alle $n = 1, 2, \ldots$ die Rekursion $b_n = -b_0(a_1 b_{n-1} + a_2 b_{n-2} + \ldots + a_n b_0)$. Ist speziell $R$ ein Körper, so ist $p \in R[[x]]^*$ genau dann, wenn $\operatorname{ord}(p) = 0$.*
7. *Wenn $R$ Integritätsbereich ist, dann gilt für alle $p \in R[x]$: Genau dann ist $p \in R[x]^*$, wenn $\operatorname{grad}(p) = 0$ und $p = a_0$ mit $a_0 \in R^*$.*

**UE 200** ► **Übungsaufgabe 3.4.6.6.** (F) Beweisen Sie Proposition 3.4.6.5, und zeigen Sie durch (möglichst einfache) Beispiele, dass man „≤“ bzw. „≥“ im Allgemeinen nicht durch „=“ ersetzen kann. ◄ **UE 200**

Ist $n$ der Grad des Polynoms[22] $p$, so nennt man $a_n$ den *führenden Koeffizienten* von $p$, $a_0$ den *konstanten*, $a_1$ den *linearen* etc. Ist $a_n = 1$, so heißt $p$ *normiert* oder *monisch*.
Klarerweise bilden Polynome wie auch formale Potenzreihen keinen Körper, selbst wenn $R$ einer ist. Dennoch ist bei Polynomen, ähnlich wie in den ganzen Zahlen, Division mit Rest möglich. Genauer:

**Satz 3.4.6.7.** *Sei $R$ ein kommutativer Ring mit Einselement, $a \in R[x]$ mit einem führenden Koeffizienten, der eine Einheit ist, und $b \in R[x]$ beliebig. (Die Voraussetzung bedeutet insbesondere, dass $a \neq 0$. Ist $R$ sogar ein Körper, so erfüllt umgekehrt jedes $a \neq 0$ diese Voraussetzung.)*
*Dann gibt es $q, r \in R[x]$ mit $b = qa + r$ und* $\operatorname{grad}(r) < \operatorname{grad}(a)$.

**UE 201** ► **Übungsaufgabe 3.4.6.8.** (W) Beweisen Sie Satz 3.4.6.7 mittels Induktion nach $\operatorname{grad}(b)$. Inwiefern lässt sich aus Ihrem Beweis ein Algorithmus zur Polynomdivision gewinnen? ◄ **UE 201**

Quotientenkörper von $R[x]$ und $R[[x]]$ existieren genau dann, wenn diese Integritätsbereiche sind, also wenn $R$ selbst einer ist.

**Definition 3.4.6.9.** Sei $R$ ein Integritätsbereich. Dann heißt der Quotientenkörper von $R[x]$ auch der Körper der *gebrochen rationalen Funktionen* über $R$ (siehe auch 5.3.5). Wir schreiben für ihn $R(x)$.

Der Körper $R(x)$ lässt sich deuten als Menge aller Ausdrücke der Gestalt $\frac{p(x)}{q(x)}$ mit $p, q \in R[x]$ und $q \neq 0$, wobei Kürzung von Brüchen in üblicher Weise möglich ist. Insbesondere enthält der Körper der gebrochen rationalen Funktionen auch den Quotientenkörper $K$ von $R$, bestehend aus allen $\frac{p}{q}$ mit $p, q \in R \leq R[x]$ und $q \neq 0$. Es gibt dann einen natürlichen Isomorphismus zwischen $R(x)$ und $K(x)$; daher werden wir Körper der Form $R(x)$ vor allem dann betrachten, wenn $R$ bereits ein Körper ist.
Sei nun $R$ ein Körper. Dann lässt sich der Quotientenkörper $Q$ von $R[[x]]$ wie folgt beschreiben. Wir schreiben eine sogenannte *formale Laurentreihe* $q = q(x)$ in der Form

$$q(x) = \sum_{n=-N}^{\infty} a_n x^n$$

mit einem beliebigen $N \in \mathbb{Z}$ und Koeffizienten $a_n \in R$ an. Der Unterschied zu den formalen Potenzreihen besteht lediglich darin, dass dort $N = 0$ fest ist. Für $a_N \neq 0$ nennt man in Analogie zu früher $N =: \operatorname{ord}(q)$ die *Ordnung* von $q$. Auf der Menge $R[[[x]]]$ aller formalen Laurentreihen (formal kann man sie als Menge aller $(a_n)_{n\in\mathbb{Z}}$ auffassen,

[22] Für $p(x)$ schreiben wir oft auch einfacher (und durchaus konsistent; ausnahmsweise also keine Schlamperei!) $p$ und sprechen von einem *Polynom* in einer Variablen über $R$.

zu denen es ein $N \in \mathbb{Z}$ gibt mit $a_n = 0$ für alle $n < N$) definiert man die Operationen auf natürliche Weise (Addition komponentenweise, Cauchyprodukt so erweitert, dass die Rechenregel $x^{m+n} = x^m \cdot x^n$ gilt). So erhält man wieder einen Integritätsbereich, in dem jedes $q \neq 0$ sogar ein multiplikatives Inverses hat. Denn für $N = \operatorname{ord}(q)$ ist

$$q(x) = \sum_{n=-N}^{\infty} a_n x^n = x^{-N} \sum_{n=0}^{\infty} a_{n-N} x^n$$

mit $a_{0-N} = a_{-N} \neq 0$. Ist $q_0^{-1}$ das multiplikative Inverse von $q_0 := \sum_{n=0}^{\infty} a_{n-N} x^n \in R[[x]]^*$, so ergibt sich damit auch das Inverse $q^{-1}$ von $q$ als $q^{-1} = (x^{-N} q_0)^{-1} = x^N q_0^{-1}$. Somit ist $R[[[x]]]$ ein Körper, in den $R[[x]]$ in offensichtlicher Weise isomorph eingebettet ist. Folglich enthält $R[[[x]]]$ einen Quotientenkörper $Q$ von $R[[x]]$. Offensichtlich ist $R[[[x]]]$ selbst aber der kleinste Unterkörper von $R[[[x]]]$, der $R[[x]]$ enthält (denn ein solcher muss sowohl die Inversen $x^{-N}$ als auch alle $p \in R[[x]]$ enthalten, somit auch deren Produkte), also ist $R[[[x]]] = Q$ selbst der gesuchte Quotientenkörper von $R[[x]]$.

**Satz 3.4.6.10.** *Ist $R$ ein Körper, so bilden die formalen Laurentreihen (zusammen mit der Inklusionsabbildung $\iota\colon R[[x]] \to R[[[x]]]$, $(a_n)_{n\in\mathbb{N}} \mapsto (a_n)_{n\in\mathbb{Z}}$ mit $a_n = 0$ für alle $n < 0$, als isomorpher Einbettung) einen Quotientenkörper von $R[[x]]$.*

**UE 202** ▶ **Übungsaufgabe 3.4.6.11.** (W) Beweisen Sie Satz 3.4.6.10, indem Sie jene Beweisschritte, die oben nur skizzenhaft angedeutet worden sind, ausführlich durchführen. Genauer sind folgende Schritte zu tun: ◀ **UE 202**

1. Definieren Sie sorgfältig die fundamentalen Operationen von $R[[[x]]]$ (Addition, Nullelement, additive Inverse, Multiplikation, Einselement).

2. Zeigen Sie, dass es sich dabei um einen kommutativen Ring mit 1 handelt.

3. Zeigen Sie, dass sich jedes $q \in R[[[x]]] \setminus \{0\}$ *eindeutig* in der Form $x^n \bar{q}(x)$ schreiben lässt, mit $n \in \mathbb{Z}$, und $\bar{q}(x) \in R[[x]]^*$. (Mit $R[[x]]^*$ bezeichnen wir die Einheiten von $R[[x]]$, siehe 3.4.6.5.)

4. Zeigen Sie, dass jedes $q \in R[[[x]]] \setminus \{0\}$ ein multiplikatives Inverses in $R[[[x]]]$ hat. (Somit ist $R[[[x]]]$ ein Körper.)

5. Zeigen Sie, dass $R[[[x]]]$ mit $\iota$ tatsächlich ein Quotientenkörper von $R[[x]]$ ist.

Auf Satz 3.4.6.10 beruhen beträchtliche Teile der Theorie der erzeugenden Funktionen, die zum Beispiel in der Kombinatorik ein unglaublich mächtiges Instrument darstellt. Der Kern dieser Macht besteht darin, dass auf der Seite der Polynome und gebrochen rationalen Funktionen die Teilbarkeitslehre mit Faktorisierungseigenschaften, Partialbruchzerlegung etc. zur Verfügung steht und über die durch Satz 3.4.6.10 beschriebene Verbindung zu den formalen Laurentreihen in Eigenschaften von Folgen (nämlich der

Koeffizienten) übersetzt werden können. Die prominenteste Anwendung ist die Lösungstheorie linearer Rekursionen. Sie wird in Lehrveranstaltungen aus Diskreter Mathematik behandelt.

Die besondere Bedeutung von Polynomen in der klassischen Algebra lässt sich besonders klar auf den Punkt bringen, wenn man Polynome über einem kommutativen Ring mit 1 nicht nur in einer Variablen $x$ betrachtet, sondern in mehreren Variablen, die einer Variablenmenge $X$ entnommen sind. Statt $R[x]$ schreibt man für den resultierenden Ring $R[X]$. Für endliches $X$ lässt sich rekursiv definieren

$$R[x_1, \dots, x_n, x_{n+1}] := R[x_1, \dots, x_n][x_{n+1}].$$

Elemente des resultierenden Ringes $R[x_1, \dots, x_n]$ stellt man als endliche Summen von Ausdrücken der Form $ax_1^{k_1} \dots x_n^{k_n}$ dar mit $a \in R$ und $k_1, \dots, k_n \in \mathbb{N}$. Formal gesprochen ist ein Element von $R[x_1, \dots, x_n]$ also gegeben durch das Koeffiziententupel $(a_{(k_1,\dots,k_n)})_{(k_1,\dots,k_n)\in\mathbb{N}^n}$ mit $a_{(k_1,\dots,k_n)} \in R$, wobei nur endlich viele $a_{(k_1,\dots,k_n)}$ von 0 verschieden sind. Das Tupel $(a_{(k_1,\dots,k_n)})_{(k_1,\dots,k_n)\in\mathbb{N}^n}$ entspricht dabei der (formal unendlichen, tatsächlich endlichen) Summe $\sum_{(k_1,\dots,k_n)\in\mathbb{N}^n} a_{(k_1,\dots,k_n)} x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$.
Für unendliches $X$ kann man $R[X]$ zum Beispiel auch als direkten Limes (siehe 2.3.4) der Ringe $R[x_1, \dots, x_n]$ mit $\{x_1, \dots, x_n\} \subseteq X$ definieren. Der Einfachheit halber beschreiben wir die Vorgangsweise nur für eine abzählbar unendliche Menge $X = \{x_1, x_2, x_3, \dots\}$. Wir setzen $R_n := R[x_1, \dots, x_n]$. Die zugehörigen Einbettungen $\iota_n : R_n \to R_{n+1} = R_n[x_{n+1}]$ liegen auf der Hand: Wir bilden $p \in R_n$ auf das bezüglich $x_{n+1}$ konstante Polynom mit Wert $p$ ab. Der Polynomring $R[X]$ ist dann die durch 2.3.4.5 erhaltene Struktur $R_\infty$. Für überabzählbare Mengen wird dieses schrittweise Vorgehen unelegant, weil man den Wohlordnungssatz aus der Mengenlehre (siehe Anhang, Satz 11.3.2.6) benötigt. Stattdessen kann man eine allgemeinere Version des direkten Limes verwenden, nämlich den direkten Limes einer Familie von Algebren, die durch eine gerichtete Menge anstatt einer Totalordnung indiziert sind; siehe Algebra II (7.1.5). Als Vorgriff sei erwähnt: Mit diesen Mitteln kann man $R[X]$ als Limes von $(R[x_1, \dots, x_n])_{\{x_1,\dots,x_n\}\in\mathfrak{P}_{\text{fin}}(X)}$ definieren, wobei $\mathfrak{P}_{\text{fin}}(X)$ durch $\subseteq$ geordnet sei.
Eine andere, konkretere Realisierung von $R[X]$ verallgemeinert unsere Definition von $R[x]$ und die obige Realisierung des Rings $R[x_1, \dots, x_n]$ in unmittelbarer Weise. Wir betrachten eine beliebige Menge $X$ und stellen Elemente des Rings $R[X]$ wieder als endliche Summen von Ausdrücken $ax_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$ dar mit $a \in R$, $n \in \mathbb{N}$, $x_1, \dots, x_n \in X$ und $k_1, \dots, k_n \in \mathbb{N}$. Bei der Präzisierung müssen wir noch darauf achten, dass jeder solche Ausdruck nur endlich viele Variablen enthalten darf. Daher definieren wir die Indexmenge $M := \{\vec{k} = (k_x)_{x\in X} \in \mathbb{N}^X \mid k_x \neq 0 \text{ für für endlich viele } x \in X\}$ und betrachten $R[X]$ als Menge aller Koeffiziententupel $(a_{\vec{k}})_{\vec{k}\in M}$, wobei wieder nur endlich viele $a_{\vec{k}}$ von 0 verschieden sind. Wir haben in den konkreten Realisierungen von sowohl $R[x_1, \dots, x_n]$ als auch $R[X]$ nur die Grundmengen angegeben, nicht aber die Operationen. Dies holen wir im Rahmen einer Übungsaufgabe nach:

**UE 203** ► **Übungsaufgabe 3.4.6.12.** (V) Sei $R$ ein kommutativer Ring mit 1. Betrachten Sie die oben definierten konkreten Realisierungen von $R[x_1, \dots, x_n]$ und $R[X]$ als Mengen ◄ **UE 203**

von Koeffiziententupeln. Definieren Sie die Operationen $+, -, \cdot$ und die Konstanten $0, 1$ auf diesen beiden Mengen. Zeigen Sie außerdem, dass $(R[x_1, \ldots, x_n], +, 0, -, \cdot, 1)$ sowie $(R[X], +, 0, -, \cdot, 1)$ kommutative Ringe mit 1 sind. Wenn Ihnen das zu langwierig ist: Geben Sie sorgfältig an, welche Aussagen nachzuprüfen sind.

Von besonderem Interesse ist die folgende Eigenschaft von $R[X]$, die an die freie Halbgruppe aus 3.1.2 erinnert, aber auch an den (Halb-) Gruppenring, siehe 4.2.4:

**Proposition 3.4.6.13.** *Sei $R$ ein kommutativer Ring mit 1 und $X$ eine Variablenmenge. Wir betrachten $R[X]$ als Ringerweiterung. Sei $S$ irgendeine Erweiterung von $R$, d.h. $R \leq S$ als kommutativer Ring mit 1. Dann lässt sich jede Abbildung $\iota\colon X \to S$ (Variablenbelegung mit Elementen aus $S$) in eindeutiger Weise zu einem Ringhomomorphismus $\varphi\colon R[X] \to S$ fortsetzen, nämlich durch*

$$\varphi : p = \sum_{i \in I} a_i x_{i,1}^{k_1} \ldots x_{i,n_i}^{k_{n_i}} \mapsto \sum_{i \in I} a_i \iota(x_{i,1})^{k_1} \ldots \iota(x_{i,n_i})^{k_{n_i}}.$$

**UE 204** ► **Übungsaufgabe 3.4.6.14.** (V) Beweisen Sie Proposition 3.4.6.13. Wenn Ihnen das zu langwierig ist: Geben Sie wenigstens sorgfältig an, welche Schritte in so einem Beweis auszuführen sind, und wo die Kommutativität der Multiplikation verwendet wird. ◄ **UE 204**

Der Homomorphismus $\varphi$ lässt sich so interpretieren, dass schlicht in der Summendarstellung des Polynoms für jede Variable $x \in X$ das Ringelement $\iota(x) \in S$ eingesetzt wird. Deshalb spricht man auch vom *Einsetzungshomomorphismus*, der durch $\iota$ induziert wird. Dass es sich um einen Homomorphismus handelt, liegt daran, dass die Operationen für die Elemente von $R[X]$ (Polynome) so definiert sind, dass man mit ihnen so rechnen kann wie in beliebigen Ringen mit 1. Der Polynomring $R[X]$ ist also in gewisser Weise die allgemeinste Ringerweiterung von $R$ um $|X|$ viele Elemente.
Diese Sichtweise wird im Mittelpunkt von Kapitel 4 stehen. Insbesondere werden wir dort Polynomalgebren über allgemeinen Algebren durch eine Eigenschaft wie in Proposition 3.4.6.13 definieren.
Beim Einsetzungshomomorphismus wurde die Variablenbelegung $\iota\colon X \to S$ vorgegeben und $p \in R[X]$ als Argument von $\varphi = \varphi_\iota\colon R[X] \to S$ betrachtet. Man kann auch umgekehrt vorgehen und $p$ festhalten. Die durch das Polynom $p$ induzierte Zuordnung $\iota \mapsto \varphi_\iota(p)$ entspricht für $S = R$ dann dem, was man gemeinhin unter einer *Polynomfunktion* in den Variablen $x \in X$ versteht. Ist $X = \{x_1, \ldots, x_n\}$ endlich, so ist jedes $\iota$ von der Form $x_j \mapsto r_j \in R$, entspricht also dem Ersetzen der Elemente $r_j \in R$ für die Variablen $x_j$ in $p$. Deshalb schreibt man $p(r_1, \ldots, r_n)$ für $\varphi_\iota(p)$.
In offensichtlicher Weise, nämlich vermittels punktweiser Definition wie z.B.

$$(p_1 + p_2)(r_1, \ldots, r_n) := p_1(r_1, \ldots, r_n) + p_2(r_1, \ldots, r_n)$$

etc., bilden die Polynomfunktionen in $n$ (oder auch beliebig vielen) Variablen selbst wieder einen kommutativen Ring mit 1, der in kanonischer Weise ein homomorphes Bild von $R[X]$ ist. Ist beispielsweise $R = \mathbb{R}$ der Ring der reellen Zahlen, so handelt es sich

sogar um eine Isomorphie. Denn jede Polynomfunktion wird von nur einem einzigen reellen Polynom induziert. Ist $R$ hingegen ein endlicher Körper, so gilt dies nicht: Zum Beispiel ist $x^2 - x \in \mathbb{Z}_2[x]$ nicht das Nullpolynom, induziert aber die konstante Funktion mit Wert 0 auf $\mathbb{Z}_2$. Später werden wir uns damit noch ausführlich beschäftigen.
Besonders interessant sind *Nullstellen* von Polynomen. Das sind jene $n$-Tupel $(r_1, \ldots, r_n)$, $r_i \in R$ mit $p(r_1, \ldots, r_n) = 0$. Für $n = 1$ wird sich dieser Aspekt fast durch das gesamte Kapitel 6 über Körper ziehen, später durch die Galoistheorie (Kapitel 9, Algebra II). Für $n > 1$ ist in diesem Zusammenhang vor allem der *Hilbertsche Nullstellensatz* zu nennen; siehe Abschnitt 10.3.

### 3.4.7 Der Chinesische Restsatz

Inhalt in Kurzfassung: Darstellungen als direkte Produkte spielen bei Ringen keine so große Rolle wie bei Gruppen. Von Interesse ist aber immerhin der Chinesische Restsatz. Er wird zunächst in einer allgemeinen, dann in seiner klassischen Fassung gebracht.

Sei $R = R_1 \times R_2$ das direkte Produkt der Ringe $R_1$ und $R_2$. Wohl liegen in Analogie zu Gruppen sowohl kanonische Projektionen $\pi_1 : R \to R_1$, $(r_1, r_2) \mapsto r_1$ und $\pi_2 : R \to R_2$, $(r_1, r_2) \mapsto r_2$, als auch kanonische Einbettungen $\iota_1 : R_1 \to R$, $r_1 \mapsto (r_1, 0)$, und $\iota_2 : R_2 \to R$, $r_2 \mapsto (0, r_2)$, vor. Es ist aber zu beachten, dass im Falle von Ringen mit $1 \neq 0$ die Einbettungen wegen $\iota_1(1_{R_1}) = (1, 0) \neq (1, 1) = 1_R$ und $\iota_2(1_{R_2}) = (0, 1) \neq (1, 1) = 1_R$ nicht mit 1 verträglich sind. So wie bei allgemeineren Klassen von Algebren ist es deshalb angemessen, die Komponenten $R_1$ und $R_2$ nicht als Unter-, sondern nur als Faktorstrukturen von $R$ aufzufassen, die nach dem Homomorphiesatz den Homomorphismen $\pi_2$ bzw. $\pi_1$ entsprechen. Schreibt man so wie bei Gruppen $R_1 \cong R/\iota_2(R_2)$ und $R_2 \cong R/\iota_1(R_1)$, so wird deutlich, dass die eingebetteten Kopien $\iota_i(R_i)$ der $R_i$ in $R$ nicht die Rollen von Unterringen, sondern von Idealen spielen.
Unter diesem Gesichtspunkt ist auch der sogenannte *Chinesische Restsatz* zu verstehen. In seiner klassischen zahlentheoretischen Form bezieht er sich darauf, die Lösung von Kongruenzen in ganzen Zahlen modulo $m$ zurückzuführen auf Kongruenzen modulo $p^e$, wenn $p \in \mathbb{P}$ und $p^e$ die höchste $p$-Potenz ist, die $m$ teilt. Eine abstraktere, algebraische Fassung im Sinn der einleitenden Bemerkungen ist die folgende.

**Satz 3.4.7.1** (Chinesischer Restsatz, allgemeine Fassung)**.** *Seien $R$ ein Ring mit 1 und $I_1, \ldots, I_n$, $n \geq 2$, Ideale von $R$ mit $I_j + I_k = R$ für alle $j \neq k$. Weiters sei $I := I_1 \cap \ldots \cap I_n$.*

*(a) Dann gibt es zu beliebig vorgegebenen Elementen $r_1, \ldots, r_n \in R$ ein modulo $I$ eindeutig bestimmtes $r \in R$ mit $r \equiv r_j \mod I_j$, $j = 1, \ldots, n$.*

*(b) Es gilt $R/I \cong \prod_{j=1}^{n} R/I_j$, wobei $\psi : r + I \mapsto (r + I_1, \ldots, r + I_n)$ ein Ringisomorphismus ist.*

*Beweis.* (a) Mittels Induktion nach $i$ sieht man $R = I + (I_2 \cap \cdots \cap I_i)$ für alle $i = 2, \ldots, n$ wie folgt: Der Induktionsanfang $i = 2$ gilt nach Voraussetzung. Für den

Induktionsschritt von $i$ auf $i+1$ behaupten wir

$$R = R \cdot R = (I_1 + (I_2 \cap \ldots \cap I_i))(I_1 + I_{i+1}) \subseteq I_1 + (I_2 \cap \ldots \cap I_{i+1}) \subseteq R.$$

Dabei folgt die erste Gleichheit wegen $1 \in R$, die zweite mittels Induktionsannahme und der Voraussetzung $I_j + I_k = R$ für alle $j \neq k$. Die erste Mengeninklusion rechts wiederum ergibt sich durch Ausmultiplizieren unter Verwendung der Idealeigenschaft für alle $I_j$, und die letzte Inklusion ist trivial. Aus dieser Formel folgt wie gewünscht $R = I + (I_2 \cap \cdots \cap I_{i+1})$. Für festes $n$ sieht man ganz analog $R = I_k + I'_k$ mit $I'_k := \cap_{j \neq k} I_j$ für $k = 1, \ldots, n$. Also gibt es zu jedem $k$ Elemente $a_k \in I_k$ und $a'_k \in I'_k$ mit $r_k = a_k + a'_k$, folglich $a'_k \equiv r_k \mod I_k$ und $a'_k \equiv 0 \mod I_j$ für $j \neq k$. Das Element $r := \sum_{k=1}^{n} a'_k$ hat somit die gewünschten Eigenschaften. Ein beliebiges weiteres Element $r'$ erfüllt ebenfalls diese Bedingungen offenbar genau dann, wenn $r - r' \in I$ gilt. Damit ist Behauptung (a) bewiesen.

(b) Die Abbildung $\psi$ ist wegen $I \subseteq I_j$ für alle $j = 1, \ldots, n$ wohldefiniert und offensichtlich ein Ringhomomorphismus. Wir zeigen die Bijektivität, indem wir die Umkehrfunktion $\lambda$ von $\psi$ angeben. Zu $(r_1 + I_1, \ldots, r_n + I_n) \in \prod_{j=1}^{n} R/I_j$ betrachten wir das Gleichungssystem $r \equiv r_j \mod I_j$, $j = 1, \ldots, n$ (klarerweise hängt dieses Gleichungssystem nicht von der konkreten Wahl der Repräsentanten $r_j$ ab). Nach (a) gibt es ein modulo $I$ eindeutig bestimmtes Element $r \in R$, das dieses Gleichungssystem löst, d.h. $(r_1 + I_1, \ldots, r_n + I_n) = (r + I_1, \ldots, r + I_n)$ und die $I$-Äquivalenzklasse $r + I$ der Lösung ist eindeutig bestimmt. Somit können wir $\lambda(r_1 + I_1, \ldots, r_n + I_n) := r + I$ setzen. Wir erhalten $\psi \circ \lambda = \mathrm{id}_{\prod_{j=1}^{n} R/I_j}$ nach Definition von $\lambda$. Umgekehrt ergibt sich $\lambda \circ \psi = \mathrm{id}_{R/I}$ unmittelbar daraus, dass für beliebiges $r \in R$ eine Lösung des zu $\psi(r + I)$ gehörigen Gleichungssystems offensichtlich durch $r + I$ gegeben ist, also $\lambda(\psi(r + I)) = r + I$.

□

Wir kehren kurz zum klassischen Fall des Hauptidealrings $R = \mathbb{Z}$ der ganzen Zahlen zurück. Seien die Ideale von der Form $I_j = m_j\mathbb{Z}$ mit $m_j = p_j^{e_j}$ mit paarweise verschiedenen $p_j \in \mathbb{P}$ und geeigneten $e_j \in \mathbb{N}$. Dann sind die $m_j$ paarweise teilerfremd. Wegen Folgerung 3.2.4.2 bedeutet das $1 = xm_j + ym_k \in I_j + I_k$ für geeignete $x, y \in \mathbb{Z}$, sofern $j \neq k$, und, wegen $I_j + I_k \lhd \mathbb{Z}$ (siehe Proposition 3.4.1.11), $I_j + I_k = \mathbb{Z}$. Das ist gerade die Voraussetzung in Satz 3.4.7.1. In diesem Fall besagt der Chinesische Restsatz daher:

**Korollar 3.4.7.2** (Chinesischer Restsatz, klassische Fassung)**.** *Sei $m = \prod_{j=1}^{n} p_j^{e_j} \in \mathbb{N}$ mit paarweise verschiedenen $p_j \in \mathbb{P}$ und mit Exponenten $e_j \in \mathbb{N}$. Dann gilt die Isomorphie der Restklassenringe*

$$\mathbb{Z}/m\mathbb{Z} \cong \prod_{j=1}^{n} (\mathbb{Z}/p_j^{e_j}\mathbb{Z}).$$

Ignoriert man die multiplikative Struktur und betrachtet nur die additive Gruppe der jeweiligen Ringe, so wird die klassische Fassung des chinesischen Restsatzes zu einer Umformulierung von Übungsaufgabe 3.3.2.13, wie wir dort bereits bemerkt haben. Der wesentliche Unterschied zur allgemeinen Fassung besteht darin, dass im klassischen Fall

die auftretenden Faktorringe $\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/p_j^{e_j}\mathbb{Z}$ (sowie natürlich das Produkt der letzteren) alle endlich sind, während im allgmeinen Fall die Ringe $R/I, R/I_j$ auch unendlich sein dürfen.
Eine weitere Folgerung ist die Formel für die Eulersche $\varphi$-Funktion (siehe Definition 3.2.4.16). Zur Erinnerung: Für eine positive Zahl $n \in \mathbb{N}^+$ ist $\varphi(n)$ definiert als die Anzahl der primen Restklassen modulo $n$. Dabei heißt eine Restklasse prim modulo $n$, wenn alle ihre Elemente (oder äquivalent: ein Element; siehe Übungsaufgabe 3.2.4.15) zu $n$ teilerfremd ist.

**Satz 3.4.7.3.** *Ist $n = \prod_{i=1}^{k} p_i^{e_i}$ mit $k \in \mathbb{N}$, paarweise verschiedenen $p_i \in \mathbb{P}$ und $e_i \in \mathbb{N}^+$, so gilt für die Eulersche $\varphi$-Funktion die Formel*

$$\varphi(n) = \prod_{i=1}^{k} (p_i - 1) p_i^{e_i - 1}.$$

**UE 205** ► **Übungsaufgabe 3.4.7.4.** (W) Beweisen Sie die Formel aus 3.4.7.3, indem Sie folgende Aussagen begründen: ◄ **UE 205**

1. Die Formel gilt für Primzahlpotenzen $n = p^e$.
2. Eine Restklasse ist genau dann prim modulo $m$, wenn sie eine Einheit in der multiplikativen Halbgruppe von $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ ist. Hinweis: 3.2.4.2
3. Man verwende 3.4.7.2, um mittels 2. das Problem für ein beliebiges $n$ auf Primzahlpotenzen zurückzuführen.

### 3.4.8 Beispiele nichtkommutativer Ringe

Inhalt in Kurzfassung: Die wichtigsten Beispiele nichtkommutativer Ringe entstehen als Endomorphismenringe von abelschen Gruppen oder von Moduln. Umgekehrt erhält man sehr natürliche Beispiele von Moduln über im Allgemeinen nichtkommutativen Ringen in Gestalt von abelschen Gruppen über ihrem Endomorphismenring. Wir begnügen uns mit einer sehr kurzen Präsentation.

Sehr wichtige Beispiele nichtkommutativer Ringe sind bereits aus der Linearen Algebra bekannt, nämlich Ringe quadratischer Matrizen bzw., äquivalent, linearer Abbildungen eines (endlichdimensionalen) Vektorraums in sich selbst. Dabei ist die Summe zweier Abbildungen gegeben durch die punktweise Addition, $(f+g)(a) := f(a) + g(a)$, und die Multiplikation zweier Abbildungen gegeben durch die Komposition, $fg(a) := f(g(a))$. Versucht man, die Gesetze eines Rings nachzurechnen, so stellt man fest, dass sich die allermeisten Gesetze von entsprechenden Gesetzen auf der zugrundeliegenden Struktur (hier: ein Vektorraum) vererben. Beispielsweise ist dies für das Assoziativgesetz $(f+g)+h = f+(g+h)$ der Fall: Da in der additiven Gruppe des Vektorraums das Assoziativgesetz gilt, folgt für jedes $a$ aus dem Vektorraum

$$\begin{aligned}((f+g)+h)(a) &= (f+g)(a) + h(a) = (f(a)+g(a)) + h(a) = f(a) + (g(a)+h(a)) \\ &= f(a) + (g+h)(a) = (f+(g+h))(a).\end{aligned}$$

Andere Gesetze wiederum folgen aus entsprechenden Gesetzen der Funktionskomposition (beliebiger!) Abbildungen, beispielsweise das Assoziativgesetz der Multiplikation (also der Komposition) oder auch das Distributivgesetz $(f+g)h = fh+gh$: Für jedes Element $a$ des Vektorraums gilt nämlich

$$((f+g)h)(a) = (f+g)(h(a)) = f(h(a)) + g(h(a)) = (fh)(a) + (gh)(a) = (fh+gh)(a).$$

Dass wir es nicht mit irgendwelchen Abbildungen sondern mit *linearen* Abbildungen zu tun haben, geht nur beim Distributivgesetz $f(g+h) = fg + fh$ ein – dieses ist somit das einzige „nichttriviale“ Gesetz[23]. Für jedes $a$ aus dem Vektorraum berechnet man

$$\begin{aligned}(f(g+h))(a) = f((g+h)(a)) = f(g(a)+h(a)) &\overset{(*)}{=} f(g(a)) + f(h(a)) \\ &= (fg)(a) + fh(a) = (fg+fh)(a);\end{aligned}$$

man sieht, dass in $(*)$ die Linearität von $f$ wesentlich ist. Etwas allgemeiner kann man von Endomorphismen abelscher Gruppen ausgehen und dann auf Moduln und Vektorräume spezialisieren.

**Proposition 3.4.8.1.** *Ist $A$ eine abelsche Gruppe, so bildet die Menge* $\mathrm{End}(A)$ *aller Endomorphismen $f\colon A \to A$ bezüglich der wie folgt definierten Operationen einen Ring mit* 1*:*

- $(f+g)(a) := f(a) + g(a)$
- $0(a) := 0$
- $(-f)(a) := -f(a)$
- $fg(a) := f(g(a))$
- $1(a) := a$.

*Ist $A$ auch ein Modul über einem Ring $R$, so bilden die $R$-Modulendomorphismen von $A$ einen Unterring* $\mathrm{End}_R(A) \leq \mathrm{End}(A)$.
$\mathrm{End}_R(A)$ *ist zum Beispiel dann sicher nicht kommutativ, wenn $R$ ein Körper und $A$ ein Vektorraum über $R$ einer Dimension $\geq 2$ ist. Insbesondere ist auch* $\mathrm{End}(A)$ *im Allgemeinen nicht kommutativ.*

**UE 206 ► Übungsaufgabe 3.4.8.2.** (F) Beweisen Sie 3.4.8.1. **◄ UE 206**

[23] Verzichtet man darauf und begnügt sich mit dem Distributivgesetz $(f+g)h = fh+gh$, so erhält man die Klasse der sogenannten *Fastringe*, für die auch nichtlineare Abbildungen auf geeigneten Strukturen Beispiele liefern

**UE 207** ► **Übungsaufgabe 3.4.8.3.** (D) Untersuchen Sie, für welche endlichen abelschen Gruppen $A$ der Endomorphismenring aus Proposition 3.4.8.1 kommutativ ist, für welche nicht. Beginnen Sie mit sehr einfachen Beispielen für $A$ und versuchen Sie nach und nach eine möglichst große Klasse abelscher Gruppen zu erfassen. Wie weit kommen Sie? (Hinweis: Der Hauptsatz 3.3.4.2 könnte sehr nützlich sein.) ◄ **UE 207**

**UE 208** ► **Übungsaufgabe 3.4.8.4.** (B) ◄ **UE 208**

1. Zeigen Sie: Ist $V$ ein endlichdimensionaler Vektorraum über einem Körper, so ist $\mathrm{End}(V)$ als Ring einfach (besitzt also nur die trivialen Ideale).
2. Zeigen Sie, dass dies für unendlichdimensionale Vektorräume nicht gilt. Hinweis: Betrachten Sie alle Endomorphismen mit endlichdimensionalem Bild.

Bisher haben wir an konkreten Beispielen von Moduln lediglich abelsche Gruppen, aufgefasst als Moduln über den Ringen $\mathbb{Z}$ oder $\mathbb{Z}_m$, kennen gelernt. Beide Ringe sind kommutativ. Da wir mit dem Endomorphismenring einer abelschen Gruppe nun einen mit der Struktur dieser Gruppe eng verbundenen, im Allgemeinen nichtkommutativen Ring zur Verfügung haben, wollen wir zum Abschluss des Abschnitts der Frage nachgehen, ob bzw. wie sich die abelsche Gruppe als Modul über ihrem Endomorphismenring auffassen lässt.
Sei $A$ eine abelsche Gruppe. Definieren wir für festes $f \in \mathrm{End}(A)$ die Multiplikation

$$A \to A, \quad a \mapsto f(a),$$

setzen wir also $fa := f(a)$ für $f \in \mathrm{End}(A)$ und $a \in A$, so gelten tatsächlich alle Gesetze für einen unitären $End(A)$-Modul:

- $(f+g)a = (f+g)(a) = f(a) + g(a) = fa + ga$
- $f(a+b) = f(a) + f(b) = fa + fb$
- $(fg)a = (f \circ g)a = f(g(a)) = f(ga)$
- $1a = \mathrm{id}_A(a) = a$

Wir erhalten also:

**Proposition 3.4.8.5.** *Jede abelsche Gruppe $A$ ist mit der Multiplikation $fa := f(a)$, $f \in \mathrm{End}(A)$ und $a \in A$, auch ein unitärer $\mathrm{End}(A)$-Modul.*

Analoges gilt, wenn man von Vektorräumen über einem Körper $K$ ausgeht. Von den Endomorphismen verlangt man dann neben der Homomorphieeigenschaft bezüglich der Addition auch noch Linearität: $f(\lambda a) = \lambda f(a)$ für $\lambda \in K$. Strukturen dieser Art spielen beim Normalformenproblem quadratischer Matrizen bzw. von Endomorphismen eines endlichdimensionalen Vektorraums eine wichtige Rolle. Wir werden darauf in Algebra II nochmals zu sprechen kommen (siehe 7.4.6).
Einige andere Konstruktionen von Moduln über im Allgemeinen nichtkommutativen Ringen ergeben sich aus der folgenden Übungsaufgabe.

**UE 209 ► Übungsaufgabe 3.4.8.6.** (F) Begründen Sie: **◄ UE 209**

1. Ist $R \leq S$ ein Unterring von $S$, dann ist $S$ in natürlicher Weise ein $R$-Modul.
2. Fasst man einen Ring (in natürlicher Weise) als Linksmodul über sich selbst auf, so sind seine Linksideale genau die Untermoduln.
3. Ist $R$ ein Ring und $I$ ein Linksideal von $R$, dann ist $R/I$ ein Links-$R$-Modul (obwohl $R/I$ nur für ein beidseitiges Ideal $I \lhd R$ ein Ring ist).
4. Sind $R, S$ Ringe, $\varphi\colon R \to S$ ein Ringhomomorphismus und $A$ ein $S$-Modul, dann ist $A$ mit der Funktion $R \times A \to A, (r, a) \mapsto ra := \varphi(r)a$ ein $R$-Modul.

## 3.5 Geordnete Gruppen und Körper

Das Monotoniegesetz als Verträglichkeit einer binären Operation mit einer (Halb-)Ordnungsrelation lässt sich ziemlich allgemein fassen (siehe 3.5.1). Etwas genauer werden wir uns geordneten Gruppen (siehe 3.5.2) und geordneten Körpern, vor allem nochmals $\mathbb{R}$ zuwenden (siehe 3.5.3).

### 3.5.1 Grundlegende Definitionen

Inhalt in Kurzfassung: So wie in den reellen Zahlen das Monotoniegesetz für Addition (eingeschränkt auch für die Multiplikation) gilt, treten auch allgemeinere relationale Strukturen auf, wo Verträglichkeitsbedingungen für Operationen und Relationen gelten. Beispiele sind geordnete Gruppen u.ä.

Geordnete Gruppen und ihre Verwandten stellen eine wichtige Brücke zur Modelltheorie und somit zur mathematischen Logik dar, weil sie algebraische mit Ordnungsstruktur verbinden und somit sehr typische Beispiele für relationale Strukturen sind. Ausgangspunkt ist das von den Zahlenbereichen vertraute Monotoniegesetz.

**Definition 3.5.1.1.** Sei $A$ eine Menge, auf der eine binäre Operation $\circ$ und eine Halbordnung $\leq$ definiert sind. Man sagt, auf $(A, \circ, \leq)$ gilt das *Monotoniegesetz* bezüglich $c \in A$, sofern für alle $a, b, c \in A$ gilt: $a \leq b$ impliziert $a \circ c \leq b \circ c$ und $c \circ a \leq c \circ b$. Das Monotoniegesetz gilt schlechthin, wenn es für alle $c \in A$ gilt.

Sowohl an die Operation $\circ$ als auch an die Halbordnung $\leq$ können zusätzliche Bedingungen gestellt werden, z.B.: $A$ kann bezüglich der Halbordnung $\leq$ verbandsgeordnet oder sogar totalgeordnet sein. Die Operation kann assoziativ oder sogar eine Gruppenoperation sein. Auch kann eine weitere binäre Operation ins Spiel kommen, für die wenigstens bezüglich gewisser Elemente das Monotoniegesetz gilt und so, dass beispielsweise ein Ring oder gar ein Körper entsteht. Auf diese Weise lassen sich zahlreiche Begriffe bilden wie: halbgeordnete Halbgruppe, verbandsgeordnete Gruppe, geordneter Ring, vollständig angeordnete Körper. Die zugehörigen Strukturtheorien dienen wie gesagt besonders in der Modelltheorie als sehr illustrative Beispiele.

Zum Beispiel fordert man von einem *angeordneten Ring*, dass die Addition das Monotoniegesetz schlechthin erfüllt, die Multiplikation bezüglich positiver Elemente $c > 0$. Ein *angeordneter Körper* ist ein angeordneter Ring, der auch ein Körper ist.
Hier wollen wir uns auf einige wenige Bemerkungen zu geordneten Gruppen und zu angeordneten Körpern beschränken.

### 3.5.2 Geordnete Gruppen

Inhalt in Kurzfassung: Unter den geordneten abelschen Gruppen sind die archimedisch angeordneten insofern von besonderem Interesse, als es sich dabei bis auf Isomorphie genau um die additiven Untergruppen von $\mathbb{R}$ handelt.

Der Deutlichkeit halber stellen wir die Definition explizit voran:

**Definition 3.5.2.1.** Eine (*total-*)*geordnete Gruppe* ist eine Gruppe $G$ zusammen mit einer binären Relation $\leq$, die $G$ zu einer Totalordnung macht, so dass bezüglich der binären Gruppenoperation das Monotoniegesetz gilt. Ist $e$ das Einheitselement, so heißt $G^+ := \{g \in G : \ g > e\}$ der *Positivteil* von $G$ und $G^- := \{g \in G : \ g < e\}$ der *Negativteil* von $G$. Die Elemente von $G^+$ heißen *positiv*. Wir schreiben auch $G^* := G^+ \cup G^-$.

Ziemlich leicht beweist man folgende elementare Sachverhalte:

**Proposition 3.5.2.2.** *Sei $G$ eine geordnete Gruppe mit Elementen $a, b, c \in G$. Dann gilt:*

1. *$G^+$ und $G^-$ sind Unterhalbgruppen von $G$.*
2. *Die Beziehung $a \leq b$ gilt genau dann, wenn $b^{-1} \leq a^{-1}$.*
3. *$G^- = \{g^{-1} : \ g \in G^+\}$*
4. *Alle $g \in G^*$ haben unendliche Ordnung.*

**UE 210 ► Übungsaufgabe 3.5.2.3.** (V) Beweisen Sie Proposition 3.5.2.2. **◄ UE 210**

**Definition 3.5.2.4.** Eine geordnete Gruppe heißt *archimedisch angeordnet*, wenn es zu je zwei Elementen $a, b \in G^*$ ein $k \in \mathbb{Z}$ gibt mit $b < a^k$.

Die additive Gruppe der reellen Zahlen und alle ihre Untergruppen (wie z.B. $\mathbb{Z}$ und $\mathbb{Q}$) sind Beispiele archimedisch geordneter Gruppen. Im kommutativen Fall handelt es sich dabei im Wesentlichen sogar um die einzigen Beispiele:

**Satz 3.5.2.5.** *Jede archimedisch angeordnete abelsche Gruppe $G$ lässt sich als solche isomorph in die geordnete additive Gruppe $\mathbb{R}$ der reellen Zahlen einbetten. (Umgekehrt ist jede additive Untergruppe von $\mathbb{R}$ archimedisch angeordnet.) Ist $\iota : G \to \mathbb{R}$ eine solche isomorphe Einbettung, so sind alle anderen gegeben durch sämtliche Abbildungen $\lambda\iota$ mit reellem $\lambda > 0$.*

**UE 211** ► **Übungsaufgabe 3.5.2.6.** (W) Beweisen Sie Satz 3.5.2.5. Anleitung für die Existenz von $\iota$: Gehen Sie für nichttriviales $G$ von einem positiven Element $g \in G$ aus, das Sie auf die reelle Zahl $1 = \iota(g)$ abbilden. Wegen der archimedischen Eigenschaft definiert das einen eindeutigen ordnungsverträglichen Homomorphismus $\iota$, der (wieder wegen der archimedischen Eigenschaft) sogar injektiv sein muss. ◄ **UE 211**

Nicht archimedisch angeordnet ist beispielsweise $\mathbb{Z} \times \mathbb{Z}$ mit der sogenannten *lexikographischen Ordnung*: $(k_1, l_1) < (k_2, l_2)$ genau dann, wenn entweder $k_1 < k_2$ oder $k_1 = k_2$ und $l_1 < l_2$ gilt.

**UE 212** ► **Übungsaufgabe 3.5.2.7.** (B) Beweisen Sie, dass diese Festlegung $\mathbb{Z} \times \mathbb{Z}$ zu einer geordneten Gruppe macht, die jedoch nicht archimedisch geordnet ist. ◄ **UE 212**

**UE 213** ► **Übungsaufgabe 3.5.2.8.** (B) Zeigen Sie, dass es überabzählbar viele Ordnungsrelationen gibt, die die Gruppe $\mathbb{Z} \times \mathbb{Z}$ zu einer geordneten Gruppe machen. Hinweis: Betrachten Sie für irrationales $\alpha$ die Abbildung $\varphi_\alpha \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{R}$, definiert durch $\varphi_\alpha(a, b) := a + \alpha b$, und übertragen Sie damit die Struktur von $\mathbb{R}$ als geordnete Gruppe auf $\mathbb{Z} \times \mathbb{Z}$. ◄ **UE 213**

### 3.5.3 Angeordnete Körper und nochmals $\mathbb{R}$

Inhalt in Kurzfassung: Wir beginnen mit der bereits in 1.2.3 angekündigten Konstruktion der reellen Zahlen mittels Dedekindscher Schnitte. Bis auf Isomorphie ist $\mathbb{R}$ eindeutig bestimmt durch die Eigenschaften eines vollständig angeordneten Körpers. Dies zu beweisen ist das Ziel. Die wichtigsten Zwischenergebnisse auf diesem Weg sind auch für sich bemerkenswert. Sie lauten: Jeder vollständig angeordnete Körper ist archimedisch angeordnet. Jeder archimedisch angeordnete Körper lässt sich (sogar auf eindeutige Weise) in $\mathbb{R}$ einbetten. Abschließend wird der Körper der gebrochen rationalen Funktionen über $\mathbb{Q}$ betrachtet.

Die Konstruktion von $\mathbb{R}$ mit Hilfe Dedekindscher Schnitte dürfte bekannt sein, wenigstens in ihren Grundgedanken:
Jede irrationale Zahl $r \in \mathbb{R} \setminus \mathbb{Q}$ definiert eine Zerlegung (einen Schnitt) der Menge $\mathbb{Q}$ in die beiden Mengen $A_r = \{q \in \mathbb{Q} : \ q < r\}$ und $B_r = \mathbb{Q} \setminus A_r = \{q \in \mathbb{Q} : \ q > r\}$. Es liegt also nahe, die Zahl $r$ mit der Partition von $\mathbb{Q}$ in die Mengen $A_r$ und $B_r$ zu identifizieren. Will man (das bietet gewisse formale Annehmlichkeiten) auch rationale $r \in \mathbb{Q}$ so repräsentieren, hat man zusätzlich lediglich festzulegen, wie man mit $r$ selbst umgeht. (Wir entscheiden uns hier für die Konvention, $r$ in der Menge $A_r$ aufzunehmen und nicht in $B_r$ und dann $r$ durch $(A_r, B_r)$ zu ersetzen.) Bei diesem auf Richard Dedekind (1831–1916) zurückgehenden Zugang fasst man also $\mathbb{R}$ im Wesentlichen auf als die Menge aller Zerlegungen $(A, B)$ von $\mathbb{Q}$ in einen linken Teil $A$ (im rationalen Fall mit Endpunkt) und einen rechten Teil $B$ (ohne Endpunkt). Setzt man $(A_1, B_1) \leq (A_2, B_2)$ sofern $A_1 \subseteq$

$A_2$, beweist man für die resultierende Struktur leicht die Vollständigkeit, dass nämlich jede nichtleere und beschränkte Teilmenge ein Supremum besitzt.

**UE 214** ► **Übungsaufgabe 3.5.3.1.** (E) Zeigen Sie, dass sich die oben skizzierte Dedekind-Vervollständigung in allgemeinerem Kontext durchführen lässt. In einer beliebigen Halbordnung $(H, \leq)$ kann man nämlich jedem $h \in H$ die Menge $\iota(h) := \{x \in H : \ x \leq h\}$ zuordnen. Gehen Sie diesem Ansatz nach und versuchen Sie einen möglichst allgemeinen Satz über die Möglichkeit der Vervollständigung von Halbordnungen zu formulieren und zu beweisen. Gibt es dazu auch eine kategorientheoretische Formulierung? (Die resultierende Konstruktion heißt *Dedekind-MacNeille-Vervollständigung*.) ◄ **UE 214**

Zurück zu den reellen Zahlen: Als Nächstes definieren wir die Rechenoperationen Addition und Multiplikation auf der Menge $\mathbb{R}$. Dies erfordert etwas mühsame Fallunterscheidungen, der Beweis, dass sich ein angeordneter Körper ergibt, noch mühsamere Rechnungen. Mit etwas Fleiß verifiziert man aber, dass alle Punkte aus der Definition des angeordneten Körpers erfüllt sind.

**Definition 3.5.3.2.** Seien $(A, B)$ und $(A', B')$ zwei Dedekindschnitte. Wir setzen $A_0 := \{q \in \mathbb{Q} \mid q \leq 0\}$, $B_0 := \mathbb{Q} \setminus A_0 = \{q \in \mathbb{Q} \mid q < 0\}$ und definieren

- Addition: $(A, B) + (A', B') := \Big(A + A', \mathbb{Q} \setminus (A + A')\Big)$

  (wobei bekanntlich $A + A' = \{a + a' \mid a \in A, a' \in A'\}$)

- Multiplikation:
  - Wenn $(A, B), (A', B') \geq (A_0, B_0)$, dann
    $(A, B) \cdot (A', B') := \Big(A \cdot A', \mathbb{Q} \setminus (A \cdot A')\Big)$.
  - Wenn $(A, B) \geq (A_0, B_0)$ und $(A', B') \leq (A_0, B_0)$, dann
    $(A, B) \cdot (A', B') := \Big( - (A \cdot (-A')), \mathbb{Q} \setminus -(A \cdot (-A'))\Big)$.
  - Wenn $(A, B) \leq (A_0, B_0)$ und $(A', B') \geq (A_0, B_0)$, dann
    $(A, B) \cdot (A', B') := \Big((-A) \cdot A', \mathbb{Q} \setminus ((-A) \cdot A')\Big)$.
  - Wenn $(A, B), (A', B') \leq (A_0, B_0)$, dann
    $(A, B) \cdot (A', B') := \Big((-A) \cdot (-A'), \mathbb{Q} \setminus ((-A) \cdot (-A'))\Big)$.

  (wobei bekanntlich $A \cdot A' = \{a \cdot a' \mid a \in A, a' \in A'\}$ und $-A = \{-a \mid a \in A\}$)

Zur Erinnerung die Definition nochmals explizit:

**Definition 3.5.3.3.** Ist $K$ ein Körper und $\leq$ eine Totalordnung auf $K$, so sprechen wir von einem *angeordneten Körper*, wenn sowohl $K$ bezüglich der Addition als auch die positiven Elemente bezüglich der Multiplikation mit $\leq$ eine geordnete Gruppe bilden. Explizit bedeutet dies, dass die Monotoniegesetze erfüllt sind: Aus $a \leq b \in K$ und $c \in K$ folgt $a + c \leq b + c$ und, sofern $c \geq 0$, auch $ac \leq bc$.

Ein angeordneter Körper $K$ heißt *vollständig angeordnet*, wenn er als Ordnung *bedingt vollständig* ist, d.h. es zu je zwei nichtleeren Teilmengen $A, B \subseteq K$ mit $a \leq b$ für alle $a \in A$ und $b \in B$ ein Element $x \in K$ gibt mit $a \leq x \leq b$ für alle $a \in A$ und $b \in B$.
Ein angeordneter Körper $K$ heißt archimedisch angeordnet, wenn seine additive Gruppe *archimedisch angeordnet* ist.

**UE 215 ► Übungsaufgabe 3.5.3.4.** (A) Zeigen Sie für jeden Körper $K$ die folgenden beiden Aussagen: **◄ UE 215**

1. Sei $\leq$ eine Ordnungsrelation auf $K$, die $K$ zu einem angeordneten Körper macht. Dann bilden die Mengen $K^+ := \{x \in K : \ x > 0\}$, $K^- := \{-x : \ x \in K^+\}$ und $\{0\}$ eine Partition von $K$. (Man beachte, dass $K^+$ additiv und multiplikativ abgeschlossen ist.)

2. Sei $K^+$ eine additiv und multiplikativ abgeschlossene Teilmenge von $K$ derart, dass für $x \in K$ genau eine der drei Bedingungen $x \in K^+$, $-x \in K^+$ oder $x = 0$ erfüllt ist. Wir definieren eine binäre Relation $\leq$ auf $K$ durch: $a \leq b$ genau dann, wenn $b - a \in K^+ \cup \{0\}$. Dann wird $K$ durch $\leq$ zu einem angeordneten Körper.

Für die Vollständigkeit gibt es zahlreiche äquivalente Bedingungen, wie die folgende Aufgabe zeigt.

**UE 216 ► Übungsaufgabe 3.5.3.5.** (D) Sei $K$ bezüglich $\leq$ ein angeordneter Körper. **◄ UE 216**

1. Zeigen Sie, dass genau dann ein vollständig angeordneter Körper vorliegt, wenn in $K$ jede nichtleere und nach oben beschränkte Menge ein Supremum hat.

2. Finden Sie noch weitere zur Vollständigkeit des angeordneten Körpers äquivalente Bedingungen.

Doch nochmals zurück zur Konstruktion von $\mathbb{R}$.

**UE 217 ► Übungsaufgabe 3.5.3.6.** (V) Besprechen Sie die einzelnen Schritte, die für die eingangs skizzierte Konstruktion von $\mathbb{R}$ mittels Dedekindscher Schnitte nötig sind sowie für den Beweis, dass man so wirklich einen vollständig angeordneten Körper erhält. **◄ UE 217**

Jeder angeordnete Körper $K$ enthält eine Kopie von $\mathbb{N}, \mathbb{Z}$ und $\mathbb{Q}$, genauer:

**Definition 3.5.3.7.** Sei $K$ ein angeordneter Körper. Dann bezeichne $\mathbb{N}_K$ den Durchschnitt (d.h. die kleinste) aller bezüglich + abgeschlossenen Teilmengen von $K$, die 0 und 1 enthalten. Ähnlich bezeichne $\mathbb{Z}_K$ die von 1 erzeugte additive Untergruppe und $\mathbb{Q}_K$ den von $\mathbb{Z}_K$ erzeugten Unterkörper von $K$, den sogenannten *Primkörper*.

**UE 218 ► Übungsaufgabe 3.5.3.8.** (W) Zeigen Sie für einen angeordneten Körper $K$: **◄ UE 218**

1. $(\mathbb{N}_K, 0_K, \nu_K)$ (bei kanonischer Interpretation, insbesondere der Nachfolgerfunktion $\nu_K : k \mapsto k +_K 1_K$) ist eine Peano-Struktur und die Einschränkungen der Körperoperationen $+_K, \cdot_K$ stimmen auf $\mathbb{N}_K$ mit den gemäß $((+))$ bzw. $((\cdot))$ in Satz 1.1.5.8 bzw. Übungsaufgabe 1.1.5.9 definierten Rechenoperationen überein. $\mathbb{N}_K$ lässt sich also auch als Halbring auffassen, der isomorph ist zum Halbring $\mathbb{N}$ der natürlichen Zahlen.

2. $\mathbb{Z}_K$ ist sogar ein Unterring von $K$ und als solcher isomorph zum Ring $\mathbb{Z}$ der ganzen Zahlen.

3. $\mathbb{Q}_K$ ist isomorph zum Körper $\mathbb{Q}$ der rationalen Zahlen.

4. Die Isomorphismen aus 1., 2. und 3. sind eindeutig und setzen einander fort.

5. Die Isomorphismen aus 1., 2. und 3. sind auch mit der Ordnungsstruktur verträglich.

(Geben Sie jeweils explizite Isomorphismen an und begründen Sie, warum Ihre Definitionen tatsächlich wohldefinierte Abbildungen liefern.)

Wir wenden uns nun der Rolle der archimedischen Eigenschaft zu.

**UE 219** ► **Übungsaufgabe 3.5.3.9.** (V) Zeigen Sie, dass für einen angeordneten Körper $K$ folgende Eigenschaften äquivalent sind: ◄ **UE 219**

- $K$ ist archimedisch angeordnet.
- $\mathbb{N}_K$ ist beschränkt.
- Sei $a \in K$ und gelte $a \leq \frac{1}{n} = n^{-1}$ für alle $n \in \mathbb{N}_K \setminus \{0\}$. Dann folgt $a \leq 0$.
- $\mathbb{Q}_K$ liegt dicht in $K$. Definitionsgemäß bedeutet dies: Für beliebige $a < b \in K$ gibt es $q \in \mathbb{Q}_K$ mit $a < q < b$.

Wichtig ist folgender Satz:

**Satz 3.5.3.10.** *Jeder vollständig angeordnete Körper ist archimedisch angeordnet. Insbesondere ist $\mathbb{R}$ archimedisch angeordnet.*

*Beweis.* Wir nehmen indirekt an, der vollständig angeordnete Körper $K$ sei nicht archimedisch angeordnet. Dann folgt mit Übungsaufgabe 3.5.3.9, dass die Menge $\mathbb{N}_K$ beschränkt ist und somit auch ein Supremum $s$ hat. Nach der Definition des Supremum ist die Zahl $s - 1 < s$ sicher keine obere Schranke von $\mathbb{N}_K$. Also gibt es ein $n \in \mathbb{N}_K$ mit $s - 1 < n$. Die Monotonie der Addition liefert $s = (s - 1) + 1 < n + 1 \in \mathbb{N}_K$. Das steht aber im Widerspruch dazu, dass $s$ eine obere Schranke von $\mathbb{N}_K$ ist. □

Aus der Dichtheit von $\mathbb{Q}_K$ in einem archimedisch angeordneten Körper $K$ folgt, dass jedes Element $k \in K$ eindeutig bestimmt ist durch den durch $k$ induzierten Dedekindschen Schnitt, d.h. durch die Menge $A_k := \{q \in \mathbb{Q}_K : \ q < k\}$ sowie durch die Menge $B_k := \{q \in \mathbb{Q}_K : \ q \geq k\}$. Ist $K$ sogar vollständig angeordnet, entspricht umgekehrt jedem Dedekindschen Schnitt $(A, B)$ ein eindeutiges $k \in K$ mit $(A, B) = (A_k, B_k)$. Sei $\varphi\colon \mathbb{Q} \to \mathbb{Q}_K$ der Körperisomorphismus aus Aufgabe 3.5.3.8. Aus unseren Überlegungen folgt, dass sich $\varphi$ zu einem eindeutigen Isomorphismus zwischen den vollständig angeordneten Körpern $\mathbb{R}$ und $K$ fortsetzen lässt. Damit haben wir im Wesentlichen folgenden wichtigen Satz bewiesen, der die ausgezeichnete Rolle der reellen Zahlen (sowohl als System als auch auf jede einzelne reelle Zahl bezogen) zum Ausdruck bringt.

**Satz 3.5.3.11.** *Ist $K$ ein archimedisch angeordneter Körper, so gibt es eine eindeutige isomorphe Einbettung $\varphi\colon K \to \mathbb{R}$ (als angeordneter Körper). Ist $K$ vollständig, so ist $\varphi$ sogar surjektiv, also ein Isomorphismus.*

**UE 220** ► **Übungsaufgabe 3.5.3.12.** (V) Rekapitulieren Sie den Beweis von Satz 3.5.3.11 und führen Sie allfällige bisher nur knapp dargestellte Argumente sorgfältig aus. ◄ **UE 220**

Bemerkenswerterweise muss man für die Eindeutigkeit des Isomorphismus $\varphi\colon K_1 \to K_2$ zwischen zwei vollständig angeordneten Körpern nicht einmal die Verträglichkeit mit der Ordnungsstruktur verlangen. Denn in diesem Fall ist jeder algebraische Isomorphismus automatisch auch ein Ordnungsisomorphismus. Das ergibt sich aus der folgenden Übungsaufgabe.

**UE 221** ► **Übungsaufgabe 3.5.3.13.** (V) Seien $K, K_1, K_2$ angeordnete Körper. Zeigen Sie: ◄ **UE 221**

1. Für $x \in K$ gilt stets $x^2 \geq 0$ (Quadrate sind nichtnegativ).

2. Ist $K$ sogar vollständig angeordnet, so ist umgekehrt jedes nichtnegative Element ein Quadrat.

3. Ist $K_1$ vollständig angeordnet, so bildet jeder algebraische Isomorphismus $\varphi\colon K_1 \to K_2$ positive Elemente auf positive ab, negative auf negative.

4. Sei die Abbildung $\varphi\colon K_1 \to K_2$ verträglich mit der Addition (d.h. $\varphi(a + b) = \varphi(a) + \varphi(b)$ für alle $a, b \in K_1$). Außerdem sei $\varphi(a) \geq 0$ für alle $a \geq 0$. Dann ist $\varphi$ monoton, d.h. aus $a \leq b \in K_1$ folgt stets $\varphi(a) \leq \varphi(b)$.

5. Die folgende Aussage ist nur mit Hilfe der ersten vier Teile dieser Übung zu beweisen, aber ohne Zuhilfenahme von Satz 3.5.3.11: Sind $K_1$ und $K_2$ vollständig angeordnete Körper, so gibt es genau einen algebraischen Isomorphismus $\varphi\colon K_1 \to K_2$. Dieses $\varphi$ ist auch ein ordnungstheoretischer Isomorphismus. Insbesondere besitzt jeder vollständig angeordnete Körper nur einen einzigen algebraischen Automorphismus, nämlich die Identität.

**Folgerung 3.5.3.14.** *Jeder vollständig angeordnete Körper $K$ ist als angeordneter Körper zu $\mathbb{R}$ isomorph. Der Isomorphismus ist sogar als algebraischer Isomorphismus eindeutig bestimmt. Insbesondere ist die Identität der einzige Automorphismus des Körpers $\mathbb{R}$.*

Diese Eindeutigkeitsaussagen rechtfertigen, dass man, obwohl formal nicht ganz präzise, schlicht von *den reellen Zahlen* sprechen kann, wenn von irgendeinem vollständig angeordneten Körper die Rede ist. Ebenso kann man die übliche Darstellung reeller Zahlen mit Hilfe unendlicher (meist dekadischer) Ziffernfolgen für die Elemente eines beliebigen vollständig angeordneten Körpers verwenden. Man beachte, dass es wegen der Überabzählbarkeit von $\mathbb{R}$ grundsätzlich unumgänglich ist, unendliche Symbolketten zur Darstellung reeller Zahlen zuzulassen. Denn über einer endlichen (oder auch abzählbar unendlichen) Menge von Symbolen gibt es nur abzählbar viele endliche Ketten (oder auch Konfigurationen in einem weiteren Sinne).

**UE 222** ► **Übungsaufgabe 3.5.3.15.** (E) Rekapitulieren Sie die Darstellung reeller Zahlen als unendliche Dezimalbrüche. Gehen Sie dabei folgendermaßen vor. ◄ **UE 222**

1. Definieren Sie eine fast (in welchem Sinne?) bijektive Abbildung $\varphi$ zwischen gewissen Symbolketten und den Elementen von $\mathbb{R}$ (gemäß einer Konstruktion Ihrer Wahl).
2. Geben Sie an, auf welcher maximalen Menge die Abbildung $\varphi$ aus Teil 1 bijektiv ist und wo nicht.
3. Beweisen Sie Ihre Behauptungen aus 2.
4. Welche Probleme treten bei der Suche nach Algorithmen für die Grundrechnungsarten reeller Zahlen auf? Welche Auswege schlagen Sie vor? (Hinweis: Denken Sie etwa an die Addition $\frac{2}{3} + \frac{1}{3}$ oder an die Multiplikation $\sqrt{2} \cdot \sqrt{2}$ in Dezimaldarstellung.)

**UE 223** ► **Übungsaufgabe 3.5.3.16.** (E) Zeigen Sie die Überabzählbarkeit[24] von $\mathbb{R}$ auf mehrere Arten: ◄ **UE 223**

1. Unter Verwendung der Zifferndarstellung.
2. Indem Sie zeigen, dass die Potenzmenge einer Menge $M$ echt größer ist als $M$ selbst, und dass die Potenzmenge von $\mathbb{N}$ injektiv nach $\mathbb{R}$ abgebildet werden kann.
3. Indem Sie explizit die Vollständigkeit von $\mathbb{R}$ verwenden: Für jede beliebige Abbildung $f\colon \mathbb{N} \to \mathbb{R}$ können wir ausgehend von der Folge der Werte $f(0), f(1), \ldots$ eine konvergente Folge konstruieren, die gegen ein $r$ konvergiert, das von allen $f(n)$ verschieden ist. Dieses $r$ liegt dann nicht im Wertebereich von $f$.

[24] Definitionsgemäß heißt eine unendliche Menge $M$ überabzählbar, wenn es keine bijektive Abbildung von $M$ nach $\mathbb{N}$ gibt; äquivalent dazu: $M$ ist nicht leer, und es gibt keine surjektive Abbildung von $\mathbb{N}$ nach $M$. Weiters äquivalent: Es gibt keine injektive Abbildung von $M$ nach $\mathbb{N}$.

Zum Abschluss sei noch kurz auf Beispiele nichtarchimedisch angeordneter Körper eingegangen. Das einfachste ergibt sich fast von selbst aus der folgenden (etwas lückenhaften) Überlegung: Ist $K$ ein angeordneter Körper, so ist $\mathrm{char}(K) = 0$. Also ist der Primkörper $\mathbb{Q}_K$ zum archimedisch angeordneten Körper $\mathbb{Q}$ isomorph (siehe auch Übungsaufgabe 3.5.3.8). Wenn $K$ nicht archimedisch angeordnet ist, muss es folglich Elemente $x \notin \mathbb{Q}_K$ geben. Soll $K$ nicht archimedisch angeordnet sein, so muss es (warum genau?) auch solche geben, die größer als alle rationalen Elemente sind. Halten wir solch ein $x$ mit $x > q$ für alle $q \in \mathbb{Q}_K$ fest. Dann muss auch $x < x^2 < x^3 < \ldots$ gelten, ganz analog zum asymptotischen Verhalten von Polynomen und auch gebrochen rationalen Funktionen $q(x)$ über $\mathbb{Q}$ für $x \to \infty$. Der Körper der gebrochen rationalen Funktionen kann tatsächlich auf diese Weise zu einem nichtarchimedisch angeordneten gemacht werden, der sich überdies in jeden anderen nichtarchimedisch angeordneten Körper einbetten lässt:

**Theorem 3.5.3.17.** Auf dem Körper $\mathbb{Q}(x)$ der gebrochen rationalen Funktionen sei eine Relation $<$ definiert durch $q_1(x) \leq q_2(x)$, falls $q_1 = q_2$ oder es ein $r_0 > 0$ gibt mit $q_1(r) < q_2(r)$ (in $\mathbb{R}$) für alle $r > r_0$. Zeigen Sie:

1. Die so definierte Relation $\leq$ macht $Q(x)$ zu einem nichtarchimedisch angeordneten Körper.
2. $Q(x)$ lässt sich als angeordneter Körper in jeden anderen nichtarchimedisch angeordneten Körper isomorph einbetten.

**UE 224 ► Übungsaufgabe 3.5.3.18.** (B) Beweisen Sie Theorem 3.5.3.17. **◄ UE 224**

Eine besondere Rolle spielen nichtarchimedisch angeordnete Körper als sogenannte Nonstandard-Modelle von $\mathbb{R}$. Obwohl sie zum Körper der reellen Zahlen natürlich nicht isomorph sein können haben Sie dieselbe Theorie erster Ordnung. Ihre Konstruktion ist in höchstem Maße nichtkonstruktiv und verwendet typischerweise Ultrafilter bzw. Ultraprodukte. Darauf einzugehen würde hier zu weit führen. Dennoch folgen einige Bemerkungen in diese Richtung.

### 3.5.4 Modelltheoretische Bemerkungen

Inhalt in Kurzfassung: Andeutungen in Richtung Logik und Entscheidbarkeit der Theorie reell abgeschlossener Körper.

Sei $K$ ein Unterkörper von $\mathbb{C}$. Wir nennen eine reelle oder komplexe Zahl $a$ *algebraisch* über $K$, wenn sie Nullstelle eines Polynoms $\sum_{k=1}^{n} a_n x^n \in K[x] \setminus \{0\}$ mit Koeffizienten in $K$ ist. Statt „algebraisch über $\mathbb{Q}$“ sagen wir oft nur „algebraisch“; die Menge aller algebraischen Zahlen $z \in \mathbb{C}$ bezeichnen wir mit $\mathbb{A}$.
Wir werden später beweisen, dass die Menge aller algebraischen Zahlen über $K$ selbst einen Körper bildet; insbesondere sind also die Mengen $\mathbb{A}$ und $\mathbb{A} \cap \mathbb{R}$ Unterkörper von $\mathbb{C}$. Ohne Beweis führen wir den folgenden Satz an, der weitere Abschlusseigenschaften der Mengen $\mathbb{A}$ und $\mathbb{A} \cap \mathbb{R}$ angibt.

**Satz 3.5.4.1.** (1) *Die Mengen $\mathbb{A}$ und $\mathbb{A} \cap \mathbb{R}$ sind abzählbare Körper.*

(2) *$\mathbb{A} \cap \mathbb{R}$ ist archimedisch angeordnet.*

(3) *Sei $p(x) \neq 0$ ein Polynom mit Koeffizienten in $\mathbb{A}$. Dann liegen alle Nullstellen von $p(x)$ auch in $\mathbb{A}$. (Wir sagen, dass $\mathbb{A}$ „algebraisch abgeschlossen“ ist.)*

(4) *Sei $\varphi(x_1, \ldots, x_n)$ eine beliebige Aussage in der Logik erster Stufe in der Sprache der Körper. Wenn $a_1, \ldots, a_n$ in $\mathbb{A}$ liegen, und in $\mathbb{C}$ die Aussage $\varphi(a_1, \ldots, a_n)$ gilt, dann gilt auch in $\mathbb{A}$ diese Aussage.*
*(Ein Spezialfall: Wenn $\varphi(a_1, \ldots, a_n)$ die Aussage „das Polynom mit den Koeffizienten $a_1, \ldots, a_n$ hat eine Nullstelle“ ist, dann ergibt sich ein Spezialfall des vorigen Punktes: jedes nichtkonstante Polynom mit algebraischen Koeffizienten hat eine Nullstelle in $\mathbb{A}$.*

(5) *Sei $p(x) \neq 0$ Polynom mit Koeffizienten in $\mathbb{A} \cap \mathbb{R}$. Dann liegen alle reellen Nullstellen von $p(x)$ auch in $\mathbb{A} \cap \mathbb{R}$. ($\mathbb{A} \cap \mathbb{R}$ ist „reell abgeschlossen“) (Eine äquivalente Definition des Begriffs „reell abgeschlossen“ finden Sie auf Seite 78.)*

(6) *Sei $\varphi(x_1, \ldots, x_n)$ eine beliebige Aussage in der Logik erster Stufe in der Sprache der angeordneten Körper. Wenn $r_1, \ldots, r_n$ in $\mathbb{A} \cap \mathbb{R}$ liegen, und in $\mathbb{C}$ die Aussage $\varphi(r_1, \ldots, r_n)$ gilt, dann gilt auch in $\mathbb{A} \cap \mathbb{R}$ diese Aussage.*

(7) *Zu jeder Formel $\varphi(x_1, \ldots, x_n)$ in der Sprache der Körper gibt es eine quantorenfreie Aussage $\varphi'(x_1, \ldots, x_n)$ in dieser Sprache, sodass in jedem algebraisch abgeschlossenen Körper $K$ die Formeln $\varphi$ und $\varphi'$ äquivalent sind, d.h.*
*$\forall x_1 \ldots \forall x_n : \varphi(x_1, \ldots, x_n) \Leftrightarrow \varphi'(x_1, \ldots, x_n)$ gilt. („Quantorenelimination“)*

(8) *Zu jeder Formel $\varphi(x_1, \ldots, x_n)$ in der Sprache der angeordneten Körper gibt es eine quantorenfreie Aussage $\varphi'(x_1, \ldots, x_n)$ in dieser Sprache, sodass in jedem algebraisch abgeschlossenen Körper $K$ die Formeln $\varphi$ und $\varphi'$ äquivalent sind, d.h.*
*$\forall x_1 \ldots \forall x_n : \varphi(x_1, \ldots, x_n) \Leftrightarrow \varphi'(x_1, \ldots, x_n)$ gilt.*

## 3.6 Verbände und Boolesche Algebren

Im Vergleich zu den bisher untersuchten klassischen algebraischen Strukturen spielen Verbände eine deutlich andere Rolle. Das liegt zu einem guten Teil an ihrem ordnungstheoretischen Charakter. Dieser zeigt sich an elementaren Eigenschaften (3.6.1), an ihren Unter- (3.6.2) und Faktorstrukturen (3.6.3) wie auch an der besonderen Rolle der vollständigen Verbände (3.6.4). Interessante Untervarietäten bilden distributive wie auch modulare Verbände (3.6.5). Besonders wichtig sind Boolesche Algebren, die sich wiederum sogar als spezielle (kommutative) Ringe, sogenannte Boolesche Ringe auffassen lassen (3.6.6). Nach der Behandlung von Atomen (3.6.7) schließt der Abschnitt in (3.6.8) mit dem wichtigsten Ergebnis dieses Abschnitts, dem Stoneschen Darstellungssatz. Ihm zufolge ist jede Boolesche Algebra isomorph zu einer Mengenalgebra.

### 3.6.1 Elementare Eigenschaften

Inhalt in Kurzfassung: Einfachste Begriffe, Rechenregeln und Beispiele zu Verbänden.

Ist $(V, \wedge, \vee)$ ein Verband, so wegen der Symmetrie der Verbandsgesetze auch $(V, \vee, \wedge)$. Wenn wir den Verband $(V, \wedge, \vee)$ kurz auch mit $V$ bezeichnen, so nennen wir den Verband $(V, \vee, \wedge)$ den zu $V$ dualen Verband und bezeichnen ihn mit $V^d$.
Zu jeder Aussage $\varphi$ über Verbände (im ordnungstheoretischen oder auch im algebraischen Sinn) definieren wir eine Aussage $\varphi^d$, die „duale“ Aussage, so: Wir ersetzen in $\varphi$ das Symbol $\wedge$ durch $\vee$, $\vee$ durch $\wedge$, $\leq$ durch $\geq$. (Alle weiteren verbandstheoretischen Konzepte müssen natürlich ebenfalls durch die dualen ersetzt werden – „minimal“ durch „maximal“, inf durch sup, etc.)
Wenn nun die Aussage $\varphi$ für den Verband $V$ zutrifft (z.B.: „$V$ hat ein größtes Element“), dann trifft die Aussage $\varphi^d$ auf den Verband $V^d$ zu (z.B.: „$V^d$ hat ein kleinstes Element“). Wenn eine Aussage $\varphi$ auf alle Verbände zutrifft, dann trifft auch $\varphi^d$ auf alle Verbände zu.[25] Man nennt dies das *Dualitätsprinzip für Verbände.*

**Satz 3.6.1.1** (Rechenregeln für Verbände)**.** (1) *Die Operationen $\vee$ und $\wedge$ sind monoton. Das heißt, aus $a_1 \leq a_2$ und $b_1 \leq b_2$ folgt $a_1 \wedge b_1 \leq a_2 \wedge b_2$ und $a_1 \vee b_1 \leq a_2 \vee b_2$.*

(2) *$a \leq b \wedge c \Leftrightarrow a \leq b$ und $a \leq c$.*

(3) *$a \geq b \vee c \Leftrightarrow a \geq b$ und $a \geq c$.*

*Beweis.* (1) ist ein Übungsbeispiel. (2) gilt, weil $b \wedge c$ die *größte* untere Schranke für $b$ und $c$ ist. (3) ist zu (2) dual. □

Wir sammeln einige Beispiele von Verbänden und spezielleren Strukturen (siehe Definition 2.1.3.6 sowie Definition 2.1.4.3).

**Proposition 3.6.1.2.** *Jede totalgeordnete Menge ist ein distributiver Verband.*

**UE 225 ► Übungsaufgabe 3.6.1.3.** (F+) Beweisen Sie Proposition 3.6.1.2. **◄ UE 225**

**UE 226 ► Übungsaufgabe 3.6.1.4.** (F) Zeigen Sie: **◄ UE 226**

(1) $(\mathfrak{P}(M), \cap, \cup)$ ist ein Verband und als solcher sogar distributiv.

(2) $(\mathfrak{P}(M), \cap, \cup, \emptyset, M)$ ist ein Verband mit Null- und Einselement.

(3) $(\mathfrak{P}(M), \cap, \cup, \emptyset, M)$ ist ein komplementärer Verband, wobei für $A \subseteq M$ das (eindeutig bestimmte) Komplement durch $A' = M \setminus A$ gegeben ist.

(4) $(\mathfrak{P}(M), \cap, \cup, \emptyset, M, ')$ ist eine Boolesche Algebra (und somit auch ein Boolescher Verband).

[25] Achtung: Es kann natürlich vorkommen, dass zwar $\varphi$ nur auf einen bestimmten Verband $L$ zutrifft, nicht aber $\varphi^d$.

(5) Sei $V$ Vektorraum über einem Körper $K$, und sei $P$ die Menge aller Unterräume von $V$. Für beliebige Unterräume $U_1, U_2 \leq V$ ist auch $U_1 \wedge U_2 := U_1 \cap U_2$ ein Unterraum, ebenso die Menge $U_1 \vee U_2 := [U_1 \cup U_2]$ (die lineare Hülle der Vereinigung der beiden Räume).

Dann ist $(P, \wedge, \vee)$ ein komplementärer Verband. Wenn $V$ mindestens 2-dimensional ist, dann ist $P$ nicht distributiv, und Komplemente sind nicht eindeutig bestimmt.

**UE 227** ► **Übungsaufgabe 3.6.1.5.** (F+) Zeigen Sie: Ist $(V, \wedge, \vee, 0, 1)$ ein beschränkter distributiver Verband, so gibt es zu jedem $a \in V$ höchstens ein Komplement. Was folgt daraus über die Beziehung zwischen Booleschen Algebren und Booleschen Verbänden? ◄ **UE 227**

### 3.6.2 Unterverbände

Inhalt in Kurzfassung: Der Begriff des Unterverbandes fügt sich nahtlos in das allgemeinere Konzept der Unteralgebra ein.

Sei $(V, \wedge, \vee)$ ein Verband. Ein *Unterverband* ist eine Teilmenge von $V$, die unter $\wedge$ und $\vee$ abgeschlossen ist.

**Beispiel 3.6.2.1.** Sei $(V, \wedge, \vee)$ ein Verband und sei $\leq$ die zugehörige Ordnung. Wenn $K \subseteq V$ eine Kette in $(V, \leq)$ ist, dann ist $K$ Unterverband von $V$. Insbesondere ist jede einelementige Teilmenge ein Unterverband, ebenso die leere Menge.

**Anmerkung 3.6.2.2.** Sei $V$ Verband mit den Operationen $\wedge$ und $\vee$ und der Ordnung $\leq$. Sei $W$ ein Unterverband; die Operationen von $W$ sind dann die Einschränkungen von $\wedge$ und $\vee$ auf die Menge $W \times W$; wir schreiben wie bisher aber meist $\wedge$ und $\vee$ (oder gelegentlich $\wedge_W$ und $\vee_W$) für diese Operationen, statt genauer $\wedge\restriction(W \times W)$ und $\vee\restriction(W \times W)$ zu schreiben.
Die partielle Ordnung von $W$ ist die Einschränkung von $\leq$ auf die Menge $W$, d.h. formal: die Menge $\{(x, y) \in W \times W \mid x \leq y\}$, oder kürzer $\leq \cap (W \times W)$; wir schreiben $\leq$ oder $\leq_W$ für diese Relation. Die Struktur $(W, \leq)$ ist ein verbandsgeordnete Menge.

**UE 228** ► **Übungsaufgabe 3.6.2.3.** (B) Geben Sie einen Verband $(V, \wedge, \vee)$ (mit zugehöriger Ordnungsrelation $\leq$) sowie zwei Untermengen $S_1, S_2 \subseteq V$ an, sodass $S_1$ ein Unterverband von $V$ ist, $S_2$ hingegen nicht, aber die partiellen Ordnungen $(S_1, \leq)$ und $(S_2, \leq)$ isomorph sind.
(Hinweis: Der kleinste solche Verband hat 5 Elemente.) ◄ **UE 228**

### 3.6.3 Kongruenzrelationen; Filter und Ideale

Inhalt in Kurzfassung: Kongruenzrelationen auf Verbänden haben auch ordnungstheoretisch interessante Eigenschaften. So sind die Kongruenzklassen stets konvexe Unterverbände. Eine besondere Rolle spielen Filter und noch spezieller Primfilter und maximale

Filter (Ultrafilter). Dual zu Filtern definiert man Ideale (im ordnungs- oder verbandstheoretischen Sinn), Primideale und maximale Ideale.

**Lemma 3.6.3.1.** *Seien $(V_1, \wedge_1, \vee_1)$ und $(V_2, \wedge_2, \vee_2)$ Verbände mit den zugehörigen Ordnungen $\leq_1$, $\leq_2$, und sei $f\colon V_1 \to V_2$ ein Verbandshomomorphismus.*
*Dann erhält $f$ die Ordnung, d.h.: $x \leq_1 y \Rightarrow f(x) \leq_2 f(y)$ für alle $x, y \in V_1$.*

*Beweis.* Wenn $x \leq_1 y$, dann $x \wedge y = x$. Daher $f(x) \wedge f(y) = f(x \wedge y) = f(x)$, also $f(x) \leq_2 f(y)$. □

Eine Kongruenzrelation ist eine Äquivalenzrelation $\theta \subseteq V \times V$, die mit den Operationen $\wedge$ und $\vee$ verträglich ist:

$$a_1 \theta a_2, b_1 \theta b_2 \Rightarrow (a_1 \vee b_1)\theta(a_2 \vee b_2),\ (a_1 \wedge b_1)\theta(a_2 \wedge b_2).$$

Aus dem allgemeinen Homomorphiesatz folgt, dass für jeden surjektiven Verbandshomomorphismus $f\colon V \to W$ die Relation $\{(x, y) \mid f(x) = f(y)\}$ eine Kongruenzrelation ist, und dass alle Kongruenzrelationen diese Form haben.
Es ist nicht immer leicht, festzustellen, ob eine vorliegende Partition tatsächlich von einer Kongruenzrelation kommt. Das folgende Konzept kann manchmal hilfreich sein:

**Definition 3.6.3.2.** Sei $(L, \leq)$ eine partielle Ordnung.

- Für $a \leq b$ in $L$ definieren wir das *Intervall* $[a, b]$ oder ausführlicher $[a, b]_L$ durch $[a, b] := \{x \in L \mid a \leq x \leq b\}$.
- Eine Teilmenge $A \subseteq L$ heißt *konvex*, wenn $\forall a, b \in A : a < b \Rightarrow [a, b]_L \subseteq A$ gilt.

**Lemma 3.6.3.3.** *Sei $\theta$ eine Kongruenzrelation auf einem Verband $(V, \wedge, \vee)$. Dann ist jede Kongruenzklasse eine konvexe Menge, und jede Kongruenzklasse ist Unterverband von $V$.*

*Beweis.* Sei $f\colon (V, \wedge, \vee) \to (W, \wedge, \vee)$ ein Homomorphismus, mit Kern $\theta$. Jede Klasse $[v]_\theta$ ist von der Form $f^{-1}(w)$ für ein $w \in W$ (nämlich $w := f(v)$).

- Konvexität: Sei $a \leq x \leq b$ mit $f(a) = f(b)$. Zu zeigen ist $f(a) = f(x)$.
  Aus Lemma 3.6.3.3 wissen wir $f(a) \leq f(x) \leq f(b) = f(a)$. Daher $f(a) = f(x)$.
- Unterverband: Seien $v_1, v_2$ in der selben Äquivalenzklasse, d.h. $f(v_1) = f(v_2) =: w$. Dann ist $f(v_1 \vee v_2) = w \vee w = w$, also ist $v_1 \vee v_2$ in derselben Klasse. Daher ist jede Klasse unter $\vee$ abgeschlossen; dual auch unter $\wedge$. □

**Anmerkung 3.6.3.4.** Nicht jede Äquivalenzrelation, deren Klassen konvexe Unterverbände sind, ist eine Kongruenzrelation.

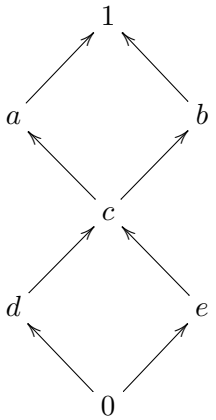
**UE 229 ▶ Übungsaufgabe 3.6.3.5.** (F) Finden Sie auf dem Verband $\mathfrak{P}(\{1, 2\})$ **◀ UE 229**

- ... alle Kongruenzrelationen.

- ... alle Partitionen, deren Klassen konvexe Unterverbände sind.

**UE 230 ► Übungsaufgabe 3.6.3.6.** (B) **◄ UE 230**

Sei $(V, \wedge, \vee)$ der durch das nebenstehende Diagramm gegebene Verband.
Finden Sie alle Kongruenzrelationen von $V$; geben Sie für jede dieser Kongruenzrelationen $\theta$ einen surjektiven Homomorphismus auf einen Verband $V_\theta$ an, und beschreiben Sie $V_\theta$ durch sein Hasse-Diagramm.




**Definition 3.6.3.7.** Sei $(V, \leq)$ ein Verband, und sei $\emptyset \neq A \subseteq V$.

- Die Menge $A$ heißt *Filter*, wenn $A$ unter $\wedge$ und nach oben abgeschlossen ist: $x, y \in A \Rightarrow x \wedge y \in A$ und $x \in A, a \in V, a \geq x \Rightarrow a \in A$.
- Dual dazu: Die Menge $A$ heißt *Ideal*, wenn $A$ unter $\vee$ und nach unten abgeschlossen ist: $x, y \in A \Rightarrow x \vee y \in A$ und $x \in A, a \in V, a \leq x \Rightarrow a \in A$.
- Ein Filter $F \subsetneq V$ heißt *Primfilter*, wenn

$$\forall x, y \in V : x \vee y \in F \Rightarrow x \in F \text{ oder } y \in F,$$

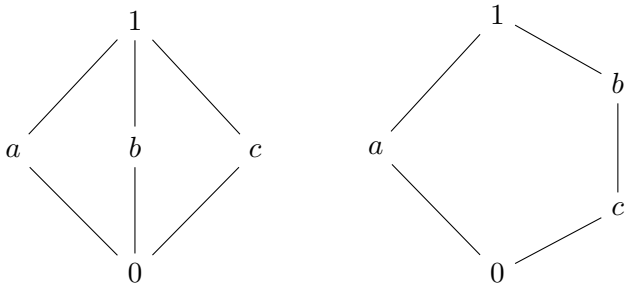
  oder äquivalent, wenn $V \setminus F$ ein Ideal ist.
- Ein Ideal $I \subsetneq V$ heißt *Primideal*, wenn $V \setminus I$ ein Filter ist.
- Ein Filter $F \subsetneq V$ heißt *maximaler Filter*, wenn es außer $V$ selbst keine Obermenge von $F$ gibt, die ein Filter ist.

Die leere Menge ist weder Ideal noch Filter. Der ganze Verband $V$ gilt als *uneigentliches Ideal* bzw. als *uneigentlicher Filter*. Maximale Filter sind maximale Elemente in der durch $\subseteq$ gegebenen partiellen Ordnung aller eigentlichen Filter.

**UE 231 ► Übungsaufgabe 3.6.3.8.** (F) Sei $V$ Verband, $F \subsetneq V$ ein Filter. Dann ist $F$ genau dann maximal, wenn für alle $x \in V \setminus F$ gilt: Für alle $v \in V$ gibt es ein $f \in F$ mit $x \wedge f \leq v$. **◄ UE 231**

**UE 232 ► Übungsaufgabe 3.6.3.9.** (B) Finden Sie im Verband $(\{0, 1, 2, 3\}, \min, \max)$ alle echten Filter, alle maximalen Filter und alle Primfilter. **◄ UE 232**

**Definition 3.6.3.10.** Mit $M_3$ bezeichnen wir jenen 5-elementigen Verband, der neben seinem kleinsten Element 0 und dem größten Element 1 noch 3 paarweise unvergleichbare Elemente enthält. Der Verband $N_5$ hat ebenfalls 5 Elemente; neben 0 und 1 enthält er 3 Elemente, von denen zwei vergleichbar sind.




**UE 233** ► **Übungsaufgabe 3.6.3.11.** (B) Finden Sie alle Primfilter und alle maximalen Filter auf $M_3$ und $N_5$. ◄ **UE 233**

**UE 234** ► **Übungsaufgabe 3.6.3.12.** (F) Seien $V_1$ und $V_2$ Verbände, und sei $F_2$ ein Filter auf $V_2$. Sei $f : V_1 \to V_2$ surjektiver Homomorphismus. Dann ist $f^{-1}(F_2)$ Filter auf $V_1$. Insbesondere ist das Urbild der 1 in $F_2$ (sofern vorhanden) ein Filter in $V_1$. ◄ **UE 234**

### 3.6.4 Vollständige Verbände

Inhalt in Kurzfassung: Wiederholung des Begriffs des vollständigen Verbands, hauptsächlich in Form von Übungsaufgaben.

**Definition 3.6.4.1.** Eine partielle Ordnung $(P, \leq)$ heißt *vollständig*, wenn jede Teilmenge $S \subseteq P$ ein Supremum und ein Infimum hat. (Statt $\sup S$ und $\inf S$ schreibt man manchmal auch $\bigvee S$ und $\bigwedge S$.) Wir nennen einen Verband $(L, \wedge, \vee)$ vollständig, wenn $L$ mit der Verbandsordnung vollständig ist.

Insbesondere ist jede vollständige partielle Ordnung eine verbandsgeordnete Menge, kann also als vollständiger Verband aufgefasst werden.

**Anmerkung 3.6.4.2.** Die reellen Zahlen $\mathbb{R}$ mit der üblichen Ordnung sind im Sinne dieser Definition also nicht vollständig, die Erweiterung $\mathbb{R} \cup \{-\infty, \infty\}$ um ein kleinstes Element $-\infty$ und ein größtes Element $\infty$ hingegen schon. Wir nennen eine Halbordnung *bedingt vollständig*[26], wenn jede nichtleere nach oben beschränkte Menge ein Supremum und jede nichtleere nach unten beschränkte Menge ein Infimum hat. Eine bedingt vollständige Halbordnung wird durch Adjunktion von zwei neuen Elementen $\infty$ und $-\infty$

[26] englisch: *conditionally complete*

zu einer vollständigen Halbordnung, daher kann man alle Sätze über vollständige Halbordnungen in Sätze über bedingt vollständige Halbordnungen übersetzen. Die Familie aller endlichen Teilmengen von $\mathbb{N}$ ist ein weiters Beispiel eines bedingt vollständigen Verbandes, der nicht vollständig ist.
Achtung! Manche Autoren verwenden die Bezeichnung *vollständig* für die Eigenschaft, die wir an dieser Stelle *bedingt vollständig* nennen – auch wir haben im Zusammenhang mit vollständig angeordneten Körpern diese Unsauberkeit im Interesse der besseren Lesbarkeit in Kauf genommen, siehe Fußnote auf Seite 58.

**UE 235** ► **Übungsaufgabe 3.6.4.3.** (F) Ist jede bedingt vollständige Halbordnung ein Verband? ◄ **UE 235**

Aus Proposition 2.1.2.17 wissen wir: Wenn $(P, \leq)$ eine Halbordnung ist, in der jede Teilmenge ein Infimum hat, dann hat auch jede Teilmenge von $P$ ein Supremum. Insbesondere liegt ein vollständiger Verband vor.

**UE 236** ► **Übungsaufgabe 3.6.4.4.** (F) Man formuliere die duale Aussage und führe einen Beweis unter Verwendung der bereits bewiesenen. ◄ **UE 236**

**UE 237** ► **Übungsaufgabe 3.6.4.5.** (B) Man bestimme das Hasse-Diagramm des Verbandes der Untergruppen der Symmetriegruppe $D_4$ des Quadrats, das ist die Menge der Isometrien $\mathbb{R}^2$, die das Quadrat $\{(1,0),(0,1),(-1,0),(0,-1)\}$ als Menge invariant lassen (also Drehungen und Spiegelungen). ◄ **UE 237**

**UE 238** ► **Übungsaufgabe 3.6.4.6.** (E) Geben Sie einen Verband $L$ an, der zu keinem Verband $\mathrm{Sub}(\mathfrak{A})$ isomorph ist: $\exists L : L$ ist Verband, und $\Big(\forall \mathfrak{A} : \mathfrak{A}$ Algebra $\Rightarrow L \not\cong \mathrm{Sub}(\mathfrak{A})\Big)$.
(Hinweis: Vergleichen Sie mit der Formulierung der nächsten UE-Aufgabe.) ◄ **UE 238**

**UE 239** ► **Übungsaufgabe 3.6.4.7.** (E) Geben Sie einen vollständigen Verband $L$ an, der zu keinem Verband $\mathrm{Sub}(A)$ isomorph ist.
(Das ist sehr anspruchsvoll. Hinweis: Recherchieren Sie den Begriff des *algebraischen Verbandes*.) ◄ **UE 239**

**UE 240** ► **Übungsaufgabe 3.6.4.8.** (D) Man gebe weitere Beispiele von vollständigen Verbänden an, die in der Mathematik eine wichtige Rolle spielen. ◄ **UE 240**

**UE 241** ► **Übungsaufgabe 3.6.4.9.** (E) Sei $L$ ein beliebiger Verband. Dann gibt es einen vollständigen Verband $V$ und einen injektiven Verbandshomomorphismus $f : L \to V$. (Der Verband $V$ ist eine Art „Vervollständigung“ von $L$.)
Hinweis: OBdA (warum?) hat $L$ ein kleinstes Element. Sei $V$ die Menge aller Ideale von $L$; dann bildet $(V, \subseteq)$ einen vollständigen Verband (warum?), in den man $L$ einbetten kann (wie?). ◄ **UE 241**

**UE 242** ► **Übungsaufgabe 3.6.4.10.** (B) Sei $P$ die Familie aller höchstens abzählbaren Teilmengen $M \subseteq \mathbb{R}$, zusammen mit $\mathbb{R}$ selbst, geordnet durch $\subseteq$:

$$P := \{A \subseteq \mathbb{R} \mid A \text{ abzählbar unendlich}\} \cup \{A \subseteq \mathbb{R} \mid A \text{ endlich}\} \cup \{\mathbb{R}\}.$$

Ist $(P, \subseteq)$ ein vollständiger Verband? ◄ **UE 242**

**UE 243** ► **Übungsaufgabe 3.6.4.11.** (E) Geben Sie einen beschränkten Verband an, in dem jede abzählbare Menge eine kleinste obere Schranke hat, der aber nicht $\sigma$-vollständig[27] ist.
(Hinweis: modifizieren Sie Aufgabe 3.6.4.10.) ◄ **UE 243**

### 3.6.5 Distributive und modulare Verbände

Inhalt in Kurzfassung: Eine wichtige Abschwächung der Distributivität von Verbänden ist die Modularität. Es folgen die Definitionen mit Übungen sowie Charakterisierungen durch die Nichtexistenz gewisser Unterverbände.

Eine Verschärfung des Begriffs des Verbands bilden die distributiven und die sogenannten *modularen* Verbände. Zur Einstimmung einige Ungleichungen, die in beliebigen Verbänden gelten:

**Lemma 3.6.5.1.** *In einem Verband $(V, \wedge, \vee)$ gelten stets die folgenden Aussagen:*

1. $\forall x, y, z \in V : x \leq z \Rightarrow x \vee (y \wedge z) \leq (x \vee y) \wedge z$
2. $\forall x, y, z \in V : x \vee (y \wedge (x \vee z)) \leq (x \vee y) \wedge (x \vee z)$
3. $\forall x, y, z \in V : x \wedge (y \vee z) \geq (x \wedge y) \vee (x \wedge z)$

3'. $\forall x, y, z \in V : x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$

4. $\forall x, y, z \in V : (x \wedge y) \vee (y \wedge z) \vee (z \wedge x) \leq (x \vee y) \wedge (y \vee z) \wedge (z \vee x)$

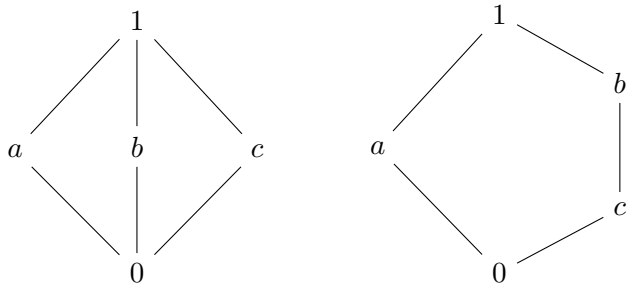
**UE 244** ► **Übungsaufgabe 3.6.5.2.** (V) Beweisen Sie Lemma 3.6.5.1. ◄ **UE 244**

[27] Ein Verband $L$ heiße $\sigma$-vollständig, wenn jede abzählbar unendliche Teilmenge von $L$ eine kleinste obere und eine größte untere Schranke hat.

Die erste Aussage gibt Anlass zur folgenden Definition:

**Definition 3.6.5.3.** Ein Verband $(V, \wedge, \vee)$ heißt modular, wenn für alle $x, y, z \in V$ aus $x \leq z$ stets $x \vee (y \wedge z) = (x \vee y) \wedge z$ folgt.

Wichtige Beispiele modularer Verbände sind – wie man leicht nachprüft – Totalordnungen $(P, \min, \max)$, Potenzmengenverbände $(\mathfrak{P}(M), \cap, \cup)$ oder auch der Verband $M_3$ aus Definition 3.6.3.10. Kein modularer Verband ist $N_5$, wie man unmittelbar erkennt, wenn man $x = c$, $y = a$ und $z = b$ setzt[28].




Weitere Beispiele und Nicht-Beispiele ergeben sich aus den folgenden Übungsaufgaben:

**UE 245 ▶ Übungsaufgabe 3.6.5.4.** (E) Man zeige: **◀ UE 245**

1. Der Verband der Normalteiler einer Gruppe ist modular, ebenso der Verband der Ideale in einem Ring.
2. Der Verband der Äquivalenzrelationen auf einer Menge $M$ mit $|M| \geq 4$ ist nicht modular. Geben Sie eine Varietät $\mathcal{V}$ an, sodass nicht alle Strukturen aus $\mathcal{V}$ einen modularen Kongruenzverband haben.

**UE 246 ▶ Übungsaufgabe 3.6.5.5.** (B) Man zeige am Beispiel der alternierenden Gruppe $A_4$, **◀ UE 246**
dass der Untergruppenverband einer Gruppe nicht modular sein muss.

Da die obige Definition eines modularen Verbands kein Gesetz im Sinne von Definition 2.1.8.6 ist (das Problem ist nicht die Ungleichung, die man nämlich auch als $x \wedge z = x$ umformulieren könnte, sondern die Implikation), ist bisher noch nicht klar, ob die modularen Verbände eine Varietät bilden. Dass folgende Lemma zeigt unter anderem, dass dies tatsächlich der Fall ist.

**Lemma 3.6.5.6.** *Sei $(M, \wedge, \vee)$ ein Verband. Dann sind die folgenden Aussagen äquivalent:*

(1) $\forall x, y, z \in M : x \leq z \Rightarrow x \vee (y \wedge z) = (x \vee y) \wedge z$ *(d.h., $M$ ist modular)*

(2) $\forall x, y, z \in M : x \leq z \Rightarrow x \vee (y \wedge z) \geq (x \vee y) \wedge z$

[28] Tatsächlich steht $M_3$ für **m**odular und $N_5$ für **n**ichtmodular.

(3) $\forall x, y, z \in M : x \vee (y \wedge (x \vee z)) = (x \vee y) \wedge (x \vee z)$

(4) $\forall x, y, z \in M : x \vee (y \wedge (x \vee z)) \geq (x \vee y) \wedge (x \vee z)$

*Insbesondere (Aussage (3)) ist die Klasse der modularen Verbände eine Varietät.*

**UE 247 ▶ Übungsaufgabe 3.6.5.7.** (V) Beweisen Sie Lemma 3.6.5.6. **◀ UE 247**

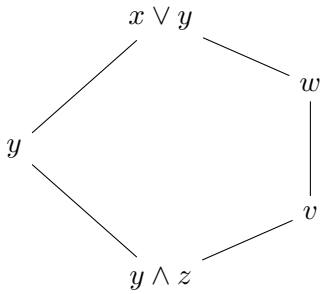
Als wesentliche Aussage über modulare Verbände wollen wir die folgende Charakterisierung beweisen:

**Satz 3.6.5.8.** *Für einen Verband $(M, \wedge, \vee)$ sind die folgenden Bedingungen äquivalent:*

(1) *$M$ ist modular.*

(2) *$M$ besitzt keinen Unterverband, der zum Fünfeck $N_5$ isomorph ist*[29]*.*

*Beweis.* Wir zeigen die Äquivalenz der Negationen. Wenn $M$ einen zu $N_5$ isomorphen Unterverband hat, dann folgt die Nichtmodularität von $M$ genauso wie die Nichtmodularität von $N_5$ – die Tatsache, dass die Kopie von $N_5$ ein Unterverband von $M$ ist, geht dadurch ein, dass dann die sich aus dem Hasse-Diagramm ergebenden Infima und Suprema genau die Ergebnisse der Operationen $\wedge$ und $\vee$ in $M$ sind.
Sei umgekehrt $M$ nicht modular. Nach Lemma 3.6.5.6 bzw. Lemma 3.6.5.1 gibt es $x, y, z \in M$ mit $x \leq z$ und $x \vee (y \wedge z) < (x \vee y) \wedge z$. Jedenfalls muss $x < z$ sein (da im Falle $x = z$ beide Seiten gleich $x$ sind). Wir setzen $v := x \vee (y \wedge z)$ und $w := (x \vee y) \wedge z$ und behaupten, dass die Elemente $y \wedge z$, $y$, $v$, $w$, $x \vee y$ wie abgebildet einen zu $N_5$ isomorphen Unterverband bilden.




Jedenfalls klar ist

$$y \wedge z \leq v < w \leq x \vee y.$$

Wäre $y = y \wedge z$, dann würde der Widerspruch $v < w \leq x \vee y = x \vee (y \wedge z) = v$ folgen. Genauso zeigt man $y \neq x \vee y$ und wir erhalten

$$y \wedge z < v < w < x \vee y.$$

[29] Man beachte: *nicht* als Unterverband mit $0, 1$, d.h. selbst wenn $M$ ein größtes und ein kleinstes Element hat, können das größte bzw. kleinste Element der Kopie von $N_5$ davon verschieden sein.

Als nächstes zeigen wir, dass $y$ mit $v$ bzw. $w$ unvergleichbar ist, indem wir jede der vier Möglichkeiten $v \lessgtr y \lessgtr w$ auf einen Widerspruch führen – daraus folgt dann

$$y \wedge z < y < x \vee y,$$

mit anderen Worten, dass $y \wedge z$, $y$, $v$, $w$, $x \vee y$ eine Kopie von $N_5$ bilden. Wäre $y \geq w$, dann wäre $w = w \wedge y = (x \vee y) \wedge z \wedge y = y \wedge z$ nach der Kommutativität von $\wedge$ und dem Verschmelzungsgesetz. Aus $y \leq w$ würde genauso $y = y \wedge z$ folgen; aus $v \leq y$ analog $y = x \vee y$. Wäre schließlich $v \geq y$, so wären auch $w$ und $y$ vergleichbar. Zu guter Letzt ist zu beweisen, dass $\{y \wedge z, y, v, w, x \vee y\}$ auch ein Unterverband von $M$ ist. Dazu ist noch $y \wedge v = y \wedge w = y \wedge z$ und $y \vee v = y \vee w = x \vee y$ zu zeigen. Dabei ist $y \wedge w = y \wedge z$ und $y \vee v = x \vee y$ durch Einsetzen unmittelbar klar, für $y \wedge v = y \wedge z$ beachten wir $y \wedge z \leq y, v$ und somit $y \wedge z \leq y \wedge v \leq y \wedge w = y \wedge z$. Analog zeigt man auch $y \vee w = x \vee y$. □

Wir beenden die Untersuchungen modularer Verbände mit einigen weiteren Übungsaufgaben.

**UE 248** ► **Übungsaufgabe 3.6.5.9.** (E) Sei $(M, \wedge, \vee)$ modularer Verband, und seien $a, b \in M$. ◄ **UE 248**
Dann sind die Intervalle (siehe 3.6.3.2)

$$[a \wedge b, a] := \{x \in M \mid a \wedge b \leq x \leq a\} \text{ und } [b, a \vee b] := \{x \in M \mid b \leq x \leq a \vee b\}$$

zueinander (verbands)isomorph, und die Abbildung $x \mapsto x \vee b$ ist ein Isomorphismus. Beweisen Sie dies, und geben Sie eine explizite Formel für die Umkehrabbildung an.

**UE 249** ► **Übungsaufgabe 3.6.5.10.** (B) Geben Sie einen nichtmodularen Verband $V$ mit der ◄ **UE 249**
Eigenschaft

$$\forall a, b \in V : [a \wedge b, a] \simeq [b, a \vee b]$$

an. (Hinweis: In der linearen Ordnung der rationalen Zahlen sind alle echten Intervalle $[a, b]$ mit $a < b$ zueinander isomorph.)

**UE 250** ► **Übungsaufgabe 3.6.5.11.** (E) Sei $M$ ein endlicher modularer Verband, und seien ◄ **UE 250**
$K \subseteq M$ und $L \subseteq M$ maximale Ketten. Dann gilt $K \cong L$.

Für distributive Verbände (siehe Definition 2.1.3.6) kann man analog zu Lemma 3.6.5.6 äquivalente Bedingungen finden (man beachte auch Lemma 3.6.5.1):

**Lemma 3.6.5.12.** *Sei $(V, \wedge, \vee)$ ein Verband. Dann sind die folgenden Aussagen äquivalent:*

*(1)* $\forall x, y, z \in V : x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ *und* $\forall x, y, z \in V : x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ *(d.h., $V$ ist distributiv)*

*(2)* $\forall x, y, z \in V : x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$

*(2')* $\forall x, y, z \in V : x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$

*(3)* $\forall x, y, z \in V : x \wedge (y \vee z) \leq (x \wedge y) \vee (x \wedge z)$

*(3')* $\forall x, y, z \in V : x \vee (y \wedge z) \geq (x \vee y) \wedge (x \vee z)$

*(4)* $\forall x, y, z \in V : (x \wedge y) \vee (y \wedge z) \vee (z \wedge x) = (x \vee y) \wedge (y \vee z) \wedge (z \vee x)$

*(5)* $\forall x, y, z \in V : (x \wedge y) \vee (y \wedge z) \vee (z \wedge x) \geq (x \vee y) \wedge (y \vee z) \wedge (z \vee x)$

**UE 251 ► Übungsaufgabe 3.6.5.13.** (V) Beweisen Sie Lemma 3.6.5.12. **◄ UE 251**
Hinweis für die Implikation (4) ⇒ (2): Zeigen Sie zunächst, dass $V$ modular ist, und betrachten Sie dann $x \wedge \Big((x \vee y) \wedge (y \vee z) \wedge (z \vee x)\Big)$.

Unmittelbar aus der Definition (bzw. als Nebenprodukt des obigen Hinweises) ergibt sich:

**Lemma 3.6.5.14.** *Wenn ein Verband $(V, \wedge, \vee)$ distributiv ist, dann ist er auch modular.*

Prominente Beispiele distributiver Verbände sind erneut Totalordnungen $(P, \min, \max)$ sowie Potenzmengenverbände $(\mathfrak{P}(M), \cap, \cup)$. Der Verband $N_5$ kann wegen Lemma 3.6.5.14 nicht distributiv sein, aber auch $M_3$ ist nicht distributiv – dazu ist nur $x = a$, $y = b$ und $z = c$ zu setzen. Ein weiteres Beispiel ergibt sich durch die folgende Serie an Übungsaufgaben, die zugleich einen Blick auf die Beweismethode des Darstellungssatzes von Stone für Boolesche Algebren (Satz 3.6.8.13) erlaubt.

**UE 252 ► Übungsaufgabe 3.6.5.15.** (F+) Sei $(V, \cap, \cup)$ Mengenverband (das heißt, $V$ ist Teilmenge der Potenzmenge einer Menge $M$, $\cap$ und $\cup$ sind mengentheoretischer Durchschnitt und Vereinigung). Man zeige, dass für jedes $m \in M$ die Abbildung $f_m \colon V \to \{0, 1\}$, $f_m(A) = 1$ für $m \in A$, $f_m(A) = 0$ sonst, ein Homomorphismus auf den zweielementigen Verband ist. **◄ UE 252**

**UE 253 ► Übungsaufgabe 3.6.5.16.** (F+) Man verwende die Homomorphismen $f_m$ aus dem vorigen Beispiel, um zu zeigen, dass jeder Mengenverband isomorph zu einem Unterverband eines direkten Produktes von zweielementigen Verbänden ist. (Anleitung: Man betrachte die Einbettung $A \mapsto (f_m(A))_{m \in M}$.) **◄ UE 253**

**UE 254 ► Übungsaufgabe 3.6.5.17.** (F+) Man folgere aus obigen Beispielen, dass Mengenverbände distributiv sind. **◄ UE 254**

Eine interessante Eigenschaft distributiver Verbände ist:

**UE 255 ► Übungsaufgabe 3.6.5.18.** (F) **◄ UE 255**

1. Sei $(V, \wedge, \vee)$ ein distributiver Verband, und seien $a, x, y \in V$ mit $a \wedge x = a \wedge y$ und $a \vee x = a \vee y$. Zeigen Sie, dass dann $x = y$.
   (Hinweis: Überlegen Sie zunächst ob/warum $(x \wedge y) \vee (x \wedge a) = (x \wedge y) \vee (a \wedge y)$ gilt.)

2. Finden Sie Elemente $a, x, y \in M_3$ mit $x \neq y$ aber $a \wedge x = a \wedge y$ und $a \vee x = a \vee y$.

3. Finden Sie Elemente $a, x, y \in N_5$ mit $x \neq y$ aber $a \wedge x = a \wedge y$ und $a \vee x = a \vee y$.

In Analogie zu Satz 3.6.5.8 kann man auch die Klasse der distributiven Verbände durchs Nichtenthalten gewisser Unterverbände charakterisieren.

**Satz 3.6.5.19.** *Für einen modularen Verband $(V, \wedge, \vee)$ sind die folgenden Bedingungen äquivalent:*

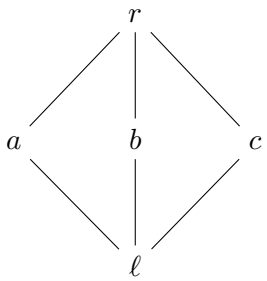
(1) *$V$ ist distributiv.*

(2) *$V$ besitzt keinen Unterverband, der zu $M_3$ isomorph ist*[30].

*Beweis.* Wir zeigen wieder die Äquivalenz der Negationen, wobei aus der Existenz eines zu $M_3$ isomorphen Unterverbands erneut sehr leicht folgt, dass $V$ nicht distributiv ist. Sei also $V$ nicht distributiv. Nach Lemma 3.6.5.12 bzw. Lemma 3.6.5.1 gibt es $x, y, z \in V$ mit

$$\ell := (x \wedge y) \vee (y \wedge z) \vee (z \wedge x) < (x \vee y) \wedge (y \vee z) \wedge (z \vee x) =: r.$$

Wir setzen $a := (r \wedge x) \vee \ell$, $b := (r \wedge y) \vee \ell$, $c := (r \wedge z) \vee \ell$ und behaupten, dass die Elemente $\ell$, $a$, $b$, $c$, $r$ wie abgebildet einen zu $M_3$ isomorphen Unterverband von $V$ bilden.




Mit der Kommutativität und dem Verschmelzungsgesetz ergibt sich $r \wedge x = x \wedge (y \vee z)$, $r \wedge y = y \wedge (z \vee x)$ und $r \wedge z = z \wedge (x \vee y)$. Wegen $\ell \leq (x \wedge (y \vee z)) \vee (y \wedge (z \vee x))$ folgt

$$a \vee b = \Big(x \wedge (y \vee z)\Big) \vee \ell \vee \Big(y \wedge (z \vee x)\Big) = \Big(x \wedge (y \vee z)\Big) \vee \Big(y \wedge (z \vee x)\Big).$$

Unter zweimaliger Verwendung der Modularität (mit den Ungleichungen $x \wedge (y \vee z) \leq z \vee x$ sowie $y \leq y \vee z$) erhalten wir

$$\begin{aligned} a \vee b &= \Big(x \wedge (y \vee z)\Big) \vee \Big(y \wedge (z \vee x)\Big) = \Big[\Big(x \wedge (y \vee z)\Big) \vee y\Big] \wedge (z \vee x) \\ &= \Big[y \vee \Big(x \wedge (y \vee z)\Big)\Big] \wedge (z \vee x) = (y \vee x) \wedge (y \vee z) \wedge (z \vee x) = r. \end{aligned}$$

[30] Siehe Fußnote auf Seite 229.

Analog sieht man $a \vee c = r = b \vee c$. Aufgrund von $\ell < r$ liefert die Modularität $a = r \wedge (x \vee \ell)$, $b = r \wedge (y \vee \ell)$ und $c = r \wedge (z \vee \ell)$, sodass man dual zu oben $a \wedge b = a \wedge c = b \wedge c = \ell$ schließen kann.
Es bleibt zu zeigen, dass die Elemente $\ell$, $a$, $b$, $c$, $r$ paarweise verschieden sind. Aus $a = b$ würde der Widerspruch $r = a \vee b = a = a \wedge b = \ell$ folgen; analog beweist man $a \neq c$ und $b \neq c$. Sei jetzt $a = \ell$ angenommen. Dann folgt $a \leq b$, also $b = a \vee b = r$. Analog beweist man $c = r$, aber – dual dazu ausgehend von $b = r$ anstatt von $a = \ell$ – auch $c = \ell$, also den Widerspruch $\ell = r$. Genauso zeigt man $b, c \neq \ell$ sowie $a, b, c \neq r$, was den Beweis abschließt. □

Kombinieren wir Satz 3.6.5.8 mit Satz 3.6.5.19 und beachten, dass ein nichtmodularer Verband auch nicht distributiv sein kann, so ergibt sich:

**Folgerung 3.6.5.20.** *Für einen Verband $(V, \wedge, \vee)$ sind die folgenden Bedingungen äquivalent:*

(1) *$V$ ist distributiv.*

(2) *$V$ besitzt keinen Unterverband, der zu $N_5$ oder zu $M_3$ isomorph ist.*

**UE 256** ► **Übungsaufgabe 3.6.5.21.** (D) Man ermittle (bis auf Isomorphie) alle modularen Verbände bis zu einer möglichst großen Kardinalität. Welche davon sind distributiv? ◄ **UE 256**

### 3.6.6 Boolesche Algebren und Boolesche Ringe

Inhalt in Kurzfassung: Boolesche Algebren sind sehr reichhaltige Spezialisierungen von Verbänden, für die starke Strukturaussagen möglich sind. Ein prominentes Beispiel ist der Potenzmengenverband zusammen mit der mengentheoretischen Komplementbildung. Boolesche Ringe sind Ringe mit 1, in denen die Multiplikation idempotent ist. Sie entsprechen in bijektiver Weise den Booleschen Algebren mit derselben Trägermenge. Dieser Zusammenhang ermöglicht es, Konzepte und Ergebnisse aus der Ringtheorie auf Boolesche Algebren zu übertragen.

Zur Wiederholung: Eine Algebra $(B, \wedge, \vee, 0, 1, ')$ vom Typ $(2, 2, 0, 0, 1)$ ist genau dann eine *Boolesche Algebra*, wenn die folgenden Gesetze gelten (jeweils quantifiziert für alle $a, b, c \in B$):

$$\begin{aligned} a \wedge b &= b \wedge a & a \vee b &= b \vee a \\ a \wedge (b \wedge c) &= (a \wedge b) \wedge c & a \vee (b \vee c) &= (a \vee b) \vee c \\ a \wedge (a \vee b) &= a & a \vee (a \wedge b) &= a \\ a \wedge (b \vee c) &= (a \wedge b) \vee (a \wedge c) & a \vee (b \wedge c) &= (a \vee b) \wedge (a \vee c) \\ 1 \wedge a &= a & 0 \vee a &= a \\ a \wedge a' &= 0 & a \vee a' &= 1 \end{aligned}$$

**Anmerkung 3.6.6.1.** Manche Autoren verwenden für die Operationen $\vee$, $\wedge$ der Booleschen Algebra die Symbole $+$ und $\cdot$. Wir tun dies nicht, um Verwechslungen mit Booleschen Ringen (siehe Definition 3.6.6.4) zu vermeiden, und um die Verwandtschaft zu Verbänden zu betonen.
Für das Komplement $x'$ werden auch oft andere Symbole verwendet, wie $x^c$, $-x$, $\neg x$, $\sim x$, $\bar{x}$. In der (sehr wichtigen) Booleschen Algebra $(\mathfrak{P}(M), \cap, \cup, \emptyset, M, ')$ ist $X \cap Y'$ genau die Mengendifferenz $X \setminus Y$, weshalb man auch für allgemeine Boolesche Algebren manchmal $x \setminus y := x \wedge y'$ schreibt.

Das Dualitätsprinzip für Verbände lässt sich auf Boolesche Algebren spezialisieren: Ist $\varphi$ eine Aussage über Boolesche Algebren, so entsteht die duale Aussage $\varphi^d$ wieder durch Ersetzen von $\wedge$ durch $\vee$, von $\vee$ durch $\wedge$ und von $\leq$ durch $\geq$; neu bei Booleschen Algebren ist ein etwaiges Auftreten des Komplementsymbols $'$, dieses bleibt unverändert. Aufseite der Strukturen beobachten wir: Ist $(B, \wedge, \vee, 0, 1, ')$ eine Boolesche Algebra, dann ist auch $B^d = (B, \vee, \wedge, 1, 0, ')$ eine Boolesche Algebra. Das *Dualitätsprinzip für Boolesche Algebren* besagt dann: Wenn in $B$ die Aussage $\varphi$ gilt, dann gilt in $B^d$ die Aussage $\varphi^d$. Wenn insbesondere $\varphi$ in alle Booleschen Algebren gilt, dann auch $\varphi^d$.

**Satz 3.6.6.2** (Satz über Komplemente)**.** *Sei $(B, \wedge, \vee, 0, 1, ')$ eine Boolesche Algebra. Dann gilt:*

*(a) Sind $a, a^*$ Elemente von $B$ mit $a \vee a^* = 1$ und $a \wedge a^* = 0$, so gilt $a^* = a'$.*

*(b) $(a')' = a$ für alle $a \in B$.*

*(c) $0' = 1$ und $1' = 0$.*

*(d) $(a \vee b)' = a' \wedge b'$ und $(a \wedge b)' = a' \vee b'$ für alle $a, b \in B$* (De Morgan'sche Gesetze).

*Beweis.* (a) folgt aus Aufgabe 3.6.1.5.
(b), (c), (d) folgen aus (a). □

**Satz 3.6.6.3** (Rechenregeln für Boolesche Algebren)**.** *Sei $B$ eine Boolesche Algebra. Dann gilt für alle $a, b \in B$:*

*a) $a \leq b \Leftrightarrow b' \leq a'$. (Man sagt auch, dass die Abbildung $a \mapsto a'$ antimonoton ist.)*

*b) $a \leq b \Leftrightarrow a' \vee b = 1 \Leftrightarrow a \wedge b' = 0$.*
*In Analogie zur Logik wird der Ausdruck $a' \vee b$ manchmal auch mit $a \to b$ abgekürzt, d.h. $\to$ wird als Name einer 2-stelligen Operation verstanden.*

*c) $a \leq b' \Leftrightarrow a \wedge b = 0 \Leftrightarrow b \leq a'$.*
*Für die Gleichung $a \wedge b = 0$ verwendet man (in Analogie zur linearen Algebra) auch die Abkürzung $a \perp b$ ab. $a$ und $b$ heißen in so einem Fall* disjunkt.

*Beweis.* a) Wir verwenden die Regel von de Morgan sowie die Tatsache, dass man $x \leq y$ in äquivalenter Weise sowohl durch $x \wedge y = x$ als auch durch $x \vee y = y$ definieren kann: $a \leq b \Leftrightarrow a \wedge b = a \Leftrightarrow (a \wedge b)' = a' \Leftrightarrow a' \vee b' = a' \Leftrightarrow b' \leq a'$.

b) Wenn $a \leq b$, dann ist $a' \vee b = a' \vee (a \vee b) = 1$. Wenn umgekehrt $a' \vee b = 1$ ist, dann gilt:

$$a = a \wedge 1 = a \wedge (a' \vee b) = (a \wedge a') \vee (a \wedge b) = a \wedge b,$$

also $a \leq b$. Die zweite Äquivalenz folgt dann aus dem Gesetz von de Morgan.
c) folgt aus b). □

Eng mit dem Begriff der Booleschen Algebra verwandt ist das Konzept des Booleschen Rings.

**Definition 3.6.6.4.** Ein Ring $(R, +, 0, -, \cdot, 1)$ mit Einselement heißt *Boolescher Ring*, wenn $\forall x \in R\ x \cdot x = x$ gilt.

Zunächst eine einfache Beobachtung:

**Lemma 3.6.6.5.** *In jedem Booleschen Ring $(R, +, 0, -, \cdot, 1)$ gilt $x+x = 0$ für alle $x \in R$. Daher ist $-x = x$ für alle $x$; statt $x - y$ kann man also genauso gut $x + y$ schreiben. denn $x + 1 = (x + 1)(x + 1) = xx + x + x + 1 = (x + x) + (x + 1)$.*

*Beweis.* Man berechnet $x + 1 = (x + 1)(x + 1) = xx + x + x + 1 = (x + x) + (x + 1)$ und subtrahiert auf beiden Seiten $x + 1$. □

Die Beziehung zwischen Booleschen Algebren und Booleschen Ringen kommt im folgenden Satz zum Ausdruck.

**Satz 3.6.6.6.**

(*a*) *Sei $(R, +, 0, -, \cdot, 1)$ ein Boolescher Ring. Mit den Operationen*

$$x \wedge y := xy, \qquad x \vee y := x + y + xy, \qquad x' := 1 + x\ (= 1 - x)$$

*ist die Algebra $(R, \wedge, \vee, 0, 1, ')$ eine Boolesche Algebra,*
*und es gilt $x + y = (x \wedge y') \vee (x' \wedge y)$.*

(*b*) *Sei $(B, \wedge, \vee, 0, 1, ')$ eine Boolesche Algebra. Mit den Operationen*

$$x \cdot y := x \wedge y, \qquad x + y := (x \wedge y') \vee (x' \wedge y), \qquad -x := x$$

*ist $(B, +, 0, -, \cdot, 1)$ ein Boolescher Ring,*
*und es gilt $x \vee y = x + y + xy = 1 + (1 + x)(1 + y)$.*

(*c*) *Die in (a) und (b) beschriebenen Abbildungen zwischen Booleschen Algebren und Booleschen Ringen sind invers zueinander.*

*Weiters gilt: Seien $(R_i, +, 0, -, \cdot, 1)$ (für $i = 1, 2$) Boolesche Ringe, mit zugehörigen Booleschen Algebren $(R_i, \wedge, \vee, 0, 1, ')$. Eine Abbildung $f\colon R_1 \to R_2$ ist genau dann Ringhomomorphismus, wenn sie ein Homomorphismus von Booleschen Algebren ist.*

**UE 257 ► Übungsaufgabe 3.6.6.7.** (V) Beweisen Sie Satz 3.6.6.6. **◄ UE 257**

**Anmerkung 3.6.6.8.** Für die Boolesche Algebra $(\mathfrak{P}(M), \cap, \cup, \emptyset, M, ')$ ist die additive Operation im zugehörien Booleschen Ring genau $X + Y = (X \wedge Y') \vee (Y \wedge X') = X \,\Delta\, Y$, also die symmetrische Differenz der beiden Mengen $X, Y \in \mathfrak{P}(M)$. Daher nennt man die Operation $+$ auch im Allgemeinen „symmetrische Differenz“ und schreibt sie manchmal als $x \,\Delta\, y$.

Boolesche Algebren und Boolesche Ringe beschreiben also „im Wesentlichen“ dieselben Strukturen. Das bedeutet, dass man Boolesche Algebren auch mit Mitteln der Ringtheorie untersuchen kann. Als Beispiel dafür kann der Homomorphiesatz für Boolesche Algebren gesehen haben, dessen Beweis weitgehend parallel zum Beweis des Homomorphiesatzes für Ringe verläuft.

**Satz 3.6.6.9** (Homomorphiesatz für Boolesche Algebren)**.** *Sei $f\colon B_1 \to B_2$ ein surjektiver Homomorphismus von Booleschen Algebren.*
*Dann ist $B_2$ zu $B_1/f^{-1}(0)$ isomorph, wobei $B_1/f^{-1}(0)$ die Menge aller Äquivalenzklassen der Relation*

$$x \sim y \Leftrightarrow x + y \in f^{-1}(0)$$

*bezeichnet.*

*Beweis.* Nach dem allgemeinen Homomorphiesatz gilt $B_2 \cong B_1/\ker(f)$, wobei $\ker(f)$ die durch

$$(x, y) \in \ker(f) \;\Leftrightarrow\; f(x) = f(y)$$

definierte Äquivalenzrelation ist. Nun gilt aber

$$f(x) = f(y) \;\Leftrightarrow\; f(x) - f(y) = 0 \;\Leftrightarrow\; f(x) + f(y) = 0 \;\Leftrightarrow\; f(x+y) = 0 \;\Leftrightarrow\; x + y \in f^{-1}\{0\},$$

also stimmt $\ker(f)$ mit $\sim$ überein. □

Jede Kongruenzrelation $\sim$ auf einem Ring, erst recht also auf jedem Booleschen Ring, ist durch ein Ideal charakterisiert, nämlich die Äquivalenzklasse von 0. Da die Ringoperationen durch die Operationen der Booleschen Algebra beschrieben werden (und umgekehrt), sind die Kongruenzrelationen eines Booleschen Rings genau die Kongruenzrelationen der entsprechenden Booleschen Algebra. Die Ringkongruenzen kann man durch Ringideale beschreiben; es wird sich als Nächstes herausstellen, dass diese genau den in Definition 3.6.3.7 definierten Idealen entsprechen.

**Definition 3.6.6.10.** Für $T \subseteq B$ schreiben wir $T^*$ für die Menge $\{b' \mid b \in T\}$.

Von besonderem Interesse sind die Mengen $T^*$, wenn $T$ ein Filter oder ein Ideal ist. Man zeigt leicht:

**Lemma 3.6.6.11.** *Sei $B$ Boolesche Algebra. Dann ist $I \subseteq B$ genau dann ein Ideal (im Sinn von Definition 3.6.3.7), wenn $I$ ein Ideal (im ringtheoretischen Sinn) des zugeordneten Booleschen Rings ist.*
*$F \subseteq B$ ist genau dann ein Filter, wenn $F^*$ ein Ideal ist.*
*$I \subseteq B$ ist genau dann ein Ideal, wenn $I^*$ ein Filter ist.*

**UE 258 ► Übungsaufgabe 3.6.6.12.** (F) Beweisen Sie Lemma 3.6.6.11. **◄ UE 258**

**Definition 3.6.6.13.** Sei $I \subseteq B$ ein Ideal. Dann definieren wir die Äquivalenzrelation $\sim_I$ durch $x \sim_I y :\Leftrightarrow x - y \in I$. ($x - y = x + y$ ist hier die Ringoperation.)
Dual dazu: Sei $F \subseteq B$ ein Filter. Dann definieren wir die Äquivalenzrelation $\sim_F$ durch $x \sim_F y \Leftrightarrow (x - y)' \in F$.

**Lemma 3.6.6.14.** *Sei $B$ Boolesche Algebra, und sei $I$ Ideal. Sei $F := I^* = \{b' \mid b \in I\}$ der dazu duale Filter. Dann sind für alle $b, c \in B$ die folgenden Aussagen äquivalent:*

(a) $b \sim_I c$.
(b) $b \sim_F c$.
(c) $\exists f \in F : b \wedge f = c \wedge f$.
(d) $\exists i \in I : b \wedge i' = c \wedge i'$.
(e) $\exists i \in I : b \vee i = c \vee i$.

*Beweis.* Die Äquivalenzen (a) $\Leftrightarrow$ (b) und (c) $\Leftrightarrow$ (d) sind klar.
(d) $\Rightarrow$ (e): Für alle $x$ gilt $x \vee i = (x \wedge i) \vee (x \wedge i') \vee i$. Somit folgt aus $b \wedge i' = c \wedge i'$ sofort $b \vee i = (b \wedge i') \vee i = (c \wedge i') \vee i = c \vee i$. (e) $\Rightarrow$ (d): Die Implikation $b \vee i = c \vee i \Rightarrow b \vee i' = c \wedge i'$ ist dual zu „(d) $\Rightarrow$ (e)“ zu beweisen.
Die Äquivalenz zwischen (b) und (c) folgt aus der Beziehung

$$b \wedge f = c \wedge f \;\Leftrightarrow\; b + c \leq f'.$$

Beweis dieser Äquivalenz: Wenn $b \wedge f = c \wedge f$, dann ist

$$b \wedge c' = (b \wedge c' \wedge f) \vee (b \wedge c' \wedge f') = (c \wedge c' \wedge f) \vee (b \wedge c' \wedge f') \leq 0 \vee f' = f',$$

analog $b' \wedge c \leq f'$, daher $b + c = (b \wedge c') \vee (b' \wedge c) \leq f'$.
Wenn umgekehrt $b + c \leq f'$ gilt, dann ist $b \wedge c' \leq b + c \leq f'$ und daher $b \wedge f = (b \wedge c \wedge f) \vee (b \wedge c' \wedge f) \leq (b \wedge c \wedge f) \vee (f' \wedge f) = (b \wedge c \wedge f) \leq b \wedge f$, also $b \wedge f = b \wedge c \wedge f$.
Analog $c \wedge f = b \wedge c \wedge f$, also $b \wedge f = c \wedge f$. □

**Beispiel 3.6.6.15.** Sei $B = \mathfrak{P}(\mathbb{N})$ die Potenzmenge der natürlichen Zahlen. Mit den Operationen $\cup$, $\cap$ wird $B$ zu einer Booleschen Algebra ($1 = \mathbb{N}$, etc.).
Sei $I$ die Famile aller endlichen Teilmengen von $\mathbb{N}$, $F := I^*$ die Familie aller ko-endlichen Teilmengen von $\mathbb{N}$ (d.h. Mengen mit endlichem Komplement). Dann gilt für beliebige Teilmengen $X, Y \subseteq \mathbb{N}$:

$X \sim_I Y \Leftrightarrow X \sim_F Y \Leftrightarrow \exists n \in \mathbb{N} : X \cap [n, \infty) = Y \cap [n, \infty)$,
d.h. genau dann, wenn $X$ und $Y$ bis auf endlich viele Elemente übereinstimmen.

**Beispiel 3.6.6.16.** Sei $B$ die Familie aller Borelmengen $X \subseteq [0, 1]$. $B$ ist Boolesche Algebra (mit den üblichen Operationen $\cup, \cap, \ldots$). Sei $\lambda$ das Lebesguemaß.

Sei $I := \{X \in B \mid \lambda(X) = 0\}$, die Familie der Nullmengen. Der dazu *duale Filter* ist die Familie der Einsmengen: $F := I^* = \{Y \in B \mid \lambda(Y) = 1\}$.
Dann gilt $X \sim_I Y$ genau dann, wenn $\lambda(X \,\Delta\, Y) = 0$, also wenn $X$ und $Y$ „bis auf eine Lebesgue-Nullmenge“ übereinstimmen. Da $I$ nicht nur bezüglich endlicher, sondern sogar bezüglich abzählbarer Vereinigungen abgeschlossen ist, spricht man sogar von einem $\sigma$-Ideal, entsprechend bei $F$ von einem $\sigma$-Filter.

### 3.6.7 Atome

Inhalt in Kurzfassung: Atome in Booleschen Algebren sind definitionsgemäß obere Nachbarn der 0. Der Stonesche Darstellungssatz für endliche Boolesche Algebren besagt, dass jede solche isomorph ist zur Potenzmengenalgebra über der Menge ihrer Atome. Die allgemeinere Version dieses Satzes folgt dann in 3.6.8.

Das wichtigste Ergebnis dieses Abschnitts, den Satz von Stone für endliche Boolesche Algebren (3.6.7.6), werden wir auch als Folgerung der allgemeinen Version des Stoneschen Satzes (3.6.8.13) erhalten. Daher werden wir den Beweis selbst nicht detailliert ausführen, sondern konzentrieren uns auf das dafür erforderliche Konzept der sogenannten Atome, die auch anderweitig wichtig und interessant sind.

**Definition 3.6.7.1.** Sei $(V, \wedge, \vee)$ ein Verband mit kleinstem Element 0. Dann heißt $a \in V$ ein *Atom* :$\Leftrightarrow$

1) $0 < a$ und

2) $\forall b \in V:\ 0 < b \leq a \Rightarrow b = a$

(d. h., $a$ ist ein oberer Nachbar von 0).
Wir schreiben $\mathrm{At}(V)$ für die Menge aller Atome von $V$.

**Lemma 3.6.7.2** (Rechenregeln für Atome)**.** *Sei $B$ Boolesche Algebra, $a \in B$ ein Atom. Dann gilt für alle $b, c \in B$:*

*(A1)* $a \leq b$ *genau dann, wenn* $a \wedge b \neq 0$. *Anders gesagt:* $a \not\leq b \ \Leftrightarrow\ a \wedge b = 0$.

*(A2)* $a \leq b'$ *genau dann, wenn* $a \not\leq b$.

*(A3)* $a \leq b \wedge c$ *genau dann, wenn* $a \leq b$ *und* $a \leq c$. *(Das gilt natürlich nicht nur für Atome $a$, sondern für beliebige Verbandselemente.)*

*(A4)* $a \leq b \vee c$ *genau dann, wenn* $a \leq b$ *oder* $a \leq c$.

**UE 259 ► Übungsaufgabe 3.6.7.3.** (V) Beweisen Sie Lemma 3.6.7.2. **◄ UE 259**

**Anmerkung 3.6.7.4.** Die Regeln (A2), (A3), (A4) geben eine Korrespondenz zwischen den algebraischen Operationen $'$, $\wedge$, $\vee$ und den logischen Junktoren „nicht“, „und“ und „oder“. Im nächsten Satz übersetzen wir diese logischen Junktoren in die mengentheoretischen Operationen $'$, $\cap$ und $\cup$.

**Lemma 3.6.7.5.** *Sei $(B, \wedge, \vee, 0, 1, ')$ eine endliche Boolesche Algebra. Dann gibt es zu jedem Element $b \in B \setminus \{0\}$ ein Atom $a \in \mathrm{At}(B)$ mit $a \leq b$. (Dies gilt sogar für beliebige endliche Verbände.)*

*Beweis.* Sei $b \in B \setminus \{0\}$. Ist $b$ Atom, so kann man $a = b$ setzen. Ist $b$ kein Atom, so gibt es ein $b_1 \in B$ mit $0 < b_1 < b$. Ist $b_1$ Atom, so kann man $a = b_1$ setzen. Andernfalls setzt man das Verfahren fort und erhält eine Kette $b > b_1 > b_2 > \ldots$, die, da $B$ endlich ist, bei einem $b_i$ abbrechen muss. Dann setzt man $a = b_i$. □

**Satz 3.6.7.6.** *[Satz von Stone für endliche Boolesche Algebren] Sei $(B, \wedge, \vee, 0, 1, ')$ eine Boolesche Algebra und $A := \mathrm{At}(B)$ die Menge der Atome von $B$.*
*Sei $\varphi : B \to \mathfrak{P}(A)$ gegeben durch $\varphi(b) := \{a \in A \mid a \leq b\}$.*
*Dann gilt:*

- *$\varphi$ ist Homomorphismus von Booleschen Algebren.*
- *Ist $B$ endlich, so ist $\varphi$ ein Isomorphismus der Booleschen Algebren $B$ und $(\mathfrak{P}(A), \cap, \cup, \emptyset, A, ')$.*

*Beweis.* Übungsaufgabe. □

**UE 260 ▶ Übungsaufgabe 3.6.7.7.** (W) Beweisen Sie Satz 3.6.7.6. **◀ UE 260**

**UE 261 ▶ Übungsaufgabe 3.6.7.8.** (B) Geben Sie eine Boolesche Algebra $B$ an, sodass die Abbildung $\varphi\colon B \to \mathfrak{P}(\mathrm{At}(B))$, $b \mapsto \{a \in \mathrm{At}(B) : a \leq b\}$ nicht surjektiv ist. **◀ UE 261**

**UE 262 ▶ Übungsaufgabe 3.6.7.9.** (B) Geben Sie eine Boolesche Algebra $B$ an, sodass die Abbildung $\varphi\colon B \to \mathfrak{P}(\mathrm{At}(B))$, $b \mapsto \{a \in \mathrm{At}(B) : a \leq b\}$ nicht injektiv ist. **◀ UE 262**

**Folgerung 3.6.7.10.** *Ist $B$ eine endliche Boolesche Algebra, dann gilt $|B| = 2^n$ für ein $n \in \mathbb{N}$. Zu jedem $n \in \mathbb{N}$ gibt es somit – bis auf Isomorphie – genau eine Boolesche Algebra mit $2^n$ Elementen, nämlich $\mathfrak{P}(\{0, 1, \ldots, n-1\})$.*

*Beweis.* Nach dem Satz von Stone ist $B$ isomorph zu $\mathfrak{P}(A)$ für eine endliche Menge $A$ (nämlich $A = \mathrm{At}(B)$, aber das benötigen wir hier nicht). Setzen wir $n = |A|$, so folgt $|B| = |\mathfrak{P}(A)| = 2^n$.
Sei $B'$ eine weitere Boolesche Algebra mit $2^n$ Elementen. Dann gilt $B' \cong \mathfrak{P}(A')$ für eine Menge $A'$ mit $|A'| = n = |A|$. Ist $\rho : A \to A'$ eine Bijektion, so ist $\hat{\rho} : \mathfrak{P}(A) \to \mathfrak{P}(A')$, $\hat{\rho}(A) := \{\rho(a) \mid a \in A\}$ ein Isomorphismus zwischen Booleschen Algebren. Also sind auch $B$ und $B'$ isomorph. □

Im nächsten Abschnitt wollen wir diesen Satz auf beliebige Boolesche Algebren verallgemeinern. Man kann nicht erwarten, dass jede Boolesche Algebra zu einer Potenzmengenalgebra isomorph ist; es gibt nämlich abzählbar unendliche Boolesche Algeben (siehe Übungsaufgabe 3.6.7.17), während die Potenzmenge einer Menge nicht abzählbar unendlich sein kann: die Potenzmenge jeder endlichen Menge ist endlich, und die Potenzmenge jeder unendlichen Menge ist überabzählbar.

**Definition 3.6.7.11.** Sei $M$ Menge. Eine Menge $\mathfrak{K} \subseteq \mathfrak{P}(M)$ heißt *Mengenalgebra*[31] :$\Leftrightarrow$ für alle $A, B \in \mathfrak{K}$ gilt

(1) $A \cup B \in \mathfrak{K}$,

(2) $A \cap B \in \mathfrak{K}$,

(3) $A' := M \setminus A \in \mathfrak{K}$,

(4) $A \cap B' = A \setminus B \in \mathfrak{K}$,

(5) $M \in \mathfrak{K}$.

**Anmerkung 3.6.7.12.** Die Liste (1)–(5) ist redundant.

**Beispiel 3.6.7.13.** $\mathfrak{P}(M)$ ist eine Mengenalgebra, genauso wie $\{M, \emptyset\}$.

**Anmerkung 3.6.7.14.** Jede Mengenalgebra ist Unteralgebra der Potenzmengenalgebra (mit den üblichen Operationen Schnitt, Vereinigung, Komplement), und ist daher selbst eine Boolesche Algebra.

Die folgenden Beispiele zeigen, dass eine Mengenalgebra Atome haben kann, aber nicht haben muss.

**Beispiele 3.6.7.15.** 1) Sei $(0, 1]$ das halboffene Intervall der reellen Zahlengeraden und $\mathfrak{K} \subseteq \mathfrak{P}((0, 1])$ gegeben durch $\mathfrak{K} := \{\emptyset\} \cup \{\bigcup_{1 \leq i \leq n}(a_i, b_i] \mid 0 \leq a_i < b_i \leq 1,\ n \in \mathbb{N}^+\}$. Dann ist $\mathfrak{K}$ Unteralgebra von $(\mathfrak{P}((0, 1]), \cap, \cup, \emptyset, (0, 1], ')$.
$\mathfrak{K}$ enthält keine Atome.

2) Sei $X$ eine beliebige unendliche Menge; sei $I$ die Menge aller endlichen Teilmengen von $X$, und sei $F := I' = \{X \setminus A \mid A \in I\}$ die Menge der *ko-endlichen Teilmengen* von $X$. Dann ist $I \cup F$ eine Unteralgebra von $(\mathfrak{P}(X), \cap, \cup, \emptyset, X, ')$. $I$ ist nämlich unter Schnitten und Vereinigungen abgeschlossen, daher auch $F$: wenn nämlich $x, y \in F$, dann $x', y' \in I$, also $x' \vee y' \in I$, daher $x \wedge y = (x' \vee y')' \in F$. Das Komplement jedes Elements von $I$ liegt in $F$, und umgekehrt.
Die Atome von $I \cup F$ sind genau die einelementigen Teilmengen von $X$.

**UE 263** ► **Übungsaufgabe 3.6.7.16.** (F) Für eine beliebige Boolesche Algebra $B$ bezeichne ◄ **UE 263**
$\mathrm{At}(B)$ die Menge der Atome von $B$. Seien $B_1$ und $B_2$ Boolesche Algebren mit Nullelementen $0_1$ und $0_2$. Betrachten Sie die Boolesche Algebra $B_1 \times B_2$ und zeigen Sie:

$$\mathrm{At}(B_1 \times B_2) = \mathrm{At}(B_1) \times \{0_2\} \cup \{0_1\} \times \mathrm{At}(B_2)$$

**UE 264** ► **Übungsaufgabe 3.6.7.17.** (B) Finden Sie möglichst viele (mindestens 4) nichtiso- ◄ **UE 264**
morphe abzählbar unendliche Boolesche Algebren.

**UE 265** ► **Übungsaufgabe 3.6.7.18.** (E) Gibt es eine abzählbar unendliche Boolesche Algebra, ◄ **UE 265**
die ein vollständiger Verband ist?

[31] englisch: *field of sets*

### 3.6.8 Der Darstellungssatz von Stone

Inhalt in Kurzfassung: Der Darstellungssatz von Stone in seiner allgemeinen Formulierung besagt, dass sich jede Boolesche Algebra in eine Potenzmengenalgebra einbetten lässt. Die Menge, deren Potenzmenge hier auftritt, ist die Menge aller Ultrafilter in der gegebenen Booleschen Algebra. Die Beweismethode ist insofern sehr lehrreich, als ähnliche Methoden in verschiedenen Teilgebieten der Mathematik auftreten. Aus dem Darstellungssatz kann u.a. die sehr bemerkenswerte Aussage gefolgert werden, dass jedes Gesetz, das in der zweielementigen Booleschen Algebra gilt, automatisch in allen Booleschen Algebren gilt.

Wir beginnen mit einer informellen Überlegung:
Sei $\mathfrak{K} \leq (\mathfrak{P}(M), \cap, \cup, \emptyset, M, ')$ eine Mengenalgebra. Wie weit können wir die Menge $M$ aus $\mathfrak{K}$ bestimmen, wenn wir $\mathfrak{K}$ nur bis auf Isomorphie, d.h. als abstrakte Boolesche Algebra kennen? Unsere Aufgabe lautet also: Gegeben eine Boolesche Algebra $B$, ist eine Menge $M$ gesucht, sodass $B$ isomorph ist zu einer Unteralgebra von $\mathfrak{P}(M)$.
Im vorigen Abschnitt haben wir uns mit endlichen Booleschen Algebren $B$ beschäftigt. Die Menge $M$ haben wir als die Menge der Atome von $B$ identifiziert. Der Isomorphismus hat jedes Element $b \in B$ auf die Menge $\{m \in M \mid m \leq b\} \in \mathfrak{P}(M)$ abgebildet. Derselbe Beweis zeigt, dass für jede Boolesche Algebra $B$ mit $M$ als Menge der Atome die Abbildung $b \mapsto \{a \in M \mid a \leq b\}$ ein Homomorphismus von $B$ in $\mathfrak{P}(M)$ ist.
Für unendliche Boolesche Algebren kann es aber vorkommen, dass es keine Atome gibt, oder dass es nur so wenige Atome gibt, dass die obige Abbildung nicht injektiv ist, oder dass es so viele Atome gibt, dass die obige Abbildung nicht surjektiv ist (Surjektivität bedeutet hier, dass man zu jeder Menge von Atomen ein Element finden kann, das *genau* über den Atomen aus der gegebenen Menge liegt); siehe Beispiel 3.6.7.15 sowie Übungsaufgabe 3.6.7.8 und 3.6.7.9. Eine natürliche Verallgemeinerung der Atome wird durch den Begriff des Ultrafilters (siehe Proposition 3.6.8.2) beschrieben. Die Rolle der Atome im vorigen Beweis werden in diesem Abschnitt gewisse Ideale (oder äquivalent: Filter) spielen. Das wird klar, wenn man annimmt, dass bereits eine Einbettung $f\colon B \to \mathfrak{P}(M)$ mit irgendeiner Menge $M$ gefunden ist. Für jedes $m \in M$ ist nämlich die Menge $F_m := \{b \in B \mid m \in f(b)\}$ ein Filter auf $B$, und die Menge $I_m := \{b \in B \mid m \notin f(b)\}$ ist das zugehörige Ideal ($I_m = F_m' = \{b' \mid b \in F_m\}$), da $f(b') = M \setminus f(b)$. Überdies ist $I_m \cup F_m = B$. Jedes Element von $M$ induziert also auf $B$ einen Filter $F_m$, für den $F_m \cup F_m' = B$ gilt (bzw. ein Ideal $I_m$, für das $I_m \cup I_m' = B$ gilt). Unsere Strategie wird daher sein, alle echten Ideale $I \subseteq B$ mit $I \cup I' = B$ zu betrachten, und mit Hilfe dieser Ideale[32] die Menge $M$ zu rekonstruieren. Zu diesem Zweck ist es nützlich und auch

[32] Daher auch der Name: wie die Fernpunkte in der projektiven Geometrie stellen die Ideale sozusagen „ideale“ Elemente dar, die nicht in der Algebra $B$ selbst liegen, wohl aber in der umgebenden Algebra $\mathfrak{P}(M)$. Ein Fernpunkt repräsentiert eine Richtung der affinen Ebene; während ein Fernpunkt in der projektiven Ebene einfach ein Punkt ist, kann man eine Richtung in der Sprache der affinen Ebene nur als komplizierteres Objekt, nämlich als „Klasse paralleler Geraden“ betrachten. Ebenso sind die Filter, die wir in der umgebenden Potenzmengenalgebra verwenden, einfach durch ihre kleinsten Punkte (Singletons) beschrieben, während sie in der ursprünglichen Algebra eine Familie von Elementen darstellen.

erhellend, einige äquivalente Bedingungen zu kennen.
Zur Vorbereitung:

**Anmerkung 3.6.8.1.** Ein Filter $F \subseteq B$ ist genau dann echt (d.h. $F \neq B$), wenn $0 \notin F$. (Aus $0 \in F$ folgt nämlich $x \in F$ für alle $x \in B$, weil für alle $x \in B$ gilt: $0 \leq x$.)

Und nun die angekündigten Äquivalenzen:

**Proposition 3.6.8.2.** *Sei $B$ eine Boolesche Algebra und $F \neq B$ ein echter Filter auf $B$. Dann sind die folgenden Aussagen äquivalent:*

1. *$F$ ist* maximaler Filter*, d.h. der unechte Filter $B$ ist der einzige Filter auf $B$, der $F$ echt umfasst.*
2. *$\forall x \in B : \; x \notin F \;\Rightarrow\; x' \in F$.*
3. *$F$ ist ein* Ultrafilter*: $\forall x \in B : \; x \notin F \;\Leftrightarrow\; x' \in F$.*
   *(Anmerkung: Aus $x \in F$ und $x' \in F$ würde $0 \in F$ folgen, was wir durch die Voraussetzung $F \neq B$ ausgeschlossen haben.)*
4. *$F$ ist ein* Primfilter*: $\forall x, y \in B : \; x \vee y \in F \;\Leftrightarrow\; x \in F$ oder $y \in F$.*
   *(Anmerkung: Die Implikation $\Leftarrow$ gilt für alle Filter. Die zur Äquivalenz duale Eigenschaft gilt für alle Filter: $\forall x, y \in B : \; x \wedge y \in F \quad\Leftrightarrow\quad x \in F$ und $y \in F$.)*
5. *$F$ ist das Urbild der 1 unter einem Epimorphismus von $B$ auf die zweielementige Boolesche Algebra $\{0, 1\}$.*
6. *$B \setminus F$ ist ein Ideal.*
7. *$F' = B \setminus F$.*

*Beweis.* Wir werden nur die Implikationen $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 4 \Rightarrow 2 \Rightarrow 1$, also die Äquivalenz von 1, 2, 3 und 4 zeigen. Die Äquivalenz mit 5, 6 und 7 verbleibt als Übungsaufgabe.
$1 \Rightarrow 2$: Sei $F$ maximal, und $x \in B$, $x \notin F$. Wir wollen $x' \in F$ zeigen.
Wir betrachten die Menge $G := \{b \in B \mid \exists f \in F : x \wedge f \leq b\}$. Offensichtlich gilt $F \cup \{x\} \subseteq G$. Die Menge $G$ ist offensichtlich nach oben abgeschlossen. Überdies ist $G$ ein Filter, denn wenn $x \wedge f_1 \leq b_1$ und $x \wedge f_2 \leq b_2$ mit $f_1, f_2 \in F$ ist, dann gilt mit $f := f_1 \wedge f_2 \in F$ auch die Beziehung $x \wedge f \leq b_1 \wedge b_2$.
Da $F$ maximal war, muss $G = B$ gelten, also insbesondere $0 \in G$. Es gibt also ein $f_0 \in F$ mit $f_0 \wedge x = 0$. Für dieses $f_0$ gilt $f_0 \leq x'$, daher $x' \in F$.
$2 \Rightarrow 3$: Aus $x \notin F$ und Bedingung 2 folgt $x' \in F$. Umgekehrt gilt $x' \in F \Rightarrow x \notin F$, weil nicht $x$ und $x'$ gleichzeitig in $F$ sein können.
$3 \Rightarrow 4$: Unter der Annahme 3 gilt die Äquivalenzkette

$$x \vee y \notin F \;\Leftrightarrow\; (x \vee y)' \in F \;\Leftrightarrow\; x' \wedge y' \in F \;\Leftrightarrow\; x' \in F \text{ und } y' \in F \;\Leftrightarrow\; x \notin F \text{ und } y \notin F.$$

Also gilt auch die Äquivalenz der Negationen: $x \vee y \in F \;\Leftrightarrow\; x \in F$ oder $y \in F$.
$4 \Rightarrow 2$: Sei $F$ Primfilter. Wegen $x \vee x' = 1 \in F$ folgt aus der Annahme $x \notin F$ sofort $x' \in F$.

$2 \Rightarrow 1$: Angenommen, es gibt einen Filter $G$ mit $F \subseteq G$ und $F \neq G$. Zu zeigen ist, dass dann $G = B$ kein echter Filter ist. Sei also $g \in G \setminus F$. Wegen Voraussetzung 2 folgt $g' \in F$ für das Komplement $g'$ von $g$. Wegen $F \subseteq G$ folgt $g' \in G$, wegen der Abgeschlossenheit eines Filter bezüglich $\wedge$ daher auch $0 = g \wedge g' \in G$. Also ist $G$ kein echter Filter. □

**UE 266** ▶ **Übungsaufgabe 3.6.8.3.** (V) Beweisen Sie die ausständigen Implikationen aus Proposition 3.6.8.2. ◀ **UE 266**

Von den verschiedenen Bezeichnungen aus Proposition 3.6.8.2 werden wir am häufigsten *Ultrafilter* verwenden. Vereinfacht ausgedrückt konnten wir für endliche Boolesche Algebren in Lemma 3.6.7.5 zeigen, dass es „genügend" Atome gibt. Daher stellt sich nun die Frage, ob auch im Fall allgemeiner Boolescher Algebren „genügend" Ultrafilter existieren; d.h. ob der Begriff des Ultrafilters eine passende Verallgemeinerung des Atombegriffs ist. Dass dies tatsächlich der Fall ist, zeigt der sogenannte Ultrafiltersatz. Für den Beweis verweisen wir auf 11.3.4.2 im Anhang.

**Satz 3.6.8.4** (Ultrafiltersatz)**.** *Sei $B$ eine Boolesche Algebra und $F_0$ ein echter Filter auf $B$. Dann gibt es einen echten Ultrafilter $U$ mit $F_0 \subseteq U \subseteq B$.*

Das folgende Lemma ist lediglich eine Umformulierung von Proposition 3.6.8.2. Wir schreiben es extra an, um die Analogie zwischen Ultrafiltern und Atomen hervorzuheben; vergleiche dazu Lemma 3.6.7.2.

**Lemma 3.6.8.5** (Rechenregeln für Ultrafilter)**.** *Sei $B$ Boolesche Algebra, $F \subseteq B$ ein Ultrafilter. Dann gilt für alle $b, c \in B$:*

*(U2) $b' \in F$ genau dann, wenn $b \notin F$.*

*(U3) $b \wedge c \in F$ genau dann, wenn $b \in F$ und $c \in F$.*

*(U4) $b \vee c \in F$ genau dann, wenn $b \in F$ oder $c \in F$.*

Die Begriffe *maximales Ideal* und *Primideal* sind analog definiert. Insbesondere heißt ein echtes Ideal *Primideal*, wenn $\forall x, y \in B: \; x \wedge y \in I \;\Leftrightarrow\; x \in I$ oder $y \in I$ gilt.

**UE 267** ▶ **Übungsaufgabe 3.6.8.6.** (D) Untersuchen Sie die Beziehung des Begriffs *Primideal* im Kontext von Booleschen Algebren wie im Kontext von Ringen. ◀ **UE 267**

**Beispiele 3.6.8.7.**

(1) Sei $B$ eine Boolesche Algebra, und sei $a \in B$ ein Atom. Dann ist die Menge $\{x \in B \mid a \leq x\}$ ein Primfilter und Ultrafilter. (In Analogie zur Terminologie bei Ringen heißen Filter von der Form $\{x \in B \mid b_0 \leq x\} = \{x \vee b_0 \mid x \in B\}$ auch *Hauptfilter*, und Ideale der Form $\{x \in B \mid x \leq c_0\} = \{x \wedge c_0 \mid x \in B\}$ auch *Hauptideale*[33]) mit $b_0$ bzw. $c_0$ als *erzeugendem Element*. Das erzeugende

[33] englisch: *principal filter*, *principal ideal* (Achtung! „principal", nicht „principle")

Element eines Hauptfilters $F$ ist eindeutig bestimmt: Denn wenn $b_0$ und $b_1$ beide $F$ erzeugen, dann liegt auch $b := b_0 \wedge b_1 \leq b_0, b_1$ in $F$ und muss nach Definition von $F_{b_0} = F_{b_1} = F$ gleichzeitig $b \geq b_0, b_1$ erfüllen, also $b_0 = b = b_1$. Ein Ultrafilter, der kein Hauptfilter ist, heißt auch ein *freier Ultrafilter*.

(2) Sei $B = \mathfrak{P}(\mathbb{N})$. Sei $I$ die Menge aller endlichen Teilmengen von $\mathbb{N}$, $F = I'$ die Menge aller ko-endlichen Mengen.
Dann ist $F$ zwar Filter (und $I$ Ideal) auf $B$, aber $F$ ist kein Ultrafilter.

(3) Seien $B$, $I$, $F$ wie in (2). Sei nun $B_0 := I \cup F$. $B_0$ ist Unteralgebra von $\mathfrak{P}(\mathbb{N})$. $I$ und $F$ sind Ideal bzw. Filter auf $B_0$; tatsächlich ist $F$ sogar maximaler Filter (Ultrafilter) auf $B_0$, und $I$ ist maximales Ideal (Primideal) auf $B_0$.

**UE 268 ► Übungsaufgabe 3.6.8.8.** (D) Untersuchen Sie die Beziehung des Begriffs *Hauptideal* im Kontext von Booleschen Algebren wie im Kontext von Ringen. **◄ UE 268**

Der Fall endlicher Boolescher Algebren verdient in Hinblick auf Filter und Ultrafilter extra Beachtung:

**Proposition 3.6.8.9.** *In einer endlichen Booleschen Algebra $B$ ist jeder Filter $F$ ein Hauptfilter, d.h. von der Form $F = F_b := \{x \in B : \ b \leq x\}$ mit eindeutig bestimmtem $b \in B$. Somit ist die Zuordnung $b \mapsto F_b$ eine Bijektion zwischen $B$ und der Menge aller Filter auf $B$. Dabei gilt $b_1 \leq b_2$ genau dann, wenn $F_{b_2} \subseteq F_{b_1}$ gilt. $F_b$ ist genau dann ein Ultrafilter, wenn $b$ ein Atom ist. Somit ist die Zuordnung $a \mapsto F_a$ eine Bijektion zwischen der Menge* $\mathrm{At}(B)$ *der Atome von $B$ und der Menge aller Ultrafilter von $B$.*

*Beweis.*

- Jeder Filter $F$ ist ein Hauptfilter $F_b$ mit eindeutig bestimmtem $b$: Als Teilmenge von $B$ ist auch $F$ endlich. Daher ist $b := \bigwedge_{x \in F} x$ wohldefiniert. Nach Definition gilt $F \subseteq \{x \in B \mid b \leq x\} = F_b$. Um umgekehrt $F_b \subseteq F$ zu zeigen, beobachten wir zunächst, dass $b$ in $F$ liegt, da $F$ unter $\wedge$ abgeschlossen ist. Weil $F$ auch nach oben abgeschlossen ist, folgt $F_b \subseteq F$.

  Die Eindeutigkeit von $b$ haben wir bereits im ersten Unterpunkt von Beispiel 3.6.8.7 nachgewiesen.

- Für $b_1, b_2 \in B$ gilt $b_1 \leq b_2$ genau dann, wenn $F_{b_2} \subseteq F_{b_1}$: Die Implikation von links nach rechts ist klar, für die umgekehrte Richtung ist nur zu bemerken, dass $F_{b_2} \subseteq F_{b_1}$ jedenfalls $b_2 \in F_{b_1}$ nach sich zieht.

- $F_b$ ist genau dann ein Ultrafilter, wenn $b$ ein Atom ist: Sei $F_b$ ein Ultrafilter. Da $0 \neq b$ (als Ultrafilter ist $F_b$ nach Definition ein echter Filter) und jedenfalls $0 \leq b$ gilt, erhalten wir $0 < b$. Für $0 < b' \leq b$ folgt $F_{b'} \supseteq F_b$ nach dem bereits Bewiesenen, also $F_{b'} = F_b$, weil $F_b$ ein Ultrafilter ist. Daraus folgt $b \leq b'$, also insgesamt $b = b'$. Somit ist $b$ als Atom nachgewiesen.

  Sei umgekehrt $b$ ein Atom. Für einen echten Filter $F' \supseteq F_b$ gibt es nach dem ersten Punkt ein Element $b' \in B$ mit $F' = F_{b'}$. Da $F'$ ein echter Filter ist, gilt

dabei $0 < b'$. Aus $F_{b'} \supseteq F_b$ folgt $b' \leq b$. Da $b$ ein Atom ist, erhalten wir $b' = b$ und weiter $F' = F_{b'} = F_b$. Folglich ist $F_b$ ein Ultrafilter.

□

**UE 269** ► **Übungsaufgabe 3.6.8.10.** (W) Sei $B$ eine unendliche Boolesche Algebra. Zeigen Sie, dass es einen Ultrafilter gibt, der kein Atom enthält. (Hinweis: Zeigen Sie, dass die Menge $I$ aller $b \in B$, zu denen es Atome $a_1, \ldots, a_k$ von $B$ mit $b \leq a_1 \vee \cdots \vee a_k$ gibt, ein echtes Ideal von $B$ ist, und betrachten Sie $B/I$.) ◄ **UE 269**

**UE 270** ► **Übungsaufgabe 3.6.8.11.** (B) Sei $B$ die Menge aller endlichen und ko-endlichen Teilmengen der natürlichen Zahlen. Finden Sie alle Ultrafilter auf $B$. ◄ **UE 270**

Eine Hauptrolle im Beweis des Satzes von Stone spielen Funktionen auf einer Booleschen Algebra $B$, die nur zwei Werte, aufgefasst als 0 und 1 in einer zweielementigen Booleschen Algebra, annehmen. Solche Funktionen sind eindeutig bestimmt durch ihren Träger $A \subseteq B$, der Menge, auf der der Wert 1 angenommen wird. Man spricht von einer *charakteristischen Funktion*, für die wir $\chi_A$ schreiben.
Die Rechenregeln aus Lemma 3.6.8.5 liefern unmittelbar die folgende entscheidende Tatsache:

**Lemma 3.6.8.12.** *Sei $B$ Boolesche Algebra, $F \subseteq B$ ein Ultrafilter. Dann ist die Abbildung $\chi_F : B \to \{0,1\}$ ein Boolescher Homomorphismus von $B$ in die zweielementige Boolesche Algebra $\{0,1\}$.*

Damit haben wir alle Vorarbeiten für den Beweis des Darstellungssatzes von Stone geleistet.

**Satz 3.6.8.13.** *[Darstellungssatz von Stone] Sei $(B, \wedge, \vee, 0, 1, ')$ eine Boolesche Algebra. Dann gibt es eine Menge $M$ und ein $\mathcal{B} \subseteq \mathfrak{P}(M)$, sodass $(B, \wedge, \vee, 0, 1, ') \cong (\mathcal{B}, \cap, \cup, \emptyset, M, ')$.*
*Zusatz: Ist $B$ endlich, so kann $\mathcal{B}$ als Potenzmenge von $\mathrm{At}(B)$, der Menge der Atome von $B$, gewählt werden. Jede endliche Boolesche Algebra ist also isomorph zu einer Potenzmengenalgebra über einer endlichen Menge, also von einer Kardinalität $2^n$ mit einem $n \in \mathbb{N}$.*

*Beweis.* Sei $B$ eine beliebige Boolesche Algebra. Wir betrachen die Menge

$$\mathcal{U} = \{F \subseteq B : F \text{ ist Ultrafilter}\}$$

und die Abbildung

$$f\colon \begin{cases} B \to \{0,1\}^{\mathcal{U}} \\ b \mapsto (\chi_F(b))_{F \in \mathcal{U}} \end{cases}$$

Zunächst behaupten wir, dass $f$ ein boolescher Homomorphismus ist; wenn wir mit $\pi_F : \{0,1\}^{\mathcal{U}} \to \{0,1\}$ die Projektion auf die $F$-Koordinate bezeichnen, so genügt es, wie man sich sofort überlegt, nachzurechnen, dass $\pi_F \circ f$ für alle $F$ ein Homomorphismus ist. Letzteres ist klar, weil $\pi_F \circ f = \chi_F$ gilt.
Für die erste Behauptung des Satzes ist noch die Injektivität von $f$ zu zeigen, d.h. $f(a) \neq f(b)$ für $a \neq b$. Nach Definition von $f$ ist dafür ein Ultrafilter $F$ zu finden, der eines der beiden Elemente enthält und das andere nicht. Dazu beobachten wir, dass aus $a \wedge b' = 0$ die Gleichung

$$a = a \wedge 1 = a \wedge (b \vee b') = (a \wedge b) \vee (a \wedge b') = (a \wedge b) \vee 0 = a \wedge b$$

und somit $a \leq b$ folgt. Analog folgt $a \geq b$ aus $a' \wedge b = 0$. Für $a \neq b$ muss also wenigstens eines der beiden Elemente $a \wedge b'$ und $a' \wedge b$ von 0 verschieden sein, oBdA $c := a \wedge b' \neq 0$. Nach dem Ultrafiltersatz 3.6.8.4 folgt, dass sich der von $c \in B \setminus \{0\}$ erzeugte Hauptfilter $\{x \in B : x \geq c\}$ zu einem Ultrafilter $F \in \mathcal{U}$ fortsetzen lässt. Wegen $c \in F$ und $c = a \wedge b' \leq a, b'$ liegen $a$ und $b' \in F$, also nicht $b$ (siehe Proposition 3.6.8.2). $F$ hat also die gewünschte Eigenschaft. Somit ist $f\colon B \to \{0,1\}^{\mathcal{U}}$ eine isomorphe Einbettung der Booleschen Algebra $B$ in die Boolesche Algebra $\{0,1\}^{\mathcal{U}}$, die wiederum in kanonischer Weise isomorph ist zur Potenzmengenalgebra $\mathfrak{P}(\mathcal{U})$. (Jeder Teilmenge wird ihre charakteristische Funktion zugeordnet.) Damit ist die erste Aussage des Satzes gezeigt.

Für den Zusatz betreffend endliches $B$ erinnern wir uns an Proposition 3.6.8.9. Demnach ist im endlichen Fall ein Filter genau dann ein Ultrafilter, wenn $F = F_a = \{x \mid a \leq x\}$ für ein Atom $a$ ist. Es genügt somit, wenn wir zeigen können, dass die oben definierte Abbildung $f$ surjektiv auf $\{0,1\}^{\mathcal{U}}$ ist. Dazu werden wir zu jeder Menge $T \subseteq \mathrm{At}(B)$ von Atomen von $B$ ein Element $b = b_T \in B$ finden, für das $\chi_{F_a}(b) = 1$ für $a \in T$ und $\chi_{F_a}(b) = 0$ für $a \in \mathrm{At}(B) \setminus T$ gilt. Und zwar behaupten wir, dass für $T = \{a_1, \ldots, a_k\}$ das Element $b := a_1 \vee \ldots \vee a_k$ diese Eigenschaft hat. Aus $b \geq a_i$ folgt $b \in F_{a_i}$ für alle $i = 1, \ldots, k$, also tatsächlich $\chi_{F_a}(b) = 1$ für alle $a \in T$. Sei nun $a \in \mathrm{At}(B) \setminus T$. Weil es sich um Atome handelt, gilt dann $a_i \wedge a = 0$ für alle $a_i \in T$ und somit

$$b \wedge a = (a_1 \vee \ldots \vee a_k) \wedge a = (a_1 \wedge a) \vee \ldots \vee (a_k \wedge a) = 0.$$

Es gilt also nicht $b \geq a$, d.h. $b$ liegt nicht in $F_a$. Also gilt $\chi_{F_a}(b) = 0$ für alle $a \in \mathrm{At}(B) \setminus T$, und der Satz ist bewiesen. □

**Korollar 3.6.8.14.** Jede Boolesche Algebra $B$ ist isomorph zu einem subdirekten Produkt der zweielementigen Booleschen Algebra, d.h.

$$B \leq \prod_{F \in \mathcal{U}} \{0,1\}.$$

Jedes Gesetz, welches in der Booleschen Algebra $\{0,1\}$ mit den Operationen

| $\wedge$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

| $\vee$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 1 |

| $'$ | |
|---|---|
| 0 | 1 |
| 1 | 0 |

gilt, muss daher in allen Booleschen Algebren gelten.

# 4 Universelle Konstruktionen in Varietäten

In Varietäten gibt es weitreichende Möglichkeiten, Algebren zu konstruieren, die gewisse vorgegebene Strukturen enthalten und unter dieser Bedingung als universelle Objekte aufgefasst werden können. Hier beschäftigen uns vor allem freie Algebren (die eine vorgegebene Menge von Variablen enthalten), siehe Abschnitt 4.1, Koprodukte (die, etwas ungenau gesprochen, alle Algebren einer vorgegebenen Familie enthalten) und Polynomalgebren (Koprodukt einer vorgegebenen mit einer freien Algebra), siehe Abschnitt 4.2.

## 4.1 Freie Algebren und der Satz von Birkhoff

Wir kennen bereits den Begriff der Varietät, also einer gleichungsdefinierten Klasse von Algebren. Diese Definition ist nach dem Vorbild der bekannten Beispiele aus der klassischen Algebra (Halbgruppen, Gruppen, etc.) gebildet. Neben dieser syntaktischen Beschreibung drängt sich aus algebraischer Sicht auch die Frage nach einer semantischen Charakterisierung auf, also nach strukturellen Eigenschaften, die unter allen Klassen von Algebren genau die Varietäten auszeichnen. Diese Frage wird vom Satz von Birkhoff beantwortet, wonach die Abgeschlossenheit unter den grundlegenden Konstruktionen (Unteralgebren, direkte Produkte und homomorphe Bilder/Faktoralgebren) entscheidend ist, wie in 4.1.1 motiviert wird. Eine gemeinsame Eigenschaft von Vektorräumen, universellen Termalgebren und freien Halbgruppen dient in 4.1.2 als Vorbild für die allgemeine Definition einer freien Algebra in einer Varietät bzw. eines freien Objekts in einer konkreten Kategorie. In 4.1.3 wird für eine vorgegebene Varietät die freie Algebra über einer beliebigen Variablenmenge konstruiert. Das wichtigste Beispiel, die freie Gruppe, ist Gegenstand von 4.1.4. Die freie Boolesche Algebra wird in 4.1.5 behandelt. Eine alternative, vielleicht abstrakter anmutende Konstruktion gelingt in 4.1.6 mit Hilfe subdirekter Produkte. Der Vorteil besteht darin, dass dabei nur die Abgeschlossenheit von Varietäten bezüglich Unteralgebren, direkter Produkte und homomorpher (hier genügt sogar: isomorpher) Bilder verwendet wird. Denn damit gelingt in 4.1.7 der Beweis des Satzes von Birkhoff.

### 4.1.1 Motivation

Inhalt in Kurzfassung: Motivation des Satzes von Birkhoffs, des Hauptergebnisses dieses Abschnitts.

**Definition 4.1.1.1.** Für eine Klasse $\mathcal{K}$ von Algebren sei

- $\mathsf{I}\mathcal{K}$ die Klasse aller Algebren $\mathfrak{A}$, die zu einer Algebra $\mathfrak{A}' \in \mathcal{K}$ isomorph sind.

- $\mathsf{H}\mathcal{K}$ Klasse aller Algebren $\mathfrak{A}$, die homomorphes Bild einer Algebra $\mathfrak{A}' \in \mathcal{K}$ sind.
- $\mathsf{S}\mathcal{K}$ die Klasse aller Algebren $\mathfrak{A}$, die zu einer Unteralgebra einer Algebra $\mathfrak{A}' \in \mathcal{K}$ isomorph sind.
- $\mathsf{P}\mathcal{K}$ die Klasse aller Algebren $\mathfrak{A}$, die zu einem Produkt[1] von Algebren aus $\mathcal{K}$ isomorph sind.

Offensichtlich ist $\mathcal{K}$ in jeder der Klassen $\mathsf{I}\mathcal{K}$, $\mathsf{H}\mathcal{K}$, $\mathsf{S}\mathcal{K}$ und $\mathsf{P}\mathcal{K}$ enthalten. Wir sagen, dass $\mathcal{K}$ unter $\mathsf{H}$ abgeschlossen ist, wenn sogar $\mathcal{K} = \mathsf{H}\mathcal{K}$ gilt, analog für $\mathsf{S}$, $\mathsf{P}$, $\mathsf{I}$.

Nach Proposition 2.3.1.3 sowie den Folgerungen 2.3.2.10 und 2.3.3.21 gilt

**Proposition 4.1.1.2.** *Gesetze im Sinne von Definition 2.1.8.6 vererben sich auf Unteralgebren, direkte Produkte und auf homomorphe Bilder. Wenn $\mathcal{K}$ eine Varietät ist, dann gilt also: $\mathcal{K} = \mathsf{H}\mathcal{K} = \mathsf{S}\mathcal{K} = \mathsf{P}\mathcal{K}$.*

Es gilt aber auch die Umkehrung: Jede unter $\mathsf{H}, \mathsf{S}, \mathsf{P}$ abgeschlossene Klasse ist von der Form $\mathcal{V}(\Gamma)$ für eine geeignete Menge $\Gamma$ von Gesetzen. (Satz von Birkhoff, siehe Satz 4.1.7.1) Der Beweis dieses Satzes ist eines der wichtigsten Ziele dieses Kapitels.

**UE 271** ► **Übungsaufgabe 4.1.1.3.** (F) Man zeige, dass sich folgende Klassen von Algebren als Varietäten auffassen lassen: Halbgruppen, Monoide, Gruppen, (kommutative) Ringe (mit 1), Verbände, Boolesche Algebren, Vektorräume über einem festen Körper $K$, (unitäre) Moduln über einem festen Ring $R$. ◄ **UE 271**

**UE 272** ► **Übungsaufgabe 4.1.1.4.** (F+) Man zeige, dass sich folgende Klassen von Algebren nicht als Varietäten auffassen lassen: Integritätsbereiche, Körper, endliche Gruppen. ◄ **UE 272**

Im Beweis des Satzes von Birkhoff spielt der Begriff der freien Algebra eine zentrale Rolle.

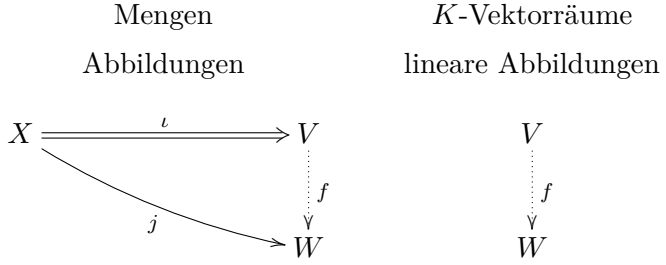
### 4.1.2 Bekannte Beispiele und Definition einer freien Algebra

Inhalt in Kurzfassung: Der aus der Linearen Algebra bekannte Satz von der linearen Fortsetzbarkeit von Abbildungen, die zunächst nur auf einer Basis eines Vektorraums definiert sind, die bereits in 3.1.2 behandelte freie Halbgruppe und die universelle Eigenschaft der Termalgebra aus 2.1.8.1 sind Beispiele für ein uns denselben allgemeinen Begriff: den der freien Algebra. Die Definition ist sowohl in der Sprache der universellen Algebra als auch, noch allgemeiner, in jener der Kategorientheorie (freies Objekt) möglich. Freie Objekte in einer Kategorie sind nach Definition initiale Objekte in einer geeignet angepassten anderen Kategorie. Daraus folgt, dass sie bis auf Isomorphie

[1] Wir erlauben hier beliebige Indexmengen, insbesondere auch unendliche Mengen sowie die leere Menge. Das leere Produkt $\prod_{i\in I} A_i$ wird als die einelementige Menge $\{\emptyset\}$ definiert, die nur das leere $\emptyset$-Tupel enthält; diese Algebra ist definitionsgemäß immer in $\mathsf{P}\mathcal{K}$ enthalten, sogar wenn $\mathcal{K}$ leer ist.

eindeutig bestimmt sind. Der Unterabschintt schließt mit einigen einfachen Beispielen, meist in Form von Übungsaufgaben.

Wir beginnen mit einer wohlbekannten Eigenschaft von Vektorräumen, Termalgebren und der freien Halbgruppe, aus der wir dann die Definition einer freien Algebra in einer Klasse von Algebren bzw. eines freien Objektes in einer konkreten Kategorie abstrahieren.
Sei $V$ ein Vektorraum über einem Körper $K$ und $X$ eine Basis von $V$. Dann gibt es zu jedem Vektorraum $W$ über $K$ und jedem $j\colon X \to W$ eine eindeutige lineare Abbildung $f\colon V \to W$, die $j$ fortsetzt. Denken wir uns $X$ vermittels $\iota\colon X \to V$ in $V$ eingebettet, lässt sich die Fortsetzungseigenschaft auch durch die Bedingung $f \circ \iota = j$ ersetzen. Im Sinne der nachfolgenden Definition 4.1.2.1 lässt sich daher sagen: Jeder Vektorraum $V$ ist frei über jeder Basis $X$ bzw. $V$ ist frei über $(X, \iota)$. Schematisch als Diagramm:




Ganz ähnlich verhält es sich mit der freien Halbgruppe aus 3.1.2. Bezeichne $F(X)$ die freie Halbgruppe über der Variablenmenge $X$, realisiert als Menge aller Zeichenketten $x_1 \dots x_n$ mit $x_i \in X$ und der Konkatenation (Aneinanderreihung) von Zeichenketten als binärer Operation. Dann gibt es zu jeder Halbgruppe $H$ und jeder Variablenbelegung $j\colon X \to H$ genau einen Halbgruppenhomomorphismus $f$ mit $f(x) = j(x)$ für alle $x \in X$. Bezeichnen wir mit $\iota\colon X \to F(X)$ jene Abbildung, die jedem $x \in X$ die Zeichenkette aus $F(X)$ zuordnet, die nur aus dem einen Zeichen $x$ besteht, so bedeutet dies $f \circ \iota = j$. Die schematische Darstellung entspricht derjenigen oben für Vektorräume, lediglich mit folgenden Ersetzungen: An die Stelle der $K$-Vektorräume treten die Halbgruppen, an die Stelle der linearen Abbildungen die Halbgruppenhomomorphismen, $V$ ist durch $F(X)$ zu ersetzen und $W$ durch $H$. Im Sinne von Definition 4.1.2.1 bedeutet das: $F(X)$ ist frei über $X$ bzw. über $(X, \iota)$ in der Klasse der Halbgruppen.

Ein drittes Beispiel ist die Termalgebra aus 2.1.8.1. Sei dazu $\mathcal{K}$ die Klasse aller Algebren eines fixen Typs $\tau = (n_i)_{i \in I}$. Dann hat die Termalgebra $\mathfrak{T}(X) \in \mathcal{K}$ in den Variablen $X$ die folgende Eigenschaft: Zu jeder Algebra $A \in \mathcal{K}$ und jeder Variablenbelegung $j\colon X \to A$ gibt es einen eindeutigen Homomorphismus $f\colon \mathfrak{T}(X) \to A$ (den Einsetzungshomomorphismus) mit $f(x) = j(x)$ für alle $x \in X$ bzw. mit $f \circ \iota = j$ für jenes $\iota\colon X \to \mathfrak{T}(X)$, das der Variablen $x \in X$ den Term $x \in \mathfrak{T}(X)$ zuordnet. Im Diagramm oben tritt $\mathcal{K}$ an die Stelle der Klasse aller $K$-Vektorräume (bzw. Halbgruppen), lineare Abbildungen werden zu Homomorphismen in $\mathcal{K}$, $V$ bzw. $F(X)$ zu $\mathfrak{T}(X)$ und $W$ bzw. $H$ zu $A$. Im Sinne von Definition 4.1.2.1 bedeutet das: $\mathfrak{T}(X)$ ist frei über $X$ bzw. über $(X, \iota)$ in $\mathcal{K}$.

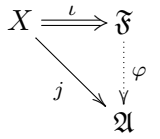
Die Termalgebra $\mathfrak{T}(X)$ heißt manchmal auch die (bezüglich des Typs $\tau$) *absolut freie Algebra* über $X$.

Wir verallgemeinern zur Definition freier Algebren innerhalb einer beliebigen Klasse von Algebren desselben Typs:

**Definition 4.1.2.1.** Sei

- $\mathcal{K}$ eine Klasse von Algebren gleichen Typs,
- $\mathfrak{F} = (F, (\omega_i)_{i\in I})$ in $\mathcal{K}$,
- $X$ eine Menge
- und $\iota\colon X \to F$ eine Funktion.

$\mathfrak{F}$ heißt *frei* über $(X, \iota)$ in $\mathcal{K}$, wenn für alle $\mathfrak{A} \in \mathcal{K}$ mit Trägermenge $A$ und für alle $j\colon X \to A$ ein eindeutiger Homomorphismus $\varphi$ mit $j = \varphi \circ \iota$ existiert.




Im Folgenden werden wir meist nur den Fall $X \subseteq F$ und $\iota = \mathrm{id}_X$ betrachten. Statt „$\mathfrak{F}$ ist frei in $\mathcal{K}$ über $(X, \mathrm{id}_X)$“ schreiben wir dann nur „$\mathfrak{F}$ ist frei in $\mathcal{K}$ über $X$“. $\mathfrak{F}$ heißt *frei* in $\mathcal{K}$, wenn es eine Menge $X$ gibt, sodass $F$ frei über $X$ in $\mathcal{K}$ ist.

Eine Bemerkung zu den graphisch verschieden gestalteten Pfeilen in obigem Diagramm: Die Pfeile mit dem dicken Schaft beziehen sich auf Abbildungen des gegebenen Objektes (hier: $\iota$). Die einfachen aber durchgängig gezeichneten Pfeile gehören zu Abbildungen, vor denen ein Allquantor zu denken ist (hier: $\forall j$). Der punktierte Pfeil bezeichnet eine Abbildung (hier: $\varphi$), deren Existenz und eventuell Eindeutigkeit behauptet wird.

Statt „$\mathcal{F}$ ist in $\mathcal{K}$ frei über $X$“ sagt man auch „$\mathcal{F}$ ist in $\mathcal{K}$ von $X$ frei erzeugt“; dies wird durch das folgende Lemma gerechtfertigt.

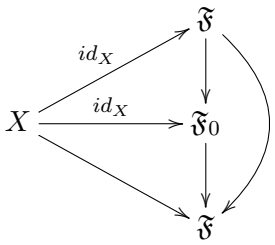
**Lemma 4.1.2.2.** *Sei $\mathcal{K}$ eine Klasse von Algebren des gleichen Typs, die $\mathsf{S}\mathcal{K} = \mathcal{K}$ erfüllt. (Z.B. erfüllt jede Varietät diese Bedingung.) Sei $\mathfrak{F} \in \mathcal{K}$ eine Algebra mit Grundmenge $F$. Sei $X \subseteq F$. Die Algebra $\mathfrak{F}$ ist genau dann frei über $X$, wenn gilt:*

(1) *Für alle Algebren $\mathfrak{A} \in \mathcal{K}$ mit Trägermenge $A$ und alle Funktionen $j\colon X \to A$ gibt es* mindestens *einen Homomorphismus $\varphi\colon \mathfrak{F} \to \mathfrak{A}$, der $j$ fortsetzt.*

(2) *Die Algebra $\mathfrak{F}$ wird von $X$ erzeugt, das heißt: Es gibt keine echte Unteralgebra von $\mathfrak{F}$, die die Menge $X$ enthält.*

**Anmerkung 4.1.2.3.** Eine analoge Aussage gilt auch, wenn $\mathfrak{F}$ nicht frei über $X$ (d.h.: frei über $(X, \mathrm{id}_X)$) ist, sondern frei über $(X, \iota)$. Bedingung (1) ist dann abzuändern zu „... Homomorphismus $\varphi : \mathfrak{F} \to \mathfrak{A}$ mit $\varphi \circ \iota = j$“ und Bedingung (2) zu „$\mathfrak{F}$ wird von $\iota(X)$ erzeugt“.

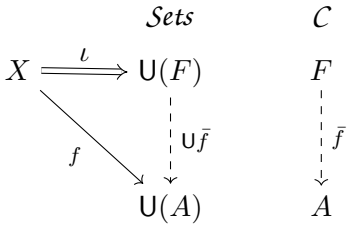
**UE 273** ► **Übungsaufgabe 4.1.2.4.** (A) Beweisen Sie Lemma 4.1.2.2. Hinweis: Die eine Richtung ergibt sich aus Proposition 2.3.1.16. Für die andere Richtung: finden Sie sinnvolle Namen und Eigenschaften der Pfeile im folgenden Diagramm: ◄ **UE 273**




Im Folgenden werden wir nur Klassen von Algebren betrachten, die unter Unteralgebren abgeschlossen sind. In solchen Klassen muss man also statt der Eindeutigkeit des gesuchten Homomorphismus nur nachprüfen, dass die angeblich freie Algebra $\mathfrak{F}$ tatsächlich von der angegebenen Menge $X$ erzeugt wird. Man beachte, dass dies oft leichter nachzuprüfen ist, da man nur die Algebra $\mathfrak{F}$ und nicht alle Algebren $\mathfrak{A} \in \mathcal{K}$ untersuchen muss.

Noch allgemeiner ist die Definition freier Objekte in konkreten Kategorien.

**Definition 4.1.2.5.** Sei $\mathcal{C}$ eine konkrete Kategorie mit Funktor $\mathsf{U}\colon \mathcal{C} \to \mathcal{S}ets$, $F \in Ob(\mathcal{C})$, $X$ eine Menge und $\iota \in \mathrm{Hom}_{\mathcal{S}ets}(X, \mathsf{U}(F))$.[2] $F$ heißt *frei* über $X$ (bezüglich $\iota$), i.Z. $F = F(X)$, wenn gilt: Für alle Objekte $A \in Ob(\mathcal{C})$ und alle Morphismen $f \in \mathrm{Hom}_{\mathcal{S}ets}(X, \mathsf{U}(A))$ gibt es einen eindeutigen Morphismus $\overline{f} \in \mathrm{Hom}_{\mathcal{C}}(F, A)$ mit $f = (\mathsf{U}\overline{f})\iota$ in $\mathcal{S}ets$. Das heißt also, dass das folgende Diagramm kommutiert.




Offensichtlich lässt sich die definierende Eigenschaft freier Objekte als universelle Eigenschaft in einer geeigneten Kategorie interpretieren. Dazu gehen wir wie in Definition 4.1.2.5 aus von einer Kategorie $\mathcal{C}$ und einer Menge $X$. Wir betrachten eine neue Kategorie, die wir mit $\mathcal{C}(X)$ bezeichnen. Ihre Objekte seien sämtliche Paare $(\mathfrak{A}, \iota)$, wobei $\mathfrak{A}$ ein Objekt in $\mathcal{C}$ mit „Trägermenge“ $A = \mathsf{U}(\mathfrak{A})$ und $\iota\colon X \to A$ eine Funktion sei. Die Morphismen $f\colon (\mathfrak{A}_1, \iota_1) \to (\mathfrak{A}_2, \iota_2)$ seien jene Morphismen $f\colon \mathfrak{A}_1 \to \mathfrak{A}_2$ in $\mathcal{C}$, die zusätzlich mit den $\iota_i$ verträglich sind, d.h. $\mathsf{U}(f) \circ \iota_1 = \iota_2$ erfüllen. Die Komposition in $\mathcal{C}(X)$ sei wie üblich die Abbildungskomposition. Dann besagt Definition 4.1.2.5 nichts anderes, als

[2] $\iota$ ist also eine gewöhnliche Abbildung von der Menge $X$ in die Trägermenge von $F$.

dass das dortige Paar $(F, \iota)$ ein initiales, insbesondere also universelles Objekt in $\mathcal{C}(X)$ ist. Nach Satz 2.2.3.2 sind universelle Objekte eindeutig bis auf Äquivalenz. Im Fall, dass $\mathcal{C}$ eine Varietät ist, bedeutet Äquivalenz in $\mathcal{C}$ erst recht Isomorphie in $\mathcal{C}$. Somit haben wir bewiesen:

**Satz 4.1.2.6.** *Freie Algebren sind in Varietäten (allgemeiner: in Klassen von Algebren gleichen Typs) bis auf Isomorphie eindeutig bestimmt. Genauer:*
*Sind $\mathcal{K}$ eine Klasse von Algebren gleichen Typs, $X$ eine Menge, $(\mathfrak{F}_1, \iota_1)$ frei in $\mathcal{K}$ über $(X, \iota_1)$ und $(\mathfrak{F}_2, \iota_2)$ frei in $\mathcal{K}$ über $(X, \iota_2)$. Dann sind $\mathfrak{F}_1$ und $\mathfrak{F}_2$ isomorph. Der Isomorphismus $\varphi\colon \mathfrak{F}_1 \to \mathfrak{F}_2$ kann so gewählt werden, dass $\iota_2 = \varphi \circ \iota_1$ gilt.*

**UE 274** ► **Übungsaufgabe 4.1.2.7.** (F) Sei $(S, +, 0, -, \cdot, 1)$ ein beliebiger Ring mit 1. Dann gibt es bekanntlich genau einen $\mathcal{Rng}_1$-Homomorphismus $f\colon \mathbb{Z} \to S$. Deuten Sie diese Aussage als eine über eine freie Algebra. ◄ **UE 274**

**Beispiel 4.1.2.8.** Sei $\mathcal{AbMon}$ die Klasse aller abelschen Monoide, $k \geq 0$. Dann ist $\mathbb{N}^k$ in $\mathcal{AbMon}$ frei über der $k$-elementigen Menge $B_k := \{b_1 := (1, 0, \ldots, 0), \ldots, b_k := (0, \ldots, 0, 1)\}$ der kanonischen Einheitsvektoren.

*Beweis.* Sei $(M, +, 0, -)$ ein beliebiges abelsches Monoid und sei $j\colon B_k \to M$.
Dann ist die durch[3]

$$\varphi(n_1, \ldots, n_k) := \sum_{i=1}^{k} n_i j(b_i)$$

definierte Abbildung ein Homomorphismus $\varphi : \mathbb{N}^k \to M$ (nachrechnen!), der $j$ fortsetzt. Umgekehrt muss jeder Homomorphismus $\varphi'\colon \mathbb{N}^k \to M$, der $j$ fortsetzt, $\varphi'(nb_i) = n\varphi'(b_i) = nj(b_i)$ erfüllen, folglich auch

$$\varphi'(n_1, \ldots, n_k) = \varphi'\left(\sum_{i=1}^{k} n_i b_i\right) = \sum_{i=1}^{k} n_i j(b_i).$$

□

Ganz analog verhält es sich bei abelschen Gruppen:

**Beispiel 4.1.2.9.** Sei $\mathcal{Ab}$ die Klasse aller abelschen Gruppen, $k \geq 0$. Dann ist $\mathbb{Z}^k$ in $\mathcal{Ab}$ frei über der $k$-elementigen Menge $B_k := \{(1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)\}$ der Einheitsvektoren. Man beachte die Analogie zwischen abelschen Gruppen und Vektorräumen.

**UE 275** ► **Übungsaufgabe 4.1.2.10.** (F+) Beschreiben Sie freie Objekte über einer beliebigen vorgegebenen Menge $X$ in der Kategorie $\mathcal{AbMon}$ der abelschen Monoide und in der Kategorie $\mathcal{Ab}$ der abelschen Gruppen. ◄ **UE 275**

[3] $n_i j(b_i)$ ist die $n_i$-fache additiv geschriebene Potenz von $j(b_i)$.

In 4.1.3 werden wir sehen, dass es in Varietäten freie Algebren in Hülle und Fülle gibt. In der Klasse der Körper ist das nicht der Fall. Die folgende Übungsaufgabe soll dies illustrieren.

**UE 276 ► Übungsaufgabe 4.1.2.11.** (F+) **◄ UE 276**

1. Sei $\mathcal{K}$ die Klasse aller Körper der Charakteristik 0 (d.h. dass $1_K$ in der additiven Gruppe unendliche Ordnung hat) mit Ring-1-Homomorphismen. Zeigen Sie, dass $\mathbb{Q}$ in dieser Klasse frei ist (über welcher Menge?).
2. Sei $K$ ein Körper der Charakteristik 0 (d.h. dass $1_K$ in der additiven Gruppe unendliche Ordnung hat), und sei $b \in K$. Dann gibt es einen Körper $L$ mit Charakteristik 0 sowie ein Element $c \in L$, sodass kein Ringhomomorphismus $\varphi$ mit $\varphi(b) = c$ existiert.
3. Über welchen Mengen gibt es freier Körper der Charakteristik 0?

**UE 277 ► Übungsaufgabe 4.1.2.12.** (A) Sei $\mathcal{K}$ eine Klasse von Algebren gleichen Typs und sei $B$ eine Menge. Sei $\mathcal{C}$ die Kategorie, deren Objekte Paare $(i, \mathfrak{A})$ mit $\mathfrak{A} \in \mathcal{K}$ und $i\colon B \to \mathfrak{A}$ sind. ($i$ ist nur Funktion, i.A. nicht Homomorphismus.) Die Morphismen von $(i, \mathfrak{A})$ nach $(i', \mathfrak{A}')$ seien alle Homomorphismen $\varphi\colon \mathfrak{A} \to \mathfrak{A}'$, die $\varphi \circ i = i'$ erfüllen. Zeigen Sie, dass $(i, \mathfrak{F})$ genau dann initial in $\mathcal{C}$ ist, wenn $i$ injektiv ist und $\mathfrak{F}$ in $\mathcal{C}$ frei von $i(B)$ erzeugt wird. **◄ UE 277**

### 4.1.3 Die freie Algebra als homomorphes Bild der Termalgebra

Inhalt in Kurzfassung: Für uns mit Abstand am wichtigsten sind freie Algebren innerhalb von Varietäten. Sie existieren immer und können ziemlich anschaulich verstanden werden als Termalgebren, wobei allerdings manche Terme identifiziert werden, und zwar genau dann, wenn sie stets dieselben Elemente darstellen. Abstrakt formuliert: Die freie Algebra ist ein homomorphes Bild der Termalgebra mit einem Kern, der sich als Durchschnitt aller möglichen Kerne in irgendwelchen Algebren der Varietät ergibt. Erwas anders und ungenau gesprochen: In der freien Algebra gelten genau jene Gesetze, die in allen Algebren und für alle Elemente der Varietät gelten.

Eine sehr transparente, weil vergleichsweise konkrete Konstruktion einer freien Algebra innerhalb einer Varietät geht von der Termalgebra (siehe Definition 2.1.8.1) aus und faktorisiert nach einer geeigneten Kongruenzrelation. Nach dem Homomorphiesatz lässt sich das auch so formulieren: Die freie Algebra ist ein homomorphes Bild der Termalgebra. Genauer: Sei $X$ eine beliebige Menge (Variablenmenge), $\tau = (n_i)_{i\in I}$ ein Typ und $\mathcal{K} = \mathcal{K}(\tau)$ die Klasse aller Algebren des Typs $\tau$. Die Termalgebra $\mathfrak{T}(X) = (T, (\omega_{\mathfrak{T}(X),i})_{i\in I})$ (die absolut freie Algebra des Typs $\tau$ über $X$) ist (zusammen mit der Inklusionsabbildung $\iota\colon X \to T$, die jeder Variablen $x \in X$ den Term $x \in T$ zuordnet) frei in $\mathcal{K}$. Haben wir es jedoch mit einer speziellen Varietät $\mathcal{V} \subseteq \mathcal{K}$ vom Typ $\tau$, die durch eine Menge $\Gamma$

von Gesetzen definiert ist, zu tun, so liegen in $\mathcal{V}$ nur jene Algebren $\mathfrak{A} = (A, (\omega_{\mathfrak{A},i})_{i\in I})$ aus $\mathcal{K}$, die alle Gesetze $\gamma \in \Gamma$ erfüllen. Eine beliebige Abbildung $j\colon X \to A$ lässt sich in eindeutiger Weise zu einem Homomorphismus $\varphi\colon \mathfrak{T}(X) \to \mathfrak{A}$ fortsetzen (Einsetzungshomomorphismus). Wir betrachten die durch $\varphi$ induzierte Kongruenzrelation $\sim_\varphi$ (den *Kern* von $\varphi$), definiert durch: $t_1 \sim_\varphi t_2$ genau dann, wenn $\varphi(t_1) = \varphi(t_2)$. Bezeichne $\sim$ den Durchschnitt aller Kongruenzrelationen auf $\mathfrak{T}(X)$, die als so ein $\sim_\varphi$ zustandekommen. Auch $\sim$ ist eine Kongruenzrelation auf $\mathfrak{T}(X)$. Nach Konstruktion stehen zwei Terme $t_1$ und $t_2$ über $X$ genau dann in der Relation $t_1 \sim t_2$, wenn für alle Algebren $\mathfrak{A} \in \mathcal{V}$ und alle $a_1, a_2, \ldots \in A$ Einsetzen in $t_1$ bzw. $t_2$ dasselbe Element $t_1(a_1, a_2, \ldots) = t_2(a_1, a_2, \ldots) \in A$ liefert. Die resultierende Faktoralgebra $\mathfrak{T}(X)/_\sim$ zusammen mit der kanonischen Einbettung $x \mapsto [x]_\sim$ von $X$ erweist sich als die in $\mathcal{V}$ freie Algebra über $X$.

**Satz 4.1.3.1.** *Varietäten enthalten freie Algebren über beliebigen Mengen, genauer: Sei $\mathcal{V}$ eine Varietät vom Typ $\tau$, $X$ eine Variablenmenge, $\mathfrak{T} = \mathfrak{T}_\tau(X) = (T, (\omega_{\mathfrak{T},i})_{i\in I})$ die zugehörige Termalgebra, $\Gamma$ die $\mathcal{V}$ definierende Menge von Gesetzen (aufgefasst als Teilmenge von $T^2$) und $\sim$ der Durchschnitt aller Kerne von Homomorphismen $\varphi\colon \mathfrak{T} \to \mathfrak{A}$ mit $\mathfrak{A} \in \mathcal{V}$. Dann ist $\sim$ eine Kongruenzrelation auf $\mathfrak{T}_\tau(X)$, und die Faktoralgebra $\mathfrak{F} := \mathfrak{T}/_\sim = (F, (\omega_{\mathfrak{F},i})_{i\in I})$ ist frei über $(X, \iota)$ mit $\iota\colon X \to T/_\sim$, $x \mapsto [x]_\sim$. Außerdem ist $\iota(X)$ ein Erzeugendensystem der Algebra $\mathfrak{F}$.*

*Beweis.* Die letzte Aussage ist klar: Weil die Variablenmenge $X$ die Termalgebra $\mathfrak{T}$ erzeugt, erzeugt auch $\iota(X)$ die Faktoralgebra $\mathfrak{F} = \mathfrak{T}/_\sim$. Nach unseren bisherigen Überlegungen sind nur noch die folgenden beiden Aussagen zu beweisen:
1. Für $\mathfrak{F}$, $X$ und $\iota$ ist die Bedingung, die eine freie Algebra definiert, erfüllt: Für jedes $\mathfrak{A} = (A, (\omega_{\mathfrak{A},i})_{i\in I}) \in \mathcal{V}$ und jede Funktion $j\colon X \to A$ gibt es genau einen Homomorphismus $\varphi\colon \mathfrak{F} \to \mathfrak{A}$ mit $j = \varphi \circ \iota$.
2. $\mathfrak{F} \in \mathcal{V}$, d.h. in $\mathfrak{F}$ gelten alle Gesetze aus $\Gamma$.

Nun zum Beweis dieser beiden Aussagen:

1. Wir betrachten die kanonische Einbettung $\iota_\mathfrak{T}\colon X \to T$, die jeder Variablen $x$ den Term $x$ zuordnet. Die universelle Eigenschaft der Termalgebra (nämlich absolut frei über $(X, \iota_\mathfrak{T})$ zu sein; siehe Satz 2.1.8.4) garantiert die Existenz eines eindeutigen Homomorphismus $\psi\colon \mathfrak{T} \to \mathfrak{A}$ mit $j = \psi \circ \iota_\mathfrak{T}$. Durch $\varphi : [t]_\sim \mapsto \psi(t)$ ist eine Abbildung $\varphi\colon \mathfrak{F} \to \mathfrak{A}$ wohldefiniert: Denn aus $t_1 \sim t_2$ folgt wegen $\mathfrak{A} \in \mathcal{V}$ und der Definition von $\sim$ als Schnitt aller Kerne von Homomorphismen (wie $\psi$ einer ist) $\psi(t_1) = \psi(t_2)$. Klarerweise erbt $\varphi$ von $\psi$ auch die Eigenschaft, ein Homomorphismus zu sein, und erfüllt überdies $j = \varphi \circ \iota$. Damit ist die Existenz eines $\varphi$ mit den behaupteten Eigenschaften gezeigt. Die Eindeutigkeit schließlich folgt mit Proposition 2.3.1.16, weil $\varphi$ durch die Bedingung $j = \varphi \circ \iota$ auf dem Bild von $\iota$, bestehend aus allen $[x]_\sim$, $x \in X$, eindeutig bestimmt ist, und diese Menge ein Erzeugendensystem für $\mathfrak{F}$ bildet.

2. Sei $\gamma = (t_1, t_2) \in \Gamma$, wobei die Terme $t_1 = t_1(x_1, \ldots, x_n)$ und $t_2 = t_2(x_1, \ldots, x_n)$ insgesamt von den endlich vielen Variablen $x_1, \ldots, x_n$ abhängen mögen. Zu zeigen ist, dass für alle $s_1, \ldots, s_n \in T$ die Beziehung $t_1(s_1, \ldots, s_n) \sim t_2(s_1, \ldots, s_n)$

gilt. (Die Terme $s_1, \ldots, s_n$ hängen ihrerseits von gewissen Variablen ab, die allerdings weiter keine Rolle spielen.) Nach Definition von $\sim$ haben wir einen beliebigen Homomorphismus $\psi\colon \mathfrak{T} \to \mathfrak{A}$ mit $\mathfrak{A} \in \mathcal{V}$ zu betrachten und für diesen $\psi(t_1(s_1, \ldots, s_n)) = \psi(t_2(s_1, \ldots, s_n))$ zu zeigen. Wegen der Homomorphieeigenschaft von $\psi$ gelten die Gleichungen $\psi(t_1(s_1, \ldots, s_n)) = t_1(\psi(s_1), \ldots, \psi(s_n))$ und $\psi(t_2(s_1, \ldots, s_n)) = t_2(\psi(s_1), \ldots, \psi(s_n))$. Die Elemente $\psi(s_i)$, $i = 1, \ldots, n$, liegen in der Algebra $\mathfrak{A}$, die zur Varietät $\mathcal{V}$ gehört, also insbesondere das Gesetz $\gamma = (t_1, t_2) \in \Gamma$ erfüllt. Also ist $\gamma$ nach Einsetzen der $\psi(s_i)$ für die $x_i$ gültig, d.h. $t_1(\psi(s_1), \ldots, \psi(s_n)) = t_2(\psi(s_1), \ldots, \psi(s_n))$. Folglich gilt tatsächlich

$$\psi(t_1(s_1, \ldots, s_n)) = t_1(\psi(s_1), \ldots, \psi(s_n)) = t_2(\psi(s_1), \ldots, \psi(s_n)) = \psi(t_2(s_1, \ldots, s_n)).$$

Somit gilt das Gesetz $(t_1, t_2)$ in $\mathfrak{F}$. Weil $\gamma = (t_1, t_2) \in \Gamma$ beliebig gewählt war, zeigt dies $\mathfrak{F} \in \mathcal{V}$. □

Hieraus ergibt sich u.a. die folgende interessante Aussage:

**Proposition 4.1.3.2.** *Sei $\mathcal{V}$ eine nichttriviale Varietät, $\mathfrak{F} \in \mathcal{V}$ mit Trägermenge $F$ und $\iota\colon X \to F$ so, dass $\mathfrak{F}$ in $\mathcal{V}$ frei über $(X, \iota)$ ist. Dann ist $\iota\colon X \to F$ injektiv. (Mit anderen Worten: Nach Identifikation vermittels $\iota$ kann $X$ als Teilmenge der freien Algebra $F$ aufgefasst werden.)*

*Beweis.* Weil die Varietät $\mathcal{V}$ nicht trivial ist, enthält sie laut Proposition 2.3.5.1 eine Algebra $\mathfrak{A}$ mit einer Trägermenge $A$ mit $|X| \geq |A|$. Dann gibt es eine injektive Variablenbelegung $j\colon X \to A$. Nach Satz 4.1.3.1 gibt es ein $\mathfrak{F}(X) \in \mathcal{V}$ und ein $\iota\colon X \to F$ so, dass $\mathfrak{F}$ in $\mathcal{V}$ frei über $(X, \iota)$ ist. Somit gibt es einen eindeutigen Homomorphismus $\varphi\colon \mathfrak{F} \to \mathfrak{A}$ mit $j = \varphi \circ \iota$. Aus der Injektivität von $j$ folgt auch die von $\iota$. □

Die Konstruktion der freien Algebra über einer Variablenmenge $X$ innerhalb einer Varietät $\mathcal{V}$ aus Satz 4.1.3.1 lässt sich so verstehen, dass man sämtliche Terme bildet und Identifikationen genau in dem Maße durchführt, wie es durch die Gesetze in $\mathcal{V}$ erzwungen wird. Allerdings darf das nicht dahingehend missverstanden werden, dass in *jeder* freien Algebra *nur* die Gesetze der Varietät gelten. Beispielsweise liegt die leere Algebra in jeder Varietät $\mathcal{V}$ ohne nullstellige Operationen, ist frei über der leeren Menge und erfüllt überhaupt alle Gesetze, nicht nur diejenigen, die in $\mathcal{V}$ generell gelten. Analoges gilt für die einelementige Algebra. Ein etwas weniger triviales Beispiel ist die vom Element 1 frei erzeugte Gruppe $\mathbb{Z}$. Sie ist abelsch, obwohl das Kommutativgesetz nicht in beliebigen Gruppen gilt. Ein anderes Beispiel ist der von zwei Elementen frei erzeugte Verband. Er erweist sich als distributiv, obwohl das Distributivgesetz nicht in allen Verbänden gilt.

**UE 278** ► **Übungsaufgabe 4.1.3.3.** (F) Beschreiben Sie den von einer zweielementigen Menge frei erzeugten Verband und zeigen Sie, dass er distributiv ist. ◄ **UE 278**

Das Phänomen, dass in gewissen freien Algebren zusätzliche Gesetze gelten können, hängt damit zusammen, dass in den Gesetzen der Varietät mehr Variablen vorkommen können als freie Erzeuger:

**Satz 4.1.3.4.** *Sei $\mathcal{V}$ eine Varietät und $\mathfrak{F}$ frei in $\mathcal{V}$ über $(X, \iota)$. Die Variablenmenge $X$ enthalte mindestens $n$ verschiedene Elemente $x_1, \ldots, x_n$. Seien $t_1 = t_1(x_1, \ldots, x_n)$ und $t_2 = t_2(x_1, \ldots, x_n)$ Terme, in denen jeweils nur die Variablen $x_1, \ldots, x_n$ (oder Teilmengen davon) vorkommen. Für $\mathfrak{C} \in \mathcal{V}$ schreiben wir $\mathfrak{C} \models t \approx t'$ (gelesen „das Gesetz $t = t'$ gilt in $\mathfrak{C}$“) als Abkürzung für*

$$\forall c_1, \ldots, c_n \in C : t(c_1, \ldots, c_n) = t'(c_1, \ldots c_n).$$

*Setzt man $b_i := \iota(x_i)$, so sind die folgenden Aussagen äquivalent:*

*(a) In $\mathfrak{F}$ gilt $t(b_1, \ldots, b_n) = t'(b_1, \ldots, b_n)$.*

*(b) Für alle $\mathfrak{C} \in \mathcal{V}$ gilt $\mathfrak{C} \models t \approx t'$.*

*(c) Es gilt $\mathfrak{F} \models t \approx t'$.*

An dieser Stelle wollen wir zwei bemerkenswerte Konsequenzen dieses Satzes betonen: Zum einen gelten, wie oben bereits angedeutet, in der freien Algebra über zumindest $n$ Erzeugern keine Gesetze zwischen $n$ Variablen, die nicht bereits in sämtlichen Algebren aus der Varietät gelten. Zum anderen ist die Gültigkeit eines Gesetzes in allen Algebren der Varietät (äquivalent in $\mathfrak{F}$) – eine Aussage, die über *alle* Elemente quantifiziert – bereits charakterisiert durch die Gültigkeit auf $n$ *konkreten* Elementen in $\mathfrak{F}$.

**UE 279 ► Übungsaufgabe 4.1.3.5.** (V) Beweisen Sie Satz 4.1.3.4. **◄ UE 279**

Steht eine wenigstens abzählbar unendliche Variablenmenge $X$ zur Verfügung, lassen sich also alle Gesetze hinsichtlich Gültigkeit oder Ungültigkeit einfangen, genauer:

**Satz 4.1.3.6.** *Sei $\mathcal{V}$ eine Varietät und die Variablenmenge $X$ unendlich. Dann gelten in der in $\mathcal{V}$ über $X$ freien Algebra genau jene Gesetze, die in ganz $\mathcal{V}$ gelten.*

Doch zurück zu einer möglichst expliziten Beschreibung freier Algebren. Im Idealfall lässt sich ein algorithmisches Verfahren angeben, wie aus jeder Äquivalenzklasse bezüglich $\sim$ (Bezeichnungsweise aus Satz 4.1.3.1) ein ausgezeichneter Vertreter in *Normalform* ausgewählt werden kann. In konkreten Fällen kann das sehr unterschiedlich kompliziert sein. Der Fall von Monoiden (abelsch oder nicht) wurde bereits in 3.1.2 abgehandelt, der abelsche Fall zusammen mit abelschen Gruppen unter einem etwas anderen Geischtspunkt in 4.1.2 Im Fall von abelschen Monoiden oder Gruppen ist es ziemlich leicht und wurde bereits abgehandelt. Ähnlich leicht ist es auch im Fall von Moduln über einem Ring, nicht viel schwerer für distributive Verbände. Auch für Gruppen und Boolesche Algebren kann man dieses Programm durchführen; wegen der Wichtigkeit freier Gruppen bzw. freier Boolescher Algebren wollen wir uns damit in den nächsten beiden Abschnitten 4.1.4 und 4.1.5 näher beschäftigen.

**UE 280 ► Übungsaufgabe 4.1.3.7.** (B) Beschreiben Sie freie Algebren in der Varietät $\mathcal{V}$, indem Sie Normalformen angeben. **◄ UE 280**

1. $\mathcal{V}$ = Varietät der unitären Moduln über einem festen Ring mit 1
2. $\mathcal{V}$ = Varietät der distributiven Verbände

Vielfältige Anwendungen hat der folgende Satz:

**Satz 4.1.3.8.** *Ist $\mathcal{V}$ eine Varietät, $\mathfrak{A} \in \mathcal{V}$ mit Trägermenge $A$ und $X \subseteq A$ ein Erzeugendensystem von $\mathfrak{A}$, so ist $\mathfrak{A}$ homomorphes Bild der in $\mathcal{V}$ über $X$ freien Algebra $\mathfrak{F}$. Insbesondere ist jede Algebra in einer Varietät homomorphes Bild einer freien Algebra.*

*Beweis.* Laut Satz 4.1.3.1 gibt es in $\mathcal{V}$ eine über $X$ freie Algebra $\mathfrak{F}$. Nach Definition der freien Algebra (4.1.2.5) lässt sich die Inklusionsabbildung $\iota : X \to A$, $x \mapsto x$, (sogar eindeutig) zu einem Homomorphismus $f : \mathfrak{F} \to \mathfrak{A}$ fortsetzen. Das Bild der Algebra $\mathfrak{F}$ unter dem Homomorphismus $f$ ist eine Unteralgebra von $\mathfrak{A}$ (siehe 2.3.1.26), die $X$ enthält, also, weil $X$ ein Erzeugendensystem von $\mathfrak{A}$ ist, bereits ganz $\mathfrak{A}$. Folglich ist $f$ surjektiv, $\mathfrak{A}$ also homomorphes Bild von $\mathfrak{F}$.
Jede Algebra hat ein Erzeugendensystem, beispielsweise die gesamte Trägermenge. Nach dem bereits Bewiesenen ist also jede Algebra einer Varietät homomorphes Bild einer freien Algebra dieser Varietät. □

**UE 281** ► **Übungsaufgabe 4.1.3.9.** (F) Zeigen Sie, dass es in jeder Varietät sowohl initiale als auch terminale Objekte gibt und beschreiben Sie diese. ◄ **UE 281**

**UE 282** ► **Übungsaufgabe 4.1.3.10.** (F) Sei $\mathcal{K}$ die Klasse aller Algebren vom Typ (1), d.h. mit einer einstelligen Operation. Beschreiben Sie die von 2 Elementen frei erzeugte Algebra $F_{\mathcal{K}}(2)$ in $\mathcal{K}$. (D.h., geben Sie explizit die Trägermenge von $F_{\mathcal{K}}(2)$ an, zB als Teilmenge von $\mathbb{N}$ oder $\mathbb{N} \times \mathbb{Z}$, etc., sowie eine explizite einstellige Operation.) ◄ **UE 282**

**UE 283** ► **Übungsaufgabe 4.1.3.11.** (F) Sei $\mathcal{K}$ die Klasse aller Algebren vom Typ $(1, 1)$, d.h. mit zwei einstelligen Operationen. Beschreiben Sie die von einem Element frei erzeugte Algebra $F_{\mathcal{K}}(1)$ in $\mathcal{K}$. (Hinweis: Verwenden Sie das von zwei Elementen frei erzeugte Monoid.) ◄ **UE 283**

### 4.1.4 Die freie Gruppe

Inhalt in Kurzfassung: Freie Gruppen spielen nicht nur unter den Gesichtspunkten der Universellen Algebra eine wichtige Rolle, sondern treten auch in anderen mathematischen Zusammenhängen auf, beispielsweise in der algebraischen Topologie als Fundamentalgruppen oder im Paradoxon von Hausdorff-Banach-Tarski. Die Elemente freier Gruppen stellt man sich am besten als „reduzierte“ Gruppenwörter vor, also als Ausdrücke wie $x^2y^{-1}x^5$, d.h. als Zeichenfolgen, in denen Potenzen der frei erzeugenden Variablen so

aneinandergefügt sind, dass keine Kürzungen mehr möglich sind. Eine sorgfältige Durchführung dieser Konstruktion ist Hauptgegenstand dieses Unterabschnitts.

In diesem Unterabschnitt widmen wir uns einer weit über die Algebra hinaus (zum Beispiel in der algebraischen Topologie, aber auch beim legendären Paradoxon von Hausdorff-Banach-Tarski) wichtigen Klasse freier Algebren, nämlich den freien Gruppen. Wir wollen die allgemeine Konstruktion in Varietäten aus Satz 4.1.3.1 für den Fall der Gruppen konkretisieren. Wir kennen bereits die über einer Menge $B$ freie Halbgruppe. Sie besteht aus allen Zeichenfolgen, die sich mit den Elementen aus $B$ bilden lassen. Wegen des Assoziativgesetzes muss man nicht zwischen verschiedenen Klammerungen unterscheiden. Das gilt bei Gruppen weiterhin. Darüber hinaus ist aber Rücksicht zu nehmen auf die inversen Elemente, durch die sich Gruppen ja von Halbgruppen unterscheiden. Dies ist möglich, indem man für jedes $b \in B$ ein zusätzliches Symbol für sein Inverses einsetzt. In den sich so ergebenden Wörtern muss dann nur noch beachtet werden, dass man kürzen darf, wann immer ein Element aus $B$ direkt mit seinem Inversen zusammentrifft. Dieses Programm soll nun umgesetzt werden.

**Konstruktion der freien Gruppe:** Sei $B$ eine Menge von „Buchstaben“. Sei $\bar{B}$ eine zu $B$ disjunkte Menge, die gleichmächtig zu $B$ ist, wobei $x \mapsto \bar{x}$ eine Bijektion sein soll. Sei $M := (B \cup \bar{B})^*$ das freie Monoid. Seine Trägermenge ist die Menge aller Zeichenfolgen, die man mit den „Buchstaben“ aus $B$ und $\bar{B}$ bilden kann (inklusive der leeren Folge $\varepsilon$). Die Folgen der Länge 1, die nur aus einem Element von $B$ bestehen, identifizieren wir mit dem entsprechenden Element, sodass wir $B \cup \bar{B} \subseteq M$ annehmen dürfen.
Wir setzen die Abbildung $x \mapsto \bar{x}$ zunächst von $B$ auf $B \cup \bar{B}$ fort, indem wir $\bar{\bar{x}} := x$ definieren, und dann auf ganz $M = (B \cup \bar{B})^*$, indem wir $\overline{x_1 \cdots x_n} := \overline{x_n} \cdots \overline{x_1}$ verlangen.
Ein Buchstabenpaar $(x, \bar{x})$, hier gilt also $x \in B \cup \bar{B}$, oder allgemeiner ein Wortpaar $(w, \bar{w})$ nennen wir „komplementär“.
Wir nennen ein Element $w \in (B \cup \bar{B})^*$ *reduziert* , wenn in $w$ keine aufeinander folgenden zueinander inversen Buchstaben vorkommen, d.h., wenn $w$ nicht von der Form $w_1 x y w_2$ ist, wobei $(x, y)$ ein komplementäres Buchstabenpaar ist.[4].
Offenbar ist die Konkatenation $w_1 w_2$ genau dann reduziert, wenn sowohl $w_1$ und $w_2$ reduziert sind, und überdies der letzte Buchstabe von $w_1$ nicht komplementär zum ersten Buchstaben von $w_2$ ist.
Daraus folgt: $w_1 w_2 w_3$ ist genau dann reduziert, wenn sowohl $w_1 w_2$ als auch $w_2 w_3$ reduziert sind.
Sei nun $G$ die Menge aller reduzierten Wörter. Auf der Menge $G$ definieren wir die folgenden zweistellige Operation $*$:

- Gegeben $u, v \in G$.
  Sei $m$ das längste Wort mit der Eigenschaft, dass $u$ mit $m$ endet und $v$ mit $\bar{m}$ beginnt, also $u = u'm$, $v = \bar{m}v'$. Wir nennen das Paar $(m, \bar{m})$ den Mittelteil von $u, v$.
  Dann definieren wir $u * v := u'v'$. Nach Wahl von $m$ ist $u'v'$ reduziert.

[4]Man beachte die Analogie zur gekürzten Darstellung von rationalen Zahlen.

- Spezialfall: Wenn $uv$ bereits reduziert ist, dann ist $m = \varepsilon$, und $u * v := uv$.
- Spezialfall: Wenn $v = \bar{u}$, dann ist $m = u$, und $u * v = \varepsilon$.

Man sieht nun leicht, dass das leere Wort $\varepsilon$ in dieser Struktur ein neutrales Element ist, und dass mit $w$ auch $\bar{w}$ reduziert ist, wobei $\bar{w}$ bezüglich $*$ zu $w$ invers ist.
Wir überprüfen nun das Assoziativgesetz $u*(v*w) = (u*v)*w$. Sei $(\bar{m}, m)$ der Mittelteil von $u, v$, und $(n, \bar{n})$ der Mittelteil von[5] $v, w$. Wir unterscheiden zwei Fälle:

- $m$ und $n$ überlappen sich nicht. Das heißt, $v$ hat die Form $mtn$, $u = u'\bar{m}$, $w = \bar{n}w'$, und $u't$ und $tw'$ sind reduziert.
  Dann ist $(u * v) * w = (u'\bar{m} * mtn) * \bar{n}w' = u'tn * \bar{n}w' = u'tw'$, und analog $u * (v * w) = u'\bar{m} * (mtn * \bar{n}w') = u'\bar{m} * mtw' = u'tw'$.
- $v$ hat die Form $pqr$, mit $m = pq$ und $n = qr$. (Die Mittelteile $m = pq$ und $n = qr$ überlappen sich also in $q$.)
  $(u * v) * w = (u'\bar{q}\bar{p} * pqr) * w = u'r * \bar{r}\bar{q}w' = u'\bar{q}w'$, und analog erhalten wir $u * (v * w) = u'\bar{q}\bar{p} * (pqr * \bar{r}\bar{q}w') = u'\bar{q}\bar{p} * (pw') = u'\bar{q}w'$.

Somit ist $(G, *, \varepsilon, \bar{\cdot})$ eine Gruppe.

**$G$ ist frei über $B$:** Sei $j\colon B \to H$ eine beliebige Abbildung von $B$ in eine Gruppe $H = (H, \cdot, 1, {}^{-1})$. Wir müssen zeigen, dass es einen eindeutigen Gruppenhomomorphimus $G \to H$ gibt, der $j$ fortsetzt.

1. Zuerst setzen wir $j$ zu einer Abbildung $\bar{j} : B \cup \bar{B} \to H$ fort, indem wir $\bar{j}(\bar{b}) := j(b)^{-1}$ definieren.
2. Weil $M$ als Monoid frei über $B \cup \bar{B}$ ist, können wir $\bar{j}$ zu einem Monoidhomomorphismus $j^* : M \to H$ fortsetzen.
3. Mit vollständiger Induktion über die Wortlänge sieht man, dass $j^*(\bar{w}) = (j^*(w))^{-1}$ für alle reduzierten Worte $w$ gilt.
4. Wir zeigen nun, dass die Einschränkung von $j^*$ auf die Menge der reduzierten Wörter ein Homomorphismus bezüglich der neu definierten Operation $*$ ist: Wenn $u = u'm$, $v = \bar{m}v'$ und $u * v = u'v'$ ist, dann ist $j^*(u) = j^*(u') \cdot j^*(m)$ und $j^*(v) = j^*(\bar{m}) \cdot j^*(v')$. Da $j^*(m)$ und $j^*(\bar{m})$ in $H$ nach dem letzten Punkt zueinander invers sind, folgt wie gewünscht $j^*(u * v) = j^*(u) \cdot j^*(v)$.
5. Als Letztes zeigen wir, dass die Einschränkung von $j^*$ auf $G$ der einzige Gruppenhomomorphismus $G \to H$ ist, der $j$ fortsetzt. Dies folgt unmittelbar aus Proposition 2.3.1.16, sobald wir gezeigt haben, dass $G$ von $B$ erzeugt wird, in Zeichen $G = \langle B \rangle$. Da die Buchstaben aus $\bar{B}$ genau die Inversen (in $G$) der Buchstaben aus $B$ sind, umfasst das Erzeugnis von $B$ jedenfalls $B \cup \bar{B}$. Ist $w = x_1 \cdots x_n$ ein beliebiges reduziertes Wort, wobei $x_i \in B \cup \bar{B}$, so gilt auch $w = x_1 * \cdots * x_n$ bezüglich der neu definierten Operation $*$ (da auch die Teilwörter $x_1 * \cdots * x_k$ reduziert sind). Daraus folgt $w \in \langle B \rangle$.

[5] Achtung: einmal $\bar{\cdot}$ vorne, einmal $\bar{\cdot}$ hinten!

Zum Abschluss noch eine Bemerkung mit Ausblick auf das berühmte *Paradoxon von Hausdorff-Banach-Tarski*. Dieses macht Gebrauch davon, dass bereits in der von zwei Elementen $x, y$ frei erzeugten Gruppe $F(x, y)$ eine Vorstellung, die in vielen Gruppen sinnvolle Intuitionen nahelegt, in $F(x, y)$ an ihre Grenzen stößt: nämlich dass Translationen in Gruppen die Größe von Teilmengen erhalten. Denn es liegt nahe, $F(x, y)$ als Vereinigung des Singletons $\{\varepsilon\}$ (leeres Wort) mit den vier zueinander gleich großen, unendlichen Teilmengen $F_x$, $F_{x^{-1}}$, $F_y$ und $F_{y^{-1}}$ anzusehen, die aus all jenen Zeichenketten bestehen, die mit $x, x^{-1}, y$ bzw. mit $y^{-1}$ beginnen. Jede dieser vier unendlichen Mengen, so könnte man argumentieren, entspricht also etwa einem Viertel der Gruppe $F(x, y)$. Für die Translation $t_x : w \mapsto xw$, die ein Element $w \in F(x, y)$ von links mit $x$ multipliziert gilt jedoch einerseits

$$t_x(F(x, y) \setminus F_{x^{-1}}) = t_x(F_x \cup F_y \cup F_{y^{-1}} \cup \{\varepsilon\}) = F_x \quad \text{(aus drei Vierteln wird eines)},$$

andererseits

$$t_x(F_{x^{-1}}) = F_{x^{-1}} \cup F_y \cup F_{y^{-1}} \cup \{\varepsilon\} = F(x, y) \setminus F_x \quad \text{(aus einem Viertel werden drei)}.$$

Man spricht von einer *paradoxen Zerlegung* von $F(x, y)$. Man kann eine zu $F(x, y)$ isomorphe Gruppe von Rotationen der dreidimensionalen Kugel finden und die paradoxe Zerlegung von $F(x, y)$ ausnutzen, um eine Einheitsvollkugel in mehrere Teile zu zerlegen, die, wenn man sie geeignet im Raum bewegt, wieder zusammensetzt zwei Einheitsvollkugeln ergeben. Da Bewegungen Volumina (d.h. das dreidimensionale Lebesguemaß) erhalten, ist dies nur möglich, wenn die Teile, die in der Zerlegung der Kugel vorkommen, nicht alle messbar sind. Tatsächlich ist die Konstruktion auch nur mit Hilfe des Auswahlaxioms möglich, ohne das die Existenz nicht messbarer Mengen nicht bewiesen werden kann.

**UE 284** ► **Übungsaufgabe 4.1.4.1.** (D) Beweisen Sie das Paradoxon von Hausdorff-Banach-Tarski. Wenn das zu schwierig ist: Machen Sie sich so weit kundig, dass Sie wichtige Grundideen präsentieren können, die das Paradoxon wenigstens plausibel machen. ◄ **UE 284**

### 4.1.5 Die freie Boolesche Algebra

Inhalt in Kurzfassung: Nun wird für Boolesche Algebren das analoge Ziel verfolgt wie zuletzt für Gruppen. Wir geben eine Beschreibung freier Boolescher Algebren als Mengenalgebren. Anwendungen haben sie beispielsweise in Aussagenlogik.

Zum Abschluss unserer Untersuchungen der konkreten Beispiele wollen wir noch freie Boolesche Algebren als Mengenalgebren darstellen. Sei die Menge $X$ vorgegeben. Gesucht ist eine Boolesche Algebra $F(X)$ zusammen mit einer Einbettung $\iota\colon X \to F(X)$, so dass $F(X)$ frei ist über $(X, \iota)$. Der Satz 4.1.3.1 liefern eine abstrakte Methode zur Konstruktion, genauso wie auch Satz 4.1.6.1 im nächsten Unterabschnitt. Der Darstellungssatz von Stone 3.6.8.13 sagt uns darüber hinaus, dass wir uns die Elemente von $F(X)$ auch als Teilmengen einer Menge $M$ denken dürfen, wo die Operationen in der

Booleschen Algebra gerade die entsprechenden mengentheoretischen sind. Eine konkrete Beschreibung gelingt wie folgt:

Als Trägermenge wählt man die Menge $M := \{0,1\}^X$ aller Funktionen $f\colon X \to \{0,1\}$.

Jedem Element $x \in X$ ordnen wir die Menge

$$\iota(x) := \{f\colon X \to \{0,1\} \mid f(x) = 1\}$$

zu. (Für endliches $X$ ist das genau die Hälfte aller Elemente von $M$. Für unendliches $X$ hat diese Menge das Maß $1/2$, wenn man das kanonische Produktmaß auf $M$ verwendet; überdies sind die Mengen $\iota(x)$ alle voneinander im wahrscheinlichkeitstheoretischen Sinn unabhängig. Insbesondere sind alle endlichen Schnitte der Form $\iota(x_1) \cap (M \setminus \iota(x_2)) \cap \iota(x_3) \cap \cdots$ nicht leer.)

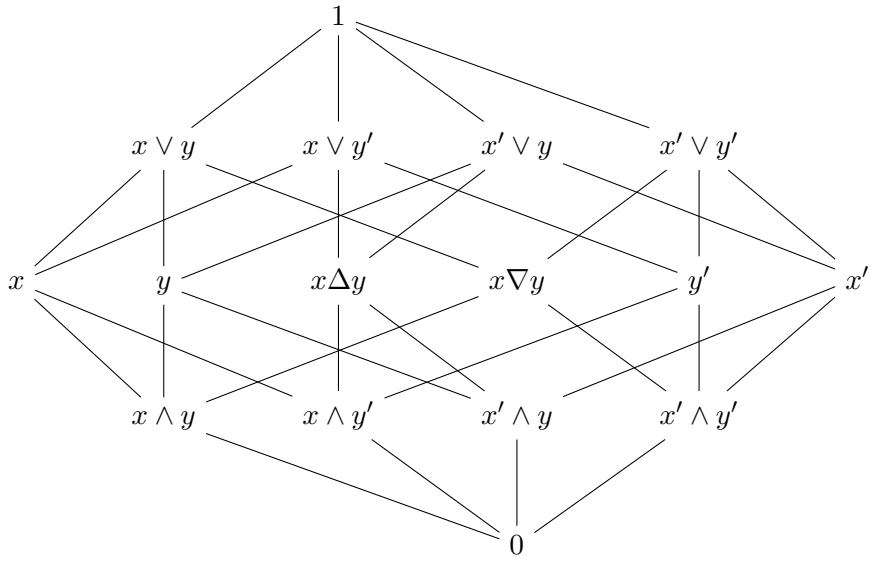
$F(X)$ kann nun realisiert werden als jene Boolesche Unteralgebra von $\mathfrak{P}(M)$, die von den $\iota(x)$ (mit $x \in X$) erzeugt wird.

**Satz 4.1.5.1.** *Mit den obigen Bezeichnungsweisen gilt: Die Algebra $F(X)$ ist in der Varietät der Booleschen Algebren frei über $(X, \iota)$.*

**UE 285 ► Übungsaufgabe 4.1.5.2.** (B) Beweisen Sie Satz 4.1.5.1. **◄ UE 285**

Ist $|X| = n \in \mathbb{N}$ endlich, so folgt $|M| = 2^n$. Man überlegt sich schnell, dass jede Teilmenge von $M$ als Element von $F(X)$ auftritt. Folglich ist $|F(X)| = 2^{2^n}$. Die von 0 Elementen frei erzeugte Boolesche Algebra ist, wenig überraschend, die zweielementige. Für $X = \{x\}$, also $n = 1$, hat $F(x)$ vier Elemente.

Die von 2 Elementen $x$ und $y$ frei erzeugte Boolesche Algebra hat die 4 Atome $x \wedge y$, $x' \wedge y$, $x \wedge y'$ und $x' \wedge y'$ und insgesamt 16 Elemente. Im folgenden Diagramm schreiben wir $xy$ statt $x \wedge y$; weiters verwenden wir die Abkürzungen $x\Delta y := (x' \wedge y) \vee (x \wedge y')$ und $x\nabla y := (x\Delta y)'$.



Die Atome entsprechen den möglichen Belegungen von 2 aussagenlogischen Variablen, also den Zeilen in einer Wahrheitstabelle; die 16 Elemente der Booleschen Algebra entsprechen den möglichen Werteverläufen, die durch eine Formel induziert werden. So entspricht etwa die Vereinigung der 3 Atome $x \wedge y$, $x' \wedge y$, $x \wedge y'$ einer Formel mit den beiden Variablen $x$ und $y$, die immer dann wahr ist, wenn zumindest eine der beiden Variablen den Wert wahr erhält — also zum Beispiel der Formel $x \vee y$ oder der dazu äquivalenten Formel $y \vee (x \wedge x)$.
In der von 3 Elementen $x, y, z$ frei erzeugten Booleschen Algebra gibt es 64 Elemente und 8 Atome, darunter etwa $x \wedge y \wedge z$ und $x \wedge y' \wedge z'$.
Jede von unendlich vielen Elementen frei erzeugte Boolesche Algebra ist atomlos. Die von abzählbar vielen Elementen frei erzeugte Boolesche Algebra ist isomorph zur Booleschen Algebra der *clopen* (d.h. sowohl „closed“, also abgeschlossenen, als auch „open“, also offenen) Teilmengen der Cantormenge.

### 4.1.6 Die freie Algebra als subdirektes Produkt

Inhalt in Kurzfassung: Die Konstruktion der freien Algebra innerhalb einer Varietät als homomorphes Bild der Termalgebra aus 4.1.3 ergänzen wir nun durch eine zweite Konstruktion, nämlich als subdirektes Produkt, d.h. als Unteralgebra eines (in der Regel sehr „großen“) direkten Produktes. Diese Konstruktion ist zwar abstrakter und weniger anschaulich als jene mit Hilfe der Termalgebra. Sie hat aber einen entscheidenden Vorteil in Hinblick auf den Beweis des Satzes von Birkhoff im nachfolgenden Unterabschnitt. In der Konstruktion muss man nicht alle Eigenschaften einer Varietät voraussetzen, sondern nur die Abgeschlossenheit bezüglich dreier Konstruktionen, nämlich bezüglich Unteralgebren, direkter Produkte und isomorpher Bilder. Genau das wird hinreichen, um die nichttriviale Implikation im Satz von Birkhoff zu beweisen.

Es soll noch ein zweites Verfahren zur Konstruktion einer freien Algebra innerhalb einer Klasse $\mathcal{K}$ beschrieben werden, und zwar als sogenanntes subdirektes Produkt. Zum Ersten ist diese Konstruktion deshalb von Interesse, weil sie nicht nur in der Algebra häufig vorkommt, sondern in ähnlicher Form auch in anderen Teilen der Mathematik auftritt. Zum Zweiten werden dabei etwas schwächere Voraussetzungen an die Klasse $\mathcal{K}$ hinreichen als in Unterabschnitt 4.1.3. Und zwar ist es nicht notwendig, dass $\mathcal{K}$ eine Varietät ist. Es genügt, wenn $\mathcal{K}$ abgeschlossen ist bezüglich der Bildung von isomorphen Kopien, direkten Produkten und Unteralgebren. Das wird sich als nützlich beim Beweis des Satzes von Birkhoff erweisen. Der Grundgedanke der Konstruktion ist der Folgende: Wir beginnen mit der Beobachtung, dass sich jede Algebra $\mathfrak{A} = (A, (\omega_{\mathfrak{A},i})_{i\in I})$ eines Typs $\tau = (n_i)_{i\in I}$ als homomorphes, insbesondere surjektives Bild der Termalgebra $\mathfrak{T} = \mathfrak{T}_\tau(A) = (T, (\omega_{\mathfrak{T},i})_{i\in I})$ (wo also die Elemente von $A$ als Variable verwendet werden) darstellen lässt, woraus $|A| \leq |T|$ folgt. (Um einen Epimorphismus $\varphi\colon \mathfrak{T} \to \mathfrak{A}$ zu erhalten, geht man von der Inklusionsabbildung $\iota : A \mapsto T$ aus, wählt als $j\colon A \to A$ die Identität und wählt, gemäß der universellen Eigenschaft der Termalgebra, einen Homomorphismus $\varphi$ mit $j = \varphi \circ \iota$.) Ist die Erzeugendenmenge $X$, über der die gesuchte Algebra $\mathfrak{F}$ in $\mathcal{K}$ frei sein soll, vorgegeben, so ist die Kardinalität der Termmenge a priori durch $|T| \leq$

$\kappa := \max\{|X|, |I|, |\mathbb{N}|\}$ beschränkt (siehe Übungsaufgabe 4.1.6.2). Weil $\mathcal{K}$ abgeschlossen ist bezüglich isomorpher Bilder, gibt es daher eine Menge $Z$ mit folgender Eigenschaft (jede Menge $Z$ mit $|Z| \geq \kappa$ leistet das): Zu jeder Algebra $\mathfrak{A} \in \mathcal{K}$, die von $X$ erzeugt wird, gibt es eine isomorphe Kopie, deren Trägermenge eine Teilmenge von $Z$ ist. Dies vor Augen definieren wir die Teilklasse $\mathcal{K}(Z)$ als die Menge aller $\mathfrak{A} = (A, (\omega_{\mathfrak{A},i})_{i\in I}) \in \mathcal{K}$ mit $A \subseteq Z$. Man beachte, dass es sich bei $\mathcal{K}(Z)$ tatsächlich um eine Menge handelt (siehe Übungsaufgabe 4.1.6.2). Nun betrachten wir die Menge $P$ aller Paare $p = (\mathfrak{A}, j)$ mit $\mathfrak{A} = (A, (\omega_{\mathfrak{A},i})_{i\in I}) \in \mathcal{K}(Z)$ und $j\colon X \to A$, wobei wir auch $\langle j(X)\rangle = A$ voraussetzen, dass also das Bild von $X$ unter $j$ ganz $A$ erzeugt. Laut Voraussetzung liegt das direkte Produkt

$$\mathfrak{M} := \prod_{p=(\mathfrak{A},j)\in P} \mathfrak{A} = (M, (\omega_{\mathfrak{M},i})_{i\in I})$$

in $\mathcal{K}$. Wir definieren $\iota\colon X \to M$ durch $\iota : x \mapsto (j(x))_{p=(\mathfrak{A},j)\in P}$ und $\mathfrak{F} := \langle \iota(X)\rangle = (F, (\omega_{\mathfrak{F},i})_{i\in I})$ als die vom Bild $\iota(X) \subseteq M$ erzeugte Unteralgebra von $\mathfrak{M}$. Als Unteralgebra (Subalgebra) des direkten Produktes $\mathfrak{M}$ mit auch auf der Einschränkung auf $\mathfrak{F}$ surjektiven Projektionen $\pi_{p_0} : (a_p)_{p\in P} \mapsto a_{p_0}$ (nur deshalb die Voraussetzung $\langle \iota_p(X)\rangle = A_p$ für alle $p \in P$, siehe Übungsaufgabe 4.1.6.2) ist $\mathfrak{F}$ ein sogenanntes *subdirektes Produkt* der Algebren $\mathfrak{A}$, $p = (\mathfrak{A}, j) \in P$. Die Behauptung lautet nun:

**Satz 4.1.6.1.** *Sei $\mathcal{K}$ eine Klasse von Algebren des gleichen Typs und abgeschlossen unter isomorphen Bildern, direkten Produkten und Unteralgebren. Dann ist das oben konstruierte subdirekte Produkt $\mathfrak{F}$ frei über $(X, \iota)$ in $\mathcal{K}$ und wird erzeugt von $\iota(X)$.*

*Beweis.* Aus den bisherigen Überlegungen folgt $\mathfrak{M} \in \mathcal{K}$, wegen der Abgeschlossenheit von $\mathcal{K}$ bezüglich Unteralgebren also auch $\mathfrak{F} \in \mathcal{K}$. Zu zeigen bleibt, dass es zu jedem $j_B\colon X \to B$ und $\mathfrak{B} = (B, (\omega_{\mathfrak{B},i})_{i\in I}) \in \mathcal{K}$ einen eindeutigen Homomorphismus $\varphi\colon \mathfrak{F} \to \mathfrak{B}$ mit $j_B = \varphi \circ \iota$ gibt. OBdA (siehe Übungsaufgabe 4.1.6.2) dürfen wir annehmen, dass $\mathfrak{B}$ vom Bild $j_B(X)$ erzeugt wird. Die Eindeutigkeit von $\varphi$ folgt, weil $\mathfrak{F}$ von $\iota(X)$ erzeugt wird (Übungsaufgabe 2.3.1.16). Zur Existenz: Laut Konstruktion und wegen $\mathfrak{B} = \langle j_B(X)\rangle$ gibt es ein $p = (\mathfrak{A}, j) \in P$, so dass $(\mathfrak{B}, j_B)$ und $(\mathfrak{A}, j)$ äquivalent sind, genauer: Es gibt einen Isomorphismus $\psi\colon \mathfrak{A} \to \mathfrak{B}$ mit $j_B = \psi \circ j$. Die Projektionsabbildung $\varphi = \varphi_p\colon \mathfrak{F} \to \mathfrak{A}$ mit $p = (\mathfrak{A}, j)$ (das ist die Einschränkung der auf ganz $M$ definierten Projektion $\pi_p$ auf die Teilmenge $F \subseteq M$), definiert durch $(a_{p'})_{p'\in P} \mapsto a_p$, ist dann der gesuchte Homomorphismus mit $j_B = \varphi \circ \iota$. □

In den Vorbereitungen bzw. im Beweis von Satz 4.1.6.1 wurden der Übersichtlichkeit halber an einigen Stellen gewisse Details nicht in maximaler Ausführlichkeit abgehandelt. Das soll nun im Rahmen einer Übungsaufgabe nachgeholt werden.

**UE 286 ► Übungsaufgabe 4.1.6.2.** (V) Führen Sie die oben knapp behandelten Argumente an folgenden Stellen genau aus: **◄ UE 286**

1. Begründen Sie die Ungleichung $|T| \leq \kappa := \max\{|X|, |I|, |\mathbb{N}|\}$. Hinweis: Bedienen Sie sich des mengentheoretischen Anhangs (Kapitel 11).

2. Warum ist $\mathcal{K}(Z)$ eine Menge? (Kapitel 11)

3. Erläutern Sie, warum die Projektionen $\pi_p$ surjektiv sind, auch wenn man sie auf $\mathfrak{F}$ einschränkt.

4. Erläutern Sie, inwiefern das Argument nach der Abkürzung *OBdA* wirklich *ohne Beschränkung der Allgemeinheit* beweist, was behauptet wird.

### 4.1.7 Der Satz von Birkhoff

Inhalt in Kurzfassung: Mit dem Beweis des Satzes von Birkhoff, einem der wichtigsten Ergebnisse der Universellen Algebra, erreichen wir nun das erste große Ziel dieses Kapitels.

Wie schon angekündigt ist die Konstruktion der freien Algebra aus Unterabschnitt 4.1.6 ein wesentliches Hilfsmittel beim Beweis des für die Gleichungstheorie der Universellen Algebra zentralen Satzes von Birkhoff.

**Satz 4.1.7.1.** *(Satz von Birkhoff) Eine Klasse $\mathcal{V}$ von Algebren vom gleichen Typ ist genau dann gleichungsdefiniert, wenn sie unter $\mathsf{H}, \mathsf{S}, \mathsf{P}$, d.h. unter der Bildung von homomorphen Bildern, Unteralgebren und direkten Produkten, abgeschlossen ist (siehe Definition 4.1.1.1).*

*Beweis.* Wir wissen, dass jede Varietät $\mathcal{V}$ die genannten Abschlusseigenschaften hat. Zu beweisen bleibt deshalb, dass es zu jeder Klasse $\mathcal{V}$, die unter $\mathsf{H}, \mathsf{S}$ und $\mathsf{P}$ abgeschlossen ist, eine Menge $\Gamma$ von Gesetzen mit $\mathcal{V} = \mathrm{Mod}(\Gamma)$ gibt, d.h. so dass $\mathcal{V}$ die durch $\Gamma$ definierte Varietät ist. Da $\mathcal{V}$ vorgegeben ist, liegt es nahe, die Menge $\Gamma$ *aller* Gesetze zu betrachten, die in sämtlichen $\mathfrak{A} \in \mathcal{V}$ gelten. Aus der Definition von $\Gamma$ ergibt sich, dass $\mathcal{V} \subseteq \mathrm{Mod}(\Gamma)$ gilt. Zu zeigen bleibt die umgekehrte Inklusion, nämlich dass jede Algebra, die alle Gesetze aus $\Gamma$ erfüllt, in $\mathcal{V}$ liegt.
Sei also $\mathfrak{A} \in \mathrm{Mod}(\Gamma)$ beliebig, mit Trägermenge $A$. Die Klasse $\mathcal{V}$ erfüllt die Voraussetzungen an $\mathcal{K}$ in Satz 4.1.6.1. Also gibt es eine Algebra $\mathfrak{F} = \mathfrak{F}(A) = (F, (\omega_{\mathfrak{F},i})_{i\in I}) \in \mathsf{SP}(\mathcal{V}) \subseteq \mathcal{V}$, die von der Menge $A$ frei erzeugt wird. Jedes Element von $\mathfrak{F}$ hat die Form $t(a_1, \ldots, a_n)$, wobei $t$ ein Term ist, und $a_1, \ldots, a_n$ Elemente der Erzeugendenmenge $A$ sind. (Allerdings sind weder der Term $t$ noch die $a_i$ im Allgemeinen eindeutig bestimmt.) Aus Satz 4.1.3.4 folgt, dass durch

$$\varphi(t^{\mathfrak{F}}(a_1, \ldots, a_n)) := t^{\mathfrak{A}}(a_1, \ldots, a_n)$$

ein Homomorphismus $\varphi : \mathfrak{F} \to \mathfrak{A}$ *wohldefiniert* wird. Offensichtlich ist $\varphi$ surjektiv. Daher ist $\mathfrak{A}$ ein homomorphes Bild von $\mathfrak{F} \in \mathcal{V}$, also $\mathfrak{A} \in \mathsf{H}(\mathcal{V}) \subseteq \mathcal{V}$. □

**Anmerkung 4.1.7.2.** Achtung: Man darf den letzten Beweisschritt (aus $\mathfrak{A} \in \mathrm{Mod}(\Gamma)$ folgt $\mathfrak{A} \in \mathsf{H}(\mathcal{V})$) nicht abkürzen, indem man den Beweis von Satz 4.1.3.8 wiederholt (also durch die Freiheit einen Homomorphismus $\varphi : \mathfrak{F} \to \mathfrak{A}$ erhält, der die identische Abbildung $j : A \to \mathfrak{A}$ fortsetzt). Der Grund dafür ist, dass $\mathfrak{F}$ nur in $\mathcal{V}$ frei ist, wir aber an dieser Stelle noch nicht wissen, dass $\mathfrak{A}$ tatsächlich in $\mathcal{V}$ liegt – das wollen wir ja gerade erst zeigen.

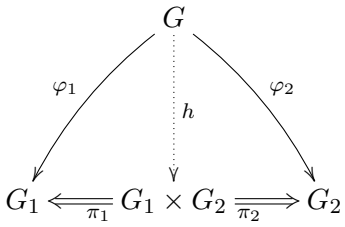
## 4.2 Koprodukte und Polynomalgebren

Koprodukte (einfache Beispiele und Definition in 4.2.1) ähneln freien Algebren in vielerlei Hinsicht. Grob lässt sich der Unterschied so fassen: Freie Algebren werden von den Elementen einer gegebenen Menge ohne weitere Struktur auf möglichst *freie* Weise erzeugt, Koprodukte von zwei oder mehreren vorgegebenen Strukturen. Tatsächlich lässt sich die freie Algebra verwenden, um in einer Varietät auch beliebige Koprodukte zu konstruieren (4.2.2). Unsere wichtigste Anwendung sind Polynomalgebren in der Varietät der kommutativen Ringe mit 1 (4.2.3). Eine ähnliche universelle Eigenschaft, allerdings als Verbindung zweier Strukturen unterschiedlichen Typs, hat der Gruppenring bzw. der Monoidring (4.2.4).

### 4.2.1 Bekannte Beispiele und Definition des Koproduktes

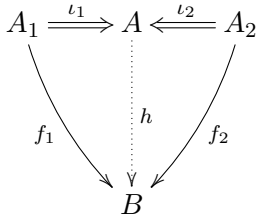
Inhalt in Kurzfassung: In Koprodukten wie in freien Algebren (in Varietäten) geht es darum, Elemente, die zunächst nichts miteinander zu tun haben, so in einer einzigen Algebra der Varietät unterzubringen, dass sie sich im Rahmen gewisser Vorgaben möglichst ungebunden verhalten. Der Unterschied: Bei freien Algebren waren die Elemente völlig ohne Beziehung zueinander, wie Variablen, die nur den Gesetzen der Varietät unterworfen sind. Bei Koprodukten entstammen die Elemente bereits vorgegebenen Algebren der Varietät, wobei die Struktur der beteiligten Algebren möglichst erhalten bleiben soll, Elemente aus derselben Algebra sich also sehr wohl weiterhin als solche verhalten sollen. Tatsächlich ähneln Koprodukte in vielen Varietäten tatsächlich freien Algebren (z.B. Gruppen und Vektorräume). Die allgemeine Definition ist aber kategorientheoretischer Natur ohne Bezugnahme auf Varietäten, wieder als initiales Objekt in einer geeigneten Kategorie. Als Folgerung sind Koprodukte bis auf Isomorphie eindeutig bestimmt.

**Beispiel 4.2.1.1** (Das Produkt als universelles Objekt)**.** Wir erinnern uns: Sind $G_1$ und $G_2$ Gruppen oder sonst zwei Algebren desselben Typs, dann hat das direkte Produkt $G_1 \times G_2$ zusammen mit den Projektionen $\pi_i \colon G_1 \times G_2 \to G_i$ $(i = 1, 2)$, definiert durch $\pi_1(x, y) = x$ und $\pi_2(x, y) = y$, nach Proposition 2.3.2.4 folgende universelle Eigenschaft: Für jede Gruppe $G$ und beliebige Homomorphismen $\varphi_i \colon G \to G_i$, $i = 1, 2$, gibt es genau einen Homomorphismus $h \colon G \to G_1 \times G_2$ mit $\varphi_i = \pi_i \circ h$ für $i = 1, 2$.




**Beispiel 4.2.1.2** (Die direkte Summe als universelles Objekt)**.** Andererseits erinnern wir uns an die direkte Summe von abelschen Gruppen (bzw. von Moduln, spezieller von Vektorräumen): Sind $A_1$ und $A_2$ abelsche Gruppen, dann hat die direkte Summe

$A = A_1 \oplus A_2$ zusammen mit den kanonischen Einbettungen $\iota_i \colon A_i \to A$ $(i = 1, 2)$, definiert durch $\iota_1(a_1) = (a_1, 0)$ und $\iota_2(a_2) = (0, a_2)$, nach Proposition 3.3.2.2 folgende universelle Eigenschaft:
Für jede abelsche Gruppe B und beliebige Homomorphismen $f_i : A_i \to B$, $i = 1, 2$, gibt es genau einen Homomorphismus $h : A \to B$ mit $f_i = h \circ \iota_i$ für $i = 1, 2$.




Man beachte, dass die charakteristische Eigenschaft der direkten Summe sehr ähnlich der charakteristischen Eigenschaft des Produktes ist; nur zeigen alle Pfeile nun in die entgegengesetzte Richtung.
Die Verallgemeinerung der direkten Summe zum Koprodukt von mehr als zwei Faktoren sowie auf beliebige Kategorien liegt mit dieser Sichtweise auf der Hand:

**Definition 4.2.1.3.** Sei $\mathcal{C}$ eine Kategorie und seien $A_i$, $i \in I$ (Indexmenge), Objekte in $\mathcal{C}$. Ein Paar $(A, (\iota_i)_{i \in I})$ heißt *Koprodukt* der $A_i$ in $\mathcal{C}$, wenn folgende Bedingungen erfüllt sind:

- $A \in \mathrm{Ob}(\mathcal{K})$.
- Für alle $i \in I$ ist $\iota_i \colon A_i \to A$ ein Morphismus in $\mathcal{C}$.
- Für alle Objekte $B \in \mathcal{C}$ und alle Familien von Morphismen $f_i \colon A_i \to B$, $i \in I$, gibt es genau einen Morphismus $f \colon A \to B$, der $f \circ \iota_i = f_i$ für alle $i \in I$ erfüllt.

Ein Objekt $A \in \mathcal{C}$ heißt Koprodukt der $A_i$ in $\mathcal{C}$, wenn es Morphismen $\iota_i \colon A_i \to A$, $i \in I$, gibt, so dass $(A, (\iota_i)_{i \in I})$ Koprodukt der $A_i$ in $\mathcal{C}$ ist. Symbolisch schreibt man kurz:

$$A = \coprod_{i \in I} A_i$$

Im Fall von nur zwei Objekten, also $|I| = 2$, oBdA $I = \{1, 2\}$ schreibt man das Koprodukt vorzugsweise in Infixnotation als $A = A_1 \coprod A_2$.

**UE 287** ► **Übungsaufgabe 4.2.1.4.** (F) Sei $\mathcal{C}$ eine Kategorie, und seien $A_1, A_1', A_2, A_2'$ Objekte von $\mathcal{C}$, wobei $A_1$ und $A_1'$ in $\mathcal{C}$ äquivalent (in Kategorien von algebraischen Strukturen: isomorph) sind, ebenso $A_2$ und $A_2'$. Sei $(s, p_1, p_2)$ ein Koprodukt von $A_1$ und $A_2$ in $\mathcal{C}$. Zeigen Sie, dass es auch ein Koprodukt von $A_1'$ und $A_2'$ in $\mathcal{C}$ gibt, und zwar eines der Form $(s, ?, ?)$.
Formulieren Sie einen analogen Satz für Produkte. ◄ **UE 287**

Offenbar lässt sich das Koprodukt gegebener Algebren $V_i \in \mathcal{K}$ als initiales Objekt in einer geeigneten Kategorie $\mathcal{C} = \mathcal{C}((V_i)_{i \in I})$ deuten, weshalb jedes Koprodukt einer gegebenen Familie von Algebren bis auf Isomorphie eindeutig bestimmt ist, vgl. Satz 2.2.3.2.

**UE 288** ► **Übungsaufgabe 4.2.1.5.** (V) Führen Sie dieses Argument im Detail aus, indem Sie insbesondere die von den $V_i$ abhängige Kategorie $\mathcal{C}((V_i)_{i\in I})$ definieren. ◄ **UE 288**

Das Koprodukt von zwei (oder mehr) Strukturen hängt nicht nur von den Strukturen selbst ab, sondern auch von der Klasse, in der man das Koprodukt sucht. In der Klasse $\mathcal{Ab}$ aller abelschen Gruppen ist das Koprodukt zweier abelscher Gruppen durch die direkte Summe gegeben. In der Klasse $\mathcal{Grp}$ aller Gruppen ist bereits das Koprodukt zweier abelscher Gruppen komplizierter, wie die folgenden Aufgaben zeigen (vgl. auch Übungsaufgabe 3.3.2.4).

**UE 289** ► **Übungsaufgabe 4.2.1.6.** (B,F) Sei $G$ ein Koprodukt von $\mathbb{Z}$ mit $\mathbb{Z}$ in $\mathcal{Grp}$. Zeigen Sie, dass $G$ nicht kommutativ und daher insbesondere nicht die Gruppe $\mathbb{Z}\times\mathbb{Z}$ sein kann. Hinweis: Wählen sie geeignete Homomorphismen $f_1, f_2\colon \mathbb{Z}\to H$ in eine (beliebige) nichtkommutative Gruppe $H$. ◄ **UE 289**

**UE 290** ► **Übungsaufgabe 4.2.1.7.** (B,E) Sei $(G, i_1, i_2)$ ein Koprodukt von $C_2$ und $C_2$ in $\mathcal{Grp}$. (Ja, 2 Mal die 2-elementige Gruppe.) Sei $F_2$ die von 2 Elementen frei erzeugte Gruppe. ◄ **UE 290**

1. Zeigen Sie, dass $G$ unendlich groß ist, und dass $G$ nicht kommutativ ist.
   Hinweis: Finden Sie verschiedene Homomorphismen von $C_2$ in die Gruppe $H$ aller Permutationen von $\mathbb{Z}$, die benachbarte Elemente immer auf benachbarte Elemente abbilden. Anders gesagt: Sei $A := \{(x,y)\in\mathbb{Z}^2 : |x-y| = 1\}$; die Gruppe $H$ ist dann die Menge aller Automorphismen der relationalen Struktur $(\mathbb{Z}, A)$.

2. Zeigen Sie, dass $G$ nicht zu $F_2$ isomorph ist.

**UE 291** ► **Übungsaufgabe 4.2.1.8.** (E) Seien $G_1$ und $G_2$ zwei Gruppen (nicht notwendig abelsch). Beschreiben Sie das Koprodukt von $G_1$ und $G_2$ in der Kategorie $\mathcal{Grp}$ der Gruppen. Hinweis: Orientieren Sie sich an der Konstruktion freier Gruppen. ◄ **UE 291**

### 4.2.2 Konstruktion des Koproduktes als freie Algebra

Inhalt in Kurzfassung: Die bereits in 4.2.1 angedeutete Ähnlichkeit zwischen freien Algebren und Koprodukten schlägt sich auch technisch wieder: In Varietäten existieren Koprodukte uneingeschränkt, und der Beweis dafür lässt sich zurückführen auf die uneingeschränkte Existenz freier Objekte in Varietäten.

Koprodukte existieren nicht in beliebigen Kategorien.

**UE 292** ► **Übungsaufgabe 4.2.2.1.** (B) Finden Sie eine (möglichst interessante) Kategorie, in der es nicht beliebige Koprodukte gibt. ◄ **UE 292**

Ähnlich wie bei freien Algebren erweist sich aber die Voraussetzung, dass es sich bei der Kategorie um eine Varietät handelt, als hinreichend für die Existenz beliebiger Koprodukte. In der Konstruktion kann man sich die Arbeit erleichtern, wenn man von der Existenz freier Algebren in Varietäten Gebrauch macht.

**Satz 4.2.2.2.** *Ist $\mathcal{V}$ eine Varietät, so existieren Koprodukte in $\mathcal{V}$ uneingeschränkt.*

*Beweis.* Sei $\mathcal{V}$ gegeben durch eine Familie $\Omega$ von Operationssymbolen $\omega_i$, $i \in I$ mit Stelligkeiten $n_i$ sowie durch eine Menge $\Gamma$ von Gesetzen. Gegeben seien Algebren $\mathfrak{A}_k = (A_k, \Omega_k) \in \mathcal{V}$, $k \in K$, mit Trägermengen $A_k$ und Familien $\Omega_k$ von Operationen $\omega_{i,k} \colon A_k^{n_i} \to A$, $i \in I$. Gesucht ist ein Koprodukt $\coprod_{k\in K} \mathfrak{A}_k$ in $\mathcal{V}$. Zu diesem Zweck werden wir eine Varietät $\mathcal{V}'$ geeignet definieren. Die in $\mathcal{V}'$ über der leeren Menge $\emptyset$ freie Algebra $F_{\mathcal{V}'}$ zusammen mit geeigneten $\iota_k$, $k \in K$, wird sich als das gesuchte Koprodukt deuten lassen. Definition von $\mathcal{V}'$: Die neue Varietät $\mathcal{V}'$ entsteht aus $\mathcal{V}$, indem die Familie der $\omega_i$ wie auch $\Gamma$ ergänzt werden. Und zwar verwenden wir alle Elemente der $A_k$ als nullstellige Operationensymbole, genauer: Sei $\Omega_0 := \bigcup_{k\in K} A_k \times \{k\}$ (disjunkte Vereinigung der $A_k$). Für jedes $(a, k) \in \Omega_0$ sei $\omega_{(a,k)}$ ein Operationssymbol mit Stelligkeit 0. Die Gesetze von $\mathcal{V}$ werden erweitert durch die folgenden. Damit sich in den Algebren aus $\mathcal{V}'$ die den neu hinzugefügten nullstelligen Operationen zugeordneten Elemente wie die entsprechenden Elemente der Strukturen $\mathfrak{A}_k$ verhalten, fügen wir zu $\Gamma$ für jedes $k \in K$, $i \in I$ und alle $a_1, \ldots, a_{n_i} \in \mathfrak{A}_k$ das Gesetz (siehe Definition 2.1.8.6)

$$\omega_i(\omega_{(a_1,k)}, \ldots, \omega_{(a_{n_i},k)}) \approx \omega_{(\omega_{i,k}(a_1,\ldots,a_{n_i}),k)}$$

hinzu, das wir mit $\gamma(k, i, a_1, \ldots, a_{n_i})$ bezeichnen. Wir definieren also $\Gamma'$ als die Vereinigung von $\Gamma$ und allen $\gamma(k, i, a_1, \ldots, a_{n_i})$. In der Varietät $\mathcal{V}'$ gibt es nach 4.1.3.1 über jeder Menge $X$ eine freie Algebra, insbesondere auch über der leeren Menge $X = \emptyset$. Diese Algebra bezeichnen wir mit $\mathfrak{F}'$, ihre Trägermenge mit $F$. Außerdem definieren wir für jedes $k \in K$ die Abbildung $\iota_k \colon A_k \to F$ durch $a \mapsto \omega_{(a,k)}^{\mathfrak{F}'}$, wobei $\omega_{(a,k)}^{\mathfrak{F}'}$ die in $\mathfrak{F}'$ dem Operationssymbol $\omega_{(a,k)}$ zugeordnete nullstellige Operation, genauer: das entsprechende Element, bezeichne. Wir behaupten, dass $\mathfrak{F}'$, aufgefasst als Algebra $\mathfrak{F} \in \mathcal{V}$, zusammen mit den $\iota_k$ ein Koprodukt der $\mathfrak{A}_k$ in $\mathcal{V}$ ist.
Um das zu beweisen, ist einerseits zu zeigen, dass die Abbildungen $\iota_k : \mathfrak{A}_k \to \mathfrak{F}$ Homomorphismen sind – dies folgt unmittelbar daraus, dass in $\mathfrak{F}'$ die Gesetze $\gamma(k, i, a_1, \ldots, a_{n_i})$ gelten. Andererseits müssen wir von einer beliebigen Algebra $\mathfrak{B} \in \mathcal{V}$ zusammen mit Homomorphismen $j_k \colon \mathfrak{A}_k \to \mathfrak{B}$, $k \in K$, ausgehen und zeigen, dass es einen eindeutigen $\mathcal{V}$-Homomorphismus $\varphi \colon \mathfrak{F} \to \mathfrak{B}$ gibt mit $j_k = \varphi \circ \iota_k$ für alle $k \in K$. Für jedes $k \in K$ und $a \in A_k$ definieren wir auf $B$ die nullstellige Operation $\omega_{(a,k)}^{\mathfrak{B}'} := j_k(a)$ und erhalten eine Algebra $\mathfrak{B}'$. Mit diesen Operationen erfüllt $\mathfrak{B}'$ auch jedes Gesetz $\gamma(k, i, a_1, \ldots, a_{n_i})$, das sich ja vermittels des Homomorphismus $j_k$ von $\mathfrak{A}_k$ auf $B$ überträgt. Da $\mathfrak{F}'$ frei in $\mathcal{V}'$ über der leeren Menge ist, gibt es einen eindeutigen $\mathcal{V}'$-Homomorphismus $\varphi \colon \mathfrak{F}' \to \mathfrak{B}'$. Das bedeutet insbesondere auch $\varphi : \omega_{(a,k)}^{\mathfrak{F}'} \mapsto \omega_{(a,k)}^{\mathfrak{B}'}$ und deshalb $j_k(a) = \varphi \circ \iota_k(a)$ für alle $k \in K$ und $a \in A_k$, also $j_k = \varphi \circ \iota_k$ für alle $k \in K$. Als $\mathcal{V}'$-Homomorphismus ist $\varphi$ erst recht $\mathcal{V}$-Homomorphismus und hat daher die gewünschten Eigenschaften. Zuletzt zur Eindeutigkeit von $\varphi \colon \mathfrak{F}'$ wird als Algebra in $\mathcal{V}'$ von der leeren Menge erzeugt, d.h.

als Algebra $\mathfrak{F}$ in $\mathcal{V}$ von den hinzugefügten 0-stelligen Operationen, nach Konstruktion also von der Vereinigung der $\iota_k(A_k)$, $k \in K$. Jeder Homomorphismus ist durch seine Werte auf einem Erzeugendensystem eindeutig bestimmt (Proposition 2.3.1.16), somit insbesondere $\varphi$ durch die Forderung $j_k = \varphi \circ \iota_k$ für alle $k \in K$. □

**UE 293** ▶ **Übungsaufgabe 4.2.2.3.** (W) Sei $\mathcal{Grp}$ die Klasse aller Gruppen, und sei $(C, \iota_1, \iota_2)$ ◀ **UE 293**
Koprodukt von $G_1$ und $G_2$ in $\mathcal{Grp}$. Dann sind $\iota_1$ und $\iota_2$ injektiv. (Hinweis: Betrachten Sie $D := G_1$.) Verallgemeinern Sie Ihr Argument auf Koprodukte beliebig vieler Gruppen.
Warum funktioniert Ihr Beweis nicht für die Klasse aller kommutativen Ringe mit Einselement? Weisen Sie auf den Schritt in Ihrem Beweis hin, den Sie in der Klasse der kommutativen Ringe mit Einselement nicht durchführen können.

**UE 294** ▶ **Übungsaufgabe 4.2.2.4.** (F) Sei $\mathcal{Rng}_1$ die Klasse aller kommutativen Ringe mit 1. ◀ **UE 294**

1. Zeigen Sie, dass der einelementige Ring in $\mathcal{Rng}_1$ ein Koprodukt von $\mathbb{Z}/2\mathbb{Z}$ und $\mathbb{Z}/3\mathbb{Z}$ ist.
2. Kontrastieren Sie dieses Resultat mit der vorigen Aufgabe.

Die freie Algebra über einer gewissen Menge kann man mithilfe des Koprodukts aus freien Algebren über kleineren Mengen zusammensetzen.

**Proposition 4.2.2.5.** *Sei $\mathcal{V}$ eine nichttriviale Varietät. Für $i = 1, 2$ sei $\mathfrak{F}_i \in \mathcal{V}$ frei über $(B_i, \iota_i)$, wobei der Einfachheit halber $B_1 \cap B_2 = \emptyset$ sei. Weiters sei $(\mathfrak{F}, j_1, j_2)$ ein Koprodukt von $\mathfrak{F}_1$ und $\mathfrak{F}_2$. Dann gilt*

1. *$(j_1 \circ \iota_1)(B_1) \cap (j_2 \circ \iota_2)(B_2) = \emptyset$*
2. *Setzt man $B = B_1 \dot\cup B_2$ und $\iota := (j_1 \circ \iota_1) \dot\cup (j_2 \circ \iota_2)$ (also $\iota(b_i) = j_i(\iota_i(b_i))$ für $b_i \in B_i$ und $i = 1, 2$), dann ist $\mathfrak{F}$ frei über $(B, \iota)$.*

**UE 295** ▶ **Übungsaufgabe 4.2.2.6.** (V) Beweisen Sie Proposition 4.2.2.5. ◀ **UE 295**

### 4.2.3 Polynomalgebren

Inhalt in Kurzfassung: Schon bei der Einführung von Polynomringen im klassischen Sinn in 3.4.6 haben wir eine universelle Eigenschaft festgestellt (siehe Proposition 3.4.6.13), die nun zum Ausgangspunkt für den viel allgemeineren Begriff der Polynomalgebra über einer beliebigen Algebra einer Varietät wird. Und zwar handelt es sich um die Kombination der beiden wichtigsten Konstruktionen dieses Kapitels, nämlich der freien Algebra und des Koproduktes. Der Beweis, dass auch Polynomalgebren in Varietäten uneingeschränkt existieren, ergibt sich nun mehr oder weniger als Korollar bereits verfügbarer

Ergebnisse.

Wir gehen von der folgenden grundlegenden Eigenschaft von Polynomen $f \in R[X]$ über einem kommutativen Ring $R$ mit 1 in Variablen aus der Variablenmenge $X$ aus: Zu jedem kommutativen Ring $S$ mit 1, der $R$ als Unterring mit 1 enthält und jeder Variablenbelegung $j\colon X \to S$ mit Elementen aus $S$ gibt es einen eindeutigen Ringhomomorphismus $\varphi\colon R[X] \to S$, der $j$ fortsetzt. Dieses $\varphi$ ist der Einsetzungshomomorphismus

$$f(x_1, \ldots, x_n) = \sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} x_1^{i_1} \ldots x_n^{i_n} \mapsto \sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} s_1^{i_1} \ldots s_n^{i_n}$$

mit $s_i := j(x_i)$ für $x_i \in X$ und $i = 1, \ldots, n$. Nun versuchen wir, den Polynomring $R[X]$ durch allgemeine Konstruktionen zu erhalten, die in beliebigen Varietäten verfügbar sind.
Wir gehen in zwei Schritten vor. Im ersten bilden wir den von der Variablenmenge $X$ frei erzeugten kommutativen Ring $F(X)$ mit 1. Weil die kommutativen Ringe mit 1 eine Varietät bilden, gibt es so ein $F(X)$ (siehe Satz 4.1.3.1). Die bestimmende Eigenschaft von $F(X)$ lautet: Sind irgendein Ring $S$ mit 1 und eine Variablenbelegung $j\colon X \to S$ vorgegeben, so gibt es einen eindeutigen Homomorphismus $\varphi_S\colon F(X) \to S$ mit $\varphi_S(x) = j(x)$ für alle $x \in X$. Nun wollen wir statt $F(X)$ allerdings einen Ring, der überdies $R$ umfasst. Es liegt nahe, das Koprodukt von $R$ und $F(X)$ zu betrachten. Wieder weil die kommutativen Ringe mit 1 eine Varietät bilden, ist die Existenz so eines Koproduktes garantiert (Satz 4.2.2.2).

**Definition 4.2.3.1.** Sei $\mathcal{C}$ eine konkrete Kategorie, $A$ ein Objekt in $\mathcal{C}$, und $X$ eine Menge (Variablenmenge). Gibt es in $\mathcal{C}$ ein über $X$ freies Objekt $(F(X), \iota)$, so heißt jedes Koprodukt $A \coprod F(X)$ (mit Morphismen $\iota_A\colon A \to A \coprod F(X)$ und $\iota_{F(X)}\colon F(X) \to A \coprod F(X)$) eine *Polynomalgebra* in den *Unbestimmten* oder *Variablen* $x \in X$ über $A$ in $\mathcal{C}$, symbolisch $A[X]$. Die Elemente von $A[X]$ heißen (verallgemeinerte) *Polynome*.

Man beachte, dass in dieser Definition nichts über die Existenz von Polynomalgebren ausgesagt wird!
Die (Bilder der) freien Erzeuger $x \in X$ von $F(X)$ nennen wir die *Unbestimmten* und bezeichnen sie weiterhin mit $x$. Im Fall $X = \{x_1, \ldots, x_n\}$ endlich vieler Variablen schreiben wir oft $A[x_1, \ldots, x_n]$ für $A[X]$.
Wie bereits erwähnt ergibt sich aus 4.1.3.1 und 4.2.2.2:

**Folgerung 4.2.3.2.** *Ist $\mathcal{V}$ eine Varietät, $A \in \mathcal{V}$ und $X$ irgendeine Menge, dann gibt es eine Polynomalgebra $A[X]$ über $A$ in den Variablen aus $X$ in $\mathcal{V}$.*

Meist ist es gewünscht, $A$ und $F(X)$ als Unteralgebren der Polynomalgebra $A[X]$ und $\iota_A\colon A \to A[X]$ sowie $\iota_{F(X)}\colon F(X) \to A[X]$ als Inklusionsabbildungen auffassen zu können. Das klappt aber nur, wenn diese Homomorphismen $\iota_A$ und $\iota_{F(X)}$ injektiv sind. Für $\iota_A$ ist dies stets der Fall:

**Proposition 4.2.3.3.** *Sei $A[X]$ die Polynomalgebra von $A$ in der Varietät $\mathcal{V}$ in der Variablenmenge $X$, $F(X)$ die in $\mathcal{V}$ von $X$ frei erzeugte Algebra. Die dem Koprodukt $A[X] =$*

*$A \coprod F(X)$ zugehörigen Homomorphismen seien mit $\iota_A \colon A \to A[X]$ und $\iota_{F(X)} \colon F(X) \to A[X]$ bezeichnet. Dann ist der Homomorphismus $\iota_A$ injektiv, d.h. eine isomorphe Einbettung von $A$ in die Polynomalgebra $A[X]$. Folglich darf $A$ oBdA als Unteralgebra der Polynomalgebra $A[X]$ aufgefasst werden.*

*Beweis.* Ist $A$ die leere Algebra, so ist die Behauptung trivial. Sei daher $a \in A$. Wir betrachten einerseits die Identität $\mathrm{id} \colon A \to A$, andererseits den die konstante Variablenbelegung $x \mapsto a$ auf die freie Algebra $F(X)$ fortsetzenden Homomorphismus $\varphi_a \colon F(X) \to A$. Nach Definition des Koproduktes gibt es einen Homomorphismus $\varphi \colon A[X] \to A$ mit $\mathrm{id}_A = \varphi \circ \iota_A$. Das ist nur möglich, wenn $\iota_A$ injektiv ist. □

Mit der Injektivität von $\iota_{F(X)}$ in 4.2.3.3 verhält es sich komplizierter als mit jener von $\iota_A$. Es ist eine lehrreiche Übung, sich das zu überlegen:

**UE 296** ► **Übungsaufgabe 4.2.3.4.** (A) Für uns besonders interessant ist die Varietät der kommutativen Ringe mit 1. Zeigen Sie, dass die Einschränkung von $\iota_{F(X)} \colon F(X) \to A[X]$ auf $X$, (gemäß Proposition 4.1.3.2 aufgefasst als Teilmenge von $F(X)$) injektiv ist. Folglich darf in diesem Fall $X$ oBdA auch als Teilmenge der Polynomalgebra $A[X]$ aufgefasst werden. Beweisen Sie das abstrakt, ohne Bezugnahme auf die konkrete Darstellung von Polynomen über einem kommutativen Ring mit 1. ◄ **UE 296**

Nach Konstruktion ist die Polynomalgebra durch folgende Eigenschaft charakterisiert, die wir im Fall der kommutativen Ringe mit 1 eingangs zur Motivation der allgemeinen Definition genommen haben:

**Satz 4.2.3.5.** *Sei $\mathcal{V}$ eine Varietät, $A \leq B \in \mathcal{V}$ und $X$ eine Variablenmenge. Dann gibt es zu jeder Variablenbelegung $j \colon X \to B$ von $X$ mit Elementen aus $B$ einen eindeutigen Homomorphismus $\varphi \colon A[X] \to B$ mit $\varphi(a) = a$ für alle $a \in A \leq A[X]$ (gemäß Proposition 4.2.3.3) und $\varphi(x) = j(x)$ für alle $x \in X \subseteq F(X)$ (gemäß Proposition 4.1.3.2 für nichttriviales $\mathcal{V}$).*

*Beweis.* Ist die Varietät $\mathcal{V}$ trivial, so auch die Behauptung. Sei daher $\mathcal{V}$ nichttrivial. Somit dürfen wir laut Proposition 4.1.3.2 die Variablenmenge $X$ als Teilmenge der von $X$ in $\mathcal{V}$ frei erzeugten Algebra $F(X)$ auffassen. Nach Definition der freien Algebra lässt sich die Variablenbelegung $j$ eindeutig zu einem auf ganz $F(X)$ definierten Homomorphismus $\varphi_0 \colon F(X) \to B$ fortsetzen. Nach Definition ist $A[X]$ ein Koprodukt $A \coprod F(X)$. Die diesem Koprodukt zugehörigen Homomorphismen seien $\iota_{A,A[X]} \colon A \to A[X]$ und $\iota_{F(X),A[X]} \colon F(X) \to A(X)$. Außerdem bezeichne $\iota_{A,B} \colon A \to B$, $a \mapsto a$, die Inklusionsabbildung. Die definierende Eigenschaft des Koproduktes garantiert, dass es einen eindeutigen Homomorphismus $\varphi \colon A[X] \to B$ gibt mit $\varphi \circ \iota_{A,A[X]} = \iota_{A,B}$ und $\varphi \circ \iota_{F(X),A[X]} = \varphi_0$. Die erste dieser Beziehungen bedeutet $\varphi(\iota_{A,A[X]}(a)) = \iota_{A,B}(a) = a$ für alle $a \in A$, die erste Behauptung. Aus der zweiten Beziehung folgt analog $\varphi(\iota_{F(X),A[X]}(x)) = j(x)$ für alle $x \in X \subseteq F(X)$. Die Eindeutigkeit von $\varphi$ folgt in gewohnter Weise, weil $\varphi$ auf dem Erzeugendensystem $A \cup X$ von $A[X]$ vorgegeben ist. □

**UE 297** ► **Übungsaufgabe 4.2.3.6.** (W) Zeigen Sie, dass Polynomalgebren $A[X]$ für gegebenes $A$ und $X$ bis auf Äquivalenz in einer geeigneten Kategorie eindeutig bestimmt sind. In Varietäten sind Polynomalgebren bis auf Isomorphie eindeutig bestimmt. ◄ **UE 297**

Für die Varietät der kommutativen Ringe mit Einselement erhält man tatsächlich die klassischen Polynomringe:

**UE 298** ► **Übungsaufgabe 4.2.3.7.** (V) Sei $\mathcal{V} = \mathcal{Rng}_1$ die Varietät der kommutativen Ringe mit 1, $R \in \mathcal{Rng}_1$ und $X$ eine Variablenmenge. ◄ **UE 298**

1. Zeigen Sie: Ist $X = \{x\}$, so lässt sich ist der Polynomring $R[x]$ im Sinn von 3.4.6 auch als Polynomalgebra $R[x]$ im Sinn von Definition 4.2.3.1 deuten.
2. Zeigen Sie: Definiert man rekursiv $R[x_1, \ldots, x_{n+1}] := R[x_1, \ldots, x_n][x_{n+1}]$, so lässt sich $R[x_1, \ldots, x_n]$ auch als Polynomalgebra $R[\{x_1, \ldots, x_n\}]$ im Sinn von Definition 4.2.3.1 deuten.
3. Beschreiben Sie $R[X]$ für unendliches $X$.

Als Hintergrund sind abstraktere Verträglichkeiten zwischen freien Algebren und Polynomalgebren interessant:

**UE 299** ► **Übungsaufgabe 4.2.3.8.** Sei $\mathcal{V}$ eine Varietät und $A \in \mathcal{V}$. Zeigen Sie: ◄ **UE 299**

1. (F) Sind $X_1$ und $X_2$ disjunkte Variablenmengen, so gilt $A[X_1][X_2] \cong A[X_1 \cup X_2]$.
2. (D) Ist $X$ eine unendliche Variablenmenge, so ist $A[X]$ ein direkter Limes der $A[X_0]$, wobei $X_0$ alle endlichen Teilmengen durchläuft. Präzisieren Sie diese Aussage und führen Sie den Beweis.

Sei $p$ ein Polynom über der Algebra $A \in \mathcal{V}$ in Variablen aus $X = \{x_1, \ldots, x_n\}$, d.h. $p \in A[x_1, \ldots, x_n]$. Wir schreiben in dieser Situation auch $p = p(x_1, \ldots, x_n)$. Zu einer Variablenbelegung $j : x_i \mapsto a_i$ gibt es laut Satz 4.2.3.5 ($B = A$ setzen) genau einen Homomorphismus (*Einsetzungshomomorphismus*) $\varphi_j \colon A[x_1, \ldots, x_n] \to A$, der $j$ fortsetzt, d.h. $\varphi_j(x_i) = a_i$ für $i = 1, \ldots, n$ erfüllt, und auf $A$ die Identität ist. Wir nennen $p(a_1, \ldots, a_n) := \varphi_j(p)$ den *Wert* des Polynoms $p$ an der Stelle $(a_1, \ldots, a_n)$. Die Funktion $A^n \to A$, $(a_1, \ldots, a_n) \mapsto p(a_1, \ldots, a_n)$ heißt die vom Polynom $p$ induzierte (verallgemeinerte) *Polynomfunktion* und wird meist gleichfalls mit $p$ bezeichnet, obwohl es sich begrifflich um verschiedene Objekte handelt. Der historische Grund: In vielen interessanten Fällen, insbesondere im klassischen Fall von Polynomen über einem unendlichen Körper, induzieren verschiedene Polynome verschiedene Polynomfunktionen. (Denn sind zwei Polynomfunktionen gleich, so ist ihre Differenz die Nullfunktion, die nur vom Nullpolynom dargestellt wird, weil jedes andere Polynom nur endlich viele Nullstellen hat. Also stimmen die Polynome überein.) Aber schon über einem endlichen Körper mit $q$ Elementen stellt nicht nur das Nullpolynom, sondern auch das Polynom $x^q - x$ die Nullfunktion dar (siehe Kapitel 6).

**UE 300** ► **Übungsaufgabe 4.2.3.9.** (V) Zeigen Sie: Ist $A \in \mathcal{V}$, so bildet die Menge $P(x_1, \ldots, x_n)$ aller Polynomfunktionen von $A^n \to A$ bezüglich der punktweise definierten Funktionen selbst wieder eine Algebra aus $\mathcal{V}$. $P(x_1, \ldots, x_n)$ ist homomorphes Bild der Polynomalgebra $A[x_1, \ldots, x_n]$. ◄ **UE 300**

**UE 301** ► **Übungsaufgabe 4.2.3.10.** (B) Sei $\mathcal{Ab}$ die Klasse aller abelschen Gruppe $\mathcal{G} = (G, +, 0, -)$. ◄ **UE 301**

1. Beschreiben Sie (möglichst explizit) das Koprodukt einer abelschen Gruppe $\mathcal{G}$ mit der von einem Element frei erzeugten abelschen Gruppe, also die Polynomalgebra $\mathcal{G}[x]$ (in $\mathcal{Ab}$). (Genauer: Beschreiben Sie die Elemente dieser Algebra, und erklären Sie, was die Gruppenoperation mit zwei solchen Elementen macht.)
2. Sei $X$ nun eine beliebige Menge von Variablen. Beschreiben Sie die Polynomalgebra $\mathcal{G}[X]$.
3. Beschreiben Sie die von einem beliebigen Element von $\mathcal{G}[X]$ induzierte Polynomfunktion.

### 4.2.4 Der Gruppenring und Monoidring

Inhalt in Kurzfassung: Auch beim Gruppenring werden (so wie beim Koprodukt zweier Algebren) zwei Strukturen in eine einzige „verklebt“, so dass man darin beide ursprünglichen möglichst „frei“ wiederfindet. Allerdings handelt es sich diesmal nicht um Algebren des gleichen Typs, sondern um eine Verschmelzung aus Gruppe und Ring. Als Anwendung beleuchten wir den Polynomring über einem kommutativen Ring mit 1 noch von einer weiteren Seite.

Eine gewisse Ähnlichkeit mit Koprodukten, wo zu gegebenen Strukturen eine diese umfassende konstruiert wird, hat auch der Gruppenring. Wie sein Name schon andeutet, liefert seine Konstruktion, ausgehend von einer Gruppe $G$ und einem Ring $R$, eine Struktur $R(G)$, in die sowohl $G$ als auch $R$ eingebettet werden können. In Hinblick auf Polynomringe über kommutativen Ringen mit 1 wollen wir auch die etwas allgemeineren aber völlig analog definierten Monoidringe betrachten.

**Definition 4.2.4.1.** Sei $R$ ein Ring mit Einselement $1_R \neq 0_R$ und $M$ ein Monoid. Der *Monoidring* $R(M)$ von $R$ über $M$ trägt die additive Struktur der direkten Summe $\bigoplus_{h \in M} R$. Für ein Element $r = (r_m)_{m \in M} \in R(M)$ schreiben wir auch $\sum_{m \in M} r_m m$, wobei nur für endlich viele $m \in M$ der Koeffizient $r_m$ von $0_R$ verschieden ist. Mit dieser Notation hat die Addition die Form

$$\sum_m r_m m + \sum_m s_m m = \sum_m (r_m + s_m) m.$$

Die Multiplikation dehnt die Festsetzung $(r_{m_1} m_1)(s_{m_2} m_2) := (r_{m_1} s_{m_2})(m_1 m_2)$ in distributiver Weise aus, also

$$\left(\sum_{m_1} r_{m_1} m_1\right) \cdot \left(\sum_{m_2} s_{m_2} m_2\right) := \sum_m t_m m.$$

Dabei entspricht

$$t_m := \sum_{(m_1,m_2)\in M^2:\ m_1m_2=m} r_{m_1}s_{m_2}$$

der *Faltung* bezüglich der Halbgruppenoperation. Zu beachten ist, dass de facto nur endliche Summen auftreten. Ist $M$ sogar eine Gruppe, so heißt $R(M)$ auch *Gruppenring*.

Von Interesse sind folgende Beobachtungen.

**Proposition 4.2.4.2.** *Sei $R$ ein kommutativer Ring mit 1 und $M$ ein Monoid mit Einselement $e_M$.*

1. *Bei der in 4.2.4.1 definierten Struktur $R(M)$ handelt es sich um einen Ring mit Einselement.*
2. *Die Abbildung $\iota_{R,R(M)}\colon R \to R(M)$, $r \mapsto re_M = \sum_{m\in M} r_m m$, mit $r_{e_M} = r$ und $r_m = 0_R$ für alle $m \in M \setminus \{e_M\}$ ist eine isomorphe Einbettung des Ringes $R$ in $R(M)$.*
3. *Die Abbildung $\iota_{M,R(M)}\colon M \to R(M)$, $m_0 \mapsto 1_R m_0 = \sum_{m\in M} r_m m$ mit $r_{m_0} = 1_R$ und $r_m = 0_R$ für alle $m \in G \setminus \{m_0\}$, ist eine isomorphe Einbettung von $M$ in die multiplikative Halbgruppe von $R(M)$.*
4. *Bei festem $M$ induziert jeder Homomorphismus $f\colon R_1 \to R_2$ kommutativer Ringe $R_1$ und $R_2$ einen eindeutigen Ringhomomorphismus $\bar{f}\colon R_1(M) \to R_2(M)$ mit $\bar{f} \circ \iota_{R_1,R_1(M)} = \iota_{R_2,R_2(M)} \circ f$.*
5. *Bei festem $R$ induziert jeder Monoidhomomorphismus $f\colon M_1 \to M_2$ einen eindeutigen Ringhomomorphismus $\bar{f}\colon R(M_1) \to R(M_2)$ mit $\bar{f} \circ \iota_{M_1,R(M_1)} = \iota_{M_2,R(M_2)} \circ f$.*

**UE 302 ► Übungsaufgabe 4.2.4.3.** (V) Beweisen Sie Proposition 4.2.4.2. **◄ UE 302**

Wir wollen uns zum Abschluss überlegen, dass der Polynomring über einem beliebigen kommutativen Ring $R$ mit 1 und einer beliebigen Variablenmenge $X$ als Monoidring realisiert werden kann. Und zwar nehmen wir als Monoid das additive Monoid $M := \bigoplus_{x\in X} \mathbb{N}$. Ein typisches Element des Monoidrings $R(M)$ hat die Gestalt $\sum_{m\in M} r_m m$, wobei $r_m \neq 0$ nur für endlich viele $m$ gilt. Ein Element $m \in M$ ist von der Form $m = (n_x)_{x\in X}$, $n_x \in \mathbb{N}$, wieder mit $n_x \neq 0$ nur für endlich viele $x \in X$, etwa $x_1, \ldots, x_k$. Dann schreiben wir das Element $m$ auch als *Monom* $x_1^{n_{x_1}} x_2^{n_{x_2}} \ldots x_k^{n_{x_k}}$ an, wobei es auf die Reihenfolge der Faktoren nicht ankommt. Somit ist jedes $\sum_{m\in M} r_m m \in R(M)$ auch als Polynom über $R$ in den Variablen $x \in X$ lesbar. Mit einiger Arbeit aber ohne grundsätzliche Schwierigkeiten überzeugt man sich davon, dass sich diese formale Ähnlichkeit auch inhaltlich rechtfertigen lässt:

**Theorem 4.2.4.4.** Sei $R$ ein kommutativer Ring mit 1 und $X$ eine Menge von Variablen. Dann lässt sich der Monoidring $R(M)$ von $R$ über dem Monoid $M := \bigoplus_{x\in X} \mathbb{N}$ (direkte Summe von $|X|$ Kopien des additiven Monoids $\mathbb{N}$) als Polynomalgebra (= Polynomring) $R[X]$ im Sinne von Definition 4.2.3.1 über $R$ in der Variablenmenge $X$ auffassen.

**UE 303 ► Übungsaufgabe 4.2.4.5.** (V) Beweisen Sie Theorem 4.2.4.4. **◄ UE 303**

# 5 Teilbarkeit

Die Frage nach Teilbarkeit stellt sich, weil die Multiplikation in Ringen wie $\mathbb{Z}$ nicht uneingeschränkt zur Division umkehrbar ist. Für den Großteil dieses Kapitels orientieren wir uns an der Teilbarkeitslehre in den natürlichen bzw. ganzen Zahlen, insbesondere am Fundamentalsatz der Arithmetik von der eindeutigen Primfaktorzerlegung (Satz 3.1.3.2). Unsere Untersuchungen sind von der Frage geleitet, in welchen Strukturen ähnliche Begriffsbildungen und Resultate möglich sind. Beginnend mit Halbgruppen werden wir in 5.1 Integritätsbereiche und in 5.2 noch speziellere Klassen betrachten: faktorielle, Hauptideal- und euklidische Ringe. Der letzte Abschnitt des Kapitels (5.3) enthält Anwendungen und Ergänzungen.

## 5.1 Elementare Teilbarkeitslehre

Wir beginnen in 5.1.1 mit einer Rekapitulation der eindeutigen Primfaktorzerlegung in $\mathbb{N}$. Dabei fällt auf, dass Teilbarkeit alleine über die multiplikative Struktur definiert ist. Um klarer zu sehen, worauf es ankommt, stellen wir zunächst einfache Beobachtungen an, die sich auf kommutative Monoide ohne zusätzliche Struktur beziehen (5.1.2). Bald jedoch (5.1.3) wird sich unser Interesse der multiplikativen Halbgruppe von Ringen und vor allem Integritätsbereichen zuwenden. Für das bessere Verständnis der Problemlage entscheidend sind ein einfacher Zusammenhang zwischen Teilbarkeit von Elementen und den erzeugten Hauptidealen sowie zwischen primen und irreduziblen Elementen (5.1.4).

### 5.1.1 Der Fundamentalsatz der Zahlentheorie als Paradigma

Inhalt in Kurzfassung: Erste Überlegungen zur Frage, was bei einer eventuellen Verallgemeinerung des Satzes von der eindeutigen Primfaktorzerlegung in $\mathbb{N}$ auf allgemeinere Situationen zu beachten ist.

Wie wir schon in Abschnitt 3.1.3 gesehen haben, eröffnet der Satz von der eindeutigen Primfaktorzerlegung in den natürlichen Zahlen einen äußerst klaren Blick auf die multiplikative Struktur. Und zwar lässt sich aufgrund dieses Satzes das multiplikative Monoid von $\mathbb{N}^+$ als mit der Menge $\mathbb{P}$ der Primzahlen indizierte unendliche direkte Summe von Kopien des additiven Monoids auf $\mathbb{N}$ interpretieren, also als freies abelsches Monoid über der (abzählbar unendlichen) freien Erzeugendenmenge $\mathbb{P}$. Daraus lässt sich überdies ablesen, dass es ggT (größte gemeinsame Teiler) und kgV (kleinste gemeinsame Vielfache) nicht nur für je zwei Zahlen gibt, sondern sogar für beliebige Teilmengen von $\mathbb{N}$ (inklusive 0). Es liegt also ein vollständiger Verband vor, der überdies distributiv ist. Unser Ziel ist es, ähnliche Einsichten in die Struktur einer möglichst großen Klasse von algebraischen Strukturen zu bekommen.

Schon angesichts der Erweiterung von $\mathbb{N}$ auf $\mathbb{Z}$ stößt man auf eine Schwierigkeit. Weil für alle $a \in \mathbb{Z}$ sowohl $a|-a$ als auch $-a|a$ gilt, lässt sich die Antisymmetrie der Teilerrelation nicht aufrecht erhalten. Es zeigt sich, dass so wie in $\mathbb{Z}$ auch in allgemeinerem Kontext diese Schwierigkeit leicht ausgeräumt werden kann, indem man zur von der Quasiordnung induzierten Halbordnung übergeht (siehe Definition 2.1.1.13).
Es fällt auf, dass die Teilbarkeitsrelation in $\mathbb{N}$ nur von der multiplikativen Struktur bestimmt ist. Es liegt also auf der Hand, mit Halbgruppen oder sogar beliebigen Algebren vom Typ (2) zu beginnen und zu studieren, welche zusätzlichen Eigenschaften der natürlichen Zahlen entscheidend sind, um die Begriffsbildungen und Ergebnisse von dort auf allgemeinere Strukturen übertragen zu können. Wenig überraschend spielen sowohl Assoziativität, Einselement als auch Kommutativität eine wichtige Rolle, aber auch Kürzbarkeit. Abgesehen von der Sonderrolle der 0 sind all diese Bedingungen in der multiplikativen Halbgruppe eines Integritätsbereichs[1] erfüllt. Tatsächlich erweist sich die Klasse der Integritätsbereiche als geeignet, um eine elementare Teilbarkeitslehre sinnvoll zu formulieren. Will man auch Analoga zur Eindeutigkeit der Primzahlzerlegung beweisen (gilt eine solche, spricht man von einem faktoriellen Ring), muss man allerdings speziellere Bedingungen voraussetzen, was Abschnitt 5.2 vorbehalten sein wird.

### 5.1.2 Teilbarkeit als Quasiordnung auf kommutativen Monoiden

Inhalt in Kurzfassung: Der Begriff der Teilbarkeit wird von $\mathbb{N}$ auf kommutative Monoide verallgemeinert, wo es sich i.A. zwar um keine Halbordnung, immerhin aber um eine Quasiordnung handelt. Die zugehörige Äquivalenzrelation (im Sinne von Definition 2.1.1.13) nennt man Assoziiertheit.

Will man lediglich die Definition von Teilbarkeit vom System $\mathbb{N}$ der natürlichen Zahlen auf möglichst allgemeine Strukturen verallgemeinern, so reicht dafür eine binäre Operation $\circ$ auf irgendeiner Trägermenge.

**Definition 5.1.2.1.** Sei $\mathfrak{G} = (G, \cdot)$ eine Algebra vom Typ (2). Sind $a, b \in G$, dann heißt $a$ ein *Teiler* von $b$, $b$ durch $a$ *teilbar* und $b$ ein *Vielfaches* von $a$, wenn es ein $c \in G$ gibt mit $b = ac := a \cdot c$. In diesem Fall sagen wir auch $a$ *teilt* $b$, symbolisch: $a|b$. Liegt ein Ring vor, so beziehen wir uns in Teilbarkeitsfragen stets auf die binäre Operation der multiplikativen Halbgruppe des Ringes.

Man könnte Teilbarkeit genauso durch die Gleichung $b = ca$ definieren statt durch $b = ac$ und z.B. zwischen Links- bzw. Rechtsteilbarkeit unterscheiden. Sehr bald werden wir uns aber auf den kommutativen Fall konzentrieren, für den dies hinfällig ist.

**Proposition 5.1.2.2.** *Für die Teilbarkeitsrelation $|$ auf einer Algebra $\mathcal{G} = (G, \cdot)$ vom Typ (2) gilt:*

1. *Gibt es in $\mathcal{G}$ ein neutrales Element $1_G$ bezüglich $\cdot$, so ist $|$ reflexiv. In diesem Fall ist $1_G$ ein kleinstes Element bezüglich $|$, d.h. $1_G|a$ für alle $a \in G$.*

[1] Bei Teilbarkeit interessiert uns die Menge $\{1, 2, 3, \ldots\}$ mehr als die Menge $\{0, 1, 2, \ldots\}$, besonders wenn der Ring sogar ein Integritätsbereich ist.

2. *Ist $\cdot$ assoziativ, so ist $|$ transitiv.*

3. *Ist $\mathcal{G}$ ein Monoid, so ist $|$ eine Quasiordnung.*

4. *Gibt es ein absorbierendes Element $0_G \in G$ (das ist ein Element mit $0_G a = a0_G = 0_G$ für alle $a \in G$), so ist $0_G$ größtes Element bezüglich $|$, d.h. $a|0_G$ für alle $a \in G$.*

*Beweis.* Die erste Behauptung liest man aus $a = 1_G a$ ab. Für die zweite schließt man von $a|b$ und $b|c$ auf die beiden Gleichungen $b = at_1$ und $c = bt_2$ mit geeigneten $t_1, t_2 \in G$. Setzt man die erste in die zweite ein, erhält man $c = (at_1)t_2 = a(t_1 t_2)$, also $a|c$. Die dritte Behauptung fasst lediglich die ersten beiden zusammen, und die vierte ist aus $0_G = a0_G$ für alle $a \in G$ ersichtlich. □

Wir wollen ab nun voraussetzen, dass wir es mit einem Monoid $\mathcal{M} = (M, \cdot, 1_M)$ und somit mit einer Quasiordnung $|$ auf $\mathcal{M}$ zu tun haben. Laut Satz 2.1.1.11 induziert $|$ als Quasiordnung eine Äquivalenzrelation $\sim$, die durch

$$a \sim b :\Leftrightarrow a|b \text{ und } b|a$$

definiert ist. Elemente mit $a \sim b$ heißen *assoziiert*. Gleichfalls nach Satz 2.1.1.11 sind die Relationen $|$ und $\sim$ miteinander verträglich in dem Sinn, dass die Definition

$$[a]_\sim | [b]_\sim :\Leftrightarrow a|b$$

der Teilbarkeit zwischen Äquivalenzklassen nicht von der speziellen Wahl der Vertreter $a, b$ abhängt und somit diese Relation $|$ auf der Menge $M/_\sim$ der Äquivalenzklassen sogar eine Halbordnungsrelation ist mit kleinstem Element $[1_M]_\sim$. Im kommutativen Fall ist nicht nur die Teilerrelation, sondern auch die binäre Operation auf $\mathcal{M}$ mit der Assoziiertheitsrelation $\sim$ verträglich:

**Satz 5.1.2.3.** *Sei $\mathcal{M} = (M, \cdot, 1_M)$ ein kommutatives Monoid. Dann gilt:*

1. *Die Assoziiertheitsrelation $\sim$ auf $\mathcal{M}$ ist eine Kongruenzrelation.*

2. *Die Teilbarkeitsrelation im Faktormonoid $\mathcal{M}/_\sim$ erhält man auch als die von der Teilbarkeitsquasiordnung auf $\mathcal{M}$ auf der Faktormenge bezüglich $\sim$ induzierte Halbordnung. Diese Halbordnung nennen wir auch die* Teilbarkeitshalbordnung *von $\mathcal{M}$ modulo Assoziiertheit.*

3. *Die Menge $E = E(\mathcal{M}) := [1_M]_\sim = \{m \in M : \ m \sim 1_M\} = \{m \in M : \ m|1_M\}$ ist eine Gruppe, genannt die* Einheitengruppe *von $\mathcal{M}$, deren Elemente (= Teiler von $1_M$)* Einheiten *heißen.*

4. *Allgemein gilt $aE \subseteq [a]_\sim$ für alle $a \in M$. Ist das Monoid $\mathcal{M}$ kürzbar[2], dann gilt sogar $[a]_\sim = aE$.*

[2] Zur Erinnerung: Eine binäre Operation heißt kürzbar, wenn die Kürzungsregel gilt, dass nämlich aus $ax = bx$ oder $xa = xb$ stets $a = b$ folgt.

*Beweis.* 1. Satz 2.1.1.11 besagt u.a., dass $\sim$ eine Äquivalenzrelation ist. Es genügt daher, die Verträglichkeit mit der binären Operation nachzuweisen. Um das zu zeigen, sei $a_1 \sim a_2$ und $b_1 \sim b_2$. Insbesondere bedeutet dies $a_1|a_2$ und $b_1|b_2$. Folglich gibt es $x, y \in M$ mit $a_2 = a_1x$ und $b_2 = b_1y$. Aufgrund von Assoziativität und Kommutativität folgt daraus $a_2b_2 = a_1xb_1y = (a_1b_1)(xy)$, also $a_1b_1|a_2b_2$. Symmetrisch zeigt man $a_2b_2|a_1b_1$; insgesamt gilt also $a_1b_1 \sim a_2b_2$.

2. Folgt direkt aus den Konstruktionen.

3. Das war Inhalt von Proposition 3.1.1.3.

4. Wenn $a' \in aE$ ist, dann gibt es eine Einheit $e \in E = E(\mathcal{M})$ mit $a' = ae$. Weil $\sim$ Kongruenz ist, können wir $e \sim 1 \Rightarrow a' = ae \sim a1 = a$ schließen, also $a' \in [a]_\sim$.
Sei umgekehrt $a' \in [a]_\sim$ beliebig. Nach Definition von $\sim$ gibt es $x, y \in M$ mit $a' = ax$ und $a = a'y$. Daraus erhalten wir $a = a'y = (ax)y = a(xy)$, also $a1 = a(xy)$. Aus der Kürzbarkeit folgt $1 = xy$. Folglich sind $x, y \in E$ Einheiten und $a' = ay \in aE$. Damit ist auch die Inklusion $[a]_\sim \subseteq aE$ gezeigt. □

**UE 304** ► **Übungsaufgabe 5.1.2.4.** (B) Geben Sie ein kommutatives (notwendig nicht kürzbares) Monoid an, in dem die Gleichheit aus der 4. Aussage von Satz 5.1.2.3 nicht gilt. ◄ **UE 304**

### 5.1.3 Teilbarkeit in Integritätsbereichen

Inhalt in Kurzfassung: Von besonderem Interesse ist Teilbarkeit bezüglich des multiplikativen Monoids in Integritätsbereichen. Zusätzliche Aspekte kommen ins Spiel, weil es in diesem Kontext mit der Addition ja auch noch eine zweite binäre Operation gibt, die durch das Distributivgesetz mit der Multiplikation verbunden ist. Als interessante Beispiele kommen quadratische Zahlringe zur Sprache, das sind Unterringe der komplexen Zahlen, die von $\mathbb{Z}$ und der Wurzel einer quadratfreien ganzen Zahl erzeugt werden.

Das kommutative Monoid, dessen Teilbarkeitshalbordnung uns besonders interessiert, ist die multiplikative Halbgruppe eines kommutativen Ringes $\mathcal{R}$ mit 1, für den wir in üblicher Weise $\mathcal{R} = (R, +, 0, -, \cdot, 1)$ schreiben. Sei $H := R/_\sim$ und $(H, |)$ die Teilbarkeitshalbordnung auf $\mathcal{R}$. Hat $A \subseteq H$ ein Supremum $v \in H$, so heißt $v$ das *kleinste gemeinsame Vielfache* der Elemente aus $A$, abgekürzt $\mathrm{kgV}(A)$; analog heißt das Infimum von $A$ (sofern vorhanden) *größter gemeinsamer Teiler* der Elemente von $A$, abgekürzt $\mathrm{ggT}(A)$. Die entsprechenden Sprechweisen verwendet man auch für die Elemente der Assoziiertenklassen $a \in A$. Genauer: Das Ringelement $s$ heißt *ein* kgV der Ringelemente $r_i$, $i \in I$, wenn $[s]_\sim = \mathrm{kgV}(A)$ in $H$ mit $A = \{[r_i]_\sim : \ i \in I\}$; analog für ggT. Man beachte, dass mit $s$ auch jedes $s' \sim s$ ein kgV bzw. ein ggT der $r_i$ oder auch von zu den $r_i$ assoziierten $r_i' \sim r_i$ ist.
In ähnlicher Weise werden wir auch andere Begriffe, die mit der Bildung von Assoziierten verträglich sind, von $H$ auf $R$ übertragen oder umgekehrt, ohne dies nochmals ausführlich zu diskutieren. Weitere Beispiele dieser Art (teilweise vorausgreifend): Ein

*unechter Teiler* von $r \in R$ ist ein solcher, der zu $r$ assoziiert ist. Jeder andere Teiler heißt ein *echter Teiler*. Ein *trivialer Teiler* von $r$ ist ein solcher, der bis auf Assoziiertheit mit 1 oder $r$ übereinstimmt. Ein Teiler, der kein trivialer Teiler ist, heißt ein *nichttrivialer Teiler* von $r$. Ein Element $r \in R$ heißt *irreduzibel*, wenn es bezüglich Teilbarkeit oberer Nachbar von $1 \in R$ ist, was eigentlich bedeutet: wenn $[r]_\sim$ in $H$ ein oberer Nachbar des (in $H$ kleinsten) Elements $[1]_\sim = E(\mathcal{R})$ ist.
Diese Diskussion wird obsolet, wenn es eine Teilmenge $T \subseteq R$ gibt, die aus jeder Assoziiertenklasse genau einen Vertreter enthält und außerdem ein multiplikatives Untermonoid des Ringes $R$ bildet. So ein $T$ wollen wir eine *Transversale* nennen. Die Elemente von $T$ nennt man oft auch *normiert*. Die wichtigsten Beispiele: $\mathbb{N}$ ist eine Transversale im Ring $\mathbb{Z}$. Im Polynomring $K[x]$ bilden die Polynome mit höchstem Koeffizienten 1 (die sogenannten *monischen* oder *normierten*) zusammen mit dem Nullpolynom eine Transversale.
Mit $E(\mathcal{R})$ oder auch $R^*$ bezeichnen wir die Einheitengruppe des multiplikativen Monoids $(R, \cdot, 1)$. Tatsächlich sind alle Voraussetzungen von Satz 5.1.2.3 erfüllt, überdies gibt es ein absorbierendes Element, nämlich $0 \in R$. Deshalb gelten Teilbarkeitsregeln in Monoiden auch für Elemente $a, b, c$ eines kommutativen Rings $R$ mit 1:

- $a|0$
- $1|a$
- $a|a$
- $a|b$ und $b|c \Rightarrow a|c$
- $a|b \Rightarrow a|bc$
- $a|b$ und $c|d \Rightarrow ac|bd$
- für $c = d$ daher $a|b \Rightarrow ac|bc$ und für kürzbares $c$ sogar $a|b \Leftrightarrow ac|bc$ (man beachte, dass im Fall eines Integritätsbereichs alle $c \neq 0$ kürzbar sind)
- $aE := \{ae : \ e \in E\} \subseteq [a]_\sim$ mit Gleichheit in Integritätsbereichen
- $a|b$ und $a|c \Rightarrow a|b+c$ (weil ja aus $b = xa$ und $c = ya$ sofort $b+c = xa+ya = (x+y)a$ folgt; dies stellt eine Verbindung zur additiven Struktur von $R$ her)

Zur Illustration folgen nun einige Beispiele:

**Beispiele 5.1.3.1.**

1. Im Integritätsbereich $\mathfrak{R} = (\mathbb{Z}, +, 0, -, \cdot, 1)$ der ganzen Zahlen ist die Einheitengruppe $E(\mathcal{R})$ gegeben durch $\{-1, 1\}$. Die Assoziiertenklasse $[a]_\sim$ eines $a \in \mathbb{Z}$ ist $\{a, -a\}$.

2. In einem Körper $\mathfrak{K} = (K, +, 0, -, \cdot, 1)$ ist $E(\mathcal{K}) = K \setminus \{0\}$. Es gibt nur zwei Assoziiertenklassen, nämlich $[0]_\sim = \{0\}$ und $[1]_\sim = K \setminus \{0\}$.

3. (vgl. Proposition 3.4.6.5) Im Polynomring $\mathfrak{R} = (R[x], +, 0, -, \cdot, 1)$ über einem Ring $\mathfrak{R}_0 = (R, +, 0, -, \cdot, 1)$ stimmen die Einheiten mit denen von $\mathfrak{R}_0$ überein, sofern man die konstanten Polynome mit den Elementen von $R$ identifiziert. Ist $\mathfrak{R}_0$ sogar ein Körper, so ist $E(\mathcal{R}) = E(\mathcal{R}_0) = R \setminus \{0\}$ und folglich $[p]_\sim = \{rp : \ r \in R, r \neq 0\}$ für $p \in R[x]$.

4. Sei $D \neq 1$ eine quadratfreie ganze Zahl, also $t^2|D$ für $t \in \mathbb{Z}$ nur, wenn $t \in \{1, -1\}$. Die Menge $\mathbb{Z}[\sqrt{D}] := \{a+b\sqrt{D} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ bildet, wie man unschwer nachweist, einen Unterring von $\mathbb{C}$, einen sogenannten *quadratischen Zahlring* . Ein nützliches Instrument bei der Analyse quadratischer Zahlringe ist die sogenannte *Normfunktion* $N\colon \mathbb{Z}[\sqrt{D}] \to \mathbb{Z}$, $N(a + b\sqrt{D}) := (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - b^2D$, weil sie als multiplikativer Homomorphismus (es gilt $N(xy) = N(x)N(y)$) die Möglichkeit eröffnet, Teilbarkeitsfragen in den sehr gut verstandenen Ring $\mathbb{Z}$ der ganzen Zahlen zu übertragen.

**UE 305** ► **Übungsaufgabe 5.1.3.2.** (B) Sei $D$ eine ganze Zahl und $R := \mathbb{Z}[\sqrt{D}]$ der von $\mathbb{Z}$ und $\sqrt{D}$ erzeugte Unterring von $\mathbb{C}$. ◄ **UE 305**

1. Man zeige, dass $R$ mit der gewöhnlichen Addition und Multiplikation von $\mathbb{C}$ einen Integritätsbereich bildet.

2. Man bestimme für $D < 0$ die Einheiten in $\mathcal{R}$.

3. Man zeige, dass für $D = 2$ unendlich viele verschiedene Einheiten in $\mathbb{Z}[\sqrt{D}] \subseteq \mathbb{R}$ existieren.

Hinweis: Übersetzen Sie die Eigenschaft „$a + b\sqrt{D}$ ist eine Einheit“ in eine Eigenschaft von $N(a + b\sqrt{D})$.

### 5.1.4 Teilbarkeit und Hauptideale – prime und irreduzible Elemente

Inhalt in Kurzfassung: Die Teilbarkeit von Elementen übersetzt sich in die umgekehrte Inklusionsbeziehung der erzeugten Hauptideale, was besonders in Hauptidealringen (das sind Integritätsbereiche, in denen jedes Ideal ein Hauptideal ist) wirksame Möglichkeiten der Strukturanalyse eröffnet. Eine wichtige Rolle spielen dabei irreduzible und Primelemente. In $\mathbb{Z}$ sind beide Begriffe äquivalent, in beliebigen Integritätsbereichen ist jedes Primelement irreduzibel, nicht jedoch umgekehrt.

Wir wollen nun den engen Zusammenhang zwischen der Teilbarkeit von Elementen und den Hauptidealen $(a) = Ra = \{ra : \ r \in R\}$, $a \in R$, in einem kommutativen Ring $R$ mit Einselement studieren. Teilbarkeit und Assoziiertheit beziehen sich dabei natürlich auf das multiplikative Monoid von $R$.

**Proposition 5.1.4.1.** *Für zwei Elemente $a, b \in R$ gilt:*

1. *$a|b$ genau dann, wenn $(b) \subseteq (a)$.*

*2. $a \sim b$ genau dann, wenn $(b) = (a)$.*

*3. $(a) = R$ genau dann, wenn $a$ eine Einheit ist.*

*Beweis.* Aus $a|b$ folgt $b = ra$ mit $r \in R$, also $b \in (a)$ und $(b) \subseteq ((a)) = (a)$. Umgekehrt folgt aus $(b) \subseteq (a)$ insbesondere $b \in (a)$, wegen Proposition 3.4.1.6 also $b = ra$ mit einem $r \in R$, folglich $a|b$. Damit ist die erste Äquivalenz bewiesen. Die zweite Äquivalenz folgt daraus unmittelbar und somit, indem man $R = (1_R)$ beachtet, auch die dritte. □

Teilbarkeit zweier Elemente lässt sich also durch die Obermengenbeziehung der von diesen Elementen erzeugten Hauptidealen beschreiben, Assoziiertheit der Elemente durch die Gleichheit der von ihnen erzeugten Hauptideale. Auch die Frage, wann ein Hauptideal ein Primideal ist, lässt sich in eine Eigenschaft eines beliebigen erzeugenden Elementes übersetzen.

**Proposition 5.1.4.2.** *Für ein Element $p \in R$ sind die folgenden beiden Aussagen äquivalent:*

*1. Das von $p$ erzeugte Ideal $(p) = \{rp : \ r \in R\}$ ist ein Primideal.*

*2. Das Element $p$ ist keine Einheit, und für alle $a, b \in R$ gilt die Implikation*

$$p|ab \quad \textit{impliziert} \quad p|a \textit{ oder } p|b.$$

*Gilt eine dieser beiden Aussagen (und damit auch die andere) und ist $p \neq 0_R$, so nennt man $p$ ein* Primelement *in $R$.*

*Beweis.* Für die Implikation $1 \Rightarrow 2$ sei $(p)$ ein Primideal. Nach Definition von Primidealen folgt daraus $(p) \neq R$, weshalb $p$ nach der dritten Aussage in Proposition 5.1.4.1 keine Einheit sein kann. Gilt nun $p|ab$, so bedeutet das nach der ersten Aussage in Proposition 5.1.4.1 genau $ab \in (p)$. Nochmals nach Definition von Primidealen heißt das $a \in (p)$ oder $b \in (p)$, d.h. $p|a$ oder $p|b$. Alle Schlüsse lassen sich auch umkehren, weshalb die behauptete Äquivalenz gilt. □

Dass im Ring $R = \mathbb{Z}$ die Primelemente genau die Primzahlen sind, folgt leicht aus Satz 3.1.3.2 von der eindeutigen Primfaktorzerlegung:

**UE 306** ► **Übungsaufgabe 5.1.4.3.** (F) Beweisen Sie, dass $p \in \mathbb{N}$ genau dann eine Primzahl ist, wenn $p \neq 0$ ist und im Ring $\mathbb{Z}$ ein Primelement im Sinne der Definition in 5.1.4.2. ◄ **UE 306**

Wir haben bereits gesehen, dass alle Ideale $I \lhd \mathbb{Z}$ mit $I \neq \{0\}$ von der Gestalt $I = (m)$ mit $m = 1, 2, \ldots$ sind. Die Faktorringe $\mathbb{Z}/(m)$ sind die Restklassenringe $\mathbb{Z}_m$. Nach Satz 3.4.2.4 handelt es sich genau dann um Integritätsbereiche, wenn $(m)$ ein Primideal, also $m = p$ eine Primzahl ist. Weil alle $\mathbb{Z}_m$ endlich sind, ist $\mathbb{Z}_p$ nach Satz 3.4.2.1 sogar ein Körper, der sogenannte *Primkörper* mit $p$ Elementen. Wir bezeichnen ihn auch mit $\mathrm{GF}(p)$ als Abkürzung für *Galoisfeld* mit $p$ Elementen.

Es fällt auf, dass die Definition von Primzahlen (über sogenannte Irreduzibilität) eine andere war als die der Primelemente. Der Zusammenhang ergab sich erst durch den Satz von der eindeutigen Primfaktorzerlegung. Die allgemeine Definition von Irreduzibilität lautet wie folgt.

**Definition 5.1.4.4.** Sei $R$ ein kommutativer Ring mit Einselement und $p \in R$ keine Einheit. Dann heißt $p$ *irreduzibel*, wenn $p$ in der Teilbarkeitshalbordnung oberer Nachbar von 1 ist. Explizit bedeutet das: In jeder Darstellung $p = ab$ mit $a, b \in R$ ist einer der Faktoren $a$ oder $b$ eine Einheit.

Enthält $R$ wenigstens zwei verschiedene Elemente $0_R \neq 1_R$, so ist 0 keine Einheit, und man kann $a := 0$ und $b := 0$ setzen, um zu sehen, dass $p := 0$ nicht irreduzibel ist.

**UE 307** ► **Übungsaufgabe 5.1.4.5.** (F) Sei $R$ ein Integritätsbereich, $q, r, s \in R^\times$ mit $q = rs$. ◄ **UE 307**
Zeigen Sie: Bei $r$ handelt es sich genau dann um eine Einheit, wenn $q \sim s$. Schließen Sie daraus, dass für jedes $p \in R^\times$ die folgenden Bedingungen äquivalent sind:

1. Für alle $a, b \in R : (p = ab \;\Rightarrow\; a \sim 1 \;\vee\; b \sim 1)$.

1'. Für alle $a, b \in R : (p = ab \;\Rightarrow\; a|1 \;\vee\; b|1)$.

2. Für alle $a, b \in R : (p = ab \;\Rightarrow\; a \sim p \;\vee\; b \sim p)$.

2'. Für alle $a, b \in R : (p = ab \;\Rightarrow\; p|a \;\vee\; p|b)$.

3 Für alle $a, b \in R : (p = ab \;\Rightarrow\; a$ trivialer Teiler $\vee\; b$ trivialer Teiler$)$.

**UE 308** ► **Übungsaufgabe 5.1.4.6.** (F) Man bestimme im Ring $\mathbb{Z}_2[x]$ alle irreduziblen Polynome bis zum Grad 3. (Der Aufwand, der mit den an dieser Stelle verfügbaren Mitteln erforderlich ist, wird sich später mit etwas Theorie, die noch kommen wird, deutlich reduzieren lassen.) ◄ **UE 308**

In Ringen mit Nullteilern lässt sich über die Beziehung zwischen Primelementen und irreduziblen Elementen wenig sagen. So ist beispielsweise in $\mathbb{Z}_6$ das Element 2 (Kurzschreibweise für $2 + 6\mathbb{Z}$) wegen $2 = 2 \cdot 4$ nicht irreduzibel jedoch prim: Aus $2|ab$ mit $a, b \in \mathbb{Z}_6$ folgt $ab \in \{0, 2, 4\}$. Weil jedes Produkt, das aus den übrigen Elementen $1, 3, 5$ gebildet werden kann, ungerade ist, muss wenigstens einer der Faktoren $a$ oder $b$ selbst in $\{0, 2, 4\}$ liegen, also durch 2 teilbar sein. Also ist 2 tatsächlich prim in $\mathbb{Z}_6$.
In Integritätsbereichen ist das jedoch unmöglich. Gilt nämlich $p = ab$ für ein Primelement $p \in R$, so folgt aus $p|ab$ nach Definition $p|a$ oder $p|b$. O.B.d.A. nehmen wir $p|a$ an, also $a = pr$ mit $r \in R$. Folglich ist $p = ab = prb$. Kürzen von $p$ liefert $rb = 1_R$. Somit ist $b$ eine Einheit, $p$ also irreduzibel. Wir haben bewiesen:

**Proposition 5.1.4.7.** *Jedes Primelement $p \in R$ in einem Integritätsbereich $R$ ist irreduzibel.*

Wie man am folgenden Beispiel sieht, gilt, anders als zum Beispiel im Ring $R = \mathbb{Z}$, die Umkehrung nicht allgemein.

**UE 309 ► Übungsaufgabe 5.1.4.8.** (B) Sei $R = \mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$. **◄ UE 309**

1. Zeigen Sie, dass die Elemente 2 und 3 in $R$ irreduzibel aber nicht prim sind.
2. Finden Sie eine Primzahl $p \in \mathbb{Z}$, die im Ring $\mathbb{Z}[\sqrt{-5}]$ nicht irreduzibel ist.

Als Konsequenz dieser Übungsaufgabe werden wir den Ring $\mathbb{Z}[\sqrt{-5}]$ später auch als Beispiel eines nicht faktoriellen Ringes bemühen.

## 5.2 Faktorielle, Hauptideal- und euklidische Ringe

Von nun an beschränken wir unsere Untersuchungen auf Integritätsbereiche. Unter ihnen sind die *faktoriellen Ringe* definitionsgemäß genau jene, für die ein Analogon zum Fundamentalsatz der Zahlentheorie gilt (5.2.1). Sie lassen sich aber auch durch andere interessante Eigenschaften charakterisieren. Integritätsbereiche, in denen alle Ideale Hauptideale sind (sogenannte *Hauptidealringe* (5.2.2); $\mathbb{Z}$ und der Polynomring $K[x]$ über einem beliebigen Körper $K$ sind die prominentesten Beispiele), haben stets diese Eigenschaft. $\mathbb{Z}$ und $K[x]$ haben sogar eine noch stärkere Eigenschaft, nämlich Division mit Rest zu ermöglichen, was sie zu *euklidischen Ringen* macht (5.2.3). In faktoriellen Ringen gibt es auch stets kgV und ggT beliebiger Teilmengen. In Hauptidealringen lässt sich jeder ggT sogar als Linearkombination darstellen; in euklidischen Ringen gibt es, noch stärker, einen Algorithmus, um so eine Darstellung zu erhalten. Letzteres hat vielfältige Anwendungen, von denen wir etwas später welche kennenlernen werden.

### 5.2.1 Faktorielle Ringe

Inhalt in Kurzfassung: Faktorielle Ringe sind so definiert, dass für sie ein Analogon des Satzes von der eindeutigen Primfaktorzerlegung gilt. Präziser lässt sich diese Eigenschaft durch mehrere äquivalente Bedingungen charakterisieren, die ungenau (modulo Assoziiertheit und Reihenfolge von Faktoren und bei Vernachlässigung der 0) durch folgende Schlagworte angedeutet seien: Existenz und Eindeutigkeit von Faktorisierungen in irreduzible Elemente; Existenz von Faktorisierungen in Primelemente; irreduzible Elemente sind prim plus Teilerkettenbedingung (d.h. es gibt keine unendlichen echt absteigenden Teilerketten); das multiplikative Monoid ist frei. Der Hauptteil dieses Unterabschnitts ist dem Beweis der Äquivalenz gewidmet. Ordnungstheoretisch gelten, wenig überraschend, für den Teilerverband eines faktoriellen Ringes modulo Assoziiertheit ganz ähnliche Aussagen wie für den Teilerverband von $\mathbb{N}$. Insbesondere gibt es größte gemeinsame Teiler etc.

Ringe mit eindeutiger Primfaktorzerlegung lassen sich auf mehrere Arten charakterisieren. Die Situation in $\mathbb{N}$ bzw. in $\mathbb{Z}$ im Auge führen wir dazu die folgende Terminologie ein.

**Definition 5.2.1.1.** Sei $\mathcal{R} = (R, +, 0_R, -, \cdot, 1_R)$ ein Integritätsbereich, $\sim$ die Assoziiertheitsrelation auf $\mathcal{R}$. Wir vereinbaren folgende Sprechweisen:
In $\mathcal{R}$ gilt *Zerlegbarkeit in irreduzible* bzw. in *Primelemente*, wenn es zu jedem $r \in R$ mit $r \neq 0_R$ endlich viele irreduzible bzw. prime Elemente $p_1, \ldots, p_n \in R$ (nicht notwendigerweise paarweise verschieden!) gibt mit

$$r \sim \prod_{i=1}^{n} p_i.$$

(Für $n = 0$ ist das Produkt als $1_R$ zu lesen.) Das Produkt rechts heißt auch eine *Zerlegung* oder *Faktorisierung* von $r$.
Man spricht von *eindeutiger* Zerlegbarkeit, wenn je zwei derartige Darstellungen bis auf Assoziiertheit und bis auf die Reihenfolge der Faktoren übereinstimmen, genauer: Für je zwei Darstellungen

$$r \sim \prod_{i=1}^{n} p_i \quad \text{und} \quad r \sim \prod_{j=1}^{m} q_j$$

eines beliebigen $r \in R$ mit irreduziblen bzw. mit Primelementen $p_1, \ldots, p_n, q_1, \ldots, q_m \in R$ (wobei die $p_1, \ldots, p_n$ wieder nicht paarweise verschieden müssen; analog für $q_1, \ldots, q_m$) gilt $n = m$, und es gibt eine Permutation $\pi$ der Menge $\{1, \ldots, n\}$ mit $q_i \sim p_{\pi(i)}$ für alle $i = 1, \ldots, n$.

Eine erste Beobachtung zeigt:

**Proposition 5.2.1.2** (Eindeutigkeit der Primelementzerlegung)**.** *Sei $\mathcal{R}$ ein Integritätsbereich, $a \in \mathcal{R} \setminus E(\mathcal{R})$, $a \neq 0$, $a = p_1 \cdots p_r = q_1 \cdots q_s$ mit Primelementen $p_1, \ldots, p_r$ und $q_1, \ldots, q_s$. Dann ist $r = s$, und es gibt eine Permutation $\pi$ von $\{1, \ldots, r\}$ mit $p_i \sim q_{\pi(i)}$, $i = 1, \ldots, r$. Folglich bedeutet für einen Integritätsbereich Zerlegbarkeit in Primelemente bereits die eindeutige Zerlegbarkeit in Primelemente.*

*Beweis.* Wegen $p_1 | q_1 \cdot \ldots \cdot q_s$ und weil $p_1$ prim ist, muss $p_1 | q_j$ für ein geeignetes $j =: \pi(1)$ gelten. Als Primelement ist $q_j$ auch irreduzibel (siehe Proposition 5.1.4.7), folglich muss auch $q_j | p_1$, also $p_1 \sim q_j$ gelten, d.h. $p_1 = q_j e_1$ mit einer geeigneten Einheit $e_1$. Nach Kürzen von $q_j$ liefert das $e_1 p_2 \cdot \cdots \cdot p_r = q_1 \cdot \ldots \cdot q_{j-1} \cdot q_{j+1} \cdots q_s = q_1 \cdot \ldots \cdot q_{\pi(1)-1} \cdot q_{\pi(1)+1} \cdots q_s$. Durch wiederholte Anwendung dieser Überlegung erhält man schließlich die Behauptung. □

Für irreduzible Elemente gilt die entsprechende Aussage nicht.

**UE 310 ► Übungsaufgabe 5.2.1.3.** (W) Verwenden Sie Aufgabe 5.1.4.8, um einen Ring $R$ und ein Element $a \in R$ anzugeben, das in irreduzible Elemente zerlegbar ist, aber nicht *eindeutig* in irreduzible Elemente zerlegbar ist. **◄ UE 310**

Sehr wohl ist die Zerlegung in irreduzible Elemente eindeutig, wenn in $\mathcal{R}$ jedes irreduzible Element auch prim ist (wegen 5.2.1.2). Wir werden sehen, dass dies die Klasse der faktoriellen Ringe sogar charakterisiert. Zunächst definieren wir diese Klasse so, wie es sich anbietet, wenn man die traditionelle Definition von Primzahlen (nämlich als irreduzible Elemente) und ihre Rolle im Integritätsbereich $\mathbb{Z}$ direkt verallgemeinert.

**Definition 5.2.1.4.** Ein Integritätsbereich $\mathcal{R}$ heißt ein *faktorieller Ring*, wenn in $\mathcal{R}$ eindeutige Zerlegbarkeit in irreduzible Elemente gilt. Alternative Bezeichnungen sind auch *Ring mit eindeutiger Primfaktorzerlegung*, *Gauß'scher Ring*, manchmal *ZPE-Ring*[3].

Um eine äquivalente Charakterisierung der faktoriellen Ringe zu finden, verwenden wir die folgende Definition:

**Definition 5.2.1.5.** Ein Integritätsbereich $\mathcal{R} = (R, +, 0_R, -, \cdot, 1_R)$ erfüllt die *Teilerkettenbedingung*, wenn es keine unendlichen absteigenden Folgen echter Teiler gibt, das heißt:
Für alle Folgen $(a_n)_{n\in\mathbb{N}}$ von Elementen in $R$ mit $a_{n+1}|a_n$ für alle $n \in \mathbb{N}$ gibt es ein $n_0 \in \mathbb{N}$, sodass für $n \geq n_0$ stets $a_n \sim a_{n_0}$ gilt.

Die Teilerkettenbedingung ist eng mit dem Begriff der Irreduzibilität verbunden, wie der folgende Satz zeigt.

**Proposition 5.2.1.6.** *Wenn der Integritätsbereich $\mathcal{R} = (R, +, 0_R, -, \cdot, 1_R)$ die Teilerkettenbedingung erfüllt, dann gilt in $\mathcal{R}$ Zerlegbarkeit in irreduzible Elemente.*

*Beweis.* Wir nehmen an, dass es ein $a_0 \in R \setminus \{0\}$ gibt, welches nicht zu einem endlichen Produkt irreduzibler Elemente assoziiert ist. Dann kann $a_0$ weder eine Einheit noch ein irreduzibles Element sein, also lässt sich (nach Aufgabe 5.1.4.5) $a_0$ als Produkt $a_0 = rs$ schreiben, wobei weder $r \sim a_0$ noch $s \sim a_0$ gilt. Einer der beiden Teiler hat keine Zerlegung in irreduzible Elemente (sonst hätte ja auch $a_0$ eine). Wir haben also einen echten Teiler $a_1|a_0$ gefunden, der keine Zerlegung in irreduzible Elemente hat. Auf diese Weise ist es möglich, induktiv (hier spielt auch das Auswahlaxiom mit) eine unendliche echte Teilerkette $a_0, a_1, a_2, \ldots$ zu konstruieren. □

Der folgende Satz gibt liefert alternative (äquivalente) Möglichkeiten, faktorielle Ringe zu definieren.

**Satz 5.2.1.7.** *Sei $\mathcal{R} = (R, +, 0_R, -, \cdot, 1_R)$ ein Integritätsbereich, $\sim$ die Assoziiertheitsrelation auf $\mathcal{R}$ und $\mathcal{M} = (M, \cdot, 1_M)$ das Faktormonoid, das entsteht, wenn man das multiplikative Monoid der von 0 verschiedenen Elemente in $\mathcal{R}$ nach der Assoziiertheitsrelation faktorisiert. Dann sind folgende Bedingungen äquivalent:*

1. *$\mathcal{R}$ ist ein faktorieller Ring (es gilt also eindeutige Zerlegbarkeit in irreduzible Elemente, siehe Definition 5.2.1.4).*
2. *In $\mathcal{R}$ gilt Zerlegbarkeit in Primelemente. (Diese ist nach 5.2.1.2 notwendig eindeutig.)*
3. *In $\mathcal{R}$ gelten die folgenden beiden Bedingungen:*
   a) *Jedes irreduzible Element ist prim.*
   b) *Teilerkettenbedingung: Es gibt keine unendlich absteigenden Folgen echter Teiler.*

[3] Z für Zerlegung, P für Primfaktor, E für Eindeutigkeit

4. *Das multiplikative Monoid $\mathcal{M}$ ist frei in der Klasse der abelschen Monoide, d.h. eine direkte Summe von Kopien des Monoids* $(\mathbb{N}, +, 0)$.

Ein Vergleich der ersten mit der zweiten Bedingung zeigt, dass der Übergang von irreduziblen zu primen Elementen die Eindeutigkeit der behaupteten Faktorisierung erzwingt, ohne dass sie extra gefordert werden muss. Das spiegelt sich auch in der dritten Bedingung wider, wo a) im Wesentlichen für die Eindeutigkeit, b) für die Existenz der Darstellung verantwortlich ist. Die vierte Bedingung, so sehr sie auch völlig andere Begriffe bemüht, entpuppt sich als schlichte Übersetzung der ersten beiden Bedingungen, sobald man erkannt hat, dass die freien Erzeugenden des Monoids $\mathfrak{M}$ mit den irreduziblen/primen Elementen von $\mathfrak{R}$ (genauer: mit deren Assoziiertenklassen) korrespondieren. Der Beweis der behaupteten Äquivalenzen ist Gegenstand des nun Folgenden.

**Proposition 5.2.1.8.** *Erfüllt ein Integritätsbereich $\mathcal{R}$ Bedingung 1 aus Satz 5.2.1.7 (eindeutige Zerlegung in irreduzible Elemente), so ist in $\mathcal{R}$ jedes irreduzible Element auch Primelement. Folglich gilt Bedingung 2 aus Satz 5.2.1.7 (Zerlegung in Primelemente).*

*Beweis.* Sei $p$ irreduzibel und $p|ab$. Nach Definition der Teilbarkeit gibt es ein $c$ mit $ab = pc$. Laut Voraussetzung gibt es Zerlegungen $a = p_1 \cdot \ldots \cdot p_l$, $b = q_1 \cdot \ldots \cdot q_m$ und $c = r_1 \cdot \ldots \cdot r_n$ von $a$, $b$ und $c$ in irreduzible Elemente $p_i$ $(i = 1, \ldots, l)$, $q_j$ $(j = 1, \ldots, m)$, und $r_k$ $(k = 1, \ldots, n)$. Folglich gilt

$$p_1 \cdot \ldots \cdot p_l \cdot q_1 \cdot \ldots \cdot q_m = a \cdot b \sim p \cdot c = p \cdot r_1 \ldots \cdot r_n,$$

wobei ganz links alle Faktoren irreduzibel sind, ebenso ganz rechts. Wegen der vorausgesetzten Eindeutigkeit von Darstellungen als Produkte irreduzibler Elemente (Bedingung 1) muss der Faktor $p$ bis auf Assoziiertheit auch links vorkommen. Ist $p \sim p_i$ für ein $i$, so folgt $p|a$, ist $p \sim q_j$ für eine $j$ so folgt $p|b$, also ist $p$ prim.
Offensichtlich folgt aus dem soeben Gezeigten unmittelbar Bedingung 2 aus Satz 5.2.1.7. □

**Proposition 5.2.1.9.** *In einem Ring $\mathcal{R}$, der Bedingung 2 aus Satz 5.2.1.7 (Zerlegung in Primelemente) erfüllt, ist jedes irreduzible Element prim.*

*Beweis.* Sei $r \in R$ irreduzibel. Laut Voraussetzung gibt es Primelemente $p_i \in R$, $i = 1, \ldots, n$, mit $r = p_1 \cdot \ldots \cdot p_n$. Wäre $n > 1$, so läge damit eine Zerlegung von $r$ vor, die der Irreduzibilität widerspricht. Also ist $n = 1$ und $r = p_1$ prim. □

**Folgerung 5.2.1.10.** *Für einen Integritätsbereich $\mathcal{R}$ sind die Bedingungen 1 (eindeutige Zerlegung in irreduzible Elemente) und 2 (Zerlegung in Primelemente) aus Satz 5.2.1.7 äquivalent.*

*Beweis.* $1 \Rightarrow 2$: Siehe Proposition 5.2.1.8.
$2 \Rightarrow 1$: Wegen Proposition 5.1.4.7 und 5.2.1.9 sind in $\mathcal{R}$ die primen Elemente genau die irreduziblen. Laut Bedingung 2 hat jedes Element eine Zerlegung in prime und somit in irreduzible Elemente. Diese Zerlegung ist, nochmals wegen der Übereinstimmung von irreduziblen und primen Elementen in $\mathcal{R}$ sowie wegen Proposition 5.2.1.2, eindeutig bis auf Assoziiertheit. □

**Proposition 5.2.1.11.** *In jedem Integritätsbereich $\mathcal{R}$, der Bedingung 1 (eindeutige Zerlegung in irreduzible Elemente) oder 2 (Zerlegung in Primelemente) aus Satz 5.2.1.7 erfüllt, gilt die Teilerkettenbedingung. (Die Teilerkettenbedingung besagt explizit: Es gibt keine unendliche Folge $(a_n)_{n\in\mathbb{N}}$ von Elementen $a_n \in \mathcal{R}$, so dass für alle $n \in \mathbb{N}$ das Element $a_{n+1}$ ein echter Teiler von $a_n$ ist.)*

*Beweis.* Gegeben sei eine Folge $(a_n)_{n\in\mathbb{N}}$ von Elementen $a_n \in \mathcal{R}$, so dass für alle $n \in \mathbb{N}$ das Element $a_{n+1}$ ein Teiler von $a_n$ ist. Nach Voraussetzung gibt es zu jedem $a \in \mathcal{R}$ mit $a \neq 0$ eine eindeutig bestimmte Zahl $k = k(a)$, so dass sich $a$ als Produkt von $k$ Primelementen schreiben lässt. (Für Einheiten $a$ setzen wir $k(a) = 0$.) Wenn $a$ ein Teiler von $b$ ist, dann gilt $k(a) \leq k(b)$, wenn $a$ echter Teiler von $b$ ist, sogar $k(a) < k(b)$. Die absteigende Folge natürlicher Zahlen $k(a_0) \geq k(a_1) \geq \ldots \geq 0$ muss ab einem gewissen Index $n_0$ konstant sein. Also sind die Teilbarkeiten $a_{n+1}|a_n$ für alle $n \geq n_0$ keine echten mehr, was zu zeigen war. □

Wir sind nun in der Lage, zu beweisen, dass für einen Integritätsbereich die eindeutige Faktorisierbarkeit in irreduzible Elemente (Bedingung 1 in Satz 5.2.1.7) oder auch Faktorisierbarkeit in Primelemente (Bedingung 2 in Satz 5.2.1.7) äquivalent ist zu Teilerkettenbedingung und Übereinstimmung von primen und irreduziblen Elementen (Bedingung 3 in Satz 5.2.1.7).

**Proposition 5.2.1.12.** *Ein Integritätsbereich $\mathcal{R}$ erfüllt eine und somit beide der Bedingungen 1 (eindeutige Zerlegung in irreduzible Elemente) und 2 (Zerlegung in Primelemente) aus Satz 5.2.1.7 genau dann, wenn er die Bedingung 3 erfüllt, d.h. wenn gilt:*

(*a*) *Jedes irreduzible Element ist prim.*

(*b*) *Teilerkettenbedingung: Es gibt keine unendliche Folge $(a_n)_{n\in\mathbb{N}}$ von Elementen in $\mathcal{R}$, so dass für alle $n \in \mathbb{N}$ das Element $a_{n+1}$ ein echter Teiler von $a_n$ ist.*

*Beweis.* Nach Proposition 5.2.1.9 und Proposition 5.2.1.11 gelten in jedem Ring, der 1 oder 2 erfüllt, auch die Bedingungen (a) und (b). Umgekehrt folgt aus (b) nach Proposition 5.2.1.6 Zerlegbarkeit in irreduzible Elemente, also nach (a) Zerlegbarkeit in Primelemente.

□

Damit wissen wir, dass die ersten drei Bedingungen in Satz 5.2.1.7 äquivalent sind und können die letzte noch ausständige Behauptung beweisen:

**Proposition 5.2.1.13.** *Die Bedingung 4 aus Satz 5.2.1.7 ist äquivalent zu den Bedingungen 1 bis 3.*

*Beweis.* Zunächst erinnern wir uns an Beispiel 4.1.2.8 und Übungsaufgabe 4.1.2.10. Daraus geht hervor, dass die freien abelschen Monoide genau diejenigen sind, die isomorph zu einer direkten Summe $\bigoplus_{i\in I}(\mathbb{N}, +, 0)$ von Kopien des abelschen Monoids $(\mathbb{N}, +, 0)$ sind. Erfülle $\mathcal{R}$ die Bedingungen 1 bis 3 in Satz 5.2.1.7. Wir wählen eine Indexmenge $I$ für ein Vertretersystem für alle Assoziiertenklassen irreduzibler (= primer, siehe Bedingung 3)

Elemente $p_i$ in $\mathcal{R}$. Wir definieren eine Zuordnung $\varphi\colon \bigoplus_{i\in I}(\mathbb{N},+,0) \to \mathcal{M}$ (Notation wie in Satz 5.2.1.7) durch

$$\varphi : (e_i)_{i\in I} \mapsto \left[\prod_{i\in I} p_i^{e_i}\right]_\sim .$$

Man beachte, dass diese Abbildung wohldefiniert ist, weil nur endlich viele der natürlichen Zahlen $e_i$ von 0 verschieden sind. Man macht sich unmittelbar klar, dass $\varphi$ ein Homomorphismus, injektiv und surjektiv ist – die Injektivität folgt wegen der vorausgesetzten Eindeutigkeit der Zerlegung in irreduzible Elemente, die Surjektivität aus der ebenfalls vorausgesetzten Existenz einer solchen Zerlegung (durch Gruppieren der auftretenden irreduziblen Faktoren; die Exponenten $e_i$ entstehen durch Abzählen, wie oft der irreduzible Faktor $p_i$ vorkommt).
Gelte umgekehrt die Bedingung 4 aus Satz 5.2.1.7, d.h. für eine geeignete Indexmenge $I$ gelte $\mathcal{M} \cong S := \bigoplus_{i\in I}(\mathbb{N},+,0)$ vermittels eines Isomorphismus $\varphi\colon S \to \mathcal{M}$. Für jedes $i_0 \in I$ sei $b_{i_0} := (e_i)_{i\in I}$ das entsprechende kanonische Basiselement mit $e_{i_0} = 1$ und $e_i = 0$ für alle $i \neq i_0$. Dann sind die $\varphi(b_i)$, $i \in I$, bezüglich Teilbarkeit in $\mathcal{R}/_\sim$ obere Nachbarn von $1_R$, also Assoziiertenklassen irreduzibler Elemente. Weil $\varphi$ surjektiv ist, tritt jede Assoziiertenklasse $[a]_\sim$, $a \neq 0$, als $\varphi(s)$ mit einem $s = (e_i)_{i\in I} \in S$ auf. Folglich gilt die Zerlegung $a \sim \prod_{i\in I} \varphi(b_i)^{e_i}$ von $a$ in irreduzible Elemente. Man beachte dabei, dass wieder nur endlich viele $e_i$ von 0 verschieden sind, das Produkt also de facto ein endliches und somit wohldefiniert ist. Wegen der Injektivität von $\varphi$ ist diese Zerlegung bis auf Assoziiertheit aber auch eindeutig. Damit ist Bedingung 1 aus Satz 5.2.1.7 nachgewiesen. □

In den folgenden Übungsaufgaben wird gezeigt, dass keine der beiden Bedingungen

(a) irreduzibel = prim

(b) Teilerkettenbedingung

ausreicht, um zu zeigen, dass ein Ring faktoriell ist.

**UE 311 ► Übungsaufgabe 5.2.1.14.** Zeigen Sie, dass in $\mathbb{Z}[\sqrt{-5}]$ die Teilerkettenbedingung gilt. ◄ **UE 311**

**UE 312 ► Übungsaufgabe 5.2.1.15.** Sei $\mathbb{Q}_{2^\infty}$ die Menge aller Brüche der Form $n/2^k$, wobei $n$ und $k$ beliebige natürliche Zahlen sind. Sei $R$ der Ring aller „Polynome“ mit Koeffizienten in $\mathbb{C}$, wobei aber als Exponenten alle Elemente von $\mathbb{Q}_{2^\infty}$ erlaubt sind. ◄ **UE 312**
Formal ist $R$ die Menge aller Funktionen von $\mathbb{Q}_{2^\infty}$ nach $\mathbb{C}$, die aber fast überall den Wert 0 annehmen; die „Länge“ eines solchen Polynom $f$ ist die Kardinalität der Menge $\{q \in \mathbb{Q}_{2^\infty} \mid f(q) \neq 0\}$, also die Anzahl der vorkommenden „Monome“.
Addition wird punktweise definiert, Multiplikation ist Cauchymultiplikation. Monome sind Funktionen der Länge 1; das Monom, das nur an der Stelle $q$ den Wert $b$ annimmt, sonst überall den Wert 0, heißt $bx^q$; es gilt $(bx^q)\cdot(b'x^{q'}) = (bb')x^{q+q'}$.
Polynome der „Länge“ 2 nennen wir „Binome“.
Zeigen Sie, dass $R$ ein Integritätsbereich ist, und dass sogar Folgendes gilt:

(∗) Jeder endlich erzeugte Unterring ist isomorph zu einem Unterring des Polynomrings $\mathbb{C}[x]$.

(Hinweis: gemeinsamen Nenner suchen.)

**UE 313** ▶ **Übungsaufgabe 5.2.1.16.** Sei $R$ der Ring aus der vorigen UE-Aufgabe. Zeigen Sie, dass die Einheiten von $R$ genau die „konstanten“ Polynome $bx^0$ sind. ◀ **UE 313**

**UE 314** ▶ **Übungsaufgabe 5.2.1.17.** Sei $R$ wie in den vorigen Aufgaben. Finden sie in $R$ eine unendliche Teilerkette. ◀ **UE 314**

**UE 315** ▶ **Übungsaufgabe 5.2.1.18.** Sei $R$ wie in den vorigen Aufgaben. Zeigen Sie, dass es in $R$ keine irreduziblen Elemente gibt, und schließen Sie, dass in $R$ die Äquivalenz „irreduzibel $\Leftrightarrow$ prim“ gilt. ◀ **UE 315**
Hinweis: Verwenden Sie die algebraische Abgeschlossenheit von $\mathbb{C}$ sowie die obige Eigenschaft (∗). Als Aufwärmübung empfehlen wir, die Reduzibilität von $x + 1$ zu zeigen. (Es gibt sogar Faktoren mit reellen Koeffizienten.)

**Beispiele 5.2.1.19.** Die Ringe $\mathbb{Z}$ und $K[x]$ ($K$ Körper) sind faktoriell. Für $K[x]$ wird das erst aus Proposition 5.2.3.3 sowie den Sätzen 5.2.3.4 und 5.2.2.2 folgen.

Etwas später (in 5.3.2) werden wir den wichtigen Satz beweisen, dass der Polynomring nicht nur über einem Körper, sondern über einem beliebigen faktoriellen Ring wieder faktoriell ist. Mittels Induktion folgt daraus, dass dies auch für Polynomringe in mehreren und, wie einfache Überlegungen zeigen, sogar in beliebig vielen Variablen gilt.
Ein weiterer Aspekt der Struktur des Teilerverbandes ergibt sich durch folgenden Satz, im Wesentlichen eine Verallgemeinerung von Satz 3.1.3.4.

**Satz 5.2.1.20.** *1. Jede Totalordnung/Kette ist eine verbandsgeordnete Menge, die sogar einen distributiven Verband bildet.*

*2. Bezeichne $K := (\mathbb{N}_\infty, \leq)$ die totalgeordnete Menge der natürlichen Zahlen ergänzt um ein größtes Element $\infty$. Diese Kette ist als Verband sogar vollständig, d.h. jede Teilmenge besitzt Supremum und Infimum.*

*3. Sei $R$ ein faktorieller Ring und $P$ die Menge aller Assoziiertenklassen von primen Elementen in $R$. Wir definieren nun eine Zuordnung $\varphi : [a]_\sim \mapsto (n_p)_{p\in P} = (n_p(a))_{p\in P}$, die zunächst für alle $a \in R \setminus \{0\}$ definiert ist. Ist $a \sim p_1^{e_1} \dots p_n^{e_n}$ mit paarweise nicht assoziierten Primelementen $p_i$, so sei $n_p = e_i$ für $p \sim p_i$ für ein $i = 1, 2, \dots, n$, andernfalls $n_p = 0$. Für $a = 0$ schließlich sei $\varphi(a) = \varphi(0) = (\infty)_{p\in P}$. Auf diese Weise wird ein Verbandsmonomorphismus (Einbettung) $\varphi\colon R/_\sim \to K^P$ des Teilerverbandes in das direkte Produkt $|P|$ vieler Kopien der Kette aus Teil 2. definiert.*

4. *Der Teilerverband in einem faktoriellen Ring modulo Assoziiertheit ist distributiv.*

5. *Der Teilerverband in einem faktoriellen Ring modulo Assoziiertheit ist vollständig.*

**UE 316 ► Übungsaufgabe 5.2.1.21.** (V) Beweisen Sie Satz 5.2.1.20. **◄ UE 316**

## 5.2.2 Hauptidealringe

Inhalt in Kurzfassung: Hauptidealringe erweisen sich als faktoriell. Der Beweis erfolgt mit Hilfe des Kriteriums mit der Teilerkettenbedingung. Als Folgerung klärt sich die ordnungstheoretische Struktur des Kongruenz-, d.h. des Idealverbandes eines Hauptidealrings mit Hilfe der bereits aus 5.2.1 bekannten Ergebnisse über den Teilerverband eines faktoriellen Ringes auf sehr befriedigende Weise. Als Folgerung erhält man den wichtigen, im Falle des Ringes $\mathbb{Z}$ bereits bekannten Satz, dass sich der größte gemeinsame Teiler von Elementen in einem Hauptidealring als Linearkombination dieser Elemente schreiben lässt.

Zur Erinnerung:

**Definition 5.2.2.1.** Ein Integritätsbereich $R$ heißt *Hauptidealring*[4], wenn jedes Ideal $I \lhd R$ ein Hauptideal ist.

Der wichtigste Inhalt dieses Unterabschnitts ist der folgende Satz.

**Satz 5.2.2.2.** *Jeder Hauptidealring ist ein faktorieller Ring.*

*Beweis.* Laut der dritten Bedingung in Satz 5.2.1.7 genügt es, für einen Hauptidealring $\mathcal{R} = (R, +, 0_R, -\cdot, 1_R)$ folgende zwei Aussagen zu beweisen:

1. Jedes irreduzible Element $p \in R$ ist ein Primelement.

2. In $\mathcal{R}$ gibt es keine unendlichen echt absteigenden Teilerketten, d.h.: Sei eine unendliche Folge $(a_n)_{n\in\mathbb{N}}$ von Elementen $a_n \in R$ gegeben, sodass für alle $n$ das Element $a_{n+1}$ ein Teiler von $a_n$ ist. Dann gibt es ein $n \in \mathbb{N}$ mit $a_n \sim a_{n+1} \sim a_{n+2} \sim \ldots$.

Zum Beweis dieser beiden Aussagen:

1. Sei $p \in R$ irreduzibel. Das bedeutet, dass $p$ in der Teilerhalbordnung ein oberer Nachbar von $1_R$ ist. Für die erzeugten Hauptideale bedeutet das nach Proposition 5.1.4.1: $(p)$ ist ein unterer Nachbar von $(1) = R$ in der Ordnung der Hauptideale. Weil $\mathcal{R}$ ein Hauptidealring ist, sind das bereits alle Ideale, also ist $(p)$ ein maximales Ideal, also erst recht Primideal (vierte Aussage in Satz 3.4.2.4). Nach Definition (siehe 5.1.4.2) ist daher $p$ ein Primelement.

[4] englisch: *principal ideal domain*

2. Die von den $a_n$ erzeugten Hauptideale bilden (siehe Proposition 5.1.4.1) eine aufsteigende Kette
$$(a_0) \subseteq (a_1) \subseteq \ldots \subseteq (a_n) \subseteq (a_{n+1}) \subseteq \ldots.$$
Für $J := \bigcup_{n=0}^{\infty}(a_n)$ gilt dann $J \lhd I$, denn: $0 \in J$; für $a, b \in J$ gibt es $n, m \in \mathbb{N}$ mit $a \in (a_n)$ und $b \in (a_m)$. Sei o. B. d. A. $n \geq m$, also $a, b \in (a_n)$. Weil $(a_n)$ ein Ideal ist, folgt $a + b, -a \in (a_n) \subseteq J$ und, für beliebiges $r \in R$, auch $ra \in (a_n) \subseteq J$. Also ist wirklich $J \lhd R$. Weil $R$ ein Hauptidealring ist, gibt es ein $d \in R$ mit $J = (d)$. Wegen $d \in J$ ist $d \in (a_n)$ für ein $n \in \mathbb{N}$ und damit sowohl $(d) \subseteq (a_n)$ als auch $(a_n) \subseteq J = (d)$. Daraus folgt aber auch $(a_n) = (a_{n+1}) = \ldots = (d)$ und somit, wieder wegen Proposition 5.1.4.1, $a_n \sim a_{n+1} \sim a_{n+2} \sim \ldots$, was zu zeigen war. □

Im Beweis von Satz 5.2.2.2 kommt ein sehr ähnliches Argument wie im Beweis von Satz 2.3.1.24 vor, den man tatsächlich zu einer (geringfügigen) Verkürzung des Beweises in 5.2.2.2 verwenden könnte.

**UE 317** ► **Übungsaufgabe 5.2.2.3.** (A) Wie könnte man im Beweis von Satz 5.2.2.2 unter Zuhilfenahme von Satz 2.3.1.24 etwas direkter argumentieren? ◄ **UE 317**

Die Umkehrung von Satz 5.2.2.2 gilt nicht. Das folgt aus:

**Proposition 5.2.2.4.** *Sei $R$ ein Integritätsbereich. Wenn der Polynomring $R[x]$ ein Hauptidealring ist, dann ist $R$ ein Körper.*

**UE 318** ► **Übungsaufgabe 5.2.2.5.** (W) Beweisen Sie Proposition 5.2.2.4. Hinweis: Betrachten Sie das von $a$ und $x$ erzeugte Ideal, wobei $a \neq 0$ eine Nichteinheit von $R$ ist. ◄ **UE 318**

Beispielsweise ist, weil $\mathbb{Q}[x]$ kein Körper ist, $\mathbb{Q}[x, y] \cong \mathbb{Q}[x][y]$ kein Hauptidealring, wegen des späteren Satzes 5.3.2.1 aber faktoriell. Sehr wohl Hauptidealringe sind hingegen $\mathbb{Z}$ (folgt wegen der Diskussion vor Proposition 3.4.1.14 oder auch mithilfe des nächsten Abschnitts wegen Satz 5.2.3.4 kombiniert mit Proposition 5.2.3.3), jeder Körper $K$ ($\{0\} = (0)$ und $K = (1)$ sind die einzigen Ideale, da $K$ einfach ist) sowie $K[x]$ für einen Körper $K$ (siehe erneut Proposition 5.2.3.3 und Satz 5.2.3.4).

Proposition 5.1.4.1 hat bereits im Beweis von Satz 5.2.2.2 eine wesentliche Rolle gespielt. Aus ihr lesen wir ab, dass die Teilerhalbordnung eines Integritätsbereichs isomorph ist zur Halbordnung der Hauptideale bezüglich $\supseteq$. Weil das in einem Hauptidealring bereits alle Ideale sind, bedeutet das:

**Proposition 5.2.2.6.** *Ist $\mathcal{R}$ ein Hauptidealring, so ist die Teilerhalbordnung $(\mathcal{R}/_\sim, |)$ isomorph zu $(\mathrm{Con}(\mathcal{R}), \supseteq)$. Also gilt auch für die Verbände im algebraischen Sinn:*
$$(\mathcal{R}/_\sim, \mathrm{ggT}, \mathrm{kgV}) \cong (\mathrm{Con}(\mathcal{R}), \vee, \wedge).$$

Der Kongruenzverband ist vollständig. Also gibt es zu beliebigen Teilmengen des Ringes sowohl ggT als auch kgV, wobei diese dem Erzeugnis $\bigvee$ bzw. dem Schnitt $\bigcap$ der entsprechenden Hauptideale entsprechen. Das von einer beliebigen Menge $A$ in $\mathcal{R}$ erzeugte Ideal $\bigvee A$ wird in Proposition 3.4.1.6 als Menge aller Linearkombinationen von Elementen aus $A$ beschrieben. Im Falle von Hauptidealen genügt es, Linearkombinationen der Erzeugenden der Hauptideale zu betrachten. Somit gilt für Hauptidealringe die folgende Verschärfung der Existenz beliebiger ggT in faktoriellen Ringen:

**Satz 5.2.2.7.** *Sei $\mathcal{R} = (R, +, 0_R, -, \cdot, 1_R)$ ein Hauptidealring und $A \subseteq R$. Dann lässt sich jeder größte gemeinsame Teiler $d$ von $A$ als Linearkombination von Elementen aus $A$ schreiben, d.h. es gibt ein $n \in \mathbb{N}$, $x_1, \ldots, x_n \in R$ und $a_1, \ldots, a_n \in A$ mit*

$$d = x_1 a_1 + \cdots + x_n a_n.$$

### 5.2.3 Euklidische Ringe

Inhalt in Kurzfassung: Euklidische Ringe sind solche Integritätsbereiche, in denen eine Art Division mit Rest möglich ist. Sehr schnell sieht man, dass es sich dabei um Hauptideal- und somit um faktorielle Ringe handelt. Iterierte Division mit Rest führt zum Euklidischen Algorithmus zur algorithmischen Berechnung des größten gemeinsamen Teilers zweier Ringelemente und darüber hinaus zur Darstellung desselben als Linearkombination. (Später wird das auch eine effektive Berechnung multiplikativer Inverser in endlichen Körpern mit $p$ Elementen, $p$ Primzahl, ermöglichen.) Wichtige Beispiele euklidischer Ringe sind $\mathbb{Z}$, $K[x]$ und $K[[x]]$ ($K$ Körper) und $\mathbb{Z}[i]$, der Ring der ganzen Gaußschen Zahlen.

**Definition 5.2.3.1.** Ein Integritätsbereich $R$ heißt ein *euklidischer Ring*, wenn es eine Abbildung $H : R \setminus \{0\} \to \mathbb{N}$ („euklidische Bewertung“) mit folgender Eigenschaft gibt: Für alle $a \in R \setminus \{0\}$, $b \in R$ gibt es $q, r \in R$, sodass $b = aq + r$ mit $r = 0$ oder $H(r) < H(a)$ („Division mit Rest“).

Manchmal ist es praktisch, auch $H(0)$ zu definieren, etwa $H(0) := 0$, sofern es sonst keine Elemente $r \in R$ mit $H(r) = 0$ gibt, gelegentlich auch $H(0) := -\infty$. Überdies wird in der Literatur von einer euklidischen Bewertung oft auch die Ungleichung $H(ab) \geq H(a)$ für alle $b \neq 0$ gefordert. Diese Modifikation des Begriffs der euklidischen Bewertung ändert aber nichts am Begriff des euklidischen Ringes:

**UE 319** ► **Übungsaufgabe 5.2.3.2.** (E) Sei $R$ ein euklidischer Ring mit der euklidischen Bewertung $H : R \setminus \{0\} \to \mathbb{N}$. Zeigen Sie, dass es dann eine euklidische Bewertung $H' : R \setminus \{0\} \to \mathbb{N}$ gibt, die zusätzlich $H'(ab) \geq H'(a)$ für alle $b \neq 0$ erfüllt. ◄ **UE 319**

Körper sind auf triviale Weise euklidische Ringe ($H$ konstant, $q = a^{-1}b$ und $r = 0$ setzen). Die typischen Beispiele euklidischer Ringe sind $\mathbb{Z}$ (mit $H(a) := |a|$) und, wegen der Polynomdivision 3.4.6.7, Polynomringe $K[x]$ über einem Körper $K$ (mit $H(f) := \operatorname{grad}(f)$). Also:

**Proposition 5.2.3.3.** *Der Ring $\mathbb{Z}$ der ganzen Zahlen ist ein euklidischer Ring, außerdem der Polynomring $K[x]$ in einer Variablen über einem beliebigen Körper $K$.*

**Satz 5.2.3.4.** *Jeder euklidische Ring $R$ ist ein Hauptidealring und somit (nach Satz 5.2.2.2) auch ein faktorieller Ring.*

*Beweis.* Sei $I \lhd R$, $I \neq (0) = \{0\}$. Zu zeigen: $\exists a \in R : I = (a) = \{aq \mid q \in R\}$. Sei $a \in I \setminus \{0\}$ so gewählt, dass $H(a) = \min\{H(x) \mid x \in I \setminus \{0\}\}$. Wir behaupten, dass dann $I = (a)$ gilt. Trivialerweise gilt $(a) \subseteq I$. Sei umgekehrt $b \in I$. Wegen $a \neq 0$ gibt es $q, r \in R$ mit $b = aq + r$ und $r = 0 \vee H(r) < H(a)$. Es ist $r = b - aq \in I$ (wegen $I \lhd R$), woraus (wegen der Minimalität von $H(a)$) $r = 0$ und damit $b = aq \in (a)$ folgt. Somit gilt auch $I \subseteq (a)$, also $I = (a)$. □

Die Umkehrung dieses Satzes gilt nicht, wie beispielsweise der quadratische Zahlring $\mathbb{Z}[\alpha]$ mit $\alpha = \frac{1+\sqrt{-19}}{2}$ zeigt. Der Nachweis ist keineswegs trivial. In 10.2.4 findet sich eine Anleitung.
Kombinieren wir Proposition 5.2.3.3 mit Satz 5.2.3.4 und Proposition 5.2.2.4, so erhalten wir:

**Proposition 5.2.3.5.** *Sei $R$ ein Integritätsbereich. Der Polynomring $R[x]$ ist genau dann ein Hauptidealring, wenn $R$ ein Körper ist.*

In euklidischen Ringen kann man mit dem sogenannten *euklidischen Algorithmus* den ggT und seine Darstellung als Linearkombination berechnen.

Sei $I$ ein Euklidischer Ring und $a, b \in I$. Für $a = b = 0$ ist $\mathrm{ggT}(a, b) = 0$. Sei o. B. d. A. $a \neq 0$.

$$
\begin{aligned}
&\Rightarrow \exists q_1, r_1 \in I : b = aq_1 + r_1,\ r_1 = 0 \vee H(r_1) < H(a),\\
\text{falls } r_1 \neq 0 &\Rightarrow \exists q_2, r_2 \in I : a = r_1 q_2 + r_2,\ r_2 = 0 \vee H(r_2) < H(r_1),\\
\text{falls } r_2 \neq 0 &\Rightarrow \exists q_3, r_3 \in I : r_1 = r_2 q_3 + r_3,\ r_3 = 0 \vee H(r_3) < H(r_2),\\
&\ \ \vdots\\
&\text{allgemein:}\\
\text{falls } r_i \neq 0 &\Rightarrow \exists q_{i+1}, r_{i+1} \in I : r_{i-1} = r_i q_{i+1} + r_{i+1},\ r_{i+1} = 0 \vee H(r_{i+1}) < H(r_i).\\
&\quad \text{(Dabei ist } a = r_0 \text{ und } b = r_{-1} \text{ zu setzen.)}
\end{aligned}
$$

Nach endlich vielen Schritten (wegen $H(a) = H(r_0) > H(r_1) > H(r_2) > \ldots$) erhält man ein $k$ mit $r_k = 0$ und $r_{k-1} \neq 0$. Wir zeigen nun: $r_{k-1} = \mathrm{ggT}(a, b)$. Wir haben:

$$
\begin{aligned}
r_{k-2} = r_{k-1} q_k + 0 &\Rightarrow r_{k-1} | r_{k-2},\\
r_{k-3} = r_{k-2} q_{k-1} + r_{k-1} &\Rightarrow r_{k-1} | r_{k-3},\\
r_{k-4} = r_{k-3} q_{k-2} + r_{k-2} &\Rightarrow r_{k-1} | r_{k-4},\\
&\ \ \vdots\\
r_1 = r_2 q_3 + r_3 &\Rightarrow r_{k-1} | r_1,\\
a = r_1 q_2 + r_2 &\Rightarrow r_{k-1} | a,\\
b = a q_1 + r_1 &\Rightarrow r_{k-1} | b,
\end{aligned}
$$

also gilt $r_{k-1}|a \wedge r_{k-1}|b$. Somit ist $r_{k-1}$ ein gemeinsamer Teiler von $a$ und $b$. Um zu zeigen, dass es sich sogar um einen *größten* gemeinsamen Teiler handelt, geben wir uns irgendeinen weiteren gemeinsamen Teiler $t$, also $t|a$ und $t|b$ vor. Dann folgt ähnlich $t|r_1$, $t|r_2$, $t|r_3$, $\ldots$, $t|r_{k-1}$. Folglich ist $r_{k-1}$ tatsächlich ein ggT von $a$ und $b$.

Wir haben für Hauptidealringe gezeigt: $\mathrm{ggT}(a,b) = ax + by$ mit $x, y \in I$. In euklidischen Ringen kann man die Koeffizienten $x, y$ sogar explizit berechnen. Und zwar liest man zunächst aus der vorletzten Gleichung $r_{k-3} = r_{k-2}q_{k-1} + r_{k-1}$ die Darstellung $r_{k-1} = r_{k-3} + r_{k-2}(-q_{k-1})$ von $r_{k-1}$ als Linearkombination der vorangegangenen Reste $r_{k-2}$ und $r_{k-3}$ ab. Sodann verwendet man die vorangegangenen Gleichungen, um für $r_{k-2}$ eine Linearkombination von $r_{k-3}$ und $r_{k-4}$ einzusetzen, die auch eine für $r_{k-1}$ liefert. Schritt für Schritt die anderen Gleichungen verwendend landet man schließlich bei einer Linearkombination von $a$ und $b$:

$$\begin{aligned}\mathrm{ggT}(a,b) = r_{k-1} &= r_{k-3} + r_{k-2}(-q_{k-1}) = r_{k-3} + (r_{k-4} - r_{k-3}q_{k-2})(-q_{k-1}) = \\ &= r_{k-4}(-q_{k-1}) + r_{k-3}(1 + q_{k-2}q_{k-1}) = \ldots = ax + by.\end{aligned}$$

Wir fassen die Unterschiede zwischen den Begriffen von Abschnitt 5.2 zusammen:

1. In jedem faktoriellen Ring $R$ gibt es zu beliebigen Elementen $a$, $b$ immer einen größten gemeinsamen Teiler.
2. Wenn $R$ ein Hauptidealring ist, weiß man überdies, dass sich der größte gemeinsame Teiler von $a$ und $b$ als $R$-Linearkombination von $a$ und $b$ schreiben lässt.
3. Wenn schließlich $R$ ein euklidischer Ring ist, dann haben wir sogar einen Algorithmus, der den ggT sowie diese Linearkombination findet. (Für den Fall $R = \mathbb{Z}$ ist dieser Algorithmus weit schneller als das Finden der Primfaktorzerlegung.)

Die Darstellung des ggT als Linearkombination kann man zu einer weiteren Beweisvariante für die eindeutige Primfaktorzerlegung in $\mathbb{Z}$ ausnutzen. Das wird in der folgenden Übungsaufgabe getan.

**UE 320** ► **Übungsaufgabe 5.2.3.6.** (A) Zeigen Sie direkt mit Hilfe des euklidischen Algorithmus, dass in einem euklidischen Ring jedes irreduzible Element $p$ prim ist. Anleitung: Angenommen $p|ab$ und $p$ sei kein Teiler von $a$. Weil $p$ irreduzibel ist, folgt $\mathrm{ggT}(a,p) = 1$. Stellen Sie 1 als Linearkombination $a$ und $p$ dar, multiplizieren Sie die Gleichung mit $b$ etc. Beweisen Sie damit neuerlich, ohne Umweg über Hauptidealringe, den Satz von der eindeutigen Primfaktorzerlegung in $\mathbb{Z}$. ◄ **UE 320**

Außerdem lässt sich der euklidische Algorithmus durch Iteration auf mehr als zwei Elemente im Ring ausdehnen.

**UE 321** ▶ **Übungsaufgabe 5.2.3.7.** (F+) Zeigen Sie, dass sich in euklidischen Ringen der ggT nicht nur von zwei Elementen als deren Linearkombination schreiben lässt, sondern für eine beliebige endliche Anzahl. Beschreiben Sie, wie man diese Darstellung algorithmisch erhalten kann. Wie verhält es sich mit dem ggT unendlich vieler Elemente? ◀ **UE 321**

**UE 322** ▶ **Übungsaufgabe 5.2.3.8.** (F) ◀ **UE 322**

(1) Man bestimme in $\mathbb{Z}$ den ggT von 6188 und 4709 und stelle ihn als ganzzahlige Linearkombination von 6188 und 4709 dar.

(2) Analog für 525 und 231.

**UE 323** ▶ **Übungsaufgabe 5.2.3.9.** (F) ◀ **UE 323**

(1) Man bestimme in $\mathbb{Q}[x]$ alle ggT von $4x^4 - 2x^3 - 16x^2 + 5x + 9$ und $2x^3 - 5x + 4$ und stelle den normierten ggT als Linearkombination der beiden Polynome dar.

(2) Analog für $2x^6 + 3x^5 - 4x^4 - 5x^3 - 2x - 2$ und $x^5 - 2x^3 - 1$.

Ein weiteres reizvolles Beispiel eines euklidischen Ringes ist das folgende:

**Proposition 5.2.3.10.** *Der von $\mathbb{Z}$ und der imaginären Einheit $i$ erzeugte Ring $\mathbb{Z}[i] = \{a + ib : \ a, b \in \mathbb{Z}\}$ (genannt der* Ring der ganzen Gauß'schen Zahlen*) ist euklidisch vermittels der euklidischen Bewertung $H(z) := |z|^2$, folglich also auch ein Hauptidealring und faktoriell.*

**UE 324** ▶ **Übungsaufgabe 5.2.3.11.** (B) Beweisen Sie Proposition 5.2.3.10. ◀ **UE 324**

Man kann zeigen, dass (bis auf multiplikative Faktoren, die Einheiten sind) sämtliche Primelemente in $\mathbb{Z}[i]$ gegeben sind durch die Primzahlen der Form $4k+3$ mit $k \in \mathbb{N}$ und durch jene $a + bi$ mit $a, b \in \mathbb{Z}$, für die $a^2 + b^2$ eine Primzahl ist. Zur Übung begnügen wir uns mit ein paar leichteren Aufgaben zu $\mathbb{Z}[i]$:

**UE 325** ▶ **Übungsaufgabe 5.2.3.12.** (B) Begründen Sie folgende Aussagen über den (nach Proposition 5.2.3.10) euklidischen Ring $\mathbb{Z}[i]$. ◀ **UE 325**

(1) Für die Einheitengruppe von $\mathbb{Z}[i]$ gilt $E(\mathbb{Z}[i]) = \{1, -1, i, -i\}$.

(2) Ist $p$ prim in $\mathbb{Z}[i]$ und eine natürliche Zahl, so auch eine Primzahl.

(3) Die Umkehrung gilt nicht: Es gibt Primzahlen, die nicht prim in $\mathbb{Z}[i]$ sind.

(4) Lässt sich $p = a^2 + b^2 = (a + ib)(a - ib) \in \mathbb{P}$ als Summe zweier Quadrate positiver ganzer Zahlen $a, b$ darstellen, so sind die Faktoren $a + ib$ und $a - ib$ prim in $\mathbb{Z}[i]$.

(5) Man bestimme alle primen Elemente $z \in \mathbb{Z}[i]$ mit $|z|^2 \leq 10$.

(6) Man bestimme in $\mathbb{Z}[i]$ die Primfaktorzerlegungen von $27 + 6i$ und $-3 + 4i$.

(7) Man bestimme in $\mathbb{Z}[i]$ einen ggT der Elemente $a = 7 + i$ und $b = 5$ und stelle ihn in der Form $ax + by$ mit $x, y \in \mathbb{Z}[i]$ dar.

**UE 326** ▶ **Übungsaufgabe 5.2.3.13.** (W) Zeigen Sie, dass der Ring $K[[x]]$ der formalen Potenzreihen über einem Körper $K$ euklidisch, folglich auch ein Hauptidealring und faktoriell ist. Bestimmen Sie alle irreduziblen Elemente modulo Assoziiertheit und geben Sie sämtliche Ideale durch Erzeugende an, jedes genau einmal. ◀ **UE 326**

## 5.3 Anwendungen und Ergänzungen

Der folgende Abschnitt bringt einige wichtige Themen, die, wenn auch in teilweise unterschiedliche Richtungen, an die bisherigen Untersuchungen zur Teilbarkeit anschließen. Zunächst gilt es in 5.3.1 einige nützliche Beobachtungen über Quotientenkörper anzustellen, wenn der zugrunde liegende Integritätsbereich sogar ein faktorieller Ring ist. Sodann beweisen wir in 5.3.2 den wichtigen Satz, dass der Polynomring über einem faktoriellen Ring selbst wieder faktoriell ist. Das reichert die Klasse verfügbarer Beispiele faktorieller Ringe wesentlich an. Klassisch sind die Inhalte von 5.3.3 über die Faktorisierung komplexer und reeller Polynome sowie der Satz von Vieta über die Beziehung zwischen den Nullstellen und den Koeffizienten eines Polynoms vermittels der elementarsymmetrischen Polynome (5.3.4). Auch der Partialbruchzerlegung (5.3.5) gebrochen rationaler Funktionen liegen Teilbarkeitsüberlegungen zugrunde. Den Abschluss von Abschnitt und Kapitel bildet Polynominterpolation nach Lagrange bzw. Newton (5.3.6), also ein ebenfalls klassisches Thema.

### 5.3.1 Der Quotientenkörper eines faktoriellen Rings

Inhalt in Kurzfassung: Ist ein Integritätsbereich sogar ein faktorieller oder gar Euklidischer Ring, so wird das Rechnen im Quotientenkörper besonders übersichtlich, weil dort jedes Element als Bruch gekürzte Darstellungen hat, unter denen durch eine sogenannte Normierungsfunktion sogar eine Normalform ausgezeichnet werden kann. Das wichtigste Beispiel (neben dem Ring $\mathbb{Z}$ und seinem Quotientenkörper $\mathbb{Q}$) ist der Polynomring über einem Körper mit dem Körper der gebrochen rationalen Funktionen als Quotientenring.

Wir erinnern an die Konstruktion des Quotientenkörpers $\mathcal{K}$ eines Integritätsbereichs $\mathcal{R} = (R, +, 0_R, -, \cdot, 1_R)$ aus 3.4.5. Auf der Menge $R \times (R \setminus \{0_R\})$, erweist sich die durch $(r_1, s_1) \equiv (r_2, s_2)$ für $r_1 s_2 = s_1 r_2$ definierte Relation als Kongruenzrelation[5] bezüglich der Operationen

$$(r_1, s_1) + (r_2, s_2) := (r_1 s_2 + r_2 s_1, s_1 s_2),$$
$$-(r, s) := (-r, s),$$

und

$$(r_1, s_1) \cdot (r_2, s_2) := (r_1 r_2, s_1 s_2).$$

[5] Die ungewöhnliche Bezeichnung $\equiv$ dient der Unterscheidung von der Assoziiertheitsrelation $\sim$ auf $\mathcal{R}$.

Die Faktoralgebra $\mathcal{K} := (K, +, 0_K, -, \cdot, 1_K)$ mit $K := (R \times R^\times)/_\equiv$, den auf $\mathcal{K}$ induzierten Operationen $+, -$ und $\cdot$ sowie $0_K := [(0_R, 1_R)]_\equiv$ und $1_K := [(1_R, 1_R)]_\equiv$ erweist sich als Körper. Die multiplikativen Inversen sind $[(r,s)]_\equiv^{-1} = [(s,r)]_\equiv$. Die Abbildung $\iota\colon \mathcal{R} \to \mathcal{K}$, $r \mapsto [(r, 1_R)]_\equiv$ ist eine isomorphe Einbettung von $\mathcal{R}$ in $\mathcal{K}$, und $\mathcal{K}$ wird als Körper von $\iota(R)$ erzeugt. Für jeden anderen Körper $\mathcal{K}'$, in den $\mathcal{R}$ durch ein $\iota'\colon \mathcal{R} \to \mathcal{K}'$ isomorph eingebettet werden kann, gibt es eine eindeutige isomorphe Einbettung $\varphi\colon \mathcal{K} \to \mathcal{K}'$ mit $\iota' = \varphi \circ \iota$. Ein Element $[(r,s)]_\equiv$ des Quotientenkörpers $\mathcal{K}$ wird üblicherweise als *Bruch* $\frac{r}{s}$ notiert, wobei $r$ der *Zähler* und $s$ der *Nenner* des Bruches heißt. Wir nennen das die *kanonische Darstellung* des Quotientenkörpers eines Integritätsbereichs.
Die Äquivalenzrelation $\equiv$ ist nicht trivial. Deshalb können verschiedene Brüche $\frac{r_1}{s_1}$ und $\frac{r_2}{s_2}$ dasselbe Element in $\mathcal{K}$ darstellen. Wünschenswert wären kanonische Vertreter. In einem ersten Schritt zeigen wir, dass es (so wie in den rationalen Zahlen) stets gekürzte Darstellungen gibt.

**Proposition 5.3.1.1.** *Sei $\mathcal{R}$ ein faktorieller Ring, $\mathcal{K}$ der Quotientenkörper von $\mathcal{R}$ in kanonischer Darstellung wie oben, und $[(r,s)]_\equiv \in K$. Dann gibt es ein $(r', s') \in R \times R^\times$ mit $(r', s') \equiv (r, s)$ und $\mathrm{ggT}(r', s') = 1$. Der Bruch $\frac{r'}{s'}$ heißt eine* gekürzte Darstellung *von $\frac{r}{s}$ und ergibt sich durch Kürzen von $\mathrm{ggT}(r,s)$ in $\frac{r}{s}$. Jede weitere gekürzte Darstellung $\frac{r''}{s''}$ von $\frac{r}{s}$ ist dazu assoziiert, d.h. es gilt $r'' \sim r'$ und $s' \sim s''$.*

*Beweis.* Man geht von Primfaktorzerlegungen von $r = p_1 \cdot \ldots \cdot p_m$ und $s = q_1 \ldots q_n$ aus. Gibt es assoziierte Faktoren $p_i \sim q_j$, so unterscheiden sich diese nur um eine multiplikative Einheit $e$, d.h. $p_i = eq_j$, und man kann kürzen. Führt man sämtliche möglichen Kürzungen durch (insgesamt kürzt man also $\mathrm{ggT}(r,s)$), so verbleiben Zähler und Nenner, die teilerfremd sind, aber, wie man aus der Definition von $\equiv$ nachprüft, immer noch dasselbe Element von $\mathcal{K}$ darstellen.
Auch dass zwei gekürzte Darstellungen assoziiert sind, erhält man sehr leicht unter Verwendung der Primfaktorzerlegung in $\mathcal{R}$ und der Definition von $\equiv$ (Übung). □

**UE 327** ► **Übungsaufgabe 5.3.1.2.** (V) Beweisen Sie die Assoziiertheitsaussage in Proposition 5.3.1.1. ◄ **UE 327**

Wir können die Eindeutigkeitsaussage modulo Assoziiertheit aus Proposition 5.3.1.1 zu einer Eindeutigkeitsaussage schlechthin verschärfen, nämlich mithilfe einer Auswahlfunktion aus den Assoziiertenklassen, einer sogenannten Normierungsfunktion. Aus technischen Gründen definieren wir diese Funktion wie folgt:

**Definition 5.3.1.3.** Sei $R$ ein faktorieller Ring. Unter einer *Normierungsfunktion* verstehen wir eine Abbildung $\nu : R \to R$, die zu jedem $r \in R$ ein assoziiertes $\nu(r) \sim r$ auswählt derart, dass stets $\nu(rs) = \nu(r)\nu(s)$ und für $r \sim s$ auch $\nu(r) = \nu(s)$ gilt.

Aus der Definition folgt insbesondere $\nu(\nu(r)) = \nu(r)$. Wegen $\nu(1_R) = \nu(1_R \cdot 1_R) = \nu(1_R)\nu(1_R)$ gilt außerdem $\nu(1_R) = 1_R$. Die Elemente $\nu(r)$, $r \in R$, nennen wir dann *normiert*. Im Quotientenkörper $K$ (in kanonischer Darstellung) eines faktoriellen Ringes $R$

mit Normierungsfunktion $\nu$ ist es möglich, unter allen gekürzten Brüchen $\frac{r}{s} = [(r,s)]_\equiv \in K$ jenen auszuwählen, dessen Nenner $s = \nu(s)$ normiert ist. Diesen Bruch nennen wir die *normierte Darstellung* von $\frac{r}{s} = [(r,s)]_\equiv \in K$:

**UE 328** ► **Übungsaufgabe 5.3.1.4.** (V) Zeigen Sie: Sei $\mathbb{R}$ ein faktorieller Ring mit einer Normierungsfunktion $\nu$ und sei $K$ der Quotientenkörper von $R$ in kanonischer Darstellung. Dann hat jedes Element aus $K$ genau eine normierte Darstellung $\frac{r}{s}$. ◄ **UE 328**

Es stellt sich Frage, ob in allen faktoriellen Ringen Normierungsfunktionen existieren. Bevor wir uns diesem Problem widmen, betrachten wir die für uns wichtigsten Beispiele. Neben dem Körper $\mathbb{Q}$ der rationalen Zahlen als Quotientenkörper von $\mathbb{Z}$ ist das der Quotientenkörper eines Polynomrings.

**Definition 5.3.1.5.** Sind $\mathcal{R}$ und somit auch die Polynomringe $\mathcal{R}[x]$ in einer Variablen $x$ und $\mathcal{R}[X]$ in einer beliebigen Variablenmenge $X$ über $\mathcal{R}$ Integritätsbereiche, so heißen die Elemente der Quotientenkörper $\mathcal{R}(x)$ und $\mathcal{R}(X)$ von $\mathcal{R}[x]$ bzw. $\mathcal{R}[X]$ *gebrochen rationale Funktionen* über $\mathcal{R}$ in einer Variablen $x$ bzw. in den Variablen $x \in X$.

**Beispiel 5.3.1.6.**

1. Im faktoriellen Ring $R = \mathbb{Z}$ gibt es die Normierungsfunktion $\nu : k \mapsto |k|$. Damit erhalten wir die bekannte Aussage, dass jede rationale Zahl (= jedes Element des Quotientenkörpers $K = \mathbb{Q}$ von $R = \mathbb{Z}$) genau eine gekürzte Darstellung mit einem Nenner hat, der eine natürliche Zahl ist.

2. Ist $R = K[x]$ der Polynomring über einem Körper $K$, so gibt es die Normierungsfunktion $\nu : a_n x^n + a_{n-1}x^{n-1} + \ldots a_1 x + a_0 \mapsto x^n + \frac{a_{n-1}}{a_n} + \ldots + \frac{a_1}{a_n}x + \frac{a_0}{a_n}$ für $a_n \neq 0$, die jedem Polynom $\neq 0$ jenes assoziierte zuordnet, dessen führender Koeffizient 1 ist, das also normiert oder, wie man auch sagt, monisch ist. Entsprechend hat jede gebrochen rationale Funktion (= jedes Element des Quotientenkörpers $K(x)$ von $K[x]$) eine eindeutige gekürzte Darstellung mit normiertem Nenner.

Wie wir im nächsten Unterabschnitt sehen werden, bilden auch die Polynome in mehreren Variablen über beispielsweise einem Körper einen faktoriellen Ring. Auch hier lässt sich eine manchmal praktische Normierungsfunktion finden; in 5.3.4 werden wir diese als Nebenprodukt definieren.
Tatsächlich erlaubt die Primfaktorzerlegung in faktoriellen Ringen, dass wir stets Normierungsfunktionen definieren können:

**Lemma 5.3.1.7.** *Sei $R$ ein faktorieller Ring. Dann existiert eine Normierungsfunktion $\nu : R \to R$.*

*Beweis.* Sei $P \subseteq R$ ein Vertretersystem der irreduziblen (also primen) Elemente modulo Assoziiertheit, d.h. für jedes irreduzible Element $q \in R$ existiere ein eindeutiges $p \in P$ mit $p \sim q$. Man überlegt sich sehr schnell, dass sich jedes Element $r \in R$ *eindeutig* in der Form $r = a\prod_{p\in P} p^{e_p}$ mit einer Einheit $a \in E(R)$ und Exponenten $e_p \in \mathbb{N}$ (wobei fast alle gleich 0 sind) schreiben lässt. Die Abbildung $\nu : R \to R$, $\nu(r) := \prod_{p\in P} p^{e_p}$, wobei $r = a\prod_{p\in P} p^{e_p}$ diese eindeutige Darstellung ist, ist wohldefiniert und eine Normierungsfunktion. □

Es sei angemerkt, dass die gerade konstruierte Normierungsfunktion sowohl konzeptuell als auch in puncto effektiver Berechenbarkeit manches zu wünschen übrig lässt – schließlich erfordert die Berechnung von $\nu(r)$ die Bestimmung der Primelemente. Selbst wenn die Primelemente bekannt sind, muss man eine Primfaktorzerlegung durchführen, was bereits in $\mathbb{Z}$ sehr aufwendig ist. Viel praktischer – sowohl abstrakt als auch in konkreten Berechnungen – ist es, wenn die Normierungsfunktion wie in $\mathbb{Z}$ oder $K[x]$ ohne Rückgriff auf die Primfaktorzerlegung direkt bestimmt werden kann.

### 5.3.2 Polynomringe über faktoriellen Ringen sind faktoriell

Inhalt in Kurzfassung: Dieser Unterabschnitt steht gänzlich im Zeichen des Beweises folgenden Satzes von Gauß: Der Polynomring über einem faktoriellen Ring ist wieder faktoriell.

In diesem Abschnitt soll vor allem der folgende Satz von Gauß bewiesen werden:

**Satz 5.3.2.1** (Gauß)**.** *Ist $R$ ein faktorieller Ring (z.B. ein Körper), so ist auch der Polynomring $R[x]$ über $R$ in einer Variablen $x$ faktoriell. Folglich sind auch die Ringe $R[x_1, \ldots, x_n]$ in $n$ Variablen und sogar der Polynomring $R[X]$ über $R$ in einer beliebigen Variablenmenge $X$ faktoriell.*

Offenbar genügt es, den Satz für eine einzige Variable zu beweisen. Denn dann folgt er mittels Induktion für endlich viele und, weil auch bei unendlicher Variablenmenge $X$ jedes Polynom nur endlich viele Variablen enthält, auch für den allgemeinen Fall.

**UE 329** ► **Übungsaufgabe 5.3.2.2.** (V) Führen Sie diese Überlegungen im Detail aus, d.h.: Beweisen Sie Satz 5.3.2.1 unter der Voraussetzung, dass er für den Polynomring $R[x]$ in einer Variablen über einem beliebigen faktoriellen Ring $R$ gilt. ◄ **UE 329**

Die Grundidee des Beweises für eine Variable besteht darin, die Frage auf zwei bekanntermaßen faktorielle Ringe zurückzuspielen: den Koeffizientenbereich $R$ und den Polynomring $Q[x]$ über dem Quotientenkörper $Q$ von $R$. Die Ausgangsüberlegung ist sehr natürlich und führt sehr schnell zum entscheidenden Punkt: Wir gehen von einem Polynom $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ aus. Ist $c_f \in R$ ein ggT der Koeffizienten $a_i$, so können wir diesen herausheben und $f = c_f f_0$ schreiben mit einem $f_0 \in R[x]$ dessen Koeffizienten teilerfremd sind. Polynome mit dieser Eigenschaft wollen wir der einfacheren Sprechweise halber und nur in diesem Kontext *primitiv*[6] nennen. (Offenbar ist jedes über $R$ irreduzible Polynom $f \in R[x]$ primitiv.) Sowohl $c_f$ als auch $f_0$ lassen sich in irreduzible Faktoren zerlegen: Bei $c_f \in R$ ist das klar, weil $R$ faktoriell ist. Und für $f_0$ – sofern es nicht schon selbst irreduzibel ist – müssen die Faktoren in einer echten Zerlegung gleichfalls primitiv sein (andernfalls hätten die $a_i$ einen nichttrivialen ggT, was der Primitivität von $f_0$ widerspräche) und kleineren Grad haben als $f$. Deshalb muss fortgesetzte Faktorisierung

[6] Diese Bedeutung des Wortes *primitiv* darf nicht mit jener verwechselt werden, die in der Theorie der endlichen Körper eine wichtige Rolle spielt (siehe Definition 6.3.3.2) und die sich ebenfalls auf Polynome beziehen kann.

nach endlich vielen Schritten zu einer Zerlegung in irreduzible Faktoren führen. Somit ist klar, dass Zerlegung in irreduzible Faktoren auch im Polynomring $R[x]$ möglich ist:

$$f = c_1 \cdot \ldots \cdot c_k \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_r$$

mit irreduziblen (daher primen, da $R$ faktoriell ist) Elementen $c_i \in R$ und irreduziblen (folglich primitiven) Polynomen $p_j \in R[x]$ vom Grad $\geq 1$. Zu zeigen bleibt noch die Eindeutigkeit dieser Zerlegung bis auf Reihenfolge der Faktoren und Assoziiertheit $\sim$ in $R[x]$. Die Einheiten von $R[x]$ sind genau die Einheiten von $R$, siehe Proposition 3.4.6.5, Aussage 6. Also gilt $f \sim g$ genau dann, wenn es eine Einheit $e \in E(R)$ in $R$ mit $f = eg$ gibt.

Wir wollen uns nun überlegen, dass der Beweis des Satzes von Gauß vollständig ist, sofern wir zeigen können, dass in $R[x]$ irreduzible Polynome $f$ sogar über dem Quotientenkörper $Q$ von $R$ irreduzibel sind – obwohl a priori ja Zerlegungen $f = f_1 f_2$ mit $f_i \in Q[x] \setminus R[x]$ denkbar wären. Unter dieser Voraussetzung (nämlich dass Irreduzibilität über $R$ auch jene über $Q$ impliziert) führen nämlich je zwei Zerlegungen

$$f = c_1 \cdot \ldots \cdot c_k \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_r = d_1 \cdot \ldots \cdot d_l \cdot q_1 \cdot q_2 \cdot \ldots \cdot q_s$$

mit irreduziblen $c_1, c_2, \ldots, c_k$ und $d_1, d_2, \ldots, d_l$ aus $R$ sowie irreduziblen (folglich auch primitiven) Polynomen $p_1, p_2, \ldots, p_r$ und $q_1, q_2, \ldots, q_s$ aus $R[x]$ zu zwei irreduziblen Zerlegungen

$$f = c \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_r = d \cdot q_1 \cdot q_2 \cdot \ldots \cdot q_s$$

über $Q$, wobei $c := c_1 \cdot \ldots \cdot c_k$ und $d := d_1 \cdot \ldots \cdot d_l$ Einheiten in $Q[x]$ sind. Weil $Q[x]$ faktoriell ist, müssen die $p_i$ und die $q_j$ bis auf Reihenfolge und Assoziiertheit in $Q[x]$ übereinstimmen. Assoziiertheit in $Q[x]$ bedeutet Übereinstimmung bis auf einen multiplikativen Faktor, der eine Einheit in $Q$, d.h. ein Element von $Q^\times$, ist. Nun sind sowohl die $p_i$ als auch die $q_j$ aber primitiv. Das ist nur möglich, wenn der entsprechende multiplikative Faktor jeweils sogar eine Einheit in $R$ ist. Folglich gilt die Assoziiertheit jedes $p_i$ mit dem zugehörigen $q_j$ sogar über $R$, was den Satz 5.3.2.1 von Gauß beweist.

Offen ist damit nur noch „irreduzibel über $R$ impliziert irreduzibel über $Q$“ für Polynome $f \in R[x]$. Um das zu beweisen, beobachten wir zunächst, dass die Zerlegung $f = c_f f_0$ mit einem primitiven $f_0 \in R[x]$ (!) auch für jedes $f \in Q[x]$ möglich ist, sofern wir $c_f \in Q$ zulassen (Herausheben eines gemeinsamen Nenners). Außerdem sind $c_f$ und $f_0$ durch $f$ bis auf $\sim$ eindeutig bestimmt. Zusammengefasst:

**Proposition 5.3.2.3.** *Sei $Q$ der Quotientenkörper des faktoriellen Ringes $R$ und $f \in Q[x]$. Dann gibt es ein $c_f \in Q$ (genannt auch ein* Inhalt *von $f$) und ein primitives Polynom $f_0 \in R[x]$ mit $f = c_f f_0$. Im folgenden Sinn besteht sogar Eindeutigkeit: Ist $f \neq 0$ und gilt überdies $f = c_f f_0 = d_f g_0$ mit $d_f \in Q$ und einem weiteren primitiven Polynom $g_0 \in R[x]$, dann gibt es eine Einheit $e \in E(R)$ von $R$ mit $c_f = d_f e$ und $g_0 = f_0 e$.*

**UE 330** ► **Übungsaufgabe 5.3.2.4.** (V) Beweisen Sie Proposition 5.3.2.3 in aller Ausführlichkeit. ◄ **UE 330**

Damit können wir das entscheidende Lemma beweisen, aus dessen letzter Aussage nach unseren Überlegungen weiter oben auch der Satz von Gauß folgt:

**Lemma 5.3.2.5.** *Seien $f, g \in Q[x]$.*

1. *Sind $f$ und $g$ aus $R[x]$ und primitiv, so auch $fg$.*
2. *Stets gilt $c_{fg} \sim c_f c_g$.*
3. *Ist $f \in R[x]$ mit $\operatorname{grad}(f) \geq 1$ irreduzibel über $R$, so auch über $Q$.*

*Beweis.* 1. Sei $f(x) = a_0 + a_1 x + \cdots + a_m x^m$, $g(x) = b_0 + b_1 x + \cdots + b_n x^n$ und $fg(x) = c_0 + c_1 x + \cdots + c_{m+n} x^{m+n}$. Weil $f$ und $g$ in $R[x]$ liegen, gilt das auch für $fg$. Angenommen $fg$ wäre nicht primitiv, dann gäbe es ein Primelement $p \in R$, das $c_0, ..., c_{m+n}$ teilt. Da $f$ und $g$ primitiv sind, gibt es ein $i$ und ein $j$ mit $0 \leq i \leq m$ und $0 \leq j \leq n$, so dass $p|a_0, ..., p|a_{i-1}$, $p \nmid a_i$ und $p|b_0, ..., p|b_{j-1}, p \nmid b_j$. Nun ist $c_{i+j} = \sum_{\mu+\nu=i+j} a_\mu b_\nu = a_i b_j + \sum'$, wobei $\sum'$ für alle anderen Summanden aus der Summe steht (für die entweder $\mu < i$ oder $\nu < j$ ist). Klarerweise teilt $p$ jeden Summanden aus $\sum'$ und somit auch $\sum'$ selbst. Da $p|c_{i+j}$, folgt daraus, dass $p|a_i b_j$. Da $p$ Primelement ist, folgt $p|a_i$ oder $p|b_j$, im Widerspruch zu $p \nmid a_i$ und $p \nmid b_j$.

2. Sei $f = c_f f_0$ und $g = c_g g_0$ mit primitiven Anteilen $f_0, g_0 \in R[x]$. Dann gilt $fg = c_f c_g f_0 g_0$, wobei $f_0 g_0$ nach dem ersten Teil primitiv ist. Also ist $c_{f_0 g_0}$ eine Einheit. Wegen $c_{af} \sim a c_f$ folgt daraus $c_{fg} = c_{c_f c_g f_0 g_0} = c_f c_g c_{f_0 g_0} \sim c_f c_g$.

3. Als über $R$ irreduzibles Polynom muss $f$ primitiv sein, weil andernfalls $f = c_f f_0$ eine nichttriviale Zerlegung über $R$ wäre. Ist $\operatorname{grad}(f) = 1$, so ist $f$ jedenfalls irreduzibel über $Q$. Wir haben also lediglich die indirekte Annahme $f = gh$ mit $g, h \in Q[x]$ und $\operatorname{grad}(g), \operatorname{grad}(h) \geq 1$ auf einen Widerspruch zu führen. Es gibt primitive Polynome $g_0, h_0 \in R[x]$ mit $g = c_g g_0$ und $h = c_h h_0$. Weil $f$ primitiv ist, ist $c_f$ eine Einheit, also wegen der zweiten Aussage auch $c_g c_h \sim c_{gh} = c_f \sim 1$, insbesondere gilt $c_g c_h \in R$. Folglich ist $f = gh = (c_g c_h) g_0 h_0$ eine Zerlegung von $f$ in $R$ mit nichttrivialen Faktoren $f_0$ und $g_0$, was der Irreduzibilität von $f$ über $R$ widerspricht. □

In unseren Überlegungen haben wir Assoziiertheitsrelationen bezüglich verschiedener Ringe verwendet. Dabei ist durchaus Sorgfalt geboten, wie die folgende Übungsaufgabe zeigt.

**UE 331** ► **Übungsaufgabe 5.3.2.6.** (E) Finden Sie drei faktorielle Ringe $R_1 \leq R_2 \leq R_3$, sodass aber die von $E(R_1)$ auf $R_3$ definierte Äquivalenzrelation $\sim_1$ ◄ **UE 331**

$$x \sim_1 y :\Leftrightarrow \exists e \in E(R_1) : y = xe,$$

die von $E(R_2)$ auf $R_3$ definierte Äquivalenzrelation $\sim_2$

$$x \sim_2 y :\Leftrightarrow \exists e \in E(R_2) : y = xe$$

und die Assoziiertheitsrelation $\sim$ auf $R_3$ (die ja analog von $E(R_3)$ induziert wird) paarweise verschieden sind.
Hinweis: Man kann $R_3 = \mathbb{Q}$ wählen.
(Wenn das zu leicht ist: Finden Sie möglichst viele Unterringe von $\mathbb{Q}$, die auf $\mathbb{Q}$ lauter verschiedene Äquivalenzrelationen induzieren.)

Mit einer ähnlichen Idee wie Teil 1 in Lemma 5.3.2.5 beweist man auch die folgende nützliche Aussage:

**Proposition 5.3.2.7** (Eisensteinsches Kriterium)**.** *Sei $R$ ein faktorieller Ring. Ist $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ mit Grad $\geq 1$ ein primitives Polynom und $p \in R$ irreduzibel mit*

$$p \nmid a_n,\ p \mid a_i \text{ für } i = 0, \ldots, n-1, \text{ und } p^2 \nmid a_0,$$

*dann ist $f$ irreduzibel in $R[x]$.*

**UE 332 ► Übungsaufgabe 5.3.2.8.** (W) Beweisen Sie Proposition 5.3.2.7. **◄ UE 332**

Hilfreich bei der Suche nach rationalen Nullstellen eines Polynoms mit ganzen Koeffizienten ist:

**Proposition 5.3.2.9.** *Seien $R$ ein faktorieller Ring, $f \in R[x]$ mit führendem Koeffizienten $a_n$ und konstantem Koeffizienten $a_0$ und $p, q \in R$ teilerfremd und das Element $\frac{p}{q}$ des Quotientenkörpers $Q$ von $R$ eine Nullstelle von $f$. Dann gilt $p|a_0$ und $q|a_n$.*

**UE 333 ► Übungsaufgabe 5.3.2.10.** (W) Beweisen Sie Proposition 5.3.2.9. **◄ UE 333**

### 5.3.3 Faktorisierung von Polynomen

Inhalt in Kurzfassung: Aus der Polynomdivision mit Rest folgt sehr schnell: Ein Polynom ist genau dann durch einen Linearfaktor mit Nullstelle $\alpha$ teilbar, wenn es selbst $\alpha$ als Nullstelle hat. Daraus ergibt sich eine Verschärfung des Fundamentalsatzes der Algebra: Jedes komplexe Polynom lässt sich in Linearfaktoren zerlegen. Daraus wiederum lässt sich folgern, dass jedes reelle Polynom in Linear- und quadratische Faktoren zerfällt. Das Ende des Unterabschnitts bildet die bekannte Lösungsformel für quadratische Gleichungen und ein kurzer Ausblick auf die Frage nach Lösungsformeln für Gleichungen höheren Grades (Schlagwort Galoistheorie, Kapitel 9).

Schon die bisherigen Untersuchungen legen das genauere Studium der Faktorisierung von Polynomen über Körpern nahe. Tatsächlich handelt es sich dabei um einen der zentralen Themenbereiche der klassischen Algebra. Das liegt zu einem guten Teil am engen Zusammenhang mit der Lösung algebraischer Gleichungen und somit mit Nullstellen von Polynomen. Entsprechend rückt auch der aus der Analysis vertraute Aspekt von Polynomen in den Vordergrund, nämlich Funktionen darzustellen. Die erste wichtige Beobachtung gilt auch allgemein:

**Proposition 5.3.3.1.** *Sei $\mathcal{R} = (R, +, 0_R, -, \cdot, 1_R)$ ein kommutativer Ring mit 1, $f \in \mathcal{R}[x]$ und $\alpha \in R$. Dann sind die folgenden beiden Aussagen äquivalent:*

1. *$f(\alpha) = 0$.*
2. *Das Polynom $p$ mit $p(x) = x - \alpha$ ist ein Teiler von $f$.*

*Beweis.* 1. $\Rightarrow$ 2.: Weil der führende Koeffizient von $p(x) = x - \alpha = 1_R x - \alpha$ das Einselement ist, lässt sich Division mit Rest durchführen (vgl. Satz 3.4.6.7) und liefert eine Darstellung $f = pq + r$ mit einem $q \in \mathcal{R}[x]$ und einem Rest $r \in \mathcal{R}[x]$, dessen Grad kleiner ist als der von $p$, also 0. Somit ist $r \in R$ eine Konstante. Einsetzen von $\alpha$ für $x$ liefert $0_R = f(\alpha) = (\alpha - \alpha)q(\alpha) + r = r$. Also ist $f = pq$ teilbar durch $p(x) = x - \alpha$.
2. $\Rightarrow$ 1.: Ist $p$ ein Teiler von $f$, so gibt es ein $q \in \mathcal{R}[x]$ mit $f = pq$. Wieder setzen wir $\alpha$ für $x$ ein und erhalten $f(\alpha) = p(\alpha)q(\alpha) = (\alpha - \alpha)q(\alpha) = 0_R$. □

Hat ein Polynom $f$ neben $\alpha = \alpha_1$ noch weitere Nullstellen $\alpha_2, \ldots, \alpha_n$ (paarweise verschieden), so lässt sich induktiv fortfahren. Laut Proposition 5.3.3.1 gilt zunächst $f(x) = (x - \alpha_1)q_1(x)$ mit einem $q_1 \in \mathcal{R}[x]$. Einsetzen von $\alpha_2$ liefert $0_R = f(\alpha_2) = (\alpha_2 - \alpha_1)q_1(\alpha_2)$. Für $\alpha_1 \neq \alpha_2$ ist der erste Faktor $\alpha_1 - \alpha_2$ von $0_R$ verschieden. Wenn $\mathcal{R}$ ein Integritätsbereich ist, folgt daraus $q_1(\alpha_2) = 0$ und somit, wieder wegen Proposition 5.3.3.1, $q_1(x) = (x - \alpha_2)q_2(x)$ mit einem $q_2 \in \mathcal{R}[x]$, also $f = (x - \alpha_1)(x - \alpha_2)q_2(x)$. Fährt man in dieser Weise fort, erhält man:

**Proposition 5.3.3.2.** *Seien $\mathcal{R} = (R, +, 0_R, -, \cdot, 1_R)$ ein Integritätsbereich, $f \in \mathcal{R}[x]$ und $\alpha_i \in R$, $i = 1, \ldots, n$, paarweise verschieden mit $f(\alpha_i) = 0_R$. Dann gibt es ein $q \in \mathcal{R}[x]$ mit*

$$f(x) = q(x) \prod_{i=1}^{n} (x - \alpha_i).$$

*Folglich ist der Grad von $f$ mindestens $n$ (die Anzahl der verschiedenen Nullstellen).*

Ein Polynom kann auch durch höhere Potenzen $(x - \alpha)^e$ von Linearfaktoren teilbar sein. Entsprechend definiert man:

**Definition 5.3.3.3.** Hat das Polynom $f$ über dem Integritätsbereich $R$ die Zerlegung

$$f(x) = q(x) \prod_{j=1}^{m} (x - \alpha_j)^{e_j}$$

mit paarweise verschiedenen $\alpha_j$, ganzzahligen Exponenten $e_j \geq 1$ und einem Polynom $q$ ohne Nullstellen, so heißt $e_j$ die *Vielfachheit* der Nullstelle $\alpha_j$ in $f$.

Ist $R$ ein faktorieller Ring (z.B. ein Körper), so nach Satz 5.3.2.1 auch $R[x]$, woraus die Eindeutigkeit der $\alpha_j$ und $e_j$ folgt.

**UE 334** ► **Übungsaufgabe 5.3.3.4.** (E) Begründen Sie diese Behauptung. Gilt das auch, wenn ◄ **UE 334** $R$ nur ein Integritätsbereich ist?

Der wichtigste Fall für $\mathcal{R}$ ist der eines Körpers $K$. Von besonderem Interesse ist dabei der Körper $\mathbb{C}$ der komplexen Zahlen. Weil nach dem Fundamentalsatz der Algebra 1.2.4.8 jedes komplexe Polynom vom Grad $\geq 1$ mindestens eine Nullstelle hat, lässt sich die Abspaltung gemäß Proposition 5.3.3.2 so lange durchführen, bis $q$ den Grad 0 hat, also konstant ist. Damit ergibt sich die zweite Fassung des Fundamentalsatzes:

**Satz 5.3.3.5** (Fundamentalsatz der Algebra, Fassung 2)**.** *Jedes komplexe Polynom*

$$f(x) = \sum_{k=0}^{n} a_k x^k,$$

$a_k \in \mathbb{C}$*, mit* $n \geq 1$ *und* $a_n \neq 0$ *zerfällt in den führenden Koeffizienten* $a_n$ *und in bis auf die Reihenfolge eindeutig bestimmte normierte Linearfaktoren:*

$$f(x) = a_n \prod_{j=1}^{m} (x - \alpha_j)^{e_j}$$

*mit paarweise verschiedenen* $\alpha_j \in \mathbb{C}$ *und* $\sum_{j=1}^{m} e_j = n$*.*

Das hat auch bemerkenswerte Konsequenzen für reelle Polynome $f(x) = \sum_{k=0}^{n} a_k x^k$, $a_k \in \mathbb{R}$, mit einer komplexen Nullstelle $\alpha \in \mathbb{C}$. Verwendet man, dass die komplexe Konjugation $\varphi : z = a + ib \mapsto \overline{z} = a - ib$ ($a, b$ Real- bzw. Imaginärteil der komplexen Zahl $z$) ein Automorphismus des Körpers $\mathbb{C}$ ist (das folgt aus Satz 1.2.4.3), der $\mathbb{R}$ punktweise fest lässt, rechnet man nämlich nach:

$$f(\varphi(\alpha)) = \sum_{k=0}^{n} a_k \varphi(\alpha)^k = \sum_{k=0}^{n} \varphi(a_k)\varphi(\alpha)^k = \varphi\left(\sum_{k=0}^{n} a_k(\alpha)^k\right) = \varphi(f(\alpha)) = \varphi(0) = 0$$

Also ist mit $\alpha = a + ib$ auch die Konjugierte $\varphi(\alpha) = \overline{\alpha} = a - ib$ eine Nullstelle von $f$. Die zugehörigen komplexen Linearfaktoren multiplizieren sich zum rein reellen Polynom

$$\begin{aligned}(x - \alpha)(x - \overline{\alpha}) = (x - a - ib)(x - a + ib) = (x - a)^2 - (ib)^2 = \\ = x^2 - 2ax + (a^2 + b^2) \in \mathbb{R}[x].\end{aligned}$$

Die Nullstellen reeller Polynome treten also einerseits als reelle auf, denen Linearfaktoren entsprechen, und andererseits als Paare komplexer, denen jeweils ein reell nicht weiter zerlegbares quadratisches Polynom entspricht.

**Satz 5.3.3.6** (Fundamentalsatz der Algebra, reelle Fassung)**.** *Jedes reelle Polynom*

$$f(x) = \sum_{k=0}^{n} a_k x^k,$$

$a_k \in \mathbb{R}$*, mit* $n \geq 1$ *und* $a_n \neq 0$ *zerfällt in ein Produkt der Gestalt*

$$f(x) = a_n \prod_{i=1}^{m} (x - \alpha_i)^{e_i} \prod_{j=1}^{l} (x^2 + \beta_j x + \gamma_j)^{f_j}$$

*mit $m, l, e_i, f_j \in \mathbb{N}$, $e_i \geq 1$, $f_j \geq 1$ und $\sum_{i=1}^{m} e_i + 2\sum_{j=1}^{l} f_j = n$, wobei die Polynome $x^2 + \beta_j x + \gamma_j$ reell irreduzibel sind. Die reellen Nullstellen $\alpha_i$, $i = 1, \ldots, m$, können paarweise verschieden gewählt werden, ebenso die Polynome $x^2 + \beta_j x + \gamma_j$. Bis auf die Nummerierung sind sie dann samt zugehörigen Vielfachheiten $e_i$ bzw. $f_j$ eindeutig bestimmt, ebenso wie $m$ und $l$.*

Die konkrete Ermittlung der Nullstellen eines komplexen Polynoms $f$ vom Grad $n$ erfolgt für $n = 2$ nach der bekannten Formel: Durch Normierung bringt man $f$ auf die Form $f(x) = x^2 + px + q$ mit $p, q \in \mathbb{C}$ und formt mittels Ergänzung auf ein vollständiges Quadrat um zu

$$f(x) = x^2 + px + q = \left(x + \frac{p}{2}\right)^2 - \frac{p^2}{4} + q.$$

Also ist $f(\alpha) = 0$ äquivalent zu $(\alpha + \frac{p}{2})^2 = \frac{p^2}{4} - q$ oder

$$\alpha = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}.$$

Weil in $\mathbb{C}$ Quadratwurzeln uneingeschränkt existieren, sind somit zwei Nullstellen von $f$ gefunden, die genau dann zusammenfallen, wenn[7] $4q = p^2$.
Allgemeine Lösungsformeln ähnlicher Art gibt es nur noch für die Grade $n = 3, 4$. Diese sind allerdings schon einigermaßen kompliziert. Für Grade $n \geq 5$ lässt sich zeigen, dass es überhaupt keine vergleichbaren Formeln mehr gibt. Dieses Thema ist der historische Ursprung der Galoistheorie, siehe Kapitel 9.
Häufig nützlich ist die folgende einfache Beobachtung:

**Proposition 5.3.3.7.** *Ein Polynom $f$ über einem Körper $K$ vom Grad 2 oder 3 ist genau dann irreduzibel, wenn $f$ in $K$ keine Nullstelle hat.*

**UE 335 ► Übungsaufgabe 5.3.3.8.** (F) Beweisen Sie Proposition 5.3.3.7. **◄ UE 335**

### 5.3.4 Symmetrische Polynome

Inhalt in Kurzfassung: Ein Polynom oder eine gebrochen rationale Funktion in mehreren Variablen heißt symmetrisch, wenn es invariant bleibt unter allen Permutationen der Variablen. Einfache Beispiele symmetrischer Polynome sind die elementarsymmetrischen. Der Hauptsatz über symmetrische Polynome besagt, dass sich jedes beliebige symmetrische Polynom in eindeutiger Weise als Polynom in diesen elementarsymmetrischen Polynomen darstellen lässt. Die elementarsymmetrischen Polynome treten auch im Satz

[7] Selbstverständlich kann man auch für nicht normierte quadratische Polynome der Form $ax^2 + bx + c$ eine analoge Lösungsformel angeben. Obwohl sie statt der beiden Parameter $p$ und $q$ drei Parameter $a$, $b$ und $c$ enthält und entsprechend komplizierter ist, erfreut sie sich unter dem Titel „große Lösungsformel“ im Schulunterricht mancherorts erstaunlicher Beliebtheit. Weil jedes quadratische Polynom mühelos normiert werden kann, leistet sie aber nicht mehr als die im Haupttext angegebene „kleine Lösungsformel“.

von Vieta auf.

Im gesamten Unterabschnitt sei $K$ ein Körper.

**Definition 5.3.4.1.** Sei $f$ eine gebrochen rationale Funktion über $K$, d.h. ein Element des Quotientenkörpers $K(x_1, \ldots, x_n)$ des Polynomrings $K[x_1, \ldots, x_n]$. Wir nennen $f$ *symmetrisch*, wenn für alle Permutationen $\pi \in S_n$ der $n$ Indizes gilt:

$$f(x_1, \ldots, x_n) = f(x_{\pi(1)}, \ldots, x_{\pi(n)}) \in K(x_1, \ldots, x_n).$$

Man beachte, dass in dieser ziemlich unmissverständlichen Schreibweise so wie auch weiter unten ein Einsetzungshomorphismus im Spiel ist. Und zwar gibt es genau einen Homomorphismus $\varphi : K[x_1, \ldots, x_n] \to K[x_1, \ldots, x_n]$ mit $\varphi(x_i) = x_{\pi(i)}$ für $i = 1, \ldots, n$. Mit $f(x_{\pi(1)}, \ldots, x_{\pi(n)})$ ist das Polynom $\varphi(f)$ gemeint. Offenbar lässt sich diese Abbildung sogar eindeutig zu einem Körperautomorphismus $K(x_1, \ldots, x_n) \to K(x_1, \ldots, x_n)$ fortsetzen.

**UE 336** ► **Übungsaufgabe 5.3.4.2.** (V) Zeigen Sie: Ist $g(y_1, \ldots, y_m) \in K[y_1, \ldots, y_m]$ ein beliebiges Polynom über $K$, und sind $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$ symmetrische Polynome über $K$, so entsteht durch Einsetzen der $f_i$ für die $y_i$ offenbar wieder ein symmetrisches Polynom $h := g(f_1, \ldots, f_m)$ in den Variablen $x_1, \ldots, x_n$. ◄ **UE 336**

Bemerkenswert ist, dass auch eine Art Umkehrung von Übungsaufgabe 5.3.4.2 gilt. Dazu definieren wir:

**Definition 5.3.4.3.** Für $n \in \mathbb{N}$ seien die *elementarsymmetrischen Polynome* $s_{n,k}$ in $n$ Variablen mit Multiplikationszahl $k = 1, \ldots, n$ gegeben durch

$$\begin{aligned}
s_{n,1} &= \sum_{i=1}^{n} x_i \\
s_{n,2} &= \sum_{1 \le i < j \le n} x_i \cdot x_j \\
&\vdots \\
s_{n,k} &= \sum_{i \le i_1 < \ldots < i_k \le n} x_{i_1} \cdot \ldots \cdot x_{i_k} \\
&\vdots \\
s_{n,n} &= x_1 \cdot \ldots \cdot x_n
\end{aligned}$$

Damit können wir formulieren:

**Satz 5.3.4.4** (Hauptsatz über symmetrische Polynome)**.** *Für jedes symmetrische Polynom $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ in $n$ Variablen über einem Körper $K$ gibt es ein eindeutiges Polynom $g \in K[x_1, \ldots, x_n]$ mit $f = g(s_{n,1}, \ldots, s_{n,n})$ und den elementarsymmetrischen Polynomen $s_{n,k}$ in $n$ Variablen.*

Für den Beweis verallgemeinern wir den Gradbegriff auf Polynome in mehreren Variablen. Der Grad eines Monoms $x_1^{i_1}x_2^{i_2}\dots x_n^{i_n} \in K[x_1,\dots,x_n]$ ist leicht zu definieren, nämlich als das Tupel $\vec{i} = (i_1, i_2, \dots, i_n) \in \mathbb{N}^n$. Um beliebigen Polynomen einen Grad zuordnen zu können, betrachten wir die *lexikographische Ordnung* $\leq_{n,\text{lex}}$ auf $\mathbb{N}^n$ (siehe auch Übungsaufgabe 2.1.10.10):
Für $\vec{i} := (i_1,\dots,i_n) \neq \vec{j} := (j_1,\dots,j_n)$ sei $k := k_{\vec{i},\vec{j}}$ der minimale Index mit $i_k \neq j_k$. Wir setzen $\vec{i} <_{n,\text{lex}} \vec{j}$ genau dann, wenn $i_{k_{\vec{i},\vec{j}}} < j_{k_{\vec{i},\vec{j}}}$. Weiters sei $\vec{i} \leq_{n,\text{lex}} \vec{j}$ genau dann, wenn $\vec{i} <_{n,\text{lex}} \vec{j}$ oder $\vec{i} = \vec{j}$. Man überzeugt sich leicht, dass $(\mathbb{N}^n, \leq_{n,\text{lex}})$ eine Totalordnung ist. Aus technischen Gründen definieren wir den Grad nur für Polynome, die nicht das Nullpolynom sind.

**Definition 5.3.4.5.** Für $f = \sum_{\vec{i}=(i_1,\dots,i_n)} c_{\vec{i}} x_1^{i_1}x_2^{i_2}\dots x_n^{i_n} \in K[x_1,\dots,x_n]$ mit $f \neq 0$ definieren wir den *Grad* von $f$ durch

$$\text{grad}(f) := \max_{\leq_{n,\text{lex}}} \left\{ \vec{i} \mid c_{\vec{i}} \neq 0 \right\}.$$

(Nach der Annahme $f \neq 0$ ist die rechte Seite nicht leer.)
Unter dem *führenden Koeffizienten* von $f$ verstehen wir $c_{\text{grad}(f)}$.

Der führende Koeffizient tritt also bei einem der Monome mit dem höchsten Grad in $x_1$ auf, und zwar unter diesen bei einem der Monome mit dem höchsten Grad in $x_2$, …, und zwar unter diesen bei dem (eindeutigen!) Monom mit dem höchsten Grad in $x_n$. Die Definition des Grads wird anhand eines Beispiels transparent:

**Beispiel 5.3.4.6.**

1. Ist $f = 3x_1^2x_2x_3^5 + 5x_1^2x_2x_3 - x_1x_2^4x_3^{10}$, so gilt $\text{grad}(f) = (2,1,5)$ und der führende Koeffizient ist 3.

2. Es gilt $\text{grad}(s_{n,k}) = (\underbrace{1,\dots,1}_{k \text{ Stellen}},0,\dots,0)$ und der führende Koeffizient von $s_{n,k}$ ist 1.

Die folgende Aussage wird sich im Beweis des Hauptsatzes über symmetrische Polynome als zentral herausstellen.

**Lemma 5.3.4.7.** *Sei $f \in K[x_1,\dots,x_n]$, $f \neq 0$, ein symmetrisches Polynom. Für* $\text{grad}\, f = (i_1,\dots,i_n)$ *gilt dann $i_1 \geq i_2 \geq \dots \geq i_n$. Außerdem ist $i_1$ der höchste Exponent* irgendeiner *Variable irgendeines Monoms, das in $f = \sum_{\vec{j}} c_{\vec{j}} x_1^{j_1}x_2^{j_2}\dots x_n^{j_n}$ vorkommt, d.h.*

$$i_1 := \max\left\{ \max_{\ell=1,\dots,n} j_\ell \mid c_{(j_1,\dots,j_n)} \neq 0 \right\}.$$

*Beweis.* Wir beobachten zunächst die folgende Tatsache: Sei $c_{\vec{j}} x_1^{j_1}x_2^{j_2}\dots x_n^{j_n}$ ein Monom, das in $f$ vorkommt. Ist $\sigma \in S_n$ eine Permutation[8] von $\{1,\dots,n\}$ mit $j_{\sigma(1)} \geq j_{\sigma(2)} \geq \dots \geq$

[8] Wenn in $\vec{j}$ ein gewisser Wert mehrfach vorkommt, dann gibt es mehrere solcher Permutationen.

$j_{\sigma(n)}$, so kommt wegen der Symmetrie von $f$ auch das Monom $c_{\vec{j}} x_1^{j_{\sigma(1)}} x_2^{j_{\sigma(2)}} \dots x_n^{j_{\sigma(n)}}$ in $f$ vor.
Daraus folgt, dass es zu jedem Monom, das in $f$ vorkommt, ein weiteres Monom mit absteigendem Grad gibt, dessen Grad $\leq_{n,\text{lex}}$-größer als der Grad des ursprünglichen Monoms ist – was die erste behauptete Aussage impliziert. Weiters folgt daraus, dass $f$ ein Monom enthält, dessen Grad in der $x_1$-Komponente genau

$$\max \left\{ \max_{\ell=1,\dots,n} j_\ell \mid c_{(j_1,\dots,j_n)} \neq 0 \right\}$$

ist – womit auch die zweite behauptete Aussage gezeigt ist. □

Der Beweis des Hauptsatzes wird gelingen, indem wir schrittweise vorgehen und den Grad von $f$ durch Subtraktion eines geeigneten Polynoms in $s_{n,1}, \dots, s_{n,n}$ laufend reduzieren. Vergleichbare Beweise für Polynome in einer Variablen funktionieren deshalb, weil es nur endlich viele mögliche Grade gibt, die kleiner oder gleich dem Grad des Ausgangspolynoms sind. Daher muss das Verfahren irgendwann zu einem Ende kommen. Bei Polynomen in mehreren Variablen ist das nicht ganz so einfach, da ein festes Element von $\mathbb{N}^n$ bezüglich $\leq_{n,\text{lex}}$ unendlich viele Vorgänger haben kann, z.B hat im Fall $n = 2$ das Paar $(1, 0)$ die unendlich vielen Vorgänger $(0, 0), (0, 1), \dots, (0, m), \dots$. Schränkt man sich aber auf symmetrische Polynome ein, dann kann dieses Phänomen wegen der zweiten Aussage von Lemma 5.3.4.7 nicht auftreten.

**Lemma 5.3.4.8.** *Sei $f \in K[x_1, \dots, x_n]$, $f \neq 0$, ein symmetrisches Polynom. Dann ist die Menge*

$$E := \{\text{grad}(f') \mid f' \in K[x_1, \dots, x_n] \text{ symmetrisch}, \text{grad}(f') \leq_{n,lex} \text{grad}(f)\} \subseteq \mathbb{N}^n$$

*endlich.*

*Beweis.* Wir schreiben $(i_1, \dots, i_n) = \vec{i} := \text{grad}(f)$ und für ein beliebiges symmetrisches $f'$ außerdem $(i'_1, \dots, i'_n) = \vec{i'} := \text{grad}(f')$.
Nach der zweiten Aussage von Lemma 5.3.4.7 ist $i'_1$ der höchste Exponent irgendeiner Variable irgendeines Monoms, das in $f'$ vorkommt. Aus $\text{grad}(f') \leq_{n,\text{lex}} \text{grad}(f)$ folgt $i'_1 \leq i_1$, also können in $f'$ insbesondere nur Monome mit Exponenten kleiner oder gleich $i_1$ vorkommen. Somit gilt $E \subseteq \{0, \dots, i_1\}^n$, womit die Behauptung bewiesen ist. □

Nach diesen Vorarbeiten können wir den Hauptsatz zeigen.

*Beweis (von Satz 5.3.4.4).* Wir zeigen zunächst die Existenz von $g$. Sei dazu ein symmetrisches Polynom $f \in K[x_1, \dots, x_n]$ gegeben. Wenn $f$ das Nullpolynom ist, so können wir $g = 0$ setzen. Wenn $f = \sum_{\vec{j}} c_{\vec{j}} x_1^{j_1} x_2^{j_2} \dots x_n^{j_n}$ nicht das Nullpolynom ist, dann betrachten wir $(i_1, \dots, i_n) = \vec{i} := \text{grad}(f)$ und den führenden Koeffizienten $c_{\vec{i}}$. Nach Lemma 5.3.4.7 gilt $i_1 \geq i_2 \geq \dots \geq i_n$. Wir definieren $g_1 := c_{\vec{i}} x_1^{i_1 - i_2} x_2^{i_2 - i_3} \dots x_{n-1}^{i_{n-1} - i_n} x_n^{i_n}$ und beobachten, dass

$$\text{grad}(g_1(s_{n,1}, \dots, s_{n,n})) = (i_1, \dots, i_n) = \vec{i}$$

sowie dass der führende Koeffizient von $\operatorname{grad}(g_1(s_{n,1},\dots,s_{n,n}))$ genau $c_{\vec{i}}$ ist. Somit ist $f' := f - g_1(s_{n,1},\dots,s_{n,n})$ ein symmetrisches Polynom, das bezüglich $\leq_{n,\mathrm{lex}}$ einen strikt kleineren Grad als $f$ hat. Wir iterieren diesen Prozess und finden ein Polynom $g_2$, sodass $f'-g_2(s_{n,1},\dots,s_{n,n})$ einen bezüglich $\leq_{n,\mathrm{lex}}$ nochmals echt kleineren Grad hat. So fortfahrend erhalten wir eine echt absteigende Folge von Graden symmetrischer Polynome, die alle $\leq_{n,\mathrm{lex}}$-kleiner als $\operatorname{grad}(f)$ sind. Wegen Lemma 5.3.4.8 muss der Prozess nach endlich vielen Schritten stoppen, sagen wir nach $\ell$ Schritten. Anders formuliert muss das symmetrische Ausgangspolynom von Schritt $\ell$ mit dem gefundenen Polynom $g_\ell(s_{n,1},\dots,s_{n,n})$ übereinstimmen. Somit gilt $f = g_1(s_{n,1},\dots,s_{n,n})+\cdots+g_\ell(s_{n,1},\dots,s_{n,n})$ und wir setzen $g := g_1+\cdots+g_\ell$.
Der Beweis der Eindeutigkeit verläuft sehr ähnlich. Wir beweisen, dass für Polynome $g,h \in K[x_1,\dots,x_n]$ aus $g(s_{n,1},\dots,s_{n,n}) = f = h(s_{n,1},\dots,s_{n,n})$ bereits $g = h$ folgt. Wenn $f$ das Nullpolynom ist, dann ist $g = 0 = h$ klar. Wenn $f$ nicht das Nullpolynom ist, dann gilt jedenfalls $g,h \neq 0$. Wir schreiben $g = \sum_{\vec{h}} a_{\vec{h}} x_1^{h_1}x_2^{h_2}\dots x_n^{h_n}$. Da der Grad von $(s_{n,1})^{h_1}(s_{n,2})^{h_2}\dots(s_{n,n})^{h_n}$ genau $(h_1+h_2+\cdots+h_n, h_2+\cdots+h_n,\dots,h_n)$ ist und da umgekehrt aus $(h_1+h_2+\cdots+h_n, h_2+\cdots+h_n,\dots,h_n)$ das Tupel $(h_1,\dots,h_n)$ eindeutig rekonstruierbar ist, gilt

$$\operatorname{grad}(g(s_{n,1},\dots,s_{n,n})) = \max\left\{(h_1+h_2+\cdots+h_n, h_2+\cdots+h_n,\dots,h_n) \mid a_{(h_1,\dots,h_n)} \neq 0\right\}.$$

Schreiben wir $\operatorname{grad}(g(s_{n,1},\dots,s_{n,n})) = (j_1+j_2+\cdots+j_n, j_2+\cdots+j_n,\dots,j_n)$, so ist der führende Koeffizient von $g(s_{n,1},\dots,s_{n,n})$ genau $a_{(j_1,\dots,j_n)}$.
Analoges gilt für $h(s_{n,1},\dots,s_{n,n})$, also muss das Monom $x_1^{j_1}x_2^{j_2}\dots x_n^{j_n}$ auch in $h$ vorkommen, und zwar mit demselben Koeffizienten $a_{(j_1,\dots,j_n)}$. Definieren wir das Monom $g_1 := a_{(j_1,\dots,j_n)}x_1^{j_1}x_2^{j_2}\dots x_n^{j_n}$, so hat folglich das symmetrische Polynom

$$f' := (g-g_1)(s_{n,1},\dots,s_{n,n}) = (h-g_1)(s_{n,1},\dots,s_{n,n})$$

einen bezüglich $\leq_{n,\mathrm{lex}}$ strikt kleineren Grad als $f$. Wenn wir das Argument wie im ersten Teil des Beweises iterieren, so muss dieser Prozess wieder wegen Lemma 5.3.4.8 nach endlich vielen Schritten stoppen, d.h. im $\ell$-ten Schritt muss das symmetrische Polynom das Nullpolynom sein. Somit sind auch die im $\ell$-ten Schritt erhaltenen Differenzpolynome $g-g_1-\cdots-g_\ell$ und $h-g_1-\cdots-g_\ell$ gleich dem Nullpolynom, woraus sich $g = h$ ergibt. □

Aus der Verallgemeinerung des Gradbegriffs für Polynome in mehreren Variablen ergibt sich eine Normierungsfunktion im Sinne von Definition 5.3.1.3, wie wir bereits in 5.3.1 angekündigt haben.

**Beispiel 5.3.4.9.** Für Polynome $f,g \in K[x_1,\dots,x_n]$ gilt $\operatorname{grad}(fg) = \operatorname{grad}(f)\operatorname{grad}(g)$. Auf dem Ring $R := K[x_1,\dots,x_n]$ ist daher

$$\nu : f = \sum_{\vec{i}} c_{\vec{i}} x_1^{i_1}x_2^{i_2}\dots x_n^{i_n} \mapsto \sum_{\vec{i}} \frac{c_{\vec{i}}}{c_{\operatorname{grad}(f)}} x_1^{i_1}x_2^{i_2}\dots x_n^{i_n}$$

eine Normierungsfunktion, zu deren Berechnung keine Primfaktorzerlegung notwendig ist.

Als mächtig in der Galoistheorie erweist sich Satz 5.3.4.4 vor allem in Verbindung mit der folgenden, auch als *Satz von Vieta*[9] bekannten Tatsache:

**Proposition 5.3.4.10** (Satz von Vieta)**.** *Die Koeffizienten eines in Linearfaktoren zerfallenden normierten Polynoms*

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 = \prod_{i=1}^{n}(x - \alpha_i)$$

*erfüllen*

$$a_k = (-1)^{n-k} s_{n,n-k}(\alpha_1, \ldots, \alpha_n).$$

*Wie oben bezeichnet dabei $s_{n,n-k}$ das elementarsymmetrische Polynom in $n$ Variablen mit Multiplikationszahl $n-k$.*

**UE 337** ► **Übungsaufgabe 5.3.4.11.** (B) Gegeben sei das Polynom $f(x) = x^4+x^3+x^2+x^1+1 = \frac{x^5-1}{x-1}$. ◄ **UE 337**

(1) Zerlegen Sie $f$ in seine irreduziblen Faktoren über $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$.

(2) Finden Sie Wurzelausdrücke für die reellen Zahlen $\cos\frac{k\pi}{5}$, $k = 1, 2, 3, 4$.

### 5.3.5 Gebrochen rationale Funktionen und ihre Partialbruchzerlegung

Inhalt in Kurzfassung: Gebrochen rationale Funktionen in einer Variablen können als Brüche dargestellt werden, die vermittels Kürzung und Normierung in eine Normalform gebracht werden können. Eine weitere Normalform gebrochen rationaler Funktionen ist aus der elementaren Analysis bekannt, wenn es um die Ermittlung einer Stammfunktion geht. Der Hintergrund ist ein algebraischer, nämlich die Primfaktorzerlegung. Dies soll nun dargelegt werden.

Gebrochen rationale Funktionen $r(x)$ in einer Variablen $x$ über einem Körper $K$ sind nach Definition Elemente des Quotientenkörpers $K(x)$ des Polynomrings $K[x]$ über $K$. Als solche haben Sie eine Darstellung als Brüche $r(x) = \frac{p(x)}{q(x)}$ mit $p(x), q(x) \in K[x]$. Durch die Forderung der Teilerfremdheit von $p$ und $q$ sowie der Normiertheit von $q$ kann man diese Darstellung eindeutig machen, womit sogar eine Normalform vorliegt, siehe Abschnitt 5.3.1. Andere Normalformen, die zum Beispiel in der Analysis bei der Integration gebrochen rationaler reeller Funktionen sehr nützlich sind, ergeben sich durch die sogenannte *Partialbruchzerlegung*, die wir nun besprechen wollen.
Polynomdivision mit Rest liefert für ein beliebiges $r(x) = \frac{p(x)}{q(x)} \in K(x)$ eine Darstellung $r(x) = f(x) + \frac{p_0(x)}{q(x)}$ mit Polynomen $f, p_0, q \in K[x]$, wobei $\operatorname{grad}(p_0) < \operatorname{grad}(q)$. Dabei ist $f$ jedenfalls eindeutig. Setzt man Teilerfremdheit von $p$ und $q$ sowie Normiertheit von $q$ voraus (was stets durch Kürzen sowie Division durch den höchsten Koeffizienten von

[9] Benannt nach dem französischen Mathematiker François Viète (1540-1603), der sich latinisiert Franciscus Vieta nannte.

$q$ erreicht werden kann), so sind auch $p_0$ und $q$ eindeutig und ebenfalls teilerfremd. Für Brüche von Polynomen, bei denen der Zählergrad kleiner ist als der Nennergrad, gibt es eine weitere Normalform, die man Partialbruchzerlegung nennt.
Sei dazu $q = q_1^{e_1} \cdot \ldots \cdot q_k^{e_k}$ mit positiven $e_i \in \mathbb{N}$ die Zerlegung des normierten Polynoms $q$ in paarweise verschiedene irreduzible und normierte Faktoren $q_i$ der Grade $m_i := \operatorname{grad}(q_i) > 0$. Wir betrachten $K(x)$ als Vektorraum über dem Körper $K$ und zwei Unterräume $U_1, U_2 \leq K(x)$, von denen wir zeigen werden, dass sie übereinstimmen. Und zwar werde $U_1$ erzeugt von den gebrochen rationalen Funktionen

$$r_{i,e,j} := \frac{x^j}{q_i^e}, \quad i = 1, \ldots, k, \quad e = 1, \ldots, e_i \quad j = 0, \ldots, m_i - 1.$$

Für die Anzahl $n$ der $r_{i,e,j}$ gilt

$$n = \sum_{i=1}^{k} \sum_{e=1}^{e_i} m_i = \sum_{i=1}^{k} e_i \operatorname{grad}(q_i) = \operatorname{grad}(q).$$

Gleichzeitig ist $n$ die Dimension des Unterraumes $U_2$, der von den (offenbar über $K$ linear unabhängigen) gebrochen rationalen Funktionen $\frac{x^l}{q}$ $(l = 0, \ldots, n-1 = \operatorname{grad}(q) - 1)$ erzeugt werde. Jede Linearkombination der $r_{i,e,j}$ lässt sich auf gemeinsamen Nenner $q$ bringen, wobei der Grad des resultierenden Zählerpolynoms stets kleiner als $n = \operatorname{grad}(q)$ bleibt. Somit ist $U_1$ in $U_2$ enthalten. Stimmen die Dimensionen überein, so folgt daraus sogar Gleichheit. Um $\dim U_1 = n = \dim U_2$ zu zeigen, genügt es nach obigen Überlegungen, die lineare Unabhängigkeit der $r_{i,e,j}$ zu überprüfen. Das ist eine Routineaufgabe:

**UE 338** ► **Übungsaufgabe 5.3.5.1.** (V) Zeigen Sie, dass die oben definierten gebrochen rationalen Funktionen $r_{i,e,j} \in K(x)$ $(i = 1, \ldots, k;\ e = 1, \ldots, e_i;\ j = 0, \ldots, m_i - 1)$ linear unabhängig über $K$ sind. ◄ **UE 338**

Damit folgt zusammenfassend der Satz von der *Partialbruchzerlegung*:

**Satz 5.3.5.2.** *Sei $K$ ein Körper und $r = \frac{p}{q}$ eine gebrochen rationale Funktion über $K$, $p, q \in K[x]$, $q$ normiert. Sei*

$$q = q_1^{e_1} \cdot \ldots \cdot q_n^{e_n}$$

*die Zerlegung des Nennerpolynoms $q$ in Potenzen irreduzibler und normierter Faktoren $q_i$, die sowohl paarweise als auch zu $p$ teilerfremd sind, und Vielfachheiten $e_i \geq 1$ haben mögen. Dann gibt es eindeutig bestimmte Polynome $f$ und $t_{i,e}$, $i = 1, \ldots, n$, $e = 1, \ldots, e_i$, mit $\operatorname{grad}(t_{i,e}) < \operatorname{grad}(q_i)$, so dass gilt:*

$$r = f + \sum_{i=1}^{n} \sum_{e=1}^{e_i} \frac{t_{i,e}}{q_i^e}$$

**Anmerkung 5.3.5.3.** 1. Sind im vorherigen Satz alle Primfaktoren $q_i$ linear, so sind die Zähler der Partialbrüche Konstante. Das ist sicher der Fall, wenn $K$ algebraisch abgeschlossen ist, also z.B. für $K = \mathbb{C}$.

2. Ist $K = \mathbb{R}$, so sind alle $q_i$ linear (reelle Nullstelle des Nennerpolynoms, dann sind die $t_{i,j}$ konstant) oder quadratisch (Paar konjugiert komplexer Nullstellen des Nennerpolynoms, dann sind die $t_{i,j}$ höchstens linear).

**UE 339** ▶ **Übungsaufgabe 5.3.5.4.** (D) Satz 5.3.5.2 spielt in der Analysis bei der Integration gebrochen rationaler Funktionen eine wichtige Rolle. Rekapitulieren Sie jene Integrationsregeln, mit deren Hilfe man zu jeder beliebigen in Partialbruchzerlegung vorgegebenen gebrochen rationalen Funktion eine Stammfunktion finden kann. Ist damit das Integrationsproblem für gebrochen rationale Funktionen auch in konventioneller Darstellung, d.h. als Quotient zweier Polynome, gelöst? ◀ **UE 339**

### 5.3.6 Interpolation nach Lagrange und nach Newton

Inhalt in Kurzfassung: Zu je $n+1$ Elementen eines Körpers $K$ zusammen mit vorgegebenen Funktionswerten gibt es genau eine interpolierende Polynomfunktion vom Grad $\leq n$. Die Formel von Lagrange liefert eine Darstellung dieses Interpolationspolynoms, dem man die geforderte Eigenschaft sehr unmittelbar ansieht. Vom algorithmischen Standpunkt ist die Interpolation nach Newton effektiver. Die Eindeutigkeit der Lösung folgt, weil die Differenz zweier Interpolationspolynome Grad $\leq n$ mit $\geq n+1$ Nullstellen hat, also das Nullpolynom sein muss.

Untersucht man Polynome unter dem Gesichtspunkt der Funktionen, die sie darstellen, so stellt sich die Frage, wie weit sich beliebige Funktionen als Polynomfunktionen darstellen lassen. Klarerweise gilt das nicht uneingeschränkt, sehr wohl aber bei Betrachtung endlich vieler Punkte (*Interpolation nach Lagrange*).

**Satz 5.3.6.1.** *Seien $K$ ein Körper, $a_0, \ldots, a_n \in K$ (*Stützstellen*) paarweise verschieden und $b_0, \ldots, b_n \in K$ (*Funktionswerte*) beliebig. Dann gibt es genau ein Polynom $p \in K[x]$ (*Interpolationspolynom*) vom Grad $\leq n$ mit $p(a_i) = b_i$ für $i = 0, 1, \ldots, n$. Dieses Polynom ist gegeben durch die Formel*

$$p(x) = \sum_{i=0}^{n} b_i \delta_i(x) \quad \textit{mit} \quad \delta_i(x) = \frac{\prod_{0 \leq j \leq n, j \neq i}(x - a_j)}{\prod_{0 \leq j \leq n, j \neq i}(a_i - a_j)}.$$

*(Die Polynome $\delta_i(x)$ heißen auch* Lagrange-Basispolynome*.)*

*Beweis.* Jedes $\delta_i$ ist nach Definition ein Polynom vom Grad $n$, daher ist $p$ als Summe der $b_i$-fachen der $\delta_i$ ein Polynom vom Grad $\leq n$. Außerdem gilt $\delta_j(a_i) = 0$ für $i \neq j$ und $\delta_i(a_i) = 1$. Hieraus liest man für $p$ selbst $p(a_i) = b_i$ für alle $i = 0, 1, \ldots, n$ ab.
Die Eindeutigkeit von $p$ ergibt sich so: Sei $q$ ein weiteres Polynom vom Grad $\leq n$ mit $q(a_i) = b_i$ für $i = 0, 1, \ldots, n$. Dann ist auch die Differenz $p - q$ ein Polynom vom Grad $\leq n$ mit den $n + 1$ verschiedenen Nullstellen $a_0, a_1, \ldots, a_n$. Das ist aber nur für das Nullpolynom $p - q = 0$ möglich, also gilt $q = p$. □

Für Anwendungen (auch) weit abseits der Algebra ist es von Interesse, das Interpolationspolynom $p$ aus 5.3.6.1 auch auf algorithmisch effektive Weise zu ermitteln. Die dort angegebene Formel lässt diesbezüglich manche Wünsche offen, insbesondere die Hoffnung, dass aus einem bereits berechneten $p$ möglichst rasch ein modifiziertes Polynom berechnet werden kann, wenn $n$ um 1 erhöht wird, d.h. wenn über die bereits gegebenen $a_i$ und $b_i$ hinausgehend für eine weitere Stelle $a_{n+1}$ ein Funktionswert $b_{n+1}$ vorgegeben wird. Die Vorgangsweise, die auf Newton zurückgeht, liegt auf der Hand:
Für die Folge $a_0, a_1, \ldots$ (paarweise verschieden) definieren wir die Polynome

$$q_j(x) := \prod_{k=0}^{j-1}(x - a_k)$$

und können Koeffizienten $\lambda_i$ (in eindeutiger Weise) so wählen, dass

$$p_i(x) := \sum_{j=0}^{i} \lambda_j q_j(x)$$

das Interpolationspolynom für $a_0, a_1, \ldots, a_i$ und $b_0, b_1, \ldots, b_i$ ist. Dass dies tatsächlich möglich ist, ergibt sich mittels Induktion: Für $i = 0$ ist $q_i = 1$ (leeres Produkt) und daher $\lambda_0 = b_0$ zu setzen. Angenommen, $p_i$ habe die behauptete Interpolationseigenschaft $p_i(a_j) = b_j$ für $j = 0, 1, \ldots, i$. Aus $p_i$ ergibt sich $p_{i+1} = p_i + \lambda_{i+1} q_{i+1}$ durch Addition des $\lambda_{i+1}$-fachen von $q_{i+1}$.
Offenbar ist $q_{i+1}$ so definiert, dass $q_{i+1}(a_j) = 0$ für $j = 0, 1, \ldots, i$ gilt, aber $q_{i+1}(a_{i+1}) \neq 0$. Folglich gilt $p_{i+1}(a_j) = p_i(a_j) + \lambda_{i+1} q_{i+1}(a_j) = p_i(a_j) = b_j$ für $j = 0, 1, \ldots, i$ und $p_{i+1}(a_{i+1}) = p_i(a_{i+1}) + \lambda_{i+1} q_{i+1}(a_{i+1}) = b_{i+1}$, wenn $\lambda_{i+1} = \frac{b_{i+1} - p_i(a_{i+1})}{q_{i+1}(a_{i+1})}$ gewählt wird.
Somit ist $p_n$ ein Interpolationspolynom wie $p$ in 5.3.6.1, muss aufgrund der dortigen Eindeutigkeitsaussage daher mit diesem übereinstimmen.

**Satz 5.3.6.2.** *Seien $K$ ein Körper, $a_0, \ldots, a_n \in K$ (*Stützstellen*) paarweise verschieden und $b_0, \ldots, b_n \in K$ (*Funktionswerte*) beliebig. Setzt man*

$$q_j(x) := \prod_{k=0}^{j-1}(x - a_k),$$

*dann kann man das eindeutige Interpolationspolynom vom Grad $\leq n$ mit $p(a_i) = b_i$ für $i = 0, 1, \ldots, n$ auch rekursiv durch die folgende Prozedur erhalten: Man setzt*

$$p_0(x) := b_0$$

*und*

$$p_{i+1}(x) := \sum_{j=0}^{i+1} \lambda_j q_j(x),$$

*wobei $\lambda_0 = b_0$ und $\lambda_{j+1} = \frac{b_{j+1} - p_j(a_{j+1})}{q_{j+1}(a_{j+1})}$. Das Interpolationspolynom ist dann $p(x) := p_n(x)$.*

*Das Polynom $p_j$ hängt dabei nur von den ersten $j+1$ Stützstellen $a_0, \ldots, a_j$ sowie von den ersten $j+1$ Funktionswerten $b_0, \ldots, b_j$ ab und kann außerdem aus dem Polynom $p_{j-1}(x)$ zusammen mit $b_j$, $a_j$ und dem Polynom $q_j(x)$ berechnet werden. Das Polynom $q_j(x)$ hängt weiters nur von den ersten $j$ Stützstellen $a_0, \ldots, a_{j-1}$ ab.*
*(Die Polynome $q_j(x)$ heißen auch* Newton-Basispolynome.*)*

# 6 Körper

Von den klassischen, an die Zahlenbereiche angelehnten algebraischen Strukturen haben die Körper die reichhaltigste Struktur und ermöglichen entsprechend die stärksten Aussagen. Recht schnell macht man sich einen Überblick über sämtliche minimalen Körper, die sogenannten Primkörper. Bis auf Isomorphie sind sie gegeben durch die endlichen Restklassenringe modulo einer Primzahl $p$ sowie durch den Körper der rationalen Zahlen. Alle anderen Körper sind Erweiterungen (siehe Abschnitt 6.1) von Primkörpern. Erweiterungen lassen sich verstehen als Zusammensetzung einer rein transzendenten Erweiterung, gefolgt von einer rein algebraischen, d.h. einer Adjunktion von Nullstellen von Polynomen. Solchen Adjunktionen ist Abschnitt 6.2 gewidmet. Einen vollständigen Überblick hat man über die endlichen Körper, genannt auch Galoisfelder. Ihre Kardinalität ist stets eine Primzahlpotenz $p^n$, $p \in \mathbb{P}$, $n \in \mathbb{N}^+$. Umgekehrt gibt es zu jedem solchen $p^n$ einen bis auf Isomorphie eindeutig bestimmten Körper (siehe Abschnitt 6.3).

## 6.1 Prim-, Unter- und Erweiterungskörper

Varietäten sind nach dem Satz von Birkhoff 4.1.7.1 charakterisiert durch ihre Abgeschlossenheit unter direkten Produkten, homomorphen Bildern und Unteralgebren. Bei Körpern verhält es sich anders: Das direkte Produkt von zwei oder mehr Körpern hat stets Nullteiler, ist also kein Körper. Homomorphe Bilder von Körpern gibt es nur die trivialen: isomorphe Bilder und den einelementigen Ring, der kein Körper ist. (Allerdings können Körper als nichttriviale homomorphe Bilder kommutativer Ringe mit 1 auftreten, wobei vor allem Polynomringe eine wichtige Rolle spielen werden.)
Nichttriviale Unterkörper hingegen kann es zuhauf geben. (Man beachte, dass es sich dabei wegen der Einschränkung bei der Bildung multiplikativer Inverser allerdings nicht um Spezialfälle des Konzepts der Unteralgebra eines Typs handelt. So ist $\mathbb{Z}$ Unteralgebra von $\mathbb{Q}$ als Ring mit 1, nicht aber Unterkörper.) Es überrascht daher nicht, dass die Theorie der Körper sehr stark um das Konzept von Unterkörpern bzw., von der anderen Seite betrachtet, von Körpererweiterungen kreist.
Die Inhalte des Abschnitts im Überblick: Jeder Körper hat einen kleinsten Unterkörper, seinen sogenannten *Primkörper* (6.1.1), lässt sich also als dessen Erweiterung auffassen. Nützlich ist es, Erweiterungskörper auch als Vektorraum über dem Grundkörper aufzufassen (6.1.2), weil dadurch mit Dimensionen gearbeitet werden kann. Von besonderem Interesse sind algebraische und transzendente Elemente (6.1.3) bzw. Körpererweiterungen (6.1.4 und 6.1.5). Jede beliebige Körpererweiterung ist eine Kombination der beiden reinen Typen, genauer: lässt sich als eine rein transzendente, gefolgt von einer rein algebraischen auffassen. Abschließend kommen wir noch auf die berühmten Konstruktionsprobleme mit Zirkel und Lineal aus der griechischen Antike zu sprechen (6.1.6), die

sich alle als unmöglich erweisen: Würfelverdoppelung, Winkeldreiteilung, Quadratur des Kreises.

### 6.1.1 Primkörper

Inhalt in Kurzfassung: Der Durchschnitt beliebig vieler Unterkörper eines Körpers $K$ ist wieder ein Unterkörper. Folglich erhält man, wenn man überhaupt alle Unterkörper schneidet, den kleinsten, den man auch den sogenannten Primkörper von $K$ nennt. Umgekehrt bedeutet das: Jeder Körper lässt sich als Erweiterung eines Primkörpers auffassen. Die Charakteristik eines Integritätsbereichs und erst recht eines Körpers kann nur 0 oder eine Primzahl $p$ sein. Im ersten Fall erhält man einen Primkörper, der zu $\mathbb{Q}$ isomorph ist, bei Primzahlcharakteristik zum Restklassenkörper $\mathbb{Z}_p$. Jeder Primkörper hat die Identität als einzigen Automorphismus.

Wir wiederholen und bauen aus:

**Definition 6.1.1.1.** Sei $L$ ein Körper, $K \subseteq L$ Unteralgebra von $L$ als Ring mit 1 und für sich genommen sogar ein Körper. Dann heißt $K$ *Unterkörper* von $L$ und $L$ *Oberkörper* oder *Erweiterungskörper* von $K$. Zusammen bilden $K$ und $L$ eine sogenannte *Körpererweiterung*. Das ist in diesem Kapitel mit der Schreibweise $K \leq L$ oder auch $L : K$ gemeint.

Eine Teilmenge $K \subseteq L$ eines Körpers $L$ ist genau dann Unterkörper von $L$, wenn $0_L, 1_L \in K$, $-a, a+b, ab \in K$ für alle $a, b \in K$ und $a^{-1} \in K$ für alle $a \in K^* = K \setminus \{0_L\}$.
So wie der Schnitt von Unteralgebren ist auch der Schnitt von Unterkörpern eines gegebenen Körpers $K$ wieder ein Unterkörper.

**UE 340** ▶ **Übungsaufgabe 6.1.1.2.** (F) Beweisen Sie, dass der Schnitt von Unterkörpern eines Körpers wieder ein Unterkörper ist, indem Sie Folgerung 2.3.1.9 möglichst wirkungsvoll einsetzen. Erklären Sie, warum es nicht genügt, sich ohne weitere Argumentation ausschließlich auf 2.3.1.9 zu berufen. ◀ **UE 340**

Die Unterkörper von $K$ bilden deshalb einen vollständigen Verband, und wir können in gewohnter Weise von *Erzeugnissen* sprechen. Insbesondere enthält dieser Verband ein kleinstes Element:

**Definition 6.1.1.3.** Ist $K$ ein Körper und $P$ der Durchschnitt sämtlicher Unterkörper von $K$ (= der kleinste Unterkörper von $K$), so heißt $P$ der *Primkörper* von $K$.

Vielfach nützlich ist folgende Beobachtung:

**Proposition 6.1.1.4.** *Ist $P$ der Primkörper des Körpers $K$ und $\sigma : K \to K$ ein Automorphismus von $K$, so gilt $\sigma(\alpha) = \alpha$ für alle $\alpha \in P$.*

**UE 341** ► **Übungsaufgabe 6.1.1.5.** (F) Beweisen Sie Proposition 6.1.1.4. Gehen Sie ähnlich vor wie in Übungsaufgabe 6.1.1.2, indem Sie diesmal Proposition 2.3.1.16 möglichst wirkungsvoll einsetzen, und erklären Sie, warum es nicht genügt, sich ausschließlich darauf zu beziehen. ◄ **UE 341**

Bei Erzeugnissen ist zwischen Körpererzeugnissen und Ringerzeugnissen, die auch im Kontext der Körper nützlich sind, zu unterscheiden. Wir verwenden folgende Notation.

**Definition 6.1.1.6.** Ist $L$ Oberkörper von $K$ und $S \subseteq L$, so definieren wir den *Erweiterungskörper* $K(S)$ von $K$ durch

$$K(S) := \bigcap \{E \subseteq L \mid E \text{ ist Unterkörper von } L, \text{ der } K \cup S \text{ enthält}\}.$$

Ist $S = \{\alpha_1, \ldots, \alpha_r\}$ endlich, so schreiben wir $K(S) =: K(\alpha_1, \ldots, \alpha_r)$. Eine Erweiterung $L$ von $K$ heißt *einfache Erweiterung von* $K$, wenn es ein $\alpha$ mit $L = K(\alpha)$ gibt.
Das *Ringerzeugnis* $K[S]$ definieren wir in bisherigen Kapiteln durch[1]

$$K[S] := \bigcap \{E \subseteq L \mid E \text{ ist Unterring mit 1 von } L, \text{ der } K \cup S \text{ enthält}\}.$$

Ist $S = \{\alpha_1, \ldots, \alpha_r\}$ endlich, so schreiben wir $K[S] =: K[\alpha_1, \ldots, \alpha_r]$.

**Anmerkung 6.1.1.7.** Es sei daran erinnert, dass wir auch für den Polynomring die Schreibweise $R[x]$ verwenden, siehe Definition 3.4.6.2. Tatsächlich ist aber der Polynomring $R[x]$ das Ringerzeugnis von $R \cup \{x\}$ im Ring der formalen Potenzreihen $R[[x]]$. Daher ist die Schreibweise $K[x]$ für das Ringerzeugnis gerechtfertigt[2].
Außerdem wird der Quotientenkörper des Polynomrings $K[x]$ wie der oben definierte Erweiterungskörper mit $K(x)$ bezeichnet, siehe Definition 3.4.6.9. Also verwenden wir die Schreibweise $K(\cdot)$ wieder für zwei scheinbar verschiedene Operationen. Tatsächlich ergibt sich aber, dass der Körper $K(x)$ aus Definition 3.4.6.9 ein Spezialfall von Definition 6.1.1.6 ist:
Schreiben wir nämlich $K(\alpha)$ (wenn $\alpha \in L \geq K$) für den kleinsten Unterkörper von $L$, der $K \cup \{\alpha\}$ enthält, und $K\langle x\rangle$ für den Quotientenkörper von $K[x]$, dann lässt sich jedes Element aus $K\langle x\rangle$ als Quotient $p(x)/q(x)$ mit $p(x), q(x) \in K[x]$, $q(x) \neq 0$ schreiben.
Offenbar enthält $K\langle x\rangle$ den gesamten Ring $K[x]$ und ist daher insbesondere eine Obermenge von $K \cup \{x\} \subseteq K[x]$. Sei umgekehrt $E \leq K\langle x\rangle$ ein beliebiger Unterkörper, der $K \cup \{x\}$ enthält, dann muss $E$ zunächst ganz $K[x]$, aber dann auch ganz $K\langle x\rangle$ enthalten. Somit ist $K\langle x\rangle$ der kleinste Unterkörper von $K\langle x\rangle$, der $K \cup \{x\}$ enthält, also $K\langle x\rangle = K(x)$.
Daher ist auch die Schreibweise $K(x)$ an Stelle von $K\langle x\rangle$ gerechtfertigt.

In 3.4.3 wurde für einen Ring $R$ mit Einselement $1_R$ der eindeutig bestimmte Homomorphismus $\varphi_R = \varphi\colon \mathbb{Z} \to R$ mit $1 \mapsto 1_R$ und sein Bild $R_0 = \varphi_R(\mathbb{Z})$ betrachtet. Der Kern $\ker \varphi_R$ ist ein Ideal im Hauptidealring $\mathbb{Z}$, wird also von einem Element $m \in \mathbb{N}$ erzeugt. Definitionsgemäß ist dieses $m$ die Charakteristik von $R$, symbolisch $\operatorname{char} R$.

[1] Hier verwenden wir ein anderes Symbol als früher.
[2] Wir haben sie sinngemäß auch bereits bei den quadratischen Zahlringen $\mathbb{Z}[\sqrt{D}]$ verwendet.

Wir wollen nun annehmen, dass $R$ nullteilerfrei ist mit $\operatorname{char} R = m$. Dann ist auch sein Unterring $R_0 \cong \mathbb{Z}/m\mathbb{Z}$ nullteilerfrei, was wiederum nur möglich ist, wenn $m = p \in \mathbb{P}$ oder $m = 0$. Im ersten Fall ist $R_0$ sogar ein Körper. Weil $R_0$ als Ring von $1_R$ erzeugt wird, handelt es sich dann um die kleinste Unteralgebra von $R$ als Ring mit 1 und erst recht um den kleinsten Unterkörper. Im zweiten Fall, nämlich bei $\operatorname{char} R = 0$, ist $R_0 \cong \mathbb{Z}$. Ist $R$ wieder ein Körper, so enthält $R$ eine isomorphe Kopie $Q_R$ des Quotientenkörpers von $\mathbb{Z}$, also von $\mathbb{Q}$. Dabei erhält man sämtliche Elemente von $Q_R$, indem man alle Brüche aus Elementen von $R_0$ mit Nenner $\neq 0_R$ bildet (siehe Proposition 3.4.5.9). Wir fassen unsere Erkenntnisse für Körper zusammen:

**Satz 6.1.1.8.** *Die Charakteristik eines Integritätsbereichs oder gar Körpers ist entweder* 0 *oder eine Primzahl* $p$*. Jeder Körper* $(K, +, 0, -, \cdot, 1)$ *enthält einen kleinsten Unterkörper* $P$*, seinen sogenannten* Primkörper*. Je nach Charakteristik* $\operatorname{char} K$ *sind folgende Fälle zu unterscheiden:*

1. *Für* $\operatorname{char} K = p \in \mathbb{P}$ *ist* $P = \varphi(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$ *isomorph zum Restklassenkörper modulo* $p$*.*
2. *Für* $\operatorname{char} K = 0$ *ist* $P \cong \mathbb{Q}$ *isomorph zum Körper* $\mathbb{Q}$ *der rationalen Zahlen, und es gilt* $P = \{ab^{-1} : \ a, b \in \varphi(\mathbb{Z}),\ b \neq 0_R\}$*.*

*Dabei bezeichnet* $\varphi$ *den Homomorphismus* $\varphi\colon \mathbb{Z} \to R$ *aus Lemma 3.4.3.1.*

**Notation 6.1.1.9.** Ab jetzt werden wir den Restklassenkörper modulo $p$ als $\mathbb{Z}_p$ und nicht als $\mathbb{Z}/p\mathbb{Z}$ notieren.

Klarerweise können endliche Körper nur Primzahlcharakteristik haben. Die Umkehrung gilt aber nicht, wie der unendliche Körper $\mathbb{Z}_p(x)$ der gebrochen rationalen Funktionen über $\mathbb{Z}_p$ beweist. Wir werden aber auch noch ein anderes wichtiges Beispiel kennen lernen, nämlich den algebraischen Abschluss $\mathrm{GF}(p^\infty)$ der endlichen Körper mit Charakteristik $p \in \mathbb{P}$.

### 6.1.2 Das Vektorraumargument

Inhalt in Kurzfassung: Jeder Erweiterungskörper lässt sich auch als Vektorraum über dem Grundkörper auffassen. Bei dieser Sichtweise schwächt man zwar die Struktur ab, gleichzeitig wird aber der Begriff der Dimension auch für Körpererweiterungen verfügbar. Der äußerst nützliche Gradsatz besagt, dass sich bei iterierten Körpererweiterungen Dimensionen aufmultiplizieren.

Ist $L$ Oberkörper von $K$, dann ist $L$ auch Vektorraum über $K$ mit den Operationen

$$\begin{aligned} a + b &\ldots \text{Summe in } L\ (a, b \in L), \\ \lambda a &\ldots \text{Produkt in } L\ (a \in L,\ \lambda \in K). \end{aligned}$$

Das gilt auch, wenn man auf die Kommutativität verzichtet und zulässt, dass $K$ ein Unterschiefkörper (Unterdivisionsring) von $L$ ist. In jedem Fall existiert daher eine Vektorraumbasis von $L$ über $K$. Diese bestimmt die Dimension $\dim_K L$. Wir definieren:

**Definition 6.1.2.1.** Für eine Körpererweiterung $K \leq L$ nennt man die Dimension $[L : K] := \dim_K L$ von L als Vektorraum über $K$ den *Grad der Körpererweiterung* $K \leq L$ bzw. von $L$ über $K$. Ist $[L : K] < \infty$, so heißt $L$ eine *endlichdimensionale Erweiterung* von $K$. Wegen Korollar 1.3.3.2 ist auch im Fall unendlicher Basen deren Kardinalität und somit die Dimension von $L$ (dann als unendliche Kardinalität) wohldefiniert. Somit kann unmissverständlich auch von *unendlichdimensionalen Erweiterungen* gesprochen werden.

Wenn $K \leq E \leq L$, dann ist $[L : E] \leq [L : K]$, weil jedes Erzeugendensystem des $K$-Vektorraums $L$ auch den $E$-Vektorraum $L$ erzeugt. Überdies ist $[E : K] \leq [L : K]$, weil $E$ Untervektorraum des $K$-Vektorraums $L$ ist. Weitreichende Konsequenzen hat der *Gradsatz*, der diese Beobachtungen verallgemeinert:

**Satz 6.1.2.2.** *Für $K \leq E \leq L$ (als Körper oder auch als Schiefkörper/Divisionsringe) gilt*

$$[L : K] = [L : E] \cdot [E : K].$$

**UE 342** ► **Übungsaufgabe 6.1.2.3.** (W) Beweisen Sie den Gradsatz, indem Sie zeigen: Ist die Familie $(a_i)_{i\in I}$ eine Basis von $E$ über $K$, die Familie $(b_j)_{j\in J}$ eine Basis von $L$ über $E$, so ist die Familie $(a_i b_j)_{(i,j)\in I\times J}$ eine Basis von $L$ über $K$. (Achtung: Ihre Argumentation muss auch für unendliches $I$ und $J$ gelten.) ◄ **UE 342**

**UE 343** ► **Übungsaufgabe 6.1.2.4.** (F) Wir fassen $\mathbb{R}$ als Vektorraum über dem Körper $\mathbb{Q}$ auf. Zeigen Sie, dass $\{1, \sqrt{5}\}$ eine linear unabhängige Menge ist. Bestimmen Sie weiters den Grad $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}]$ von $\mathbb{Q}(\sqrt{5})$ über $\mathbb{Q}$. ◄ **UE 343**

### 6.1.3 Algebraische und transzendente Elemente

Inhalt in Kurzfassung: Für ein Element $\alpha$ eines Erweiterungskörpers sind in Bezug auf den Grundkörper $K$ zwei grundsätzlich verschiedene Möglichkeiten denkbar. Entweder es besteht eine algebraische Beziehung zwischen $\alpha$ und Elementen aus $K$. In diesem Fall gibt es auch eine einfachste solche Beziehung, nämlich $f(\alpha) = 0$, wobei $f \in K[x]\setminus\{0\}$ das normierte Polynom von kleinstem Grad über $K$ mit dieser Eigenschaft ist, das sogenannte Minimalpolynom von $\alpha$. Dieses ist stets irreduzibel. Alle weiteren Polynome über $K$ mit $\alpha$ als Nullstelle sind Vielfache des Minimalpolynoms. In diesem Fall heißt $\alpha$ algebraisch über $K$. Im anderen Fall, d.h. wenn $\alpha$ nicht Nullstelle eines $f \in K[x] \setminus \{0\}$ ist, heißt $\alpha$ transzendent über $K$. In beiden Fällen lässt sich die Struktur des Erweiterungskörpers einfach beschreiben: $K(\alpha) \cong K[x]/(f)$ (Faktorisierung des Polynomrings nach dem vom Minimalpolynom erzeugten Hauptideal) im algebraischen Fall und $K(\alpha) \cong K(x)$ (Körper der gebrochen rationalen Funktionen über $K$) im transzendenten Fall. Auch einige verfeinerte Aussagen in diese Richtung, die später noch verwendet werden, sind Inhalt dieses Unterabschnitts.

Sei $\alpha \in L$, $L$ Körper, und $K \leq L$ ein Unterkörper. Das Verhalten von $\alpha$ in Bezug auf $K$ lässt sich mit Hilfe des Polynomringes $K[x]$ und des durch $\alpha$ induzierten Einsetzungshomomorphismus sehr gut verstehen. Der Hintergrund ist die universelle Eigenschaft der Polynomalgebra, wie sie in Abschnitt 4.2 behandelt wurde. Im Kontext der Körpertheorie ist es zunächst wichtig, sich zu vergegenwärtigen:

**Definition 6.1.3.1.** Seien $K \leq L$ Körper, und sei $\alpha \in L$. Sei $\varphi_\alpha \colon K[x] \to L$ der natürliche *Einsetzungshomomorphismus*:

$$a_0 + a_1 x + \cdots + a_n x^n \quad \mapsto \quad a_0 + a_1 \alpha + \cdots + a_n \alpha^n.$$

Offenbar ist die Wertemenge von $\varphi_\alpha$ genau das Ringerzeugnis $K[\alpha]$, der kleinste $K \cup \{\alpha\}$ enthaltende Unterring von $L$.
Aus dem Homomorphiesatz für Ringe wissen wir, dass der Kern $\ker(\varphi_\alpha)$ von $\varphi_\alpha$ ein Ideal von $K[x]$ ist, und dass $K[\alpha] \cong K[x]/\ker(\varphi_\alpha)$. $K[\alpha]$ ist als Unterring von $L$ ein Integritätsbereich, also ist $\ker(\varphi_\alpha)$ nach Proposition 3.4.2.4 ein Primideal. Weil der Polynomring $K[x]$ über dem Körper $K$ ein Hauptidealring ist, gibt es ein erzeugendes Element $m = m_\alpha = m_\alpha(x)$ von $\ker(\varphi_\alpha)$. Ist $m = 0$, so ist $\varphi_\alpha$ injektiv und man nennt $\alpha$ *transzendent*, andernfalls *algebraisch*. Man kann die Definition explizit auch so fassen:

**Definition 6.1.3.2.** Sei $L$ Oberkörper von $K$ und $\alpha \in L$. $\alpha$ heißt *algebraisch* über $K$, wenn es ein $f \in K[x] \setminus \{0\}$ gibt mit $f(\alpha) = 0$. Ist $n$ der minimale Grad eines solchen $f$, so sagt man auch, $\alpha$ ist *algebraisch vom Grad n*. Ist $\alpha$ nicht algebraisch, so heißt $\alpha$ *transzendent* über $K$. Im algebraischen Fall gibt es unter allen Polynomen, die $\ker(\varphi_\alpha)$ erzeugen, genau ein normiertes, d.h. mit höchstem Koeffizienten 1. Dieses Polynom $m(x) \in K[x]$ nennt man das *Minimalpoynom* von $\alpha$ über $K$.

Zunächst kurz zum transzendenten Fall: $\varphi_\alpha$ ist dann injektiv, also eine isomorphe Einbettung des Integritätsbereichs $K[x]$ in $L$. Als Körper enthält $L$ sogar eine isomorphe Kopie des Quotientenkörpers $K(x)$ von $K[x]$, nämlich $K(\alpha)$. Weil das auch für jedes weitere über $K$ transzendente Element $\beta$ gilt, ist auch $K(\alpha) \cong K(x) \cong K(\beta)$. Explizit:

**Satz 6.1.3.3** (Einfache transzendente Erweiterungen)**.** *Sei $K \leq L$, $\alpha \in L$ transzendent über $K$. Dann ist $K(x) \cong K(\alpha)$ (wobei $K(x)$ wieder der Quotientenkörper des Polynomrings $K[x]$ ist). Es gibt einen eindeutig bestimmten Isomorphismus $\varphi \colon K(x) \to K(\alpha)$, der $K$ punktweise fest lässt und $x$ auf $\alpha$ abbildet.*
*Insbesondere gilt: Seien $K \leq L_\alpha$ und $K \leq L_\beta$ irgendwelche Körpererweiterungen und $\alpha \in L_\alpha$ sowie $\beta \in L_\beta$ transzendent über $K$. Für die Körper $K(\alpha) \leq L_\alpha$ und $K(\beta) \leq L_\beta$ gilt dann $K(\alpha) \cong K(\beta)$, mit einem Isomorphismus, der $K$ punktweise fest lässt und $\alpha$ auf $\beta$ abbildet.*

Jetzt zum algebraischen Fall: Weil es ein Primideal erzeugt, muss $m$ ein Primelement sein, was in einem Hauptidealring äquivalent ist zur Irreduzibilität von $m$ und somit dazu, dass $K[\alpha] \cong K[x]/\ker(\varphi_\alpha)$ sogar ein Körper ist, also $K(\alpha) = K[\alpha]$.
Sei umgekehrt $\beta \in L$ irgendeine Nullstelle von $m_\alpha$. Dann ist $\beta$ algebraisch, hat also ein Minimalpolynom $m_\beta$, welches als Ideal $\ker(\varphi_\beta)$ erzeugt. Aus $m_\alpha \in \ker(\varphi_\beta)$ folgt $m_\beta | m_\alpha$.

Wegen der Irreduzibilität von $m_\alpha$ ist das nur möglich, wenn $m_\beta \sim m_\alpha$, woraus wegen der Normiertheit $m_\beta = m_\alpha$ folgt. Elemente $\alpha, \beta \in L$, deren Minimalpolynome über $K$ übereinstimmen, heißen *konjugiert* in $L$ über $K$. Wir fassen zusammen und ergänzen:

**Satz 6.1.3.4** (Einfache algebraische Erweiterungen)**.** *Sei $K \leq L$ und $\alpha \in L$ algebraisch über $K$. Sei $m$ das Minimalpolynom von $\alpha$ über $K$ und $k = \operatorname{grad}(m)$. Dann gilt:*

1. *Die Abbildung*

$$\psi : a_0 + a_1 x + \cdots + a_{k-1}x^{k-1} + (m) \quad \mapsto \quad a_0 + a_1\alpha + \cdots + a_{k-1}\alpha^{k-1}$$

   *ist wohldefiniert und ein Isomorphismus $K[x]/(m) \cong K[\alpha]$, und zwar der einzige mit $x + (m) \mapsto \alpha$ und $c + (m) \mapsto c$ für alle $c \in K$.*

2. *$K(\alpha) = K[\alpha]$.*

3. *Jedes Element $\beta \in K(\alpha)$ lässt sich eindeutig in der Form $\beta = a_0 + a_1\alpha + \cdots + a_{k-1}\alpha^{k-1}$ mit $a_0, \ldots, a_{k-1} \in K$ darstellen.*

4. *Die Elemente $1 = \alpha^0, \alpha = \alpha^1, \alpha^2, \ldots, \alpha^{k-1}$ bilden eine Basis des Vektorraums $K(\alpha)$ über $K$.*

5. *$[K(\alpha) : K] = k$.*

6. *Wenn $\alpha, \beta \in L$ dasselbe Minimalpolynom $m(x)$ über $K$ haben, dann gibt es einen eindeutigen Isomorphismus $\varphi\colon K(\alpha) \to K(\beta)$ mit $\varphi(\alpha) = \beta$ und $\varphi(c) = c$ für alle $c \in K$.*

Für eine spätere Anwendung arbeiten wir auch folgende Variante explizit heraus:

**Proposition 6.1.3.5.** *Sei $\varphi\colon K_1 \to K_2$ Körperisomorphismus, $\varphi_x\colon K_1[x] \to K_2[x]$ der eindeutig bestimmte Isomorphismus, der auf den konstanten Polynomen mit $\varphi$ übereinstimmt und $x \in K_1[x]$ auf $x \in K_2[x]$ abbildet. Weiters seien $K_1 \leq L_1$ und $K_2 \leq L_2$ Körpererweiterungen. Das Element $\alpha_1 \in L_1$ sei algebraisch über $K_1$ mit Minimalpolynom $m_1$, und $\alpha_2 \in L_2$ sei eine Nullstelle von $m_2 := \varphi_x(m_1)$.*
*Dann ist $m_2$ irreduzibel und es gibt einen eindeutigen Isomorphismus $\psi\colon K_1(\alpha_1) \to K_2(\alpha_2)$, der $\varphi$ fortsetzt und $\alpha_1$ auf $\alpha_2$ abbildet.*

*Beweis.* Als Isomorphismus bildet $\varphi_x$ irreduzible Polynome wieder auf irreduzible Polynome ab, insbesondere ist $m_2 = \varphi_x(m_1)$ irreduzibel.
Die Abbildung

$$\psi_0\colon K_1[x]/(m_1) \to K_2[x]/(m_2), \quad f + (m_1) \mapsto \varphi_x(f) + (m_2)$$

ist wohldefiniert und sogar ein Isomorphismus. Zusammensetzung mit den Isomorphismen $\psi_i\colon K_i(\alpha_i) \to K_i[x]/(m_i)$, $i = 1, 2$, wie sie in der ersten Aussage von Satz 6.1.3.4 beschrieben werden, ergibt einen Isomorphismus $\psi := \psi_2^{-1} \circ \psi_0 \circ \psi_1\colon K_1(\alpha_1) \to K_2(\alpha_2)$ mit den behaupteten Eigenschaften, der sogar eindeutig ist, weil seine Werte auf dem Erzeugendensystem $K_1 \cup \{\alpha_1\}$ vorgegeben sind. □

**Beispiele 6.1.3.6.** 1) Für $\alpha \in K$ ist $x - \alpha$ Minimalpolynom von $\alpha$ über $K$.

2) $x^2 - 2$ ist Minimalpolynom von $\sqrt{2}$ über $\mathbb{Q}$.

3) $x^3 - 3$ ist Minimalpolynom von $\sqrt[3]{3}$ über $\mathbb{Q}$.

4) $x^2 + 1$ ist Minimalpolynom von $i$ über $\mathbb{R}$ und auch über $\mathbb{Q}$.

5) Sei $\alpha := \frac{\sqrt{2}}{2}(1+i)$. Dann ist $\alpha^2 = i$, $\alpha^4 = -1$. Das Minimalpolynom von $\alpha$ über $\mathbb{R}$ ist $x^2 - \sqrt{2}x + 1$, über $\mathbb{Q}$ ist es $x^4 + 1$.

6) Das Minimalpolynom der Kreiszahl $\pi$ über $\mathbb{Q}(\pi^2)$ ist $x^2 - \pi^2$, über $\mathbb{Q}(\pi)$ ist es $x - \pi$, und über $\mathbb{Q}$ hat $\pi$ kein Minimalpolynom, weil $\pi$ transzendent ist. Analoges gilt für die ebenfalls transzendente Eulersche Zahl $e$. Auf die Beweise für die Transzendenz von $\pi$ und $e$ müssen wir auf zahlentheoretische Lehrveranstaltungen verweisen. Hier würden sie den Rahmen sprengen.

**UE 344 ► Übungsaufgabe 6.1.3.7.** (F) Sei $p$ eine Primzahl. Zeigen Sie, dass das Polynom $q(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ (das man auch als $\frac{x^p-1}{x-1}$ schreiben kann) in $\mathbb{Z}[x]$ irreduzibel ist. **◄ UE 344**
Hinweis: Betrachten Sie stattdessen das Polynom $r(x) = q(x+1)$ und verwenden Sie 5.3.2.7.

**UE 345 ► Übungsaufgabe 6.1.3.8.** (F) Geben Sie ein irreduzibles Polynom $p(x) \in \mathbb{Z}[x]$ vom Grad 6 an, welches die Nullstelle **◄ UE 345**

$$\cos\frac{2\pi}{7} + i\,\sin\frac{2\pi}{7}$$

hat. Finden Sie alle Nullstellen dieses Polynoms. (Hinweis: Siehe Aufgabe 6.1.3.7)

**UE 346 ► Übungsaufgabe 6.1.3.9.** (B) Sei $p \in \mathbb{Z}$ eine Primzahl. Wir betrachten das Polynom $f(x) := x^3 - p$ zunächst über $\mathbb{Q}$. **◄ UE 346**

(1) Geben Sie sämtliche Nullstellen von $f$ in der Form $a + ib$ mit $a, b \in \mathbb{R}$ an und skizzieren Sie diese in der komplexen Zahlenebene.

(2) Zeigen Sie, dass $f$ über $\mathbb{Q}$ (d.h., im Ring $\mathbb{Q}[x]$) irreduzibel ist.

(3) Sei $L$ ein Körper mit $\mathbb{Q} \leq L$ und $\alpha \in L$ mit $\alpha^3 = p$. Zeigen Sie, dass das Polynom $(x^3 - p)/(x - \alpha) = x^2 + \alpha x + \alpha^2$ über $\mathbb{Q}(\alpha)$ irreduzibel ist. (Hinweis: Betrachten Sie zunächst den Fall $\alpha = \sqrt[3]{p} \in \mathbb{R}$ und überlegen Sie dann, dass es genügt, diesen Fall zu betrachten.)

**UE 347 ► Übungsaufgabe 6.1.3.10.** (F) Für $a \in \mathbb{R}$ sei $\varphi_a \colon \mathbb{Z}[x] \to \mathbb{R}$ durch $\varphi_a(p(x)) = p(a)$ definiert. Finden Sie Polynome $p(x)$, $q(x)$, $r(x)$, sodass **◄ UE 347**

- $\ker(\varphi_0) = (p(x))$,
- $\ker(\varphi_1) = (q(x))$,
- $\ker(\varphi_{\sqrt{2}}) = (r(x))$.

### 6.1.4 Algebraische Erweiterungen und endliche Dimension

Inhalt in Kurzfassung: Auf den ersten Blick ist überhaupt nicht klar, dass die Iteration rein algebraischer Körpererweiterungen stets wieder rein algebraische Erweiterungen erzeugt. Verständlich wird dies aber sehr schnell mit Hilfe des Dimensionsarguments, weil nämlich Endlichdimensionalität und Algebraizität sehr eng miteinander zusammenhängen und somit das eine auf das andere zurückgeführt werden kann. Denn die Iteration endlichdimensionaler Erweiterungen ist wegen des Gradsatzes in offensichtlicher Weise wieder endlichdimensional.

Ist wieder $L$ ein Körper, $K \leq L$ ein Unterkörper und $\alpha \in L$ algebraisch über $K$ mit Minimalpolynom $m$ über $K$, so haben wir gesehen, dass der von $K$ und $\alpha$ erzeugte Unterkörper $K(\alpha) = K[\alpha] \leq L$ endliche Dimension $[K(\alpha) : K] = \operatorname{grad}(m)$ über $K$ hat. Es gilt aber auch die Umkehrung im folgenden Sinn: Ist $[L : K] = n < \infty$ und $\alpha \in L$, so muss zwischen den $n + 1$ Elementen $1, \alpha, \alpha^2, \ldots, \alpha^n$ eine lineare Abhängigkeit

$$\sum_{i=0}^{n} a_i \alpha^i = 0$$

mit Koeffizienten $a_i \in K$ bestehen. Also ist $f(\alpha) = 0$ für das Polynom $f(x) := \sum_{i=0}^{n} a_i x^i$ mit $a_i \in K$. Folglich ist $\alpha$ algebraisch über $K$. Also ist jede endlichdimensionale Körpererweiterung $K \leq L$ *algebraisch* im folgenden Sinne:

**Definition 6.1.4.1.** Eine Körpererweiterung $K \leq L$ heißt *algebraisch*, wenn alle $\alpha \in L$ algebraisch über $K$ sind.

Aufgrund des Gradsatzes 6.1.2.2 führt endliche Iteration von endlichdimensionalen Erweiterungen immer wieder nur zu endlichdimensionalen, also algebraischen Erweiterungen. Also lässt sich auch folgern: Endliche Iteration von einfachen algebraischen Erweiterungen führt stets zu algebraischen Erweiterungen. Explizit formuliert: Wenn $\alpha$ algebraisch über $K$ und $\beta$ algebraisch über $K(\alpha)$ ist, dann ist $K \leq K(\alpha, \beta)$ eine algebraische Erweiterung.
Wir fassen zusammen und ergänzen:

**Satz 6.1.4.2.** *Algebraizität und endliche Dimension von Körpererweiterungen hängen zusammen bzw. vererben sich in folgender Weise. Sei dazu $K \leq L$.*

1. *Ist $[L : K] < \infty$, so ist $L$ algebraisch über $K$ (d.h. alle Elemente von $L$ sind algebraisch über $K$).*
2. *Genau dann ist $\alpha \in L$ algebraisch über $K$, wenn $[K(\alpha) : K] < \infty$.*

3. *Sei $K \leq L \leq M$, $L$ algebraisch über $K$ und $M$ algebraisch über $L$, so ist $M$ algebraisch über $K$.*

4. *Die Menge aller über $K$ algebraischen Elemente in $L$ bildet einen Unterkörper von $L$.*

*Beweis.* Die ersten beiden Aussagen haben wir bereits bewiesen.

3. Sei $\alpha \in M$. Dann ist $\alpha$ algebraisch über $L$, also gibt es ein Minimalpolynom von $\alpha$ mit Koeffizienten $\beta_0, \ldots, \beta_n \in L$, die selbst algebraisch über $K$ sind. Also liegt $\alpha$ in einer Erweiterung von $K$, die durch endlich viele einfache algebraische Erweiterungen zustande kommt: nämlich zunächst um $\beta_0$, dann um $\beta_1$, …, um $\beta_n$ und zuletzt um $\alpha$ selbst. Also ist $\alpha$ nach dem obigen algebraisch auch über $K$.

4. Seien $\alpha, \beta \in L$ algebraisch über $K$. Dann liegen $\alpha$ und $\beta$ gemeinsam in der Erweiterung $K(\alpha, \beta)$ von $K$, die durch endlich viele einfache algebraische Erweiterungen zustande kommt: nämlich zuerst um $\alpha$ und dann um $\beta$. Nach dem obigen ist $K \leq K(\alpha, \beta)$ eine algebraische Erweiterung. Somit sind $\alpha + \beta$, $-\alpha$, $\alpha \cdot \beta$ und – wenn $\alpha$ ungleich 0 ist – $\alpha^{-1}$ als Elemente von $K(\alpha, \beta)$ allesamt algebraisch über $K$. Schließlich sind $0, 1 \in K$ selbstverständlich algebraisch über $K$.

□

**UE 348 ▶ Übungsaufgabe 6.1.4.3.** (B) Man gebe das Minimalpolynom von ◀ **UE 348**

1. $\sqrt{2} + \sqrt{3}$,
2. $\sqrt{3} + i$

über $\mathbb{Q}$ an.

**UE 349 ▶ Übungsaufgabe 6.1.4.4.** (B) Man bestimme den Grad von $\mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15})$ über $\mathbb{Q}$. ◀ **UE 349**

**UE 350 ▶ Übungsaufgabe 6.1.4.5.** (F) Seien $\alpha, \beta, \gamma \in \mathbb{C}$ die Nullstellen von $x^3 - 2$. Man bestimme den Grad des Körpers $\mathbb{Q}(\alpha, \beta, \gamma)$ (des Zerfällungskörpers, siehe 6.2.1) über $\mathbb{Q}$. Hinweis: Übungsaufgabe 6.1.3.9. ◀ **UE 350**

**UE 351 ▶ Übungsaufgabe 6.1.4.6.** (E) Eine komplexe Zahl $\alpha$ heißt *ganz algebraisch*, wenn es ein ganzzahliges und monisches (normiertes) Polynom $p(x) = \sum_{i=0}^{n} a_i x^i$ (also mit $a_i \in \mathbb{Z}$ für $i = 0, \ldots, n$ und mit $a_n = 1$) mit $p(\alpha) = 0$ gibt. ◀ **UE 351**

(1) Zeigen Sie, dass $\alpha := \frac{1}{2}(1 + \sqrt{5})$ ganz algebraisch ist.

(2) Zeigen Sie, dass eine rationale Zahl genau dann ganz algebraisch ist, wenn sie in $\mathbb{Z}$ liegt. Folgern Sie daraus, dass für $m, n \in \mathbb{N}^+$ die Wurzel $\sqrt[n]{m}$ entweder ganz oder irrational ist.

**Anmerkung 6.1.4.7.** Man kann zeigen, dass die Menge der ganzen algebraischen Zahlen einen Unterring von $\mathbb{C}$ bilden, siehe *Algebra II*. Die Methode ähnelt dem Beweis, dass die algebraischen Zahlen einen Körper bilden (siehe Satz 6.1.4.2), wobei die Rolle der endlichen Dimension von Körpererweiterungen übernommen wird von der endlichen Erzeugtheit von Moduln.

Nachdem wir uns mit algebraischen Körpererweiterungen einigermaßen vertraut gemacht haben, wenden wir uns nun den transzendenten zu.

### 6.1.5 Transzendente Körpererweiterungen

Inhalt in Kurzfassung: Rein transzendente Körpererweiterungen $E$ eines Grundkörpers $K$ lassen sich (bis auf Isomorphie) recht klar beschreiben, nämlich als Körper gebrochen rationaler Funktionen $K(X)$ in einer geeigneten Menge $X$ von Variablen. Aber auch beliebige Körpererweiterungen werden dadurch zugänglich. Und zwar lassen sie sich beschreiben als Iteration einer vorangehenden rein transzendenten Körpererweiterung, gefolgt von einer rein algebraischen Erweiterung. Dabei geht es lediglich darum, eine sogenannte Transzendenzbasis, d.h. eine maximale algebraisch unabhängigen Menge zu finden. Das gelingt ganz ähnlich (z.B. mit Hilfe des Lemmas von Zorn) wie bei dem Satz aus der Linearen Algebra, dass sich linear unabhängige Mengen in Vektorräumen zu Basen ergänzen lassen. Es gilt auch ein Analogon zum Austauschsatz von Steinitz, wonach (hier für den endlichen Fall bewiesen) je zwei Transzendenzbasen gleich viele Elemente haben, weshalb der Begriff des Transzendenzgrades einer Körpererweiterung wohldefiniert ist.

Die folgenden Begriffsbildungen lassen sich am besten in weitgehender Analogie zu den Konzepten rund um lineare (Un-)Abhängigkeit, siehe 1.3.3, verstehen.

**Definition 6.1.5.1.** Ist $K \leq E$ eine Körpererweiterung, so heißt eine Menge $S \subseteq E$ *algebraisch abhängig* über $K$, falls es ein positives $n \in \mathbb{N}$, ein $f \in K[x_1, \ldots, x_n] \setminus \{0\}$ und paarweise verschiedene $s_1, \ldots, s_n \in S$ gibt mit $f(s_1, \ldots, s_n) = 0$. Andernfalls heißt $S$ *algebraisch unabhängig*.
Ist $E = K(S)$ mit einer algebraisch unabhängigen Menge $S$, so heißt $E : K$ eine *rein transzendente Erweiterung*.
Eine Menge $S \subseteq E$ heißt *Transzendenzbasis* von $E$ über $K$, falls $S$ algebraisch unabhängig und mit dieser Eigenschaft maximal ist.

Nicht schwer ist der Beweis folgender Tatsache:

**Proposition 6.1.5.2.** *Seien $L_1$ und $L_2$ Erweiterungskörper von $K$, und seien $S_1 \subseteq L_1$ und $S_2 \subseteq L_2$ jeweils algebraisch unabhängig über $K$. Gilt überdies $|S_1| = |S_2|$ vermittels einer Bijektion $\varphi : S_1 \to S_2$, dann folgt $K(S_1) \cong K(S_2)$ vermittels eines Isomorphismus, der sowohl die Identität auf $K$ als auch $\varphi$ fortsetzt.*

**UE 352** ► **Übungsaufgabe 6.1.5.3.** (V) Beweisen Sie Proposition 6.1.5.2. ◄ **UE 352**

**Lemma 6.1.5.4.** *Sei $K \leq E$ eine Körpererweiterung, und $S \subseteq E$. Dann sind die folgenden Aussagen äquivalent:*

(1) *$S$ ist maximale algebraisch unabhängige Teilmenge.*

(2) *$E$ ist algebraisch über $K(S)$ und $S$ ist minimal (bezüglich $\subseteq$) mit dieser Eigenschaft.*

(3) *$S$ ist algebraisch unabhängig und $E$ ist algebraisch über $K(S)$.*

**UE 353** ► **Übungsaufgabe 6.1.5.5.** (F) Beweisen Sie Lemma 6.1.5.4. ◄ **UE 353**

**Satz 6.1.5.6.** *Für jede Körpererweiterung $K \leq E$ existiert eine Transzendenzbasis $S \subseteq K$. Folglich lässt sich $K \leq E$ als rein transzendente Erweiterung $K \leq K(S)$, gefolgt von der algebraischen Erweiterung $K(S) \leq E$ auffassen.*

*Beweis.* Analog zum Beweis der Existenz einer Basis in Vektorräumen: Das System aller algebraisch unabhängigen Teilmengen bildet eine $\subseteq$-Halbordnung und ist abgeschlossen bezüglich der Vereinigung von Ketten. Nach dem Lemma von Zorn (11.3.2) gibt es daher ein maximales Element.[3] Jedes solche maximale Element ist eine Transzendenzbasis. Damit ist die erste Behauptung bewiesen. Die zweite folgt daraus in offensichtlicher Weise. □

Klarerweise ist eine Transzendenzbasis $S$ genau dann leer, wenn $K \leq E$ algebraisch ist. Wir modifizieren nun die Sätze und Beweise über Basen und die Dimension eines Vektorraums aus Abschnitt 1.3.2 so, dass wir analoge Sätze über Transzendenzbasen und den Transzendenzgrad bekommen.

**Definition 6.1.5.7.** Für jede Körpererweiterung $K \leq E$ und jede Teilmenge $A \subseteq E$ schreiben wir $[A]$ für die *algebraische Hülle* von $A$ über $K$, das heißt: für die Menge aller Elemente $e \in E$, die über $K(A)$ algebraisch sind.
Wenn $E = [K(A)]$ ist, d.h. wenn $E$ algebraisch über $K(A)$ ist, dann nennen wir $A$ ein *algebraisches Erzeugendensystem* für $E$ über $K$.

Ähnlich wie im Fall der linearen Hülle gilt $[[A]] = [A]$ für alle $A$ (siehe Satz 6.1.4.2).

**Lemma 6.1.5.8** (Algebraisches Austauschlemma)**.** *Sei $K \leq E$ Körpererweiterung, $A \subseteq E$, $b, c \in E$. Wenn $c \in [A \cup \{b\}]$ aber $c \notin [A]$ gilt, dann ist $b \in [A \cup \{c\}]$.*

*Beweis.* Sei $f(x)$ ein Polynom in $K(A \cup \{b\})[x] \setminus \{0\}$ mit $f(c) = 0$. Nach Multiplikation mit einem geeigneten Element von $K[A \cup \{b\}]$ (gemeinsamer Nenner der Koeffizienten) erhalten wir ein Polynom $g(x) \in K[A \cup \{b\}][x] \setminus \{0\}$ mit Nullstelle $c$. Man findet ein Polynom $\tilde{g}(x, y) \in K[A][x, y] \setminus \{0\}$ mit $\tilde{g}(x, b) = g(x)$, also $\tilde{g}(c, b) = 0$. Das Polynom

[3] Alternativ: Das System aller algebraisch unabhängigen Teilmengen hat offensichtlich endlichen Charakter, daher nach dem Lemma von Teichmüller-Tukey (11.3.2.5) ein maximales Element.

$\tilde{g}(x,y)$, aufgefasst als Element des Polynomrings $K[x][y]$ über dem Ring $K[x]$, hat (in Bezug auf $y$) mindestens Grad 1 (denn sonst wäre $\tilde{g}(x,b)$ ein Polynom über $K[A]$ mit $\tilde{g}(c,b)=0$, also $c \in [A]$).
Daher ist $\hat{g}(y) := \tilde{g}(c,y)$ ein nichtkonstantes Polynom über $K[A \cup \{c\}]$ mit Nullstelle $b$. □

**Korollar 6.1.5.9.** Wenn $K \leq E$, $A$, $b$, $c$ die Voraussetzungen des algebraischen Austauschlemmas erfüllen, dann gilt $[A \cup \{b\}] = [A \cup \{c\}]$.
Wenn $A$ überdies algebraisch unabhängig war, dann sind auch $A \cup \{b\}$ und $A \cup \{c\}$ algebraisch unabhängig.

**Korollar 6.1.5.10.** Wenn $B$ und $C$ Transzendenzbasen für $K \leq E$ sind, dann gibt es für jedes $b \in B$ ein $c \in C$, sodass $(B \setminus \{b\}) \cup \{c\}$ wiederum eine Transzendenzbasis ist.

*Beweis.* Sei $b \in B$. Die Annahme $C \subseteq [B \setminus \{b\}]$ führt via $V = [C] \subseteq [[B \setminus \{b\}]] = [B \setminus \{b\}]$ zu einem Widerspruch, daher gibt es ein $c \in C$ mit $c \notin [B \setminus \{b\}]$. Nach dem algebraischen Austauschlemma gilt $b \in [(B \setminus \{b\}) \cup \{c\}]$. Daher ist $(B \setminus \{b\}) \cup \{c\}$ ein algebraisches Erzeugendensystem, und nach Korollar 6.1.5.9 sogar eine Transzendenzbasis. □

**Lemma 6.1.5.11.** *Sei $K \leq E$ Körpererweiterung, und sei $B \subseteq E$ eine endliche Transzendenzbasis von $E$ über $K$. Dann gilt: Für jede Transzendenzbasis $C$ von $E$ gilt $|B| = |C|$, also: alle Transzendenzbasen von $E$ haben die gleiche (endliche) Kardinalität.*

*Beweis.* Sei $C_0 := C$. Wenn $B \neq C_0$ ist, sei $c \in C_0 \setminus B$ beliebig. (So ein $c$ gibt es, sonst wäre $C_0 \subsetneq B$, was für Transzendenzbasen unmöglich ist.)
Nach Korollar 6.1.5.10 (mit vertauschten Rollen von $B$ und $C$) existiert $b \in B$, sodass $C_1 := (C_0 \setminus \{c\}) \cup \{b\}$ noch immer eine Transzendenzbasis ist, wobei $|C_0| = |C_1|$. Wir wissen $b \notin C_0$, denn sonst wäre ja $C_0 \setminus \{c\}$ eine Transzendenzbasis; weil $b$ ein neues Element von $B \cap C_1$ ist, gilt $|B \cap C_1| = |B \cap C_0| + 1$. Mit Induktion finden wir weitere Transzendenzbasen $C_2, C_3, \ldots$ die alle gleich groß sind, aber immer größeren Schnitt mit $B$ haben. Nach höchstens $|B|$ Schritten müssen wir eine Transzendenzbasis $C_k$ erhalten, für die $C_k = B$ gilt. Wegen $|C_0| = |C_1| = \cdots = |C_k|$ erhalten wir $|C| = |B|$. □

Für *unendliche* Transzendenzbasen gilt ein analoger Satz, allerdings mit einem anderen Beweis:

**Lemma 6.1.5.12.** *Sei $K \leq E$ Körpererweiterung, und sei $B \subseteq E$ eine unendliche Transzendenzbasis von $E$ über $K$. Für jede Transzendenzbasis $C$ von $V$ gilt dann $|B| = |C|$, also: alle Transzendenzbasen von $V$ haben die gleiche (unendliche) Kardinalität.*

*Beweis.* So wie sich der Beweis von Lemma 6.1.5.11 durch geringfügige Umformulierungen aus dem Beweis von Lemma 1.3.2.4 ergibt, lässt sich auch der Beweis der aktuellen Aussage aus dem Beweis von Korollar 1.3.3.2 gewinnen. Der entscheidende Punkt ist der Folgende: wenn $c \in [K(B)]$, etwa bezeugt durch ein Polynom $f(x) \in K(B)[x]$, dann gibt es eine endliche Teilmenge $B' \subseteq B$, sodass alle Koeffizienten von $f(x)$ bereits in $K(B')$ liegen. □

Die letzten beiden Lemmata motivieren die folgenden Definition:

**Definition 6.1.5.13.** Die (nach den Lemmata 6.1.5.11 und 6.1.5.12 eindeutig bestimmte) Kardinalität einer Transzendenzbasis von $E$ über $K$ heißt *Transzendenzgrad* von $E$ über $K$.

**Anmerkung 6.1.5.14.** Ist $\alpha$ transzendent über $K$, dann ist der Körpergrad $[K(\alpha) : K]$ unendlich, weil die Potenzen $\alpha^n$ linear unabhängig über $K$ sind.
Wenn $K$ endlich ist, dann ist $K(\alpha)$ abzählbar unendlich und hat daher abzählbar unendliche Dimension über $K$. Wenn $K$ unendlich ist, so kann man in $K(\alpha)$ eine über $K$ linear unabhängige Menge finden, die gleichmächtig zu $K$ ist, zum Beispiel $\{\frac{1}{q-\alpha} \mid q \in K\}$. Also gilt $[K(\alpha) : K] \geq |K|$. Wegen $|K(\alpha)| = |K|$ ist aber auch $[K(\alpha) : K] \leq |K|$, insgesamt also $[K(\alpha) : K] = |K|$ .

### 6.1.6 Anwendung: Konstruierbarkeit mit Zirkel und Lineal

Inhalt in Kurzfassung: Übersetzt man die klassischen geometrischen Konstruktionsaufgaben mittels Zirkel und Lineal in eine algebraische Sprache, so entsprechen sie der Lösung von Gleichungen ersten und zweiten Grades, ausgehend vom Grundkörper $\mathbb{Q}$. Gleichungen ersten Grades haben innerhalb eines Körpers stets eine Lösung, bei zweitem Grad sind in der Regel Quadratwurzeln zu adjungieren, d.h. Körpererweiterungen vom Grad 2 nötig. Durch Iteration entstehen laut Gradsatz Erweiterungen, deren Dimension in jedem Fall von der Form $2^n$ sind. Dies hat beispielsweise zur Folge, dass Konstruktionen dritter Wurzeln wie $\sqrt[3]{2}$ (Diagonale des Würfels vom Volumen 2, Delisches Problem der Würfelverdopplung), sofern sie nicht schon im Grundkörper liegen, ebenso wenig mit Zirkel und Lineal ausgeführt werden können wie die Dreiteilung beliebig vorgegebener Winkel. Auch die Konstruktion regelmäßiger $n$-Ecke mit Zirkel und Lineal wird durch derartige Überlegungen angreifbar, auch wenn für eine endgültige Klassifikation jener $n$, für die das möglich ist, auch noch Galoistheorie erforderlich wird. Weiß man, dass die Kreizahl $\pi$ transzendent ist, folgt auch die Unmöglichkeit der legendären Quadratur des Kreises, d.h. die Konstruktion des Radius eines Kreises mit Einheitsfläche.

**Definition 6.1.6.1.** Sei $A$ eine Menge von Punkten in der Ebene $\mathbb{R} \times \mathbb{R}$, die die Punkte $(0, 0)$ und $(1, 0)$ enthält. Unter einer *Konstruktion (mit Zirkel und Lineal)* aus $A$ verstehen wir eine endliche Folge $(X_1, \ldots, X_n)$, sodass für alle $i = 1, \ldots, n$ gilt:

1. $X_i$ ist entweder ein Punkt, oder eine Gerade, oder ein Kreis in der Ebene, oder eine reelle Zahl.

2. Wenn $X_i$ ein Punkt $p$ ist, dann gilt $p \in A$, oder $p$ wird als Durchschnitt von früheren Kreisen und/oder Geraden erhalten, d.h.: es gibt $j_1, j_2 < i$, sodass $p$ im Durchschnitt von $X_{j_1}$ und $X_{j_2}$ enthalten ist, wobei $X_{j_1}$ und $X_{j_2}$ verschieden[4] sind und $X_{j_1}$ ein Kreis oder eine Gerade ist, ebenso $X_{j_2}$.

[4] Äquivalent: Der Durchschnitt von $X_{j_1}$ und $X_{j_2}$ ist endlich.

3. Wenn $X_i$ eine Gerade $g$ ist, dann geht $g$ durch zwei vorher konstruierte Punkte, d.h.: es gibt $j_1, j_2 < i$, sodass $p_1 = X_{j_1}$ und $p_2 = X_{j_2}$ zwei verschiedene Punkte sind, die beide auf $g$ liegen.

4. Wenn $X_i$ ein Kreis $k$ mit Mittelpunkt $M$ und Radius $r$ ist, dann wurden Mittelpunkt und Radius schon früher konstruiert, d.h.: es gibt $j_1, j_2 < i$, so dass $M = X_{j_1}$ und $r = X_{j_2}$.

5. Wenn $X_i$ eine Zahl $z \in \mathbb{R}$ ist, dann ist $|z|$ die Distanz zwischen zwei früher konstruierten Punkten, d.h.: es gibt $j_1, j_2 < i$ (nicht notwendigerweise verschieden), so dass $p_1 := X_{j_1}$ und $p_2 := X_{j_2}$ Punkte mit Abstand $|z|$ sind.

Wir nennen einen Punkt / eine Gerade / einen Kreis / eine Zahl *konstruierbar (mit Zirkel und Lineal)* aus $A$, wenn der Punkt / die Gerade / der Kreis / die Zahl in einer Konstruktion aus $A$ vorkommen.
Statt „konstruierbar aus $A$“ schreiben wir oft einfach „konstruierbar“, wenn sich die Menge $A$ aus dem Kontext ergibt. Insbesondere werden wir im folgenden oft Konstruierbarkeit aus der Menge $A = \{(0,0),(1,0)\}$ betrachten.

**UE 354** ▶ **Übungsaufgabe 6.1.6.2.** (V) Wenn die Gerade $g$ und der Punkt $P$ aus $A$ konstruierbar sind, dann sind sowohl die Parallele zu $g$ durch $P$ als auch die Normale von $P$ auf $g$ aus $A$ konstruierbar. ◀ **UE 354**

**UE 355** ▶ **Übungsaufgabe 6.1.6.3.** (V) Für $a, b \in \mathbb{R}$ sind die folgenden Aussagen äquivalent: ◀ **UE 355**

1. Der Punkt $(a,b) \in \mathbb{R}^2$ ist konstruierbar.

2. Die Punkte $(a,0)$ und $(b,0)$ sind beide konstruierbar.

3. Die Zahlen $a$ und $b$ sind beide konstruierbar.

Um die Koordinaten (oder deren Distanzen) von konstruierbaren Punkten zu berechnen, muss man offensichtlich endlich oft ein Gleichungssystem aus 2 Gleichungen mit 2 Unbekannten lösen, wobei

- entweder beide Gleichungen linear sind
- oder eine Gleichung linear ist, die andere die Form $(x-a)^2 + (y-b)^2 - c^2 = 0$ hat,
- oder beide Gleichungen die obige quadratische Form haben.

In jedem Fall[5] kann man explizite Formeln für die Lösungen angeben, die nur Körperoperationen sowie das Ziehen von Quadratwurzeln verwenden.

[5] Man beachte, dass man aus dem Gleichungssystem $(x-a)^2 + (y-b)^2 = c^2$, $(x-p)^2 + (y-q)^2 = r^2$ durch Substraktion eine lineare Gleichung erhält; indem man diese in eine der quadratischen Gleichungen substituiert, lässt sich die Lösung auf die Lösung einer quadratischen Gleichung mit einer Unbekannten zurückführen.

Umgekehrt kann man (zum Beispiel) den Strahlensatz verwenden, um das Produkt bzw. den Quotienten von zwei bereits konstruierten Zahlen zu erhalten, und den Höhensatz samt Thaleskreis, um aus einer bereits konstruierten positiven Zahl ihre Quadratwurzel zu erhalten:

**UE 356** ► **Übungsaufgabe 6.1.6.4.** (W) Die Menge aller konstruierbaren reellen Zahlen bildet einen Unterkörper von $\mathbb{R}$, der unter Quadratwurzeln abgeschlossen ist. ◄ **UE 356**

Dies legt folgende Definition nahe:

**Definition 6.1.6.5.** Sei $K$ Körper. Unter einer *Quadratwurzelerweiterung* von $K$ verstehen wir einen Erweiterungskörper $L \geq K$, für den es eine endliche Folge $K = K_1 \leq K_2 \leq \cdots \leq K_n = L$ von Körpererweiterungen und $\alpha_i \in K_{i+1}$ gibt, so dass $K_{i+1} = K_i(\alpha_i)$ und $\alpha_i^2 \in K_i$ ist.

**Lemma 6.1.6.6.** *Sei $L$ Quadratwurzelerweiterung von $K$. Dann gibt es eine natürliche Zahl $n$ mit $[L : K] = 2^n$.*

*Beweis.* Als Dimension $[K_{i+1} : K_i]$ jeder einzelnen Körpererweiterung kommt nur 1 oder 2 in Frage. Nach dem Gradsatz multiplizieren sich diese Dimensionen auf. □

Daraus erhält man recht schnell zusammenfassend:

**Satz 6.1.6.7.** *Sei $A$ eine Menge von Punkten, die den Ursprung $(0, 0)$ und den Punkt $(1, 0)$ enthält. Dann gilt:*

1. *Ein Punkt $p$ ist genau dann aus $A$ konstruierbar, wenn seine beiden Koordinaten aus $A$ konstruierbar sind.*
2. *Die Menge der aus $A$ konstruierbaren reellen[6] Zahlen bilden einen Körper $K_A$, der unter Quadratwurzelziehen abgeschlossen ist, d.h.:*

$$\forall \alpha \in K_A : \alpha > 0 \Rightarrow \exists \beta \in K_A : \beta^2 = \alpha.$$

3. *Sei $B$ die Menge aller Koordinaten von Punkten in $A$. Dann ist $z \in \mathbb{R}$ genau dann aus $A$ konstruierbar, wenn $z$ in einer Quadratwurzelerweiterung von $\mathbb{Q}(B)$ liegt.*

**UE 357** ► **Übungsaufgabe 6.1.6.8.** (V) Beweisen Sie Satz 6.1.6.7. ◄ **UE 357**

**Folgerung 6.1.6.9.** *Sei $A$ eine Menge von Punkten mit rationalen Koordinaten. Dann gilt:*

1. *$\sqrt[3]{2}$ ist nicht aus $A$ konstruierbar.*

[6] Man könnte auch für *komplexe* Zahlen den Begriff der Konstruierbarkeit einführen, z.B. indem man definiert, dass $z \in \mathbb{C}$ genau dann konstruierbar ist, wenn sowohl Real- als auch Imaginärteil von $z$ konstruierbar sind; die hier angeführten Sätze lassen sich leicht auf komplexe Zahlen übertragen.

2. *Keine transzendente Zahl (wie etwa $\pi$) ist aus $A$ konstruierbar.*

3. *Eine Dreiteilung des Winkels $60°$ ist unmöglich, genauer: Die Eckpunkte eines Dreiecks mit den Winkeln $90°$, $70°$, $20°$ sind nicht alle aus $A$ konstruierbar.*

*Beweis.* 1. Sei $L$ eine Quadratwurzelerweiterung von $\mathbb{Q}$ mit $\sqrt[3]{2} \in L$. Dann ist $[L : \mathbb{Q}] = 2^n$ für eine natürliche Zahl $n$; nach dem Gradsatz muss nun $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ ein Teiler von $2^n$ sein, was unmöglich ist.

2. Klar.

3. Wenn so ein Dreieck konstruierbar wäre, könnte man auch so ein Dreieck mit Hypotenuse der Länge 1 konstruieren und hätte somit die Zahl $\alpha := \cos(20°)$ konstruiert.

   Aus $\cos(60°) + i\sin(60°) = (\cos(20°) + i\sin(20°))^3$ erhält man aus dem Vergleich der Realteile unter Verwendung von $\sin^2 = 1 - \cos^2$ die Beziehung $\frac{1}{2} = \cos(60°) = 4\sin^3(20°) - 3\sin(20°)$. Daher ist $\alpha$ Nullstelle des Polynoms $4x^3 - 3x - \frac{1}{2}$ bzw., gleichbedeutend, des ganzzahligen Polynoms $f(x) := 8x^3 - 6x - 1$. Wegen 5.3.2.9 kommen als rationale Nullstellen $\alpha$ von $f$ nur die Möglichkeiten $\alpha = \pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}$ in Frage. Einsetzen dieser acht Werte liefert aber stets $f(\alpha) \neq 0$. Also hat dieses Polynom keine rationalen Nullstellen. Als Polynom vom Grad 3 ohne rationale Nullstellen muss $f$ sogar irreduzibel über $\mathbb{Q}$ sein (Proposition 5.3.3.7). Für eine (notwendig irrationale) Nullstelle $\alpha$ von $f$ ist somit $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Wie in 1. folgt nun, dass $\alpha$ nicht aus $A$ konstruierbar ist. □

Weitere prominente Beispiele in diesem Zusammenhang sind die regelmäßigen $n$-Ecke (auf dem Einheitskreis). Elementare Konstruktionen mit Zirkel und Lineal sind bis $n = 6$ möglich, nicht jedoch für $n = 7$, dann wieder für $n = 8, 10, 12$ etc. Gauß konnte beweisen, dass das regelmäßige $n$-Eck sicher dann konstruiert werden kann, wenn $n = 2^k p_1 \dots p_n$ mit $k \in \mathbb{N}$ und paarweise verschiedenen sogenannten *Fermatschen Primzahlen* $p_1, \dots, p_n$. Dabei heißt eine Primzahl $p$ eine Fermatsche Primzahl, wenn sie von der Form $p = 2^{2^e} + 1 =: F_e$ mit $e \in \mathbb{N}$ ist. (Man beachte, dass für solche $n$ die Eulersche $\varphi$-Funktion als Wert $\varphi(n)$ eine Potenz von 2 annimmt.) Allerdings sind bisher nur die Zahlen $F_e$ für $e = 0, 1, 2, 3, 4$, also $p = 3, 5, 17, 257, 65537$ als Primzahlen ausgewiesen. Die Zahl $F_5 = 4294967297$ ist, wie Euler entdeckte, durch 641 teilbar. Weil Primzahlen immer seltener[7] und die Fermatschen Zahlen $F_e$ mit wachsendem $e$ extrem schnell riesengroß werden, vermutet man, dass es außer den genannten keine weiteren Fermatschen Primzahlen gibt. Dem Franzosen Pierre-Laurent Wantzel (1814-1848) gelang der Nachweis, dass außer den von Gauß angegebenen keine weiteren regelmäßigen $n$-Ecke mit Zirkel und Lineal konstruiert werden können. Das auszuführen übersteigt an dieser Stelle aber unsere Möglichkeiten.

[7] Der erstmals 1793 vom damals erst 16-jährigen Gauß und 1798 von Legendre vermutete, aber erst 1896 von den beiden Franzosen Hadamard und de la Vallée Poussin unabhängig voneinander bewiesene Primzahlsatz besagt, dass für die Anzahl $\pi(x)$ der Primzahlen $p \leq x$ die asymptotische Formel $\pi(x) \sim \frac{x}{\ln x}$ gilt. Ein Vergleich diese Häufigkeitsaussage mit der Seltenheit Fermatscher Zahlen kann als Indiz dafür angesehen werden, dass es gar keine weiteren Fermatschen Primzahlen gibt.

**UE 358** ► **Übungsaufgabe 6.1.6.10.** (D) Versuchen Sie wenigsten gewisse der oben aufgestellten Behauptungen im Zusammenhang mit dem regelmäßigen $n$-Eck zu beweisen. ◄ **UE 358**

## 6.2 Adjunktion von Nullstellen von Polynomen

Im vorigen Abschnitt haben wir die Situation studiert, dass zwei Körper bereits vorliegen, von denen einer, der Grund- oder Unterkörper $K$, im anderen, dem Erweiterungs- oder Oberkörper $L$, enthalten ist. Für Elemente $\alpha \in L$ war vor allem von Interesse, ob es ein Polynom $f \in K[x]$, $f \neq 0$, mit $f(\alpha) = 0$ gibt, also ob $\alpha$ algebraisch oder transzendent über $K$ ist. Nun gehen wir umgekehrt vor, indem wir uns neben $K$ ein $f \in K[x]$ vorgeben, das in $K$ eventuell keine Nullstelle hat. Wir suchen nach einer Erweiterung $L$ von $K$ mit einer oder mehreren Lösungen $\alpha$ der Gleichung $f(x) = 0$. In einem weiteren Schritt sucht man Erweiterungen für nicht nur ein solches $f$, sondern für beliebige Teilmengen von $K[x]$. Es zeigt sich, dass solche Erweiterungen in Form von Nullstellen- bzw. Zerfällungskörpern stets existieren.
Man beachte die Analogie zu den Zahlenbereichserweiterungen von $\mathbb{N}$ zu $\mathbb{Z}$ und $\mathbb{Q}$ sowie von $\mathbb{R}$ zu $\mathbb{C}$, die auch durch die Lösung von Gleichungen motiviert waren. Gleichungen der Form $a + x = b$ machen, sofern $a > b$, die Erweiterung von $\mathbb{N}$ zu $\mathbb{Z}$ erforderlich, Gleichungen der Form $ax = b$, sofern $a$ kein Teiler von $b$ ist, die von $\mathbb{Z}$ zu $\mathbb{Q}$. Die sehr spezielle Gleichung $f(x) := x^2 + 1 = 0$ führt von $\mathbb{R}$ zu $\mathbb{C}$. Letzteres soll in diesem Abschnitt auf beliebige Polynome $f$ über irgendeinem Körper $K$ (statt $\mathbb{R}$) verallgemeinert werden.
Der Überblick über den Abschnitt: In 6.2.1 behandeln wir den entscheidenden Schritt der Adjunktion einer Nullstelle eines gegebenen irreduziblen Polynoms. Iteriert man diesen Schritt geeignet (nötigenfalls auch unendlich oft), so erhält man den Zerfällungskörper einer beliebigen Menge von Polynomen. Nimmt man die Menge aller Polynome über dem Ausgangskörper, so landet man beim algebraischen Abschluss des Ausgangskörpers (6.2.2). In 6.2.3 ergibt sich die Eindeutigkeit des Zerfällungskörpers (bis auf Isomorphie bzw. sogar Äquivalenz). Die Frage, wann Polynome in ihrem Zerfällungskörper mehrfache Nullstellen haben können, lässt sich mit Hilfe einer formalen Ableitung erfolgreich untersuchen (6.2.4). Reizvoll ist auch die Untersuchung von Einheitswurzeln und Kreisteilungspolynomen (6.2.5). Den Abschnitt schließen zwei Ergebnisse ab, nach denen gewisse Körpererweiterungen (eine algebraische und eine transzendente) von einem einzigen geeigneten Element erzeugt werden (6.2.6).

### 6.2.1 Adjunktion einer Nullstelle

Inhalt in Kurzfassung: Die Erkenntnisse aus dem vorangegangenen Abschnitt über algebraische Körpererweiterungen werden nun verwendet, um den umgekehrten Weg zu beschreiten. Zu gegebenem Körper $K$ und Polynom $f \in K[x]$ ist ein Erweiterungskörper $E$ von $K$ gesucht, der eine Nullstelle von $f$ enthält. Ist $f$ irreduzibel (andernfalls ist $f$ durch einen irreduziblen Faktor zu ersetzen), so gelingt dies mit $E := K[x]/(f)$, der Faktorisierung des Polynomrings nach dem von $f$ erzeugten Hauptideal (Satz von

Kronecker).

Wir gehen also aus vom Beispiel der Adjunktion der imaginären Einheit $i$ zu $\mathbb{R}$, wodurch $\mathbb{C}$ entsteht. Wegen $i^2 = -1$ ist $i$ Nullstelle des Polynoms $f(x) = x^2 + 1$, das in $\mathbb{R}$ bekanntlich keine Nullstelle hat. Durch diese Eigenschaft ist das Rechnen in $\mathbb{C}$ eindeutig festgelegt. Ganz Ähnliches gilt, wenn wir von einer Nullstelle $\alpha$ eines beliebigen irreduziblen Polynoms $f \in K[x]$ über irgendeinem Körper $K$ ausgehen. OBdA dürfen wir annehmen, dass $f$ monisch ist, also $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ mit $a_i \in K$. Dann gilt $\alpha^n = -a_{n-1}\alpha^{n-1} - \ldots - a_1\alpha - a_0$, wodurch iterativ auch noch höhere Potenzen von $\alpha$ als Linearkombinationen von $1 = \alpha^0, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ ausgedrückt werden können, zum Beispiel

$$\begin{aligned}\alpha^{n+1} &= \alpha \cdot \alpha^n = -a_{n-1}\alpha^n - \ldots - a_1\alpha^2 - a_0\alpha \\ &= -a_{n-1}(-a_{n-1}\alpha^{n-1} - \ldots - a_1\alpha - a_0) - a_{n-2}\alpha^{n-1} \ldots - a_1\alpha^2 - a_0\alpha\end{aligned}$$

Es zeigt sich, dass all diese Ausdrücke bereits einen Körper bilden. Etwas präziser formuliert lässt sich diese Konstruktion wie folgt fassen:

**Proposition 6.2.1.1** (*Satz von Kronecker*)**.** *Sei $f \in K[x]$ irreduzibel. Dann ist der Faktorring $L := K[x]/(f)$ des Polynomrings $K[x]$ nach dem von $f$ erzeugten Hauptideal $(f)$ ein Körper. Die Abbildung $\iota\colon K \to L = K[x]/(f)$, $k \mapsto k + (f)$, ist eine isomorphe Einbettung. Die eindeutige homomorphe Fortsetzung $\bar{\iota}\colon K[x] \to L[x]$ von $\iota$ auf $K[x]$ mit $\bar{\iota} : x \mapsto x$ ist gleichfalls eine isomorphe Einbettung, und zwar des Polynomrings über $K$ in den über $L$. Das Element $x + (f) \in K[x]/(f) = L$ ist Nullstelle von $\bar{f} := \bar{\iota}(f) \in L[x]$. Identifizieren wir $K$ und $\iota(K)$ vermittels $\iota$ sowie $K[x]$ und $\bar{\iota}(K[x]) \leq L[x]$ vermittels $\bar{\iota}$, so ist mit $L$ also eine Erweiterung von $K$ mit einer Nullstelle von $f$ gefunden. Die Dimension $[L : K]$ stimmt mit dem Grad* $\operatorname{grad}(f)$ *überein. Als endlichdimensionale Erweiterung ist $L$ also insbesondere algebraisch über $K$.*

*Beweis.* Weil $f \in K[x]$ irreduzibel und $K[x]$ ein Hauptidealring ist, ist das von $f$ erzeugte Ideal $(f)$ maximal wegen Proposition 5.1.4.1 und $L = K[x]/(f)$ tatsächlich ein Körper (siehe Satz 3.4.2.4). Klarerweise ist $\iota$ injektiv und ein Homomorphismus, also eine isomorphe Einbettung. Die einzige homomorphe Fortsetzung $\bar{\iota}$ ist

$$\bar{\iota} : \sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} \iota(a_i) x^i,$$

offenbar ebenfalls eine isomorphe Einbettung $\bar{\iota}\colon K[x] \to L[x]$. Aufgrund der Rechenregeln für Nebenklassen von Idealen in Faktorringen gilt:

$$(\bar{\iota}(f))(\bar{\iota}(x)) = \bar{f}(x + (f)) = f(x) + (f) = (f) = 0_{K[x]/(f)} = 0_L.$$

Also ist die Behauptung betreffend die Nullstelle im Erweiterungskörper bewiesen. Jene betreffend die Dimension der Körpererweiterung ergibt sich aus Satz 6.1.3.4, da $\bar{\iota}(f)$ (bzw. nach Identifikation $f$) das Minimalpolynom von $\bar{\iota}(x)$ ist. □

Den in Proposition 6.2.1.1 beschriebenen Erweiterungsprozess von $K$ nennt man auch *Adjunktion einer Nullstelle* des irreduziblen Polynoms $f$. Durch iterierte Adjunktion von Nullstellen irreduzibler Polynome kann man sogenannte Zerfällungskörper von Polynomen oder, nach eventuell transfiniter Fortsetzung, von beliebigen Polynommengen $P \subseteq K[x]$ konstruieren. Dem wollen wir uns nun zuwenden.

### 6.2.2 Die Konstruktion von Zerfällungskörpern und algebraischem Abschluss

Inhalt in Kurzfassung: Durch Iteration der Konstruktion aus 6.2.1 lässt sich zu vorgegebenem $f \in K[x]$ eine Erweiterung $E$ von $K$ konstruieren, in der $f$ nicht nur eine Nullstelle hat, sondern sogar in Linearfaktoren zerfällt. Eine minimale Erweiterung mit dieser Eigenschaft heißt Zerfällungskörper. Offenbar ist damit auch die Verallgemeinerung zunächst auf endlich viele Polynome $f_1, \ldots, f_n$ möglich, sodann, bei transfiniter Fortsetzung des Erweiterungsprozesses, auf eine beliebige Teilmenge von $K[x]$. Im Extremfall kann man auch die gesamte Menge $K[x]$ wählen. Der resultierende Zerfällungskörper $Z$ erweist sich sogar als algebraisch abgeschlossen, enthält also nicht nur sämtliche Nullstellen aller Polynome aus $K[x]$ sondern sogar aller Polynome aus $Z[x]$. Man spricht auch von einem algebraischen Abschluss von $K$.

Zu Beginn dieses Unterabschnitts definieren wir die zentralen Begriffe:

**Definition 6.2.2.1.** Sei $K \leq E$ eine Körpererweiterung und $P \subseteq K[x]$ eine Menge von Polynomen. Zerfällt jedes $f \in P$ über $E$ in Linearfaktoren, so heißt $E$ ein *Nullstellenkörper* von $P$. Ist überdies $E$ minimal mit dieser Eigenschaft (d.h. dass $E$ von $K$ und sämtlichen Nullstellen aller $f \in P$ erzeugt wird), so heißt $E$ ein *Zerfällungskörper* von $P$. Ist $P = \{f\}$ einelementig, so heißt $E$ auch Nullstellen- bzw. Zerfällungskörper von $f$. Unter einem *algebraischen Abschluss* von $K$ versteht man einen Zerfällungskörper von $P := K[x]$. Der Körper $K$ heißt *algebraisch abgeschlossen*, wenn $K$ ein algebraischer Abschluss von sich selbst ist.

Einfach einzusehen sind folgende Äquivalenzen für einen Körper $K$:

**Proposition 6.2.2.2.** *Für einen Körper $K$ sind die folgenden Aussagen äquivalent:*

(1) *Jedes nichtkonstante Polynom $p(x) \in K[x]$ hat eine Nullstelle in $K$.*
(2) *Jedes nichtkonstante irreduzible Polynom $p(x) \in K[x]$ hat eine Nullstelle in $K$.*
(3) *Jedes nichtkonstante irreduzible Polynom $p(x) \in K[x]$ hat Grad 1.*
(4) *Jedes nichtkonstante Polynom $p(x) \in K[x]$ zerfällt in Linearfaktoren. (Mit anderen Worten: $K$ ist Nullstellenkörper von $K[x]$.)*
(5) *Für jede algebraische Erweiterung $L \geq K$ gilt $L = K$.*

**UE 359 ► Übungsaufgabe 6.2.2.3.** (F) Beweisen Sie Proposition 6.2.2.2. **◄ UE 359**

Von ähnlichem Charakter sind die folgenden Äquivalenzen für Körpererweiterungen:

**Proposition 6.2.2.4.** *Für eine Körpererweiterung $K \leq L$ sind die folgenden Aussagen äquivalent:*

(1) *$L$ ist ein algebraischer Abschluss von $K$, d.h. ein Zerfällungskörper von $K[x]$ über $K$.*

(2) *$L$ ist Nullstellenkörper von $K[x]$ und $L$ ist algebraisch über $K$ (d.h., jedes Element von $L$ ist algebraisch über $K$).*

(3) *$L$ ist algebraisch über $K$ und für alle $L' \geq L$ gilt: Wenn $L'$ algebraisch über $K$ ist, dann ist $L = L'$.*

**UE 360 ▶ Übungsaufgabe 6.2.2.5.** (F) Beweisen Sie Proposition 6.2.2.4. **◀ UE 360**

Wir wollen uns nun an die Konstruktion von Nullstellen- und Zerfällungskörpern machen. Das gelingt mittels iterierter Adjunktion von Nullstellen gemäß 6.2.1, und zwar für eine beliebig vorgegebene Menge $P \subseteq K[x]$ von Polynomen über einem ebenfalls beliebigen Körper $K$. Insbesondere erhält man so auch einen algebraischen Abschluss von $K$. Nützlich sind dabei die folgende Abschätzung der Kardinalität algebraischer Erweiterungen sowie die daran anschließenden Überlegungen. (Man beachte die Ähnlichkeit zu Überlegungen bei der Konstruktion freier Algebren in 4.1.6.)

**Proposition 6.2.2.6.** *Sei $L$ eine algebraische Körpererweiterung von $K$. Dann gilt $|L| \leq \max\{|K|, |\mathbb{N}|\}$.*

*Beweis.* Für jedes $f \in K[x] \setminus \{0\}$ sei $N_f$ die (endliche) Menge der Nullstellen von $f$ in $L$. Weil $L$ algebraisch über $K$ ist, folgt

$$L \subseteq \bigcup_{f \in K[x] \setminus \{0\}} N_f.$$

Zu jedem Grad $n$ gibt es $|K^{n+1}| = |K|^{n+1}$ Polynome vom Grad $\leq n$. Ist $K$ endlich, so sind das für jedes $n$ endlich viele, insgesamt also abzählbar unendlich viele, womit auch $L$ abzählbar ist.
Ist $K$ hingegen unendlich, so ist $|K|^{n+1} = |K|$ (siehe 11.4.8.6 im Anhang). Zu jedem Grad $n \in \mathbb{N}$ gibt es also nicht mehr Polynome als $|K|$, somit auch $|K[x]| \leq |\mathbb{N}| \cdot |K| = |K|$ (nochmals 11.4.8.6) und analog weiterschließend $|L| \leq |K|$. Damit ist die Behauptung sowohl für endliches als auch für unendliches $K$ bewiesen. □

Für die Konstruktion benötigen wir die folgende Begriffsbildung, die auch im nächsten Unterabschnitt zur Eindeutigkeit des Zerfällungskörpers eine tragende Rolle spielen wird.

**Definition 6.2.2.7.** Seien $K_1 \leq E_1$ und $K_2 \leq E_2$ Körpererweiterungen und $\varphi : K_1 \to K_2$ ein Isomorphismus. Ein Isomorphismus $\psi : E_1 \to E_2$ heißt *Äquivalenz* und die Erweiterungen $E_1$ und $E_2$ heißen *äquivalent* bezüglich $\varphi$, wenn $\psi$ auf $K_1$ mit $\varphi$ übereinstimmt. Ist $K_1 = K_2 =: K$ und $\varphi$ die Identität auf $K$, so spricht man schlicht von Äquivalenz, auch ohne explizite Bezugnahme auf $\varphi = \mathrm{id}_K$.

**UE 361** ► **Übungsaufgabe 6.2.2.8.** (F) Die Äquivalenz von zwei Körpererweiterungen $K \leq E_1$ und $K \leq E_2$ bezüglich $\varphi = \mathrm{id}_K$ aus Definition 6.2.2.7 kann auch als Äquivalenz im kategorientheoretischen Sinn aufgefasst werden. Wie? ◄ **UE 361**

Ist $X$ nun irgendeine überabzählbare Obermenge von $K$ mit größerer Kardinalität als $|K|$ (zum Beispiel $X := K \cup \mathfrak{P}(K) \cup \mathbb{R}$), so lässt sich jede algebraische Erweiterung $E$ von $K$ bis auf Äquivalenz auf einer Teilmenge von $X$ realisieren, das heißt genauer: Es gibt eine Teilmenge $E' \subseteq X$ mit $K \subseteq E'$ und Operationen $+_{E'}, 0_{E'}, -_{E'}, \cdot_{E'}, 1_{E'}$ auf $E'$, sodass $(E', +_{E'}, 0_{E'}, -_{E'}, \cdot_{E'}, 1_{E'})$ ein Erweiterungskörper von $K$ ist und sodass die Erweiterungen $K \leq E$ und $K \leq E'$ äquivalent sind[8]. Im Beweis des folgenden Satzes wird es daher möglich sein, sich auf solche Erweiterungen von $K$ zu beschränken, deren Trägermenge eine Teilmenge von $X$ ist.

**Satz 6.2.2.9.** *Sei $K$ ein Körper. Dann gibt es für jede Teilmenge $P \subseteq K[x]$ einen Zerfällungskörper $Z_P$. Insbesondere gibt es einen Zerfällungskörper $Z = Z_{K[x]}$ der Menge aller Polynome über $K$. Alle $Z_P$ sind algebraisch über $K$. Der Körper $Z$ ist sogar algebraisch abgeschlossen und somit ein algebraischer Abschluss von $K$. Inbesondere gibt es also zu jedem Körper einen algebraischen Abschluss.*

*Beweis.* Ist $Z$ mit den behaupteten Eigenschaften einmal gefunden, so ist für beliebiges $P \subseteq K[x]$ der Körper $Z_P := K(S) \leq Z$ ein Zerfällungskörper von $P$ und algebraisch über $K$, sofern $S \subseteq Z$ die Menge aller Nullstellen von Polynomen $f \in P$ bezeichnet.
Um $Z$ zu erhalten, betrachten wir für eine (feste) Menge $X$ wie oben (d.h. $X$ sei überabzählbar mit $K \subseteq X$ und $|X| > |K|$) das System[9] $\mathcal{S}$ aller algebraischen Körpererweiterungen $E$ von $K$ mit Trägermenge $\subseteq X$. Dieses System $\mathcal{S}$ ist durch die Relation $\leq$ (Unterkörper) halbgeordnet und nach der Variante von Satz 2.3.4.2 für Körper (und für beliebige Ketten anstatt abzählbare) abgeschlossen bezüglich der Vereinigung von Ketten. Nach dem Lemma von Zorn gibt es daher ein bezüglich $\leq$ maximales Element $E_0 \in \mathcal{S}$. Wir wollen zeigen, dass $E_0$ algebraisch abgeschlossen ist.
Sei also $f \in E_0[x]$ irreduzibel. Nach Proposition 6.2.1.1 gibt es eine algebraische Erweiterung $E_1$ von $E_0$ mit einer Nullstelle $\alpha \in E_1$ von $f$. Der Körper $E_0 \in \mathcal{S}$ ist algebraisch über $K$, folglich (Satz 6.1.4.2) ist $E_1$ algebraisch über $K$. Außerdem können wir wegen der Überlegungen vor diesem Satz annehmen, dass $E_1$ eine Teilmenge von $X$ ist, mit anderen Worten $E_1 \in \mathcal{S}$. Wegen der Maximalität von $E_0$ in $\mathcal{S}$ muss $E_1 = E_0$ gelten,

[8] Man kann $E'$ und die Operationen folgendermaßen erhalten: Wähle zunächst irgendeine Injektion $\psi : E \to X$, die auf $K$ mit $\mathrm{id}_K$ übereinstimmt (insbesondere ist $K$ im Bild von $\psi$ enthalten), setze $E' = \psi(E)$ und definiere die Operationen auf $E'$ so, dass $\psi$ ein Isomorphismus wird, also zum Beispiel $0_{E'} := \psi(0_E) = \psi(0_K) = 0_K$ und $\psi(\alpha) +_{E'} \psi(\beta) := \psi(\alpha + \beta)$.

[9] Das System $\mathcal{S}$ ist tatsächlich eine Menge, weil es aus Elementen einer festen Menge $Y$ besteht: Jedes Element von $\mathcal{S}$ ist ein Tupel $(E, +, 0, -, \cdot, 1)$, wobei $E$ eine Teilmenge von $X$ ist; 0 und 1 Elemente von $E$ sind (insbesondere Elemente von $X$); $-$ eine Funktion $E \to E$ ist, also eine Teilmenge von $E \times E$ (insbesondere eine Teilmenge von $X \times X$); und $+, \cdot$ Funktionen $E \times E \to E$ sind, also analog Teilmengen von $(E \times E) \times E$ (insbesondere Teilmengen von $(X \times X) \times X$). Zusammenfassend kann man also $Y := \mathfrak{P}(X) \times \mathfrak{P}((X \times X) \times X) \times X \times \mathfrak{P}(X \times X) \times \mathfrak{P}((X \times X) \times X) \times X$ setzen. Hätten wir beliebige algebraische Körpererweiterungen von $K$ betrachtet, dann wäre $\mathcal{S}$ (sofern nicht $K$ selbst bereits algebraisch abgeschlossen ist) eine echte Klasse, d.h. keine Menge.

also $\alpha \in E_0$. Somit hat $f$ eine Nullstelle. Nach Proposition 6.2.2.2 ist $E_0$ algebraisch abgeschlossen.
Wegen $K[x] \subseteq E_0[x]$ ist $E_0$ auch Nullstellenkörper von $K[x]$, enthält also einen Zerfällungskörper $Z$ von $K[x]$, nämlich den Durchschnitt aller Unterkörper von $E_0$, die sämtliche Nullstellen von Polynomen $f \in K[x]$ enthalten. Weil $E_0$ über $K$ algebraisch ist und somit jedes $\alpha \in E_0$ Nullstelle eines $f \in K[x]$ ist, folgt $Z = E_0$. □

### 6.2.3 Die Eindeutigkeit von Zerfällungskörpern und algebraischem Abschluss

Inhalt in Kurzfassung: Die Konstruktionen in 6.2.2 haben gezeigt, dass es zu jeder Menge von Polynomen über einem Körper einen Zerfällungskörper gibt. Dieser ist (bis auf Äquivalenz, also erst recht bis auf Isomorphie) sogar eindeutig bestimmt. Das entscheidende technische Hilfsmittel für den Beweis ist ein Fortsetzungssatz für Körperisomorphismen auf entsprechende Zerfällungskörper.

Bei der Konstruktion des Zerfällungskörpers war Proposition 6.2.1.1 das wesentliche technische Instrument. In Satz 6.1.3.4 haben wir aber auch eine Eindeutigkeitsaussage kennen gelernt, nämlich $K(\alpha) \cong K(\beta)$ mit einem Isomorphismus, der $\alpha$ in $\beta$ überführt, sofern $\alpha$ und $\beta$ dasselbe Minimalpolynom haben. Weil die Konstruktion jedes Zerfällungskörpers sich als (eventuell transfinite) Iteration dieses zentralen Konstruktionsschrittes deuten lässt, erwarten wir eine ähnliche Eindeutigkeitsaussage für Zerfällungskörper. Satz 6.2.3.1 wird dieser Erwartung gerecht werden. Dabei wird Definition 6.2.2.7 ihre volle Stärke ausspielen – fasst sie doch die Idee von „isomorphen Körpererweiterungen“. Mit dieser Begriffsbildung lässt sich folgender Satz aussprechen:

**Satz 6.2.3.1.** *Seien $K_1 \cong K_2$ Körper, $\varphi\colon K_1 \to K_2$ ein Isomorphismus und $\varphi_x\colon K_1[x] \to K_2[x]$ jener (eindeutige) Isomorphismus zwischen den Polynomringen, dessen Einschränkung auf die konstanten Polynome mit $\varphi$ übereinstimmt und der das Polynom $x \in K_1[x]$ auf das Polynom $x \in K_2[x]$ abbildet. Seien weiters $P_1 \subseteq K_1[x]$ und $P_2 \subseteq K_2[x]$ Mengen von Polynomen mit $P_2 = \varphi_x(P_1)$, sowie $Z_1 \geq K_1$ und $Z_2 \geq K_2$ Zerfällungskörper von $P_1$ über $K_1$ bzw. von $P_2$ über $K_2$.*
*Dann sind $Z_1$ und $Z_2$* äquivalent *bezüglich $\varphi$. Insbesondere sind je zwei Zerfällungskörper derselben Menge $P$ von Polynomen über einem Körper $K$ äquivalent.*

*Beweis.* Die letzte Aussage ergibt sich unmittelbar aus der allgemeineren ersten, wenn man $K := K_1 = K_2$, $\varphi = \mathrm{id}_K$ und $P = P_1 = P_2$ setzt. Es genügt deshalb, die erste Aussage zu beweisen. Wie bei der Konstruktion des Zerfällungskörpers verwenden wir zur Konstruktion des gesuchten Isomorphismus das Lemma von Zorn. Diesmal betrachten wir das System $\mathcal{S}$ aller Tripel $(E_1, \psi, E_2)$ mit $K_1 \leq E_1 \leq Z_1$, $K_2 \leq E_2 \leq Z_2$ und einem Isomorphismus $\psi\colon E_1 \to E_2$, der $\varphi$ fortsetzt. Die Halbordnungsrelation $\leq$ auf $\mathcal{S}$ sei definiert wir folgt: $(E_1, \psi, E_2) \leq (E_1', \psi', E_2')$ genau dann, wenn $E_1 \leq E_1'$, $E_2 \leq E_2'$ und wenn $\psi'$ auf $E_1$ mit $\psi$ übereinstimmt. Zu jeder $\leq$-Kette von Elementen $(E_1, \psi, E_2) \in \mathcal{S}$ gibt es die obere Schranke $(E_1^*, \psi^*, E_2^*)$, in der jede der drei Komponenten als Vereinigung der entsprechenden Komponenten aus der Kette zustande kommt. Nach dem Lemma von Zorn gibt es folglich ein maximales Element in $\mathcal{S}$, das wir der Einfachheit halber wieder

mit $(E_1, \psi, E_2)$ bezeichnen. Der Satz ist bewiesen, wenn wir $E_1 = Z_1$ und $E_2 = Z_2$ beweisen können. Nehmen wir zunächst indirekt $E_1 \neq Z_1$ an, also $E_1 < Z_1$.
Weil $Z_1$ als Zerfällungskörper von $P_1$ von sämtlichen Nullstellen aller $f \in P_1$ erzeugt wird, muss es eine Nullstelle $\alpha_1 \in Z_1$ eines $f_1 \in P_1$ geben, die nicht in $E_1$ liegt. Sei $m_1$ das Minimalpolynom von $\alpha_1$ über $E_1$. Klarerweise gilt $m_1 | f_1$ in $E_1[x]$. Wie $\varphi\colon K_1 \to K_2$ induziert auch der Isomorphismus $\psi\colon E_1 \to E_2$ einen (eindeutigen) Isomorphismus $\psi_x\colon E_1[x] \to E_2[x]$ der zugehörigen Polynomringe, der auf den konstanten Polynomen mit $\psi$ übereinstimmt und $x \in E_1[x]$ auf $x \in E_2[x]$ abbildet. Somit geht das irreduzible Polynom $m_1$ in ein irreduzibles Polynom $m_2 := \psi_x(m_1)$ über, wobei $m_2 | f_2$ für $f_2 := \psi_x(f_1) = \varphi_x(f_1)$ gilt. Weil $Z_2$ ein Zerfällungskörper von $P_2$ und $f_2 \in P_2$ ist, zerfällt $f_2$ über $Z_2$ in Linearfaktoren, von denen gewisse Teiler von $m_2$ sind. Ein solcher (oBdA normierter) sei $x - \alpha_2$.[10] Also ist $m_2(\alpha_2) = 0$ mit $\alpha_2 \in Z_2$. Laut Proposition 6.1.3.5 lässt sich $\psi\colon E_1 \to E_2$ fortsetzen zu einem Isomorphismus $\psi^*\colon E_1(\alpha_1) \to E_2(\alpha_2)$. Dann wäre aber $(E_1(\alpha_1), \psi^*, E_2(\alpha_2)) \in \mathcal{S}$ echt größer als $(E_1, \psi, E_2)$, was der Maximalität von $(E_1, \psi, E_2)$ in $\mathcal{S}$ widerspräche. Folglich wurde die indirekte Annahme widerlegt, und es gilt $E_1 = Z_1$. Aus Symmetriegründen (Rollen von $E_1$ und $E_2$ vertauschen und $\psi$ durch $\psi^{-1}$ ersetzen) muss dann auch $E_2 = Z_2$ gelten. Damit ist $\psi\colon Z_1 \to Z_2$ tatsächlich der gesuchte Isomorphismus. □

**Anmerkung 6.2.3.2.** Man beachte, dass wir (trotz der Tatsache, dass man die Äquivalenz von Körpererweiterungen eines festen Körpers $K$ als kategorientheoretische Äquivalenz auffassen kann) die Eindeutigkeit des Zerfällungskörperes bis auf Äquivalenz *nicht* dadurch beweisen können, dass wir den Zerfällungskörper als universelles Objekt in einer geeigneten Kategorie deuten. Das wesentliche Problem liegt darin, dass – anders als es für ein kategorientheoretisches universelles Objekt gefordert und zentral wäre – der Isomorphismus zwischen zwei Zerfällungskörpern nicht eindeutig sein muss. In sehr vielen Fällen gibt es sogar für eine feste Körpererweiterung $K \leq E$ einen Automorphismus $\psi : E \to E$ mit $\psi \neq \mathrm{id}_E$, der auf $K$ mit $\mathrm{id}_K$ übereinstimmt. Das Studium derartiger Automorphismen ist Gegenstand der Galoistheorie und erlaubt tiefe Einsichten über die Körpererweiterung.

Wir ziehen zwei Folgerungen.

**Folgerung 6.2.3.3.** *Jeder Zerfällungskörper $Z$ einer Menge von Polynomen $P \subseteq K[x]$ ist algebraisch über dem Grundkörper $K$.*

*Beweis.* Der in Satz 6.2.2.9 konstruierte Zerfällungskörper $Z_P$ ist algebraisch über $K$. Wegen Satz 6.2.3.1 muss das folglich für jeden Zerfällungskörper von $P$ gelten. □

**Folgerung 6.2.3.4.** *Jeder algebraische Abschluss $E$ eines Körpers $K$ ist algebraisch über $K$ und bis auf Äquivalenz eindeutig. Wenn $K$ endlich oder abzählbar ist, dann ist $E$ abzählbar, für größeres $K$ gilt stets $|E| = |K|$.*

[10] An dieser Stelle stehen eventuell mehrere Linearfaktoren $x - \alpha$ mit verschiedenen $\alpha$ zur Auswahl. Deshalb muss der Isomorphismus zwischen $Z_1$ und $Z_2$ nicht eindeutig sein.

*Beweis.* Als Zerfällungskörper über $K$ ist $E$ nach Satz 6.2.3.1 bis auf Äquivalenz eindeutig und nach Folgerung 6.2.3.3 algebraisch über $K$. Die Kardinalitätsaussage ergibt sich nun fast zur Gänze aus Proposition 6.2.2.6; es bleibt nur zu zeigen, dass $E$ auch im Falle eines endlichen Körpers $K$ immer unendlich ist. Dies übersteigt an dieser Stelle unserer Möglichkeiten, sodass wir den Beweis in Unterabschnitt 6.3.5, inbesondere Satz 6.3.5.1, vollenden werden, wenn wir mehr Theorie zur Verfügung haben (tatsächlich werden wir den algebraischen Abschluss von endlichen Körpern explizit bestimmen). □

Der Körper $\mathbb{C}$ der komplexen Zahlen ist nach dem Fundamentalsatz der Algebra algebraisch abgeschlossen. Insbesondere enthält er den Zerfällungskörper von $P := \mathbb{Q}[x] \subseteq \mathbb{C}[x]$, also einen algebraischen Abschluss $\mathbb{A} := \overline{\mathbb{Q}}$ von $\mathbb{Q}$. Die Elemente von $\mathbb{A}$ heißen *algebraische Zahlen*. Im Gegensatz dazu versteht man unter einer *transzendenten Zahl* ein Element aus $\mathbb{R} \setminus \mathbb{A}$. Nach Folgerung 6.2.3.4 gibt es, weil $\mathbb{Q}$ abzählbar ist, nur abzählbar viele algebraische Zahlen, während $\mathbb{R}$ überabzählbar ist. Cantors „Diagonalverfahren“ liefert (im Prinzip) sogar eine explizite Aufzählung aller algebraischen Zahlen und dadurch eine explizite Intervallschachtelung, deren innerster Punkt transzendent sein muss. Andere Konstruktionen von transzendenten Zahlen (zahlentheoretischer Natur), z.B. von Liouville, waren zu Cantors Zeit schon bekannt. Die Transzendenz von $e$ wurde von Hermite 1873 bewiesen, also im selben Jahr, in dem Cantor die Überabzählbarkeit von $\mathbb{R}$ entdeckte. Der Beweis der Transzendenz von $\pi$ durch Lindemann folgte 1882.

**UE 362** ► **Übungsaufgabe 6.2.3.5.** (E) Geben Sie explizit Glieder $a_n \in \mathbb{Q}$ an, so dass die daraus gebildete unendliche Reihe gegen eine transzendente Zahl $s$ konvergiert. Hinweis: Gehen Sie in folgenden Schritten vor: ◄ **UE 362**

1. Zeigen Sie: Jede algebraische Zahl ist Nullstelle eines Polynoms $f \in \mathbb{Z}[x]$ mit ganzen Koeffizienten.

2. Zeigen Sie: Das ganzzahlige Polynom $f \in \mathbb{Z}[x]$ vom Grad $n$ habe die rationale Zahl $r = \frac{p}{q}$ $(p, q \in \mathbb{Z})$ nicht als Nullstelle. Dann gilt $|f(r)| \geq \frac{1}{q^n}$.

3. Nutzen Sie die Ungleichung aus Teil 2 zu einer unteren asymptotischen Abschätzung für rationale Approximierbarkeit algebraischer Zahlen. Genauer: Ist $\alpha \in \mathbb{R}$ irrational und algebraisch vom Grad $n$, dann gibt es ein $c > 0$ derart, dass für alle $p \in \mathbb{Z}$, $q \in \mathbb{N}^+$ die Ungleichung $|\alpha - \frac{p}{q}| > \frac{c}{q^n}$ gilt.

4. Finden Sie rationale Zahlen $a_n > 0$, die so schnell gegen 0 konvergieren, dass die Partialsummen der resultierenden Reihe ihren Grenzwert $\alpha$ so gut approximieren, dass wegen Teil 3 die Zahl $\alpha$ nicht algebraisch sein kann.

### 6.2.4 Mehrfache Nullstellen und formale Ableitung

Inhalt in Kurzfassung: Hat ein reelles Polynom eine mehrfache Nullstelle, so liegt in dieser eine waagrechte Tangente vor. Es gilt auch die Umkehrung sowie eine Verallgemeinerung auf beliebige Körper. Dazu ist die Definition einer formalen Ableitung erforderlich, für

die auch auf rein algebraischem Wege die aus der Analysis vertrauten Differentiationsregeln bewiesen werden können. Mit Hilfe der Produktregel können dann die angedeuteten Zusammenhänge zwischen mehrfachen Nullstellen und dem Verschwinden von Ableitungen bewiesen werden.

An vielen Stellen der Theorie, vor allem bei endlichen Körpern und in der Galoistheorie, wird es von Interesse sein, ob ein (irreduzibles) Polynom in seinem Zerfällungskörper nur einfache oder auch mehrfache Nullstellen hat.
Als Beispiel betrachten wir das Polynom $f(x) := x^p - a$ mit einer Primzahl $p \in \mathbb{P}$ und einem Element $a$ aus dem Grundkörper $K$. Ist z.B. $K = \mathbb{Q}$ (also $\operatorname{char} K = 0$) und $a \neq 0$, so lassen sich die Nullstellen von $f$ als die $p$ verschiedenen $p$-ten Wurzeln von $a$ in $\mathbb{C}$ deuten. Ist hingegen $\operatorname{char} K = p$ und $\alpha$ eine Nullstelle von $f$ in irgendeinem Erweiterungskörper $L$ von $K$, so heißt das $\alpha^p = a$ und somit nach Satz 3.4.4.3: $x^p - a = x^p - \alpha^p = (x - \alpha)^p$. Also ist $\alpha$ sogar eine $p$-fache Nullstelle von $f$.
Ein bewährter Trick, um dieses Phänomen in den Griff zu bekommen, liegt in der Verwendung der formalen Ableitung von Polynomen. In der Analysis spiegeln sich Nullstellen höherer Vielfachheit im Verschwinden von Ableitungen wider. Wir nehmen dies zum Vorbild und definieren, allerdings ganz ohne Bezugnahme auf Grenzwerte, die Ableitung von Polynomen über beliebigen Körpern rein formal:

**Definition 6.2.4.1.** Sei $f(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$, $K$ ein beliebiger Körper. (Diese Definition ist auch allgemeiner für kommutative Ringe mit 1 sinnvoll.) Die *formale Ableitung* $f' \in K[x]$ von $f$ ist definiert durch $f'(x) := \sum_{i=1}^{n} i a_i x^{i-1} = \sum_{i=0}^{n-1} (i+1) a_{i+1} x^i \in K[x]$. (Die Multiplikation mit der natürlichen Zahl $i$ ist im Sinne der $\mathbb{Z}$-Modulstruktur abelscher Gruppen zu verstehen, d.h. als $i$-fache additive Potenz $ia := a + a + \ldots + a$ mit $i$ Summanden.)

**Proposition 6.2.4.2.** *Die formale Ableitung von Polynomen über einem Körper $K$ erfüllt die üblichen Differentiationsregeln:*

1. *Summenregel:* $(f + g)' = f' + g'$.
2. *Multiplikation mit einer Konstanten:* $(cf)' = cf'$ *für* $c \in K$.
3. *Produktregel:* $(fg)' = fg' + f'g$.
4. *Kettenregel:* $(f \circ g)'(x) = f'(g(x))g'(x)$.

**UE 363 ► Übungsaufgabe 6.2.4.3.** (V) Beweisen Sie Proposition 6.2.4.2. **◄ UE 363**

Der angekündigte Zusammenhang zwischen mehrfachen Nullstellen und formaler Ableitung lautet wie folgt:

**Lemma 6.2.4.4.** *Sei $f \in K[x]$ und $L$ der Zerfällungskörper von $f$. Dann sind die folgenden beiden Aussagen äquivalent:*

1. *Mindestens eine Nullstelle $\alpha \in L$ von $f$ ist mehrfach.*

2. *Die Polynome $f$ und $f'$ haben einen nichttrivialen* $\mathrm{ggT}(f, f')$ *in* $K[x]$.

*Beweis.* $1 \Rightarrow 2$: Habe $f \in K[x]$ in einem Erweiterungskörper $L$ (also insbesondere im Zerfällungskörper) eine mehrfache Nullstelle $\alpha$, also $f(x) = (x-\alpha)^2 g(x)$ mit $g \in L[x]$. Dann ergibt sich nach der Produktregel aus Proposition 6.2.4.2

$$f'(x) = (x-\alpha)^2 g'(x) + 2(x-\alpha)g(x) = (x-\alpha)\left((x-\alpha)g'(x) + 2g(x)\right),$$

also $f'(\alpha) = 0$. Das Minimalpolynom $m$ von $\alpha$ teilt daher sowohl $f$ als auch $f'$. Mit anderen Worten: $f$ und $f'$ haben einen nichttrivialen gemeinsamen Teiler.
$2 \Rightarrow 1$: Sei nun vorausgesetzt, dass $f$ und $f'$ einen nichttrivialen gemeinsamen Teiler haben und indirekt angenommen, dass $f$ im Zerfällungskörper $L$ nur einfache Nullstellen habe. Ist $\alpha$ eine solche einfache Nullstelle von $f$ in $L$, also $f(x) = (x-\alpha)g(x)$ mit $g \in L[x]$ und $g(\alpha) \neq 0$, so berechnen wir wieder mit der Produktregel $f'(x) = (x-\alpha)g'(x) + g(x)$, also $f'(\alpha) = g(\alpha) \neq 0$. Weil nichttriviale gemeinsame Teiler von $f$ und $f'$ aber gemeinsame Nullstellen im Zerfällungskörper bedeuten, folgt daraus, dass $f$ und $f'$ teilerfremd sind, Widerspruch. □

Für irreduzibles $f \in K[x]$ hat das bemerkenswerte Konsequenzen. Denn als Teiler von $f$ kommen dann nur konstante Polynome und (bis auf Assoziiertheit, also bis auf multiplikative Konstante) $f$ selbst in Frage. Ist $\mathrm{ggT}(f, f')$ nichttrivial, so folgt also $\mathrm{ggT}(f, f') = f$ und somit $f | f'$. Weil aber $\mathrm{grad}(f) \leq \mathrm{grad}(f')$ nicht möglich ist, gilt $f | f'$ genau dann, wenn $f' = 0$. Das schließt $\mathrm{char}\, K = 0$ aus. Im Fall $\mathrm{char}\, K = p \in \mathbb{P}$ hingegen ist $f' = 0$ sehr wohl möglich, nämlich genau dann, wenn in $f$ nur solche Exponenten von $x$ auftreten, die ein Vielfaches von $p$ sind. In diesem Fall ist tatsächlich $\mathrm{ggT}(f, f') = \mathrm{ggT}(f, 0) = f$. Nach Lemma 6.2.4.4 hat $f$ eine mehrfache Nullstelle. Damit haben wir bewiesen:

**Satz 6.2.4.5.** *Sei $K$ ein Körper und $f(x) \in K[x]$ irreduzibel. In seinem Zerfällungskörper hat $f$ genau dann eine mehrfache Nullstelle, wenn* $\mathrm{char}\, K = p$ *eine Primzahl und $f$ von der Form $f(x) = g(x^p)$ mit $g \in K[x]$ ist.*

### 6.2.5 Einheitswurzeln und Kreisteilungspolynome

Inhalt in Kurzfassung: Die Zerlegung des Polynoms $x^n - 1$ in Linearfaktoren entspricht dem Aufsuchen von $n$-ten Einheitswurzeln, was in $\mathbb{C}$ geometrisch als Konstruktion des dem Einheitskreis eingeschriebenen regelmäßigen $n$-Ecks interpretiert werden kann. Daher rührt die Bezeichnung „Kreisteilungspolynom“ für gewisse, rekursiv definierte (sich bei Charakteristik 0 sogar als irreduzibel erweisende) Faktoren des Polynoms $x^n - 1$, dessen Nullstellen offenbar eine endliche multiplikative Untergruppe des Körpers bilden. Eine solche ist stets zyklisch.

Wir beginnen mit einem Satz, der auch für die Theorie endlicher Körper noch sehr wichtig sein wird.

**Satz 6.2.5.1.** *Jede endliche Untergruppe $G$ der multiplikativen Gruppe eines Körpers, insbesondere die multiplikative Gruppe jedes endlichen Körpers, ist zyklisch.*

*Beweis.* Nach Lemma 3.3.3.1 gibt es ein $g_0 \in G$, dessen multiplikative Ordnung $n_0$ ein Vielfaches aller Ordnungen $n_g$ von Elementen $g \in G$ ist. Also erfüllen alle $g \in G$ die Gleichung $g^{n_0} = 1$. Somit hat das Polynom $x^{n_0} - 1$ mindestens $|G|$ Nullstellen. Es folgt $|G| \leq n_0$ wegen Proposition 5.3.3.2. Da nach dem Satz von Lagrange umgekehrt $n_0$ ein Teiler von $|G|$ ist, folgt $|G| = n_0$, also ist $g_0$ erzeugendes Element der zyklischen Gruppe $G$. □

In jedem Körper $K$ bilden die sogenannten $n$-ten *Einheitswurzeln*, das sind die Nullstellen des Polynoms $f_n(x) := x^n - 1$ ($n \in \mathbb{N}^+$), eine Untergruppe $E_n$ der multiplikativen Gruppe von $K$. Weil es nur höchstens $n$ Lösungen dieser Polynomgleichung geben kann, ist $E_n$ endlich, nach Satz 6.2.5.1 also zyklisch. Die nun folgenden Überlegungen beziehen sich auf den Fall von $\operatorname{char} K = 0$, d.h. wir dürfen oBdA $\mathbb{Q}$ als Primkörper von $K$ annehmen. Verwandte Überlegungen bei Primzahlcharakteristik werden in 6.3.3 folgen.
Die Ableitung $f_n'(x) = nx^{n-1}$ hat nur $x$ als irreduziblen Faktor, ist also zu $f_n(x) = x^n - 1$ teilerfremd. Folglich hat $f_n$ nach Lemma 6.2.4.4 in seinem Zerfällungskörper $Z_n$ nur einfache Nullstellen. In $Z_n$ ist also $E_n \cong C_n$ (nochmals wegen Satz 6.2.5.1) eine zyklische Gruppe der Ordnung $n$. Ihre Erzeugenden heißen *primitive $n$-te Einheitswurzeln.* Zu ihrer Bezeichnung werden wir traditionsgemäß meist den griechischen Buchstaben $\zeta$ verwenden. OBdA dürfen wir $Z_n \leq \mathbb{C}$ annehmen. Sei $\zeta_n$ eine primitive $n$-te Einheitswurzel, also z.B. $\zeta_n := e^{\frac{2\pi i}{n}}$ ($i \in \mathbb{C}$ imaginäre Einheit). $E_n$ besteht genau aus den Potenzen $\zeta_n^j$, $j = 0, \ldots, n-1$, der primitiven Einheitswurzel, folglich gilt

$$f_n(x) = x^n - 1 = \prod_{j=0}^{n-1} (x - \zeta_n^j).$$

Insbesondere enthält der von $\zeta_n$ erzeugte Körper $K_n := \mathbb{Q}(\zeta_n)$ alle $n$-ten Einheitswurzeln und stimmt daher bereits mit dem Zerfällungskörper $Z_n$ von $x^n - 1$ überein. Weil die Elemente von $E_n$ in der komplexen Ebene ein regelmäßiges $n$-Eck auf dem Einheitskreis bilden, heißt $K_n$ auch der $n$-te *Kreisteilungskörper*. Nach Satz 3.2.4.13 sind die Untergruppen der zyklischen Gruppe $E_n$ genau die Gruppen $E_k$ mit $k|n$. Weil $E_k$ der Zerfällungskörper von $x^k - 1$ ist, gilt $f_k(x) = x^k - 1 | x^n - 1 = f_n(x)$ genau dann, wenn $k|n$. Diese Erkenntnis hilft bei der Suche nach Zerlegungen von $f_n(x) = x^n - 1 = \prod_{j=0}^{n-1}(x - \zeta_n^j)$ über $K$, bei der es offenbar darum geht, wie man gewisse der Faktoren $x - \zeta_n^j$ zusammenfassen kann, um wieder Polynome mit Koeffizienten in $K$ zu bekommen. Analysiert man die Situation genauer, erkennt man:

**Satz 6.2.5.2.** *Definiert man die Polynome $g_n$, die sogenannten* Kreisteilungspolynome*, für $n \in \mathbb{N}^+$ rekursiv durch $g_1(x) := x - 1$ und*

$$g_n(x) := \prod_{j:\ 0 \leq j < n-1,\ \operatorname{ggT}(j,n)=1} (x - \zeta_n^j),$$

*so gilt*

$$x^n - 1 = \prod_{d|n, 1 \leq d \leq n} g_d(x)$$

*für alle $n \in \mathbb{N}^+$. Die Kreisteilungspolynome sind normiert, haben ausschließlich ganzzahlige Koeffizienten, der konstante Koeffizient ist entweder 1 oder $-1$, und die Grade erfüllen* $\operatorname{grad}(g_n) = \varphi(n)$ *(Eulersche $\varphi$-Funktion).*

*Beweis.* Beachtet man $x^n - 1 = \prod_{j=0}^{n-1}(x - \zeta_n^j)$, so ergibt sich die behauptete Zerlegung $x^n - 1 = \prod_{d|n} g_d(x)$ aus der Tatsache, dass jede der $n$-ten Einheitswurzeln $\zeta_n^j$, $j = 0, \ldots, n-1$, für genau ein $d|n$ eine primitive $d$-te Einheitswurzel ist. Außerdem gilt nach Definition $\operatorname{grad}(g_n) = \varphi(n)$. Aus $x^n - 1 = g_n(x)g_n^*(x)$ mit $g_n^*(x) := \prod_{d|n, 1 \leq d < n} g_d(x)$, liest man ab, dass sich induktiv die Normiertheit der $g_d$ mit $d < n$ auf die von $g_n^*$ und somit auf $g_n$ überträgt, analog dass der konstante Koeffizient immer nur $\pm 1$ sein kann. Das Polynom $g_n$ erhält man durch Polynomdivision des ganzzahligen Polynoms $x^n - 1$ durch den normierten und ganzzahligen Teiler $g_n^*$, was die Ganzzahligkeit sämtlicher Koeffizienten von $g_n$ garantiert. □

**UE 364** ► **Übungsaufgabe 6.2.5.3.** (B) Ermitteln Sie die Kreisteilungspolynome $g_n(x)$ für alle $n \leq N$ und möglichst großes $N$. ◄ **UE 364**

**Anmerkung 6.2.5.4.** Mit etwas größerem Aufwand lässt sich zeigen, dass die Kreisteilungspolynome $g_n$ sogar irreduzibel über $\mathbb{Q}$ sind.

**UE 365** ► **Übungsaufgabe 6.2.5.5.** (E) Beweisen Sie Anmerkung 6.2.5.4. Wenn es zu schwierig ist, recherchieren Sie in der Literatur. ◄ **UE 365**

### 6.2.6 Beispiele einfacher Erweiterungen

Inhalt in Kurzfassung: Der Satz vom primitiven Element wird bewiesen: In Charakteristik 0 ist jede endlichdimensionale Erweiterung einfach (d.h. sie wird von einem einzigen, geeignet zu wählenden Element erzeugt). Erwähnt wird außerdem der Satz von Lüroth: Jeder Zwischenkörper $Z$ mit $K \leq Z \leq K(x)$ ist eine einfache, für $K \neq Z$ transzendente Erweiterung über $K$.

Wir haben bereits systematisch alle Möglichkeiten einfacher Körpererweiterungen $K(\alpha)$ eines Körpers $K \leq L$ mit $\alpha \in L$ untersucht und sind dabei auf die Unterscheidung zwischen algebraischen und transzendenten Elementen $\alpha$ gestoßen. Manchmal ist es umgekehrt von Interesse, von einer gegebenen Erweiterung $K \leq L$ entscheiden zu können, ob sie einfach ist. In diesem Unterabschnitt werden für beide Fälle, algebraisch und transzendent, hinreichende Bedingungen gegeben. Auf den algebraischen Fall bezieht sich der sogenannte *Satz vom primitiven Element*, der übrigens auch unter etwas allgemeineren Voraussetzungen gilt, siehe 9.2.4.10.

**Satz 6.2.6.1.** *Ist $L$ eine endlichdimensionale Körpererweiterung von $K$ mit* $\operatorname{char} K = \operatorname{char} L = 0$*, so gibt es ein $\alpha \in L$ mit $L = K(\alpha)$.*

*Beweis.* Wegen der endlichen Dimension der Erweiterung gibt es $u_1, \ldots, u_r \in L$ mit $L = K(u_1, \ldots, u_r)$. Wir führen den Beweis mittels Induktion nach $r$.
Für $r = 1$ ist die Aussage trivial. Wir nehmen daher an, der Satz gelte für $r-1$ ($r > 1$). Wir haben dann: $L = K(u_1, \ldots, u_r) = K(u_1, \ldots, u_{r-1})(u_r) = K(\alpha)(u_r) = K(\alpha, \beta)$ für ein geeignetes $\alpha \in L$ und für $\beta = u_r$. Wegen $[K(\alpha, \beta) : K] < \infty$ sind $\alpha, \beta$ algebraisch über $K$. Wir zeigen: $\exists \delta \in L$ mit $K(\alpha, \beta) = K(\delta)$.
Seien $f(x)$ bzw. $g(x)$ die Minimalpolynome von $\alpha$ bzw. $\beta$. Wir betrachten einen Erweiterungskörper $M$ von $L$ (insbesondere von $K$), der zugleich Nullstellenkörper von $f(x)$ und $g(x)$ ist, d. h. es gibt $\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_t \in M$ mit $f(x) = (x - \alpha_1) \cdots (x - \alpha_s)$ und $g(x) = (x - \beta_1) \cdots (x - \beta_t)$. Dabei sei o.B.d.A. $\alpha_1 = \alpha$ und $\beta_1 = \beta$. Nach Satz 6.2.4.5 ist $\beta \neq \beta_k$ für $k = 2, \ldots, t$, daher hat die Gleichung $\alpha_i + x\beta_k = \alpha + x\beta$ für jedes $i = 1, \ldots, s$ und $k = 2, \ldots, t$ höchstens eine Lösung in $K$. Da $K$ unendlich ist (wegen $\operatorname{char} K = 0$), haben wir also für fast alle $c \in K$ (d. h. für alle $c \in K$ bis auf endlich viele) $\alpha_i + c\beta_k \neq \alpha + c\beta$ für alle $i = 1, \ldots, s$ und $k = 2, \ldots, t$. Wir wählen ein solches $c$, halten es fest und behaupten

$$K(\alpha, \beta) = K(\delta) \text{ mit } \delta := \alpha + c\beta \in L.$$

Trivialerweise ist $K(\delta) \subseteq K(\alpha, \beta)$. Für die umgekehrte Inklusion genügt es zu zeigen, dass $\alpha, \beta \in K(\delta)$. Dazu betrachten wir das Polynom $\bar{f}(x) := f(\delta - cx) \in K(\delta)[x]$. Es ist dann $\bar{f}(\beta) = f(\delta - c\beta) = f(\alpha) = 0$, aber für $k = 2, \ldots, t$ gilt: $\bar{f}(\beta_k) = f(\delta - c\beta_k) = f(\alpha + c\beta - c\beta_k) \neq 0$, da ja $\alpha + c\beta - c\beta_k \neq \alpha_i$ für $i = 1, \ldots, s$ nach Wahl von $c$. Also haben $g(x)$ und $\bar{f}(x)$ genau die eine Nullstelle $\beta$ gemeinsam. Daher ist in $K(\delta)[x]$: $\operatorname{ggT}(g(x), \bar{f}(x)) = x - \beta$, insbesondere also $\beta \in K(\delta)$ und somit auch $\alpha = \delta - c\beta \in K(\delta)$. □

**UE 366 ► Übungsaufgabe 6.2.6.2.** (F) Man bestimme $\alpha \in \mathbb{C}$ so, dass $\mathbb{Q}(i, \sqrt{3}) = \mathbb{Q}(\alpha)$. **◄ UE 366**

Für transzendente Erweiterungen von Interesse ist der folgende *Satz von Lüroth*, der hier ohne Beweis erwähnt sei:

**Satz 6.2.6.3.** *Sei $K$ ein Körper und $L := K(x)$ der Körper der gebrochen rationalen Funktionen über $K$. Dann ist jeder Zwischenkörper $Z$ (d.h. jeder Körper mit $K \leq Z \leq L$) eine einfache Körpererweiterung von $K$. Es gibt also ein $r = r(x) \in K(x)$ mit $Z = K(r(x))$. Ist $K \neq Z$, so ist $r \notin K$ transzendent über $K$ und somit $K(r) \cong K(x) = L$.*

**UE 367 ► Übungsaufgabe 6.2.6.4.** (E) Beweisen Sie den Satz 6.2.6.3 von Lüroth, eventuell unter Zuhilfenahme von Literatur. **◄ UE 367**

**UE 368** ► **Übungsaufgabe 6.2.6.5.** (B) Sei $L := \mathbb{Q}(x)$ der Körper der gebrochen rationalen Funktionen über $\mathbb{Q}$. ◄ **UE 368**

(1) Berechnen Sie $[L : K]$ für $K := \mathbb{Q}(x^3) \leq L$, indem Sie das Minimalpolynom von $x$ über $K$ finden.

(2) Wie Teil 1, nur mit $K := \mathbb{Q}(x + \frac{1}{x})$.

(3) Zeigen Sie: $[L : K]$ ist endlich für jeden Körper $K := \mathbb{Q}(\alpha)$ mit $\alpha \in \mathbb{Q}(x) \setminus \mathbb{Q}$. Schließen Sie, dass jedes $\alpha \in \mathbb{Q}(x) \setminus \mathbb{Q}$ transzendent über $\mathbb{Q}$ ist.

**UE 369** ► **Übungsaufgabe 6.2.6.6.** (F) Sei $R$ der Polynomring $\mathbb{Z}_5[t]$, und sei $U \subseteq R$ der kleinste Unterring mit 1 von $R$, der das Polynom $t^5$ enthält. Beschreiben Sie $U$ (d.h., erklären Sie, wie Sie von einem beliebigen Polynom in $R$ entscheiden können, ob es in $U$ liegt). ◄ **UE 369**

**UE 370** ► **Übungsaufgabe 6.2.6.7.** (F) Seien $R$ und $U$ wie in der vorigen Aufgabe. Geben Sie ein Polynom $p(x) \in U[x]$ an, welches in $R$ die Nullstelle $t$ hat. (Wenn Ihnen das zu leicht ist: Finden Sie so ein Polynom, welches in $U[x]$ irreduzibel ist.) ◄ **UE 370**

## 6.3 Endliche Körper (Galoisfelder)

Die wichtigsten Inhalte dieses Abschnitts sind die folgenden: In 6.3.1 verwenden wir vor allem unser Wissen über Zerfällungskörper, um die endlichen Körper zu klassifizieren: Jeder endliche Körper $K$ hat $|K| = p^n$ Elemente mit einer Primzahl $p$ und $n \in \mathbb{N}$, $n \geq 1$. Umgekehrt gibt es zu jeder Primzahlpotenz $p^n$ bis auf Isomorphie genau ein $K$ mit $|K| = p^n$, nämlich den Zerfällungskörper des Polynoms $x^{p^n} - x$ über dem Primkörper $\mathbb{Z}_p$. Man nennt $K$ das Galoisfeld[11] mit $p^n$ Elementen und schreibt dafür auch $\mathrm{GF}(p^n)$. Üblich ist auch die Bezeichnung $\mathbb{F}_{p^n}$, die wir hier jedoch nicht verwenden. Die additive Gruppe von $\mathrm{GF}(p^n)$ ist isomorph zum $n$-fachen Produkt $(C_p)^n$ einer zyklischen Gruppe mit $p$ Elementen, die multiplikative Gruppe ist selbst zyklisch, also isomorph zu $C_{p^n-1}$. Die Unterkörper von $\mathrm{GF}(p^n)$ sind genau jene $\mathrm{GF}(p^k)$ mit $k|n$ (6.3.2). Wegen $\mathrm{GF}(p^n) \cong \mathbb{Z}_p[x]/(f)$ für jedes irreduzible $f \in \mathbb{Z}_p[x]$ vom Grad $n$ muss für die Konstruktion von $\mathrm{GF}(p^n)$ (6.3.4) nur so ein $f$ gefunden werden, was auch möglich ist, wie wir zuvor in 6.3.3 klären. Am Ende des Abschnitts (6.3.5) wird auch noch der algebraische Abschluss $\mathrm{GF}(p^\infty)$ von $\mathbb{Z}_p$ und gleichzeitig jedes endlichen Körpers mit Charakteristik $p$ beschrieben. Dass mit den endlichen Körpern auch sämtliche endliche Schiefkörper gegeben sind, ist Inhalt des Satzes von Wedderburn, den wir ohne Beweis anführen.

### 6.3.1 Klassifikation endlicher Körper

Inhalt in Kurzfassung: Sei $K$ ein endlicher Körper, $P \cong \mathbb{Z}_p$, $p \in \mathbb{P}$, sein Primkörper und $n$ die Dimension von $K$ über $P$. Dann gilt offenbar $|K| = p^n$. Außerdem erweist sich

[11] Nach Évariste Galois (1811-1832)

$K$ sehr schnell als Zerfällungskörper des Polynoms $x^{p^n} - x$ über $P$. Als solcher ist $K$ aufgrund der Ergebnisse aus 6.2.3 durch seine Kardinalität bis auf Isomorphie eindeutig bestimmt. Umgekehrt lässt sich mit Hilfe der Methoden aus 6.2.2 der Zerfällungskörper des Polynoms $x^{p^n} - x$ über $P$ konstruieren und hat auch tatsächlich $p^n$ Elemente. Damit ist ein Klassifikationssatz für endliche Körper vollständig bewiesen.

Sei $K$ ein endlicher Körper. Dann ist $\operatorname{char} K = p \in \mathbb{P}$, und der Primkörper $P$ von $K$ ist isomorph zu $\mathbb{Z}_p$ (vgl. 6.1.1.8). Da $K$ ein Vektorraum über dem Unterkörper $P$ ist, gibt es eine Basis $\{a_1, \ldots, a_n\}$ von $K$ über $P$, also $[K : P] = n \in \mathbb{N}^+$. Daher ist $K = \{\lambda_1 a_1 + \cdots + \lambda_n a_n \mid \lambda_i \in P\}$ und $|K| = p^n$, da jeder Koeffizient $\lambda_i$ auf $|P| = p$ Arten gewählt werden kann.

**Frage:** Seien umgekehrt $p \in \mathbb{P}$ und $n \in \mathbb{N}^+$ gegeben. Gibt es einen Körper $K$ mit $|K| = p^n$?

Wenn es einen solchen Körper $K$ gibt, dann mit $\operatorname{char} K = p$, also können wir ihn jedenfalls mit Primkörper $\mathbb{Z}_p$ finden. Die multiplikative Gruppe $K^* = K \setminus \{0\}$ von $K$ hat $p^n - 1$ Elemente. Nach dem Satz von Lagrange gilt daher $a^{p^n-1} = 1$ für alle $a \in K^*$. Alle $a \in K^*$ sind daher Nullstellen des Polynoms $x^{p^n-1} - 1$. Multiplizieren wir dieses Polynom mit $x$, so ist auch 0 Nullstelle, nämlich des Polynoms $f(x) := x^{p^n} - x \in \mathbb{Z}_p[x]$. Sein Grad ist $p^n$, und es hat $p^n$ verschiedene Nullstellen, nämlich alle Elemente von $K$. Es gilt daher:

$$f(x) = x^{p^n} - x = \prod_{\alpha \in K} (x - \alpha),$$

und $K$ ist der Zerfällungskörper von $f$ über $\mathbb{Z}_p$. Als solcher ist $K$ nach Satz 6.2.3.1 bis auf Isomorphie eindeutig bestimmt.
Wir haben also gezeigt: Wenn es einen Körper $K$ mit $p^n$ Elementen gibt, so muss $K$ der Zerfällungskörper des Polynoms $f(x) := x^{p^n} - x$ über $\mathbb{Z}_p$ sein.
Für den angestrebten Klassifikationssatz haben wir nur noch zu beweisen, dass der Zerfällungskörper $Z$ von $f$ wirklich $p^n$ Elemente hat. Zunächst schließen wir aus $f'(x) = p^n x^{p^n-1} - 1 = -1$, dass $f$ und $f'$ teilerfremd sind, was nach Lemma 6.2.4.4 sicherstellt, dass alle Nullstellen von $f$ im Zerfällungskörper $Z$ einfach sind. Die Menge $N$ aller Nullstellen von $f$ in $Z$ hat somit $p^n$ Elemente. Um $N$ bereits als den gesuchten Körper mit $p^n$ Elementen zu identifizieren, genügt der Beweis von:

**Lemma 6.3.1.1.** *Im Zerfällungskörper $Z$ des Polynoms $f(x) := x^{p^n} - x$ über dem Primkörper $\mathbb{Z}_p$ bildet die Menge $N$ aller Nullstellen von $f$ einen Unterkörper. Folglich ist $N = Z$.*

*Beweis.* $N$ besteht genau aus jenen $\alpha \in Z$ mit $\alpha^{p^n} = \alpha$, insbesondere also $0, 1 \in N$. Für $\alpha, \beta \in N$, also $\alpha^{p^n} = \alpha$ und $\beta^{p^n} = \beta$, gilt außerdem:

- $(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$, also $\alpha + \beta \in N$. (nach Satz 3.4.4.3)
- $(-\alpha)^{p^n} = (-1)^{p^n}(\alpha^{p^n}) = -\alpha$, also $-\alpha \in N$. (Man beachte, dass für $p = 2$ die Gleichung $1 = -1$ gilt.)

- $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$, also $\alpha\beta \in N$.
- $(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}$, also $\alpha^{-1} \in N$, sofern $\alpha \neq 0$. □

Aus dem Bisherigen folgt nun unmittelbar der *Klassifikationssatz für endliche Körper*:

**Satz 6.3.1.2.** *Die Kardinalität jedes endlichen Körpers ist eine Primzahlpotenz $p^n$ ($p \in \mathbb{P}$, $n \in \mathbb{N}^+$). Umgekehrt gibt es zu jeder Primzahlpotenz $p^n$ bis auf Isomorphie genau einen Körper $K$ mit $|K| = p^n$, nämlich den Zerfällungskörper des Polynoms $x^{p^n} - x$, der ausschließlich aus den Nullstellen dieses Polynoms besteht.*

**Definition 6.3.1.3.** Sei $p \in \mathbb{P}$ und $n \in \mathbb{N}^+$. Man schreibt den bis auf Isomorphie eindeutigen Körper mit $p^n$ Elementen als $\mathrm{GF}(p^n)$ und nennt ihn das *Galoisfeld* mit $p^n$ Elementen. Statt $\mathrm{GF}(p)$ schreiben wir wie schon bisher meistens $\mathbb{Z}_p$.

Für die spätere (Wieder-)Verwendung isolieren wir aus den obigen Überlegungen über die formale Ableitung von $x^{p^n} - x$ noch die folgende Tatsache:

**Lemma 6.3.1.4.** *Das Polynom $x^{p^n} - x \in \mathbb{Z}_p[x]$ hat in seinem Zerfällungskörper nur einfache Nullstellen.*

Der Satz von Wedderburn besagt, dass alle endlichen Schiefkörper kommutativ sind, dass man also keine weiteren Strukturen vorfindet, wenn man auf die Kommutativität der Multiplikation eines Körpers verzichten würde. Der Beweis erfordert die sogenannte *Klassengleichung*, ein Instrument aus der Theorie der *Gruppenaktionen*; siehe Algebra II.

**Satz 6.3.1.5.** *Jeder endliche Schiefkörper ist ein Körper, also isomorph zu einem* $\mathrm{GF}(p^n)$.

Die Quaternionen als prominentestes Beispiel eines Schiefkörpers belegen, dass unendliche Schiefkörper, die keine Körper sind, sehr wohl existieren.

## 6.3.2 Die Unterkörper eines endlichen Körpers

Inhalt in Kurzfassung: Ist $K$ ein Unterkörper des endlichen Körpers $E$, so muss, weil beide denselben Primkörper $P \cong \mathbb{Z}_p$ haben, ihre Charakteristik $p \in \mathbb{P}$ übereinstimmen. Folglich gilt $|K| = p^k$ und $|E| = p^n$ mit geeigneten positiven natürlichen Zahlen $k$ und $n$. Aus dem Gradsatz folgt daraus fast unmittelbar $k|n$. Umgekehrt erweist sich bei $k|n$ das Polynom $x^{p^k} - x$ (dessen Zerfällungskörper ja $K$ ist) als Teiler des Polynoms $x^{p^n} - x$ (dessen Zerfällungskörper wiederum $E$ ist), sodass jeder Körper $E$ mit $p^n$ Elementen einen (sogar eindeutig bestimmten) Unterkörper $K$ mit $p^k$ Elementen als Unterkörper enthält. Damit sind die Inklusionsbeziehungen zwischen endlichen Körpern vollständig geklärt.

Sei $p$ eine feste Primzahl. Unser Ziel ist zu verstehen, welche Unterkörper ein endlicher Körper hat. Vollständige Auskunft darüber wird Satz 6.3.2.4 geben. Zur Vorbereitung brauchen wir aber noch ein Lemma über die Teilbarkeit gewisser ganzzahliger Polynome:

**Lemma 6.3.2.1.** *Seien $k, n \in \mathbb{N}$ mit $k|n$ und $p \in \mathbb{P}$. Dann gilt:*

1. $x^k - 1 | x^n - 1$ *in* $\mathbb{Z}[x]$ *und in* $\mathbb{Z}_p[x]$.
2. $p^k - 1 | p^n - 1$ *in* $\mathbb{Z}$.
3. $x^{p^k-1} - 1 | x^{p^n-1} - 1$ *in* $\mathbb{Z}[x]$ *und in* $\mathbb{Z}_p[x]$. *Insbesondere gilt* $x^{p^k} - x | x^{p^n} - x$.

*Die dabei auftretenden Polynome können alternativ sogar als Polynome über einem beliebigen kommutativen Ring mit* 1 *aufgefasst werden.*

*Beweis.* 1. Folgt aus $x^n - 1 = (x^k - 1)(x^{n-k} + x^{n-2k} + \cdots + x^k + 1)$.

2. In der ersten Behauptung $x = p$ einsetzen.
3. In Aussage 1 kann (wegen Aussage 2) $k$ durch $p^k - 1$ sowie $n$ durch $p^n - 1$ ersetzt werden. □

Es stellt sich heraus, dass ein endlicher Körper nur eine einzige Kopie jedes Unterkörpers enthalten kann. Tatsächlich gilt sogar etwas mehr – es kommt nämlich nur darauf an, dass der Unterkörper endlich ist.

**Proposition 6.3.2.2.** *Sei $L$ ein Körper und seien $K_1, K_2 \leq L$ endliche Unterkörper mit $|K_1| = |K_2| = p^n$. Dann gilt $K_1 = K_2$.*

*Beweis.* Da $L$ Unterkörper der Kardinalität $p^n$ enthält, muss $L$ Charakteristik $p$ haben, d.h. sein Primkörper ist $P \cong \mathbb{Z}_p$. Wir wissen aus Satz 6.3.1.2, dass alle Elemente von $K_1$ und von $K_2$ Nullstellen des Polynoms $x^{p^n} - x \in P[x]$ sind. Würden $K_1$ und $K_2$ nicht übereinstimmen, dann würde $L$ mehr als $p^n$ Nullstellen eines Polynoms vom Grad $p^n$ enthalten, was Proposition 5.3.3.2 widerspricht. □

**UE 371** ► **Übungsaufgabe 6.3.2.3.** Finden Sie zwei Beispiele, die zeigen, dass Proposition 6.3.2.2 für unendliche Körper $K_1, K_2$ nicht gilt; genauer: Finden Sie einen Körper $L$ und zwei (notwendigerweise unendliche) *isomorphe aber verschiedene* Unterkörper $K_1, K_2 \leq L$, indem Sie ◄ **UE 371**

1. $L$ als den Zerfällungskörper von $x^3 - 2$ über $\mathbb{Q}$ wählen und Satz 6.1.3.4 verwenden.
2. $L = \mathbb{Q}(x)$ wählen und Satz 6.1.3.3 verwenden.

Mit dieser Proposition können wir nun den folgenden Satz beweisen:

**Satz 6.3.2.4.** *Als Unterkörper von* $\mathrm{GF}(p^n)$ *treten genau die* $\mathrm{GF}(p^k)$ *mit* $k|n$ *auf, jeder genau einmal.*

*Beweis.* Dass als Unterkörper von $\mathrm{GF}(p^n)$ nur die $\mathrm{GF}(p^k)$ mit $k|n$ auftreten können, ergibt sich schnell aus dem Gradsatz 6.1.2.2. Sei dazu $\mathrm{GF}(p^k) \leq \mathrm{GF}(p^n)]$ und $d := [\mathrm{GF}(p^n) : \mathrm{GF}(p^k)]$. Es folgt

$$n = [\mathrm{GF}(p^n) : \mathrm{GF}(p)] = [\mathrm{GF}(p^n) : \mathrm{GF}(p^k)] \cdot [\mathrm{GF}(p^k) : \mathrm{GF}(p)] = d \cdot k,$$

also $k|n$.
Wegen Proposition 6.3.2.2 kann $\mathrm{GF}(p^n)$ höchstens eine einzige Kopie von $\mathrm{GF}(p^k)$ als Unterkörper enthalten. Das ist für $k|n$ auch tatsächlich der Fall: Denn laut der dritten Aussage von Lemma 6.3.2.1 ist $x^{p^k} - x$ ein Teiler von $x^{p^n} - x$ im Polynomring über dem Primkörper $P \cong \mathbb{Z}_p$, weshalb jede Nullstelle von $x^{p^k} - x$ auch eine von $x^{p^n} - x$ ist. Also ist der Zerfällungskörper $\mathrm{GF}(p^k)$ des Polynoms $x^{p^k} - x$ im Zerfällungskörper $\mathrm{GF}(p^n)$ des Polynoms $x^{p^n} - x$ enthalten. □

**UE 372** ► **Übungsaufgabe 6.3.2.5.** (E) Sei $p \in \mathbb{P}$. Man zeige, dass in jedem Polynomring über einem kommutativen Ring mit 1 gilt: $x^{p^k} - x | x^{p^n} - x \Leftrightarrow k|n$. ◄ **UE 372**

### 6.3.3 Irreduzible Polynome über endlichen Primkörpern

Inhalt in Kurzfassung: Die Klassifikation endlicher Körper aus 6.3.1 und ihrer Unterkörper aus 6.3.2 zusammen mit der Zerlegung der Polynome $x^{p^n} - x$ über dem Primkörper $P \cong \mathbb{Z}_p$, $p \in \mathbb{P}$, $n \in \mathbb{N}^+$, in (normierte) irreduzible Faktoren zeigt, dass als solche Faktoren genau jene irreduziblen (und normierten) Polynome über $P$ auftreten, deren Grad ein Teiler von $n$ ist, wobei jeder Faktor Vielfachheit 1 hat. Daraus ergeben sich mehrere interessante Folgerungen: Zu jedem positiven Grad gibt es mindestens ein irreduzibles Polynom über $P$, das sogar als primitiv gewählt werden kann. Letzteres bedeutet, dass seine Nullstellen die multiplikative Gruppe seines Zerfällungskörpers $K$ erzeugen. Da jeder Automorphismus von $K$ die Nullstellen jedes irreduziblen Faktors von $x^{p^n} - x$ permutiert, schließt man daraus, dass $K$ genau $n$ verschiedene Automorphismen hat – ein erstes Ergebnis im Geiste der Galoistheorie, siehe Kapitel 9.

Nach den Ergebnissen in 6.3.1 und 6.3.2 sind endliche Körper der Kardinalität $p^n$ eng verbunden mit dem Polynom $x^{p^n} - x$ über dem Primkörper $P \cong \mathbb{Z}_p$. Andererseits führt auch die Konstruktion aus dem Satz von Kronecker (Proposition 6.2.1.1) angewandt auf ein in $\mathbb{Z}_p[x]$ irreduzibles Polynom vom Grad $n$ auf einen Körper vom Grad $n$ über $\mathbb{Z}_p$, also mit $p^n$ Elementen. Die Verbindung dieser beiden Blickwinkel führt auf einige interessante Einsichten, denen wir uns in diesem Unterabschnitt widmen wollen.

**Proposition 6.3.3.1.** *Sei $n \in \mathbb{N}$ mit $n \geq 1$, $p$ eine Primzahl, $K \cong \mathrm{GF}(p^n)$ ein Körper mit $p^n$ Elementen und $P \cong \mathbb{Z}_p$ der Primkörper von $K$. Dann gilt:*

1. *$K$ ist der Zerfällungskörper nicht nur des Polynoms $x^{p^n} - x$, sondern jedes irreduziblen Polynoms $f \in P[x]$ vom Grad $n$. Ist $\alpha \in K$ eine Nullstelle von $f$, so gilt sogar $K = P(\alpha)$.*

2. *Ist $f \in P[x]$ ein irreduzibles Polynom vom Grad $n$, so ist $f$ in $P[x]$ ein Teiler von $x^{p^n} - x$.*

3. *Ist $f \in P[x]$ ein irreduzibles Polynom vom Grad $n$, so hat $f$ genau $n$ paarweise verschiedene Nullstellen in $K$ – es gibt also keine mehrfachen Nullstellen.*

4. *Die irreduziblen und normierten Faktoren von $x^{p^n} - x$ sind genau jene irreduziblen und normierten Polynome über $P$, deren Grad ein Teiler von $n$ ist. Die Vielfachheit all dieser Faktoren ist* 1.

*Beweis.*

1. Sei $f \in P[x]$ irreduzibel vom Grad $n$, oBdA normiert. Wir betrachten den Zerfällungskörper der Menge $\{x^{p^n} - x, f\}$ über $P$ und nennen ihn $L$. Sei weiters $\alpha \in L$ eine Nullstelle von $f$. Da $f$ irreduzibel ist, ist $f$ sogar das Minimalpolynom von $\alpha$, sodass $P(\alpha) \leq L$ wegen Satz 6.1.3.4 ein Körper mit $[P(\alpha) : P] = n$ ist. Somit gilt $|P(\alpha)| = p^n$. Der Körper $K$ (mit ebenfalls $p^n$ Elementen) ist als Zerfällungskörper von $x^{p^n} - x$ ebenfalls in $L$ enthalten. Nach Proposition 6.3.2.2 gilt $K = P(\alpha)$, insbesondere $\alpha \in K$. Da $\alpha$ beliebig war, ist $K$ ein Nullstellenkörper von $f$, der von einer Nullstelle von $f$ (insbesondere also von der Menge aller Nullstellen) erzeugt wird. Mit anderen Worten ist $K$ der Zerfällungskörper von $f$.

2. Sei $\alpha \in K$ eine Nullstelle von $f$. (Nach dem ersten Punkt enthält $K$ sogar alle Nullstellen.) Wir wissen bereits aus Satz 6.3.1.2, dass $K$ genau aus den Nullstellen von $x^{p^n} - x$ besteht. Als Minimalpolynom von $\alpha$ teilt $f$ jedes Polynom, das $\alpha$ als Nullstelle hat, insbesondere also $x^{p^n} - x$.

3. Das Polynom $x^{p^n} - x$ hat keine mehrfachen Nullstellen, daher auch nicht sein Teiler $f$.

4. Sei $f \in P[x]$ ein irreduzibles (und normiertes) Polynom vom Grad $k$, das $x^{p^n} - x$ teilt. Im Körper $K$ zerfällt $f$ daher in Linearfaktoren. Sei $\alpha \in K$ eine Nullstelle von $f$. Dann folgt $P(\alpha) \cong P[x]/(f) \cong \mathrm{GF}(p^k)$ aus Satz 6.1.3.4. Weil es sich bei $P(\alpha)$ um einen Unterkörper von $K \cong \mathrm{GF}(p^n)$ handelt, erhalten wir $k|n$ gemäß Satz 6.3.2.4.

   Sei nun umgekehrt $f \in P[x]$ ein irreduzibles (und normiertes) Polynom vom Grad $k|n$. Nach dem ersten Punkt (angewandt auf $k$ anstatt $n$) gilt $f|x^{p^k} - x$. Wegen Lemma 6.3.2.1 gilt $x^{p^k} - x|x^{p^n} - x$, sodass insgesamt $f|x^{p^n} - x$ folgt.

   Schließlich bemerken wir, dass die Vielfachheit aller irreduzibler normierter Faktoren von $x^{p^n} - x$ genau 1 sein muss, da $x^{p^n} - x$ nach Lemma 6.3.1.4 in seinem Zerfällungskörper (also $K$) nur einfache Nullstellen hat.

□

Der Körper $K \cong \mathrm{GF}(p^n)$ wird also von der Nullstelle eines beliebigen irreduziblen Polynoms über dem Primkörper, das Grad $n$ hat, erzeugt – man beachte, dass es sich dabei um das Erzeugnis als Körper handelt. Tatsächlich kann man dies für gewisse Polynome auf das Erzeugnis in der multiplikativen Gruppe verstärken.

**Definition 6.3.3.2.** Sei $f \in \mathbb{Z}_p[x]$ ein irreduzibles Polynom vom Grad $n$. Das Polynom heißt *primitiv*[12], wenn $f$ eine Nullstelle $\alpha \in \mathrm{GF}(p^n)$ hat, die die multiplikative Gruppe

[12] Achtung: Dieser Begriff eines primitiven Polynoms ist zu unterscheiden von jenem mit dem gleichem Namen aus Abschnitt 5.3.2, als es um Polynome über faktoriellen Ringen ging.

$\mathrm{GF}(p^n)^\times = \mathrm{GF}(p^n) \setminus \{0\}$ erzeugt, d.h. $\mathrm{GF}(p^n)^\times = \{\alpha^j \mid j \in \mathbb{N}\}$ (äquivalent: wenn jede Nullstelle von $f$ die multiplikative Gruppe erzeugt; siehe Übungsaufgabe 6.3.3.3).

**UE 373** ► **Übungsaufgabe 6.3.3.3.** (F) Zeigen Sie: Ein Polynom $f \in \mathbb{Z}_p[x]$ vom Grad $n$ ist genau dann primitiv, wenn *jede* Nullstelle $\alpha \in \mathrm{GF}(p^n)$ von $f$ die multiplikative Gruppe von $\mathrm{GF}(p^n)$ erzeugt. ◄ **UE 373**
Äquivalent: Wenn $f \in \mathbb{Z}_p[x]$ primitiv vom Grad $n$ ist und $\alpha \in \mathrm{GF}(p^n)$ eine Nullstelle von $f$ ist, dann gilt $\mathrm{GF}(p^n)^\times = \{\alpha^j \mid j = 0, \ldots, p^n - 2\} = \{\alpha^j \mid j = 1, \ldots, p^n - 1\}$.

Will man einen endlichen Körper explizit konstruieren bzw. beschreiben, so sind primitive Polynome sehr nützlich; siehe Unterabschnitt 6.3.4.

**Lemma 6.3.3.4.** *Zu jedem $n \geq 1$ gibt es mindestens ein primitives (insbesondere also ein irreduzibles) Polynom vom Grad $n$.*

*Beweis.* Nach Satz 6.2.5.1 ist die ($(p^n - 1)$-elementige) multiplikative Gruppe $\mathrm{GF}(p^n)^\times$ zyklisch, wird also von einem $\alpha \in \mathrm{GF}(p^n)^\times$ erzeugt, d.h. $\mathrm{GF}(p^n)^\times = \{\alpha^j \mid j = 0, \ldots, p^n - 2\}$. Sei $f \in \mathbb{Z}_p[x]$ das Minimalpolynom über $\mathbb{Z}_p$ von $\alpha$. Da $\alpha$ jedenfalls den Körper $\mathrm{GF}(p^n)$ erzeugt, also $\mathrm{GF}(p^n) = \mathbb{Z}_p(\alpha)$, schließen wir aus Satz 6.1.3.4, dass $n = [\mathrm{GF}(p^n) : \mathbb{Z}_p] = [\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = \mathrm{grad}(f)$. Somit haben wir das gesuchte Polynom gefunden. □

Bemerkenswert ist auch die folgende Betrachtung der Automorphismen eines endlichen Körpers, die auf die Galoistheorie (siehe Kapitel 9) vorausweist.

**Proposition 6.3.3.5.** *Sei $n \in \mathbb{N}$ mit $n \geq 1$, $p$ eine Primzahl, $K \cong \mathrm{GF}(p^n)$ ein Körper mit $p^n$ Elementen und $P \cong \mathbb{Z}_p$ der Primkörper von $K$. Dann gilt:*

1. *Ist $f$ irgendein irreduzibles Polynom über $P$ vom Grad $n$ und sind $\alpha_1, \ldots, \alpha_n \in K$ die Nullstellen von $f$ (nach Proposition 6.3.3.1 paarweise verschieden), so permutiert jeder Automorphismus $\varphi\colon K \to K$ die Elemente $\alpha_1, \ldots, \alpha_n$. Zu jedem $i = 1, \ldots, n$ gibt es genau einen Automorphismus $\varphi_i$ von $K$ mit $\varphi_i : \alpha_1 \mapsto \alpha_i$.*
2. *Es gibt genau $n$ Automorphismen von $K \cong \mathrm{GF}(p^n)$.*

*Beweis.*

1. Wir schreiben $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ mit $a_0, \ldots, a_{n-1} \in P$. Wegen Proposition 6.1.1.4 hält $\varphi$ die Elemente des Primkörpers punktweise fest. Insbesondere gilt $\varphi(a_j) = a_j$ für alle $j = 0, \ldots, n-1$. Daraus folgt
$$\begin{aligned} f(\varphi(\alpha_i)) &= \varphi(\alpha_i)^n + a_{n-1}\varphi(\alpha_i)^{n-1} + \cdots + a_0 \\ &= \varphi(\alpha_i^n) + \varphi(a_{n-1})\varphi(\alpha_i^{n-1}) + \cdots + \varphi(a_0) \\ &= \varphi(\alpha_i^n + a_{n-1}\alpha_i^{n-1} + \cdots + a_0) = \varphi(f(\alpha_i)) = \varphi(0) = 0, \end{aligned}$$
also $\varphi(\alpha_i) \in \{\alpha_1, \ldots, \alpha_n\}$. Als Automorphismus ist $\varphi$ und damit auch die Einschränkung auf $\{\alpha_1, \ldots, \alpha_n\}$ jedenfalls injektiv. Da diese Menge endlich ist, folgt, dass die Einschränkung eine Permutation von $\{\alpha_1, \ldots, \alpha_n\}$ ist.

Um die zweite Aussage zu zeigen, bemerken wir, dass es für jedes $i = 1, \ldots, n$ nach Satz 6.1.3.4 genau einen Isomorphismus $\varphi_i : P(\alpha_1) \to P(\alpha_i)$ gibt, der $P$ punktweise festlässt und $\alpha \mapsto \alpha_i$ leistet. Nach Proposition 6.3.3.1 gilt $P(\alpha_1) = K = P(\alpha_i)$. Folglich ist $\varphi_i$ ein Automorphismus von $K$. Da jeder Automorphimus von $K$ den Primkörper $P$ jedenfalls festhalten muss, ist $\varphi_i$ sogar der eindeutige Automorphismus von $K$ mit $\alpha_1 \mapsto \alpha_i$.

2. Sei $f \in P[x]$ ein irreduzibles Polynom vom Grad $n$ und seien $\alpha_1, \ldots, \alpha_n \in K$ die Nullstellen von $K$. Im ersten Punkt haben wir bereits $n$ verschiedene Automorphismen gefunden, nämlich die eindeutigen Automorphismen $\varphi_i$, die $\alpha_1 \mapsto \alpha_i$ leisten. Es bleibt zu zeigen, dass es keine weiteren Automorphismen geben kann. Nach Proposition 6.3.3.1 gilt $P(\alpha_1) = K$, sodass ein Automorphismus von $K$ durch das Bild von $\alpha_1$ eindeutig bestimmt ist (da die Elemente des Primkörpers jedenfalls punktweise festgehalten werden müssen). Wieder wegen des ersten Punktes kommen als Bilder nur $\alpha_1, \ldots, \alpha_n$ infrage, also sind $\varphi_1, \ldots, \varphi_n$ tatsächlich die einzigen Automorphismen. □

Die letzte Proposition liefert theoretisch auch eine explizite Beschreibung aller Automorphismen eines endlichen Körpers. Viel praktischer ist aber der folgende Satz:

**Satz 6.3.3.6.** *Die Automorphismen von* $\mathrm{GF}(p^n)$ *sind genau die Abbildungen der Form* $a \mapsto a^{p^k}$ *mit* $k = 0, 1, \ldots, n-1$ *(die sogenannten* Frobeniusautomorphismen*). Sie bilden eine zyklische Gruppe, die vom Automorphismus* $a \mapsto a^p$ *erzeugt wird.*

**UE 374** ► **Übungsaufgabe 6.3.3.7.** (W) Beweisen Sie Satz 6.3.3.6, indem Sie folgendes zeigen: ◄ **UE 374**

1. Ist $p$ eine Primzahl, $k, n \in \mathbb{N}$, $n \geq 1$, so ist die Abbildung $\varphi : a \mapsto a^p$ ein Automorphismus von $\mathrm{GF}(p^n)$.

2. Die in der Automorphismengruppe $\mathrm{Aut}(\mathrm{GF}(p^n))$ von $\varphi$ erzeugte Untergruppe besteht aus allen $\varphi^k : a \mapsto a^{p^k}$ mit $k = 0, \ldots, n-1$.[13] Dabei sind die $\varphi^k$ für $k = 0, \ldots, n-1$ paarweise verschieden. Wieso ist damit der Beweis abgeschlossen?

Bei unendlichen Körpern hingegen kann es auch Automorphismen geben, die keine Frobeniusautomorphismen sind:

**UE 375** ► **Übungsaufgabe 6.3.3.8.** (B) Sei $p$ eine Primzahl. Finden Sie einen Körper $K$ der Charakteristik $p$ und einen nichttrivialen Automorphismus $f\colon K \to K$, der nicht von der Form $f(a) = a^{p^k}$ ist. (Hinweis: Finden Sie zunächst einen nichttrivialen Automorphismus des Rings $\mathbb{Z}_p[x, y]$.) ◄ **UE 375**

Umgekehrt kann $a \mapsto a^p$ bei unendlichen Körpern ein Automorphismus sein, muss es aber nicht.

[13] Mit $a^{p^k}$ ist natürlich $a^{(p^k)}$ gemeint, nicht $(a^p)^k = a^{pk}$.

**UE 376** ► **Übungsaufgabe 6.3.3.9.** (B) Geben Sie einen unendlichen Körper $K$ der Charakteristik $p$ an, für den die Abbildung $a \mapsto a^p$ einen Automorphismus von $K$ definiert. (Hinweis: algebraischer Abschluss) ◄ **UE 376**

**UE 377** ► **Übungsaufgabe 6.3.3.10.** (B) Geben Sie einen unendlichen Körper $K$ der Charakteristik $p$ an, für den die Abbildung $a \mapsto a^p$ *keinen* Automorphismus von $K$ definiert. ◄ **UE 377**

**UE 378** ► **Übungsaufgabe 6.3.3.11.** (F) Sei $K$ endlicher Körper, $P$ der Primkörper von $K$. Zeigen Sie, dass es einen Automorphismus $\varphi$ von $K$ gibt mit $\{x \in K \mid \varphi(x) = x\} = P$. ◄ **UE 378**

**UE 379** ► **Übungsaufgabe 6.3.3.12.** (F) Sei $K$ ein Körper der Charakteristik $p > 0$. Man zeige: $x^p + a \in K[x]$ ist entweder irreduzibel, oder $p$-te Potenz eines linearen Polynoms. ◄ **UE 379**

### 6.3.4 Konstruktion endlicher Körper

Inhalt in Kurzfassung: Wir wissen bereits, dass jeder endliche Körper $K$ der Kardinalität $p^n$, $p \in \mathbb{P}$, $n \in \mathbb{N}^+$, als Zerfällungskörper des Polynoms $x^{p^n} - x$ über seinem Primkörper $P \cong \mathbb{Z}_p$ bis auf Isomorphie eindeutig bestimmt ist. Was also soll es heißen, wenn von der „Konstruktion“ von $K$ die Rede ist? Weil $K$ ein Vektorraum über $P$ ist, entpuppt sich seine additive Struktur sehr schnell als die direkte Summe $C_p \oplus \ldots \oplus C_p$ von $n$ Kopien der zyklischen Gruppe $C_p$ mit $p$ Elementen. Ähnlich ist die multiplikative Gruppe für sich wegen Satz 6.2.5.1 als zyklische Gruppe $\cong C_{p^n-1}$ ebenfalls bereits geklärt. Um mit diesen Darstellungen effektiv zu arbeiten, ist allerdings für die additive Struktur eine Basis von $K$ über $P$ gefragt, für die multiplikative hingegen ein primitives Element, d.h. ein erzeugendes Element der multiplikativen Gruppe. Ein Zusammenhang der beiden ist zunächst aber noch nicht sichtbar. In Hinblick auf eine algorithmische Bewältigung der Körperstruktur von entscheidendem Wert ist daher eine Art „Übersetzungstabelle“. Dafür genügt es, für ein (durch eine multiplikative Eigenschaft definiertes) primitives Element auch die Darstellung seiner Potenzen bezüglich einer Basis der Vektorraumstruktur anzugeben. Wir untersuchen im Folgenden, wie das mit Hilfe der mittlerweile entwickelten Strukturtheorie gelingt. Als Beispiel wird ein Körper mit $9 = 3^2$ Elementen konstruiert.

Jeder endliche Körper $K$ ist isomorph zu einem $\mathrm{GF}(p^n)$ und somit ein $n$-dimensionaler Vektorraum über dem Primkörper $P \cong \mathbb{Z}_p$. Folglich ist die additive Gruppe isomorph zu $(C_p)^n$, der direkten Summe von $n$ Kopien der zyklischen Gruppe $C_p$. Auch die multiplikative Struktur von $\mathrm{GF}(p^n)$ ist sehr einfach. $\mathrm{GF}(p^n)^*$ ist nämlich wegen Satz 6.2.5.1 isomorph zu $C_{p^n-1}$, der zyklischen Gruppe der Ordnung $p^n - 1$. Für endliche Körper kennen wir also sowohl die additive als auch die multiplikative Struktur vollständig. Dennoch ist damit aber noch nicht geklärt, wie additive und multiplikative Struktur zusammenspielen. Auskunft darüber bietet die Theorie, indem sie sagt, dass ein Körper

$K \cong \mathrm{GF}(p^n)$, $p \in \mathbb{P}$, $n \in \mathbb{N}^+$ über dem Primkörper $P := \mathbb{Z}_p$ als Faktorring $\mathbb{Z}_p[x]/(f)$ mit einem irreduziblen Polynom $f \in \mathbb{Z}_p$ vom Grad $n$ erhalten werden kann. Aus Lemma 6.3.3.4 wissen wir, dass es so ein $f$ gibt, auch ein primitives. Exemplarisch soll nun GF(9) konstruiert werden.

**Beispiel 6.3.4.1.** Bestimmung von $K = \mathrm{GF}(9) = \mathrm{GF}(3^2)$: Wir nehmen $\mathbb{Z}_3 = \{0, 1, 2\}$ als Primkörper. Das Polynom $x^2-x-1 \in \mathbb{Z}_3[x]$ ist irreduzibel, da es in $\mathbb{Z}_3$ keine Nullstelle hat. Somit ist $\mathbb{Z}_3[x]/(x^2 - x - 1) \cong \mathbb{Z}_3(\alpha) = \mathrm{GF}(9)$, wobei $\alpha^2 = \alpha + 1$ gilt. Daraus folgt auch $\alpha^3 = \alpha\alpha^2 = \alpha(\alpha + 1) = \alpha^2 + \alpha = \alpha + 1 + \alpha = 1 + 2\alpha$ etc. Es ist $[\mathrm{GF}(9) : \mathbb{Z}_3] = 2$, und eine Basis ist gegeben durch $\{1, \alpha\}$. Wir berechnen nun die Elemente von GF(9) sowie deren Koordinatendarstellung in der Basis $\{1, \alpha\}$:

| Elemente | Koordinatendarstellung |
|---|---|
| $0$ | $(0, 0)$ |
| $\alpha^0 = 1$ | $(1, 0)$ |
| $\alpha^1 = \alpha$ | $(0, 1)$ |
| $\alpha^2 = 1 + \alpha$ | $(1, 1)$ |
| $\alpha^3 = 1 + 2\alpha$ | $(1, 2)$ |
| $\alpha^4 = 2$ | $(2, 0)$ |
| $\alpha^5 = 2\alpha$ | $(0, 2)$ |
| $\alpha^6 = 2 + 2\alpha$ | $(2, 2)$ |
| $\alpha^7 = 2 + \alpha$ | $(2, 1)$ |
| $\alpha^8 = 1$ | $(1, 0)$ |

Hier sind die Potenzen $\alpha^j$, $0 \leq j < 8$, alle verschieden, $\alpha$ ist also ein primitives Element von GF(9) und $x^2 - x - 1$ ein primitives Polynom in $\mathbb{Z}_3[x]$.
Damit können die Operationstafeln nach folgenden Regeln angegeben werden.

- Multiplikation: $0 \cdot \alpha^i = \alpha^i \cdot 0 = 0$, $\alpha^i\alpha^j = \alpha^{(i+j) \bmod 8}$ ($(\mathrm{GF}(9) \setminus \{0\}, \cdot)$ ist eine zyklische Gruppe).

- Addition: zum Beispiel

$$\begin{array}{ccccc} \alpha^2 & + & \alpha^4 & = & ? \\ \downarrow & & \downarrow & & \\ (1,1) & + & (2,0) & = & (0,1) \\ \downarrow & & \downarrow & & \downarrow \\ \alpha^2 & + & \alpha^4 & = & \alpha \end{array}$$

In diesem Beispiel haben wir davon profitiert, dass das Polynom $f(x) = x^2 - x - 1$, nach dem wir den Polynomring faktorisiert haben, primitiv ist. Doch ist nicht jedes irreduzible Polynom primitiv, wie wir uns nun anhand des obigen Beispiels mit $p = 3$ und $n = 2$ überlegen wollen. Und zwar gibt es über $\mathbb{Z}_3$ neun normierte quadratische Polynome (der lineare und der konstante Koeffizient können beliebig gewählt werden). Von ihnen sind sechs als Produkte der drei normierten linearen Polynome $x$, $x + 1$ und $x + 2$ reduzibel, die restlichen drei müssen irreduzibel sein. Schnell findet man, dass es

sich dabei neben $f_1(x) := f(x) = x^2 - x - 1$ um die beiden Polynome $f_2(x) := x^2 + x - 1$ und $f_3(x) := x^2 + 1$ handelt.
Nimmt man oben statt $f = f_1$ das Polynom $f_2$ für die Konstruktion von GF(9), so verläuft alles ganz analog wie mit $f_1$, weil sich auch $f_2$ als primitiv erweist. Mit $f_3(x) = x^2+1$ jedoch erhält man für jede Nullstelle $\alpha$ die Beziehung $\alpha^2 = -1$ und somit $\alpha^4 = 1$. Bezeichnen wir eine Nullstelle von $f_3$ mit $\alpha$, so ist die zweite Nullstelle gegeben durch $-\alpha = \alpha^3 = 2\alpha$. Die Nullstellen von $f_3$ können also keine primitiven Elemente in GF(9) sein, daher ist auch $f_3$ kein primitives Polynom. Jedoch muss z.B. das Element $\beta := \alpha+1$ (genauso könnte man $\alpha+2$, $2\alpha+1$ oder $2\alpha+2$ nehmen) ein primitives sein, weil es nicht in der von $\alpha$ erzeugten multiplikativen Gruppe liegt. Tatsächlich rechnet man sofort $\beta^2 = (\alpha+1)^2 = \alpha^2 + 2\alpha + 1 = -1 + 2\alpha + 1 = 2\alpha$ etc. nach, woraus man ebenfalls eine Übersetzung zwischen den Potenzen von $\beta$ und den Koordinatendarstellungen bezüglich der Basis $\{1, \alpha\}$ gewinnen kann. Die genaue Ausführung dieses Programms ist eine lehrreiche Übungsaufgabe:

**UE 380 ► Übungsaufgabe 6.3.4.2.** (B) Finden Sie mehrere Darstellungen von GF(9) samt Isomorphismen zwischen denselben, indem Sie wie folgt vorgehen: **◄ UE 380**

(1) Konstruieren Sie GF(9) mit Hilfe von $f_2$.
(2) Konstruieren Sie GF(9) mit Hilfe von $f_3$.
(3) Geben Sie Isomorphismen zwischen den drei Darstellungen von GF(9), die vermittels der irreduziblen Polynome $f_1$ (weiter oben) sowie $f_2$ und $f_3$ (als erster und zweiter Teil dieser Aufgabe) gefunden worden sind.

Eine weitere Möglichkeit der Konstruktion besteht darin, auch die Multiplikation direkt im Faktorring $\mathbb{Z}_p/(f)$ für ein irreduzibles (jetzt nicht unbedingt primitives) Polynom $f \in \mathbb{Z}_p[x]$ vom Grad $n$ durchzuführen, d.h. man multipliziert zwei Repräsentanten und reduziert anschließend modulo $f$. Beispielsweise kann man in $\mathbb{Z}_3/(x^2 - x - 1)$

$$\begin{aligned}(x + 1 + (x^2 - x - 1)) \cdot (2x + 1 + (x^2 - x - 1)) &= 2x^2 + 1 + (x^2 - x - 1) \\ &= 2(x + 1) + 1 + (x^2 - x - 1) = 2x + (x^2 - x - 1)\end{aligned}$$

berechnen (dies entspricht der Rechnung $\alpha^2 \cdot \alpha^3 = \alpha^5$ in der Konstruktion aus Beispiel 6.3.4.1). Etwas schwieriger ist die Bestimmung der multiplikativen Inversen von, sagen wir, $s+(f) \neq 0+(f)$. Wenn $s$ konstant ist, d.h. $s \in \mathbb{Z}_p$, dann können wir $s^{-1}$ in $\mathbb{Z}_p$ berechnen und die Inverse ist gegeben durch $s^{-1} + (f)$. Wenn $s$ zumindest Grad 1 hat, dann gelingt die Berechnung mit dem Euklidischen Algorithmus: Da $f$ irreduzibel und $s$ kein Vielfaches von $f$ ist, gilt $\mathrm{ggT}(s, f) = 1$. Der Euklidische Algorithmus, angewendet in $\mathbb{Z}_p[x]$, liefert Polynome $a, b \in \mathbb{Z}_p[x]$ mit $as + bf = 1$. Multiplizieren gemäß

$$(a + (f)) \cdot (s + (f)) = 1 - bf + (f) = 1 + (f)$$

zeigt $(s + (f))^{-1} = a + (f)$ (möglicherweise kann man in $a + (f)$ noch reduzieren).

**UE 381** ▶ **Übungsaufgabe 6.3.4.3.** (B) Konstruieren Sie einen Körper mit 8 Elementen nach dem Vorbild der Konstruktion von GF(9) weiter oben. Wenn Sie dazu das Polynom $f$ über dem Körper $P$ benutzt haben, berechnen Sie weiters das Inverse von $x + (f)$ in $P/(f)$ mit dem Euklidischen Algorithmus. ◀ **UE 381**

**UE 382** ▶ **Übungsaufgabe 6.3.4.4.** (F) Bestimmen Sie die Anzahl der normierten irreduziblen Polynome vom Grad 2 über $\mathrm{GF}(q) = \mathrm{GF}(p^n)$ mit $p \in \mathbb{P}$ und $n \in \mathbb{N}^+$. ◀ **UE 382**

**UE 383** ▶ **Übungsaufgabe 6.3.4.5.** (A) (Alternativer Beweis der Eindeutigkeit von $\mathrm{GF}(p^n)$. Wir verwenden, dass $\mathrm{GF}(p^n)$ Zerfällungskörper von $x^{p^n} - x$ ist, aber nicht den Satz über die Eindeutigkeit des Zerfällungskörpers.)
Seien $K_1$ und $K_2$ endliche Körper der Kardinalität $p^n$, wobei die multiplikative Gruppe von $K_1$ von $\alpha$ erzeugt wird; sei $q(x)$ das Minimalpolynom von $\alpha$. Zeigen Sie, dass $q(x)$ eine Nullstelle in $K_2$ hat und schließen Sie $K_1 \cong K_2$.
Hinweis: $x^{p^n} - x$ zerfällt über dem Primkörper in irreduzible Faktoren; $\alpha$ ist Nullstelle in $K_1$ eines solchen Faktors. ◀ **UE 383**

### 6.3.5 Der algebraische Abschluss eines endlichen Körpers

Inhalt in Kurzfassung: Für festes $p \in \mathbb{P}$ haben alle endlichen Körper der Charakteristik $p$ (bis auf Isomorphie) denselben algebraischen Abschluss. Dieser lässt sich als direkter Limes endlicher Körper realisieren.

Es lohnt, die nachfolgende Konstruktion im Lichte von Abschnitt 2.3.4 zu betrachten. Und zwar untersuchen wir zu gegebenem $p \in \mathbb{P}$ das System der endlichen Körper $K_n := \mathrm{GF}(p^n)$ mit Charakteristik $p$. Da sich $K_m$ nur dann als Unterkörper von $K_n$ auffassen lässt, wenn $m|n$ gilt, ist Satz 2.3.4.2 nur nach einer kleinen (notationelltechnischen) Änderung anwendbar. Dazu betrachten wir nur die Körper $K_{n!} = \mathrm{GF}(p^{n!})$ für $n = 1, 2, \ldots$. Indem wir gemäß isomorpher Einbettungen identifizieren, erhalten wir eine aufsteigende Kette:

$$\mathrm{GF}(p) \leq \mathrm{GF}(p^2) \leq \mathrm{GF}(p^6) \leq \mathrm{GF}(p^{24}) \leq \mathrm{GF}(p^{120}) \leq \cdots$$

Die Vereinigung aller dieser Körper bezeichnen wir mit $\mathrm{GF}(p^\infty)$. Offenbar ist $\mathrm{GF}(p^\infty)$ ein unendlicher Körper. Für jede Zahl $k \geq 1$ gilt $\mathrm{GF}(p^k) \leq \mathrm{GF}(p^{k!}) \leq \mathrm{GF}(p^\infty)$, also enthält $\mathrm{GF}(p^\infty)$ alle endlichen Körper der Charakteristik $p$.

**Satz 6.3.5.1.** *Der unendliche Körper* $\mathrm{GF}(p^\infty)$ *der Charakteristik* $p \in \mathbb{P}$ *ist ein algebraischer Abschluss jedes seiner Unterkörper und damit isomorph zum algebraischen Abschluss jedes endlichen Körpers der Charakteristik* $p$.

*Beweis.* Jedes irreduzible $f$ über $P := \mathbb{Z}_p$ zerfällt in $\mathrm{GF}(p^n)$ mit $n = \mathrm{grad}(f)$, also erst recht in $\mathrm{GF}(p^\infty)$. Also enthält $\mathrm{GF}(p^\infty)$ einen Zerfällungskörper $Z$ von $P[x]$, der nach

Definition mit dem algebraischen Abschluss von $P$ übereinstimmt. Weil jedes $\mathrm{GF}(p^n)$ endlichdimensional und somit algebraisch über dem Primkörper $P$ ist, ist $\mathrm{GF}(p^\infty)$ als Vereinigung aller $\mathrm{GF}(p^n)$ ebenfalls algebraisch über $P$. Deshalb muss gemäß Proposition 6.2.2.4 der Körper $\mathrm{GF}(p^\infty)$ selbst bereits der algebraische Abschluss von $P$ wie auch von sämtlichen $\mathrm{GF}(p^n)$ sein. Da jeder endliche Körper der Charakteristik $p$ isomorph ist zu einem $\mathrm{GF}(p^n)$, ist damit der Satz bewiesen. □

# 7 Vertiefung der Modultheorie

In diesem Kapitel greifen wir das Thema von Abschnitt 3.3 wieder auf. Zur Einstimmung beginnen wir zwecks Motivation mit einer Rekapitulation bekannter Tatsachen.
Die Theorie der Vektorräume und ihrer strukturverträglichen Abbildungen, nämlich der linearen, ist Gegenstand der Linearen Algebra. Von den wichtigen algebraischen Strukturen haben Vektorräume $V$ über einem Körper $K$ die einfachste Strukturtheorie: Ist $K$ vorgegeben, so ist die Dimension nicht nur eine Invariante (je zwei isomorphe Vektorräume haben dieselbe Dimension), sondern auch umgekehrt: Je zwei Vektorräume derselben Dimension über $K$ sind isomorph.
Im vorliegenden Kapitel beschäftigen wir uns mit der nächst allgemeineren Klasse algebraischer Strukturen. Sie entsteht im Wesentlichen dadurch, dass man die Forderung, $K$ sei ein Körper, abschwächt. Verlangt man lediglich einen Ring $R$ (mit oder ohne Einselement) bei sinngemäßer Beibehaltung aller anderen Forderungen, so erhält man die Klasse der Moduln $A$ über $R$. Im Falle eines Einselementes $1_R \in R$ mit $1_R a = a$ für alle $a \in A$ spricht man von unitären Moduln über $R$. Die strukturverträglichen Abbildungen heißen $R$-Modulhomomorphismen. Man beachte, dass stets auch die abelschen Gruppen mit den Gruppenhomomorphismen sich in diesen Rahmen einfügen, nämlich als unitäre Moduln über dem Ring $\mathbb{Z}$. Um lästige Komplikationen zu vermeiden, werden wir uns, wenn nicht anders vermerkt, auf unitäre Moduln über Ringen mit 1 beschränken.
Wir beginnen mit wichtigen Beispielen, den Prüfergruppen und den $p$-adischen Zahlen samt einigem Drumherum zum Aufwärmen (7.1). Der darauf folgende Abschnitt (7.2) beschäftigt sich mit grundlegenden Themen der allgemeinen Strukturtheorie der Moduln wie der Frage, wie weit sich das Konzept der Dimension auf Moduln übertragen lässt. Als äußerst nützlich für die Strukturanalyse von Moduln erweisen sich exakte Sequenzen. Das zeigt sich bereits in Abschnitt 7.3 über projektive und injektive Moduln. Unter den abelschen Gruppen (aufgefasst als $\mathbb{Z}$-Moduln) sind die projektiven genau die freien, die injektiven genau die teilbaren. Der Struktursatz über endlich erzeugte Moduln über Hauptidealringen (bzw. endlich erzeugte abelsche Gruppen) ist Gegenstand von 7.4. Abschnitt 7.5 bildet den Abschluss des Kapitels und beschäftigt sich mit Verallgemeinerungen rund um das aus der Linearen Algebra bekannte Konzept des Dualraums. Ist $R$ nicht kommutativ erfordert das die Unterscheidung von Links-, Rechts- und Bimoduln, was einige technische Komplikationen zur Folge hat.

## 7.1 Wichtige Beispiele: Prüfergruppen und $p$-adische Zahlen

Die $p$-Prüfergruppe $C_{p^\infty}$, $p \in \mathbb{P}$, lässt sich als multiplikative Untergruppe von $\mathbb{C}$ realisieren. Ihre Elemente sind sämtliche $z \in \mathbb{C}$ mit $z^{p^n} = 1$ für ein positives $n \in \mathbb{N}$. Offenbar ist $C_{p^\infty}$ die Vereinigung zyklischer Gruppen $C_{p_n}$ der Ordnung $p^n$. Gemeinsam erzeugen

alle $C_{p^\infty}$, $p \in \mathbb{P}$, die sogenannte universelle Prüfergruppe, die ihrerseits isomorph ist zur additiven Gruppe $\mathbb{Q}/\mathbb{Z}$. Nach einem Prolog über topologische Algebren (7.1.1) ist die Interpretation der Prüfergruppen als direkte Limiten Gegenstand von 7.1.2. In einem gewissen Sinn dual dazu sind die ganzen $p$-adischen Zahlen $\overline{\mathbb{Z}}_p$, die sich auch als Integritätsbereich mit Quotientenkörper $\overline{\mathbb{Q}}_p$ auffassen lassen, siehe 7.1.3. Das Wesen dieser Dualität wird in 7.1.4 genauer untersucht sowie in 7.1.5 kategorientheoretisch beleuchtet.

### 7.1.1 Prolog über topologische Algebren und insbesondere Gruppen

Viele Objekte in der Mathematik tragen sowohl eine algebraische als auch eine topologische Struktur. Von Interesse ist das insbesondere, wenn diese beiden Strukturen miteinander verträglich sind. Eine naheliegende Definition aus Sicht der Universellen Algebra lautet daher:

**Definition 7.1.1.1.** Sei $\mathfrak{A} = (A, \Omega)$ mit einer Familie $\Omega = (\omega_i)_{i\in I}$ von Operationen $\omega_i : A^{n_i} \to A$ der Stelligkeiten $n_i \in \mathbb{N}$ eine Algebra vom Typ $\tau = (n_i)_{i\in I}$. Außerdem sei eine Topologie $\mathcal{T}$ auf $A$ gegeben und $\mathcal{T}_n$ die Produkttopologie auf $A^n$ für alle $n \in \mathbb{N}$. Dann nennt man $\mathfrak{A}$ eine (universelle) *topologische Algebra*, wenn für alle $i \in I$ die Abbildung $\omega_i$ stetig ist bezüglich der Topologien $\mathcal{T}_{n_i}$ auf $A^{n_i}$ und $\mathcal{T}$ auf $A$.

Üblicherweise spricht man bei einer topologischen Algebra, die gleichzeitig eine Halbgruppe, ein Monoid, eine Gruppe, ein Ring etc. ist, von einer *topologischen Halbgruppe*, einem *topologischen Monoid*, einer *topologischen Gruppe*, einem *topologischen Ring* etc. Doch ist Vorsicht geboten, weshalb wir keine allgemeine Definition dieser Art aussprechen. Denn nicht in allen Fällen, wo algebraische und topologische Struktur zusammentreffen, leistet Definition 7.1.1.1 das Gewünschte: In topologischen Körpern wird die Stetigkeit der multiplikativen Inversenbildung extra gefordert. In Definition 7.1.1.1 ist diese Eigenschaft nicht inkludiert.

**UE 384** ► **Übungsaufgabe 7.1.1.2.** Können Sie einen topologischen Ring finden, der algebraisch sogar ein Körper ist, nicht jedoch ein topologischer Körper? ◄ **UE 384**

Auch bei topologischen Moduln und Vektorräumen ist es üblich, Definition 7.1.1.1 zu verschärfen. Sei also $A$ ein Modul über dem Ring $R$. Von einem topologischen $R$-Modul verlangt man nicht nur die Stetigkeit der einstelligen Abbildungen $a \mapsto ra$ für jedes $r \in R$. Man verlangt, dass neben $A$ (als abelsche topologische Gruppe) auch der Ring $R$ eine Topologie trägt, bezüglich der $R$ ein topologischer Ring ist, und darüber hinaus die Abbildung $(r, a) \mapsto ra$ vom Produktraum $R \times A$ nach $A$ stetig ist.

**UE 385** ► **Übungsaufgabe 7.1.1.3.** Können Sie einen topologischen Ring $R$ und einen $R$-Modul $A$ mit folgenden Eigenschaften finden? $A$ soll eine abelsche topologische Gruppe sein und die Abbildungen $a \mapsto ra$ für jedes $r \in R$ stetig, nicht aber $(r, a) \mapsto ra$ als Abbildung $R \times A \to A$. ◄ **UE 385**

Die insgesamt wohl wichtigste Klasse algebraisch-topologischer Strukturen, die *topologischen Gruppen* entspricht aber der Definition 7.1.1.1, explizit:
Eine Gruppe mit Trägermenge $G$, auf der zusätzlich eine Topologie $\mathcal{T}$ vorliegt, ist genau dann eine topologische Gruppe, wenn sowohl binäre Operation $G \times G \to G$, $(g_1, g_2) \mapsto g_1 g_2$, als auch Inversenbildung $G \to G$, $g \mapsto g^{-1}$, stetig sind. Für das neutrale Element muss nichts extra gefordert werden: Die 0-stellige Funktion $G^0 = \{\emptyset\} \to G$, $\emptyset \mapsto e_G$, ist bezüglich der einzigen Topologie auf der einelementigen Menge $G^0$ jedenfalls stetig.
Hier soll die Theorie topologischer Gruppen nicht breit entwickelt werden. Wir begnügen uns mit einigen, teilweise durch Übungsaufgaben ergänzte Beobachtungen, die sich für unsere Zwecke immer wieder als nützlich erweisen. Elementare Begriffe aus der Topologie werden dabei als bekannt vorausgesetzt.
Aus der Stetigkeit der binären Operation auf einer topologischen Gruppe $G$ folgt sehr leicht die Stetigkeit aller Links- und Rechtstranslationen $\lambda_g : G \to G$, $x \mapsto gx$, bzw. $\rho_g : G \to G$, $x \mapsto xg$. Weil auch ihre Umkehrabbildungen $\lambda_{g^{-1}}$ und $\rho_{g^{-1}}$ stetig sind, handelt es sich um Homöomorphismen. Sowohl durch $\lambda_g$ als auch durch $\rho_g$ wird daher der Umgebungsfilter der Eins (d.h. des neutralen Elements) in den Umgebungsfilter von $g$ übergeführt. Man kann sagen: Eine topologische Gruppe sieht topologisch an jedem Punkt gleich aus. Liegt die algebraische Struktur von $G$ vor, so genügt es für die Kenntnis der Topologie auf $G$, den Umgebungsfilter der 1 zu kennen, oder noch sparsamer: eine Umgebungsbasis der 1. In der Regel werden wir von dieser Einsicht Gebrauch machen und die Topologie einer topologischen Gruppe durch Angabe einer Umgebungsbasis der Eins definieren. Natürlich muss ein Mengensystem $\mathcal{U}$ auf $G$ gewisse Bedingungen erfüllen, damit es eine (dann eindeutig bestimmte) Topologie $\mathcal{T}$ auf $G$ gibt, so dass $G$ bezüglich $\mathcal{T}$ eine topologische Gruppe und $\mathcal{U}$ eine Umgebungsbasis der Eins in $G$ bezüglich $\mathcal{T}$ ist. Mit folgendem Kriterium werden wir bevorzugt arbeiten. Wir schreiben für $g \in G$ und für Teilmengen $U, V \subseteq G$ zur Abkürzung $U^{-1} := \{u^{-1} : u \in U\}$, $UV := \{uv : u \in U,\ v \in V\}$, $gU := \{g\}U$, $Ug := U\{g\}$ etc.

**Proposition 7.1.1.4.** *Sei $G$ eine Gruppe mit neutralem Element $1_G$ und $\mathcal{U}$ ein System von Teilmengen von $G$ mit folgenden Eigenschaften:*

- *(Umgebung der Eins): $1_G \in U$ für alle $U \in \mathcal{U}$.*
- *(Filtereigenschaft): Zu allen $U, V \in \mathcal{U}$ gibt es ein $W \in \mathcal{U}$ mit $W \subseteq U \cap V$.*
- *(Stetigkeit der binären Operation): Zu allen $U \in \mathcal{U}$ gibt es ein $V \in \mathcal{U}$ mit $VV \subseteq U$.*
- *(Stetigkeit der Inversenbildung): Zu allen $U \in \mathcal{U}$ gibt es ein $V \in \mathcal{U}$ mit $V^{-1} \subseteq U$.*

*Dann gilt:*

1. $$\mathcal{T} := \{O \subseteq G : \forall g \in O\ \exists U \in \mathcal{U} : Ug \subseteq O\}$$

   *ist eine Topologie auf $G$.*

2. *Für jedes $g \in G$ ist*
$$\mathcal{U}_g := \{Ug : \ U \in \mathcal{U}\}$$
*eine Umgebungsbasis für $g$.*

3. *$G$ ist bezüglich $\mathcal{T}$ eine topologische Gruppe.*

4. *Ist $\mathcal{U} \subseteq \mathcal{T}$, so auch $\mathcal{U}_g \subseteq \mathcal{T}$ für alle $g \in G$, und*
$$\mathcal{B} := \bigcup_{g \in G} \mathcal{U}_g$$
*ist eine Basis für die Topologie $\mathcal{T}$.*

5. *Die Topologie $\mathcal{T}$ ist genau dann T2 (d.h. eine Hausdorff-Topologie, je zwei verschiedene Punkte besitzen disjunkte Umgebungen), wenn der Schnitt aller $U \in \mathcal{U}$ nur $1_G$ enthält.*

6. *(Stetigkeit der Konjugationen): Zu allen $U \in \mathcal{U}$ und $g \in G$ gibt es ein $V \in \mathcal{U}$ mit $gVg^{-1} \subseteq U$.*

**UE 386** ▶ **Übungsaufgabe 7.1.1.5.** Beweisen Sie Proposition 7.1.1.4. ◀ **UE 386**

Bemerkung: In der letzten Aussage von Proposition 7.1.1.4 kann das Trennungsaxiom T2 auch durch eines der Trennungsaxiome T0, T1, T3 oder T$3\frac{1}{2}$ ersetzt werden.

**UE 387** ▶ **Übungsaufgabe 7.1.1.6.** Rekapitulieren Sie aus der Topologie die Hierarchie der Trennungsaxiome. In topologischen Gruppen sind T0, T1, T2, T3 und T$3\frac{1}{2}$ äquivalent. Zeigen Sie möglichst viele der Implikationen, seien Sie aber nicht frustriert, wenn Ihnen nicht alle Beweise gelingen. ◀ **UE 387**

Wir werden uns mit zwei wichtigen Beispielklassen topologischer Gruppen befassen, den lokalkompakten abelschen Gruppen in 7.1.4 und in der (unendlichdmiensionalen) Galoistheorie mit gewissen Automorphismengruppen, siehe 9.3.4, also speziellen Permutationsgruppen. Als Vorbereitung auf die letzteren sind schon hier ein paar Überlegungen am Platze.
Jede Menge $X$ trägt die diskrete Topologie, die Menge $X^X$ aller Abbildungen von $X$ nach $X$ entsprechend die Produkttopologie, die wir in diesem Kontext auch die Topologie der punktweisen Topologie oder auch die schwache Topologie nennen. Als Rechtfertigung für diese Sprechweise dient die folgende etwas allgemeiner formulierte Tatsache:

**Proposition 7.1.1.7.** *Sind $X_i$, $i \in I$, topologische Räume. Auf dem kartesischen Produkt $X := \prod_{i \in I} X_i$ stimmen folgende drei Topologien überein:*

***Produkttopologie:*** *Das ist jene Topologie auf $X$, für die alle Mengen $[O_{i_0}]$, $O_{i_0}$ offen in $X_{i_0}$, $i_0 \in I$, eine Subbasis bilden. Dabei bezeichnet $[O_{i_0}]$ die Menge aller $(x_i)_{i \in I} \in X$ mit $x_{i_0} \in O_{i_0}$.*

***schwache Topologie:*** *Das ist die schwächste Topologie auf $X$, bezüglich der alle Projektionen $\pi_j : X \to X_j$, $(x_i)_{i\in I} \mapsto x_j$, $j \in I$, stetig sind.*

***Topologie der punktweisen Konvergenz:*** *Das ist jene Topologie auf $X$, bezüglich der ein Netz aus $X$ genau dann gegen $(x_i)_{i\in I}$ konvergiert, wenn für jedes $j \in I$ das Netz der Bilder unter $\pi_j$ gegen $x_j \in X_j$ konvergiert.*

**UE 388 ► Übungsaufgabe 7.1.1.8.** Beweisen Sie Proposition 7.1.1.7. **◄ UE 388**

Im Spezialfall des Produktraumes $X^X$ aller Abbildungen $X \to X$ liegt zusätzlich die binäre Operation der Hintereinanderausführung und somit ein Monoid mit $\mathrm{id}_X$ als neutralem Element vor, das sogenannte symmetrische Monoid auf $X$, siehe auch Definition 3.1.2.4. Für diskretes $X$ ist diese Verknüpfung stetig:

**Proposition 7.1.1.9.** *Ist $X$ eine Menge mit diskreter Topologie. Dann bildet die Menge $X^X$ aller Abbildungen von $X$ nach $X$ bezüglich der Hintereinanderausführung $\circ$ und bezüglich der Produkttopologie ein topologisches Monoid. Dieses erfüllt das Hausdorffsche Trennungsaxiom: Je zwei $f \neq g \in X^X$ haben disjunkte Umgebungen.*
*Die symmetrische Gruppe $S(X)$ (bestehend aus allen bijektiven $f : X \to X$) bildet ein Untermonoid von $X^X$, das sogar eine topologische Gruppe ist.*

*Beweis.* Wir müssen die Stetigkeit von $\circ$ an einer Stelle $(f, g) \in X^X \times X^X$ überprüfen. Sei dazu eine Umgebung $U$ von $f \circ g$ gegeben. Nach Definition der Topologie gibt es eine endliche Menge $E \subseteq X$ derart, dass $U$ sicher all jene $h \in X^X$ enthält, die $h(x) = (f\circ g)(x) = f(g(x))$ für alle $x \in E$ erfüllen. Wir haben Umgebungen $U_f$ von $f$ und $U_g$ von $g$ zu finden mit $f_1 \circ g_1 \in U$ für alle $f_1 \in U_f$ und $g_1 \in U_g$. Die Menge $U_f$, bestehend aus jenen $f_1 \in X^X$, die $f_1(g(x)) = f(g(x))$ für alle $x \in E$ erfüllen, ist eine offene Umgebung von $f$. Analog ist die Menge $U_g$, bestehend aus jenen $g_1 \in X^X$, die $g_1(x) = g(x)$ für alle $x \in E$ erfüllen eine offene Umgebung von $g$. Für alle $x \in E$, $f_1 \in U_f$ und $g_2 \in U_g$ gilt $(f_1 \circ g_1)(x) = f_1(g_1(x)) = f_1(g(x)) = f(g(x))$, also liegt $f_1 \circ g_1$ für $f \in U_f$ und $g \in U_g$ tatsächlich in $U$.
Um zu zeigen, dass auf $S(X)$ auch die Inversenbildung stetig ist, sei $f \in S(X)$ und $U$ eine Umgebung von $f^{-1}$. Wieder gibt es eine endliche Menge $E \subseteq X$ derart, dass $U$ sicher all jene $g \in S(X)$ enthält, die $g(x) = f^{-1}(x)$ für alle $x \in E$ erfüllen. Wir betrachten die Menge $E'$ aller $f^{-1}(x)$ mit $x \in E$. Weil mit $f$ auch $f^{-1}$ bijektiv, insbesondere also injektiv ist, sind diese Elemente paarweise verschieden. All jene $g \in S(X)$, die auf $E'$ mit $f$ übereinstimmen, bilden eine offene Umgebung $V$ von $f$. Jedes solche $g$ hat eine Umkehrabbildung, die auf $E$ mit $f^{-1}$ übereinstimmt, also liegt $g^{-1}$ für $g \in V$ tatsächlich in $U$.
Zur Hausdorffschen Trennungseigenschaft: Sind $f, g \in X^X$ verschieden, so gibt es ein $x \in X$ mit $f(x) \neq g(x)$. $U_f := \{f_1 \in X^X : \ f_1(x) = f(x)\}$ ist eine Umgebung von $f$, $U_g := \{g_1 \in X^X : \ g_1(x) = g(x)\}$ ist eine Umgebung von $g$, und es gilt $U_f \cap U_g = \emptyset$. □

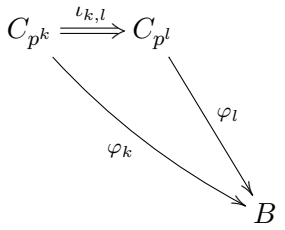
**UE 389** ► **Übungsaufgabe 7.1.1.10.** Zeigen Sie in der Situation von Proposition 7.1.1.9, dass bei unendlichem $X$ die Teilmenge $S(X)$ in $X^X$ nicht abgeschlossen ist. ◄ **UE 389**

Bei der Strukturanalyse topologischer Algebren, insbesondere topologischer Gruppen ist ein Homomorphismus bzw. Isomorphismus der algebraischen Struktur besonders dann von Interesse, wenn es sich zugleich um eine stetige Abbildung bzw. um einen Homöomorphismus, einen sogenannten *topologischen Isomorphismus* handelt.

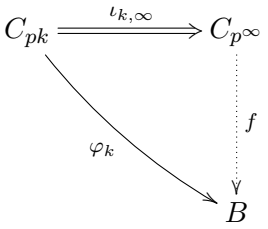
### 7.1.2 Beispiel Prüfergruppe

Beispielsweise bei der Konstruktion von Erweiterungskörpern in Kapitel 6 haben wir aufsteigende Familien ineinander enthaltener, genauer: injektiv ineinander eingebetteter Strukturen betrachtet. Wir wollen die Konstruktion auf ein relativ einfaches, gleichzeitig aber sehr typisches und auch wichtiges Beispiel anwenden, nämlich auf zyklische Gruppen.
Bezeichne wieder $C_n$ die zyklische Gruppe der Ordnung $n$. Wir können uns $C_n$ als Untergruppe der multiplikativen Gruppe aller komplexen Zahlen $z$ vom Betrag $|z| = 1$ vorstellen, nämlich als Gruppe der $n$-ten komplexen Einheitswurzeln.
Sei $p$ eine feste natürliche Zahl.[1] Für beliebige natürliche Zahlen $k \leq l$ ist $C_{p^k}$ somit Untergruppe von $C_{p^l}$. Wir bezeichnen die Inklusionsabbildung mit $\iota_{k,l}$, außerdem die Vereinigung der aufsteigenden Folge $C_p \leq C_{p^2} \leq C_{p^3} \leq \ldots$ mit $C_{p^\infty}$; diese Vereinigung ist offensichtlich eine Gruppe. Für $p$ prim heißt $C_{p^\infty}$ auch *$p$-Prüfergruppe*. Die Inklusionsabbildung von $C_{p^k}$ nach $C_{p^\infty}$ bezeichnen wir mit $\iota_{k,\infty}$. Die $p$-Prüfergruppe ist durch folgende Eigenschaft ausgezeichnet:

**Proposition 7.1.2.1.** *Sei $B$ eine beliebige Gruppe, und sei $(\varphi_k)_{k\in\mathbb{N}}$ eine Familie von Homomorphismen, so dass alle Diagramme*




*kommutieren. (Das heißt, für alle $k < l$ gilt $\varphi_l \circ \iota_{k,l} = \varphi_k$.)*
*Dann gibt es einen eindeutig bestimmten Homomorphismus $f\colon C_{p^\infty} \to B$, so dass alle Diagramme der Form*




[1] Üblicherweise betrachtet man hier vor allem Primzahlen $p$, das ist an dieser Stelle aber nicht relevant.

*kommutieren.*

Ganz analoge Konstruktionen sind möglich, wenn statt aufsteigender $p$-Potenzen irgendeine aufsteigende Teilerfolge natürlicher Zahlen $m_0|m_1|m_2|\dots$ gegeben ist. Die resultierende verallgemeinerte Prüfergruppe bezeichnen wir mit $C_{(m_n)_{n\in\mathbb{N}}}$. Die genaue Untersuchung solcher Gruppen ist Gegenstand der folgenden Übungsaufgabe.

**UE 390 ► Übungsaufgabe 7.1.2.2.** 1. Beweisen Sie Proposition 7.1.2.1. **◄ UE 390**

2. Verwenden Sie Proposition 7.1.2.1, um $C_{p^\infty}$ als universelles Objekt in einer geeigneten Kategorie zu kennzeichnen.

3. Führen Sie die oben angedeutete Konstruktion von $C_{(m_n)_{n\in\mathbb{N}}}$ im Detail durch.

4. Seien $m_0|m_1|m_2|\dots$ und $m'_0|m'_1|m'_2|\dots$ aufsteigende Teilerketten. Finden Sie ein Kriterium dafür, dass $C_{(m_n)_{n\in\mathbb{N}}}$ und $C_{(m'_n)_{n\in\mathbb{N}}}$ isomorph sind.

### 7.1.3 Beispiel $p$-adische Zahlen

Dual zur eben besprochenen Situation einer unendlichen Folge injektiv ineinander eingebetteter Strukturen sind surjektiv aufeinander abgebildete. Auch hier eignen sich zur Illustration zyklische Gruppen als geradezu archetypische Beispiele. Wir verwenden additive Notation und halten wieder eine Primzahl $p$ fest.
Die zyklischen Gruppe $C_{p^{n+1}}$ der Ordnung $p^{n+1}$ lässt sich homomorph auf die zyklische Gruppe $C_{p^n}$ abbilden, etwa indem man eine Restklasse $k + p^{n+1}\mathbb{Z}$ modulo $p^{n+1}$ auf die Restklasse $k + p^n\mathbb{Z}$ modulo $p^n$ abbildet. Es liegt also eine Serie von Epimorphismen $\varphi_n\colon C_{p^{n+1}} \to C_{p^n}$ vor. Im Gegensatz zur Prüfergruppe werden die Gruppen in Richtung der Urbilder größer. Eine natürliche Möglichkeit, die gesamte Serie in ein Objekt zu fassen, besteht also darin, gewissermaßen alle unendlichen Rückwärtspfade als Elemente zu betrachten. Formal lässt sich ihre Gesamtheit als eine Untergruppe des unendlichen direkten Produktes $P = \prod_{n\in\mathbb{N}} C_{p^n}$ auffassen. Wir bezeichnen diese Untergruppe mit $\overline{\mathbb{Z}}_p$ (nicht mit dem endlichen Restklassenring modulo $p$ verwechseln!). Man nennt sie die Gruppe der *ganzen $p$-adischen Zahlen*. Sie tragen auch eine multiplikative Struktur, der wir uns etwas später zuwenden werden. $\overline{\mathbb{Z}}_p$ besteht aus jenen Elementen $(k_n)_{n\in\mathbb{N}} \in P$, die $\varphi_n(k_{n+1}) = k_n$ für alle $n \in \mathbb{N}$ erfüllen.
Es gibt eine sehr ansprechende Darstellung von $\overline{\mathbb{Z}}_p$ bzw. seiner Elemente. Wir fassen dazu jedes $C_{p^{n+1}}$ als Restklassengruppe $\mathbb{Z}/p^{n+1}\mathbb{Z}$ auf, deren Elemente die Gestalt $k + p^{n+1}\mathbb{Z}$ haben. Dabei steht $p^{n+1}\mathbb{Z}$ für den Normalteiler in $\mathbb{Z}$, der aus allen Vielfachen von $p^{n+1}$ besteht. Die ganze Zahl $k$ wird eindeutig, wenn man $0 \le k < p^{n+1}$ fordert. Sei $k = \sum_{i=0}^{n} a_i p^i$ mit $a_i \in \{0, \dots, p-1\}$ die übliche Darstellung von $k$ zur Basis $p$. Dann lässt sich die Wirkung von $\varphi_n$ beschreiben durch

$$\varphi_n : \quad \sum_{i=0}^{n} a_i p^i + p^{n+1}\mathbb{Z} \quad \mapsto \quad \sum_{i=0}^{n-1} a_i p^i + p^n\mathbb{Z}.$$

Der Epimorphismus $\varphi_n$ vergisst also gewissermaßen den Koeffizienten $a_n$. Da alle Wahlen von Folgen $(a_n)_{n\in\mathbb{N}}$ mit $a_n \in \{0,\dots,p-1\}$ sinnvoll sind, kann man die Elemente von $\overline{\mathbb{Z}}_p$ mit diesen Folgen $(a_n)_{n\in\mathbb{N}}$ identifizieren, oder, der arithmetischen Struktur noch besser angepasst, mit den entsprechenden, zunächst nur formalen, unendlichen Summen (Potenzreihen in $p$)[2]

$$\sum_{n=0}^{\infty} a_n p^n.$$

Die Bausteine $C_{p^n}$ von $\overline{\mathbb{Z}}_p$ tragen wie schon angedeutet nicht nur Gruppen-, sondern, vermittels der Darstellung als $\mathbb{Z}/p^n\mathbb{Z}$ mit dem Ideal $p^n\mathbb{Z}$ sogar Ringstruktur. Überdies sind die $\varphi_n$ auch mit der multiplikativen Struktur verträglich. Folglich trägt auch $\overline{\mathbb{Z}}_p$ eine Ringstruktur. Üblicherweise ist diese gemeint, wenn von den *ganzen p-adischen Zahlen* die Rede ist. Wie man sofort nachprüft, ist $\overline{\mathbb{Z}}_p$ sogar ein Integritätsbereich und besitzt daher einen Quotientenkörper $\overline{\mathbb{Q}}_p$, den *Körper der p-adischen Zahlen*. O.B.d.A. wollen wir $\overline{\mathbb{Z}}_p$ als Unterring von $\overline{\mathbb{Q}}_p$ auffassen. Das Element $p = 0p^0 + 1p^1 + 0p^2 + 0p^3 + \ldots \in \mathbb{Z}_p$ besitzt, wie man leicht einsieht, innerhalb $\overline{\mathbb{Z}}_p$ kein multiplikatives Inverses. Folglich liegt $p^{-1}$ in $\overline{\mathbb{Q}}_p \backslash \overline{\mathbb{Z}}_p$, entsprechend auch $p^{-2}$, $p^{-3}$ etc. Da in $\overline{\mathbb{Q}}_p$ beliebige endliche Produkte und Summen gebildet werden können, muss $\overline{\mathbb{Q}}_p$ also wenigstens alle Elemente der Gestalt

$$\sum_{n=-N}^{\infty} a_n p^n \quad (\textit{formale Laurentreihen} \text{ in } p, \text{ Operationen jedoch mit Übertrag})$$

mit $N \in \mathbb{N}$ und $a_n \in \{0,1,\dots,p-1\}$ enthalten. In der Tat überzeugt man sich, dass damit sogar ganz $\overline{\mathbb{Q}}_p$ beschrieben wird.
Wir beschränken uns nochmals kurz auf die ganzen $p$-adischen Zahlen und ihre Darstellung als Potenzreihen in $p$. Offenbar gibt es für alle $n \in \mathbb{N}$ natürliche Homomorphismen $\psi_n \colon \overline{\mathbb{Z}}_p \to \mathbb{Z}/p^n\mathbb{Z}$, nämlich

$$\psi_n : \quad \sum_{i=0}^{\infty} a_i p^i \quad \mapsto \quad \sum_{i=0}^{n-1} a_i p^i + p^n\mathbb{Z},$$

die den Bedingungen $\psi_n = \varphi_n \circ \psi_{n+1}$ für alle $n \in \mathbb{N}$ genügen. Diese Eigenschaft werden wir etwas später als Motivation für den kategorientheoretischen Begriff des indirekten, projektiven oder auch inversen Limes verwenden.
In den Überlegungen, die uns zu den $p$-adischen Zahlen geführt haben, wurden manche Schritte nicht vollständig ausgeführt. Diese, aber auch weitere interessante Eigenschaften und Aspekte der $p$-adischen Zahlen sind Gegenstand der folgenden mehrteiligen und relativ umfangreichen Übungsaufgabe. Teile davon involvieren auch topologische Begriffe, die aber weitgehend im Zuge der Aufgabenstellung erklärt werden.

**UE 391** ► **Übungsaufgabe 7.1.3.1.** In den topologischen Teilen dieser Aufgabe dürfen Sie sich, wenn Sie wollen, auch auf 7.1.1 beziehen. ◄ **UE 391**

[2] Die Bezeichnung als *Potenzreihe* ist hier mit Vorsicht zu genießen. Denn anders als beim Umgang mit Unbestimmten (die wir eher mit $x, y, \ldots$ bezeichnen) wird hier mit Übertrag gerechnet. Der einfacheren Sprechweise halber wollen wir aber an dieser Terminologie festhalten.

(1) Rekapitulieren Sie die Konstruktion des Ringes $\overline{\mathbb{Z}}_p$ der ganzen $p$-adischen Zahlen und beweisen Sie im Zuge dessen, dass die Elemente von $\overline{\mathbb{Z}}_p$ tatsächlich in einer bijektiven Beziehung zu den formalen Potenzreihen in $p$ stehen. Verwenden Sie im Weiteren diese Potenzreihendarstellung als Normalform.

(2) Beschreiben Sie die Operationen im Ring $\overline{\mathbb{Z}}_p$ anhand der Normalform. (Rechnen mit Übertrag, im Gegensatz zum Rechnen mit Potenzreihen in einer Unbestimmten)

(3) Zeigen Sie, dass die im Text definierten Abbildungen $\psi_n$ tatsächlich der Bedingung $\psi_n = \varphi_n \circ \psi_{n+1}$ genügen.

(4) Rekapitulieren Sie die Definition des Quotientenkörpers eines Integritätsbereiches und beweisen Sie, dass speziell die formalen Laurentreihen in $p$ mit Übertrag wie oben angesprochen tatsächlich einen Quotientenkörper von $\overline{\mathbb{Z}}_p$ bilden. (Insbesondere erfordert dies die Beschreibung der Operationen auf $\overline{\mathbb{Q}}_p$ inklusive multiplikativer Inversenbildung.) Verwenden Sie im Weiteren diese Darstellung von Laurentreihen als Normalform.

(5) Die Menge $\overline{\mathbb{Q}}_p$ trägt eine natürliche Topologie $\tau$. Eine topologische Basis ist gegeben durch alle Mengen $B(N, a_{-N}, a_{-N+1}, \ldots, a_0, \ldots, a_{k-1})$ mit $N, k \in \mathbb{N}$ und $a_i \in \{0, 1 \ldots, p-1\}$. Dabei bestehe $B(N, a_{-N}, a_{-N+1}, \ldots, a_0, \ldots, a_{k-1})$ definitionsgemäß aus allen formalen Laurentreihen der Form $\sum_{n=-N}^{\infty} b_n p^n$, $b_n \in \{0, \ldots, p-1\}$, mit $b_i = a_i$ für $i = -N, -N+1, \ldots, 0, 1, \ldots, k-1$. (Anmerkung: Insbesondere gilt $B(0) = \overline{\mathbb{Z}}_p$.)

Sei dazu $\tau$ die Menge aller beliebigen – endlichen oder unendlichen – Vereinigungen von Basismengen $B(N, a_{-N}, a_{-N+1}, \ldots, a_0, \ldots, a_k)$. Zeigen Sie, dass $\tau$ tatsächlich eine Topologie auf $\overline{\mathbb{Q}}_p$ ist. Das bedeutet wiederum nach Definition, dass $\tau$ abgeschlossen ist bezüglich endlicher Durchschnitte und beliebiger Vereinigungen. Insbesondere müssen $\emptyset$ und $\overline{\mathbb{Q}}_p$ in $\tau$ liegen.

(6) Zeigen Sie: Die Topologie $\tau$ aus Teil 5 wird durch eine Metrik $d$ induziert, die sogar Ultrametrik ist, d.h. die der verschärften Dreiecksungleichung $d(x, z) \leq \max\{d(x, y), d(y, z)\}$ genügt. Anleitung: Wählen Sie als Abstand zweier verschiedener formaler Laurentreihen z.B. die positive Zahl $p^{-k}$, sofern $k$ der kleinste Index mit unterschiedlichen Gliedern ist.

(7) Beweisen Sie, dass die Mengen $B(N, a_{-N}, a_{-N+1}, \ldots, a_0, \ldots, a_k)$ bezüglich $\tau$ abgeschlossen und sogar kompakt sind, und folgern Sie daraus, dass $\overline{\mathbb{Z}}_p$ kompakt, $\overline{\mathbb{Q}}_p$ lokalkompakt ist (d.h. jedes Element in $\overline{\mathbb{Q}}_p$ besitzt eine kompakte Umgebung).

Anleitung: Hier soll Kompaktheit auch das Hausdorffsche Trennungsaxiom inkludieren: Je zwei verschiedene Elemente besitzen disjunkte Umgebungen. Dieses folgt aber bereits aus der Metrisierbarkeit (Teil 6). Der interessante Teil ist die Überdeckungseigenschaft (jede offene Überdeckung hat eine offene Teilüberdeckung). Wenn bekannt, können Sie den Satz von Tychonoff (der Produktraum kompakter Räume ist wieder kompakt) einsetzen. Alternativ können Sie beweisen und dann verwenden, dass ein metrischer Raum (nach Teil 6 liegt ein solcher vor) dann (und nur dann) kompakt ist, wenn der Satz von Bolzano-Weierstraß gilt: Jede unendli-

che Teilmenge $A$ hat einen Häufungspunkt. (Definitionsgemäß ist das ein solcher Punkt, zu dem jede Umgebung von diesem verschiedene Punkte von $A$ enthält.)

(8) Zeigen Sie, dass $\tau$ sowohl $\overline{\mathbb{Z}}_p$ als auch $\overline{\mathbb{Q}}_p$ zu 0-dimensionalen und somit total unzusammenhängenden topologischen Räumen macht. (Ein topologischer Raum heißt 0-dimensional, wenn er eine topologische Basis hat, deren Elemente sowohl offen als auch abgeschlossen sind. Total unzusammenhängend bedeutet, dass die einelementigen Teilmengen die einzigen zusammenhängenden sind.)

(9) Zeigen Sie, dass in $\overline{\mathbb{Q}}_p$ Addition, Multiplikation und Inversenbildung (additiv wie multiplikativ) stetig sind. Anleitung: Weil es sich um einen metrischen Raum handelt, kann man mit Folgenstetigkeit arbeiten. Für die Addition beispielsweise genügt es daher zu beweisen: Konvergieren Elemente $q_n, r_n \in \mathbb{Q}_p$ gegen $q$ bzw. $r$, so konvergieren ihre Summen $q_n + r_n$ gegen $q + r$. (Definitionsgemäß besagt die hier zu beweisende Stetigkeit der Operationen, dass $\overline{\mathbb{Q}}_p$ sogar ein topologischer Körper ist, $\overline{\mathbb{Z}}_p$ ein topologischer Ring.)

(10) Zeigen Sie: $\overline{\mathbb{Z}}_p$ ist als topologischer Raum homöomorph zur Cantormenge[3], insbesondere also überabzählbar. Anleitung: Zeigen Sie zunächst den für sich äußerst interessanten Satz, dass jeder nichtleere, total unzusammenhängende und kompakte metrische Raum ohne isolierte Punkte homöomorph zur Cantormenge ist. (Statt total unzusammenhängend dürfen Sie auch 0-dimensional voraussetzen.)

(11) Zeigen Sie: Eine unendliche Reihe $\sum_{n=0}^{\infty} q_n$ $p$-adischer Zahlen $q_n$ ist konvergent (d.h. definitionsgemäß: die Folge der Partialsummen ist konvergent) genau dann, wenn die $q_n$ eine Nullfolge in $\overline{\mathbb{Q}}_p$ bilden.

(12) Bei der Konstruktion von $\overline{\mathbb{Z}}_p$ ist es nur auf die Surjektivität der Homomorphismen $\varphi_n$ angekommen. Da zwischen zwei beliebigen zyklischen Gruppen bzw. Restklassenringen $\mathbb{Z}/(m_i)$ ein Epimorphismus $\varphi\colon \mathbb{Z}/(m_2) \to \mathbb{Z}/(m_1)$ genau dann existiert, wenn $m_1$ ein Teiler von $m_2$ ist, können wir statt der Teilerkette $p^0 \mid p^1 \mid p^2 \mid \ldots$ auch irgendeine andere aufsteigende Teilerkette $1 = m_0 \mid m_1 \mid m_2 \mid \ldots$ in $\mathbb{N}$ betrachten, wobei wir o.B.d.A. $m_i < m_{i+1}$ für alle $i \in \mathbb{N}$ voraussetzen wollen. Der anstelle von $\overline{\mathbb{Z}}_p$ entstehende Ring sei mit $\overline{\mathbb{Z}}_{(m_n)_{n\in\mathbb{N}}}$ bezeichnet.

Untersuchen Sie, welche Aussagen, die bisher über $\overline{\mathbb{Z}}_p$ gemacht wurden, entsprechend auch für $\overline{\mathbb{Z}}_{(m_n)_{n\in\mathbb{N}}}$ gelten und welche falsch werden.

(13) Zeigen Sie: Der Ring $\overline{\mathbb{Z}}_{(m_n)_{n\in\mathbb{N}}}$ lässt sich als direktes Produkt gewisser Ringe $R_p$ darstellen, wobei $p$ alle Primzahlen durchläuft. Dabei ist $R_p$ entweder isomorph zu einem endlichen Restklassenring $\mathbb{Z}/p^n\mathbb{Z}$ oder zum Ring $\overline{\mathbb{Z}}_p$ der ganzen $p$-adischen Zahlen. Erklären Sie auch, wie diese Fälle von $(m_n)_{n\in\mathbb{N}}$ abhängen.

Ebenfalls einen lokalkompakten topologischen Ring bzw. Körper erhält man auf ganz

[3] Betrachten Sie die Cantormenge als die Menge aller reellen Zahlen $x$ der Gestalt $x = \sum_{n=1}^{\infty} \frac{a_n}{3^n}$ mit $a_n \in \{0, 2\}$, ausgestattet mit jener Topologie, die diese Menge als Spurtopologie (Unterraumtopologie) von der natürlichen Topologie auf $\mathbb{R}$ erbt.

ähnliche Weise, wenn man von formalen Potenz- bzw. Laurentreihen

$$\sum_{n=-N}^{\infty} a_n x^n$$

in einer *Unbestimmten* $x$ (statt von Elementen $p$ aus einem vorgegebenen endlichen Ring) ausgeht. Aus ziemlich offensichtlichen Gründen spricht man bei festem $N = 0$ vom Ring $\mathbb{Z}_p[[x]]$ der formalen Potenzreihen über dem Körper $\mathbb{Z}_p = \mathbb{Z}/(p)$ mit $p$ Elementen (siehe auch 3.4.6). Bei variablem $N \in \mathbb{Z}$ lässt sich der resultierende Ring $\mathbb{Z}_p[[[x]]]$ der formalen Laurentreihen als dessen Quotientenkörper auffassen. Topologisch besteht kein Unterschied zu $\overline{\mathbb{Z}}_p$ bzw. $\overline{\mathbb{Q}}_p$, sehr wohl aber algebraisch. Denn mit den Koeffizienten $a_i \in \{0, 1, \ldots, p-1\}$ wird jetzt nicht mit Übertrag gerechnet, sondern modulo $p$. Man hat es also mit Potenz- bzw. Laurentreihen in einer Variablen $x$ im eigentlichen Sinn zu tun. Statt des Primkörpers $\mathbb{Z}_p$ kann man genauso von einem beliebigen endlichen Körper ausgehen.

**UE 392 ► Übungsaufgabe 7.1.3.2.** (1) Welche der Teile von Aufgabe 7.1.3.1 gelten identisch oder wenigstens sinngemäß auch mit $\mathbb{Z}_p[[x]]$ statt mit $\overline{\mathbb{Z}}_p$? **◄ UE 392**

(2) Begründen Sie, warum $\overline{\mathbb{Z}}_p$ und $\mathbb{Z}_p[[x]]$ schon als additive Gruppen und somit erst recht als Ringe nicht isomorph sein können, analog für ihre Quotientenkörper.

(3) Wie verhält es sich mit der Isomorphie der vorkommenden Strukturen bei variierendem $p$?

(4) Wie steht es mit topologischen Homöomorphismen zwischen den betrachteten Strukturen?

Aus Aufgabe 7.1.3.2 ergeben sich zwei unendliche Serien paarweise nicht isomorpher lokalkompakter topologischer Körper: jene der $\overline{\mathbb{Q}}_p$ und jene der $\mathbb{Z}_p[[[x]]]$ mit $p \in \mathbb{P}$. Auch endliche Erweiterungen dieser Körper (siehe Kapitel 6) sind lokalkompakt, ebenso wie klarerweise $\mathbb{R}$ und $\mathbb{C}$. Schließlich sind diskrete Körper trivialerweise lokalkompakt. Denn in der diskreten Topologie sind alle Teilmengen offen, insbesondere ist $\{x\}$ eine kompakte Umgebung eines beliebigen Punktes $x$. Lässt man auch nichtkommutative Körper (Schiefkörper) zu, so kommen noch die Hamiltonschen Quaternionen $\mathbb{H}$ dazu (siehe Übungsaufgabe 1.2.4.10). Ein bemerkenswerter Satz besagt, dass es bis auf topologische Isomorphie keine weiteren Beispiele gibt.
Einige der obigen Erkenntnisse fassen wir knapp zusammen:

**Theorem 7.1.3.3.** Die ganzen $p$-adischen $\overline{\mathbb{Z}}_p$ bilden einen kompakten topologischen Ring, der sogar ein Integritätsbereich ist. Sein Quotientenkörper ist (zusammen mit der kanonischen Einbettung) der lokalkompakte Körper $\overline{\mathbb{Q}}_p$ der $p$-adischen Zahlen.
Ganz analog gilt: Die formalen Potenzreihen $K[[x]]$ über einem endlichen Körper $K$ bilden einen kompakten topologischen Ring, der sogar ein Integritätsbereich ist. Sein Quotientenkörper ist (zusammen mit der kanonischen Einbettung) der lokalkompakte Körper $K[[[x]]]$ der formalen Laurentreihen über $K$.

### 7.1.4 Pontrajaginsche Dualität

Als Motivation, Prüfergruppen und $p$-adische Zahlen unmittelbar hintereinander einzuführen, diente bisher eine gewisse Dualität zwischen injektiven Einbettungen und surjektiven Homomorphismen. Diese Dualität zwischen beiden Objekten lässt sich präzisieren und zeigt noch weitere reizvolle Aspekte. Betrachten wir dazu $C_{p^\infty}$ und $\overline{\mathbb{Z}}_p$ als abelsche Gruppen, die überdies mit Topologien ausgestattet sind, welche sie zu topologischen Gruppen machen. Bei $C_{p^\infty}$ ist das die diskrete Topologie, bei $\overline{\mathbb{Z}}_p$ die kompakte aus Übungsaufgabe 7.1.3.1. Insbesondere handelt es sich in beiden Fällen um lokalkompakte abelsche Gruppen, die sich als dual zueinander im Rahmen der Pontrjaginschen Dualitätstheorie erweisen. Weitgehend ohne Beweise soll nun erklärt werden, was dies bedeutet. Man beachte dabei die Analogie zu (stetigen) linearen Funktionalen auf (topologischen) Vektorräumen, auf die wir uns vergleichsweise beziehen wollen.
In der Pontrjaginschen Dualität tritt an die Stelle des Skalarkörpers (des Wertebereichs der Funktionale) die kompakte Gruppe $\mathbb{T} = \mathbb{R}/\mathbb{Z}$. Die Topologie auf $\mathbb{T}$ ist die Quotiententopologie, in der genau jene Teilmengen $O$ offen sind, deren Urbilder $\kappa^{-1}(O)$ unter der kanonischen Abbildung $\kappa\colon \mathbb{R} \to \mathbb{T}$, $r \mapsto r + \mathbb{Z}$, offen in $\mathbb{R}$ sind.
Oft ist es praktisch, die Elemente von $\mathbb{T}$ als komplexe Zahlen vom Betrag 1 aufzufassen und die Operation als Multiplikation. Entsprechend wird in diesem Zusammenhang oft die multiplikative Schreibweise bevorzugt. Es gilt: Übungsaufgabe dies zu rechtfertigen.

**Proposition 7.1.4.1.** *Bezeichne $C$ die multiplikative Gruppe aller $z \in \mathbb{C}$ mit $|z| = 1$ mit der als Unterraum von $\mathbb{C}$ ererbten Topologie. Dann ist durch $\varphi : r + \mathbb{Z} \mapsto e^{2\pi ir} = \cos(2\pi r) + i\sin(2\pi r)$ eine Abbildung $\varphi\colon \mathbb{T} \to C$ definiert ist, die sowohl Gruppenisomorphismus als auch Homöomorphismus topologischer Räume ist. Insbesondere ist $\mathbb{T}$ eine kompakte topologische Gruppe.*

**UE 393 ▶ Übungsaufgabe 7.1.4.2.** Beweisen Sie Proposition 7.1.4.1. **◀ UE 393**

Trotz der Beziehung zur Multiplikation komplexer Zahlen wollen wir hier an der additiven Schreibweise festhalten.

Jeder lokalkompakten abelschen Gruppe $G$ wird ihr sogenanntes *Pontrjaginsches Dual* $G^*$ zugeordnet, das sich ebenfalls als lokalkompakte abelsche Gruppe erweist. Die Trägermenge von $G^*$ enthält als Elemente sämtliche so genannten *Charaktere* $\chi$ von $G$, das sind definitionsgemäß die stetigen Homomorphismen $\chi\colon G \to \mathbb{T}$. Die Operation auf $G^*$ ist punktweise definiert, d.h. durch $(\chi_1 + \chi_2)(g) := \chi_1(g) + \chi_2(g)$, analog $(-\chi)(g) := -\chi(g)$. Nullelement ist der konstante Charakter $\chi_0$ mit Wert 0. Auf $G^*$ ist die *kompakt-offene Topologie* $\mathcal{T}$ definiert, genannt auch die *Topologie der gleichmäßigen Konvergenz auf kompakten Teilmengen*. Nach Proposition 7.1.1.4 genügt es eine Umgebungsbasis $\mathcal{U}$ von $\chi_0$ mit den dort vorausgesetzten Eigenschaften anzugeben. Und zwar bestehe $\mathcal{U}$ aus allen Mengen $B(K, U)$, $K \subseteq G$ kompakt, $U$ Umgebung von 0 in $\mathbb{T}$. Und zwar enthalte $B(K, U)$ genau jene $\chi \in G^*$ mit $\chi(K) \subseteq U$. Leicht prüft man nach, dass alle Bedingungen an $\mathcal{U}$ aus Proposition 7.1.1.4 mit $G^*$ an der Stelle von $G$ erfüllt sind.

**UE 394** ▶ **Übungsaufgabe 7.1.4.3.** Prüfen Sie diese Bedingungen aus Proposition 7.1.1.4 nach. ◀ **UE 394**

Also macht die dort definierte Topologie $\mathcal{T}$ die Gruppe $G^*$ zu einer topologischen Gruppe, eben das *Pontrjaginsche Dual* von $G$.

**Theorem 7.1.4.4.** Ist $G$ eine lokalkompakte abelsche Gruppe, so auch das Dual $G^*$ von $G$.

Der Beweis dieses Satzes ist anspruchsvoll und würde den Rahmen sprengen, und wir verzichten auf den Beweis bzw. lagern ihn in die folgende Übungsaufgabe für Ambitionierte aus.

**UE 395** ▶ **Übungsaufgabe 7.1.4.5.** Beweisen Sie Satz 7.1.4.4. (Achtung, anspruchsvoll!) ◀ **UE 395**

Viel einfacher sind die Beobachtungen der nächsten Übungsaufgabe.

**UE 396** ▶ **Übungsaufgabe 7.1.4.6.** Zeigen Sie für eine lokalkompakte Gruppe $G$ und die kompakt-offene Topologie $\mathcal{T}$ auf dem Dual $G^*$: ◀ **UE 396**

1. Konvergenz von Charakteren (genauer: eines Netzes von Charakteren) in $G^*$ bezüglich $\mathcal{T}$ ist äquivalent mit gleichmäßiger Konvergenz auf jeder kompakten Teilmenge von $G$.
2. Ist $G$ kompakt, so beschreibt $\mathcal{T}$ die gleichmäßige Konvergenz auf $G$ und ist diskret.
3. Ist $G$ diskret, so beschreibt $\mathcal{T}$ die punktweise Konvergenz und ist kompakt.

Aus Satz 7.1.4.4 folgt, dass der Prozess des Dualisierens für jede lokalkompakte abelsche Gruppe $G$ iteriert werden kann. Insbesondere besitzt jede lokalkompakte Gruppe $G$ ein so genanntes *Bidual* $G^{**} := (G^*)^*$. Bevor wir dieses näher in Augenschein nehmen, interessieren wir uns in der nächsten Übungsaufgabe aber vorerst für die Duale von besonders einfachen und wichtigen Beispielen lokalkompakter abelscher Gruppen:

**UE 397** ▶ **Übungsaufgabe 7.1.4.7.** Zeigen Sie folgende Strukturaussagen über Pontrjaginsche Duale. Isomorphien $\cong$ sind durchwegs sowohl algebraisch als auch topologisch zu verstehen. Beschreiben Sie auch den Isomorphismus. ◀ **UE 397**

1. $(\prod_{i\in I} G_i)^* \cong \bigoplus_{i\in I} G_i^*$ für kompakte abelsche Gruppen $G_i$.
2. $(\bigoplus_{i\in I} G_i)^* \cong \prod_{i\in I} G_i^*$ für diskrete abelsche Gruppen $G_i$.
3. $G^* \cong G$ für jede (diskrete) endliche abelsche Gruppe $G$. (Sie dürfen den Hauptsatz über endlich erzeugte abelsche Gruppen 3.3.4.2 verwenden. Er besagt insbesondere, dass jede endliche abelsche Gruppe direkte Summe, äquivalent: Produkt, zyklischer Gruppen ist.)
4. $\mathbb{Z}^* \cong \mathbb{T}$.

5. $\mathbb{T}^* \cong \mathbb{Z}$.
6. $\mathbb{R}^* \cong \mathbb{R}$.
7. $C_{p^\infty}^* \cong \overline{\mathbb{Z}}_p$.
8. $\overline{\mathbb{Z}}_p^* \cong C_{p^\infty}$.

Es fällt auf, dass in allen behandelten Fällen $G \cong G^{**}$ gilt. Der verantwortliche Isomorphismus erweist sich stets als natürlich in einer Weise, die an den letzten Absatz in Abschnitt 2.2.4 erinnert. Es handelt sich nämlich um jene Abbildung $G \to G^{**}$, die jedem Element $g \in G$ die Auswertungsabbildung $\chi \mapsto \chi(g)$ zuordnet, welche ja tatsächlich ein Homomorphismus von $G^*$ nach $\mathbb{T}$ ist, der sich auch als stetig (bezüglich der kompakt-offenen Topologie auf $G^*$ und der natürlichen Topologie auf $\mathbb{T}$) erweist. Der tiefliegende Dualitätssatz von Pontrjagin besagt, dass dies nicht nur für die behandelten Beispiele gilt, sondern für jede lokalkompakte Gruppe.

**Theorem 7.1.4.8. (Dualitätssatz von Pontrjagin)** Ist $G$ eine lokalkompakte abelsche Gruppe mit Dual $G^*$ und Bidual $G^{**}$, dann ist die kanonische Abbildung

$$\Phi\colon G \to G^{**}, \quad g \mapsto g^{**},$$

mit

$$g^{**}\colon G^* \to \mathbb{T}, \quad \chi \mapsto \chi(g),$$

ein sowohl algebraischer als auch topologischer Isomorphismus zwischen $G$ und $G^{**}$.

Lokalkompakte Gruppen besitzen also die analoge Eigenschaft wie reflexive (topologische) Vektorräume.

### 7.1.5 Der kategorientheoretische Aspekt

Nochmals rufen wir uns folgende interessante Eigenschaft der Prüfergruppe $C_{p^\infty}$ aus Proposition 7.1.2.1 in Erinnerung:

Zu jedem $n \in \mathbb{N}$ gibt es eine natürliche Einbettung $\iota_n\colon C_{p^n} \to C_{p^\infty}$, ebenso zu beliebigen $m \leq n \in \mathbb{N}$ Einbettungen $\varphi_{m,n}\colon C_{p^m} \to C_{p^n}$ derart, dass $\iota_m = \iota_n \circ \varphi_{m,n}$. Jede andere (abelsche) Gruppe $G$, in die sich in analoger Weise alle $C_{p^n}$ einbetten lassen, enthält eine isomorphe Kopie der $p$-Prüfergruppe $C_{p^\infty}$, wobei sich die Einbettung in natürlicher Weise ergibt.
Wir werden diese Situation gleich durch eine allgemeine kategorientheoretische Definition des direkten Limes einfangen. Als ersten Schritt dorthin erinnern wir uns aber noch an die Situation, wo auch zyklische Gruppen $C_n$ mit einem $n \in \mathbb{N}$, das keine $p$-Potenz ist, mitspielen. Dann existieren Einbettungen nur für gewisse Paare $(m, n)$, hier: wenn $m$ ein Teiler von $n$ ist. Diese Situation verallgemeinernd fassen wir die folgende Definition.

**Definition 7.1.5.1.** Unter einer *gerichteten Menge* versteht man eine Halbordnung $(N, \leq)$, in der es zu je zwei Elementen $\nu_1, \nu_2 \in N$ stets ein $\nu \in N$ gibt mit $\nu_1 \leq \nu$ und $\nu_2 \leq \nu$.

Gerichtete Mengen fungieren in der Topologie als Indexmengen für sogenannte Netze, die den Begriff der Folge dahingehend verallgemeinern, dass an die Stelle des Spezialfalles $(\mathbb{N}, \leq)$ eine beliebige gerichtete Menge $(N, \leq)$ tritt. So wie in metrischen Räumen die Topologie vollständig durch sämtliche konvergente Folgen samt ihrer Grenzwerte eindeutig bestimmt ist, kann mit Hilfe der Konvergenz von Netzen die Topologie auch von nicht metrisierbaren topologischen Räumen eingefangen werden. Das spielt für uns im Folgenden allerdings kaum eine Rolle. Wir verwenden gerichtete Mengen lediglich zur Definition von injektiven und projektiven Systemen sowie Limiten.

**Definition 7.1.5.2.** Sei $\mathcal{C}$ eine Kategorie und $(N, \leq)$ ein gerichtete Menge. Gegeben seien für jedes $\nu \in N$ ein Objekt $A_\nu$ in $\mathcal{C}$ und, für alle $\nu_1 \leq \nu_2 \in N$, Morphismen $\varphi_{\nu_1 \to \nu_2} \colon A_{\nu_1} \to A_{\nu_2}$ mit der Eigenschaft, dass für alle $\nu_1 < \nu_2 < \nu_3 \in N$ die Beziehung $\varphi_{\nu_2,\nu_3} \circ \varphi_{\nu_1,\nu_2} = \varphi_{\nu_1,\nu_3}$ gilt. Weiters verlangen wir $\varphi_{\nu,\nu} = id_{A_\nu}$ für alle $\nu$. Dann nennt man die $A_\nu$ zusammen mit den $\varphi_{\nu_1,\nu_2}$ ein *injektives System* in $\mathcal{C}$.

Bilden die $A_\nu$ zusammen mit den $\varphi_{\nu_1,\nu_2}$ ein injektives System in der Kategorie $\mathcal{C}$, so können wir die folgende Kategorie $\mathcal{C}^+$ betrachten. Ihre Objekte seien Tupel $(A, (\psi_\nu)_{\nu \in N})$ mit Objekten $A$ und Morphismen $\psi_\nu \colon A_\nu \to A$ aus $\mathcal{C}$ derart, dass für alle $\nu_1 < \nu_2 \in N$ die Beziehung $\psi_{\nu_1} = \psi_{\nu_2} \circ \varphi_{\nu_1,\nu_2}$ gilt. Die Morphismen von $(A, (\psi_\nu)_{\nu \in N})$ nach $(A', (\psi'_\nu)_{\nu \in N})$ in $\mathcal{C}^+$ seien jene Morphismen $f \colon A \to A'$ in $\mathcal{C}$, die für alle $\nu \in N$ die Beziehung $\psi'_\nu = f \circ \psi_\nu$ erfüllen. Die Komposition von Morphismen in $\mathcal{C}^+$ ist die aus $\mathcal{C}$. Mit diesen Notationen lautet die Definition eines direkten Limes nun wie folgt.

**Definition 7.1.5.3.** Jedes initiale Objekt in der Kategorie $\mathcal{C}^+$ heißt *direkter* oder *injektiver Limes* (manchmal auch *Kolimes*) des vorgegebenen injektiven Systems. Für so ein initiales Objekt schreibt man (etwas ungenau, weil die Abhängigkeit vom injektiven System dabei nur sehr unvollständig zum Ausdruck kommt) auch $\lim_{\to} A_\nu$.

Als universelles Objekt in der Kategorie $\mathcal{C}^+$ ist ein injektiver Limes bis auf Äquivalenz eindeutig bestimmt (siehe Satz 2.2.3.2), also – wie man sich sofort klar macht – auch in der ursprünglich vorgegebenen Kategorie $\mathcal{C}$.

**UE 398** ► **Übungsaufgabe 7.1.5.4.** Über injektive Limiten sind folgende Aussagen zu beweisen. ◄ **UE 398**

1. Bei der Prüfergruppe $C_{p^\infty}$ handelt es sich tatsächlich um einen injektiven Limes innerhalb der Kategorie der abelschen Gruppen (wie auch in der der Gruppen).
2. In der Kategorie der abelschen Gruppen gibt es zu jedem injektiven System einen direkten Limes.
3. Verallgemeinern Sie Aussage (2) von der Kategorie der abelschen Gruppen auf Varietäten.

Auch im Fall der $p$-adischen Zahlen $\mathbb{Z}_p$ ist die Situation ähnlich, nur dass sich die Richtungen der Morphismen umdrehen und Epimorphismen an die Stelle der Monomorphismen treten. Fasst man den Begriff entsprechend allgemein, gelangt man zu einem zum direkten Limes dualen Begriff, dem des indirekten oder projektiven Limes.

**UE 399 ► Übungsaufgabe 7.1.5.5.** (1) Geben Sie eine rein kategorientheoretische Definition eines projektiven Systems derart, dass dieser Begriff dual zu dem des injektiven Systems ist und zyklische Gruppen mit Epimorphismen $C_{p^n} \to C_{p^m}$, $k + p^n\mathbb{Z} \mapsto k + p^m\mathbb{Z}$, für $m \leq n$ darunter fallen. **◄ UE 399**

(2) Geben Sie eine rein kategorientheoretische Definition eines projektiven Limes derart, dass dieser Begriff dual zu dem des injektiven Limes ist und die $p$-adischen Zahlen $\overline{\mathbb{Z}}_p$ als projektiver Limes aufgefasst werden können.

(3) Zeigen Sie, dass es in der Kategorie der abelschen Gruppen zu jedem projektiven System einen projektiven Limes gibt.

(4) Verallgemeinern Sie Aussage (3) auf Varietäten.

## 7.2 Grundbegriffe der Strukturtheorie der Moduln

Der Begriff der Dimension eines Vektorraums baut auf dem der Basis auf. Die dazu erforderlichen Begriffe *Erzeugnis* und *lineare (Un-)Abhängigkeit* lassen sich zwar problemlos auf Moduln übertragen. Im Gegensatz zu Vektorräumen hat aber nicht jeder Modul eine Basis, d.h. nicht alle Moduln sind frei. Zunächst haben wir uns mit den daraus resultierenden Komplikationen zu beschäftigen (7.2.1). Beschränkt man den Dimensionsbegriff auf freie Moduln, so nennt man Ringe, über denen je zwei Basen ein und desselben Moduls gleiche Kardinalität haben, dimensionsinvariant. Viele Ringe haben diese Eigenschaft, z.B. Divisions- und auch kommutative Ringe mit 1 (7.2.2). Für das Studium von Modulhomomorphismen und somit für die allgemeine Strukturtheorie von Moduln erweisen sich schließlich sogenannte exakte Sequenzen als sehr nützlich (7.2.3).

### 7.2.1 Freie Moduln, Basen und Dimension

Auf sehr einfache Weise lassen sich die Komplikationen, mit denen wir uns in der Theorie der Moduln oder auch abelschen Gruppen herumschlagen müssen, folgendermaßen illustrieren:
Ist $K$ ein Körper, so hat jeder eindimensionale, d.h. jeder von einem Element $\neq 0$ erzeugte Vektorraum dieselbe Struktur, nämlich die von $K$, aufgefasst als Vektorraum über sich selbst. Nehmen wir statt $K$ den Ring $\mathbb{Z}$ und die abelschen Gruppen als unitäre $\mathbb{Z}$-Moduln, so gilt dies nicht mehr. Denn es gibt neben $\mathbb{Z}$ selbst zu jedem $n \in \mathbb{N}$ mit $n \geq 2$ eine von einem Element $\neq 0$ erzeugte abelsche Gruppe $A$ mit $|A| = n$, die zyklische Gruppe $C_n$. Wir definieren etwas allgemeiner:

**Definition 7.2.1.1.** Ein $R$-Modul $A$ heißt *zyklisch*, wenn er von einem Element erzeugt wird.

Ist der Ring $R$ mit dem Einselement $1_R$ vorgegeben, so überblickt man die Struktur der zyklischen $R$-Moduln recht schnell. Denn wann immer $a \in A$ ein erzeugendes Element eines zyklischen $R$-Moduls $A$ ist, gilt $A = Ra = \{ra \mid r \in R\}$. Folglich ist der $R$-Modul-Homomorphismus $f\colon R \to A$, $r \mapsto a$, surjektiv, nach dem Homomorphiesatz daher $A \cong R/\ker f$. In dieser Faktorisierung ist $\ker f$ ein $R$-Untermodul des (selbst zyklischen,

weil von $1_R$ erzeugten) $R$-Moduls $R$ Die $R$-Untermodule von $R$ sindgenau die Linksideale von $R$. Also:

**Proposition 7.2.1.2.** *Die unitären zyklischen $R$-Moduln sind bis auf Isomorphie gegeben durch sämtliche Faktor-$R$-Moduln $R/I$ nach Linksidealen $I$ von $R$.*

**UE 400 ► Übungsaufgabe 7.2.1.3.** Beweisen Sie Proposition 7.2.1.2 ausführlich. **◄ UE 400**

Wir wollen uns nicht auf zyklische Moduln beschränken. Deshalb definieren wir in völliger Analogie zur Theorie der Vektorräume:

**Definition 7.2.1.4.** Sei $I$ eine Menge, $A$ ein $R$-Modul und $(a_i)_{i\in I} \in A^I$ eine mit $I$ indizierte Familie von Elementen $a_i \in A$.
Die Familie $(a_i)_{i\in I} \in A^I$ heißt *linear abhängig*, wenn es paarweise verschiedene Indizes $i_1, \ldots, i_n \in I$ mit $n \geq 1$, $n \in \mathbb{N}$, und Elemente $r_1, \ldots, r_n \neq 0$ aus $R$ gibt, so dass $\sum_{k=1}^n r_k a_{i_k} = 0$ gilt. Ist die Familie $(a_i)_{i\in I} \in A^I$ nicht linear abhängig, so nennt man sie, ebenso wie die Menge $\{a_i : i \in I\}$, *linear unabhängig*.
Die Familie $(a_i)_{i\in I} \in A^I$ heißt eine *Basis!eines Vektorraums* von $A$, wenn sie linear unabhängig ist und $\{a_i : i \in I\}$ ein Erzeugendensystem von $A$, d.h. wenn es zu jedem $a \in A$ endlich viele Indizes $i_1, \ldots, i_n \in I$ und Elemente $r_1, \ldots, r_n \in R$ gibt mit $\sum_{k=1}^n r_k a_{i_k} = a$. Ist die Familie $(a_i)_{i\in I} \in A^I$ eine Basis von $A$, so nennt man auch die Menge $\{a_i : i \in I\}$ eine Basis von $A$.

In dieser Definition fällt auf, dass wir lineare Abhängigkeit nur für Familien definiert haben, lineare Unabhängigkeit hingegen auch für Mengen. Den Grund erkennt man aus folgenden Beobachtungen: Ist $(a_i)_{i\in I} \in A^I$ eine Basis von $A$, so gilt $a_{i_1} \neq a_{i_2}$ für alle $i_1 \neq i_2 \in I$, weil sonst $1a_{i_1} - 1a_{i_2} = 0$ eine nichttriviale Darstellung der 0 wäre. Folglich ist die Zuordnung $f\colon i \mapsto a_i$ bijektiv zwischen der Indexmenge $I$ und $\{a_i : i \in I\}$. Es ist offensichtlich, dass die lineare Abhängigkeit bzw. Unabhängigkeit von $(a_i)_{i\in I} \in A^I$ weder von $I$ noch von der speziellen Bijektion $f$ abhängt. Das bedeutet umgekehrt: Ist irgendeine Teilmenge $B \subseteq A$ gegeben, so liefern alle bijektiven Indizierungen von $B$ hinsichtlich linear abhängig/unabhängig denselben Befund. Lassen wir hingegen auch nicht bijektive Indizierungen zu, so können manche davon linear abhängige Familien definieren, obwohl $B$ als Menge linear unabhängig ist. Einfachstes Beispiel: Für $a = a_1 = a_2$ und $I = \{1, 2\}$ ist die Familie $(a_i)_{i\in I}$ wunschgemäß linear abhängig im Sinne von Definition 7.2.1.4, während die Menge $\{a_1, a_2\} = \{a, a\} = \{a\}$ als Singleton linear unabhängig sein kann (und sicher auch ist, sofern $a \neq 0$ und $A$ ein Vektorraum ist). Doch nun zurück zu unserem Hauptthema.
Weil die Moduln über einem Ring $R$ (analog die unitären Moduln, wenn $R$ ein Einselement hat) eine Varietät bilden, gibt es nach 4.1.3.1 auch über jeder Menge $X$ einen freien $R$-Modul. Seine Struktur wird durch folgenden Satz beschrieben:

**Satz 7.2.1.5.** *Für einen unitären $R$-(Links-)Modul $F$ sind die folgenden Aussagen äquivalent.*

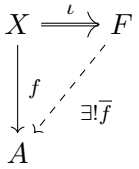
*(i)* *$F$ hat eine Basis.*

*(ii)* *$F$ ist die innere direkte Summe einer Familie zyklischer (d.h. von jeweils einem Element erzeugter) $R$-Moduln, wobei jeder davon als Links-Modul isomorph zu $R$ ist, genauer: $F = \bigoplus_{i\in I} Ra_i$ und $R \cong Ra_i$ via $r \mapsto ra_i$.*

*(iii)* *$F$ ist als $R$-Modul isomorph zu einer direkten Summe von Kopien von $R$.*

*(iv)* *Es existiert eine Menge $X$ und eine Funktion $\iota\colon X \to F$ mit der folgenden Eigenschaft:*

*Sind ein beliebiger unitärer $R$-Modul $A$ und eine Funktion $f\colon X \to A$ gegeben, dann gibt es einen eindeutigen $R$-Modul-Homomorphismus $\overline{f}\colon F \to A$ mit $\overline{f}\iota = f$.*




*Mit anderen Worten: $F$ ist zusammen mit $\iota$ ein freies Objekt in der konkreten Kategorie der unitären $R$-Moduln.*

**UE 401 ► Übungsaufgabe 7.2.1.6.** (1) Beweisen Sie Satz 7.2.1.5. **◄ UE 401**

(2) Untersuchen Sie die Situation für den Fall, dass $F$ nicht unitär ist oder $R$ kein Einselement hat.

Aus Satz 7.2.1.5 kann man direkt, d.h. auch ohne den entsprechenden allgemeinen Satz für Varietäten (4.1.3.8) folgern:

**Korollar 7.2.1.7.** *Jeder Modul $A$ über einem Ring $R$ ist homomorphes Bild eines freien $R$-Moduls $F$. Hat $A$ ein Erzeugendensystem $X$, so kann $F$ als frei über $X$ gewählt werden.*

*Beweisskizze.* Sei $F$ der freie $R$-Modul über $X$. Nach Satz 7.2.1.5 induziert die Einbettung $X \to A$ einen Modul-Homomorphismus $\overline{f}\colon F \to A$, sodass $X \subseteq \operatorname{Im}\overline{f}$. Da $X$ schon ganz $A$ erzeugt, muss auch $\operatorname{Im}\overline{f} = A$ gelten. □

Weil jeder Vektorraum nach 1.3.1.3 eine Basis hat, sehen wir auch:

**Korollar 7.2.1.8.** *Jeder Vektorraum über einem Schiefkörper ist frei, und zwar über jeder beliebigen Basis.*

### 7.2.2 Dimensionsinvarianz

**Definition 7.2.2.1.** Sei $R$ ein Ring mit 1 und $F$ ein freier unitärer $R$-Modul mit Basis $X$. Dann heißt $\kappa := |X|$ die *Dimension* oder der *Rang* von $F$ über $R$, wenn $|B| = |X|$ für jede Basis $B$ von $F$ gilt. Wir schreiben $\dim_R F = \operatorname{rang}_R F = \kappa = |X|$. $R$ heißt *dimensionsinvariant,* wenn jeder freie $R$-Modul $F$ eine Dimension hat.

Um auch den Fall unendlicher Dimension untersuchen zu können, werden wir folgende Tatsachen über unendliche Kardinalitäten brauchen.

**Proposition 7.2.2.2.** *Für die Kardinalitäten von Mengen $A, B$ gelten folgende Beziehungen:*

1. *(Satz von Cantor-Schröder-Bernstein) Aus $|A| \leq |B|$ und $|B| \leq |A|$ folgt $|A| = |B|$.*
2. *Ist $A$ unendlich, $B \neq \emptyset$ und $|B| \leq |A|$ (d.h. es gibt ein injektives $f\colon B \to A$), so gilt $|A \times B| = |A|$ (d.h. es gibt ein bijektives $f\colon A \times B \to A$). Insbesondere gilt das für abzählbares $B$.*
3. *Ist $A$ eine unendliche Menge und $\mathfrak{P}_{\text{fin}}(A)$ die Menge aller endlichen Teilmengen von $A$, dann ist $|\mathfrak{P}_{\text{fin}}(A)| = |A|$.*

**UE 402** ► **Übungsaufgabe 7.2.2.3.** Beweisen Sie Proposition 7.2.2.2. Hinweis: Anhang, 11.4.4. ◄ **UE 402**

Wir wichtigsten Resultate im Zusammenhang mit Dimensionsinvarianz sind in folgendem Satz zusammengefasst:

**Satz 7.2.2.4.** *1. Ist $R$ ein Ring mit 1 und $F$ ein freier $R$-Modul mit einer unendlichen Basis. Dann haben je zwei Basen von $F$ dieselbe Kardinalität. (Man beachte, dass die Kardinalität einer Basis $(b_i)_{i\in I}$ gleich der Kardinalität der Indexmenge $I$ ist.)*

2. *Divisionsringe (also insbesondere Körper) sind dimensionsinvariant.*
3. *Seien $R$ und $S$ Ringe mit 1, $f\colon R \to S$ ein Epimorphismus. Ist $S$ dimensionsinvariant, so auch $R$.*
4. *Jeder kommutative Ring mit $1 \neq 0$ ist dimensionsinvariant.*

*Beweis.* 1. Sei $X$ eine unendliche Basis und $Y$ eine weitere Basis von $F$. Wir zeigen zuerst, dass $Y$ unendlich ist, indem wir indirekt annehmen, $Y = \{y_1, \ldots, y_n\}$ wäre endlich. Jedes $y_i$ lässt sich darstellen als Linearkombination von Elementen aus $X$:

$$y_i = \sum_{k=1}^{n_i} r_{i,k} x_{i,k}$$

Das würde aber bedeuten, dass die endlich vielen $x_{i,k}$ ($i = 1, \ldots, n$ und $k = 1, \ldots, n_i$) schon $F$ erzeugen, Widerspruch. Also muss $Y$ unendlich sein.

Wir definieren nun eine Funktion $f\colon X \to \mathfrak{P}_{\text{fin}}(Y)$ von $X$ in die Menge $\mathfrak{P}_{\text{fin}}(Y)$ aller endlichen Teilmengen von $Y$ so, dass

$$f\colon x \mapsto \{y_1, \ldots, y_n\},$$

wobei $x = \sum_{i=1}^{n} r_i y_i$ mit $r_i \neq 0$ und paarweise verschiedenen $y_i \in Y$. Ganz symmetrisch sei die Funktion $g : Y \to \mathfrak{P}_{\text{fin}}(X)$ definiert, indem $f(y) = \{x_1, \ldots, x_m\}$, sofern $y = \sum_{j=1}^{m} s_j x_j$ mit $s_j \neq 0$ und paarweise verschiedenen $x_j \in X$.

Das Bild $\operatorname{Im} f$ von $f$ ist unendlich. Andernfalls erzeugte die endliche Menge $\bigcup \operatorname{Im} f$ ganz $F$, Widerspruch. Als nächstes wollen wir zeigen, dass auch $f^{-1}(T)$ endlich ist für alle $T \in \operatorname{Im} f$. Dazu definieren wir für eine beliebiges $T \in \operatorname{Im} f$ die endliche Menge

$$S_T := \bigcup_{y \in T} g(y) \subseteq X.$$

Weil jedes $y \in T$ in der linearen Hülle von $g(y) \subseteq S_T$ liegt, gilt $\langle T \rangle \subseteq \langle S_T \rangle$. Damit zeigen wir nun $f^{-1}(T) \subseteq S_T$: Aus $x \in f^{-1}(T)$ folgt $x \in \langle T \rangle \subseteq \langle S_T \rangle \subseteq X$. Weil $X$ als Basis linear unabhängig ist, ist das nur für $x \in S_T$ möglich. Damit ist $f^{-1}(T)$ enthalten in der endlichen Menge $S_T$ und daher selbst endlich.

Für jedes $T \in \operatorname{Im} f$ sei $f^{-1}(T) = \{x_{T,1}, x_{T,2}, \ldots, x_{T,n}\}$ mit paarweise verschiedenen $x_{T,i}$. Wir definieren eine injektive Funktion $\varphi_T\colon f^{-1}(T) \to \operatorname{Im} f \times \mathbb{N}$ durch

$$\varphi_T : x_{T,k} \mapsto (T, k).$$

Da die Mengen $f^{-1}(T)$, $T \in \operatorname{Im} f$, eine Partition von $X$ bilden, ist die Funktion

$$\varphi := \left( \bigcup_{T \in \operatorname{Im} f} \varphi_T \right) : X \to \operatorname{Im} f \times \mathbb{N}$$

wohldefiniert und injektiv. Folglich gilt (siehe Proposition 7.2.2.2, Aussage 2)

$$|X| \leq |\operatorname{Im} f \times \mathbb{N}| = |\operatorname{Im} f| \cdot \aleph_0 = |\operatorname{Im} f| \leq |\mathfrak{P}_{\text{fin}}(Y)| = |Y|.$$

Analog zeigt man $|Y| \leq |X|$, woraus (wieder nach Proposition 7.2.2.2, Satz von Schröder-Bernstein) $|X| = |Y|$ folgt.

2. Siehe Lineare Algebra (Austauschsatz von Steinitz) im Fall einer endlichen Basis, andernfalls Aussage 1.

3. Beweisskizze (genaue Ausarbeitung Übung): Es genügt folgendes zu zeigen: Sei $R$ ein Ring und $I \lhd R$ ein echtes Ideal von $R$, $F$ ein freier $R$-Modul mit Basis $X$. Dann ist $IF \leq F$. Sei weiters $\pi\colon F \to F/IF$ der kanonische Epimorphismus von $F$ nach $F/IF$. Dann ist $F/IF$ ein freier $R/I$-Modul mit Basis $\pi(X)$ und $|\pi(X)| = |X|$.

4. Sei $M$ ein maximales Ideal von $R$. (Ein solches existiert in jedem kommutativen Ring mit 1 nach 3.4.2.4). Es existiert ein Epimorphismus von $R$ auf den Körper $R/M$ (nochmals 3.4.2), nämlich die kanonische Abbildung. Nach den Aussagen 2 und 3 ist damit auch $R$ dimensionsinvariant. □

**UE 403** ► **Übungsaufgabe 7.2.2.5.** Arbeiten Sie die Beweisskizze für Aussage (3) in Satz 7.2.2.4 im Detail aus. ◄ **UE 403**

### 7.2.3 Exakte Sequenzen

Weiterhin betrachten wir, wenn nicht ausdrücklich anders vermerkt, nur unitäre $R$-Moduln über einem Ring $R$ mit Einselement. Wir werden nun exzessiv von (kommutativen) Diagrammen in der Kategorie der (Links- oder Rechts-) Moduln über einem Ring $R$ Gebrauch machen. Eine besondere Rolle spielen Sequenzen, nämlich Diagramme von der Form

$$\ldots \xrightarrow{f_{i-2}} A_{i-1} \xrightarrow{f_{i-1}} A_i \xrightarrow{f_i} A_{i+1} \xrightarrow{f_{i+1}} \ldots,$$

wobei die Folgen der $R$-Moduln $A_i$ und Morphismen $f_i$ nach links und rechts endlich oder unendlich sein dürfen. Man beachte, dass Diagramme dieser Art immer auf eindeutige Weise zu kommutativen ergänzt werden können. Diese Ergänzungen wollen wir bei Bedarf stillschweigend verwenden, so dass wir es also tatsächlich mit kommutativen Diagrammen im Sinne von 2.2.5 zu tun haben.
Der folgende Begriff lässt sich nicht in beliebigen Kategorien definieren, erweist sich im Fall der Moduln aber als äußerst fruchtbar.

**Definition 7.2.3.1.** Ein Paar von Modul-Homomorphismen $A \xrightarrow{f} B \xrightarrow{g} C$ heißt *exakt*, sofern $\operatorname{Im} f = \ker g$. Eine Folge von Modul-Homomorphismen

$$\ldots \xrightarrow{f_{i-2}} A_{i-1} \xrightarrow{f_{i-1}} A_i \xrightarrow{f_i} A_{i+1} \xrightarrow{f_{i+1}} \ldots$$

heißt *exakt bei* $A_i$, falls $\operatorname{Im} f_{i-1} = \ker f_i$, *(schlechthin) exakt*, wenn dies für alle $i$, für die diese Beziehung definiert ist, gilt.

Exakte Sequenzen der Form $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ heißen *kurzexakt.* (Hierin sowie an entsprechenden Stellen in der Folge steht 0 für einen einelementigen Modul.)

**Beispiel 7.2.3.2.** (a) Jeder $R$-Modulhomomorphismus $f : A \to B$ induziert eine exakte Sequenz, nämlich

$$0 \to \ker f \xrightarrow{\iota} A \xrightarrow{f} \operatorname{Im} f \to 0$$

mit der Einbettung $\iota$.

(b) Sei $U \leq A$ ein Untermodul von $A$. Dann ist

$$0 \to U \xrightarrow{\iota} A \xrightarrow{\kappa} A/U \to 0$$

mit der Inklusionsabbildung $\iota$ und dem kanonischen Epimorphismus $\kappa : a \mapsto a + U$ kurzexakt.

(c) Von besonderem Interesse für das Weitere (siehe Satz 7.2.3.8) ist die folgende Situation. Seien $A, B$ Moduln über $R$. Dann ist

$$0 \to A \xrightarrow{\iota_1} A \oplus B \xrightarrow{\pi_2} B \to 0$$

mit $\iota_1 : a \mapsto (a, 0)$ und $\pi_2 : (a, b) \mapsto b$ kurzexakt.

Wie in 2.2.5 beschrieben, fassen wir Sequenzen einer gegebenen Länge selbst wieder als Objekte einer Kategorie auf. Für uns ist der zugehörige Äquivalenzbegriff von besonderem Interesse. Ohne den kategorientheoretischen Hintergrund aufzurollen (dem interessierten Leser[4] sei allerdings sehr wohl ans Herz gelegt, diese Zusammenhänge zu rekapitulieren, siehe auch Übungsaufgabe 7.2.3.4, sei der für uns relevante Kontext durch die folgende Definition explizit hervorgehoben.

**Definition 7.2.3.3.** Zwei kurzexakte Sequenzen

$$S: \ 0 \to A \to B \to C \to 0$$

und

$$S': \ 0 \to A' \to B' \to C' \to 0$$

heißen *isomorph*, falls es Modulisomorphismen $\alpha, \beta, \gamma$ gibt, so dass das Diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

kommutativ ist.

**UE 404** ► **Übungsaufgabe 7.2.3.4.** Rekapitulieren Sie den kategorientheoretischen Rahmen, innerhalb dessen Definition 7.2.3.3 als Spezialfall des Begriffs der Äquivalenz in einer geeigneten Kategorie aufgefasst werden kann. ◄ **UE 404**

Die folgende Definition hat diese Situation im Verbindung mit Beispiel 7.2.3.2 (c) im Visier.

**Definition 7.2.3.5.** $S$ bezeichne die kurzexakte Sequenz

$$0 \to A_1 \xrightarrow{f} B \xrightarrow{g} A_2 \to 0.$$

Angenommen $S$ kann zu einem kommutativen Diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1 & \xrightarrow{\iota_1} & A_1 \oplus A_2 & \xrightarrow{\pi_2} & A_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_{A_1}} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \mathrm{id}_{A_2}} & & \\ 0 & \longrightarrow & A_1 & \xrightarrow{f} & B & \xrightarrow{g} & A_2 & \longrightarrow & 0 \end{array}$$

[4] Siehe Fußnote auf Seite 121.

ergänzt werden, wobei $\mathrm{id}_{A_1}$ und $\mathrm{id}_{A_2}$ die identischen Abbildungen auf $A_1$ bzw. $A_2$ sind, $\iota_1 : a_1 \mapsto (a_1, 0)$ die Einbettung in die erste Komponente, $\pi_2 : (a_1, a_2) \mapsto a_2$ die Projektion auf die zweite Komponente und (das ist die interessanteste Bedingung) $\varphi$ ein Isomorphismus. Dann sagt man, die Sequenz $S$ *zerfällt* bzw. $S$ ist eine *zerfallende Sequenz.*

An zerfallenden Sequenzen ist die Beobachtung von Interesse, dass im obigen Diagramm die Homomorphismen $\pi_1 \colon A_1 \oplus A_2 \to A_1$, $(a_1, a_2) \mapsto a_1$, mit $\pi_1\iota_1 = \mathrm{id}_{A_1}$ und $\iota_2 \colon A_2 \to A_1 \oplus A_2$, $a_2 \mapsto (0, a_2)$, mit $\pi_2\iota_2 = \mathrm{id}_{A_2}$ existieren. Das wird etwas später in der Charakterisierung zerfallender Sequenzen zum Ausdruck kommen (7.2.3.8). Dabei treten zum Beispiel Diagramme wie im nachfolgenden Lemma 7.2.3.6 auf. Darin ist die Sequenz der $A_i$ mit den sie verbindenden $R$-Modul-Homomorphismen (waagrechten Pfeilen) ein Objekt der Kategorie der 5-Sequenzen (hier über der Kategorie der $R$-Linksmoduln), die der $B_i$ ein anderes. Das 5-tupel $(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$ von $R$-Modul-Homomorphismen $\alpha_i$, $i = 1, \ldots, 5$, ist definitionsgemäß genau dann ein Morphismus in der neuen Kategorie, wenn das Diagramm kommutiert. Für solche Diagramme gilt das folgende nützliche Resultat.

**Lemma 7.2.3.6.** *[Fünferlemma] Für $i = 1, 2, 3, 4, 5$ seien die $R$-Moduln $A_i, B_i$ sowie die Homomorphismen $\alpha_i \colon A_i \to B_i$ gegeben. Im kommutativen Diagramm*

$$\begin{array}{ccccccccc}
A_1 & \xrightarrow{f_1} & A_2 & \xrightarrow{f_2} & A_3 & \xrightarrow{f_3} & A_4 & \xrightarrow{f_4} & A_5 \\
\downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_3} & & \downarrow{\scriptstyle \alpha_4} & & \downarrow{\scriptstyle \alpha_5} \\
B_1 & \xrightarrow{g_1} & B_2 & \xrightarrow{g_2} & B_3 & \xrightarrow{g_3} & B_4 & \xrightarrow{g_4} & B_5
\end{array}$$

*mögen beide Zeilen exakte Sequenzen bilden. Dann gilt:*

*(a) Ist $\alpha_1$ surjektiv, und sind $\alpha_2, \alpha_4$ injektiv, dann ist $\alpha_3$ injektiv.*

*(b) Ist $\alpha_5$ injektiv und sind $\alpha_2, \alpha_4$ surjektiv, dann ist $\alpha_3$ surjektiv.*

*Beweis.* Um Aussage (a) zu beweisen, setzen wir voraus, dass $\alpha_1$ surjektiv ist, $\alpha_2$ und $\alpha_4$ injektiv und dass $\alpha_3(a_3) = 0$ gilt für ein $a_3 \in A_3$. Wir haben daraus $a_3 = 0$ zu folgern. Weil das Diagramm (drittes Quadrat) kommutiert, gilt $g_3\alpha_3 = \alpha_4 f_3$. Wegen $g_3\alpha_3(a_3) = 0$ bedeutet das $\alpha_4 f_3(a_3) = 0$, was wegen der Injektivität von $\alpha_4$ nur für $f_3(a_3) = 0$ möglich ist. Folglich liegt $a_3$ im Kern von $f_3$, der wegen der Exaktheit der oberen Zeile bei $A_3$ mit dem Bild von $f_2$ übereinstimmt. Also gibt es ein $a_2 \in A_2$ mit $f_2(a_2) = a_3$. Es folgt mit der Kommutativität des Diagramms (zweites Quadrat) $g_2\alpha_2(a_2) = \alpha_3 f_2(a_2) = \alpha_3(a_3) = 0$. Also liegt $\alpha_2(a_2)$ im Kern von $g_2$, der wegen der Exaktheit der unteren Zeile bei $B_2$ mit dem Bild von $g_1$ übereinstimmt. Folglich gibt es ein $b_1 \in B_1$ und somit, wegen der Surjektivität von $\alpha_1$, ein $a_1 \in A_1$ mit (Kommutativität des ersten Quadrats) $\alpha_2 f_1(a_1) = g_1\alpha_1(a_1) = \alpha_2(a_2)$. Das wiederum zeigt, dass $f_1(a_1) - a_2$ im Kern von $\alpha_2$ liegt. Weil $\alpha_2$ injektiv ist, folgt daraus $f_1(a_1) = a_2$. Wir setzen das ein

in $a_3 = f_2(a_2) = f_2f_1(a_1)$. Wegen der Exaktheit der oberen Zeile bei $A_2$ ist $f_2f_1$ aber die Nullabbildung. Somit ist $a_3 = 0$ bewiesen.
Für den Beweis von Aussage (b) seien $\alpha_2$ und $\alpha_4$ surjektiv, $\alpha_5$ injektiv und $b_3 \in B_3$. Wir müssen ein $a_3 \in A_3$ finden mit $\alpha_3(a_3) = b_3$. Wegen der Surjektivität von $\alpha_4$ gibt es ein $a_4 \in A_4$ mit $\alpha_4(a_4) = g_3(b_3)$. Die Exaktheit der unteren Zeile bei $B_4$ garantiert, dass das Bild $g_3(b_3)$ im Kern von $g_4$ liegt, also $0 = g_4g_3(b_3) = g_4\alpha_4(a_4) = \alpha_5f_4(a_4)$ (Kommutativität des vierten Quadrats). Weil $\alpha_5$ injektiv ist, folgt daraus $f_4(a_4) = 0$. Somit liegt $a_4$ im Kern von $f_4$. Wegen der Exaktheit der oberen Zeile bei $A_4$ garantiert das die Existenz eines $a'_3 \in A_3$ mit $f_3(a'_3) = a_4$. Die Kommutativität des dritten Quadrats liefert $\alpha_4f_3(a'_3) = g_3\alpha_3(a'_3)$. Wir würden gerne zeigen, dass die Differenz $d := b_3 - \alpha_3(a'_3)$ gleich 0 ist. Das gelingt zwar nicht. Doch gilt $g_3(d) = g_3(b_3) - g_3\alpha_3(a'_3) = \alpha_4(a_4) - \alpha_4f_3(a'_3) = \alpha_4(a_4 - f_3(a'_3)) = \alpha_4(0) = 0$. Folglich liegt $d$ im Kern von $g_3$, der (Exaktheit der unteren Zeile) mit dem Bild von $g_2$ übereinstimmt. Beachten wir außerdem die Surjektivität von $\alpha_2$, so gibt uns das ein $a_2 \in A_2$ in die Hand mit $d = g_2\alpha_2(a_2) = \alpha_3f_2(a_2)$ (Kommutativität des zweiten Quadrats). Das Element $a_3 := a'_3 + f_2(a_2)$ erfüllt nun tatsächlich $\alpha_3(a_3) = \alpha_3(a'_3 + f_2(a_2)) = \alpha_3(a'_3) + \alpha_3f_2(a_2) = (b_3 - d) + d = b_3$. □

Etwas leichter einzuprägen und für unsere späteren Anwendungen völlig ausreichend ist der Spezialfall, wo $A_1, A_5, B_1$ und $B_5$ und folglich auch $\alpha_1$ und $\alpha_5$ trivial sind.

**Korollar 7.2.3.7** (Kurzes Fünferlemma)**.** Sei $R$ ein Ring und

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\ 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \longrightarrow & 0 \end{array}$$

ein kommutatives Diagramm von $R$-Moduln und $R$-Modul-Homomorphismen, so dass beide Zeilen kurzexakte Sequenzen sind. Sind $\alpha, \gamma$ Mono-/ Epi-/ Isomorphismen, so ist auch $\beta$ ein Mono-/ Epi-/ Isomorphismus.

*Beweis.* Unmittelbare Folgerung aus 7.2.3.6. □

Es folgt das für die weitere Strukturtheorie wichtigste Hilfsmittel im Zusammenhang mit kurzexakten Sequenzen.

**Satz 7.2.3.8.** *Für eine kurzexakte Sequenz $S$ der Form $0 \to A_1 \xrightarrow{f} B \xrightarrow{g} A_2 \to 0$ sind äquivalent:*

*(i)* $\exists\sigma\colon A_2 \to B : g\sigma = \mathrm{id}_{A_2}$ *(Ein solches $\sigma$ heißt Sektion.)*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1 & \xrightarrow{f} & B & \underset{\sigma}{\overset{g}{\rightleftarrows}} & A_2 & \longrightarrow & 0 \end{array}$$

*(ii)* $\exists\rho\colon B \to A_1 : \rho f = \mathrm{id}_{A_1}$ *(Ein solches $\rho$ heißt Retraktion.)*

$$0 \longrightarrow A_1 \underset{\rho}{\overset{f}{\rightleftarrows}} B \xrightarrow{g} A_2 \longrightarrow 0$$

*(iii) Die gegebene Sequenz $S$ zerfällt. Insbesondere ist $B \cong A_1 \oplus A_2$.*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1 & \underset{\pi_1}{\overset{\iota_1}{\rightleftarrows}} & A_1 \oplus A_2 & \underset{\iota_2}{\overset{\pi_2}{\rightleftarrows}} & A_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_{A_1}} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \mathrm{id}_{A_2}} & & \\ 0 & \longrightarrow & A_1 & \xrightarrow{f} & B & \xrightarrow{g} & A_2 & \longrightarrow & 0 \end{array}$$

*Beweis.* Wir zeigen die Implikationen (i)⇒(iii), (ii)⇒(iii) und (iii)⇒(i),(ii).
(i)⇒(iii): Wir definieren $\varphi\colon A_1 \oplus A_2 \to B$ durch $(a_1, a_2) \mapsto f(a_1) + \sigma(a_2)$. Klarerweise ist $\varphi$ ein $R$-Modul-Homomorphismus. Wir zeigen nun, dass das Diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1 & \xrightarrow{\iota_1} & A_1 \oplus A_2 & \xrightarrow{\pi_2} & A_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_{A_1}} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \mathrm{id}_{A_2}} & & \\ 0 & \longrightarrow & A_1 & \xrightarrow{f} & B & \xrightarrow{g} & A_2 & \longrightarrow & 0 \end{array}$$

kommutiert. Wegen

$$\varphi\iota_1(a_1) = f(a_1) + \sigma(0) = f(a_1)$$

für alle $a_1 \in A_1$ kommutiert das linke Quadrat im Diagramm; wegen $\operatorname{Im} f = \ker g$, also $gf = 0$, $g\sigma = \mathrm{id}_{A_2}$ und somit

$$g\varphi(a_1, a_2) = g(f(a_1) + \sigma(a_2)) = gf(a_1) + g\sigma(a_2) = 0 + a_2 = \pi_2(a_1, a_2)$$

für alle $(a_1, a_2) \in A_1 \oplus A_2$ auch das rechte. Nach dem kurzen Fünferlemma 7.2.3.7 ist $\varphi$ daher ein Isomorphismus.

(ii)⇒(iii): Wir definieren einen $R$-Modul-Homomorphismus $\psi\colon B \to A_1 \oplus A_2$ durch $\psi : b \mapsto (\rho(b), g(b))$. Wir zeigen, dass das Diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1 & \xrightarrow{f} & B & \xrightarrow{g} & A_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_{A_1}} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \mathrm{id}_{A_2}} & & \\ 0 & \longrightarrow & A_1 & \xrightarrow{\iota_1} & A_1 \oplus A_2 & \xrightarrow{\pi_2} & A_2 & \longrightarrow & 0 \end{array}$$

kommutiert. Wegen

$$\pi_2\psi(b) = \pi_2(\rho(b), g(b)) = g(b)$$

für alle $b \in B$ kommutiert das rechte Quadrat; wegen $\operatorname{Im} f = \ker g$, also $gf = 0$, $\rho f = \mathrm{id}_{A_1}$ und somit

$$\psi f(a_1) = (\rho f(a_1), gf(a_1)) = (a_1, 0) = \iota_1(a_1)$$

für alle $a_1 \in A_1$ auch das linke. Wieder nach dem kurzen Fünferlemma 7.2.3.7 ist $\psi$ ein Isomorphismus.

(iii)⇒(i),(ii): Gegeben ist das kommutative Diagramm

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A_1 & \xrightarrow{\iota_1} & A_1 \oplus A_2 & \xrightarrow{\pi_2} & A_2 & \longrightarrow & 0 \\
 & & \Big\downarrow{\scriptstyle \mathrm{id}_{A_1}} & \overset{\pi_1}{\nwarrow} & \Big\downarrow{\scriptstyle \varphi} & \overset{\iota_2}{\nwarrow} & \Big\downarrow{\scriptstyle \mathrm{id}_{A_2}} & & \\
0 & \longrightarrow & A_1 & \xrightarrow{f} & B & \xrightarrow{g} & A_2 & \longrightarrow & 0
\end{array}$$

mit einem Isomorphismus $\varphi$. Definiere $\sigma := \varphi\iota_2 \colon A_2 \to B$ und $\rho := \pi_1\varphi^{-1} \colon B \to A_1$. Nun gilt wegen der Kommutativität des Diagramms

$$\begin{aligned}
g\sigma(a_2) &= g(\varphi(0, a_2)) = \pi_2(0, a_2) = a_2 \text{ und} \\
\rho f(a_1) &= \pi_1\varphi^{-1} f(a_1) = \pi_1\varphi^{-1}\varphi\iota_1(a_1) = \pi_1\iota_1(a_1) = a_1
\end{aligned}$$

für alle $a_1 \in A_1$, $a_2 \in A_2$. Somit sind die gesuchte Sektion $\sigma$ und Retraktion $\rho$ gefunden. □

## 7.3 Injektive und projektive Moduln

In $\mathbb{Q}$ hat jede Gleichung der Form $nx = a$ für gegebenes $a \in \mathbb{Q}$ und $n \in \mathbb{N} \setminus \{0\}$ eine (in diesem Fall sogar eindeutige) Lösung, nämlich $x = \frac{a}{n}$. Für eine abelsche Gruppe $G$ nimmt man diese Eigenschaft als Definition für die sogenannte *Teilbarkeit* von $G$ (siehe 7.3.1). Eine sinnvolle Verallgemeinerung von abelschen Gruppen auf Moduln ist etwas komplizierter. Sie erfolgt mit Hilfe eines geeigneten kommutativen Diagramms und führt zum Begriff des *injektiven Moduls* (siehe 7.3.2). Durch Dualisierung dieses Konzeptes (d.h. durch Umkehrung von Pfeilrichtungen u.ä.) ergibt sich der Begriff des *projektiven Moduls*, der sich wiederum als eine Abschwächung der Eigenschaft *frei* auffassen lässt (siehe 7.3.3). Über Hauptidealringen sind die projektiven Moduln sogar genau die freien. Die Resultate aus 7.3.3 werden sich u.a. beim Beweis des Hauptsatzes über endlich erzeugte Moduln über Hauptidealringen als sehr fruchtbar erweisen.

### 7.3.1 Teilbare Gruppen

**Definition 7.3.1.1.** Sei $D$ eine abelsche Gruppe, $a \in D$ und $n \in \mathbb{Z} \setminus \{0\}$. Das Element $a$ heißt *teilbar durch* $n$ in $D$, wenn es ein $d \in D$ gibt mit $nd = a$; $a$ heißt (schlechthin) *teilbar in* $D$, wenn $a$ durch alle $n \in \mathbb{Z} \setminus \{0\}$ teilbar ist. $D$ heißt *teilbar durch* $n$, wenn alle $a \in D$ durch $n$ teilbar sind; $D$ heißt (schlechthin) *teilbar*, wenn alle $a \in D$ teilbar sind.

Beispiele teilbarer Gruppen sind $\mathbb{Q}$ und $\mathbb{R}$, außerdem direkte Summen und Produkte teilbarer Gruppen sowie deren homomorphe Bilder. Die wichtigsten Beispiele teilbarer Torsionsgruppen sind die Prüfergruppen.

**UE 405** ► **Übungsaufgabe 7.3.1.2.** Beweisen Sie, dass tatsächlich $\mathbb{Q}$, $\mathbb{R}$ und die Prüfergruppen teilbar sind sowie dass sich Teilbarkeit sowohl auf direkte Summen und Produkte als auch auch auf homomorphe Bilder überträgt. ◄ **UE 405**

Als Ausgangspunkt für das Weitere dient die Beobachtung, dass jeder Homomorphismus von einer Untergruppe einer Gruppe $G$ in eine teilbare Gruppe $D$ stets auf ganz $G$ fortgesetzt werden können.

**Satz 7.3.1.3.** *Ist $D$ eine teilbare Gruppe, $U \leq A$ und $f_U \colon U \to D$ ein Homomorphismus, so gibt es eine homomorphe Fortsetzung von $f_U$ auf ganz $A$, d.h. einen Homomorphismus $f \colon A \to D$ mit $f(u) = f_U(u)$ für alle $u \in U$.*

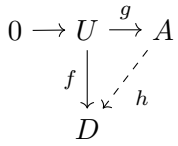
*Beweis.* Das System $\mathcal{S}$ aller Homomorphismen $f_B \colon B \to D$ mit $U \leq B \leq A$, die $f_B(u) = f_U(u)$ für alle $u \in U$ erfüllen, bildet bezüglich $\subseteq$ eine Halbordnung, in der jede Kette nach oben beschränkt ist (z.B. durch ihre Vereinigung). Also ist das Lemma von Zorn anwendbar und liefert ein maximales $f_0 \colon A_0 \to D$ in $\mathcal{S}$. Wir zeigen, dass bereits $A_0 = A$ gilt und folglich $f := f_0$ das Gewünschte leistet.
Wir nehmen indirekt an, es gebe ein $a \in A \setminus A_0$, und setzen $A_1 := A_0 + \langle a \rangle \leq A$. $H := \langle a \rangle \cap A_0$ ist als Untergruppe der zyklischen Gruppe $\langle a \rangle$ selbst zyklisch mit $H = \langle ma \rangle$, $m \in \mathbb{N}$. Wir halten fest, dass $ka$ für $k \in \mathbb{Z}$ genau dann in $H$ liegt, wenn es ein $n \in \mathbb{Z}$ mit $k = nm$ gibt. Ist $m \neq 0$, so gibt es wegen der Teilbarkeit von $D$ ein $d \in D$ mit $md = f_0(ma)$, für $m = 0$ nehmen wir $d = 0$. Wir behaupten, dass die Zuordnung $f_1 : a_0 + ka \mapsto f_0(a_0) + kd$ für $a_0 \in A_0$ und $k \in \mathbb{Z}$ einen wohldefinierten Homomorphismus $f_1 \colon A_1 \to D$ definiert. Zu zeigen ist: Aus $a_0 + ka = a_0' + k'a$ mit $a_0, a_0' \in A_0$ und $k, k' \in \mathbb{Z}$ folgt $f_0(a_0) + kd = f_0(a_0') + k'd$; die Homomorphieeigenschaft ist dann offensichtlich. Zunächst gilt $f_0(a_0') + k'd = f_0(a_0 + a_0' - a_0) + (k + k' - k)d = f_0(a_0) + kd + r$ mit dem Rest $r = f_0(a_0' - a_0) - (k - k')d$, von dem wir $r = 0$ zu zeigen haben. Wegen $a_0 - a_0' = (k' - k)a \in A_0 \cap \langle a \rangle = H$ gibt es ein $n \in \mathbb{Z}$ mit $nm = k - k'$. Somit gilt $f_0(a_0' - a_0) = f_0((k - k')a) = f_0(nma) = nf_0(ma) = nmd$ und $(k - k')d = nmd$, folglich $r = f_0(a_0' - a_0) - (k - k')d = 0$. □

Die Fortsetzungseigenschaft aus Satz 7.3.1.3 lässt sich einprägsam mittels Diagrammen darstellen. Es gilt sogar:

**Satz 7.3.1.4.** *Eine abelsche Gruppe $D$ ist genau dann teilbar, wenn zu jedem Diagramm*

$$\begin{array}{ccc} 0 \longrightarrow U & \xrightarrow{g} & A \\ & \big\downarrow f & \\ & D & \end{array}$$

*mit injektivem $g$ ein Homomorphismus $h$ existiert, so dass das Diagramm*




*kommutiert.*

*Beweis.* Wegen der Injektivität von $g$ dürfen wir $U$ oBdA als Untergruppe von $A$ betrachten. Dass aus der Teilbarkeit von $D$ die im Satz behauptete Diagrammeigenschaft folgt, ist daher nur eine Umformulierung von Satz 7.3.1.3. Zu zeigen bleibt daher die Umkehrung. Gelte also für $D$ die im Satz formulierte Diagrammeigenschaft, sei $a \in D$ und $n \in \mathbb{Z} \setminus \{0\}$. Ist $a$ von unendlicher Ordnung (Fall 1), so wählen wir $A := \mathbb{Q}$, $U := \mathbb{Z} \leq \mathbb{Q} = A$, $f\colon k \mapsto ka$ und die Inklusionsabbildung $g = \iota\colon \mathbb{Z} \to \mathbb{Q}$, $k \mapsto k$. Laut Voraussetzung gibt es einen Homomorphismus $h\colon \mathbb{Q} \to D$ mit $f = h \circ g$. Dann hat das Element $d := h(\frac{1}{n}) \in D$ die gewünschte Eigenschaft: $nd = nh(\frac{1}{n}) = h(n\frac{1}{n}) = h \circ g(1) = f(1) = a$. Hat $a$ hingegen eine endliche Ordnung $m \in \mathbb{N}$ (Fall 2), so wählt man statt $\mathbb{Q}$ die Gruppe $A := \mathbb{Q}/m\mathbb{Z}$, ihre Untergruppe $U := \mathbb{Z}/m\mathbb{Z}$, den (wohldefinierten) Homomorphismus $f\colon k+m\mathbb{Z} \mapsto ka$ und die Inklusionsabbildung $g = \iota\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Q}/m\mathbb{Z}$, $k+m\mathbb{Z} \mapsto k+m\mathbb{Z}$. Die laut Voraussetzung existierende Fortsetzung $h$ von $f$ liefert wie im Fall 1 ein Element $d := h(\frac{1}{n} + m\mathbb{Z}) \in D$ mit

$$nd = nh(\frac{1}{n}+m\mathbb{Z}) = h(n(\frac{1}{n}+m\mathbb{Z})) = h(1+m\mathbb{Z}) = (h\circ g)(1+m\mathbb{Z}) = f(1+m\mathbb{Z}) = 1a = a.$$

□

Die Erweiterung der additiven Gruppe $\mathbb{Z}$ zur teilbaren Gruppe $\mathbb{Q}$ lässt sich auf beliebige abelsche Gruppen verallgemeinern:

**Satz 7.3.1.5.** *Jede abelsche Gruppe lässt sich in eine teilbare Gruppe einbetten.*

*Beweis.* Sei $A$ eine beliebige abelsche Gruppe. Es gibt eine freie abelsche Gruppe $F$ (zum Beispiel die von sämtlichen $a \in A$ frei erzeugte abelsche Gruppe) und einen surjektiven Homomorphismus $\varphi\colon F \to A$. Sei $K \leq F$ der Kern von $\varphi$. Als freie abelsche Gruppe ist $F$ isomorph zur Gruppe $\bigoplus_{i\in I} \mathbb{Z}$, wobei eine Indexmenge $I$ mit $|I| = \dim_{\mathbb{Z}} F$ zu wählen ist. Diese Isomorphie werde durch den Isomorphismus $\psi\colon F \to \bigoplus_{i\in I} \mathbb{Z}$ vermittelt. Bezeichne $\iota$ die kanonische Einbettung $\iota\colon \bigoplus_{i\in I} \mathbb{Z} \to D_0 := \bigoplus_{i\in I} \mathbb{Q}$ (Inklusionsabbildung). $D_0$ ist teilbar, folglich auch die Faktorgruppe $D := D_0/\iota\psi(K)$. Offenbar gilt

$$A \cong F/K \cong \frac{\iota\psi(F)}{\iota\psi(K)} \leq \frac{D_0}{\iota\psi(K)} = D.$$

Also lässt sich $A$ in die teilbare Gruppe $D$ einbetten. □

Eine der wichtigsten Eigenschaften teilbarer Gruppen besteht darin, dass sie, eingebettet in eine umfassende abelsche Gruppe, stets direkte Summanden derselben sind.

**Satz 7.3.1.6.** *Jede teilbare Untergruppe $D$ einer abelschen Gruppe $A$ ist direkter Faktor, d.h. es gibt eine Untergruppe $U \subseteq A$ mit $A = D \oplus U$.*

*Beweis.* Der Beweis gelingt überraschend einfach mit Hilfe zerfallender Sequenzen: Zur kurzexakten Sequenz $0 \to D \to A \to A/D \to 0$ gibt es nach Satz 7.3.1.3 einen die Identität auf $D$ fortsetzenden Homomorphismus $\rho\colon A \to D$, also eine Retraktion. Nach Satz 7.2.3.8 ist also $A = D \oplus U$ mit geeignetem $U$. □

Mit den nunmehr zur Verfügung stehenden Hilfsmitteln lässt sich ohne allzu große Schwierigkeiten ein vollständiger Überblick über die Struktur teilbarer Gruppen gewinnen:

**Satz 7.3.1.7.** *Jede teilbare Gruppe $D$ ist isomorph zu einer direkten Summe von Kopien der additiven Gruppe $\mathbb{Q}$ der rationalen Zahlen sowie von Prüferschen Gruppen $\mathbb{C}_{p^\infty}$, $p \in \mathbb{P}$, also*

$$D \cong \bigoplus_{i \in I_0} \mathbb{Q} \oplus \bigoplus_{p \in \mathbb{P}} \bigoplus_{i \in I_p} C_{p^\infty},$$

*wobei die Kardinalitäten der Indexmengen $I_0$ und $I_p$, $p \in \mathbb{P}$, durch $D$ eindeutig bestimmt sind.*

Der Beweis dieses Satzes ergibt sich aus der folgenden Übungsaufgabe, die mit einigen Anleitungen versehen ist.

**UE 406** ► **Übungsaufgabe 7.3.1.8.** Beweisen Sie Satz 7.3.1.7, indem Sie mit Hilfe der bisherigen Resultate folgende Aussagen beweisen. ◄ **UE 406**

1. Ist $p \in \mathbb{P}$ und $D$ eine teilbare $p$-Gruppe (d.h. die Ordnungen sämtlicher Elemente sind $p$-Potenzen), so ist $D \cong \bigoplus_{i \in I} C_{p^\infty}$ eine direkte Summe von isomorphen Kopien der $p$-Prüfergruppe $C_{p^\infty}$. Hinweis: Die Menge aller Elemente der Ordnung $p$ bilden in natürlicher Weise einen Vektorraum über $\mathrm{GF}(p)$. Sei $X$ eine Basis. Zu jedem $x \in X$ wähle man eine Folge von $x_n \in D$ mit $x_1 = x$ und $px_{n+1} = x_n$ für $n = 1, 2, \ldots$. Die von den $x_n$ erzeugte Untergruppe $U_x \leq D$ ist isomorph zu $C_{p^\infty}$. Damit gilt $D \cong \bigoplus_{x \in X} U_x$.

2. Jede Torsionsgruppe $G$ (d.h. alle Elemente von $G$ haben endliche Ordnung) ist nach Satz 3.3.3.6 die direkte Summe ihrer $p$-Komponenten $G_p$ (= Mengen aller Elemente von $p$-Potenz-Ordnung), $p \in \mathbb{P}$. Ist $G$ teilbar, so müssen die $G_p$ ebenfalls teilbar sein.

3. Ist $D$ torsionsfrei und $x \in D$, so gibt es zu jedem $n \in \mathbb{Z} \setminus \{0\}$ ein sogar eindeutiges Element $y \in D$ mit $ny = x$. Bezeichnet man dieses mit $\frac{1}{n}x$, so ist für alle $\frac{p}{q} \in \mathbb{Q}$, $p, q \in \mathbb{Z}$, das Element $\frac{p}{q}x := p(\frac{1}{q}x)$ wohldefiniert. Auf diese Weise wird $D$ zu einem Vektorraum über $\mathbb{Q}$. Daraus folgt die Isomorphie $D \cong \bigoplus_{i \in I} \mathbb{Q}$ abelscher Gruppen, wenn $I$ geeignet gewählt wird.

4. Die Torsionselemente (Elemente endlicher Ordnung) bilden eine teilbare Untergruppe $D_t$ mit $D \cong D_0 \oplus D_t$ und torsionsfreiem, teilbarem $D_0 \cong D/D_t$.

5. Setzen Sie das Bisherige zu einem Beweis für die Existenz der behaupteten Darstellung zusammen.

6. Beweisen Sie die Eindeutigkeitsaussage in Satz 7.3.1.7, indem Sie geeignete Vektorräume und deren Dimension betrachten.

### 7.3.2 Injektive Moduln

Als natürliche Verallgemeinerung des Begriffs einer teilbaren Gruppe von abelschen Gruppen, d.h. von Moduln über dem Ring $\mathbb{Z}$, auf Moduln über beliebigen Ringen erweist sich der Begriff des injektiven Moduls. Zunächst zur Definition von Injektivität, wie sie durch Satz 7.3.1.4 motiviert wird.

**Definition 7.3.2.1.** Ein $R$-Modul $J$ heißt *injektiv*, wenn für alle Diagramme von $R$-Modul-Homomorphismen

$$\begin{array}{ccc} 0 \longrightarrow A & \xrightarrow{g} & B \\ & \downarrow{\scriptstyle f} & \\ & J & \end{array}$$

mit injektivem $g$ ein $R$-Modul-Homomorphismus $h$ existiert, so dass das Diagramm

$$\begin{array}{ccc} 0 \longrightarrow A & \xrightarrow{g} & B \\ & {\scriptstyle f}\downarrow \swarrow {\scriptstyle h} & \\ & J & \end{array}$$

kommutiert.

Aus Satz 7.3.1.4 folgt unmittelbar:

**Proposition 7.3.2.2.** *Eine abelsche Gruppe ist teilbar genau dann, wenn sie als unitärer $\mathbb{Z}$-Modul injektiv ist.*

Viele Eigenschaften teilbarer Gruppen lassen sich auf den allgemeineren Fall injektiver Moduln übertragen, allerdings nicht immer auf triviale Weise. Für Resultate, die wir im Folgenden nicht mehr benötigen, begnügen wir uns teilweise mit recht knappen Beweisskizzen. Noch relativ einfach ist die folgende Übungsaufgabe:

**UE 407 ► Übungsaufgabe 7.3.2.3.** Zeigen Sie: **◄ UE 407**

1. Vektorräume sind als Moduln injektiv.

2. Das direkte Produkt von $R$-Moduln $\prod_{i\in I} J_i$ ist genau dann injektiv, wenn alle $J_i$, $i \in I$ injektiv sind.

Deutlich mehr Aufwand erfordert der Beweis der Verallgemeinerung von Satz 7.3.1.5:

**Satz 7.3.2.4.** *Jeder unitäre $R$-Modul lässt sich in einen injektiven unitären $R$-Modul einbetten.*

**UE 408** ► **Übungsaufgabe 7.3.2.5.** (Anspruchsvoll!) Beweisen Sie Satz 7.3.2.4, indem Sie folgende Aussagen zeigen: ◄ **UE 408**

1. Zeigen Sie: Sei $R$ ein Ring mit 1 und $J$ ein unitärer $R$-Modul. Dann ist $J$ genau dann injektiv, wenn es zu jedem Linksideal $L$ von $R$ und jedem $R$-Modulhomomorphismus $f\colon L \to J$ eine Fortsetzung $h\colon R \to J$ gibt. (Hinweis: Schlagen Sie in der Literatur nach. Der Beweis dieser Aussage ist beispielsweise als Lemma 3.8 in Kapitel IV von Hungerfords Algebra-Buch enthalten.)

2. Ist $J$ eine teilbare abelsche Gruppe und $R$ ein Ring mit 1, dann ist $\mathrm{Hom}_{\mathbb{Z}}(R, J)$ (auf natürliche Weise) ein injektiver unitärer $R$-Modul. Hinweis: Verwenden Sie den ersten Teil und die entsprechende Eigenschaft teilbarer Gruppen.

3. Folgern Sie Satz 7.3.2.4, indem Sie den $R$-Modul zunächst als $\mathbb{Z}$-Modul auffassen und in $\mathrm{Hom}_{\mathbb{Z}}(R, J)$ einbetten.

Diese Hilfsmittel dienen auch beim Beweis der folgenden Charakterisierung injektiver Moduln, die an Satz 7.3.1.6 anschließt.

**Satz 7.3.2.6.** *Sei $R$ ein Ring mit 1 und $J$ ein unitärer $R$-Modul. Dann sind folgende Aussagen äquivalent:*

*(i)* *$J$ ist injektiv.*

*(ii)* *Jede kurzexakte Sequenz $0 \to J \xrightarrow{f} A \xrightarrow{g} B \to 0$ zerfällt. Insbesondere ist $A \cong J \oplus B$.*

*(iii)* *Sei $J \leq B$. Dann existiert ein $R$-Modul $K$, sodass $B = J \oplus K$.*

**UE 409** ► **Übungsaufgabe 7.3.2.7.** Beweisen Sie Satz 7.3.2.6. Hinweis für die erste Implikation: Dualisieren Sie den späteren Beweis von Satz 7.3.3.4. ◄ **UE 409**

### 7.3.3 Projektive Moduln

Die Definition von Projektivität eines Moduls ergibt sich aus jener von Injektivität durch Dualisierung.

**Definition 7.3.3.1.** Ein $R$-Modul $P$ heißt *projektiv*, wenn für alle Diagramme von $R$-Modul-Homomorphismen

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow{\scriptstyle f} & & \\ A & \xrightarrow{g} & B & \longrightarrow & 0 \end{array}$$

mit surjektivem $g$ ein $R$-Modul-Homomorphismus $h$ existiert, sodass das Diagramm

$$\begin{array}{ccccc} & & P & & \\ & {\scriptstyle h}\swarrow & \downarrow{\scriptstyle f} & & \\ A & \xrightarrow{g} & B & \longrightarrow & 0 \end{array}$$

kommutiert.

Die wichtigsten Beispiele projektiver Moduln sind die freien:

**Satz 7.3.3.2.** *Jeder freie $R$-Modul ist projektiv.*

*Beweis.* Sei $F$ ein freier $R$-Modul mit Basis $X$. Für den Beweis des Satzes haben wir uns irgendwelche $R$-Moduln $A$ und $B$ sowie $R$-Modulhomomorphismen $g\colon A \to B$ und $f\colon F \to B$ vorzugeben, wobei $g$ surjektiv sei. Wir müssen einen Homomorphismus $h\colon F \to A$ mit $f = g \circ h$ finden.

$$\begin{array}{ccccc} & & F & & \\ & {\scriptstyle h}\swarrow & \downarrow{\scriptstyle f} & & \\ A & \xrightarrow{g} & B & \longrightarrow & 0 \end{array}$$

Wegen der Surjektivität von $g$ gibt es zu jedem $x \in X$ ein $a_x \in A$ mit $g(a_x) = f(x)$. Da $F$ frei über $X$ ist, gibt es einen (eindeutigen) Homomorphismus $h\colon F \to A$ mit $h(x) = a_x$ für alle $x \in X$. Somit gilt $(g \circ h)(x) = g(a_x) = f(x)$ für alle $x$ aus dem Erzeugendensystem $X$ von $F$. Weil sowohl $g \circ h$ als auch $f$ Homomorphismen sind, müssen sie sogar auf dem Erzeugnis von $X$, also auf ganz $F$ übereinstimmen, womit $f = g \circ h$ bewiesen ist. □

Später (siehe Korollar 7.4.2.5) werden wir sehen, dass für Moduln über Hauptidealringen die Begriffe frei und projektiv sogar zusammenfallen. Im allgemeinen Fall müssen projektive Moduln aber nicht frei sein. Zur Illustration einfache Übungen:

**UE 410 ► Übungsaufgabe 7.3.3.3.** Zeigen Sie: **◄ UE 410**

1. Der $\mathbb{Z}$-Modul $\mathbb{Q}$ ist nicht projektiv.
2. $\mathbb{Z}_2$ und $\mathbb{Z}_3$ sind projektive $\mathbb{Z}_6$-Moduln, aber nicht frei.
3. Die direkte Summe von $R$-Moduln $\bigoplus_{i\in I} P_i$ ist genau dann projektiv, wenn alle $P_i$, $i \in I$, projektiv sind.

Die für uns wichtigsten Strukturaussagen über projektive Moduln sind in folgendem, zu 7.3.2.6 dualem Satz enthalten.

**Satz 7.3.3.4.** *Für einen $R$-Modul $P$ sind folgende Bedingungen äquivalent:*

*(i)* *$P$ ist projektiv.*

*(ii)* *Jede kurzexakte Sequenz $0 \to A \xrightarrow{f} B \xrightarrow{g} P \to 0$ zerfällt. Insbesondere ist $B \cong A \oplus P$.*

*(iii)* *Es existiert ein freier Modul $F$ und ein $R$-Modul $K$, so dass $F \cong K \oplus P$.*

*Beweis.* Wir gehen zyklisch vor, indem wir die drei Implikationen (i)⇒(ii), (ii)⇒(iii) unf (iii)⇒(i) beweisen.
(i)⇒(ii): Sei die kurzexakte Sequenz

$$0 \to A \xrightarrow{f} B \xrightarrow{g} P \to 0$$

vorgegeben. Die Projektivität von $P$ liefert ein $h$, so dass

$$\begin{array}{ccccc} & & & & P \\ & & \overset{h}{\swarrow} & \overset{\nearrow}{\underset{g}{\searrow}} & \downarrow{\scriptstyle \mathrm{id}_P} \\ B & \xrightarrow{\quad} & P & \longrightarrow & 0 \end{array}$$

kommutiert. So ein $h$ ist eine Sektion:

$$0 \longrightarrow A \xrightarrow{f} B \underset{h}{\overset{g}{\rightleftarrows}} P \longrightarrow 0$$

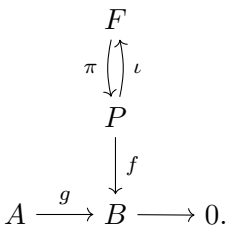
Nach Satz 7.2.3.8 zerfällt dann die kurzexakte Sequenz, und $B \cong A \oplus P$.

(ii)⇒(iii): Nach Korollar 7.2.1.7 ist $P$ homomorphes Bild eines freien $R$-Moduls $F$ unter einem Homomorphismus $\kappa$. Definiere $K := \ker \kappa$. Die Sequenz $0 \to K \xrightarrow{\iota} F \xrightarrow{\kappa} P \to 0$ ist kurzexakt. Nach (ii) ist damit $F \cong K \oplus P$.

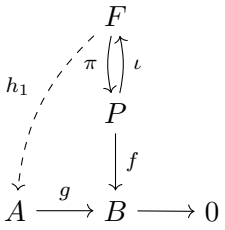
(iii)⇒(i): Sei o.B.d.A. $F = K \oplus P$ frei. Gegeben sei ein Diagramm

$$\begin{array}{ccccc} & & & & P \\ & & & & \downarrow{\scriptstyle f} \\ A & \xrightarrow{g} & B & \longrightarrow & 0 \end{array}$$

mit surjektivem $g$. Betrachte nun




Darin ist $\iota : p \mapsto (0,p)$ und $\pi : (k,p) \mapsto p$. Da $F$ frei und somit nach Satz 7.3.3.2 projektiv ist, gibt es einen $R$-Modul-Homomorphismus $h_1$, so dass




kommutiert. Dann leistet $h := h_1\iota$ das Gewünschte. Somit ist $P$ projektiv. □

## 7.4 Moduln über Hauptidealringen

Wir spezialisieren nun auf den Fall eines Hauptidealrings $R$ (siehe auch Abschnitt 5.2, insbesondere 5.2.2). Definitionsgemäß ist das ein Integritätsbereich, in dem jedes Ideal $I$ von der Form $I = rR$ mit einem Erzeugenden $r \in R$ ist. Insbesondere ist $R$ also faktoriell, und die Primelemente in $R$ sind genau die irreduziblen. Alle $R$-Moduln seien unitär. Speziell sind damit für $R = \mathbb{Z}$ auch weiterhin die abelschen Gruppen erfasst. Wir beginnen mit einigen Definitionen und Schreibweisen, die das Konzept der Ordnung eines Gruppenelementes verallgemeinern (7.4.1). Sodann wenden wir uns den freien Moduln zu und zeigen, dass deren Untermoduln wieder frei sind. Als Folgerung ergibt sich daraus, dass unter den Moduln über Hauptidealringen die freien genau die projektiven sind und weiters, dass endlich erzeugte torsionsfreie Moduln frei sind (7.4.2). Besonders gut versteht man die Struktur endlich erzeugter Moduln, die durch den Hauptsatz beschrieben wird. Ihm zufolge sind sie direkte Summen endlich vieler zyklischer Moduln. Die genaue Formulierung sowie ein Überblick über die Beweisstrategie sind Gegenstand von 7.4.3. Nach einer genaueren Untersuchung von Torsionsmoduln (7.4.4), kann der Beweis in 7.4.5 abgeschlossen werden. Als interessante Anwendung davon ergibt sich daraus die aus der Linearen Algebra bekannte Jordansche Normalform quadratischer Matrizen (7.4.6).

### 7.4.1 Notationen und Sprechweisen

Bevor wir den Hauptsatz formulieren, brauchen wir die Verallgemeinerungen einiger Begriffe, Schreib- und Sprechweisen für $R$-Moduln vom Fall abelscher Gruppen ($R = \mathbb{Z}$)

auf einen beliebigen Hauptidealring $R$. (Manche der Begriffe lassen sich sogar für einen beliebigen Integritätsbereich $R$ definieren.)
Sei also $R$ ein Hauptidealring, $r \in R$, $p \in R$ prim, $A$ ein unitärer $R$-Modul (geschrieben als Linksmodul) und $a \in A$. Die Assoziiertheitsrelation in $R$ sei mit $\sim$ bezeichnet, d.h.: $r \sim s$ bedeutet $r = es$ für eine Einheit (ein multiplikativ invertierbares Element) $e \in R$. Die Assoziiertenklasse von $r$ wird also mit $[r]_\sim$ bezeichnet. Der einfacheren Notation halber werden wir nicht immer streng zwischen $r$ und $[r]_\sim$ unterscheiden. Über diese Konventionen hinausgehend verwenden wir folgende Schreibweisen, die im Lichte der anschließenden Proposition 7.4.1.1 zu sehen sind: :

- $\mathbb{P}(R) := \{p \in R : p \text{ prim}\}$ und $\mathbb{P}_\sim(R) := \{[p]_\sim : \ p \in \mathbb{P}(R)\}$. Häufig wird es vorteilhaft sein, Vertretersysteme $P$ der Assoziertenklassen sämtlicher Primelemente zu betrachten.
- $\mathcal{O}_a := \{r \in R : r \cdot a = 0\} \lhd R$ heißt *Ordnungsideal* von $a \in A$.[5] Ist $\mathcal{O}_a = rR$, so heißt $r$ oder, genauer, $[r]_\sim$ auch die *Ordnung* von $a$.
- $A_t := \{a \in A : \mathcal{O}_a \neq \{0\}\} \leq A$ heißt der *Torsionsmodul* von $A$. Elemente $a \in A_t$ heißen *Torsionselemente*.
- $A$ heißt *Torsionsmodul,* wenn $A = A_t$, und *torsionsfrei,* wenn $A_t = \{0\}$.
- Der von einem Element $a$ erzeugte Untermodul hat die Form $Ra$ und heißt *zyklischer* Untermodul der Ordnung $r$.
- $A$ heißt *$p$-primär,* $p \in \mathbb{P}$, falls es zu jedem $a \in A$ ein $n \in \mathbb{N}$ mit $\mathcal{O}_a = p^n R$ gibt.
- Für $p \in \mathbb{P}(R)$ heißt $A(p) := \{a \in A : \exists n \in \mathbb{N} : \ p^n a = 0\} \leq A$ der *$p$-Anteil* von $A$ (Man beachte: $p_1 \sim p_2$ impliziert $A(p_1) = A(p_2)$. Deshalb ist auch $A([p]_\sim) := A(p)$ wohldefiniert.)

Sehr leicht überprüft man die impliziten Behauptungen in obigen Definitionen:

**Proposition 7.4.1.1.** *Mit obigen Bezeichnungen gilt:*

(1) *$\mathcal{O}_a$ ist tatsächlich ein Ideal von $R$.*
(2) *$A_t \leq A$.*
(3) *Für jedes $p \in \mathbb{P}(R)$ ist $A(p) \leq A_t$.*
(4) *Für $a \in A$ und $r \sim s \in R$ ist $ra = 0$ genau dann, wenn $sa = 0$.*
(5) *Aus $p_1 \sim p_2$ folgt $A(p_1) = A(p_2)$.*
(6) *Sind $p_1, p_2 \in \mathbb{P}(R)$ nicht assoziiert, so ist $A(p_1) \cap A(p_2) = \{0\}$.*

**UE 411 ► Übungsaufgabe 7.4.1.2.** Beweisen Sie Proposition 7.4.1.1. **◄ UE 411**

[5] Man unterscheide die so definierten Ordnungsideale im ringtheoretischen Sinn von Idealen in Halbordnungen, die manchmal gleichfalls Ordungsideale genannt werden.

### 7.4.2 Untermoduln freier Moduln

Fasst man abelsche Gruppen als $\mathbb{Z}$-Moduln auf, so sind die Torsionselemente offenbar genau jene mit endlicher Ordnung. Deshalb sind freie abelsche Gruppen auch torsionsfrei. Im endlich erzeugten Fall werden sich auch umgekehrt torsionsfreie Moduln als frei erweisen. Allgemein gilt das nicht, wie der torsionsfreie aber nicht freie $\mathbb{Z}$-Modul $\mathbb{Q}$ zeigt.
Weiters werden wir von der folgenden Beobachtung Gebrauch machen.

**Proposition 7.4.2.1.** *Sei $R$ ein Hauptidealring, $I \lhd R$ ein Ideal von $R$ und $A$ ein zyklischer unitärer $R$-Modul mit erzeugendem Element $a$.*

1. *Jedes $I \lhd R$ ist als $R$-Modul frei, wobei nur zwei Fälle auftreten können: $I \cong \{0\}$ (frei über der leeren Menge) oder $I \cong R$ (frei über dem Singleton seines Erzeugers).*

2. *Sei $A$ zyklisch mit erzeugendem Element $a \in A$. Gilt $\mathcal{O}_a = \{0\}$, so ist $A \cong R$ und und $A$ frei über $\{a\}$. Gilt hingegen $\mathcal{O}_a = (p^n) = p^n R$ mit $p \in \mathbb{P}(R)$ und positivem $n \in \mathbb{N}$, so ist $A$ nicht frei und $p$-primär.*

Der Beweis ist nicht schwierig und Gegenstand einer Übungsaufgabe:

**UE 412** ► **Übungsaufgabe 7.4.2.2.** Beweisen Sie Proposition 7.4.2.1. Hinweis: Betrachten Sie den Homomorphismus $f_a \colon R \to A$, $r \mapsto ra$. Überlegen Sie weiter, dass $f_a$ surjektiv ist mit Kern $\mathcal{O}_a = rR$ für ein $r \in R$ und verwenden Sie den Homomorphiesatz. ◄ **UE 412**

Der berühmte Satz von Nielsen-Schreier besagt, dass jede Untergruppe einer freien Gruppe wieder frei ist. Ein Beweis (zum Beispiel unter Zuhilfenahme von Fundamentalgruppen und Überlagerungen aus der algebraischen Topologie) würde uns hier zu weit führen. Leichter zu beweisen ist das analoge Resultat für abelsche Gruppen, hier etwas allgemeiner ausgesprochen für Moduln über Hauptidealringen:

**Satz 7.4.2.3.** *Sei $F$ ein freier Modul über dem Hauptidealring $R$ und $G \leq F$ ein Untermodul. Dann ist auch $G$ ein freier $R$-Modul, und es gilt* $\operatorname{rang}(G) \leq \operatorname{rang}(F)$.

*Beweis.* Sei $X = \{x_i : i \in I\}$ eine Basis von $F$ und $\leq$ eine Wohlordnung von $I$, also $|I| = \operatorname{rang}(F)$. Wir schreiben $i+1$ für den Nachfolger von $i \in I$ und definieren

$$F_i := \langle x_j : j \leq i \rangle$$
$$G_i := G \cap F_i.$$

Die $F_i$ bilden eine aufsteigende transfinite Mengenfolge, was sich auch auf die $G_i$ überträgt. Man beachte, dass auch $G_i = G \cap F_i = G_{i+1} \cap F_i$ gilt. Deshalb gilt nach dem ersten Isomorphiesatz 2.3.6.3:

$$G_{i+1}/G_i = G_{i+1}/(G_{i+1} \cap F_i) \cong (G_{i+1} + F_i)/F_i \leq F_{i+1}/F_i \cong R.$$

Also ist $G_{i+1}/G_i$ isomorph zu einem Untermodul von $R$. Jeder Untermodul von $R$ ist ein Ideal von $R$ und nach Proposition 7.4.2.1 frei vom Rang 0 oder 1. Laut Satz 7.3.3.4 und 7.3.3.2 zerfällt die Sequenz

$$0 \to G_i \to G_{i+1} \to G_{i+1}/G_i \to 0,$$

und es gilt $G_{i+1} \cong G_i \oplus (G_{i+1}/G_i) \cong G_i \oplus y_i R$. (Hier ist $y_i = 0$ genau dann, wann $G_i = G_{i+1}$.) Mittels transfiniter Induktion zeigt man (Übung) $G \cong \bigoplus_{i\in I} y_i R \cong \bigoplus_{i\in I_1} R$ mit $I_1 = \{i : y_i \neq 0\}$. $B := \{y_i : i \in I_1\}$ ist dann eine Basis von $G$, folglich gilt $\operatorname{rang}(G) = |B| \leq |I| = \operatorname{rang}(F)$. □

**UE 413** ► **Übungsaufgabe 7.4.2.4.** Führen Sie jenen Schritt im Beweis von Satz 7.4.2.3 in Einzelnen aus, wo mittels transfiniter Induktion auf $G \cong \bigoplus_{i\in I_1} R$ geschlossen wird. ◄ **UE 413**

An dieser Stelle erinnern wir uns an Satz 7.3.3.4, wonach jeder projektive Modul $P$ direkter Summand und daher Untermodul eines freien Moduls, über einem Hauptidealring laut Satz 7.4.2.3 also selbst frei ist. Umgekehrt sind freie Moduln nach Satz 7.3.3.2 immer projektiv, also:

**Korollar 7.4.2.5.** Ein Modul über einem Hauptidealring ist frei genau dann, wenn er projektiv ist.

Eine weitere Konsequenz von Satz 7.4.2.3 bezieht sich auf die Kardinalität von Erzeugendensystemen beliebiger Moduln:

**Korollar 7.4.2.6.** Ist $A$ ein $R$-Modul mit Erzeugendensystem $E \subseteq A$ und $B \leq A$ ein Untermodul. Dann hat $B$ ein Erzeugendensystem $E_B \subseteq B$ mit $|E_B| \leq |E|$. Insbesondere ist jeder Untermodul eines endlich erzeugten Moduls endlich erzeugt.

*Beweis.* Nach 7.2.1.7 ist $A$ homomorphes Bild eines über $E$ freien $R$-Moduls $F$ unter einem Epimorphismus $f : F \to A$. Sei $G := f^{(-1)}(B) \leq F$ das Urbild von $B$ unter $f$. Nach Satz 7.4.2.3 ist $G$ frei mit einem Erzeugendensystem $X \subseteq F$ mit $|X| \leq |E|$. Dann ist $E_B := f(X) \subseteq B$ ein Erzeugendensystem von $B$ mit $|E_B| \leq |X| \leq |E|$, was zu zeigen war. □

Im endlich erzeugten Fall gilt folgende bemerkenswerte Äquivalenz:

**Satz 7.4.2.7.** *Ist $A$ ein endlich erzeugter Modul über dem Hauptidealring $R$, so ist $A$ genau dann frei, wenn $A$ torsionsfrei ist.*

*Beweis.* Dass jeder freie Modul torsionsfrei ist, werden wir im Weiteren nicht benötigen. Der Beweis ist nicht sehr schwierig und Inhalt einer Übungsaufgabe. Hier führen wir nur den Beweis, dass jeder endlich erzeugte torsionsfreie Modul $A$ frei ist.
Sei dazu $X$ ein endliches Erzeugendensystem von $A$ mit $0 \notin X$ und $S = \{x_1, \ldots, x_k\}$ eine maximale linear unabhängige Teilmenge von $X$. $F$ sei der von $S$ frei erzeugte $R$-Modul. Für jedes $y \in X \setminus S$ gibt es wegen der Maximalität von $S$ Koeffizienten $r_y, r_i \in$

$R$, $i = 1, \ldots, k$, (nicht alle gleich 0), so dass $r_y y + \sum_{i=1}^{k} r_i x_i = 0$. Dann gilt $r_y y = -\sum_{i=1}^{k} r_i x_i \in F$ und außerdem ist $r_y \neq 0$ für jedes $y \in X \setminus S$, da sonst auch alle $r_i = 0$ sein müssten. Wir setzen $r := \prod_{y \in X \setminus S} r_y$. Dann ist $rX \subseteq F$ und damit $rA = r\langle X \rangle \leq F$. Nach Satz 7.4.2.3 ist $rA$ als Untermodul eines freien Moduls selbst frei. Die Abbildung $f\colon A \to rA,\ a \mapsto ra$ ist ein $R$-Modul-Epimorphismus, und wegen der Torsionsfreiheit von $A$ gilt $\ker f = \{0\}$. Also ist $A \cong rA$ ebenfalls frei. □

**UE 414** ► **Übungsaufgabe 7.4.2.8.** Zeigen Sie, dass jeder freie Modul über einem Hauptidealring torsionsfrei ist. ◄ **UE 414**

Für die Strukturtheorie werden wir noch folgenden Satz benötigen, wonach endlich erzeugte Moduln in eine direkte Summe aus einem freien und einem Torsionsmodul zerfallen.

**Satz 7.4.2.9.** *Sei $R$ ein Hauptidealring und $A$ ein endlich erzeugter $R$-Modul. Dann gilt $A = A_t \oplus F$, wobei $F$ ein freier $R$-Modul von endlichem Rang ist mit $F \cong A/A_t$.*

*Beweis.* Für jedes Erzeugendensystem $E \subseteq A$ von $A$ bilden sämtliche $a + A_t$ ein Erzeugendensystem des Faktormoduls $A/A_t$. Folglich vererbt sich die endliche Erzeugtheit von $A$ auf $A/A_t$. $A/A_t$ ist aber auch torsionsfrei: Sei $r(a + A_t) = 0$ in $A/A_t$ mit $r \neq 0$ und $a \in A$. Zu zeigen ist $a \in A_t$. Zunächst folgt aus unserer Annahme $ra \in A_t$. Weil $A_t$ ein Torsionsmodul ist, gibt es in $R$ ein $s \neq 0$ mit $sra = 0 \in A$. Aus der Nullteilerfreiheit von $R$ folgt $rs \neq 0$ und somit $a \in A_t$. Also ist $F := A/A_t$ tatsächlich torsionsfrei, als Faktor von $A$ außerdem endlich erzeugt, nach Satz 7.4.2.7 daher frei und nach Satz 7.3.3.2 projektiv. Laut Satz 7.3.3.4 zerfällt dann die Sequenz

$$0 \to A_t \to A \to F \to 0,$$

und es gilt $A \cong A_t \oplus F$. □

### 7.4.3 Formulierung des Hauptsatzes und Beweisstrategie

Der Hauptsatz besagt nun, dass jeder endlich erzeugte $R$-Modul $A$ die direkte Summe endlich vieler zyklischer Moduln ist. Diese zyklischen Summanden können so gewählt werden, dass eine gewisse Teilerkettenbedingung erfüllt ist, oder, alternativ, dass jeder der zyklischen Summanden entweder frei oder $p$-primär für ein geeignetes $p \in \mathbb{P}(R)$ ist. Die folgende Formulierung enthält beide Varianten:

**Satz 7.4.3.1** (Hauptsatz über endlich erzeugte $R$-Moduln)**.** *Sei $A$ ein endlich erzeugter Modul über dem Hauptidealring $R$. Dann folgt:*

*(a) $A \cong R^n \oplus \bigoplus_{i=1}^{k} R/(p_i^{s_i} R)$ mit $p_i \in \mathbb{P}(R)$. Sowohl die Zahlen $k, n \in \mathbb{N}$ als auch die Ideale $p_i^{s_i} R$ (und somit die $s_i$ sowie bis auf Assoziiertheit die $p_i$) sind dabei bis auf die Reihenfolge eindeutig bestimmt. Die $p_i^{s_i}$ heißen auch die* Elementarteiler *von $A$.*

*(b)* $A \cong R^n \oplus \bigoplus_{i=1}^{t} R/(r_i R)$ *mit* $n \in \mathbb{N}$ *und* $r_1 \mid r_2 \mid \ldots \mid r_t \in R$*, wobei die* $r_i$ *weder* $0$ *noch Einheiten sind. Sowohl die Zahlen* $n, t \in \mathbb{N}$ *als auch die Ideale* $r_1 R, \ldots, r_t R$ *(und somit bis auf Assoziiertheit die* $r_i$*) sind dabei eindeutig bestimmt, genannt die* invarianten Faktoren *von* $A$*.*

*In beiden Formulierungen bezeichnet* $n$ *dieselbe natürliche Zahl, genannt der* Rang *von* $A$*, symbolisch* $n = \operatorname{rang}(A)$*.*

Durch Spezialisierung auf den Fall $r = \mathbb{Z}$ und abelsche Gruppen erhalten wir:

**Satz 7.4.3.2** (Hauptsatz über endlich erzeugte abelsche Gruppen)**.** *Sei* $G$ *eine endlich erzeugte abelsche Gruppe. Dann folgt:*

*(a)* $G \cong \mathbb{Z}^n \oplus \bigoplus_{i=1}^{k} C_{p_i^{s_i}}$ *mit* $p_i \in \mathbb{P}$*. Sowohl die Zahlen* $k, n \in \mathbb{N}$ *als auch die Primzahlpotenzen* $p^{s_i}$ *sind dabei bis auf die Reihenfolge eindeutig bestimmt. Die* $p_i^{s_i}$ *heißen auch die* Elementarteiler *von* $G$*.*

*(b)* $G \cong \mathbb{Z}^n \oplus \bigoplus_{i=1}^{t} C_{m_i}$ *mit* $n, t \in \mathbb{N}$ *und* $1 < m_1 \mid m_2 \mid \ldots \mid m_t \in \mathbb{N}$*. Sowohl die Zahlen* $n, t \in \mathbb{N}$ *als auch die Zahlen* $m_1, \ldots, m_t \in \mathbb{N}$ *sind dabei eindeutig bestimmt, genannt die* invarianten Faktoren *von* $G$*.*

*In beiden Formulierungen bezeichnet* $n$ *dieselbe natürliche Zahl, genannt der* Rang *von* $G$*, symbolisch* $n = \operatorname{rang}(G)$*.*

Der Rest dieses Abschnitts ist dem Beweis von Satz 7.4.3.1 und somit auch von Satz 7.4.3.2 gewidmet. Wir werden wie folgt vorgehen:
Nach Satz 7.4.2.9 lässt sich jeder endlich erzeugte Modul $A$ als direkte Summe $A = A_t \oplus F$ eines Torsions- und eines freien Moduls schreiben. Dass der freie Summand $F$ in eine direkte Summe zerfällt, wissen wir schon aus dem sehr allgemeinen Satz 7.2.1.5, wo die Hauptidealeigenschaft von $R$ gar keine Rolle spielt. Klarerweise können in einer direkten Zerlegung eines endlich erzeugten Moduls auch nur endlich viele nichttriviale Summanden auftreten. Somit bleibt der Torsionsmodul $A_t$ zu untersuchen. Zunächst werden wir, ganz in Analogie zur Situation bei abelschen Gruppen, zeigen, dass jeder Torsionsmodul – endlich oder unendlich erzeugt – die direkte Summe seiner $p$-Anteile ($p \in \mathbb{P}(R)$) ist. Als letzter substantieller Beweisteil des Hauptsatzes bleibt dann die Zerlegung eines endlich erzeugten $p$-Moduls in zyklische Summanden. Auch hier kann man wie bei endlichen abelschen Gruppen vorgehen, indem man zunächst einen einzigen, in einem naheliegenden Sinn maximalen zyklischen Summanden abspaltet. Dieser Schritt kann dann iteriert werden und wird wegen der Endlichkeitsvoraussetzung schließlich zum Ziel führen.

### 7.4.4 Torsionsmoduln

Wir rekapitulieren: Für einen Hauptidealring $R$, einen $R$-Modul $A$ besteht der *Torsionsanteil* $A_t$ von $A$ aus jenen $a \in A$, für die es ein $r \in R \setminus \{0\}$ gibt mit $ra = 0$. Für ein Primelement $p \in R$ heißt $A(p) := \{a \in A : \exists n \in \mathbb{N} :\ p^n a = 0\} \leq A$ der $p$-Anteil von $A$.

Jedes $a \in A_t$ heißt *Torsionselement* von $A$, jedes $a \in A(p)$ heißt $p$-Element.

Diese Begriffsbildungen sind unmittelbare Verallgemeinerungen entsprechender Konzepte für abelsche Gruppen aus Abschnitt 3.3. Das gilt auch für die folgenden Strukturaussagen: Jeder Torsionsmodul $A$ über $R$ ist die direkte Summe seiner $p$-Anteile $A(p)$, wobei $p$ ein Vertretersystem aller primen Assoziiertenklassen durchläuft. Im endlich erzeugten Fall lässt sich jedes $A(p)$ in eine direkte Summe zyklischer $p$-Moduln zerlegen. Man beachte die Analogie zu Satz 3.3.3.6.

**Satz 7.4.4.1.** *Ist $A$ ein unitärer Torsionsmodul über dem Hauptidealring $R$, dann gilt*

$$A = \bigoplus_{p \in P} A(p),$$

*wobei $p$ ein Vertretersystem $P$ sämtlicher Assoziiertenklassen primer Elemente von $R$ durchläuft. Ist $A$ endlich erzeugt, so sind nur endlich viele $A(p)$ nichttrivial.*

*Beweis.* Im ersten Teil zeigen wir, dass jedes $a \in A$ als endliche Summe geeigneter $p$-Elemente dargestellt werden kann. Da $R$ ein Hauptidealring ist, ist $\mathcal{O}_a = rR$ mit einem $r \in R$, insbesondere gilt $ra = 0$. Weil $a$ ein Torsionselement ist, folgt $r \neq 0$. Ist $r$ eine Einheit von $R$, so folgt $1 \in \mathcal{O}_a = (r) = R$. Daher ist $a = 1a = 0$ als leere Summe von $p$-Elementen darstellbar. Wir dürfen ab nun also annehmen, dass $r$ weder 0 noch eine Einheit ist. In diesem Fall gibt es eine Primfaktorzerlegung $r = \prod_{i=1}^{k} p_i^{e_i}$ mit $k \geq 1$, paarweise nicht assoziierten $p_i \in \mathbb{P}(R)$ und $e_i > 0$. Definiere

$$r_i := \frac{r}{p_i^{e_i}} \in R$$

für jedes $i = 1, \ldots, k$. Dann ist $\mathrm{ggT}(r_1, \ldots, r_k) = 1$. Daher gibt es $s_i \in R$, so dass $1_R = \sum_{i=1}^{k} s_i r_i$. Es folgt

$$a = 1_R a = \sum_{i=1}^{k} s_i r_i a,$$

und $p_i^{e_i} s_i r_i a = s_i r a = 0$, das heißt $s_i r_i a \in A(p_i)$. Also wird $A$ von den $A(p)$, $p$ prim, erzeugt.
Im zweiten Teil des Beweises bleibt zu zeigen, dass die Zerlegung direkt ist, d.h.

$$A(p) \cap \sum_{q \in P \setminus \{p\}} A(q) = \{0\}.$$

Sei also $a \in A(p) \cap \sum_{q \in P \setminus \{p\}} A(q)$. Dann gibt es ein $m \in \mathbb{N}$ mit $p^m a = 0$ und paarweise verschiedene $q_i \in P \setminus \{p\}$ sowie $a_i \in A(q_i)$, $q_i \neq p$, mit $a = \sum_{i=1}^{k} a_i$. Nun gibt es auch $m_i \in \mathbb{N}$ mit $q_i^{m_i} a_i = 0$. Definiere $d := \prod_{i=1}^{k} q_i^{m_i}$, dann ist $d$ teilerfremd zu $p^m$, und es gibt $s, t \in R$ mit $1_R = sp^m + td$. Nun folgt

$$a = 1_R a = sp^m a + tda = 0 + t \sum_{i=1}^{k} da_i = 0,$$

also ist die Summe direkt. Weil jedes Element $a \in A$ somit eine endliche Summe geeigneter $a_p \in A(p)$ ist, können bei endlich erzeugtem $A$ nur endlich viele nichttriviale $A(p)$ auftreten. □

Der wichtigste noch ausständige Schritt im Beweis des Hauptsatzes besteht darin, aus einem endlich erzeugten $p$-Modul einen zyklischen direkten Summanden abzuspalten. Auch hier kann man so vorgehen wie bei abelschen Gruppen, indem man zunächst folgendes Lemma beweist.

**Lemma 7.4.4.2.** *Sei $A$ ein $R$-Modul und $p \in \mathbb{P}(R)$, so dass $p^n A = \{0\}$ aber $p^{n-1}A \neq \{0\}$ für ein $n \in \mathbb{N}$. Habe $a \in A$ die Ordnung $p^n$, d.h. $p^n a = 0 \neq p^{n-1}a$. Dann gilt:*

*(a) Ist $A \neq Ra$, dann existiert ein $b \in A \setminus \{0\}$ mit $Ra \cap Rb = \{0\}$.*

*(b) Es gibt einen Untermodul $C$ von $A$ mit $A = Ra \oplus C$.*

*Beweis.* Zu Punkt (a): Zwecks Konstruktion von $b$ sei zunächst $c \in A \setminus Ra$ und $j \in \mathbb{N}\setminus\{0\}$ minimal mit $p^j c = r_1 a \in Ra$. Wir schreiben $r_1 = rp^k$ mit $k \in \mathbb{N}$ und $p \nmid r$. Daher gilt

$$0 = p^n c = p^{n-j}(p^j c) = p^{n-j} r_1 a = p^{n-j}(rp^k)a = p^{n-j+k} ra.$$

Da $p^{n-1}a \neq 0$ und $p \nmid r$, muss $n - j + k \geq n$ sein, also $1 \leq j \leq k$. Definiere

$$b := \underbrace{p^{j-1}c}_{\notin Ra} - \underbrace{rp^{k-1}a}_{\in Ra} \notin Ra.$$

Insbesondere ist $b \neq 0$, gleichzeitig $pb = p^j c - rp^k a = p^j c - r_1 a = 0$. Wir müssen $Ra \cap Rb = \{0\}$ zeigen. Wäre $Ra \cap Rb \neq \{0\}$, so gäbe es ein $s \in R$ mit $0 \neq sb \in Ra$. Da aber $pb = 0$, kann $s$ kein Vielfaches von $p$ sein. Daher sind $s$ und $p$ zueinander teilerfremd, und es gibt $x, y \in R$ mit $1_R = sx + py$. Damit erhält man

$$b = 1_R b = sxb + pyb = x(sb) \in Ra,$$

Widerspruch.

Zu Punkt (b): Sei $U \leq A$ maximal mit $U \cap Ra = \{0\}$. Die Existenz eines solchen $U$ folgt in der üblichen Weise aus dem Lemma von Zorn. Nach 3.3.2.11 oder (einfacher) **??** ist $A_0 := U + Ra = U \oplus Ra$. Somit bleibt lediglich $A_0 = A$ zu zeigen. Dazu gehen wir indirekt vor:
Angenommen es wäre $A_0 \neq A$. Dann ist der von $a + U$ im Faktormodul $A/U$ erzeugte zyklische Untermodul nicht ganz $A/U$. Außerdem hat $a+U$ in $A/U$ die Ordnung $p^n$, was unter den $p$-Elementen in $A/U$ sicher maximal ist. Nach Teil (a), angewendet auf $A/U$ statt $A$ und $a+U$ statt $a$, gibt es folglich ein $b \in A \setminus U$ mit $\langle a+U\rangle \cap \langle b+U\rangle = U$. Damit wäre der Untermodul $U' := U + Rb \leq A$ eine echte Obermenge von $U$ mit $U' \cap Ra = \{0\}$, im Widerspruch zur Maximalität von $U$. □

Im endlich erzeugten Fall können wir damit die gewünschte direkte Zerlegung eines $p$-Moduls in zyklische Summanden herleiten:

**Satz 7.4.4.3.** *Ist $A$ ein endlich erzeugter $p$-primärer $R$-Modul für ein $p \in \mathbb{P}$, dann gilt $A \cong \bigoplus_{i=1}^{k} R/p^{n_i}R$ mit $k \in \mathbb{N}$ und $n_1 \geq \ldots \geq n_k \geq 1$.*

*Beweis.* Der Beweis erfolgt durch Induktion nach der Anzahl $r$ der Erzeugenden $a_1, \ldots, a_r$ von $A$. Der Fall $r = 1$ ist trivial. Gelte nun die Aussage für $r-1$ und werde $A$ von $a_1, \ldots, a_r \in A$ mit $\mathcal{O}_{a_i} = (p^{m_i})$ für $i = 1, \ldots, r$ erzeugt. O.B.d.A. sei $n_1$ maximal unter der $n_i$. Dann ist $p^{n_1}A = \{0\} \neq p^{n_1-1}A$. Lemma 7.4.4.2 liefert daher einen Untermodul $C \leq A$ mit $A = Ra_1 \oplus C$. Sei $\pi : A \to C$, $ra + c \mapsto c$ für $r \in R$ und $c \in C$ die dieser direkten Zerlegung entsprechende Projektion auf $C$. Dann wird $C$ von den Bildern $\pi(a_1), \pi(a_2), \ldots, \pi(a_r)$ erzeugt, wobei wegen $\pi(a_1) = 0$ mit $\{\pi(a_2), \ldots, \pi(a_r)\}$ sogar ein $r-1$-elementiges Erzeugendensystem von $C$ vorliegt. Laut Induktionsannahme gibt es folglich eine direkte Zerlegung

$$C \cong \bigoplus_{i=2}^{k} R/p^{n_i}R.$$

Wegen $Ra_1 \cong R/p^{n_1}R$ gilt also insgesamt die Behauptung

$$A = Ra_1 \oplus C \cong \bigoplus_{i=1}^{k} R/p^{n_i}R.$$

□

## 7.4.5 Abschluss des Beweises des Hauptsatzes

Der Beweis des Hauptsatzes 7.4.3.1 über endlich erzeugte $R$-Moduln über einem Hauptidealring $R$ ist nun recht schnell vervollständigt, wie die folgende Beweisskizze zeigt:

*Skizze der verbleibenden Beweisteile von Satz 7.4.3.1:* Zuerst zur Existenz einer Zerlegung wie in 7.4.3.1 (a): Die Sätze 7.4.2.9, 7.4.4.1 und 7.4.4.3 liefern eine Darstellung wie in (a), wobei wegen „endlich erzeugt“ nur endlich viele Summanden $\neq 0$ auftreten können. Die Darstellung aus (b) erhält man durch geeignetes Zusammensetzen von Faktoren $R/p_j^{e_j}R$, $j = 1, \ldots, s$, zu $R/rR \cong \bigoplus_{j=1}^{s} R/p_j^{e_j}R$ mit $r = \prod_{j=1}^{s} p_j^{e_j}R$ (man beachte die Analogie zum Chinesischen Restsatz 3.4.7.1).
Zur Eindeutigkeit einer Zerlegung wie in 7.4.3.1 (a): $A_t$ ist eindeutig bestimmt, somit muss der Rang von $F$ gleich dem Rang von $A/A_t$ sein (Dimensionsinvarianz, Satz 7.2.2.4). Innerhalb $A_t$ sind die $A(p)$ als $p$-Anteile ebenfalls eindeutig bestimmt. Für (a) zu zeigen bleibt daher noch: Für $p$-primäre $A$ sind die $e_n$ in $A \cong \bigoplus_{n=1}^{N}(R/p^nR)^{e_n}$ eindeutig bestimmt. Dies folgt, weil die Dimension von $A[p^m]/A[p^{m-1}]$ über dem Körper $R/pR$ sich als die Summe $\sum_{k \geq m} e_k$ ergibt. (Hier sei an die Notation $A[l] := \{a \in A : l \cdot a = 0\}$ erinnert.) Daraus ergeben sich die $e_n$ eindeutig. Verwendet man die oben angedeutete Isomorphie $R/rR \cong \bigoplus_{j=1}^{s} R/(p_j^{e_j}R)$ mit $r = \prod_{j=1}^{s} p_j^{e_j}$, so erhält man auch die Eindeutigkeitsaussage für die Darstellung in 7.4.3.1 (b). □

**UE 415** ▶ **Übungsaufgabe 7.4.5.1.** Arbeiten Sie obige Beweisskizze vollständig aus. Insbesondere sind ausführlich zu begründen: Die Übersetzung zwischen den Darstellungen aus (a) und (b) und die Eindeutigkeitsaussagen. ◀ **UE 415**

**Beispiel 7.4.5.2.** Zur näheren Erläuterung der $A[l]$ aus obigem Beweis.
Sei $A = \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_8$, $R = \mathbb{Z}$ und $p = 2$. Dann ist

$$\begin{aligned} A[1] &= \{0\}, \\ A[2] &\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, \\ A[4] &\cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \text{ und} \\ A[8] &= \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_8 = A. \end{aligned}$$

Dabei ist $\dim(A[2]/A[1]) = 4 = e_1 + e_2 + e_3$, $\dim(A[4]/A[2]) = 3 = e_2 + e_3$ und $\dim(A[8]/A[4]) = 1$, also $e_1 = 1, e_2 = 2$ und $e_3 = 1$.

### 7.4.6 Eine Anwendung des Hauptsatzes: Jordansche Normalformen

Ein Beispiel für eine Anwendung des Hauptsatzes 7.4.3.1 auf Moduln über einem Hauptidealring $R \neq \mathbb{Z}$ (und damit nicht schlicht auf abelsche Gruppen) liefert ein Ergebnis, das aus der Linearen Algebra bekannt ist: die Jordansche Normalform eines Endomorphismus eines endlichdimensionalen Vektorraums. Wie diese beiden Themen in Zusammenhang gebracht werden können, soll nun sehr kurz und nur andeutungsweise skizziert werden.

Sei $V$ ein $n$-dimensionaler Vektorraum über einem Körper $K$ und $\varphi : V \to V$ linear, also eine Endomorphismus von $V$. Weil die Endomorphismen von $V$ sogar eine Algebra bilden, induziert jedes Polynom $f \in K[x]$ über $K$ die lineare Abbildung $f_\varphi := f(\varphi)$. Diese lässt sich auf Elemente $x \in V$ anwenden. Wir betrachten nun die Abbildung

$$\cdot_\varphi : K[x] \times V \to V, \quad (f, x) \mapsto f_\varphi(x).$$

Sie macht $V$ zu einem endlich erzeugten $K[x]$-Modul. Da jeder Polynomring über einem Körper ein Hauptidealring ist (siehe 5.2.3), lässt sich der Hauptsatz 7.4.3.1 anwenden. Um zu verstehen, was seine Aussage im vorliegenden Kontext bedeutet, hat man sich zum Beispiel zu überlegen, was zyklische Unter-$K[x]$-Moduln von $V$ sind etc. Führt man all diese Überlegungen durch, kommt man zu direkten Zerlegungen des Vektorraumes $V$ in sogenannte $\varphi$-zyklische Unterräume, aus denen man sich Basen konstruieren kann, bezüglich derer man $\varphi$ auf Normalform bringen kann.

**UE 416** ▶ **Übungsaufgabe 7.4.6.1.** Arbeiten Sie diese Ansätze aus. ◀ **UE 416**

## 7.5 Hom-Funktor und Dualität

Es überrascht nicht, dass das Konzept des Dualraums $V^*$ eines Vektorraums $V$ über einem Körper $K$, d.h. des Vektorraums aller linearen Funktionale $f\colon V \to K$ aus der Linearen Algebra bzw. Funktionalanalysis auf Moduln über einem Ring $R$ verallgemeinert

werden kann. Allerdings müssen mancherlei Komplikationen beachtet werden, vor allem für den Fall, dass $R$ nicht kommutativ ist. Dies sowie daran anschließende Konzepte sind Gegenstand des vorliegenden Abschnitts, des letzten zur Modultheorie.
In 7.5.1 wird ein hinreichend weiter begrifflicher Rahmen gesteckt. Insbesondere wird der Hom-Funktor eingeführt. Die Komplikationen bei Nichtkommutativität werden in 7.5.2 behandelt. Es folgen das Konzept des dualen Moduls in 7.5.3 und des Tensorproduktes in 7.5.4. Abschnitt und Kapitel schließen in 7.5.5 mit dem allgemeinen Begriff einer Algebra über einem Ring.

### 7.5.1 Die abelsche Gruppe $\mathrm{Hom}_R(A,B)$ und der Hom-Funktor

Wir beginnen mit einer sehr allgemeinen Situation, zunächst sogar unabhängig von jeglicher algebraischen Struktur.

**Definition 7.5.1.1.** Seien $A, B, C, D$ beliebige Mengen. Gegeben seien zwei Abbildungen $\varphi\colon C \to A$ und $\psi\colon B \to D$. Für $f : A \to B$ sei $\theta(f) := \psi \circ f \circ \varphi : C \to D$.

$$C \xrightarrow{\varphi} A \xrightarrow{f} B \xrightarrow{\psi} D$$

Dadurch ist eine Abbildung $\theta\colon B^A \to D^C$ definiert. (Die Potenzschreibweise $B^A$ steht wie üblich für die Menge aller Abbildungen von $A$ nach $B$.)
Seien $A, B, C, D$ Moduln über einem Ring $R$ und $\varphi, \psi$ entsprechend $R$-Modulhomomorphismen. Schränkt man $\theta$ auf die abelsche Gruppe $\mathrm{Hom}_R(A,B)$ aller $R$-Homomorphismen $f\colon A \to B$ ein, so nennt man diese Einschränkung

$$\mathrm{Hom}(\varphi,\psi) := \theta|_{\mathrm{Hom}(A,B)} : \mathrm{Hom}(A,B) \to \mathrm{Hom}(C,D), \quad f \mapsto \psi \circ f \circ \varphi$$

den von $\varphi$ und $\psi$ *induzierten Homomorphismus.*
Ist, noch spezieller, $B = D$ und $\psi = \mathrm{id}_B$, so ist $\theta : f \mapsto f \circ \varphi$, und wir schreiben für den Homomorphismus $\mathrm{Hom}(\varphi,\psi)$ auch $\bar{\varphi}$; im Fall $A = C$, $\varphi = \mathrm{id}_C$ und somit $\theta : f \mapsto \psi \circ f$ schreiben wir entsprechend $\bar{\psi}$.

Man beachte: $\mathrm{Hom}_R(A,B)$ ist eine Menge von $R$-Modulhomomorphismen. Hingegen ist $\mathrm{Hom}(\varphi,\psi)$ selbst ein Homomorphismus (zwischen abelschen Gruppen), der auf der Menge $\mathrm{Hom}_R(A,B)$ definiert ist.

**Proposition 7.5.1.2.** *Mit der Notation aus Definition 7.5.1.1 gilt:*

1. $\mathrm{Hom}_R(A,B)$ *ist (wie in Definition 7.5.1.1 implizit behauptet) eine abelsche Gruppe bezüglich der punktweisen Addition* $(f+g)(a) := f(a) + f(b)$.

2. $\mathrm{Hom}_R(A,B)$ *ist bezüglich der punktweisen Definition* $(rf)(a) := rf(a)$ *im Allgemeinen* kein *$R$-Linksmodul.*

3. *Bei geeigneter (natürlicher) Wahl der Definitions- und Zielmengen der involvierten Abbildungen gilt:* $\mathrm{Hom}(\varphi\varphi', \psi'\psi) = \mathrm{Hom}(\varphi',\psi')\,\mathrm{Hom}(\varphi,\psi)$

*Beweis.* Übungsaufgabe. □

**UE 417 ► Übungsaufgabe 7.5.1.3.** Beweisen Sie 7.5.1.2. Als Hinweis für die zweite Aussage sei lediglich die Möglichkeit **◄ UE 417**

$$(r_1 f)(r_2 a) = r_1 f(r_2 a) = r_1 r_2 f(a) \neq r_2 r_1 f(a) = r_2((r_1 f)(a))$$

hervorgehoben.

Mehr Klarheit schafft die kategorientheoretische Betrachtungsweise, siehe auch 2.2: Gegeben sei ein Ring $R$ (mit oder ohne 1) und ein $R$-Modul $D$ (unitär oder auch nicht).
Im kovarianten Fall wird jedem $R$-Modul $A$ die abelsche Gruppe $\mathrm{Hom}_R(D, A)$ und jedem $R$-Homomorphismus $\varphi : A \to B$ der induzierte Homomorphismus

$$\bar{\varphi} : \mathrm{Hom}_R(D, A) \to \mathrm{Hom}_R(D, B), \quad f \mapsto f \circ \varphi$$

zugeordnet. Diese Zuordnung ist, wie man leicht nachprüft, ein Funktor, der von $D$ induzierte *kovariante Hom-Funktor* $A \mapsto \mathrm{Hom}_R(D, A)$, $\varphi \mapsto \bar{\varphi}$.
Im kontravarianten Fall wird dem $R$-Modul $A$ statt der abelschen Gruppe $\mathrm{Hom}_R(D, A)$ entsprechend die abelsche Gruppe $\mathrm{Hom}_R(A, D)$ zugeordnet, und ein Homomorphismus $\psi$ geht in den induzierten Homomorphismus $\bar{\psi}$ über. Man erhält so den *kontravarianten* Hom-*Funktor* $A \mapsto \mathrm{Hom}_R(A, D)$.
Wie meist in der Kategorientheorie kann man das Spiel weitertreiben. Wir wollen auch kommutative Diagramme von $R$-Moduln und $R$-Modulhomomorphismen betrachten. Dazu gibt man sich einen Graphen $\Gamma$ vor. Die Objekte einer neuen Kategorie sind dann kommutative Diagramme von $R$-Moduln über $\Gamma$. Als Morphismen zwischen zwei solchen Objekten dienen dann Familien von $R$-Modulhomomorphismen, die entsprechende Knoten verbinden und insgesamt wieder ein kommutatives Diagramm liefern. Bei gegebenem $R$-Modul $D$ induzieren ko- wie auch kontravarianter Hom-Funktor auf Modulebene je einen entsprechenden Funktor auf Diagrammebene.
Für die Modultheorie (und, darauf aufbauend, für die homologische Algebra, die wir aber nicht vertiefen werden) sind, wie wir wissen, Sequenzen $S$ von besonderer Bedeutung, etwa von der Form $S: \ 0 \to A \to B \to C \to 0$. Weil in ihnen keine Kreise auftreten, lassen sie sich automatisch als kommutative Diagramme deuten, und alle Konstruktionen sind sinnvoll.

**UE 418 ► Übungsaufgabe 7.5.1.4.** Rekapitulieren Sie die erforderlichen kategorientheoretischen Begriffe, um die angedeutete Konstruktion ausführlich zu beschreiben. Begründen Sie auch, warum man tatsächlich wieder Kategorien bzw. Funktoren erhält. **◄ UE 418**

In den folgenden Untersuchungen werden wir uns auf sehr einfache Beispiele beschränken und nur einige wenige Tatsachen erwähnen, die einen ersten Eindruck von homologischer Algebra geben mögen.
Konzentrieren wir uns zunächst auf einen $R$-Modulhomomorphismus $\varphi : A \to B$. Bei Vorgabe eines weiteren $R$-Moduls $D$ induziert $\varphi$ gemäß Definition 7.5.1.1 einen Homomorphismus $\bar{\varphi} : \mathrm{Hom}_R(D, A) \to \mathrm{Hom}_R(D, B)$, definiert durch $f \mapsto \varphi \circ f$. Entsprechend geht die Sequenz $S : 0 \to A \to B \to D \to 0$ von $R$-Moduln in eine Sequenz

$$S_D : \ 0 \to \mathrm{Hom}_R(D, A) \to \mathrm{Hom}_R(D, B) \to \mathrm{Hom}_R(D, C) \to 0$$

abelscher Gruppen über, die wir die (von $S$ durch $D$) *induzierte Sequenz* nennen. Klarerweise ist diese Konstruktion für Sequenzen beliebiger Länge wie auch für (kommutative) Diagramme möglich.
Dual dazu kann man $D$ statt als Definitions- auch als Zielbereich von Modulhomomorphismen einsetzen. Dann induziert jedes $\psi : A \to B$ gemäß Definition 7.5.1.1 einen Homomorphismus $\bar{\psi} : \mathrm{Hom}_R(B, D) \to \mathrm{Hom}_R(A, D)$, definiert durch $f \mapsto f \circ \psi$. Entsprechend geht die Sequenz $S : \ 0 \to A \to B \to C \to 0$ von $R$-Moduln in eine Sequenz

$$S_D^* : \ 0 \to \mathrm{Hom}_R(C, D) \to \mathrm{Hom}_R(B, D) \to \mathrm{Hom}_R(A, D) \to 0$$

über. Zur Unterscheidung der beiden von $D$ induzierten Sequenzen $S_D$ und $S_D^*$ könnte man $S_D$ die *ko-* und $S_D^*$ die *kontravariant* induzierte Sequenz nennen.

Wir begnügen uns mit den folgenden Aussagen über die Verträglichkeit der Hom-Funktoren mit diversen Konstruktionen und der Exaktheit von Sequenzen. Die Beweise sind mit Hilfe der bereits verfügbaren Theorie nicht sehr schwierig, erfordern insgesamt aber beträchtlichen Aufwand. Wir verlagern sie in Übungsaufgaben.

**Proposition 7.5.1.5.** *Alle nachfolgenden Aussagen beziehen sich, wenn nicht anders spezifiziert, auf die Kategorie der (unitären) Moduln über einem Ring $R$ (mit $1$).*

1. *Die Sequenz*
$$S : \ 0 \to A \to B \to C$$
*von $R$-Moduln ist genau dann exakt, wenn die kovariant induzierte Sequenz*
$$S_D : \ 0 \to \mathrm{Hom}_R(D, A) \to \mathrm{Hom}_R(D, B) \to \mathrm{Hom}_R(D, C)$$
*abelscher Gruppen für alle $R$-Moduln $D$ exakt ist.*

2. *Die Sequenz*
$$S : \ A \to B \to C \to 0$$
*von $R$-Moduln ist genau dann exakt, wenn die kontravariant induzierte Sequenz*
$$S_D^* : \ 0 \to \mathrm{Hom}_R(C, D) \to \mathrm{Hom}_R(B, D) \to \mathrm{Hom}_R(A, D)$$
*abelscher Gruppen für alle $R$-Moduln $D$ exakt ist.*

3. *Für die Sequenz*
$$S : \ 0 \to A \to B \to C \to 0$$
*von $R$-Moduln sind die folgenden drei Bedingungen äquivalent:*
   a) *$S$ ist kurzexakt und zerfällt.*
   b) *Die kovariant induzierte Sequenz*
$$S_D : \ 0 \to \mathrm{Hom}_R(D, A) \to \mathrm{Hom}_R(D, B) \to \mathrm{Hom}_R(D, C) \to 0$$
   *ist kurzexakt und zerfällt für alle $R$-Moduln $D$.*

*c) Die kontravariant induzierte Sequenz*

$$S_D^* : \ 0 \to \mathrm{Hom}_R(C, D) \to \mathrm{Hom}_R(B, D) \to \mathrm{Hom}_R(A, D) \to 0$$

*ist kurzexakt und zerfällt für alle $R$-Moduln $D$.*

*4. Für einen $R$-Modul $P$ sind äquivalent:*

*a) $P$ ist projektiv.*

*b) Jeder surjektive Homomorphismus $\varphi : B \to C$ induziert kovariant einen surjektiven Homomorphismus $\bar{\phi} : \mathrm{Hom}_R(P, B) \to \mathrm{Hom}_R(P, C)$ abelscher Gruppen.*

*c) Jede kurzexakte Sequenz*

$$S : \ 0 \to A \to B \to C \to 0$$

*von $R$-Moduln induziert kovariant eine gleichfalls kurzexakte Sequenz*

$$S_P : \ 0 \to \mathrm{Hom}_R(P, A) \to \mathrm{Hom}_R(P, B) \to \mathrm{Hom}_R(P, C) \to 0$$

*abelscher Gruppen.*

*5. Für einen $R$-Modul $J$ sind äquivalent:*

*a) $J$ ist injektiv.*

*b) Jeder injektive Homorphismus $\psi : A \to B$ induziert kontravariant einen surjektiven Homomorphismus $\bar{\psi} : \mathrm{Hom}_R(B, J) \to \mathrm{Hom}_R(A, J)$ abelscher Gruppen.*

*c) Jede kurzexakte Sequenz*

$$S : \ 0 \to A \to B \to C \to 0$$

*von $R$-Moduln induziert kontravariant eine gleichfalls kurzexakte Sequenz*

$$S_J^* : \ 0 \to \mathrm{Hom}_R(C, J) \to \mathrm{Hom}_R(B, J) \to \mathrm{Hom}_R(A, J) \to 0$$

*abelscher Gruppen.*

*6. Für $R$-Moduln $A$, $B$, $A_i$ $(i \in I)$ und $B_j$ $(j \in J)$ gelten folgende Isomorphien abelscher Gruppen:*

*a)* $\mathrm{Hom}_R(\sum_{i\in I} A_i, B) \cong \prod_{i\in I} \mathrm{Hom}_R(A_i, B)$

*b)* $\mathrm{Hom}_R(A, \prod_{j\in J} B_j) \cong \prod_{j\in J} \mathrm{Hom}_R(A, B_j)$

**UE 419 ▶ Übungsaufgabe 7.5.1.6.** Beweisen Sie Proposition 7.5.1.5. **◀ UE 419**

### 7.5.2 Rechts-, Links- und Bimoduln

Für $R$-Moduln $A, B$ wollen wir die abelsche Gruppe $\mathrm{Hom}_R(A,B)$ strukturell anreichern und selbst zu einem $R$-Modul machen. Es überrascht kaum, dass dies möglich ist. Allerdings ist dabei Vorsicht nötig, um eine mögliche Nichtkommutativität von $R$ und die daraus resultierende Unterscheidung zwischen Links- und Rechtsmoduln zu berücksichtigen (siehe beispielsweise Aussage 2 in Proposition 7.5.1.2).

**Definition 7.5.2.1.** Sind $R$ und $S$ Ringe und $A$ eine abelsche Gruppe, die sowohl $R$-Links- als auch $S$-Rechtsmodul ist. Dann nennen wir $A$ einen *$R$-$S$-Bimodul*, sofern

$$r(as) = (ra)s$$

für alle $r \in R$, $a \in A$ und $s \in S$ gilt. Wir verwenden die Schreibweisen ${}_RB$, ${}_RA_S$ und $C_S$, um anzudeuten, dass $B$ ein $R$-Links-, $A$ ein $R$-$S$-Bi- und $C_S$ ein $S$-Rechtsmodul ist.

Klarerweise wird jeder Linksmodul $A$ über einem kommutativen Ring $R$ durch die Festsetzung $ar := ra$ für $r \in R$ und $a \in A$ zu einem $R$-$R$-Bimodul. Aus $r(as) = r(sa) = (rs)a$ und $(ra)s = s(ra) = (sr)a$ ersieht man allerdings, dass hier die Kommutativität essenziell ist. Allein wegen der Assoziativität der Multiplikation hingegen, also unabhängig von Kommutativität, ist jeder Ring $R$ ein $R$-$R$-Bimodul.
Die angekündigte Modulstruktur auf $\mathrm{Hom}_R(A,B)$ lässt sich folgendermaßen beschreiben.

**Proposition 7.5.2.2.** *Über den Ringen $R$ und $S$ seien die Moduln ${}_RA$, ${}_RB_S$, ${}_RC_S$ und ${}_RD$ gegeben. Dann gilt:*

1. $\mathrm{Hom}_R(A,B)$ *wird zu einem $S$-Rechtsmodul, wenn man für $a \in A$, $s \in S$ und $f \in \mathrm{Hom}_R(A,B)$ definiert:* $(fs)(a) := (f(a))s$.
2. *Jeder Homomorphismus $\varphi\colon A \to A'$ von $R$-Links-Moduln induziert einen Homomorphismus $\bar{\varphi}\colon \mathrm{Hom}_R(A',B) \to \mathrm{Hom}_R(A,B)$ von $S$-Rechts-Moduln.*
3. $\mathrm{Hom}_R(C,D)$ *wird zu einem $S$-Linksmodul, wenn man für $c \in C$, $s \in S$ und $g \in \mathrm{Hom}_R(C,D)$ definiert:* $(sf)(c) := f(cs)$.
4. *Jeder Homomorphismus $\psi\colon D \to D'$ von $R$-Links-Moduln induziert einen Homomorphismus $\bar{\psi}\colon \mathrm{Hom}_R(C,D) \to \mathrm{Hom}_R(C,D')$ von $S$-Links-Moduln.*
5. *Ist $R$ kommutativ und fassen wir $A$ und $B$ als $R$-$R$-Bimoduln auf, so ist auch $\mathrm{Hom}_R(A,B)$ ein $R$-$R$-Bimodul.*

**UE 420 ► Übungsaufgabe 7.5.2.3.** Beweisen Sie Proposition 7.5.2.2 und geben Sie eine funktorielle Deutung. **◄ UE 420**

Ein nützliche Beobachtung an einem $R$-Linksmodul $A$ ist die Isomorphie

$$A \cong \mathrm{Hom}_R(R,A) \quad \text{via} \quad a \mapsto f_a \quad \text{mit} \quad f_a(r) := ra,$$

sofern $R$ ein Einselement hat und $A$ als $R$-Modul unitär ist. Betrachtet man $\mathrm{Hom}_R(A,R)$ statt $\mathrm{Hom}_R(R,A)$ erhält man den zu $A$ dualen $R$-Rechtsmodul. Ihm gilt nun unser Interesse.

### 7.5.3 Duale Moduln

Ist $A$ ein Linksmodul über dem Ring $R$, so ist nach Proposition 7.5.2.2 $A^* := \mathrm{Hom}_R(A, R)$ ein $R$-Rechtsmodul über $R$. Etwas ausführlicher:

**Definition 7.5.3.1.** Seien $A$ und $B$ zwei $R$-Linksmoduln und $\mathrm{Hom}_R(A, B)$ die abelsche Gruppe aller $R$-Modul-Homomorphismen von $A$ nach $B$. Dann ist $\mathrm{Hom}_R(A, R)$ ein Rechts-$R$-Modul bzgl.

$$\begin{aligned}(f_1 + f_2)(a) &= f_1(a) + f_2(a)\\ (fr)(a) &= f(a) \cdot r,\end{aligned}$$

genannt der *duale Modul,* i.Z. $A^*$. Jedes $f \in A^*$ heißt auch *lineares Funktional.* Für $\varphi \in Hom_R(A, B)$ heißt

$$\begin{aligned}\varphi^* \colon B^* &\to A^*\\ f &\mapsto f \circ \varphi\end{aligned}$$

die *duale Abbildung.*
Geht man von einem $R$-Rechtsmodul aus, so werden die dualen Moduln in analoger Weise zu $R$-Linksmoduln. Somit führt Iteration der Konstruktion von einem $R$-Linksmodul $A$ wieder zu einem $R$-Linksmodul $A^{**}$, von einem $R$-Rechtsmodul $A$ wieder zu einem $R$-Rechtsmodul $A^{**}$. In beiden Fällen heißt $A^{**}$ der *biduale Modul* zu $A$.
Die *natürliche Abbildung* $\Phi$ ist durch

$$\Phi : A \to A^{**},\ a \mapsto a^{**} \quad \text{mit} \quad a^{**} : A^* \to R,\ f \mapsto f(a)$$

definiert. Ist $\Phi$ ein Isomorphismus, so heißt $A$ *reflexiv.*

**Proposition 7.5.3.2.** *Sei $R$ ein Ring. Die Zuordnung $^*$ führe einen $R$-Linksmodul $A$ in sein Dual (den $R$-Rechtsmodul $A^*$) über sowie einen Homomorphismus $f \colon A \to B$ von $R$-Linksmoduln in den Homomorphismus $f^* \colon B^* \to A^*$ (die zu $f$ duale Abbildung). Dann ist $^*$ ein kontravarianter Funktor von der Kategorie der $R$-Linksmoduln in die Kategorie der $R$-Rechtsmoduln. Folglich ist die Iteration $A \mapsto A^{**}$, $f \mapsto f^{**}$ ein kovarianter Funktor von der Kategorie der $R$-Linksmoduln (bzw. der $R$-Rechtsmoduln) in sich selbst.*

**UE 421 ► Übungsaufgabe 7.5.3.3.** Prüfen Sie Proposition 7.5.3.2 nach. **◄ UE 421**

Von Interesse sind die in folgender Übungsaufgabe behandelten Gesichtspunkte und Sachverhalte.

**UE 422 ► Übungsaufgabe 7.5.3.4.** (1) Zeigen Sie: $(A \oplus B)^* \cong A^* \oplus B^*$ **◄ UE 422**

(2) Zeigen Sie: Ist $R$ ein Divisionsring, dann führt $^*$ kurzexakte Sequenzen von Vektorräumen über $R$ in kurzexakte Sequenzen über.

(3) Beschreiben Sie $F^*$ für einen freien $R$-Linksmodul $F$. Ist $F^*$ ebenfalls frei? (Hierzu wäre eine „duale“ Basis zu finden.)

(4) Zeigen Sie: Hat $R$ ein Einselement, und ist der unitäre $R$-Linksmodul $F$ frei, so ist die natürliche Abbildung von $F$ nach $F^{**}$ eine Einbettung.

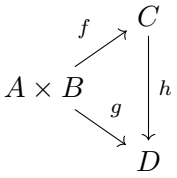
(5) Besitzt überdies $F$ sogar eine endliche Basis, so ist $F$ reflexiv.

### 7.5.4 Das Tensorprodukt

Sei $A$ ein Rechts-$R$-Modul und $B$ ein Links-$R$-Modul. Das *Tensorprodukt* $A \otimes_R B$ ist definiert als initiales Objekt in der folgenden Kategorie $\mathcal{M}(A, B)$.
Die Objekte von $\mathcal{M}(A, B)$ sind die sogenannten *mittellinearen Abbildungen*, genauer: Paare $(f, C)$ mit Abbildungen $f\colon A \times B \to C$ in eine abelsche Gruppe $C$, die den Gleichungen

$$\begin{aligned} f(a_1 + a_2, b) &= f(a_1, b) + f(a_2, b) \\ f(a, b_1 + b_2) &= f(a, b_1) + f(a, b_2) \\ f(ar, b) &= f(a, rb) \end{aligned}$$

genügen. Ist $R$ kommutativ, so lassen sich die mittellinearen Abbildungen durch *bilineare* Abbildungen ersetzen: $f(ar, b) = rf(a, b) = f(a, rb)$
Die Menge $hom_{\mathcal{M}(A,B)}(f, g)$ der Morphismen von $f$ nach $g$ in der Kategorie $\mathcal{M}(A, B)$ ist die Menge aller Gruppenhomomorphismen $h\colon C \to D$, für die das Diagramm




kommutiert. Komposition in $\mathcal{M}(A, B)$ ist die Abbildungskomposition.

Eine alternative Beschreibung des Tensorprodukts lautet wie folgt: Sei $F$ die freie abelsche Gruppe über der Menge $A \times B$ und $K$ die von allen

$$\begin{aligned} &(a_1 + a_2, b) - (a_1, b) - (a_2, b), \\ &(a, b_1 + b_2) - (a, b_1) - (a, b_2) \text{ und} \\ &(ar, b) - (a, rb) \end{aligned}$$

erzeugte Untergruppe. Dann ist $A \otimes_R B \cong F/K$.

**UE 423** ▶ **Übungsaufgabe 7.5.4.1.** Zeigen Sie, dass die abelsche Gruppe $F/K$ tatsächlich als initiales Objekt in $\mathcal{M}(A, B)$ aufgefasst werden kann. ◀ **UE 423**

Elemente des so definierten Tensorproduktes schreiben wir als $a \otimes b := (a, b) + K$ an.

**UE 424** ▶ **Übungsaufgabe 7.5.4.2.** $A, B$ seien (Links-) Moduln über dem Ring $R$. ◀ **UE 424**

1. Formulieren und beweisen Sie Rechengesetze wie $(a_1 + a_2) \otimes b = a_1 \otimes b + a_2 \otimes b$.
2. Wir nehmen an, die Elemente $a_i, i \in I$, bilden ein Erzeugendensystem von $A$, die $b_j$, $j \in J$ von $B$. Zeigen Sie, dass sich dann jedes Element von $A \otimes B$ als $\sum_{i,j} n_{i,j}(a_i \otimes b_i)$ mit $n_{i,j} \in \mathbb{Z}$ schreiben lässt, wobei nur endlich viele $n_{i,j}$ von 0 verschieden sind.
3. Unter welchen Bedingungen ist diese Darstellung eindeutig?

Ist $R$ kommutativ, so können $A$ und $B$ als Bimoduln aufgefasst und auf dem Tesorprodukt $A \otimes B$ eine Operation $R \times (A \otimes B) \to A \otimes B$, $(r, a \otimes b) \mapsto ra \otimes b$ mit $r(a \otimes b) = (ra) \otimes b = a \otimes (rb)$ definiert werden, die das Tensorprodukt wieder zu einem $R$-Modul macht.

**UE 425** ▶ **Übungsaufgabe 7.5.4.3.** Führen Sie diesen Ansatz aus, insbesondere für den Fall, dass $R = K$ ein Körper ist. Dann sind $A$ und $B$ Vektorräume. Was kann über ihre Dimension ausgesagt werden? ◀ **UE 425**

### 7.5.5 Algebren

**Definition 7.5.5.1.** Sei $A$ ein Ring, $K$ ein Ring mit 1 zusammen mit einer Abbildung $\cdot : K \times A \to A$. $A$ heißt eine *$K$-Algebra*, wenn gilt:

(i) $(A, +)$ ist bezüglich $\cdot$ ein unitärer (Links-) $K$-Modul und

(ii) $k \cdot (ab) = (k \cdot a)b = a(k \cdot b)$ für alle $k \in K$, $a, b \in A$.

Eine $K$-Algebra, die ein Divisionsring ist, nennt man *Divisionsalgebra.* Im klassischen Fall ist $K$ ein Körper, also $A$ ein Vektorraum.

Ohne die Theorie der Algebren zu vertiefen begnügen wir uns mit der Angabe einiger wichtiger Beispiele:

**Beispiel 7.5.5.2.** Folgende Strukturen sind Algebren:

(a) Jeder Ring ist auch eine $\mathbb{Z}$-Algebra.

(b) $K[x_1, \ldots, x_n], K[[x]]$ über einem Körper $K$.

(c) $\mathrm{Hom}_K(V, V)$ für einen Vektorraum über einem Körper $K$.

(d) Ist $A$ ein Ring mit 1 und $K$ ein Unterring des Zentrums von $A$ mit $1 \in K$, dann ist $A$ eine $K$-Algebra, wobei die $K$-Modul-Struktur gegeben ist durch die Multiplikation in $A$.

(e) Der Divisionsring der Quaternionen $\mathbb{H}$ und auch der Körper der komplexen Zahlen $\mathbb{C}$ sind Divisionsalgebren über $\mathbb{R}$.

(f) Sei $G$ eine Gruppe und $K$ ein kommutativer Ring mit 1. Dann ist der Gruppenring $K(G)$ eine $K$-Algebra, wobei die $K$-Modul-Struktur gegeben ist durch

$$k\left(\sum r_i g_i\right) = \sum (kr_i) g_i$$

für $k, r_i \in K$, $g_i \in G$. $K(G)$ nennt man die *Gruppenalgebra* von $G$ über $K$.

(g) Ist $K$ ein kommutativer Ring mit 1, dann ist der Matrizenring $Mat_n(K)$ aller $n \times n$-Matrizen eine $K$-Algebra.

# 8 Vertiefung der Gruppentheorie

In einführenden Kapiteln haben wir lediglich grundlegende Konzepte der Gruppentheorie kennengelernt, wobei als wichtigstes das des Normalteilers zu nennen ist. Unser Verständnis der Struktur von Gruppen geht noch kaum über den Cayleyschen Darstellungssatz (jede Gruppe $G$ ist isomorph zu einer Permutationsgruppe auf der Trägermenge von $G$) und, für endliche Gruppen, den Satz von Lagrange (die Ordnung einer Untergruppe teilt die Gruppenordnung) hinaus. In Kapitel 7 haben wir die Struktur von abelschen Gruppen und, allgemeiner, von Moduln untersucht. Das vorliegende Kapitel bringt Vertiefungen vor allem für den nichtabelschen Fall, wobei in den ersten beiden Abschnitten endliche Gruppen im Zentrum des Interesses stehen. Ziel in 8.1 sind vor allem die für die Strukturtheorie endlicher Gruppen grundlegenden Sylowsätze, wobei es sich als fruchtbar erweist, zunächst sogenannte Aktionen auch von beliebigen Gruppen in den Fokus zu nehmen. Abschnitt 8.2 versammelt einige Beispiele von Gruppen unter den vorangegangenen allgemeineren Gesichtspunkten. Für Gruppen der Ordnung $\leq 15$ ergibt sich eine vollständige Klassifikation. In 8.3 geht es um Nilpotenz, Auflösbarkeit und Subnormalreihen. Das sind Begriffsbildungen, die um die Frage kreisen, wie weit und in welchem Sinn eine Gruppe davon entfernt ist, abelsch zu sein. Die beiden darauf folgenden Abschnitte konzentrieren sich auf die (bereits im Zusammenhang mit Normalreihen aufgetauchte) Frage, wie man sich komplizierte Gruppen eventuell aus einfacheren aufgebaut denken kann. In 8.4 ist das im Sinne von sogenannten Gruppenerweiterungen zu verstehen, in 8.5 über den Satz von Krull-Schmidt im Sinne von direkten Produkten.

## 8.1 Gruppenaktionen und Sylowsätze

Wir beginnen den Abschnitt in 8.1.1 mit dem weit über die Theorie endlicher Gruppen hinaus bedeutsamen Begriff der *Wirkung* oder *Aktion* einer Gruppe, stoßen dabei auf die Klassengleichung und spezialisieren in 8.1.2 auf den Spezialfall der Konjugation. Das erste darauf fußende bemerkenswerte Resultat ist der Satz von Cauchy in 8.1.3. Damit lassen sich als Kern der klassischen Theorie endlicher Gruppen in 8.1.4 die drei Sylowsätze beweisen. Wir schließen in 8.1.5 mit dem Satz von Wedderburn als Anwendung der Klassengleichung: Jeder endliche Schiefkörper ist sogar ein Körper.

### 8.1.1 Gruppenaktionen und allgemeine Klassengleichung

Mit jeder Transformation $T\colon S \to S$ einer Menge $S$ ist vermittels der Iterationen von $T$ durch $(n, x) \mapsto T^n(x)$ eine Aktion $\alpha\colon \mathbb{N} \times S \to S$ der (additiven) Halbgruppe $\mathbb{N}$ gegeben. Ist $T$ bijektiv, ist diese Definition auch für beliebige $n \in \mathbb{Z}$ sinnvoll. Allgemeiner definiert man:

**Definition 8.1.1.1.** Eine Halbgruppe $G$ *agiert (wirkt)* auf einer Menge $S$, wenn eine Abbildung $\alpha\colon G \times S \to S$, $(g,x) \mapsto gx$, vorliegt mit

$$\alpha(g1g_2, x) = (g_1g_2)x = g_1(g_2x) = \alpha(g_1, \alpha(g_2, x))$$

für alle $x \in S$ und $g_1, g_2 \in G$. Die Abbildung $\alpha$ heißt *Aktion* oder auch *Wirkung* von $G$. Für festes $g \in G$ bezeichnen wir die Abbildung $x \mapsto \alpha(g,x)$ mit $\alpha_g$. Ist $G$ sogar eine Gruppe mit neutralem Element $e$, so spricht man von einer *Gruppenaktion*, wenn zusätzlich $ex = x$ für alle $x \in S$ gilt.

Wir wollen uns hier auf Gruppenaktionen $\alpha\colon G \times S \to S$ konzentrieren. Dann gelten die Beziehungen $\alpha_e = \mathrm{id}_S$ und, wegen $\alpha_{g_1} \circ \alpha_{g_2} = \alpha_{g_1 \cdot g_2}$, für $g_1 = g$ und $g_2 = g^{-1}$ insbesondere $\alpha_g \circ \alpha_{g^{-1}} = \alpha_{g^{-1}} \circ \alpha_g = \mathrm{id}_S$. Also sind alle $\alpha_g$ Permutationen der Menge $S$, mit anderen Worten: Elemente von $\mathrm{Sym}(S)$. Wie üblich bezeichnet dabei $\mathrm{Sym}(S) := \{f\colon S \to S \text{ bijektiv}\}$ die symmetrische Gruppe auf der Menge $S$ mit der Komposition von Abbildungen als Gruppenoperation.
Jede Aktion $\alpha$ einer Gruppe $G$ auf einer Menge $S$ induziert eine Abbildung

$$\varphi_\alpha\colon G \to \mathrm{Sym}(S), \quad g \mapsto \pi_g, \quad \pi_g(x) := \alpha(g,x),$$

die sogar ein Homomorphismus ist:

$$\pi_{g_1g_2}(x) = \alpha(g_1g_2, x) = (g_1g_2)x = g_1(g_2x) = \pi_{g_1}(\pi_{g_2}(x)) = (\pi_{g_1} \circ \pi_{g_2})(x)$$

für alle $x \in S$, also

$$\varphi_\alpha(g_1g_2) = \pi_{g_1g_2} = \pi_{g_1} \circ \pi_{g_2} = \varphi_\alpha(g_1) \circ \varphi_\alpha(g_2).$$

Umgekehrt induziert jeder Homomorphismus $\varphi\colon G \to \mathrm{Sym}(S)$, $g \mapsto \pi_g$ die Aktion $\alpha : (g,x) \mapsto \pi_g(x)$, denn es gilt

$$\alpha(g_1g_2, x) = \pi_{g_1g_2}(x) = (g_1g_2)x = g_1(g_2x) = \alpha(g_1, \alpha(g_2, x)).$$

Die beiden Zugänge über Aktionen bzw. Homomorphismen in eine Permutationsgruppe sind also äquivalent.

Der Satz von Cayley, wonach jede Gruppe $G$ via $g \mapsto \pi_g$, $\pi_g(x) := gx$, isomorph ist zu einer Permutationsgruppe (d.h. definitionsgemäß zu einer Untergruppe einer symmetrischen Gruppe) auf ihrer eigenen Trägermenge, lässt sich also auch so formulieren:

**Satz 8.1.1.2** (Cayley)**.** *Jede Gruppe $G$ agiert auf ihrer Trägermenge vermittels der Aktion $\alpha$ (Linkstranslation), wobei die Abbildung $g \mapsto \alpha_g$, $\alpha_g : x \mapsto gx$, eine isomorphe Einbettung ist.*

Die Definition einer Gruppenaktion legt unmittelbar einige weitere Begriffe nahe.

**Definition 8.1.1.3.** Die Gruppe $G$ agiere auf der Menge $S$. Für $x \in S$ sei $G_x := \{g \in G : gx = x\} \leq G$. $G_x$ heißt *Stabilisator* oder *Isotropiegruppe* von $x$. (Offenbar handelt es sich tatsächlich um eine Untergruppe von $G$.)
Die Klassen bzgl. der Äquivalenz (um eine solche handelt es sich offenbar) $x \sim x' :\Leftrightarrow \exists g \in G : gx = x'$ auf $S$ heißen *Orbits*, die wir mit $\overline{x} := [x]_\sim$ oder auch $O(x)$ bezeichnen. Wenn es zu je zwei Elementen $x, y \in S$ ein $g \in G$ mit $gx = y$ gibt (wenn ganz $S$ also der einzige Orbit der Gruppenaktion ist), heißt die Aktion *transitiv*.

Wir wollen uns noch kurz der in der Definition auftretenden Äquivalenzrelation $\sim$ zuwenden. Angenommen, aus den Orbits sei je ein Vertreter $x_i \in S$ ausgewählt. Darunter seien jene $x \in S$, die für sich bereits eine einelementige $\sim$-Äquivalenzklasse $\overline{x} = \{x\} = [x]_\sim$ bilden, zur Menge $S_0 \subseteq S$ zusammengefasst und die anderen mit $i \in I$ indiziert. Mit dieser Notation gilt offenbar:

**Proposition 8.1.1.4. (Klassengleichung für allgemeine Gruppenaktionen)***: Agiere $G$ auf $S$ und mögen die Elemente $x_i$, $i \in I$, ein vollständiges Vertretersystem für die Orbits mit mehr als einem Element bilden. Dann gilt:*

$$|S| = |S_0| + \sum_I |O(x_i)|.$$

Für uns wird der Fall, dass $S$ endlich ist, also $I = \{1, \ldots, n\}$ mit $n \in \mathbb{N}$, von besonderem Interesse sein. So werden wir sehen, dass im Falle der Aktion einer Gruppe durch Konjugation auf sich selbst diese an sich triviale Beziehung zu überraschend starken Einsichten in die Struktur endlicher Gruppen führt. Das hat auch mit der nächsten Beobachtung zu tun.

**Proposition 8.1.1.5.** *Sei $G$ eine Gruppe, die auf $S$ agiert, und $x \in S$. Dann gilt $|O(x)| = [G : G_x]$ (Index = Anzahl der Nebenklassen von $G_x$ in $G$). Für endliches $G$ ist insbesondere $|O(x)|$ eine Teiler von $|G|$.*

*Beweis.* Seien $g_1, g_2 \in G$. Dann gilt

$$g_1 x = g_2 x \Longleftrightarrow g_1^{-1} g_2 x = x \Longleftrightarrow g_1^{-1} g_2 \in G_x \Longleftrightarrow g_1 G_x = g_2 G_x.$$

Also entsprechen den Elementen im Orbit von $x$ die Linksnebenklassen von $G_x$ in $G$ in bijektiver Weise. □

Anwendung dieses Faktums auf Proposition 8.1.1.4 liefert:

**Korollar 8.1.1.6.** *Ist die Ordnung der endlichen, auf der endlichen Menge $S$ agierenden Gruppe $G$ eine Primzahlpotenz $p^n = |G|$ ($p \in \mathbb{P}$, $n \in \mathbb{N}$), so ist $|S| \equiv |S_0| \mod p$.*

*Beweis.* In der Gleichung $|S| = |S_0| + \sum_{i=1}^n |O(x_i)|$ aus Proposition 8.1.1.4 sind nach Proposition 8.1.1.5 und dem Satz von Lagrange (3.2.1.4) alle Summanden $|O(x_i)|$ durch $p$ teilbar. □

### 8.1.2 Aktion durch Konjugation und spezielle Klassengleichung

Im Zentrum steht nun eine besondere Gruppenaktion, die mit jeder (auch abstrakten) Gruppe automatisch einhergeht.

**Definition 8.1.2.1.** Ist $H$ eine Untergruppe von $G$, dann agiert $H$ via $\alpha : (h, x) \mapsto hxh^{-1}$ auf $G$. Diese Gruppenaktion $\alpha$ heißt *Konjugation*. Dabei sind die $\alpha_h : x \mapsto hxh^{-1}$ sogar Automorphismen von $G$, die so genannten *inneren Automorphismen*. Insbesondere agiert $H$ auch auf $\mathrm{Sub}(G) := \{U : U \leq G\}$. (Dabei sind alle Normalteiler Fixpunkte; im Fall $H = G$ sind die Normalteiler genau die Fixpunkte.) Die Orbits bezüglich Konjugation heißen *Konjugiertenklassen* (sowohl auf $\mathrm{Sub}(G)$ als auch auf $G$).

Durch Spezialisierung der Konzepte aus Unterabschnitt 8.1.1 auf Konjugation stoßen wir auf weitere wichtige Begriffe.

**Definition 8.1.2.2.** Sei $H$ eine Untergruppe von $G$. Der Stabilisator eines Elementes $x \in G$ bezüglich der Konjugation von $H$ auf $G$, d.h. die Untergruppe $Z_H(x) := H_x = \{h \in H : hxh^{-1} = x\} = \{h \in H : hx = xh\}$ von $H$ heißt *Zentralisator* von $x$ in $H$.
Der Schnitt aller $Z_G(x)$ (d.h. der Kern der Abbildung $g \mapsto \alpha_g$, der aus allen $x \in G$ mit $xg = gx$ für alle $g \in G$ besteht) wird mit $Z(G)$ bezeichnet und heißt *Zentrum* von $G$.
Schließlich nennt man den Stabilisator einer Untergruppe $K \leq G$ bezüglich der Aktion von $H$ durch Konjugation, also die Untergruppe $N_H(K) := \{h \in H : hKh^{-1} = K\}$ von $H$ den *Normalisator* von $K$ in $H$.

*Bemerkung* 8.1.2.3. Offenbar ist $N_G(K)$, der Normalisator von $K$, die größte Untergruppe von $G$, in der $K$ Normalteiler ist. Insbesondere gilt stets $K \lhd N_G(K)$.

Bezüglich der Aktion von $G$ durch Konjugation auf sich selbst bildet ein Element $x$ genau dann für sich eine einelementige Konjugiertenklasse $\overline{x} = \{x\}$, wenn $gxg^{-1} = x$, also $gx = xg$ für alle $g \in G$ gilt, wenn also $x \in Z(G)$. Sämtliche Konjugierten eines beliebigen $x \in G$ bilden den Orbit $O(x) = \overline{x}$, dessen Kardinalität nach Proposition 8.1.1.5 der Index des Stabilisators von $x$ in $G$ ist, hier also des Zentralisators $Z_G(x)$. Wir fassen zusammen:

**Proposition 8.1.2.4.** *Sei $G$ eine endliche Gruppe. Dann gilt*

1. *Für jedes $x \in G$ ist die Anzahl $|\overline{x}|$ der Elemente in der Konjugiertenklasse von $x$ gleich $[G : Z_G(x)]$ und teilt daher $|G|$.*

2. *Die Anzahl der zu $K \leq G$ konjugierten Untergruppen ist $[G : N_G(K)]$ und teilt daher $|G|$.*

3. *Seien $\overline{x}_1, \ldots, \overline{x}_n$ sämtliche Konjugiertenklassen (jede genau einmal). Dann ist*

$$|G| = \sum_{i=1}^{n} [G : Z_G(x_i)].$$

*Die Klassengleichung aus 8.1.1.4 nimmt damit folgende Form an: Bilden die Elemente $x_1, \ldots, x_m \in G$ ein vollständiges Vertretersystem der Konjugiertenklassen außerhalb des Zentrums $Z(G)$, so gilt*

$$|G| = |Z(G)| + \sum_{i=1}^{m} [G : Z_G(x_i)]. \tag{8.1}$$

*Beweis.* Alle Aussagen ergeben sich mit Hilfe des Vorangegangenen unmittelbar durch Spezialisierung der entsprechenden Aussagen aus Abschnitt 8.1.1. □

Bezeichne $\alpha$ die Aktion einer Gruppe $G$ auf sich selbst vermittels Konjugation, d.h. $\alpha_g \colon G \to G$, $x \mapsto gxg^{-1}$, ist der durch $g \in G$ induzierte innere Automorphismus. Der Gruppenhomomorphismus $\varphi : g \mapsto \alpha_g$ ist injektiv genau dann, wenn $|Z(G)| = 1$. Insbesondere ist dies der Fall, wenn $G = S_n$ eine symmetrische Gruppe mit $n \geq 3$ ist. In diesem Fall ist $\varphi$ also sogar eine isomorphe Einbettung von $G$ in seine Automorphismengruppe $\mathrm{Aut}(G)$, siehe auch Proposition 3.2.5.6.

### 8.1.3 Folgerungen aus der Klassengleichung und der Satz von Cauchy

Die erste von mehreren wichtigen Konsequenzen der Klassengleichung für Konjugation ist die folgende.

**Korollar 8.1.3.1.** *Jede endliche Gruppe $G$ von Primzahlpotenzordnung $p^n = |G|$ ($p \in \mathbb{P}$, $n \in \mathbb{N}$ mit $n \geq 1$) hat ein nichttriviales Zentrum $Z(G)$.*

*Beweis.* Nach der Klassengleichung aus 8.1.2.4 gilt

$$\underbrace{|G|}_{\equiv 0 \mod p} = |Z(G)| + \sum_{i=1}^{m} \underbrace{[G : Z_G(x_i)]}_{\equiv 0 \mod p}$$

Daher teilt $p$ auch $|Z(G)|$. Nun ist aber sicher $e \in Z(G)$, also gibt es mindestens $p > 1$ verschiedene Elemente in $Z(G)$. □

Nach den bisherigen Beobachtungen verwundert es nicht, dass die Theorie endlicher Gruppen stark kombinatorischen Charakter hat und dass überdies Teilbarkeiten eine besonders wichtige Rolle spielen, folglich auch Primzahlen und Primzahlpotenzen.
Als ersten Schritt in Richtung einer Analyse endlicher Gruppen mittels $p$-Untergruppen beweisen wir eine Art Umkehrung des Satzes von Lagrange.

**Satz 8.1.3.2** (Cauchy)**.** *Sei $G$ eine endliche Gruppe und $p \in \mathbb{P}$ ein Teiler der Gruppenordnung $|G|$. Dann gibt es ein $x \in G$ mit Ordnung $p$. Insbesondere existiert ein $H \leq G$ mit Ordnung $|H| = p$, nämlich $H = \langle x \rangle$ (die von $x$ erzeugte Untergruppe).*

*Beweis.* Die $p$-elementige zyklische Gruppe $C_p$ (aufgefasst als Addition modulo $p$) agiert auf der Menge $S := \{(a_1, \ldots, a_p) \in G^p : a_1 \ldots a_p = e\}$ mittels

$$\alpha(k, (a_1, \ldots, a_p)) := (a_{1+k}, a_{2+k}, \ldots, a_p, a_1, \ldots, a_k) \in S.$$

Diese Aktion ist wohldefiniert, weil für $s \in S$ und $k \in C_p$ auch $\alpha(k,s) \in S$ gilt. Denn für $k \in C_p$ und $s = (a_1, \ldots, a_p) \in S$ folgt aus $a_1 \ldots a_p = e$ mit $x := a_1 \ldots a_k$ und $y := a_{1+k} \ldots a_p$ sofort $xy = e$, also $y = x^{-1}$ und somit auch $yx = a_{1+k} \ldots a_p a_1 \ldots a_k = e$, was

$$\alpha(k,s) = (a_{1+k}, \ldots, a_p, a_1, \ldots a_k) \in S$$

bedeutet, wie behauptet. Offensichtlich ist $(a_1, \ldots, a_p) \in S_0$ genau dann, wenn $a_1 = \ldots = a_p$. Insbesondere gilt $(e, \ldots, e) \in S_0$, also $|S_0| \geq 1$. Weil sich jedes der $p^{n-1}$ verschiedenen $n-1$-Tupel $(a_1, \ldots, a_{p-1}) \in G^{p-1}$ durch genau ein $a_p$ zu einem $p$-Tupel $(a_1, \ldots, a_{p-1}, a_p) \in S$ ergänzen lässt, ist $|S| = |G|^{p-1} \equiv 0 \mod p$ (beachte $p \geq 2$). Korollar 8.1.1.6 (die Rolle des dortigen $G$ spielt hier $C_p$) zeigt $|S_0| \equiv |S| \equiv 0 \mod p$ und somit $|S_0| \geq p$. Das bedeutet aber gerade, dass es mindestens $p$ Elemente $x$ gibt mit $(x, \ldots, x) \in S_0 \subseteq S$, also mit $x^p = e$. Davon ist wegen $p \geq 2$ mindestens eines von $e$ verschieden. So ein $x$ hat die Ordnung $p$. □

**Definition 8.1.3.3.** Sei $G$ eine beliebige Gruppe und $p \in \mathbb{P}$. Ist für alle $x \in G$ die Ordnung von $x$ eine $p$-Potenz, so heißt $G$ eine *$p$-Gruppe*, im Fall $|G| > 1$ eine *nichttriviale $p$-Gruppe*.
$H \leq G$ heißt *$p$-Untergruppe* von $G$, wenn $H$ eine $p$-Gruppe ist. Maximale $p$-Untergruppen von $G$ heißen *$p$-Sylow-Gruppen* von $G$ (diese existieren nach dem Lemma von Zorn auch für unendliche Gruppen).

**Korollar 8.1.3.4.** *Die Ordnung jeder endlichen $p$-Gruppe $G$ ist eine $p$-Potenz.*

*Beweis.* Andernfalls hätte $|G|$ einen von $p$ verschiedenen Primteiler $q$, nach dem Satz 8.1.3.2 von Cauchy also auch ein Element $x \in G$ der Ordnung $q$, was der Definition einer $p$-Gruppe widerspricht. □

### 8.1.4 Die drei Sylow-Sätze

Die drei Sylow-Sätze, deren Beweis unser nächstes Ziel ist, geben Auskunft über die $p$-Sylowgruppen $P$ einer endlichen Gruppe $G$. Grob gesprochen besagen sie: Erstens gibt es in jedem $G$ und zu jedem $p \in \mathbb{P}$ ein $P$, dessen Ordnung die maximale Potenz von $p$ ist, durch die $|G|$ teilbar ist. Zweitens sind je zwei solcher $P$ zueinander konjugiert. Und drittens ist ihre Anzahl $n$ einerseits Teiler von $|G|$ und andererseits kongruent 1 modulo $p$.
Ein wesentliches Hilfsmittel im Beweis des ersten Sylow-Satzes ist das nachfolgende Lemma. Gemeinsam mit dem Satz von Cauchy hat es zur Folge, dass man Untergruppen von $p$-Potenzordnung $p^i$ zu solchen der Ordnung $p^{i+1}$ erweitern kann, bis man bei der maximalen $p$-Potenz, welche die Gruppenordnung $|G|$ teilt, angelangt ist.

**Lemma 8.1.4.1.** *Sei $G$ eine endliche Gruppe und $H$ eine $p$-Untergruppe von $G$. Dann ist $[N_G(H) : H] \equiv [G : H] \mod p$. Gilt zusätzlich $p|[G : H]$, so ist insbesondere $H \subsetneq N_G(H)$.*

*Beweis.* Sei $S := \{aH : a \in G\}$. Dann agiert $H$ auf $S$ durch Linkstranslation mit $|S| = [G : H]$. Nach Korollar 8.1.1.6 gilt $|S| \equiv |S_0| \mod p$. Die Behauptung des Lemmas folgt,

sofern wir zeigen können, dass $S_0$ gerade aus jenen Nebenklassen $xH$ mit $x \in N_G(H)$ besteht. Denn dann folgt

$$[N_G(H) : H] = |S_0| \equiv |S| = [G : H] \mod p,$$

die erste Behauptung. Tatsächlich gilt folgende Kette von Äquivalenzen:

$$\begin{aligned} xH \in S_0 &\Leftrightarrow hxH = xH \quad \forall h \in H \\ &\Leftrightarrow x^{-1}hxH = H \quad \forall h \in H \\ &\Leftrightarrow x^{-1}hx \in H \quad \forall h \in H \\ &\Leftrightarrow xHx^{-1} = H \\ &\Leftrightarrow x \in N_G(H) \end{aligned}$$

Die zweite Behauptung folgt daraus unmittelbar. □

**Satz 8.1.4.2. (Erster Sylow-Satz)** *Sei $G$ eine endliche Gruppe mit $|G| = p^n m$, $n \in \mathbb{N}$ und $p \in \mathbb{P}$, wobei $m$ nicht durch $p$ teilbar ist. Dann gibt es in $G$ eine $p$-Sylow-Gruppe der (nach dem Satz von Lagrange maximal möglichen $p$-Potenz-) Ordnung $p^n$.*
*Es gilt sogar stärker: Es gibt eine aufsteigende Kette von Untergruppen $H_i \leq G$ mit $|H_i| = p^i$ für $i = 0, \ldots, n$ und*

$$H_0 = \{e\} \lhd H_1 \lhd \ldots \lhd H_i \lhd H_{i+1} \lhd \ldots \lhd H_n.$$

*Beweis.* Wir zeigen mit Induktion nach $k$, dass es für $k = 0, 1, \ldots, n$ eine aufsteigende Kette von Untergruppen $H_i \leq G$ gibt mit $|H_i| = p^i$ für $i = 0, \ldots, k$ und

$$H_0 = \{e\} \lhd H_1 \lhd \ldots \lhd H_i \lhd H_{i+1} \lhd \ldots \lhd H_k.$$

Für $k = 0$ ist nichts zu zeigen, und für $k = 1$ folgt die Behauptung unmittelbar aus dem Satz von Cauchy (8.1.3.2). Gelte also die Behauptung für ein $k$ mit $1 \leq k < n$ und sei $H_k \leq G$ mit Ordnung $|H_k| = p^k$. Aus $k < n$ folgt $p|[G : H_k]$. Aus Lemma 8.1.4.1 schließen wir

$$1 \leq [N_G(H_k) : H_k] \equiv [G : H_k] \equiv 0 \mod p,$$

also $p|[N_G(H) : H_k]$. Wendet man nochmals den Satz von Cauchy an, diesmal auf $N_G(H_k)/H_k$, dann erhält man eine Untergruppe $H'$ von $N_G(H_k)/H_k$ der Ordnung $p$. Nun ist $H' = H_{k+1}/H_k$ mit $H_k < H_{k+1} \leq N_G(H_k)$, daher $|H_{k+1}| = |H_k| \cdot [H_{k+1} : H_k] = p^k \cdot p = p^{k+1}$ und wegen $H_k \lhd N_G(H)$ auch $H_k \lhd H_{k+1}$. □

**Satz 8.1.4.3. (Zweiter Sylow-Satz)** *Sei $G$ eine endliche Gruppe und $p \in \mathbb{P}$, $H \leq G$ eine $p$-Untergruppe und $P$ eine $p$-Sylow-Gruppe von $G$. Dann existiert ein $x \in G$, so dass $H \leq xPx^{-1}$. Insbesondere sind je zwei $p$-Sylow-Gruppen konjugiert und somit auch isomorph.*

*Beweis.* $H$ agiert auf der Menge $S := \{aP : a \in G\}$ via Linkstranslation. Aus Korollar 8.1.1.6 und weil $P$ eine $p$-Sylow-Gruppe ist, folgt $|S_0| \equiv |S| = [G : P] \not\equiv 0 \mod p$. Also ist $|S_0| > 0$, d.h. es gibt ein $xP \in S_0$. Das bedeutet $hxP = xP$ und somit $x^{-1}hx \in P$ für alle $h \in H$. Somit ist $x^{-1}Hx \leq P$ bzw. $H \leq xPx^{-1}$, die erste Behauptung. Ist speziell $H$ eine weitere $p$-Sylow-Gruppe, so folgt aus Kardinalitätsgründen $H = xPx^{-1}$. □

**Korollar 8.1.4.4.** *Sei $P$ eine $p$-Sylowgruppe der endlichen Gruppe $G$. Dann ist $P$ genau dann die einzige $p$-Sylowgruppe von $G$, wenn $P$ Normalteiler in $G$ ist.*

*Beweis.* Ist $P$ die einzige $p$-Sylowgruppe, so muss $P$ mit allen seinen Konjugierten $xPx^{-1} = P$ übereinstimmen, also $P \lhd G$. Offenbar gilt auch die Umkehrung. □

**Satz 8.1.4.5. (Dritter Sylow-Satz)** *Sei $G$ eine endliche Gruppe, $p \in \mathbb{P}$ und $n := |S|$ für die Menge $S$ aller $p$-Sylow-Gruppen von $G$. Dann teilt $n$ die Gruppenordnung $|G|$, und außerdem ist $n \equiv 1 \mod p$.*

*Beweis.* Für beide Behauptungen betrachten wir Aktionen auf $S$ durch Konjugation – für die erste die Aktion von $G$, für die zweite die Aktion von $P$, einer $p$-Sylowgruppe, die nach dem ersten Sylow-Satz 8.1.4.2 ja existiert.
Agiert $G$, so ist $S$ nach dem zweiten Sylow-Satz (8.1.4.3) gerade der Orbit von $P$. Seine Kardinalität $n$ teilt nach Proposition 8.1.2.4 (i) die Gruppenordnung $|G|$.
In Hinblick auf die zweite Behauptung $n \equiv 1 \mod p$ bemühen wir Korollar 8.1.1.6, wonach ja $n = |S| \equiv |S_0| \mod p$ für die Menge $S_0$ aller gemeinsamen Fixpunkte der Aktion gilt. Bei der Aktion von $P$ auf $S$ sind das jene $Q \in S$ mit $xQx^{-1} = Q$ für alle $x \in P$, d.h. mit $P \subseteq N_G(Q)$. Wegen $Q \lhd N_G(Q)$ kann es innerhalb $N_G(Q)$ nach Korollar 8.1.4.4 aber nur eine $p$-Sylowgruppe geben, also $P = Q$. Somit ist $S_0 = \{P\}$, folglich $n \equiv 1 \mod p$, wie behauptet. □

**Korollar 8.1.4.6.** *Sei $G$ eine endliche Gruppe, $p \in \mathbb{P}$ und $P$ eine $p$-Sylow-Gruppe von $G$. Für $N := N_G(P)$ gilt dann $N_G(N) = N$.*

*Beweis.* Wir müssen die Inklusion $N_G(N) \subseteq N$ beweisen. Sei dazu $x \in N_G(N)$, d.h. $xNx^{-1} = N$. Folglich ist neben $P$ auch $P' := xPx^{-1} \subseteq xNx^{-1} = N$ eine $p$-Sylowgruppe innerhalb von $N$. Wegen $P \lhd N = N_G(P)$ und Korollar 8.1.4.4 ist $P$ aber die einzige $p$-Sylow-Gruppe von $N$. Also ist $P = P' = xPx^{-1}$ und somit auch $x \in N_G(P) = N$. □

**UE 426** ► **Übungsaufgabe 8.1.4.7.** Beschreiben Sie für eine möglichst große Menge von Paaren $(n, p) \in \mathbb{N} \times \mathbb{P}$ alle $p$-Sylowgruppen der symmetrischen Gruppe $S_n$. ◄ **UE 426**

### 8.1.5 Eine Anwendung der Klassengleichung: Der Satz von Wedderburn

In 6.3 wurden die endlichen Körper klassifiziert: Unter den natürlichen Zahlen sind es genau die Primzahlpotenzen $p^n$, $p \in \mathbb{P}$ und $n \in \mathbb{N}$ mit $n \geq 1$, zu denen es einen Körper $K$ mit dieser Kardinalität gibt, und je zwei Körper der Kardinalität $p^n$ sind isomorph zueinander. Es ist bemerkenswert, dass diese Aussage auch gilt, wenn man auch Schiefkörper (Divisionsringe) zulässt, also Ringe mit Einselement, wo die von 0 verschiedenen Elemente eine mutiplikative Gruppe bilden, die im Gegensatz zu den Körpern aber nicht kommutativ sein muss. Mit anderen Worten: Jeder endliche Schiefkörper ist sogar ein Körper. Nichtkommutative Schiefkörper müssen also unendlich sein, so wie die Hamiltonschen Quaternionen, das prominenteste Beispiel eines Schiefkörpers. Unser Ziel ist also der Beweis folgenden Satzes:

**Satz 8.1.5.1** (Wedderburn)**.** *Jeder endliche Divisionsring (Schiefkörper) $D$ ist ein Körper.*

*Beweis.* Für jedes $a \in D$ sei $Z(a) := \{d \in D : \ da = ad\}$. Wir behaupten zunächst, dass $Z(a)$ ein Unterdivisionsring von $D$ ist, folglich auch der Schnitt $K$ aller $Z(a)$, $a \in D$. Weil

$$K = \{a \in D : \forall d \in D : ad = da\}$$

selbst kommutativ ist, handelt es sich um einen endlichen Körper. Nach dem Klassifikationssatz 6.3.1.2 ist daher $q := |K| = p^m$ mit $p \in \mathbb{P}$ und positivem $m \in \mathbb{N}$.
Zum Beweis, dass $Z(a)$ ein Unterdivisionsring von $D$ ist, stellen wir zunächst $0, 1 \in Z(a)$ fest. Außerdem beachte man, dass $Z(a)$ der Zentralisator von $a$ innerhalb der multiplikativen Gruppe $D^* = D \setminus \{0\}$ erweitert um die 0 ist. Daraus folgt, dass $Z(a)^*$ eine Untergruppe von $D^*$ ist. Klarerweise ist dann auch $Z(a) = Z(a)^* \cup \{0\}$ multiplikativ abgeschlossen. $Z(a)$ ist aber auch eine additive Untergruppe von $D$: Aus $d_1, d_2 \in Z(a)$ folgt $ad_1 = d_1a$ und $ad_2 = d_2a$, somit auch $a(d_1+d_2) = ad_1+ad_2 = d_1a+d_2a = (d_1+d_2)a$, also $d_1 + d_2 \in Z(a)$. Schließlich liegt mit $d \in Z(a)$ auch $-d$ in $Z(a)$, wie die Umformung $a(-d) = -(ad) = -(da) = (-d)a$ beweist.
Wir können $D$ also auch als Vektorraum auffassen, sowohl über $K$ als auch über $Z(a)$, überdies $Z(a)$ als Vektorraum über $K$. Seien $n := \dim_K D$, $d_a := \dim_{Z(a)} D$ und $n_a := \dim_K Z(a)$ die zugehörigen Dimensionen. Zu zeigen ist $n = 1$. Nach dem Gradsatz 6.1.2.2 gilt $n = n_a d_a$, insbesondere also $n_a | n$. Außerdem ist $|D| = |K|^n = q^n = p^{mn}$. Für die multiplikativen Gruppen $Z(a)^* \leq D^*$ gilt $|D^*| = q^n - 1$ und $|Z(a)^*| = q^{n_a} - 1$, nach dem Satz von Lagrange folglich $q^{n_a} - 1 | q^n - 1$ bzw., äquivalent, $\frac{q^n-1}{q^{n_a}-1} \in \mathbb{N}$.
Für $D^*$ bringen wir nun die Klassengleichung aus 8.1.2.4 ins Spiel:

$$q^n - 1 = |D^*| = |K^*| + \sum_{a \in A} [D^* : C(a)^*] = q - 1 + \sum_{a \in A} \frac{q^n - 1}{q^{n_a} - 1} \in \mathbb{N},$$

wobei $a$ ein vollständiges Repräsentantensystem $A$ für jene Konjugiertenklassen durchläuft, die aus mehr als einem Element bestehen.
Außerdem ziehen wir die Kreisteilungspolynome $g_n$ aus 6.2.5 zu Rate. Zur Erinnerung: Diese Polynome haben ganzzahlige Koeffizienten mit konstantem Term $\pm 1$ und zerfallen in das Produkt

$$g_n = \prod_{k \in \mathbb{Z}_n^*} (x - \zeta^k),$$

wobei $\zeta$ eine primitive $n$-te Einheitswurzel ist. Die Einheitengruppe $\mathbb{Z}_n^*$ besteht aus den zu $n$ teilerfremden Restklassen modulo $n$. Weil $\zeta$ auf dem komplexen Einheitskreis liegt und $q$ eine natürliche Zahl mit $q > 1$ ist, gilt in der komplexen Zahlenebene die später noch nützliche Abschätzung $|q - \zeta| > q - 1 \geq 1$. Das Polynom $x^n - 1$ lässt sich wie folgt zerlegen:

$$x^n - 1 = \prod_{d|n} g_d(x) = (x^{n_a} - 1) g_n(x) \prod_{\substack{d|n; d \nmid n_a \\ d \neq n}} g_d(x).$$

Wegen der Ganzzahligkeit der Koeffizienten der Kreisteilungspolynome zeigt Einsetzen von $q$ für $x$ die Teilbarkeiten $g_n(q) \mid q^n - 1$ und $g_n(q) \mid \frac{q^n-1}{q^{n_a}-1}$. Weil letzteres für alle $a$

gilt, lesen wir aus der Klassengleichung ab, dass auch der verbleibende Summand $q-1$ durch $g_n(q)$ teilbar ist, also $g_n(q)|q-1$. Daraus und aus der indirekten Annahme $n>1$ werden wir nun einen Widerspruch ableiten können:
Sei $\zeta = a+ib$ mit $a^2+b^2=1$, $a,b\in\mathbb{R}$, irgendeine der primitiven $n$-ten Einheitswurzeln mit Realteil $a$ und Imaginärteil $b$. Für $n>1$ ist $a<1$. Daraus ergibt sich

$$|q-\zeta|^2 = |q-a-ib|^2 = (q-a)^2+b^2 = q^2-2aq+a^2+b^2 = q^2-2aq+1 > q^2-2q+1 = (q-1)^2,$$

folglich $|q-\lambda| > q-1 \geq 1$ und, weil das für alle primitiven Einheitswurzeln $\zeta$ gilt,

$$|g_n(q)| = \prod_{\zeta} |q-\zeta| > q-1.$$

Das verträgt sich aber nicht mit der zuvor hergeleiteten Teilbarkeit $g_d(q)|q-1$. Der Widerspruch zur Annahme $n>1$ zeigt $n=1$, also ist $D=K$ tatsächlich ein Körper. □

## 8.2 Einige konkrete Beispiele

In diesem Abschnitt nehmen wir uns ein paar konkrete Beispiele vorwiegend endlicher Gruppen vor. Der Fokus liegt auf den nichtabelschen Gruppen, weil wir die abelschen Dank Hauptsatz 7.4.3.2 schon sehr gut verstehen. Für die nichtabelschen gelingt selbst unter Zuhilfenahme der bisher entwickelten allgemeinen Theorie ein vollständiger Überblick lediglich für kleine Ordnungen. Als nützlich erweist sich die (nicht auf endliche Gruppen beschränkte) Methode der Darstellung durch Erzeuger und Relationen (8.2.1). Mit ihrer Hilfe lassen sich auch die sogenannten Diedergruppen (sprich: Di-eder-gruppen) $D_n$ der Ordnung $2n$ (8.2.2), die Alternierenden Gruppen $A_n$ der Ordnung $\frac{n!}{2}$ (8.2.3), die achtelementige *Quaternionengruppe* $Q_8$ und eine verwandte 12-elementige Gruppe als Spezialfälle sogenannter dizyklischer Gruppen beschreiben (8.2.4), die sich für die Klassifikation aller Gruppen bis zur Ordnung 15 (8.2.6) als zweckmäßig erweist.

### 8.2.1 Die Beschreibung von Gruppen durch Erzeuger und Relationen

Eine wichtige Möglichkeit zur Beschreibung von Gruppen, insbesondere von endlichen, besteht vermöge *Erzeuger und Relationen*:

**Definition 8.2.1.1.** Sei $X$ eine Menge, und $F(X)$ die von $X$ frei erzeugte Gruppe, die wir als Menge (reduzierter) Gruppenwörter (siehe 4.1.4) auffassen. Für eine Teilmenge $Y\subseteq F(X)$ sei $N=N(Y)$ der von $Y$ erzeugte Normalteiler in $F(X)$. Die Gruppe $G := F(X)/N$ heißt die durch $X$ und die Relationen „$w=e$“, $w\in Y$, dargestellte Gruppe. Man schreibt für $G$ auch $\langle X|Y\rangle$ und spricht dabei von einer *Darstellung durch Erzeuger und Relationen*.

Als Beispiel bestehe $X=\{x,y\}$ aus zwei Elementen $x\neq y$, $Y=\{w\}$ aus dem einzigen Wort $w=xyx^{-1}y^{-1}$. Die Gruppe $\langle X|Y\rangle$ ist dann isomorph zu $\mathbb{Z}^2$. Denn die Relation $w=xyx^{-1}y^{-1}=e$ ist äquivalent zu $xy=yx$, drückt also das Vertauschen der beiden

Elemente $x$ und $y$ aus. Somit ist die von $X = \{x, y\}$ erzeugte Gruppe kommutativ. Weitere Einschränkungen gibt es nicht, also ist $\langle X|Y\rangle$ die von zwei Elementen frei erzeugte abelsche Gruppe, die isomorph ist zu $\mathbb{Z}^2$.

**UE 427 ▶ Übungsaufgabe 8.2.1.2.** 1. Geben Sie einen strengen Beweis für die oben behauptete Isomorphie $\langle X|Y\rangle \cong \mathbb{Z}^2$ für $X = \{x, y\}$ und $Y = \{xyx^{-1}y^{-1}\}$ unter Verwendung von Definition 8.2.1.1. **◀ UE 427**

2. Zeigen Sie allgemein: Ist $H$ eine beliebige von $X$ erzeugte Gruppe, welche die Relationen $w = e, w \in Y$, erfüllt, so existiert ein eindeutiger Epimorphismus von $G := \langle X|Y\rangle$ nach $H$, der die Elemente $xN(Y) \in F(X)/N(Y)$, $x \in X$, auf $x \in H$ abbildet. Deuten Sie entsprechend $G$ auch als universelles Objekt in einer geeigneten Kategorie.

### 8.2.2 Die Diedergruppen $D_n$

Die *Diedergruppe* $D_n$ lässt sich am einfachsten beschreiben als Symmetriegruppe des regelmäßigen $n$-Ecks. Definitionsgemäß ist damit die Menge $D_n$ aller Isometrien $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ gemeint ($f$ soll also den euklidischen Abstand zwischen zwei Punkten der Ebene unverändert lassen), welche die Menge $E_n$ der Eckpunkte $\zeta_k = (\cos(\frac{2k\pi}{n}), \sin(\frac{2k\pi}{n}))$, $k = 0, 1, \ldots, n-1\}$, permutiert. Gruppenoperation ist die Komposition von Abbildungen. Klarerweise lassen sich isomorphe Kopien von $D_n$ auch anders beschreiben. Zwei derartige Beschreibungen ergeben sich aus der folgenden Aufgabe.

**UE 428 ▶ Übungsaufgabe 8.2.2.1.** Beschreiben Sie eine zu $D_n$ isomorphe Gruppe $G$ als: **◀ UE 428**

1. Untergruppe der symmetrischen Gruppe $S_n$.

2. Durch zwei Erzeuger $a, b$ und drei geeignete Relationen, von denen zwei $a^n = e$ und $b^2 = e$ lauten.

### 8.2.3 Die alternierenden Gruppen $A_n$

Die *alternierende Gruppe* $A_n$ ist jene Untergruppe der $S_n$, die aus den geraden Permutationen besteht.

**UE 429 ▶ Übungsaufgabe 8.2.3.1.** Behandeln Sie im Zusammenhang mit der alternierenden Gruppe $A_n$ folgende Aufgaben. **◀ UE 429**

1. Rekapitulieren Sie die Schreibweise von Permutationen mittels paarweise elementfremder Zyklen und wie sich daraus ihre Ordnungen als Gruppenelemente ablesen lassen.

2. Wiederholen Sie aus 3.2.5, wie gerade und ungerade Permutationen definiert sind und warum für $n \geq 2$ die geraden innerhalb der symmetrischen Gruppe $S_n$ einen Normalteiler der Ordnung $\frac{n!}{2}$ bilden.

3. Beschreiben Sie allgemein anhand der Zyklenschreibweise, welche Permutationen aus der symmetrischen Gruppe $S_n$ zu $A_n$ gehören.

4. Bestimmen Sie in $A_4$ die Ordnungen der Elemente, das Zentrum und sämtliche Untergruppen und Normalteiler.

5. Geben Sie eine Darstellung von $A_4$ durch Relationen und Erzeuger an.

Interesante Implikationen in der Galoistheorie hat der folgende Satz:

**Satz 8.2.3.2.** *$A_n$ ist für alle $n \geq 5$ einfach.*

**UE 430** ▶ **Übungsaufgabe 8.2.3.3.** Beweisen Sie Satz 8.2.3.2, indem Sie für einen beliebigen Normalteiler $N \lhd A_n$ mit $|N| > 1$ zeigen, dass $N = A_n$ folgt. Das ergibt sich durch die unten vorgeschlagenen Schritte. Dabei beziehen wir uns auf Zyklenschreibweise, d.h. auf die Darstellung von Elementen in $S_n$ als Produkte paarweise elementfremder Zyklen. $N$ bezeichne einen Normalteiler $N \lhd A_n$ mit $|N| > 1$. ◀ **UE 430**

1. $A_n$ wird von sämtlichen Dreierzyklen erzeugt.

2. Beliebige 3-Zyklen lassen sich durch spezielle erzeugen, nämlich für beliebig fest gewählte $a \neq b \in \{1, \ldots, n\}$ durch alle $(abc)$, $c = 1, \ldots, n$.

3. Enthält $N$ einen 3-Zyklus, so folgt $N = A_n$. Hinweis: Aussage 2 verwenden.

4. Enthält $N$ ein Element, in dessen Zyklenschreibweise ein $k$-Zyklus mit $k \geq 4$ vorkommt, so folgt $N = A_n$.

5. Enthält $N$ ein Element, in dessen Darstellung zwei 3-Zyklen vorkommen, so folgt $N = A_n$.

6. Enthält $N$ ein Element, in dessen Darstellung ein 3-Zyklus und sonst lauter 2-Zyklen vorkommen, so folgt $N = A_n$.

7. $N$ enthalte ein Element $\sigma$ mit disjunkter Zyklendarstellung $\sigma = (a_1a_2)(a_3a_4)\tau$, wobei sich $\tau$ ausschließlich aus (zueinander und zu $\{a_1, a_2, a_3, a_4\}$ disjunkten) 2-Zyklen zusammensetze. Sei $b$ verschieden von $a_1, a_2, a_3, a_4$ (hier geht $n \geq 5$ ein), $\xi = (a_1a_2b) \in A_n$ und $\zeta = (a_1a_3)(a_2a_4)$. Zeigen Sie $\zeta \in N$ (Hinweis: $\zeta = \sigma^{-1}(\delta\sigma\delta^{-1})$ mit $\delta = (a_1a_2a_3)$) und $\zeta\xi\zeta\xi^{-1} = (a_1a_3a_4ba_2) \in N$, um auf $N = A_n$ zu schließen.

8. Schließen Sie den Beweis von Satz 8.2.3.2 ab.

### 8.2.4 Die Quaternionengruppe $Q_8$ und dizyklische Gruppen

Die achtelementige *Quaternionengruppe* $Q_8$ lässt sich definieren als die (multiplikative) Gruppe komplexer $2 \times 2$-Matrizen, die von den Elementen $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ und $B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ erzeugt wird. Leicht sieht man einige hilfreiche Eigenschaften ein.

**UE 431** ► **Übungsaufgabe 8.2.4.1.** Zeigen Sie für $Q_8$: ◄ **UE 431**

(1) Die oben angegebenen Erzeugenden erfüllen $BA = A^3B$.

(2) $|Q_8| = 8$.

(3) Es gibt eine Darstellung von $Q_8$ mit Hilfe der oben angegebenen Erzeugenden $A$ und $B$ und geeigneten Relationen. Mit welchen?

(4) Eine zu $Q_8$ isomorphe Gruppe $G$ besteht aus den Elementen $\pm 1, \pm i, \pm j, \pm k$ mit $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$ und $ik = -j$ etc. Führen Sie diesen Ansatz aus.

(5) Bestimmen Sie die Ordnungen der Elemente von $Q_8$ sowie sämtliche Untergruppen, Normalteiler und das Zentrum $Z(Q_8)$.

Die Darstellung von $Q_8$ mittels Erzeugern und Relationen, nach der in Teil (3) obiger Übungsaufgabe gefragt wurde, lässt sich verallgemeinern:

**Satz 8.2.4.2.** *Zu jeder positiven natürlichen Zahl $n$ gibt es eine (bis auf Isomorphie eindeutig bestimmte Gruppe), genannt die* dizyklische Gruppe *$Dic_n$ der Ordnung $4n$ (für Zweierpotenzen auch:* verallgemeinerte Quaternionengruppe*), mit der Darstellung $Dic_n = \langle X|Y\rangle$, wobei $X$ die beiden Erzeuger $x, y$ enthält, und $Y$ den Relationen $x^{2n} = e$, $x^n = y^2$ und $yxy^{-1} = x^{-1}$ entspricht. Für $n = 1$ ist diese Gruppe isomorph zu $C_2 \times C_2$, für $n = 2$ zu $Q_8$.*

**UE 432** ► **Übungsaufgabe 8.2.4.3.** Beweisen Sie Satz 8.2.4.2. ◄ **UE 432**

Über die dizyklische Gruppe $\mathrm{Dic}_3$ der Ordnung 12 lassen sich noch weitere interessante Aussagen machen, die Gegenstand der folgenden Übungsaufgabe sind.

**UE 433** ► **Übungsaufgabe 8.2.4.4.** Zeigen Sie, dass es eine Gruppe $G \leq S_3 \times C_4$ mit folgenden Eigenschaften gibt. ◄ **UE 433**

1. $|G| = 12$.
2. $G$ wird von zwei Elementen $a, b$ erzeugt. Dabei hat $a$ die Ordnung 6, und es gelten die Gleichungen $a^3 = b^2$ und $ba = a^{-1}b$.
3. Jede Gruppe der Ordnung 12 mit den Eigenschaften aus 1 und 2 ist zu $\mathrm{Dic}_3$ isomorph.

### 8.2.5 Zwei weitere Struktursätze

Wir erwähnen noch zwei weitere für die Strukturtheorie endlicher Gruppen typische Sätze. In 8.2.6 werden sie sich als hilfreich bei der Klassifikation aller Gruppen der Ordnung $\leq 15$ erweisen.

**Satz 8.2.5.1.** *Jede Gruppe der Ordnung $p^2$, $p \in \mathbb{P}$, ist abelsch.*

**UE 434** ▶ **Übungsaufgabe 8.2.5.2.** Beweisen Sie Satz 8.2.5.1. Anleitung: Zeigen Sie, dass jede Gruppe mit zyklischem $G/C(G)$ abelsch ist. ◀ **UE 434**

**Satz 8.2.5.3.** *Sei $G$ eine Gruppe der Ordnung $pq$ mit $p > q \in \mathbb{P}$. Ist $G$ nicht zyklisch (d.h. nicht isomorph zu $C_{pq}$), dann liegt folgende Situation vor:*
*Der Faktor $q$ von $|G|$ teilt $p-1$, und $G$ wird von zwei Elementen $a, b$ mit den Ordnungen $p$ bzw. $q$ erzeugt. Außerdem gibt es ein $s \not\equiv 1 \mod p$ mit $s^q \equiv 1 \mod p$.*

**UE 435** ▶ **Übungsaufgabe 8.2.5.4.** Beweisen Sie Satz 8.2.5.3. (Recherchieren Sie in der Literatur, zum Beispiel in Hungerfords Buch, wenn die Aufgabe zu schwierig ist.) ◀ **UE 435**

**Korollar 8.2.5.5.** *Ist $p \in \mathbb{P} \setminus \{2\}$ und $|G| = 2p$, dann ist entweder $G \cong C_{2p}$ oder $G \cong D_p$.*

**UE 436** ▶ **Übungsaufgabe 8.2.5.6.** Beweisen Sie Korollar 8.2.5.5. ◀ **UE 436**

### 8.2.6 Bemerkungen zur Klassifikation endlicher Gruppen

Die Klassifikation aller endlichen Gruppen scheint aus heutiger Sicht illusorisch. Immerhin gelang 1982 als Zusammenfassung fast unüberschaubar vieler Einzelresultate die Klassifikation aller endlichen einfachen Gruppen (also jener endlichen Gruppen, die nur die trivialen Normalteiler haben). Neben den zyklischen Gruppen $C_p$ von Primzahlordnung $p$ und den alternierenden Gruppen $A_n$ mit $n \geq 5$ treten darin 16 unendliche Serien auf (man nennt sie *Gruppen vom Lie-Typ*) und darüber hinaus 26 sogenannte *sporadische Gruppen*. Doch schon eine genaue Formulierung des entsprechenden Klassifikationssatzes würde unseren Rahmen hier bei Weitem sprengen.
Im Lichte späterer Resultate – nämlich des Satzes von Jordan-Hölder, siehe 8.3.4.3, und der Erweiterungstheorie, siehe 8.4 – wird die Bedeutung der Klassifikation der endlichen einfachen Gruppen deutlicher. Denn jede endliche Gruppe $G$ hat eine Kompositionsreihe (siehe 8.3.3). Die Faktoren irgendeiner Kompositionsreihe sind nach Jordan-Hölder bis auf Isomorphie und Reihenfolge durch $G$ eindeutig eindeutige bestimmt. Wenn man auch noch versteht, wie diese Faktoren zu verschiedenen Gruppen $G$ zusammengesetzt werden können – und das ist der Gegenstand der Erweiterungstheorie – überblickt man alle endlichen Gruppen. Leider ist die Erweiterungstheorie nicht so mächtig. Erst recht müssen wir uns in dieser Vorlesung äußerst bescheiden mit einer Klassifikation der endlichen Gruppen $G$ der Ordnung $n = |G| \leq 15$ begnügen. Die Tabelle in Abbildung 8.1 gibt darüber hinaus die Anzahl der abelschen und nichtabelschen Isomorphietypen bis zur Ordnung 20 an.
Ähnlich wie bei den meisten Klassifikationen besteht der schwierigste Teil auch hier darin zu beweisen, dass in der Tabelle keine Gruppe fehlt. Dass je zwei Gruppen daraus nicht isomorph sind, folgt relativ leicht mit ein paar bereits bekannten, typischen Eigenschaften

| **n** | **abelsch**<br>zyklisch / nicht zyklisch | **Anzahl** | **nichtabelsch** | **Anzahl** |
|---|---|---|---|---|
| 1 | $C_1$ | 1 | | |
| 2 | $C_2$ | 1 | | |
| 3 | $C_3$ | 1 | | |
| 4 | $C_4, C_2 \times C_2$ | 2 | | |
| 5 | $C_5$ | 1 | | |
| 6 | $C_6$ | 1 | $S_3 \cong D_3$ | 1 |
| 7 | $C_7$ | 1 | | |
| 8 | $C_8, C_4 \times C_2, C_2^3$ | 3 | $D_4, Q_8 \cong \mathrm{Dic}_2$ | 2 |
| 9 | $C_9, C_3 \times C_3$ | 2 | | |
| 10 | $C_{10}$ | 1 | $D_5$ | 1 |
| 11 | $C_{11}$ | 1 | | |
| 12 | $C_{12}, C_2 \times C_6$ | 2 | $A_4, D_6 \cong S_3 \times C_2, \mathrm{Dic}_3$ | 3 |
| 13 | $C_{13}$ | 1 | | |
| 14 | $C_{14}$ | 1 | $D_7$ | 1 |
| 15 | $C_{15}$ | 1 | | |
| 16 | $C_{16}, C_8 \times C_2, C_4^2, C_4 \times C_2^2, C_2^4$ | 5 | ... | 9 |
| 17 | $C_{17}$ | 1 | | |
| 18 | $C_{18}, C_6 \times C_3$ | 2 | ... | 3 |
| 19 | $C_{19}$ | 1 | | |
| 20 | $C_{20}, C_{10} \times C_2$ | 2 | ... | 3 |

Abbildung 8.1: Klassifikation aller Gruppen $G$ mit kleinem $n = |G|$

der Gruppen. Dieses Programm soll nun etwas genauer besprochen werden, wobei wir die Details allerdings auf mehrere Übungsaufgaben auslagern.
Die in der Tabelle enthaltene Klassifikation der abelschen Gruppen folgt, wie gesagt, aus dem Hauptsatz 7.4.3.2 über endlich erzeugte abelsche Gruppen bzw. bereits aus Satz 3.3.4.2.

**Proposition 8.2.6.1.** *Die in der Tabelle von Abbildung 8.1 angegebenen abelschen Gruppen sind paarweise nicht isomorph zueinander.*

**UE 437 ▶ Übungsaufgabe 8.2.6.2.** Beweisen Sie Proposition 8.2.6.1. **◀ UE 437**

Klarerweise kann eine derartige Klassifikation für abelsche Gruppen beliebiger Ordnung durchgeführt werden. Behandeln Sie als Test die folgende Frage.

**UE 438 ▶ Übungsaufgabe 8.2.6.3.** Was können Sie über die Anzahl paarweise nichtisomorpher abelscher Gruppen $G$ mit folgender Ordnung $n$ aussagen? **◀ UE 438**

1. $n = p^e$, $p \in \mathbb{P}$, $e \in \mathbb{N}$
2. $n = \prod_{p\in\mathbb{P}} p^{e(p)}$
3. $n \leq 100$
4. $n \leq N$ für wachsendes $N$ (Asymptotik in $N$?)

Wir wenden uns nun den nichtabelschen Gruppen in Abbildung 8.1 zu.

**Proposition 8.2.6.4.** *Die in der Tabelle von Abbildung 8.1 angegebenen nichtabelschen Gruppen $G$ mit $n = |G| \leq 15$ sind paarweise nicht isomorph zueinander.*

**UE 439 ▶ Übungsaufgabe 8.2.6.5.** Begründen Sie Proposition 8.2.6.4. (Offenbar sind lediglich die drei Gruppen $A_4$, $D_6$ und $T$ untereinander zu vergleichen sowie $D_4$ mit $Q_8$.) **◀ UE 439**

**UE 440 ▶ Übungsaufgabe 8.2.6.6.** Zeigen Sie, dass jede Gruppe $G$ mit $|G| = n$ zu einer der in der Tabelle in Abbildung 8.1 angegebenen Gruppen isomorph ist für: **◀ UE 440**

1. $n = 8$
2. $n = 12$.

Damit sind alle Bestandteile für folgenden zusammenfassenden Satz gesammelt.

**Satz 8.2.6.7.** *Jede Gruppe mit einer Ordnung $|G| \leq 15$ ist zu genau einer der Gruppen in der Tabelle aus Abbildung 8.1 isomorph.*

**UE 441 ▶ Übungsaufgabe 8.2.6.8.** Kontrollieren Sie, ob Satz 8.2.6.7 tatsächlich vollständig bewiesen wurde und ergänzen Sie gegebenenfalls fehlende Argumente. **◀ UE 441**

## 8.3 Nilpotenz, Auflösbarkeit und Subnormalreihen

Die Struktur abelscher Gruppen ist, wenig überraschend, wesentlich überschaubarer als die beliebiger Gruppen. Es liegt daher nahe, nichtabelsche Gruppen unter dem Gesichtspunkt zu untersuchen, wie stark sie vom Abelschsein abweichen. Zwei wichtige Konzepte, die das zum Ausdruck bringen, sind Nilpotenz und Auflösbarkeit. Nilpotenz (8.3.1) kommt gewissermaßen von unten, indem sie vom Zentrum einer Gruppe ausgeht, also von der Untergruppe (sogar Normalteiler) jener Elemente, die mit allen anderen vertauschen. Iteration der Zentrumsbildung in einem geeigneten Sinn führt zur sogenannten aufsteigenden Zentralreihe. Bei Auflösbarkeit (8.3.2) geht es, sozusagen von oben kommend, darum, ob eine Gruppe durch Faktorisierung nach einem nicht zu großen Normalteiler abelsch gemacht werden kann. Iteriert man auch diesen Prozess, so stößt man in sehr natürlicher Weise auf die Konzepte Normal-, Subnormal- und Kompositionsreihe (8.3.3), über die der Satz von Jordan-Hölder, fußend auf dem Lemma von Zassenhaus und dem Satz von Schreier, eine sehr starke Aussage macht (8.3.4).

### 8.3.1 Nilpotente Gruppen

Wie bisher bezeichne $Z(G)$ das Zentrum einer Gruppe $G$.

**Definition 8.3.1.1.** Sei $G$ eine Gruppe. Die *aufsteigende Zentralreihe* ist eine Folge von Untergruppen $Z_i = Z_i(G) \leq G$ mit

$$Z_0 \leq Z_1 \leq Z_2 \leq \ldots,$$

die rekursiv definiert sind durch:

$$Z_0 := \{e\},\ Z_{i+1} := \kappa_i^{-1}(Z(G/Z_i))$$

mit den kanonischen Homomorphismen $\kappa_i \colon G \to G/Z_i(G),\ g \mapsto gZ_i$. $G$ heißt *nilpotent*, wenn es ein $n \in \mathbb{N}$ gibt mit $Z_n = G$.

Man beachte, dass wegen $Z(G/Z_i) \lhd G/Z_i$ die Faktorgruppe $\frac{G/Z_i}{Z(G/Z_i)} = (G/Z_i)/Z(G/Z_i)$ gebildet werden kann. Als Urbild des Normalteilers $Z(G/Z_i)$ unter dem kanonischen Homomorphismus $\kappa_i$ ist auch $Z_{i+1}$ Normalteiler von $G$, und nach dem Zweiten Isomorphiesatz 2.3.6.7 gilt $\frac{G/Z_i}{Z(G/Z_i)} \cong G/Z_{i+1}$.

**Satz 8.3.1.2.** *Jede endliche p-Gruppe ist nilpotent.*

**UE 442 ▶ Übungsaufgabe 8.3.1.3.** Folgern Sie Satz 8.3.1.2 aus Korollar 8.1.3.1. **◀ UE 442**

Wenig überraschend und nicht sehr schwer zu beweisen sind folgende Vererbungseigenschaften von Nilpotenz.

**Proposition 8.3.1.4.**

1. *Das direkte Produkt endlich vieler nilpotenter Gruppen ist nilpotent.*
2. *Jede Untergruppe einer nilpotenten Gruppe ist nilpotent.*
3. *Jede Faktorgruppe einer nilpotenten Gruppe ist nilpotent.*

**UE 443 ► Übungsaufgabe 8.3.1.5.** Beweisen Sie Proposition 8.3.1.4. **◄ UE 443**

Unter den endlichen Gruppen lassen sich die nilpotenten auf sehr griffige Weise charakterisieren. Hilfreich ist dabei das folgende Lemma.

**Lemma 8.3.1.6.** *Sei $G$ eine nilpotente Gruppe mit einer echten Untergruppe $H \lneqq G$. Dann ist $H \lneqq N_G(H)$, d.h. $H$ ist eine echte Untergruppe auch seines Normalisators $N_G(H)$.*

*Beweis.* Sei $n$ maximal mit $Z_n \leq H$. Dann gibt es ein $a \in Z_{n+1} \setminus H$. Es genügt zu zeigen, dass so ein $a$ auch im Normalisator $N_G(H)$ liegt. Weil $a$ in $Z_{n+1} = \kappa_n^{-1}(Z(G/Z_n))$ liegt, vertauscht es modulo $Z_n$ mit allen $g \in G$. Insbesondere bedeutet das für ein beliebiges $h \in H$, dass $Z_n ah = (Z_n a)(Z_n h) = (Z_n h)(Z_n a) = Z_n ha \in G/Z_n$. Folglich gibt es ein $h' \in Z_n \leq H$, so dass $ah = h'ha$ bzw. $aha^{-1} = h'h \in H$, also tatsächlich $a \in N_G(H)$. □

Damit können wir die angekündigte Charakterisierung nilpotenter Gruppen beweisen.

**Satz 8.3.1.7.** *Sei $G$ eine endliche Gruppe. Dann sind die folgenden Aussagen äquivalent.*

1. *$G$ ist nilpotent.*
2. *Zu jedem $p \in \mathbb{P}$ hat $G$ genau eine $p$-Sylowgruppe.*
3. *$G = \prod_{p\in\mathbb{P}} G_p$ mit einer $p$-Sylow-Gruppe $G_p$ von $G$ zu jedem $p \in \mathbb{P}$.*

*Beweis.* $1 \Rightarrow 2$ : Sei $G$ nilpotent und $G_p \lneqq G$ eine $p$-Sylow-Gruppe von $G$. Laut Korollar 8.1.4.6 gilt $H := N_G(G_p) = N_G(N_G(G_p))$. Nach Lemma 8.3.1.6 ist das nur für $H = G$ möglich, also ist

$$G_p \lhd N_G(G_p) = N_G(N_G(G_p)) = H = G.$$

Daher ist $G_p$ wegen Korollar 8.1.4.4 die einzige $p$-Sylowgruppe von $G$.
$2 \Rightarrow 3$ : Sei $|G| = \prod_{p\in\mathbb{P}} p^{n_p}$ (nur endlich viele $n_p$ sind von 0 verschieden), und sei für jedes $p \in \mathbb{P}$ die (laut Voraussetzung eindeutige) $p$-Sylow-Gruppe von $G$ mit $G_p$ bezeichnet. Nach Korollar 8.1.4.4 sind alle $G_p$ Normalteiler. Je zwei verschiedene $G_p$ haben nur $e$ gemeinsam. Das Komplexprodukt von Normalteilern ist wieder ein Normalteiler (siehe 3.2.2.8). Nach Satz **??** bilden die $G_p$ daher ein direktes Produkt $P := \prod_{p\in\mathbb{P}} G_p \leq G$. Wegen $G_p \leq P \leq G$, also

$$|G_p| = p^n \mid |P| \mid |G| = \prod_{p\in\mathbb{P}} p^{n_p}$$

für alle $p \in \mathbb{P}$ muss $P$ bereits ganz $G$ sein.
$3 \Rightarrow 1$ : Nach Satz 8.3.1.2 sind die $p$-Sylow-Gruppen $G_p$ als $p$-Gruppen nilpotent, und nach Proposition 8.3.1.4 ist es auch ihr de facto nur endliches direktes Produkt $G$. □

### 8.3.2 Auflösbare Gruppen

Zwei Gruppenelemente $a, b$ vertauschen genau dann, wenn $ab = ba$ oder, äquivalent, wenn $aba^{-1}b^{-1} = e$ gilt. Von dieser Beobachtung gehen wir aus, wenn wir die Frage untersuchen, wie ein Normalteiler $N \lhd G$ beschaffen sein muss, damit $G/N$ abelsch ist.

**Definition 8.3.2.1.** Für $a, b \in G$ heißt das Element $[a, b] := aba^{-1}b^{-1}$ *Kommutator* von $a$ und $b$. Die von allen Kommutatoren erzeugte Gruppe $G' := \langle \{[a, b] : \ a, b \in G\} \rangle$ heißt die *Ableitung Kommutatorgruppe* von $G$.
Die (höheren) *abgeleiteten Untergruppen*

$$G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \ldots$$

sind rekursiv definiert durch:

$$G^{(0)} := G, \ G^{(i+1)} := (G^{(i)})'.$$

$G$ heißt *auflösbar*, wenn es ein $n \in \mathbb{N}$ gibt mit $G^{(n)} = \{e\}$.

Jeder Endomorphismus $f\colon G \to G$ erfüllt $f([a, b]) = [f(a), f(b)]$, bildet also Kommutatoren auf Kommutatoren ab. Entsprechendes gilt für die erzeugten Untergruppen, also $f(G') \leq G'$. Insbesondere gilt diese Beziehung, wenn $f$ ein innerer Automorphismus von $G$ ist, also $G' \lhd G$.
Für einen Homomorphismus $f\colon G \to H$ in eine abelsche Gruppe $H$ liegt wegen $f([a, b]) = f(a)f(b)f(a)^{-1}f(b)^{-1} = e$ jeder Kommutator im Kern, also ist ganz $G'$ im Kern von $f$ enthalten. Sei $\kappa\colon G \to G/G'$ die kanonische Abbildung. Der Kern von $\kappa$ ist genau $G'$. Folglich gibt es nach dem Homomorphiesatz genau einen Homomorphismus $g\colon G/G' \to H$ mit $f = g \circ \kappa$, nämlich $gG' \mapsto f(g)$. Ist speziell $N \lhd G$ und $f\colon G \to G/N$, $g \mapsto gN$, der kanonische Homomorphismus, lesen wir insbesondere ab:

**Proposition 8.3.2.2.** *Für einen Normalteiler $N \lhd G$ sind äquivalent:*

1. *$G/N$ ist abelsch.*
2. *$G' \subseteq N$.*

Auflösbarkeit vererbt sich in ähnlicher Weise wie Nilpotenz:

**Proposition 8.3.2.3.**

1. *Das direkte Produkt endlich vieler auflösbarer Gruppen ist auflösbar.*
2. *Jede Untergruppe einer auflösbaren Gruppe ist auflösbar.*
3. *Jede Faktorgruppe einer auflösbaren Gruppe ist auflösbar.*
4. *Ist $N \lhd G$ und sind $N$ und $G/N$ auflösbar, dann ist auch $G$ auflösbar.*

**UE 444** ► **Übungsaufgabe 8.3.2.4.** Beweisen Sie Proposition 8.3.2.3. ◄ **UE 444**

Von großem Interesse ist der folgende Satz:

**Satz 8.3.2.5.** *Jede nilpotente Gruppe ist auflösbar.*

*Beweis.* Ist $G$ nilpotent, so gibt es ein $n \in \mathbb{N}$ mit $Z_n = G$. Wir zeigen mittels Induktion nach $i$, dass $G^{(i)} \leq Z_{n-i}$ gilt, was für $i = n$ die Behauptung beweist.
Für $i = 0$ ist die Behauptung $G^{(0)} \leq Z_n = G$ trivialerweise wahr. Für den Schritt von $i$ auf $i+1$ dürfen wir von der Induktionsannahme $G^{(i)} \leq Z_{n-i}$ ausgehen. Laut Definition der aufsteigenden Zentralreihe ist $Z_{n-i}/Z_{n-(i+1)}$ abelsch und daher nach Proposition 8.3.2.2 $Z'_{n-i} \leq Z_{n-(i+1)}$. Daraus folgt aber bereits die Induktionsbehauptung $G^{(i+1)} = (G^{(i)})' \leq Z'_{n-i} \leq Z_{n-(i+1)}$. □

**UE 445** ► **Übungsaufgabe 8.3.2.6.** Man untersuche interessante Beispiele (endlicher und unendlicher) nichtabelscher Gruppen auf Nilpotenz und Auflösbarkeit, insbesondere alle Gruppen der Ordnung $\leq 15$ oder Gruppen linearer Transformationen von Vektorräumen. ◄ **UE 445**

### 8.3.3 Subnormalreihen

**Definition 8.3.3.1.** Sei $G$ eine Gruppe. Eine absteigende Folge

$$G = G_0 \geq G_1 \geq \ldots \geq G_n = \{e\}$$

von Untergruppen heißt *Subnormalreihe*, sofern $G_{i+1} \lhd G_i$ für $i = 1, \ldots, n-1$ gilt. Die $F_i := G_i/G_{i+1}$ heißen die *Faktoren* der Subnormalreihe. Die Anzahl der $F_i$ mit $|F_i| > 1$ heißt die *Länge* der Subnormalreihe.
Ist $G_{i+1} \lhd N \lhd G_i$, so nennt man

$$G = G_0 \geq G_1 \geq \ldots \geq G_i \geq N \geq G_{i+1} \geq \ldots \geq G_n = \{e\}$$

eine *Einschrittverfeinerung* der Subnormalreihe. Iteration von Einschrittverfeinerungen liefert beliebige *Verfeinerungen* der Subnormalreihe. Die Verfeinerung heißt *echt*, wenn sich durch sie die Länge der Subnormalreihe vergrößert (wenn also $G_{i+1} \neq N \neq G_i$).
Sind alle Faktoren einfach und $\ncong \{e\}$ sowie $G_n = \{e\}$, so spricht man von einer *Kompositionsreihe*.
Ist $G_i \lhd G$ für alle $i = 1, \ldots, n$, sind also die $G_i$ Normalteiler sogar in ganz $G$, so nennt man eine Subnormalreihe auch eine *Normalreihe*.
Eine Subnormalreihe mit $G_n = \{e\}$ heißt *auflösbar*, wenn alle Faktoren abelsch sind.
Zwei Subnormalreihen heißen *äquivalent*, wenn es eine Bijektion zwischen den Faktoren gibt, wobei je zwei Partner zueinander isomorph sind.

Zur Einübung der Begriffe eine leichte Übungsaufgabe:

**UE 446 ► Übungsaufgabe 8.3.3.2.** Begründen Sie: **◄ UE 446**

(i) Sei $N$ ein echter Normalteiler der Gruppe $G$. Dann ist $G/N$ genau dann einfach, wenn $N$ als echter Normalteiler maximal ist.

(ii) Jede endliche Gruppe besitzt eine Kompositionsreihe.

(iii) Jede Verfeinerung einer auflösbaren Subnormalreihe ist auflösbar.

(iv) Eine Subnormalreihe mit Faktoren $|F_i| > 1$ ist genau dann Kompositionsreihe, wenn keine echte Verfeinerung existiert.

(v) Eine Gruppe ist genau dann auflösbar, wenn sie eine auflösbare Subnormalreihe besitzt. Hinweis: Zeigen Sie zu einer vorgegebenen auflösbaren Subnormalreihe $G = G_0 \geq G_1 \geq \ldots \geq G_n = \{e\}$ mittels Induktion $G_i$ die Inklusion $G^{(i)} \leq G_i$.

(vi) Eine endliche Gruppe ist genau dann auflösbar, wenn sie eine Kompositionsreihe mit Faktoren $F_i \cong C_{p_i}$, $p_i \in \mathbb{P}$, besitzt.

Hinweis: Oft sind Isomorphiesätze nützlich.

### 8.3.4 Die Sätze von Zassenhaus, Schreier und Jordan-Hölder

Das Hauptergebnis dieses Unterabschnitts ist der Satz 8.3.4.3 von Jordan-Hölder, wonach je zwei Kompositionsreihen einer Gruppe $G$ äquivalent sind. Somit stellt, sofern es überhaupt eine Kompositionsreihe von $G$ gibt, die (ungeordnete) Familie der Faktoren eine Isomorphieinvariante für $G$ dar.
Der Grundgedanke des Beweises besteht darin, zu je zwei Subnormalreihen Verfeinerungen zu finden, die äquivalent zueinander sind. Ist dies immer möglich – und das ist der Inhalt des Satzes 8.3.4.2 von Schreier –, so folgt der Satz von Jordan-Hölder sehr schnell. Für den Beweis des Satzes von Schreier besteht die Aufgabe also darin, zwei gegebene Subnormalreihen

$$\text{(I)} \quad G = G_0 \geq G_1 \geq \ldots \geq G_n = \{e\}$$

und

$$\text{(II)} \quad G = H_0 \geq H_1 \geq \ldots \geq H_m = \{e\}$$

von $G$ geeignet zu verfeinern. Das gelingt, indem man zwischen aufeinanderfolgende Glieder $G_i \geq G_{i+1}$ in (I) jeweils eine die zweite Subnormalreihe (II) imitierende Folge von Gruppen $G(i,j)$ dazwischen schaltet, so dass

$$G_i = G(i,0) \geq G(i,1) \geq \ldots \geq G(i,j) \geq \ldots \geq G(i,m{-}1) \geq G(i,m) = G(i{+}1,0) = G_{i+1},$$

und vice versa mit vertauschten Rollen von (I) und (II). Naheliegenderweise soll $G(i,j)$ (monoton) von $H_j$ abhängen. Rein verbandstheoretisch betrachtet bieten sich, um die Nebenbedingung $G_i \geq G(i,j) \geq G_{i+1}$ zu garantieren, an dieser Stelle zwei Definitionen für $G(i,j)$ an, nämlich $G_i \wedge (G_{i+1} \vee H_j)$ und $G_{i+1} \vee (G_i \wedge H_j)$. Die erste scheidet schnell aus, weil die von $G_{i+1}$ und $H_j$ erzeugte Untergruppe $G_{i+1} \vee H_j$ im allgemeinen Fall

schwer zu handhaben ist. Im Gegensatz dazu lässt sich mit der Definition $G(i,j) := G_{i+1} \vee (G_i \wedge H_j) = G_{i+1}(G_i \cap H_j)$ (hier fließt $G_{i+1} \lhd G_i$ ein) bestens weiterarbeiten. Es zeigt sich nämlich $G(i,j+1) \lhd G(i,j)$, außerdem natürlich $G(i,m) = G(i+1,0)$. Also liegt eine Subnormalreihe mit Länge $\leq nm$ vor. Symmetrisches gilt, wenn man $H(i,j) := H_{j+1}(H_j \cap G_i)$ setzt.
Die beiden auf diese Weise erhaltenen Subnormalreihen sind äquivalent, sofern

$$G(i,j)/G(i,j+1) =: \frac{G(i,j)}{G(i,j+1)} \cong \frac{H(i,j)}{H(i+1,j)} := H(i,j)/H(i+1,j)$$

für $0 \leq i < n$ und $0 \leq j < m$ gezeigt werden kann. Denn dadurch wird offenbar eine bijektive Beziehung zwischen paarweise isomorphen Faktoren hergestellt. Der Nachweis dieser Isomorphie wiederum gelingt, indem man ein symmetrisches Zwischenglied identifiziert, welches zu beiden Gruppen isomorph ist. Dieses Zwischenglied ist die Gruppe

$$\frac{G_i \cap H_j}{(G_{i+1} \cap H_j)(G_i \cap H_{j+1})}.$$

Genau diese Situation wird im nun folgenden sogenannten *Lemma von Zassenhaus*, genannt auch *Schmetterlingslemma* (vgl. Abbildung 8.2), behandelt, wobei $G_i = A$, $G_{i+1} = A^*$, $H_j = B$ und $H_{j+1} = B^*$ zu setzen ist.

**Lemma 8.3.4.1** (Zassenhaus, vgl. Abbildung 8.2)**.** *Sei $G$ eine Gruppe, $A^* \lhd A \leq G$ und $B^* \lhd B \leq G$. Dann folgt*

*(a)* $A^*(A \cap B^*) \lhd A^*(A \cap B)$,

*(b)* $B^*(A^* \cap B) \lhd B^*(A \cap B)$ *und*

*(c)* $\frac{A^*(A\cap B)}{A^*(A\cap B^*)} \cong \frac{B^*(A\cap B)}{B^*(A^*\cap B)}$.

*Beweis.* Wegen $B^* \lhd B$ ist auch $A \cap B^* = (A \cap B) \cap B^* \lhd A \cap B$. Analog folgt $A^* \cap B \lhd A \cap B$. Daraus erhält man unmittelbar $D := (A^* \cap B)(A \cap B^*) \lhd A \cap B$. Außerdem gilt $A^*(A \cap B) \leq A$ und $B^*(A \cap B) \leq B$. Wir werden einen surjektiven Homomorphismus $f\colon A^*(A \cap B) \to (A \cap B)/D$ mit $\ker f = A^*(A \cap B^*)$ definieren. Dann folgt nämlich $A^*(A \cap B^*) \lhd A^*(A \cap B)$, also Aussage (a), analog (b). Nach dem Homomorphiesatz gilt dann aber auch $\frac{A^*(A\cap B)}{A^*(A\cap B^*)} \cong \frac{A\cap B}{D}$, womit, wieder aus Symmetriegründen, auch $\frac{A\cap B}{D} \cong \frac{B^*(A\cap B)}{B^*(A^*\cap B)}$ und somit die Behauptung (c) folgt.
Wir definieren $f$ folgendermaßen: Für $a \in A^*, c \in A \cap B$ sei

$$f(ac) := Dc \in (A \cap B)/D.$$

Damit ist $f$ wohldefiniert, denn sind $a_1, a_2 \in A^*, c_1, c_2 \in A \cap B$ mit $a_1 c_1 = a_2 c_2$, dann ist

$$a_2^{-1} a_1 = c_2 c_1^{-1} \in A^* \cap (A \cap B) = A^* \cap B \subseteq D,$$

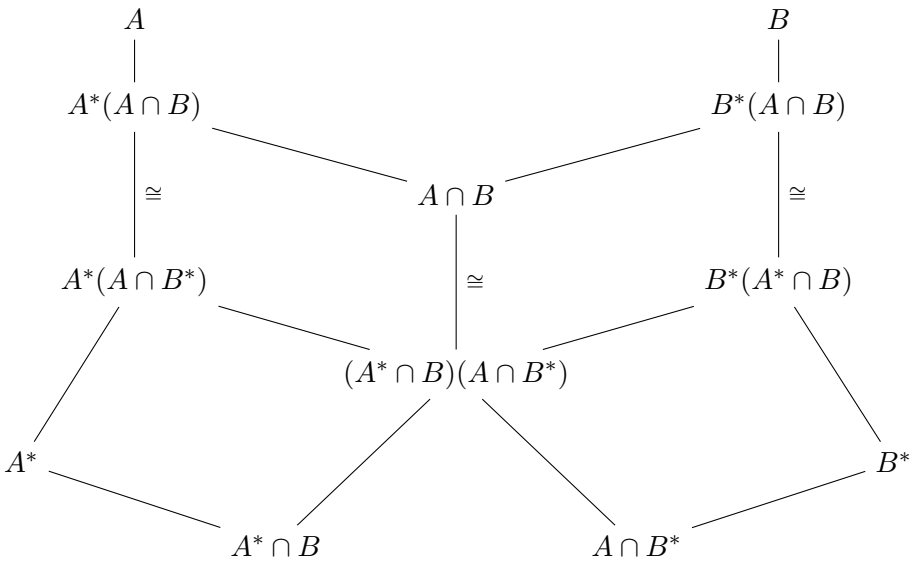



Abbildung 8.2: „Schmetterlingslemma“

also $Dc_1 = Dc_2$. Offensichtlich ist $f$ surjektiv. Wir zeigen nun die Homomorphiebedingung: Wegen $A^* \lhd A$ gibt es für beliebige $a_1, a_2 \in A^*$ und $c_1, c_2 \in A \cap B$ ein $a_3 \in A^*$ mit $c_1 a_2 = a_3 c_1$. Daraus folgt

$$f((a_1c_1)(a_2c_2)) = f(a_1a_3c_1c_2) = Dc_1c_2 = Dc_1Dc_2 = f(a_1c_1)f(a_2c_2).$$

Also ist $f$ ein Homomorphismus.
Wir müssen nur noch zeigen, dass auch $\ker f = A^*(A \cap B^*)$ gilt. Für $a \in A^*$ und $c \in A \cap B$ ist $ac \in \ker f$ genau dann, wenn $c \in D$. Für den Beweis der ersten Inklusion $\ker f \subseteq A^*(A \cap B^*)$ nehmen wir also $a \in A$ und $c \in A \cap B$ mit $ac \in \ker f$, d.h. $c \in D$ an. Nach Definition von $D$ gibt es dann Elemente $a_1 \in A^* \cap B$ und $c_1 \in A \cap B^*$ mit $c = a_1c_1$, folglich liegt $ac = (aa_1)c_1$ in $A^*(A \cap B^*)$. Für die umgekehrte Inklusion $A^*(A \cap B^*) \subseteq \ker f$ seien nun Elemente $a \in A^*$ und $c \in A \cap B^*$ gegeben. Dann ist $f(ac) = Dc = (A^* \cap B)(A \cap B^*)c = (A^* \cap B)(A \cap B^*) = D$, das neutrale Element in $(A \cap B)/D$, also $ac \in \ker f$. □

In der oben (vor Lemma 8.3.4.1) beschriebenen Weise folgt hieraus der Satz von Schreier.

**Satz 8.3.4.2** (Schreier)**.** *Je zwei Subnormalreihen ein und derselben Gruppe $G$ haben äquivalente Verfeinerungen.*

Da zwei Kompositionsreihen nur sich selbst als Verfeinerung besitzen, ist damit auch unser Hauptresultat bewiesen:

**Satz 8.3.4.3** (Jordan-Hölder)**.** *Je zwei Kompositionsreihen ein und derselben Gruppe $G$ sind äquivalent.*

Für die Galoistheorie von Bedeutung ist die hieraus folgende Nichtauflösbarkeit der symmetrischen Gruppen großer Ordnung:

**Korollar 8.3.4.4.** *Die symmetrische Gruppe $S_n$ ist für $n < 5$ auflösbar, sonst nicht.*

**UE 447 ▶ Übungsaufgabe 8.3.4.5.** Beweisen Sie Korollar 8.3.4.4. Hinweis: Satz 8.2.3.2. **◀ UE 447**

Eines der spektakulärsten Resultate über die Auflösbarkeit von Gruppen ist der *Satz von Feit-Thompson*: Jede Gruppe ungerader Ordnung ist auflösbar. Die Aussage wurde schon im Jahr 1911 vom bedeutenden Gruppentheoretiker William Burnside (1852-1927) vermutet, aber erst im Jahr 1963 von Walter Feit (1930-2004) und John Griggs Thompson (geb. 1932) in einer 250 Seiten langen Arbeit bewiesen. Vielleicht erweisen sich die folgenden Übungsaufgaben als leichter:

**UE 448 ▶ Übungsaufgabe 8.3.4.6.** Zeigen Sie: **◀ UE 448**

(1) Eine abelsche Gruppe besitzt genau dann eine endliche Kompositionsreihe, wenn sie endlich ist.

(2) Eine auflösbare Gruppe mit einer Kompositionsreihe ist endlich.

**UE 449 ▶ Übungsaufgabe 8.3.4.7.** Finden Sie (wenn möglich alle) Kompositionsreihen verschiedener Gruppen $G$: **◀ UE 449**

(1) $G$ endlich und abelsch mit vorgegebener Ordnung $n = |G| = \prod_{p\in\mathbb{P}} p^{e(p)}$

(2) $G$ nichtabelsch mit $|G| \leq 15$

(3) $G = S_4$

(4) $G = S_n$ mit $n \geq 5$

(5) Ein unendliches $G$ Ihrer Wahl mit endlicher Kompositionsreihe

**UE 450 ▶ Übungsaufgabe 8.3.4.8.** Zeigen Sie: Ist $G$ eine endliche nilpotente Gruppe. Dann gibt es zu jedem Teiler $t$ von $n := |G|$ eine Untergruppe $U \leq G$ mit $|U| = t$. Hinweis: Betrachten Sie eine Kompositionsreihe von $G$. **◀ UE 450**

## 8.4 Konstruktionen zur Erweiterung von Gruppen

Der Satz von Jordan-Hölder (8.3.4.3) besagt, dass jede Gruppe $G$, die eine Kompositionsreihe $\{e\} = G_0 \leq G_1 \leq \ldots \leq G_n = G$ besitzt, eine bis auf Isomorphie und Reihenfolge eindeutige Familie von einfachen Faktoren $F_i \cong G_i/G_{i-1}$, $i = 1, \ldots, n$, bestimmt. Umgekehrt kann man fragen, welche Struktur für $G$ möglich ist, wenn man die Faktoren $F_i$ vorgibt. Sicher ist das direkte Produkt $P = \prod_{i=1}^{n} F_i$ eine Möglichkeit. Im Allgemeinen

gibt es aber viele andere, zu $P$ nicht isomorphe Gruppen $G$ mit Faktoren, die zu den $F_i$ isomorph sind.
Schon der Fall mit $n = 2$ und vorgegebenem $F_1 \cong G_1 = N \lhd G$ und $F_2 = K \cong G/N$ ist von Interesse und keineswegs trivial. Man spricht von Erweiterungen von $N$ mit $K$ (8.4.1). Einen wichtigen Spezialfall davon bilden semidirekte Produkte (8.4.2). Er ist dadurch gekennzeichnet, dass der Faktor $K$ auch als Untergruppe in $G$ realisiert werden kann, so dass die Einbettung von $K$ in $G$ mit der Faktorisierung nach $N$ in einem natürlichen Sinn verträglich ist. In Analogie zu direkten Produkten, die den einfachsten Spezialfall darstellen und wo man gleichfalls innere und äußere unterscheidet, spricht man in dieser Situation auch von einem *inneren semidirekten Produkt*. Dabei erweist sich die Aktion von $K$ durch Konjugation auf $N$ vermittels innerer Automorphismen als interessant. Wenn man nämlich umgekehrt diese drei Daten – Struktur von $N$, Struktur von $K$ und Aktion von $K$ mittels Automorphismen auf $N$ – vorgibt, kann daraus $G$ als sogenanntes *äußeres semidirektes Produkt* (8.4.2) rekonstruiert werden. Universell nicht nur für sämtliche Aktionen von $K$ auf $N$, sondern überhaupt für alle Erweiterungen von $N$ mit $K$ ist schließlich das *Kranzprodukt* (8.4.3), das selbst wieder in geeigneter Weise als semidirektes Produkt, allerdings größerer Gruppen, definiert ist.

### 8.4.1 Allgemeine Gruppenerweiterungen

Die Ausgangssituation lässt sich durch eine *kurzexakte Sequenz* von (diesmal i.A. nichtkommutativen) Gruppen beschreiben:

$$1 \to N \xrightarrow{\iota} G \xrightarrow{\kappa} K \to 1$$

Am Anfang und Ende der Sequenz steht jeweils die mit 1 (bei additiver Notation mit 0) bezeichnete einelementige Gruppe. Zur Erinnerung: Wie schon bei Sequenzen von Moduln bedeutet Exaktheit der Sequenz in einem bestimmten Glied (nicht am Anfang oder Ende der Sequenz), dass das Bild der Abbildung, die durch den Pfeil von links symbolisiert wird, übereinstimmt mit dem Kern der Abbildung, die zum Pfeil nach rechts gehört. Konkret im Beispiel: Bei $N$ bedeutet die Exaktheit die Injektivität von $\iota$, bei $K$ die Surjektivität von $\kappa$ und bei $G$, dass das Bild von $\iota$ gerade mit dem Kern von $\kappa$ übereinstimmt. In diesem Fall ist nach dem Homomorphiesatz $\iota(N) \lhd G$ und $K \cong G/\iota(N)$. Ist umgekehrt ein Normalteiler $N \lhd G$ einer Gruppe vorgegeben, so können wir $K := G/N$ setzen, und es liegt eine kurzexakte Sequenz obiger Gestalt mit der Einbettung $\iota\colon N \to G$, $n \mapsto n$ und der kanonischen Abbildung $\kappa\colon G \to K = G/N$, $g \mapsto gN$ vor.
Wir werden uns beispielsweise für die Frage interessieren, inwiefern sich $G$ mittels $N$ und $K$ beschreiben lässt, und fassen die allgemeine Situation in folgende Definition.

**Definition 8.4.1.1.** $\mathcal{E} = (G, \iota, \kappa)$ heißt *Erweiterung* der Gruppe $N$ durch die Gruppe $K$[1], wenn $\iota\colon N \to G$ injektiv, $\kappa\colon G \to K$ surjektiv und $\iota(N) = \ker \kappa$ ist, d.h. wenn die Sequenz

$$1 \to N \xrightarrow{\iota} G \xrightarrow{\kappa} K \to 1$$

[1] In der englischen Version von Bourbaki wird $G$ (mit vertauschten Präpositionen) *extension of $K$ by $N$* genannt.

(kurz)exakt ist.

Dabei ist die Struktur von $G$ durch jene von $N$ und $K$ allein nicht eindeutig bestimmt. Ein einfaches Beispiel dafür ist gegeben durch die Gruppen $G_1 := C_6$ und $G_2 := S_3$. Beide haben einen Normalteiler $N \cong C_3$ mit Quotienten $K \cong C_2$. Somit hat die kurzexakte Sequenz

$$1 \to C_3 \xrightarrow{\iota} G \xrightarrow{\kappa} C_2 \to 1$$

für $G$ die beiden zueinander nicht isomorphen Lösungen $G = C_6$ und $G = S_3$.
Will man $G$ aus $N$ und $K$ rekonstruieren, reichen die Isomorphietypen von $N$ und $K$ alleine also nicht aus. Man braucht zusätzliche Information darüber, wie $K$ und $N$ in $G$ zusammenwirken. Das lässt sich wie folgt besser verstehen.
Wie auch schon in der Theorie der Moduln kann man die Situation näher untersuchen, wenn es $\rho$ und/oder $\sigma$ der Form

$$N \underset{\rho}{\overset{\iota}{\rightleftarrows}} G \underset{\sigma}{\overset{\kappa}{\rightleftarrows}} K$$

gibt, wobei $\rho\colon G \to N$ die Relation $\rho \circ \iota = \mathrm{id}_N$ und $\sigma\colon K \to G$ die Relation $\kappa \circ \sigma = \mathrm{id}_K$ erfüllt. Wieder nennt man dann $\rho$ eine *Retraktion* und $\sigma$ eine *Sektion* von $\mathcal{E}$.

**Beispiel 8.4.1.2.** Die *triviale Erweiterung*: $G = N \times K$, $\iota(n) = (n, 1)$, $\kappa(n, k) = k$. Hier gibt es die Sektion $\sigma : k \mapsto (1, k)$ und die Retraktion $\rho : (n, k) \mapsto n$.

Das einfache Beispiel der kurzexakten Sequenz

$$0 \to 2\mathbb{Z} \xrightarrow{\iota} \mathbb{Z} \xrightarrow{\kappa} \mathbb{Z}/(2\mathbb{Z}) \to 0$$

zeigt, dass Sektionen und Retraktionen nicht immer existieren. Von besonderem Interesse ist der Fall, wo es eine Sektion $\sigma$ gibt. Er führt uns zu den semidirekten Produkten.

## 8.4.2 Semidirekte Produkte

Wir gehen davon aus, dass für die kurzexakte Sequenz

$$1 \longrightarrow N \xrightarrow{\iota} G \underset{\sigma}{\overset{\kappa}{\rightleftarrows}} K \longrightarrow 1$$

eine Sektion $\sigma$ vorliegt, d.h. ein Homomorphismus $\sigma\colon K \to G$ mit $\kappa \circ \sigma = \mathrm{id}_K$. So ein $\sigma$ ist notwendig injektiv, also können wir $K$ o.B.d.A. mit $\sigma(K) \leq G$ in $G$ identifizieren, d.h. als Untergruppe von $G$ auffassen. Aus der Exaktheit der Sequenz folgt leicht sowohl $N \cap K = \{e\}$ als auch $NK = G$.

**Definition 8.4.2.1.** Die Gruppe $G$ heißt *inneres semidirektes Produkt* von $N \lhd G$ und $K \leq G$, sofern $N \cap K = 1$ und $NK = G$.

Diese Überlegungen lassen sich umkehren, so dass man zusammenfassend erhält:

**Proposition 8.4.2.2.** *Sei $G$ eine Gruppe, $N \lhd G$ und $K \leq G$, $\sigma : K \to G$ die Inklusionsabbildung. Dann sind folgende Aussagen äquivalent:*

1. *$G$ ist das innere semidirekte Produkt von $N \lhd G$ und $K \leq G$, d.h. es gilt $N \cap K = 1$ und $NK = G$.*
2. *Bezeichne $\kappa\colon G \to G/N$ die kanonische Abbildung. Dann ist $\kappa \circ \sigma\colon K \to G/N$ ein Isomorphismus.*
3. *Für die Inklusionsabbildung $\iota : N \to G$ gibt es ein $\kappa$, so dass eine kurzexakte Sequenz vorliegt, für die $\sigma$ eine Sektion ist:*

$$1 \longrightarrow N \xrightarrow{\iota} G \underset{\sigma}{\overset{\kappa}{\rightleftarrows}} K \longrightarrow 1$$

*Insbesondere entspricht jedes semidirekte Produkt einer Gruppenerweiterung.*

Man beachte die partielle Analogie zu Satz 7.2.3.8 über das Zerfallen von Sequenzen von Moduln.

**UE 451 ► Übungsaufgabe 8.4.2.3.** 1. Beweisen Sie Proposition 8.4.2.2 in allen Details. **◄ UE 451**

2. Zeigen Sie anhand eines Beispiels, dass in der dritten äquivalenten Bedingung in Proposition 8.4.2.2 nicht auf die Sektion $\sigma$ verzichtet werden kann.

Das einfachste Beispiel eines semidirekten Produktes liegt offenbar vor, wenn $G = N \times K$ das direkte Produkt zweier Untergruppen ist, die dann notwendig beide sogar Normalteiler sind. Denkt man sich $N$ und $K$ vorgegeben, so liefert die Konstruktion des äußeren direkten Produktes eine Gruppe $G$, in die $N$ und $K$ in natürlicher Weise eingebettet sind. Klarerweise ist jedes direkte Produkt auch ein semidirektes. Für ein semidirektes Produkt bestehen aber noch andere Möglichkeiten, weil ja nur $N$, aber nicht unbedingt $K$ Normalteiler sein muss.
Zum besseren Verständnis des Beziehung von $N$ und $K$ gehen wir von der Situation beim inneren semidirekten Produkt aus. Sei also $N \lhd G$, $K \leq G$ mit $N \cap K = \{e\}$ und $NK = G$. Dann besitzt jedes $g \in G$ eine eindeutige Darstellung als $g = nk$ mit $n \in N$ und $k \in K$. Außerdem sei $\tau\colon K \to \mathrm{Aut}(N)$ mit $\tau(k) = \alpha_k$, wobei $\alpha_k(n) = knk^{-1}$, d.h. $K$ agiert vermittels Konjugation auf $N$. Es gilt $\alpha_{k_1} \circ \alpha_{k_2} = \alpha_{k_1 k_2}$, d.h. $\tau$ ist Homomorphismus. Außerdem gilt

$$(n_1k_1)(n_2k_2) = n_1k_1n_2k_1^{-1}k_1k_2 = n_1\alpha_{k_1}(n_2)k_1k_2.$$

Wir gehen nun umgekehrt von folgender Situation aus:
Vorgegeben seien $N$ und $K$ sowie ein Homomorphismus $\tau\colon K \to \mathrm{Aut}(N)$, d.h. eine Aktion $\alpha : (k, n) \mapsto \tau(k)(n)$ von $K$ auf $N$ vermittels Automorphismen. Wir schreiben

$${}^k n := \tau(k)(n)$$

und definieren auf der Trägermenge $G := N \times K$ die Operation $\cdot_\tau$ durch

$$(n_1, k_1) \cdot_\tau (n_2, k_2) := (n_1 \, {}^{k_1}n_2, k_1 k_2).$$

Die Operation $\cdot_\tau$ ist eine Gruppenoperation auf $G$ mit neutralem Element $e_G = (e_N, e_K)$ und Inversen $(n, k)^{-1} = ({}^{k^{-1}}n^{-1}, k^{-1})$.
Diese Gruppe wird *(äußeres) semidirektes Produkt* von $N$ und $K$ genannt, i.Z. $G = N \rtimes K$ oder (präziser, weil dadurch die Abhängigkeit von $\tau$ zum Ausdruck kommt, aber weniger verbreitet) $N \rtimes_\tau K$.
Offenbar ist

$$1 \to N \xrightarrow{\iota} G = N \rtimes K \xrightarrow{\kappa} K \to 1$$

mit $\iota(n) = (n, e_K)$ und $\kappa(n, k) = k$ kurzexakt, also ist $G = N \rtimes K$ eine Erweiterung von $N$ durch $K$. Außerdem gilt

$$(e_N, k) \cdot_\tau (n, e_K) \cdot_\tau (e_N, k)^{-1} = ({}^k n, k) \cdot_\tau (e_N, k^{-1}) = ({}^k n, e_K),$$

d.h. $K$ agiert auf $N$ via Konjugation, wie beim inneren semidirekten Produkt weiter oben beschrieben.
Wir haben bereits in Proposition 8.4.2.2 gesehen, dass jedes semidirekte Produkt einer Gruppenerweiterung entspricht. Die Umkehrung gilt nicht. Das ergibt sich aus dem letzten Teil der folgenden Übungsaufgabe.

**UE 452 ► Übungsaufgabe 8.4.2.4.** (1) Ergänzen Sie bei der Konstruktion des äußeren semidirekten Produktes die nicht explizit ausgeführten Rechnungen. **◄ UE 452**

(2) Sei die Gruppe $G$ inneres semidirektes Produkt von $N \lhd G$ und $K \leq G$. Zeigen Sie, dass $G$ isomorph zum äußeren direkten Produkt $G = N \rtimes K$ (bezüglich der Aktion von $K$ auf $N$ vermittels Konjugation) ist.

(3) Zeigen Sie umgekehrt explizit, dass sich jedes äußere semidirekte Produkt auch als inneres deuten lässt.

(4) Geben Sie ein Beispiel einer Gruppenerweiterung, die kein semidirektes Produkt ist.

Bildet $\tau$ immer auf $\mathrm{id}_N$ ab (d.h.: ist $\tau$ die triviale Aktion von $K$ auf $N$), so erhält man das direkte Produkt mit $(n_1 k_1)(n_2 k_2) = n_1 n_2 k_1 k_2$. Die Rolle der trivialen Aktion $\tau$ wird noch deutlicher durch folgende, nicht schwer zu beweisende Aussage:

**Proposition 8.4.2.5.** *Sei $\tau$ eine Aktion der Gruppe $K$ vermittels Automorphismen auf der Gruppe $N$. Dann ist das semidirekte Produkt $G := N \rtimes_\tau K$ genau dann abelsch, wenn folgende drei Bedingungen erfüllt sind:*

1. *Die Gruppe $N$ ist abelsch.*
2. *Die Gruppe $K$ ist abelsch.*
3. *Die Aktion $\tau$ ist trivial, d.h. $\tau(k) = \mathrm{id}_N$ für alle $k \in K$.*

**UE 453** ▶ **Übungsaufgabe 8.4.2.6.** Beweisen Sie Proposition 8.4.2.5. ◀ **UE 453**

Die Abhängigkeit der Konstruktion des semidirekten Produktes $G := N \rtimes_\tau K$ von der Aktion $\tau$ schlägt sich auch in der Struktur der resultierenden Gruppe $G$ nieder. Zum Beispiel lassen sich sowohl $C_6$ als auch $S_3$ als semidirektes Produkt $C_3 \rtimes C_2$ erhalten.

**UE 454** ▶ **Übungsaufgabe 8.4.2.7.** Führen Sie das aus, indem Sie die entsprechenden Aktionen von $C_2$ als Automorphismen von $C_3$ angeben. ◀ **UE 454**

Etwas anspruchsvoller:

**UE 455** ▶ **Übungsaufgabe 8.4.2.8.** Beschreiben Sie sämtliche Aktionen $\tau$ von $K := C_2$ auf $N := C_8$ vermittels Automorphismen und die zugehörigen semidirekten Produkte $G_\tau := C_8 \rtimes_\tau C_2$. und $G_2 := C_8 \rtimes_{\tau_2} C_2$ zueinander nicht isomorph sind. Wie ordnen sich diese in Tabelle 8.1 ein? ◀ **UE 455**

### 8.4.3 Das Kranzprodukt

Wie wir gesehen haben, ist ein semidirektes Produkt und erst recht eine Erweiterung $G$ von $N$ durch $K$ durch die Isomorphietypen von $N$ und $K$ nicht eindeutig bestimmt. Deshalb entsteht der Wunsch, einen Überblick über alle Möglichkeiten zu bekommen. Als Schritt in diese Richtung lässt sich das auch für sich interessante Kranzprodukt deuten, welches alle Erweiterungen von $N$ mit $K$ enthält.
Um die Konstruktion besser zu verstehen, denken wir an Permutationsgruppen. $N$ können wir gemäß Cayley mittels linkskürzbarer Aktion auf sich selbst realisieren. Im Fall eines semidirekten Produktes agiert auch $K$ auf $N$. Für beliebige Erweiterungen, noch dazu für alle auf einmal, kommen wir damit aber nicht aus. Um Platz zu schaffen denken wir uns für jedes $k \in K$ eine isomorphe Kopie $N_k$ von $N$, in der sich alle Möglichkeiten für Produkte $nk$ mit $n \in N$ realisieren lassen. Die Aktion von $K$ spiegelt sich wider in Permutationen der Kopien $N_k$ gemäß der Gruppenoperation in $K$. Es lohnt sich, noch etwas weiter auszuholen.
Sei $\Sigma$ eine Partition der Menge $\Omega$ in gleich große Klassen $C_i$ (sie werden den Kopien $N_k$ entsprechen). Wir definieren die sogenannte *Automorphismengruppe*

$$G = \mathrm{Aut}(\Sigma) := \{f \in \mathrm{Sym}(\Omega) : f(\Sigma) = \Sigma\} = \{f \in \mathrm{Sym}(\Omega) : \ f(C) \in \Sigma \ \text{ für alle } C \in \Sigma\}$$

*der Partition* $\Sigma$. Diese Definition garantiert, dass alle $C \in \Sigma$ sogenannte Blöcke unter der Aktion von $G$ sind.) Dann wird durch $\rho(g, C) := g(C)$ eine Aktion von $G$ auf $\Sigma$ definiert. Bezeichne

$$B := \{g \in G : g(C) = C \ \text{ für alle } C \in \Sigma\} \cong \prod_{C \in \Sigma} \mathrm{Sym}(C) \cong \mathrm{Sym}(C)^\Sigma$$

(die letzte Isomorphie gilt für jedes $C \in \Sigma$) die so genannte *Basisgruppe*. $B$ besteht also aus jenen Permutationen, die Elemente nur innerhalb der Klassen $C \in \Sigma$ vertauschen. Dann ist $G \cong B \rtimes \mathrm{Sym}(\Sigma)$ bezüglich der Aktion $\rho$.

**UE 456** ▶ **Übungsaufgabe 8.4.3.1.** Prüfen Sie nach, dass $G$ tatsächlich semidirektes Produkt der angegebenen Form ist. ◀ **UE 456**

Wir untersuchen nun den Fall, dass jede Klasse $C \in \Sigma$ eine isomorphe Kopie einer vorgegebenen Gruppe $N$ ist. Sei $N^\Sigma$ das direkte Produkt von mit $\sigma \in \Sigma$ indizierten Kopien von $N$. Agiert $K$ auf $\Sigma$, dann agiert $K$ auch auf $N^\Sigma$ durch Automorphismen, nämlich vermittels

$$^k(n_\sigma)_{\sigma\in\Sigma} := (n_{k(\sigma)})_{\sigma\in\Sigma}, \quad n_\sigma \in N, k \in K.$$

Das semidirekte Produkt $N^\Sigma \rtimes K$ bezüglich dieser Aktion heißt dann *Kranzprodukt* (englisch: wreath product), bezeichnet mit $N\mathrm{wr}_\Sigma K$. $B := \{(n, 1) : n \in N^\Sigma\}$ wird *Basisgruppe* des Kranzproduktes genannt.
Als Standardfall betrachten wir den Spezialfall $\Sigma = K$ mit linkskürzbarer Aktion auf sich selbst, also $^k k' = kk'$. Entsprechend heißt $N\mathrm{wr}K := N\mathrm{wr}_K K = N^K \rtimes K$ auch das *Standardkranzprodukt*.

**UE 457** ▶ **Übungsaufgabe 8.4.3.2.** Beschreiben Sie explizit Elemente und Operationen im Kranzprodukt $N^\Sigma \rtimes K$ und im Standardkranzprodukt $N\mathrm{wr}K$ ◀ **UE 457**

Wie bereits angekündigt ist die wichtigste Eigenschaft des Kranzproduktes die folgende.

**Satz 8.4.3.3** (Universelle Eigenschaft des Kranzproduktes bzgl. Erweiterung)**.** *Sind $N$ und $K$ Gruppen, so lässt sich jede Erweiterung von $N$ durch $K$ isomorph in das Kranzprodukt $N\mathrm{wr}K$ einbetten.*

**UE 458** ▶ **Übungsaufgabe 8.4.3.4.** Beweisen Sie Satz 8.4.3.3. ◀ **UE 458**

**UE 459** ▶ **Übungsaufgabe 8.4.3.5.** Besprechen Sie interessante Beispiele von Kranzprodukten. ◀ **UE 459**

## 8.5 Direkte Zerlegung: Der Satz von Krull-Schmidt

Durch den Satz von Jordan-Hölder wird jeder Gruppe mit einer Kompositionsreihe als Isomorphieinvariante die (ungeordnete) Liste der Isomorphietypen der (dann notwendig einfachen) Faktoren zugeordnet. Damit verwandt ist die Frage nach Darstellungen als direktes Produkt von Faktoren, die selbst nicht mehr echt in ein direktes Produkt zerlegt werden können. Klar ist einerseits, dass endliche Gruppen solche Zerlegungen haben, andererseits aber sicher nicht alle Gruppen. Man denke an ein direktes Produkt unendlich vieler isomorpher Kopien ein und derselben Gruppe. Relativ schnell kann man erkennen, dass jede der sogenannten Kettenbedingungen für Normalteiler, aufsteigend (ACC) wie absteigend (DCC), hinreicht für eine Zerlegung in endlich viele selbst unzerlegbare direkte Faktoren. Diese Kettenbedingungen besagen, dass es keine unendlichen, echt

aufsteigenden bzw. absteigenden Folgen von Normalteilern gibt. Die Argumente dafür sind durchaus verwandt mit jenen für die Existenz der Primfaktorzerlegung einer natürlichen Zahl. Keineswegs leicht einzusehen ist die bemerkenswerte Aussage des Satzes von Krull-Schmidt: Sind beide Kettenbedingungen erfüllt, gilt für direkte Zerlegungen sogar Eindeutigkeit bis auf Isomorphie und Reihenfolge der Faktoren. Der Beweis des Satzes von Krull-Schmidt ist das Ziel dieses Abschnitts.
In 8.5.1 werden die beiden Kettenbedingungen definiert und der Satz von Krull-Schmidt präzise formuliert. Wie schon erwähnt, reicht bereits jede der beiden für sich hin, um die Existenz einer direkten Zerlegung zu zeigen. Zum Beweis der viel schwieriger zu beweisenden Eindeutigkeitsaussage des Satzes von Krull-Schmidt kann an dieser Stelle nur eine Andeutung der Methoden gegeben werden. Die Beweisarbeit im Detail beginnt in 8.5.2 mit der Einführung des Begriffs des normalen Endomorphismus und dem Beweis eines ersten wichtigen Lemmas, das eine Beziehung zu den Kettenbedingungen herstellt. Diese Stoßrichtung wird in 8.5.3 mit dem Fitting-Lemma vertieft, wonach für eine Gruppe $G$ mit ACC und DCC und jeden normalen Endomorphismus $f$ von $G$ ein $n \in \mathbb{N}$ mit $G = \ker f^n \times \operatorname{Im} f^n$ existiert – eine erste interessante direkte Zerlegung. Der Abschluss des Beweises des Satzes von Krull-Schmidt gelingt schließlich in 8.5.4.

### 8.5.1 Kettenbedingungen und Formulierung des Satzes

**Definition 8.5.1.1.** Eine Gruppe $G$ heißt *direkt zerlegbar*, wenn es nichttriviale Untergruppen $A, B \leq G$ mit $G = A \times B$ gibt. Andernfalls heißt $G$ *direkt unzerlegbar*.
$G$ erfüllt die *aufsteigende Kettenbedingung (ACC)* für Normalteiler, falls

$$G_1 \leq G_2 \leq G_3 \leq \ldots, \quad G_i \lhd G \Longrightarrow \exists n \in \mathbb{N}\, \forall i \geq n : G_i = G_n.$$

$G$ erfüllt die *absteigende Kettenbedingung (DCC)* für Normalteiler, falls

$$G_1 \geq G_2 \geq G_3 \geq \ldots, \quad G_i \lhd G \Longrightarrow \exists n \in \mathbb{N}\, \forall i \geq n : G_i = G_n.$$

**Satz 8.5.1.2.** *Erfüllt eine Gruppe $G$ wenigstens eine der beiden Bedingungen ACC oder DCC, dann existieren direkt unzerlegbare $G_1, G_2, \ldots, G_s$, so dass $G = G_1 \times G_2 \times \ldots \times G_s$.*

**UE 460 ▶ Übungsaufgabe 8.5.1.3.** Beweisen Sie Satz 8.5.1.2: **◀ UE 460**

1. Unter der Voraussetzung von ACC.
2. Unter der Voraussetzung von DCC.

Man beachte die Analogie zur Rolle der Teilerkettenbedingung im Zusammenhang mit der Faktorisierung in $\mathbb{Z}$.

**UE 461 ▶ Übungsaufgabe 8.5.1.4.** Untersuchen Sie interessante Gruppen auf direkte Zerlegbarkeit, ACC und DCC. **◀ UE 461**

**UE 462** ► **Übungsaufgabe 8.5.1.5.** Die Gruppe $G = G_1 \times G_2 \times \ldots \times G_s$ erfülle ACC bzw. DCC. Zeigen Sie, dass dann auch alle $G_i$ ACC bzw. DCC erfüllen. ◄ **UE 462**

**UE 463** ► **Übungsaufgabe 8.5.1.6.** Zeigen Sie anhand eines Beispiels, dass direkte Unzerlegbarkeit durch Epimorphismen nicht übertragen werden muss. ◄ **UE 463**

Das Ziel dieses Abschnitts ist der Beweis des folgenden Satzes.

**Satz 8.5.1.7** (Krull-Schmidt)**.** *Sei $G$ eine Gruppe, die ACC und DCC erfüllt, und gelte $G = G_1 \times G_2 \times \ldots \times G_s$ und $G = H_1 \times H_2 \times \ldots \times H_t$ für direkt unzerlegbare $G_i, H_j$, dann folgt:*
*Es gilt $s = t$ und es existiert eine Permutation $\pi$ der Indizes 1 bis $s$ derart, dass $G_i \cong H_{\pi(i)}$ für $i = 1, \ldots, s$ und für jedes $r \leq s$ gilt:*

$$G = G_1 \times G_2 \times \ldots \times G_r \times H_{\pi(r+1)} \times \ldots \times H_{\pi(s)}.$$

**UE 464** ► **Übungsaufgabe 8.5.1.8.** Zur Illustration des Satzes von Krull-Schmidt sind Beispiele folgender Art zu finden (Notation wie im Satz): ◄ **UE 464**

1. Eine Gruppe $G$ mit zwei direkten Zerlegungen, welche die Voraussetzungen (und somit auch die Behauptungen) des Satzes erfüllen, wo aber tatsächlich nur auf Isomorphie der $G_i$ mit den $H_{\pi(i)}$ geschlossen werden kann, nicht aber auf Gleichheit.
2. Eine Gruppe $G$, die ACC erfüllt, nicht aber DCC und wo die Eindeutigkeitsaussage im Satz von Krull-Schmidt nicht gilt.
3. Eine Gruppe $G$, die DCC erfüllt, nicht aber ACC und wo die Eindeutigkeitsaussage im Satz von Krull-Schmidt nicht gilt.

Der Beweis der Eindeutigkeitsaussage ist einigermaßen anspruchsvoll und wird uns für den Rest des Abschnitts beschäftigen, selbst wenn zahlreiche Beweisschritte in Übungsaufgaben ausgelagert werden. Bevor wir ins technische Detail gehen, seien hier ein paar Andeutungen zur Beweisidee vorangestellt.
Der Einfachheit halber wollen wir dazu von zwei Zerlegungen $G = G_1 \times G_2 = H_1 \times H_2$ in jeweils nur zwei unzerlegbare Bestandteile ausgehen. Mit jeder direkten Zerlegung gehen Einbettungs- und Projektionsabbildungen für die Komponenten einher. Solche Endomorphismen haben eine interessante Eigenschaft, die man *normal* nennt. Eine Konsequenz von Normalität besteht darin, dass nicht nur Urbilder, sondern auch Bilder von Normalteilern wieder Normalteiler sind. Damit lässt sich unter Verwendung von ACC und DCC für jeden normalen Endomorphismus $f$ eine Zerlegung der Gestalt $G = \ker f^n \times \operatorname{Im} f^n$ konstruieren (Fitting-Lemma 8.5.3.1). Für unzerlegbare Faktoren in einer Zerlegung heißt dies, dass $f$ entweder nilpotent ist ($\operatorname{Im} f^n$ trivial) oder injektiv ($\ker f^n$ trivial). Der zweite Fall lässt sich bei Anwendung auf geeignete $f$, die sich aus Einbettungen und Projektionen zusammensetzen, so weit ausbeuten, dass schlussendlich Isomorphismen zwischen (oBdA) $G_1 \cong H_1$ und $G_2 \cong H_2$ gefunden werden können.

### 8.5.2 Normale Endomorphismen

In unserer Strukturanalyse direkter Zerlegungen $G = G_1 \times G_2 \times \dots G_n$ werden die natürlichen Projektionen $\pi_i \colon G \to G_i$, Einbettungen $\iota_i \colon G_i \to G$ sowie deren Kompositionen, die Endomorphismen $\varphi_i := \iota_i \pi_i \colon G \to G$ eine wichtige Rolle spielen, außerdem die Möglichkeit, aus den $\varphi_i$, $i = 1, 2, \dots, n$, wieder die Identität auf $G$ zusammenzusetzen. Vor allem auf derartige Situationen werden wir die nachfolgende Definition anwenden.

**Definition 8.5.2.1.** Sei $G$ eine Gruppe. Mit $\mathrm{End}(G)$ bezeichnen wir die Menge aller Endomorphismen $f \colon G \to G$. Ein $f \in \mathrm{End}(G)$ heißt *normal*, wenn $f$ mit allen inneren Automorphismen $\varphi_a : x \mapsto axa^{-1}$ vertauscht, d.h. wenn für alle $a, b \in G$ gilt: $af(b)a^{-1} = f(aba^{-1})$. Wir bezeichnen die Menge aller normalen Endomorphismen mit $End_{\lhd}(G)$.
$f$ heißt *nilpotent*, wenn ein $n \in \mathbb{N}$ existiert, so dass $f^n \equiv e$ konstant ist.
Für beliebige $f, g \in \mathrm{End}(G)$ definieren wir außerdem eine (i.a. nicht kommutative) Summe $f + g$ durch $(f + g)(a) := f(a)g(a)$.

**Proposition 8.5.2.2.** *Sei $G$ eine Gruppe und $f, g \in \mathrm{End}(G)$. Dann gilt:*

*(i) Genau dann ist $f + g \in \mathrm{End}(G)$, wenn für alle $a \in \mathrm{Im}\, f$ und alle $b \in \mathrm{Im}\, g$ gilt $ab = ba$.*

*(ii) Aus $f, g \in End_{\lhd}(G)$ folgt auch $fg := f \circ g \in End_{\lhd}(G)$.*

*(iii) Normale Endomorphismen $f \in End_{\lhd}(G)$ bilden Normalteiler auf Normalteiler ab: $H \lhd G \Rightarrow f(H) \lhd G$*

*(iv) Ist für $f, g \in End_{\lhd}(G)$ die Summe $f + g$ ein Endomorphismus, dann sogar ein normaler, d.h. $f + g \in End_{\lhd}(G)$.*

*(v) Für $G = G_1 \times \dots \times G_n$ und $j = 1, \dots, n$ seien*

$$\iota_j \colon G_j \to G, \quad a_j \mapsto (e_1, \dots, e_{j-1}, a_j, e_{j+1}, \dots, e_n),$$

*die kanonischen Einbettungen,*

$$\pi_j : G \to G_j, \quad (a_1, \dots, a_n) \mapsto a_j$$

*die kanonischen Projektionen und*

$$\varphi_j := \iota_j \pi_j \in \mathrm{End}(G).$$

*Dann sind für alle Auswahlen von Indizes $1 \le j_1 < \dots < j_k \le n$ die Summen $\varphi_{j_1} + \dots + \varphi_{j_k}$ normale Endomorphismen von $G$.*

**UE 465 ▶ Übungsaufgabe 8.5.2.3.** Beweisen Sie Proposition 8.5.2.2 **◀ UE 465**

**Lemma 8.5.2.4.** *Sei $G$ eine Gruppe.*

*(a) $G$ erfülle ACC und sei $f \in \mathrm{End}(G)$. Dann folgt aus der Surjektivität von $f$ bereits Bijektivität, also $f \in \mathrm{Aut}(G)$.*

*(b) $G$ erfülle DCC und sei sogar $f \in End_{\lhd}(G)$. Dann folgt auch aus der Injektivität von $f$ bereits Bijektivität, also $f \in \mathrm{Aut}(G)$.*

*Beweis.* Zu Punkt (a): Wir betrachten die folgende aufsteigende Kette von Normalteilern von $G$:

$$\{e\} \leq \ker f \leq \ker f^2 \leq \dots.$$

Wegen ACC gibt es ein $n$, so dass $\ker f^n = \ker f^{n+1}$. Sei $a \in \ker f$. Da mit $f$ auch $f^n$ surjektiv ist, gibt es ein $b \in G$ mit $f^n(b) = a$ und es folgt $e = f(a) = f^{n+1}(b)$. Also ist $b \in \ker f^{n+1} = \ker f^n$, d.h. $a = f^n(b) = e$. Also ist $f$ auch injektiv und somit bijektiv.
Zu Punkt (b): Da $f$ ein normaler Endomorphismus ist, gilt $\mathrm{Im}\, f^k \lhd G$ für alle $k \geq 1$. Wir betrachten also die absteigende Kette

$$G \geq \mathrm{Im}\, f \geq \mathrm{Im}\, f^2 \geq \dots.$$

Wegen DCC gibt es ein $n$, sodass $\mathrm{Im}\, f^n = \mathrm{Im}\, f^{n+1}$, das heißt für jedes $a \in G$ gibt es ein $b \in G$, so dass $f^n(a) = f^{n+1}(b) = f^n(f(b))$. Mit $f$ ist auch $f^n$ injektiv, und es folgt $a = f(b)$. Also ist $f$ auch surjektiv und somit bijektiv. □

**UE 466** ► **Übungsaufgabe 8.5.2.5.** Versuchen Sie, die Endomorphismenmonoide $\mathrm{End}(G)$ und $\mathrm{End}_{\lhd}(G)$ für einige Gruppen $G$ zu beschreiben. Welche der Endomorphismen von $G$ sind sogar Automorphismen? Unverbindliche Vorschläge für $G$: ◄ **UE 466**

1. zyklisches $G$
2. endlich erzeugtes abelsches $G$ (Hauptsatz verwenden)
3. $G = S_3$ als die kleinste nichtabelsche Gruppe
4. $G = S_4$ oder eine andere endliche nichtabelsche Gruppe
5. ein davon verschiedenes $G$, insbesondere ein unendliches und nichtabelsches

### 8.5.3 Normale Endomorphismen induzieren direkte Zerlegungen

**Lemma 8.5.3.1.** *[Fittings Lemma] Sei $G$ eine Gruppe, die ACC und DCC erfüllt, und sei $f \in End_{\lhd}(G)$. Dann gibt es ein $n \in \mathbb{N} \setminus \{0\}$, so dass $G = \ker f^n \times \mathrm{Im}\, f^n$.*

*Beweis.* Da $f$ ein normaler Endomorphismus ist, gilt $\mathrm{Im}\, f^k \lhd G$ für alle $k \geq 1$. Betrachte also die Ketten

$$G \geq \mathrm{Im}\, f \geq \mathrm{Im}\, f^2 \geq \dots \quad \text{und} \quad \{e\} \leq \ker f \leq \ker f^2 \leq \dots.$$

Wegen ACC und DCC gibt es ein $n \in \mathbb{N}$, sodass $\mathrm{Im}\, f^k = \mathrm{Im}\, f^n$ und $\ker f^k = \ker f^n$ für alle $k \geq n$. Für den Nachweis von $\ker f^n \cap \mathrm{Im}\, f^n = \{e\}$ sei $a \in \ker f^n \cap \mathrm{Im}\, f^n$. Dann gibt es

ein $b$ mit $f^n(b) = a$. Wir schließen daraus $f^{2n}(b) = f^n(a) = e$, also $b \in \ker f^{2n} = \ker f^n$, folglich tatsächlich $a = f^n(b) = e$. Gelingt auch der Nachweis von $G = \ker f^n \cdot \operatorname{Im} f^n$, so folgt die Behauptung aus Satz **??**. Sei also $c \in G$, dann ist $f^n(c) \in \operatorname{Im} f^n = \operatorname{Im} f^{2n}$, also gibt es ein $d \in G$, so dass $f^n(c) = f^{2n}(d)$. Nun gilt

$$f^n(cf^n(d^{-1})) = f^n(c)f^{2n}(d^{-1}) = f^n(c)f^{2n}(d)^{-1} = f^n(c)f^n(c)^{-1} = e.$$

Also ist $cf^n(d^{-1}) \in \ker f^n$. Es folgt $c = (cf^n(d^{-1}))f^n(d) \in \ker f^n \cdot \operatorname{Im} f^n$. □

**Korollar 8.5.3.2.** *Sei $G$ eine direkt unzerlegbare Gruppe, die ACC und DCC erfüllt, und sei $f \in End_{\triangleleft}(G)$. Dann ist $f$ nilpotent oder ein Automorphismus von $G$.*

*Beweis.* Aus Fittings Lemma 8.5.3.1 folgt, dass $G = \ker f^n \times \operatorname{Im} f^n$ für ein $n \geq 1$. Da $G$ direkt unzerlegbar ist, ist entweder $\ker f^n = \{e\}$ oder $\operatorname{Im} f^n = \{e\}$. Gilt $\operatorname{Im} f^n = \{e\}$, so ist $f$ nilpotent. Gilt $\ker f^n = \{e\}$ dann auch $\ker f = \{e\}$, also ist $f$ injektiv und daher nach Lemma 8.5.2.4(b) ein Automorphismus auf $G$. □

**Korollar 8.5.3.3.** *Sei $G$ eine direkt unzerlegbare Gruppe, die ACC und DCC erfüllt, und seien $f_1, \ldots, f_n \in End_{\triangleleft}(G)$ nilpotent mit $f_{i_1} + \ldots + f_{i_r} \in End(G)$ für alle $1 \leq i_1 < \ldots < i_r \leq n$. Dann ist $f_1 + \ldots + f_n \in End_{\triangleleft}(G)$ nilpotent.*

*Beweisskizze.* Wegen 8.5.2.2 genügt es, die Aussage für $n = 2$ zu zeigen, der allgemeine Fall folgt dann mit Induktion. Angenommen, $f_1 + f_2$ ist nicht nilpotent, dann folgt aus Korollar 8.5.3.2 $f_1 + f_2 \in \operatorname{Aut}(G)$. Definiere $g := (f_1 + f_2)^{-1}$, $g_1 := f_1 g$ und $g_2 := f_2 g$. Es folgt:

$$(g_1 + g_2)(x) = g_1(x)g_2(x) = (f_1 g)(x)(f_2 g)(x) = (f_1 + f_2)(g(x)) = x,$$

also $g_1 + g_2 = \mathrm{id}_G$. Nun ist $x^{-1} = (g_1 + g_2)(x^{-1}) = g_1(x^{-1})g_2(x^{-1})$ und damit

$$x = \left(g_1(x^{-1})g_2(x^{-1})\right)^{-1} = g_2(x)g_1(x) = (g_2 + g_1)(x).$$

Also gilt insgesamt $g_2 + g_1 = \mathrm{id}_G = g_1 + g_2$, und damit

$$g_1 g_1 + g_1 g_2 = g_1(g_1 + g_2) = g_1 \,\mathrm{id}_G = \mathrm{id}_G \, g_1 = (g_1 + g_2)g_1 = g_1 g_1 + g_2 g_1.$$

Daraus erhält man $g_1 g_2 = g_2 g_1$. Mittels Induktion folgt daraus

$$(g_1 + g_2)^m = \sum_{i=0}^{m} \binom{m}{i} g_1^i g_2^{m-i}$$

für alle $m \geq 1$: Da $g$ surjektiv ist und $f_1, f_2$ nicht injektiv (da nilpotent) sind, können die $g_i = f_i g$, $i = 1, 2$ nicht injektiv sein. Also folgt wieder aus 8.5.3.2, dass $g_1, g_2$ beide nilpotent sind. Das heißt aber

$$\mathrm{id}_G = (g_1 + g_2)^m = \sum_{i=0}^{m} \binom{m}{i} g_1^i g_2^{m-i} \equiv e$$

für hinreichend großes $m$. Widerspruch. □

### 8.5.4 Beweis der Eindeutigkeit

Für $G$ mit ACC und DCC folgt aus 8.5.1.2 die Existenz einer Zerlegung in direkt unzerlegbare Untergruppen. Zu beweisen ist daher nur noch die Eindeutigkeitsaussage von Satz 8.5.1.7.
Sei also $G = G_1 \times \ldots \times G_s = H_1 \times \ldots \times H_t$ mit $G_i, H_j$ direkt unzerlegbar. Zu zeigen ist $s = t$ und nach geeigneter Umnummerierung $G_i \cong H_i$ für $i = 1, \ldots, s = t$ und $G = G_1 \times \ldots \times G_r \times H_{r+1} \times \ldots \times H_t$ für $0 \leq r \leq t$.
Im Folgenden bedeute die Aussage $A(r)$ für $r \leq \min(s,t)$: Es existiert eine Umnummerierung der $H_j$ mit $G_i \cong H_i$ für $i = 1, \ldots, r$ und $G = G_1 \times \ldots \times G_r \times H_{r+1} \times \ldots \times H_t$. Der Beweis erfolgt durch Induktion nach $r$.
$A(0)$ bedeutet $G = H_1 \times \ldots \times H_t$, gilt also nach Voraussetzung.
Sei also $A(r-1)$, $1 \leq r \leq \min(s,t)$ vorausgesetzt, d.h.

$$G = G_1 \times \ldots \times G_{r-1} \times H_r \times \ldots \times H_t$$

nach geeigneter Umnummerierung der $H_j$, wobei $G_i \cong H_i$ für $i = 1, \ldots, r-1$. Seien $\pi_1, \ldots, \pi_s$ bzw. $\pi'_1, \ldots, \pi'_t$ die Projektionen für die Darstellungen $G = G_1 \times \ldots \times G_s$ und $G = G_1 \times \ldots \times G_{r-1} \times H_r \times \ldots \times H_t$, $\iota_1, \ldots, \iota_s$ bzw. $\iota'_1, \ldots, \iota'_t$ die zugehörigen Einbettungen. Wir definieren $\varphi_i := \iota_i \pi_i$ bzw. $\psi_j := \iota'_j \pi'_j$ und halten fest, dass es sich dabei laut Proposition 8.5.2.2 um normale Endomorphismen handelt. Dann gilt:

$$\begin{array}{lll} \varphi_i|_{G_i} = \mathrm{id}_{G_i} & \varphi_i\varphi_i = \varphi_i & \varphi_{i_1}\varphi_{i_2} \equiv e \ (i_1 \neq i_2) \\ \psi_1 + \ldots + \psi_t = \mathrm{id}_G & \psi_j\psi_j = \psi_j & \psi_{j_1}\psi_{j_2} \equiv e \ (j_1 \neq j_2) \\ \mathrm{Im}\,\varphi_i = G_i & \mathrm{Im}\,\psi_j = G_j \ (j < r) & \mathrm{Im}\,\psi_j = H_j \ (j \geq r) \end{array}$$

Es folgt, dass $\varphi_r\psi_j \equiv e$ für $j < r$, denn

$$\varphi_r\psi_j(x) = \varphi_r \,\mathrm{id}_{G_j}\, \psi_j(x) = \varphi_r\varphi_j\psi_j(x) = e.$$

Daher gilt

$$\varphi_r = \varphi_r \,\mathrm{id}_G = \varphi_r(\psi_1 + \ldots + \psi_t) = \varphi_r\psi_1 + \ldots + \varphi_r\psi_t. = \varphi_r\psi_r + \ldots + \varphi_r\psi_t.$$

Aus Proposition 8.5.2.2 folgt, dass alle „Partialsummen“ normale Endomorphismen sind. Da $\varphi_r|_{G_r}$ nicht nilpotent sein kann (es gilt $\varphi_r^2 = \varphi_r$) und mit $G$ nach Übungsaufgabe 8.5.1.5 auch $G_r$ ACC und DCC erfüllt, muss es nach Korollar 8.5.3.2 und 8.5.3.3 zumindest einen Summanden $\varphi_r\psi_j$ in $\varphi_r\psi_r + \ldots + \varphi_r\psi_t$ geben, dessen Einschränkung auf $G_r$ in $\mathrm{Aut}(G_r)$ liegt. Also ist auch

$$(\varphi_r\psi_j)^{n+1}|_{G_r} = \varphi_r(\psi_j\varphi_r)^n\psi_j|_{G_r} \in \mathrm{Aut}(G_r)$$

und $\psi_j\varphi_r|_{H_j} \in End_{\triangleleft}(H_j)$ nicht nilpotent. Weil auch $H_j$ sowohl ACC als auch DCC erfüllt, folgt aus 8.5.3.2, dass $\psi_j\varphi_r|_{H_j}$ ein Automorphismus auf $H_j$ ist. Daher sind $\psi_j|_{G_r} \colon G_r \to H_j$ und $\varphi_r|_{H_j} \colon H_j \to G_r$ Isomorphismen. Es folgt nach geeigneter Umnummerierung $G_r \cong H_r$.

Zu zeigen bleibt $G = G_1 \times \ldots \times G_r \times H_{r+1} \times \ldots \times H_t$. Sei zu diesem Zwecke

$$G^* := G_1 \cdot \ldots \cdot G_r \cdot H_{r+1} \cdot \ldots \cdot H_t = \{g_1 \cdot \ldots \cdot g_r \cdot h_{r+1} \cdot \ldots \cdot h_t : g_i \in G_i, h_j \in H_j\}.$$

Nach der Induktionsannahme können wir

$$G_* := G_1 \cdot \ldots \cdot G_{r-1} \cdot H_{r+1} \cdot \ldots \cdot H_t = G_1 \times \ldots \times G_{r-1} \times H_{r+1} \times \ldots \times H_t$$

betrachten. Für $j < r$ ist $\psi_r(G_j) = \psi_r\psi_j(G) = \{e\}$, für $j > r$ ist $\psi_r(H_j) = \psi_r\psi_j(G) = \{e\}$, also $\psi_r(G_*) = \{e\}$. Da $\psi_r|_{G_r}$ ein Isomorphismus ist, folgt $G_r \cap G_* = \{e\}$. Außerdem sind alle Faktoren in der nachfolgenden Zerlegung Normalteiler, weshalb wirklich eine direkte Zerlegung vorliegt:

$$G^* = G_* \times G_r = G_1 \times \ldots \times G_r \times H_{r+1} \times \ldots \times H_t \leq G.$$

Wir definieren $\theta\colon G = G_* \times H_r \to G_* \times G_r$ durch

$$g = g_1 \cdot \ldots \cdot g_{r-1} \cdot h_r \cdot \ldots \cdot h_t \in G \mapsto g_1 \cdot \ldots \cdot g_{r-1} \cdot \varphi_r(h_r) \cdot h_{r+1} \cdot \ldots \cdot h_t,$$

wobei $g_i \in G_i, h_j \in H_j$. Anhand der Darstellung $G = G_1 \times \ldots \times G_{r-1} \times H_r \times \ldots \times H_t$ (Induktionsannahme) sieht man, dass $\theta$ auf $G$ wohldefiniert ist, wegen der Injektivität von $\varphi_r$ auf $H_r$ auch injektiv. Auch die Normalität von $\varphi_r$ vererbt sich auf $\theta$ (nachrechnen, Übung). Wegen Lemma 8.5.2.4 ist daher $\theta \in \mathrm{Aut}(G)$, also $G = \mathrm{Im}\,\theta = G^*$. Damit ist $A(r)$ gezeigt und der Induktionsbeweis erbracht. Nach Umnummerierung gilt also $G_i \cong H_i$ für $0 \leq i \leq \min(s,t)$. Ist $\min(s,t) = s$, dann gilt

$$G_1 \times \ldots \times G_s = G = G_1 \times \ldots \times G_s \times H_{s+1} \times \ldots \times H_t.$$

Ist $\min(s,t) = t$, dann gilt

$$G_1 \times \ldots \times G_s = G = G_1 \times \ldots \times G_t.$$

Da aber alle $G_i, H_j \neq \{e\}$ sind, muss in jedem Fall $s = t$ gelten.

**UE 467** ► **Übungsaufgabe 8.5.4.1.** Überprüfen Sie, dass der in obigem Beweis auftretende Endomorphismus $\theta$ tatsächlich ein normaler ist. ◄ **UE 467**

# 9 Galoistheorie

Die Galoistheorie ist eine Vertiefung der Körpertheorie mit vorwiegend gruppentheoretischen Methoden. Das vorliegende Kapitel kann daher als eine Fortsetzung von Kapitel 6 unter essenzieller Verwendung von Ergebnissen aus Kapitel 8 betrachtet werden.
Die Galoistheorie erfreut sich innerhalb der Algebra – um nicht zu sagen innerhalb der gesamten Mathematik – eines besonderen Status. Sie entsprang historisch einem klassischen Anliegen der Mathematik, nämlich dem Lösen von Gleichungen. Indem die Galoistheorie auf geniale Weise Automorphismengruppen von Körpern nutzbar macht, sind gleichzeitig ihre Methoden und Sichtweisen darüber hinaus von einer Originalität, von der im Laufe der Geschichte auch viele andere Gebiete der Mathematik außerhalb der Algebra profitiert haben.
Um diese Besonderheiten ins rechte Licht zu stellen, ist dem Kapitel ein eigener Abschnitt über das sehr allgemeine Konzept der Galoiskorrespondenz vorangestellt – von einer beliebigen zweistelligen Relation induziert wie auch der abstrakten (9.1). Sodann wenden wir uns der klassischen Galoiskorrespondenz zu, die durch Körpererweiterungen $K \leq E$ über die Fixpunktrelation von $K$-Automorphismen von $E$ induziert wird. Dabei stößt man auf sehr natürliche Weise auf den Begriff der Galoisschen Erweiterung, dem Abschnitt 9.2 gewidmet ist. Der Hauptsatz der Galoistheorie ist Gegenstand von 9.3. Er beschreibt die Galois-abgeschlossenen Elemente bei Galoisschen Erweiterungen. Konkret geht es um die bijektive Beziehung zwischen den Körpern $Z$ mit $K \leq Z \leq E$ einerseits und den (bezüglich einer natürlichen Topologie abgeschlossenen) Untergruppen der sogenannten Galoisgruppe $\mathrm{Aut}_K(E)$ andererseits. Dabei besteht $\mathrm{Aut}_K(E)$ definitionsgemäß aus den $K$-Automorphismen von $E$, d.h. aus jenen Automorphismen von $E$, die $K$ punktweise fest lassen. Der Spezialfall, dass $E$ der Zerfällungskörper eines Polynoms über $K$ ist, wird in 9.4 ausführlich untersucht. Der letzte Abschnitt der Kapitels (9.5) widmet sich schließlich dem historischen Ursprung der Galoistheorie, der sogenannten Auflösbarkeit von Gleichungen durch Radikale.

## 9.1 Historie und allgemeine Grundkonzepte

Ein wenn auch kurzer, so doch eigener einleitender Abschnitt zum Kapitel über Galoistheorie ist dem bereits in der Kapiteleinleitung hervorgehobenen Umstand geschuldet, dass die Galoistheorie in vielerlei Hinsicht paradigmatisch für zahlreiche wichtige Teile der Mathematik ist. In 9.1.1 wird das unter historischem Blickpunkt relativ ausführlich besprochen – ausführlicher jedenfalls als Historisches in anderen Kapiteln zur Sprache kommt. Auf mathematischer Ebene spiegelt sich die paradigmatische Rolle der Galoistheorie wider im sehr allgemeinen und von der Theorie der Körper an sich unabhängigen Begriff der Galoiskorrespondenz. Meist treten Galoiskorrespondenzen als durch eine Re-

lation induziert auf. Das ist Gegenstand von 9.1.2. Man kann aber auch von einer die Galoiskorrespondenz induzierenden Relation abstrahieren und den Begriff der abstrakten Galoiskorrespondenz prägen. Das geschieht in 9.1.3. Abschnließend werden noch einige andere prominente Beispiele aus unterschiedlichen Gebieten des Mathematik erwähnt (9.1.4).

### 9.1.1 Historisches

Ihren historischen Ausgangspunkt nahm die Galoistheorie bei der Suche nach Lösungsformeln für algebraische Gleichungen in einer Variablen, also Gleichungen der Form $f(x) = 0$ mit einem Polynom $f$. Klarerweise wird diese Aufgabe mit wachsendem Grad $n$ von $f$ zunehmend schwieriger. Die Lösungen für $n = 1$ und teilweise auch $n = 2$ waren schon Mathematikern antiker Hochkulturen vertraut. Nach Europa gelangten diese Einsichten aber erst im Mittelalter. Die Lösung für $n = 3, 4$ geht auf italienische Mathematiker des 16. Jahrhunderts zurück, dann stand man an. Erst um 1800 gelang Carl Friedrich Gauß (1777-1855) der erste Beweis des sogenannten Fundamentalsatzes der Algebra, dass jedes nichtkonstante Polynom eine komplexe Nullstelle hat. Allgemeine Lösungsformeln für $n \geq 5$ wurden aber keine gefunden. Langsam kam man zur Überzeugung, dass dies gar nicht möglich ist. Die wichtigsten Namen in diesem Zusammenhang sind Niels Henrik Abel (1802–1829) und Évariste Galois (1811–1832). Abel konnte zeigen, dass es keine allgemeine Lösungsformel für algebraische Gleichungen vom Grad $\geq 5$ gibt, und Galois schuf eine Theorie, die sehr genau erklärt, woran das liegt und welche speziellen Gleichungen sehr wohl durch solche Formeln gelöst werden können. Berühmt ist die Geschichte von dem Duell, in dem der nicht einmal 21-jährige Galois umkam. In der Nacht davor hatte er seine Ideen in einem Brief an einen Freund hastig zu Papier gebracht. Hermann Weyl (1885-1955) schreibt darüber in seinem Buch über Symmetrie: „Ich wage die Behauptung, daß dieser Brief, auf die Originalität und die Tiefe der darin niedergelegten Ideen hin beurteilt, das inhaltreichste Stück Literatur ist, das wir besitzen.“ Wir werden in 9.5 ausführlich auf das Hauptresultat von Galois zurückkommen.

Aus heutiger Perspektive ist die Lösung des ursprünglichen Problems vergleichsweise eine Randerscheinung. Von ungeheurer Tragweite hingegen ist die Methode, mit der die Einsichten gewonnen wurden. Und zwar stellt sich heraus, dass für die Auflösbarkeit einer algebraischen Gleichung die Symmetrien zwischen den verschiedenen Lösungen entscheidend sind, technisch gesprochen: Die sogenannte Galoisgruppe des Polynoms $f$ muss auflösbar im Sinne der Gruppentheorie sein.

Natürlich ist die Chronologie der Terminologie umgekehrt. Denn Galois führte erst im Zuge seiner Problemlösung den Begriff der Gruppe ein, und die Bezeichnung „auflösbar“ in Bezug auf eine Gruppe ergab sich erst im Anschluss daran in Hinblick auf die Auflösbarkeit von Gleichungen durch Lösungsformeln. Damit wurde eine Abstraktionsebene ganz neuer Art geschaffen – in ähnlicher Weise wie etwa zur gleichen Zeit János Bolyai (1802–1860), Nikolai Iwanowitsch Lobatschewski (1792–1856) und Gauß gleichfalls Unmöglichkeitsbeweise führten. Indem sie Beispiele nichteuklidischer Geometrien angaben, zeigten sie, dass das legendäre Parallelenpostulat, das für die euklidische Geometrie typisch ist, in diesen Modellen aber verletzt ist, aus den anderen Grundannahmen, die

in ihren Geometrien sehr wohl erfüllt sind, also nicht denknotwendig folgt. Derartige Gedankengänge waren damals von einer revolutionären Abstraktheit und führten die Mathematik in eine neue Epoche.
Revolutionär an der Galoistheorie war es, den unmittelbar gegebenen Objekten – in diesem Fall algebraische Gleichungen bzw. Polynome – abstrakte Strukturen zuzuordnen: einerseits Erweiterungs- und Zwischenkörper, andererseits die Gruppen von Automorphismen – eben die Galoisgruppen. Die neugeschaffenen Gebilde können ihrerseits unter völlig neuen Gesichtspunkten betrachtet werden, wodurch wiederum neue Phänomene – gefasst im Begriff der Galoiskorrespondenz – sichtbar werden. Das führt zu Einsichten, die auf der ursprünglichen, elementaren Ebene von einem Dickicht technischer Details überwuchert werden, in dem sie anders wahrscheinlich nie entdeckt worden wären.
Es ist sehr bemerkenswert, dass der Gesichtspunkt der Galoistheorie, mathematische Objekte durch ihre (eventuell auch sehr abstrakten) Symmetrien besser zu verstehen, auch dort, wo Symmetrie scheinbar ihren Ursprung hat, nämlich in der Geometrie, erst später zum Paradigma wurde. Berühmt ist in diesem Zusammenhang das sogenannte Erlangener Programm von Felix Klein (1849–1925) aus dem Jahr 1872. Darin werden Eigenschaften geometrischer Objekte dadurch als interessant und untersuchenswürdig ausgezeichnet, dass sie unter Transformationen unterschiedlicher Art invariant bleiben. Im Vergleich mit der Galoistheorie wird die Rolle der Galoisgruppe nun von geometrisch motivierten Transformationsgruppen übernommen.
Im 20. Jahrhundert erfuhr diese Herangehensweise auf nochmals gesteigertem Abstraktionsniveau eine Fortsetzung in der Modelltheorie, einem der mittlerweile als klassisch etablierten Teilgebiete der mathematischen Logik, das gleichzeitig eine sehr lebendige und fruchtbare Verbindung wieder zurück zur Algebra darstellt. Im Vergleich mit der Galoistheorie treten in der Modelltheorie an die Stelle von Körpern allgemeinere Klassen von Strukturen, wie wir sie in 2.1 und insbesondere in 2.1.4 behandelt haben. Auch in der Modelltheorie spielen Erweiterungen und Automorphismengruppen eine große Rolle. Dabei wird auch die eminente Bedeutung der zugrunde liegenden formalen Sprache deutlich, was auch der Grund dafür ist, dass die Modelltheorie traditionell der Logik und nicht mehr der Algebra zugeordnet wird.

Abgesehen von der prägenden Rolle der Galoistheorie in der Ideengeschichte der gesamten Mathematik empfinden viele Mathematiker an ihr auch einen ganz außergewöhnlichen ästhetischen Reiz. Um diesen zu genießen, wollen wir nach unserem historischen Exkurs zurückkehren zum mathematisch konkret Fassbaren. Es beginnt mit einem der Galoistheorie zugrunde liegenden sehr allgemeinen Konzept, das in vielen Teilen der Mathematik wirksam ist.

### 9.1.2 Die von einer Relation induzierte Galoiskorrespondenz

Wir wollen unsere Überlegungen mit einer einfachen Beobachtung beginnen. Seien $X$ und $Y$ Mengen (oder gar Klassen, die keine Mengen sind) und $R \subseteq X \times Y$ eine Relation, $f_R \colon \mathcal{P}(X) \to \mathcal{P}(Y)$ definiert als

$$f_R : A \mapsto A^{(R)} := \{y \in Y : \forall x \in A : xRy\}$$

und $g_R\colon \mathcal{P}(Y) \to \mathcal{P}(X)$ als

$$g_R : B \mapsto {}^{(R)}B := \{x \in X : \forall y \in B : xRy\}.$$

Dann sind

(a) $f_R, g_R$ *antiton*, d.h.

$$A_1 \subseteq A_2 \Rightarrow f_R(A_1) \supseteq f_R(A_2)$$
$$B_1 \subseteq B_2 \Rightarrow g_R(B_1) \supseteq g_R(B_2).$$

und

(b) $g_R f_R, f_R g_R$ *extensiv*, d.h.

$$\overline{A} = \overline{A}^{(R)} := g_R f_R(A) \supseteq A$$
$$\overline{B} = \overline{B}^{(R)} := f_R g_R(B) \supseteq B.$$

Das Paar $(f_R, g_R)$ heißt die *von der Relation $R$ induzierte Galoiskorrespondenz* oder auch *Galoisverbindung*. Die Mengen $A \in \mathrm{Im}(g_R)$ und $B \in \mathrm{Im}(f_R)$ (die also als Bilder unter $g_R$ bzw. $f_R$ auftreten), heißen *Galois-abgeschlossen*.

In diesem Kapitel wird das folgende klassische Beispiel einer Galoiskorrespondenz im Zentrum stehen:

**Beispiel 9.1.2.1.** Sei $K \leq E$ eine Körpererweiterung,

$$X := Aut_K(E) := \{\sigma \in Aut(E) : \forall \alpha \in K : \sigma(\alpha) = \alpha\}$$

die Menge aller *$K$-Automorphismen* des Erweiterungskörpers $E$, also jener $\sigma \in \mathrm{Aut}(E)$, die jedes Element $\alpha$ des Grundkörpers $K$ auf sich selbst abbilden, weiters $Y := E$ und

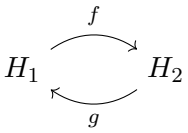
$$R := \{(\sigma, \alpha) \in X \times Y : \sigma(\alpha) = \alpha\}.$$

Für $A \subseteq X$ ist $A^{(R)}$ offenbar stets ein $K$ umfassender Unterkörper von $E$, für $B \subseteq Y$ ist ${}^{(R)}B$ stets eine Untergruppe von $Aut_K(E)$. Die von $R$ induzierte Galoiskorrespondenz ist die klassische, die der Galoistheorie zugrunde liegt.

Man kann das Konzept der Galoiskorrespondenz auch von einer Relation loslösen und eine abstrakte Definition geben.

### 9.1.3 Abstrakte Galoiskorrespondenzen

**Definition 9.1.3.1.** Seien die Halbordnungen $(H_1, \leq_1), (H_2, \leq_2)$ gegeben zusammen mit Abbildungen $f : H_1 \to H_2$, $g : H_2 \to H_1$.




Dann heißt $(f, g)$ *(abstrakte) Galoisverbindung* oder *Galoiskorrespondenz* auf den Halbordnungen $(H_1, \leq_1)$ und $(H_2, \leq_2)$, falls $f, g$ antiton sind (d.h. explizit: $h_1 \leq h_1'$ impliziert $f(h_1) \geq f(h_1')$ und $h_2 \leq h_2'$ impliziert $f(h_2) \geq f(h_2')$ für alle $h_i, h_i' \in H_i$) und die Verkettungen $gf, fg$ extensiv (d.h. explizit: $h_1 \leq g(f(h_1))$ und $h_2 \leq f(g(h_2))$ für alle $h_i \in H_i$). Elemente von $H_1$ und $H_2$, die als Bilder unter $g$ bzw. $f$ auftreten, heißen *Galois-abgeschlossen*.

Nach 9.1.2 ist jede von einer Relation $R \subseteq X \times Y$ induzierte Galoiskorrespondenz auch eine abstrakte Galoiskorrespondenz auf den Halbordnungen $(\mathcal{P}(X), \subseteq)$ und $(\mathcal{P}(Y), \subseteq)$. Es zeigt sich, dass sogar eine Art Umkehrung gilt: Jede abstrakte Galoiskorrespondenz $(f, g)$ hängt sehr eng mit einer Galoiskorrespondenz zusammen, die von einer Relation $R$ induziert wird.
Um das zu sehen, wählen wir mit der Notation aus Definition 9.1.3.1 die Mengen $X := H_1$ und $Y := H_2$ sowie die Relation

$$R := \{(x, y) : f(x) \geq_2 y\} \subseteq X \times Y.$$

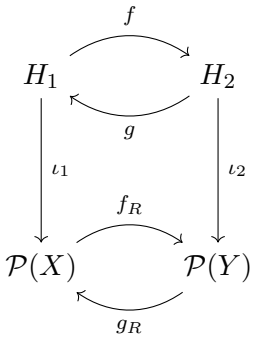
Nach 9.1.2 induziert $R$ auf den Halbordnungen $(\mathcal{P}(X), \subseteq)$ und $(\mathcal{P}(Y), \subseteq)$ eine Galoiskorrespondenz $(f_R, g_R)$. Vermittels der injektiven Abbildungen

$$\iota_1 : X \to \mathcal{P}(X), \quad \iota_1(h_1) := \{x \in X : x \leq_1 h_1\}$$

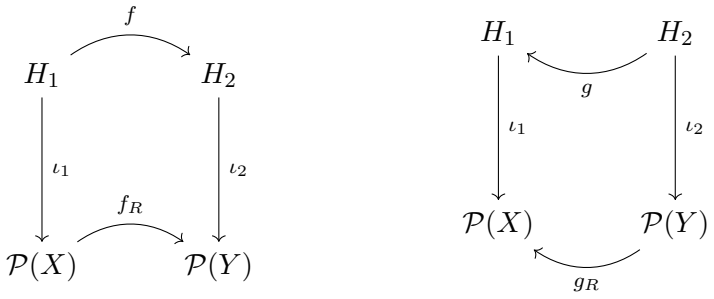
und

$$\iota_2 : Y \to \mathcal{P}(Y), \quad \iota_2(h_2) := \{y \in Y : y \leq_2 h_2\}$$

wird die ursprüngliche Galoiskorrespondenz $(f, g)$ in die von $R$ induzierte Galoiskorrespondenz $(f_R, g_R)$ eingebettet. Die Situation wird durch das Diagramm




veranschaulicht. Als ganzes ist es zwar *nicht* kommutativ, weil die Abbildungen $f$ und $g$ sowie $f_R$ und $g_R$ nicht auf ihrem gesamten Definitionbereich invers zueinander sind. Zerlegt man das ursprüngliche Diagramm in einen $f$- und einen $g$-Teil, so erhält man aber zwei Diagramme, von denen jedes für sich sehr wohl kommutiert:




Da also $f_R\iota_1 = \iota_2 f$ und $g_R\iota_2 = \iota_1 g$ gilt, ist es durchaus suggestiv und nicht abwegig, von einer Einbettung von $(f, g)$ in $(f_R, g_R)$ zu sprechen.

**UE 468** ► **Übungsaufgabe 9.1.3.2.** Verifizieren Sie alle die Einbettung von $(f, g)$ in $(f_R, g_R)$ betreffenden Behauptungen. ◄ **UE 468**

Wir fassen die wichtigsten Eigenschaften abstrakter Galoiskorrespondenzen zusammen:

**Satz 9.1.3.3.** *Für eine (abstrakte) Galoiskorrespondenz $(f, g)$ auf den Halbordnungen $(H_1, \leq_1)$ und $(H_2, \leq_2)$ gilt*

*(a) Idempotenz: $f = fgf$ und $g = gfg$.*

*(b)* $\operatorname{Im} f = \operatorname{Im} fg$ *und* $\operatorname{Im} g = \operatorname{Im} gf$ *(die Mengen der Galois-abgeschlossenen Elemente).*

*(c) $f|_{\operatorname{Im} g}$ und $g|_{\operatorname{Im} f}$ sind zueinander inverse antitone Bijektionen, insbesondere gilt:*

$$(\operatorname{Im} g, \leq_1) \cong (\operatorname{Im} f, \geq_2)$$

*Beweis.* (a): Da $fg$ und $gf$ extensiv sind, gilt $h_1 \leq gf(h_1)$ und $f(h_1) \leq fg(f(h_1))$ für alle $h_1 \in H_1$. Da $f$ antiton ist, folgt aus der ersten Ungleichung auch $f(h_1) \geq f(gf(h_1))$, zusammen mit der zweiten daher insgesamt $f = fgf$. Analog erhält man $g = gfg$.
(b): Es gilt

$$\operatorname{Im} f \supseteq \operatorname{Im} fg \supseteq \operatorname{Im} fgf \overset{(a)}{=} \operatorname{Im} f,$$

also $\operatorname{Im} f = \operatorname{Im} fg$. $\operatorname{Im} g = \operatorname{Im} gf$ folgt analog.
(c): Aus (a) ergibt sich $fg|_{\operatorname{Im} f} = \mathrm{id}_{\operatorname{Im} f}$ und $gf|_{\operatorname{Im} g} = \mathrm{id}_{\operatorname{Im} g}$, woraus direkt die Behauptung folgt. □

### 9.1.4 Beispiele von Galoiskorrespondenzen

Anhand einiger typischer Beispiele von Galoiskorrespondenzen aus verschiedenen Teilgebieten der Mathematik (teils nicht zwischen Mengen, sondern zwischen echten Klassen $X, Y$ definiert) soll nun illustriert werden, dass in solchen Situationen immer wieder die Galois-abgeschlossenen Mengen von besonderem Interesse sind. Vieles wird im Rahmen von Übungsaufgaben abgehandelt.

Auf relativ elementarem Niveau gilt das für $X := V$ (Vektorraum über einem Körper $K$), $Y := V^*$ (Dualraum von $V$) und die Relation $R := \{(x, y) : \ y(x) = 0\} \subseteq X \times Y$ (Annihilatorrelation). Ist $V$ endlichdimensional, so sind genau die Unterräume von $V$ bzw. $V^*$ die Galois-abgeschlossenen Mengen. Bei unendlichdimensionalem $V$ ist die Situation jedoch komplizierter. Eine genauere Analyse ist Gegenstand der folgenden Übungsaufgabe, die in vielerlei Hinsicht schon einen Vorgeschmack auf den Hauptsatz der Galoistheorie liefert.

**UE 469** ► **Übungsaufgabe 9.1.4.1.** Sei $V$ ein Vektorraum über einem Körper $K$ und $V^*$ sein Dualraum, d.h. der Vektorraum aller linearen Funktionale $f : V \to K$. Die Relation $R := \{(f, v) \in V^* \times V : \ f(v) = 0\}$ induziert eine Galoisverbindung, von der im Folgenden die Rede ist. Sei $B$ eine Basis von $V$ und $B_0^*$ die Menge aller $f_b \in V^*$, $b \in B$, die durch die Forderung $f_b(b') = \delta_{b,b'}$ (Kronecker-$\delta$), $b' \in B$, eindeutig definiert sind. Rekapitulieren Sie aus der Linearen Algebra und/oder Funktionalanalysis bzw. beweisen Sie: ◄ **UE 469**

1. Die bezüglich $R$ Galois-abgeschlossenen Teilmengen von $V$ sind genau die Unterräume von $V$.

2. Die bezüglich $R$ Galois-abgeschlossenen Teilmengen von $V^*$ sind durchwegs Unterräume von $V^*$.

3. Ist $V$ endlichdimensional, so ist umgekehrt jeder Unterraum von $V^*$ auch Galois-abgeschlossen.

4. Sei $K = \mathbb{Q}$, $V := \bigoplus_{n\in\mathbb{N}} \mathbb{Q}$ und $b_n := (\delta_{n,k})_{k\in\mathbb{N}}$ für alle $n \in \mathbb{N}$. Dann gibt es Unterräume von $V^*$, die nicht Galois-abgeschlossen sind. Beweisen Sie das zunächst in dieser Teilaufgabe mit einem Kardinalitätsargument. Hinweis: $B := \{b_n : \ n \in \mathbb{N}\}$ ist eine abzählbare Basis von $V$, $V$ selbst ist abzählbar, und die Menge $\mathrm{Sub}(V) := \{U : \ U \leq V\}$ aller Unterräume von $V$ hat die Kardinalität $c$ des Kontinuums. Hingegen ist $V^*$ überabzählbar von der Kardinalität $c$. Daraus folgt, dass $\mathrm{Sub}(V^*)$ von der Kardinalität $2^c$ ist. Nach Cantor kann es also keine Bijektion zwischen $\mathrm{Sub}(V)$ und $\mathrm{Sub}(V^*)$ geben.

5. Bezeichne $\tau$ die schwach-$*$-Topologie. Das ist per definitionem die schwächste Topologie auf $V^*$, bezüglich der alle Auswertungsfunktionale $v^* : V^* \to K$, $f \mapsto f(v)$, $v \in V$, stetig sind. Wenn $K$ mit der diskreten Topologie versehen ist, ist eine Umgebungsbasis des Nullfunktionals $0_{V^*} \equiv 0_K$ bezüglich $\tau$ gegeben durch das System sämtlicher Mengen $O_E := \{f \in V^* : \ f(v) = 0 \text{ für alle } v \in E\}$, wobei $E$ alle endlichen Teilmengen (oder äquivalent: alle endlich erzeugten Unterräume) von $V$ durchläuft.

6. Die schwach-$*$-Topologie $\tau$ macht $V^*$ zu einem topologischen Vektorraum.

7. Alle Galois-abgeschlossenen Unterräume von $V^*$ sind auch bezüglich der schwach-$*$-Topologie $\tau$ abgeschlossen.

8. Es gilt auch die Umkehrung: Jeder schwach-$*$-abgeschlossene Unterraum von $V^*$ ist Galois-abgeschlossen. Die ordnungsumkehrenden Bijektionen der Galoiskorrespondenz bestehen also zwischen sämtlichen Unterräumen von $V$ und den schwach-$*$-abgeschlossenen Unterräumen von $V^*$.

Eine ganz ähnliche Situation wird uns in der eigentlichen Galoistheorie begegnen. Der Hauptsatz in seiner allgemeinen Fassung (9.3.4.2) wird in ganz ähnlicher Weise eine mit einer zur schwach-$*$ analogen Topologie angereicherte Verallgemeinerung des endlichdimensionalen Falles sein.
Der Übergang von den Sichtweisen der Linearen Algebra zu jenen der Funktionalanalysis wird in der folgenden Übungsaufgabe vollzogen:

**UE 470** ► **Übungsaufgabe 9.1.4.2.** Versuchen Sie Übungsaufgabe 9.1.4.1 so weit wie möglich von diskreten auf lokalkonvexe Vektorräume $V$ zu verallgemeinern. Der Dualraum $V^*$ besteht dann lediglich aus den stetigen Funktionalen. Aus welchem berühmten Satz der Funktionalanalysis ergibt sich sehr schnell eine Beschreibung der Galois-abgeschlossenen Teilmengen von $V$? Was können Sie über jene in $V^*$ aussagen? ◄ **UE 470**

Sehr ähnlich verhält es sich, wenn man lokalkonvexe Vektorräume durch lokalkompakte abelsche Gruppen, den Skalarkörper $\mathbb{R}$ durch die Gruppe $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ und lineare Funktionale durch stetige Homomorphismen ersetzt.

**UE 471** ► **Übungsaufgabe 9.1.4.3.** Rekapitulieren Sie die Pontrjagin-Dualität aus 7.1.4 so weit wie nötig, um analoge Fragen für eine lokalkompakte abelsche Gruppe $G$, ihr Pontrjagin-Dual $G^*$ und die Annihilatorrelation $\chi(g) = 0$ für $g \in G$ und $\chi \in G^*$ zu behandeln. Es wird nicht erwartet, dass Sie alle Beweise für die hier interessanten Aussagen führen. Es genügt, wenn Sie die Ergebnisse recherchieren. ◄ **UE 471**

Als weiteres Beispiel für die Beschreibung von Galois-Abgeschlossenheit ist der Satz von Birkhoff 4.1.7.1 zu nennen. Er lässt sich als Beschreibung der Galois-abgeschlossenen Elemente (nämlich der Varietäten) bezüglich einer geeigneten Galoiskorrespondenz interpretieren. Diese wird induziert von der Relation der Gültigkeit einer Gleichung in einer bestimmten Algebra. Allerdings muss man hier den Rahmen von Mengen verlassen und auch Klassen (nämlich von Algebren) zulassen.

**UE 472** ► **Übungsaufgabe 9.1.4.4.** Präzisieren Sie diese Andeutungen. Beschreiben Sie insbesondere genauer die Relation, bezüglich derer laut dem Satz von Birkhoff 4.1.7.1 auf der einen Seite genau die Varietäten Galois-abgeschlossen sind. Wie könnte eine Beschreibung der Galois-abgeschlossenen Mengen auf der anderen Seite dieser Galoiskorrespondenz aussehen? ◄ **UE 472**

Man kann die Betrachtung auf der einen Seite von rein algebraischen Strukturen auf beliebige algebraisch-relational gemischte Strukturen eines bestimmten Typs (einer bestimmten Signatur) $(\tau, \sigma)$ ausweiten, siehe 2.1.4. Auf der anderen Seite entspricht dem

eine Anreicherung der formalen Sprache von Gleichungen für algebraische Operationen und Variablen (um die es im Satz von Birkhoff geht) zu einer vollen prädikatenlogischen Sprache für $(\tau, \sigma)$. Die Relation ist wieder die Gültigkeit einer Formel in einer Struktur. Die Frage nach den Galois-abgeschlossenen Elementen führt direkt in das Zentrum der mathematischen Logik. Wer sich dafür interessiert, sollte an der folgenden Übungsaufgabe Freude finden.

**UE 473** ► **Übungsaufgabe 9.1.4.5.** Untersuchen Sie die angedeutete Galoiskorrespondenz, die von jener Relation $R$ induziert wird, die aus gewissen Paaren $(\mathfrak{A}, \varphi)$ besteht mit folgenden Eigenschaften: $\mathfrak{A}$ ist eine relationale Struktur mit der (als vorgegeben zu denkenden) Signatur $(\tau, \sigma)$ und $\varphi$ ein Satz (d.h. eine Formel ohne freie Variable, der somit in jedem Modell ein eindeutig bestimmter Wahrheitswert zukommt) einer zugehörigen formalen Sprache. Zu $R$ gehört das Paar $(\mathfrak{A}, \varphi)$ genau dann, wenn $\varphi$ in $\mathfrak{A}$ wahr ist. ◄ **UE 473**

Die bisher angedeuteten Galoiskorrespondenzen wurden hier nur als illustrierende Beispiel erwähnt. Genauer untersuchen werden wir in dieser Vorlesung zwei Beispiele: in diesem Kapitel die klassische Galoiskorrespondenz (siehe 9.2.1) sowie im letzten Kapitel den Hilbertschen Nullstellensatz (siehe 10.3).

**UE 474** ► **Übungsaufgabe 9.1.4.6.** Fallen Ihnen noch weitere interessante Beispiele von Galoiskorrespondenzen ein? Wenn ja erklären Sie solche. Geben Sie insbesondere jeweils $X, Y$ und $R$ an und beschreiben Sie nach Möglichkeit die Galois-abgeschlossenen Elemente $\subseteq X$ und/oder $\subseteq Y$. ◄ **UE 474**

## 9.2 Galoissche Körpererweiterungen

Nach dem Studium allgemeiner Galoiskorrespondenzen in 9.1 wenden wir uns nun der klassischen Galoiskorrespondenz zu (siehe 9.2.1). Diese wird bei gegebener Körpererweiterung $K \leq E$ durch die Fixpunktrelation zwischen $K$-Automorphismen und Körperelementen von $E$ induziert. Die Erweiterung heißt Galoissch, wenn der Grundkörper $K$ bezüglich dieser Galoiskorrespondenz Galois-abgeschlossen ist. Ist dies der Fall, so lassen sich für algebraische Erweiterungen sehr schnell zwei Eigenschaften herleiten: normal und separabel (siehe 9.2.2). Beiden ist jeweils ein Unterabschnitt gewidmet (9.2.3 bzw. 9.2.4). Nur einzelne Ergebnisse von Abschnitt 9.2 sind für den Beweis des Hauptsatzes der Galoistheorie in Abschnitt 9.3 erforderlich. Trotzdem wurde (im Unterschied zu früheren Versionen des Skriptums) dieser Abschnitt als der weniger technische und stärker konzeptionell geprägte vorgezogen.

### 9.2.1 Die klassische Galoiskorrespondenz

Wie schon in der Einleitung erwähnt, geht es in der klassischen Galoistheorie um die Untersuchung von Körpererweiterungen $K \leq E$ mit gruppentheoretischen Methoden. Und zwar geht es um die Galoisgruppe, deren Elemente sogenannte $K$-Automorphismen von

$E$ sind, die definitionsgemäß $K$ punktweise fest lassen. Die $K$-Automorphismen bilden die Galoisgruppe. Die Galoiskorrespondenz wird von der Fixpunktrelation induziert. Es folgt eine Zusammenfassung dieser sowie unmittelbar daran anschließender Definitionen.

**Definition 9.2.1.1.** Sei $K \leq E$ eine Körpererweiterung. Unter einem *$K$-Automorphismus* von $E$ versteht man einen Automorphismus $\sigma \in \mathrm{Aut}(E)$ mit $\sigma(\alpha) = \alpha$ für alle $\alpha \in K$. Die Menge

$$G_K(E) = Aut_K(E) := \{\sigma \in \mathrm{Aut}(E) : \forall \alpha \in K\ \sigma(\alpha) = \alpha\}$$

aller $K$-Automorphismen von $E$ heißt die *Galoisgruppe* von $E$ über $K$.
Die von der Relation (*Fixpunktrelation*)

$$R := \{(\sigma, \alpha) \in G_K(E) \times E : \sigma(\alpha) = \alpha\}$$

auf $G_K(E) \times E$ induzierte Galoiskorrespondenz $(f_R, g_R)$ heißt die von der Erweiterung $K \leq E$ induzierte *(klassische) Galoiskorrespondenz*. Für die Wirkung von $f_R$ und $g_R$ auf Teilmengen $H \subseteq G_K(E)$ bzw. $Z \subseteq E$ schreiben wir vorzugsweise auch

$$f_R : \quad \mathrm{Aut}_K(E) \supseteq H \quad \mapsto \quad H' := \{\alpha \in E : \sigma(\alpha) = \alpha \text{ für alle } \sigma \in H\} \leq E$$

bzw.

$$g_R : \quad E \supseteq Z \quad \mapsto \quad Z' := \{\sigma \in Aut_K(E) : \sigma(\alpha) = \alpha \text{ für alle } \alpha \in Z\} \leq Aut_K(E).$$

Für $K \leq Z \leq E$ ist $Z'$ die *Galoisgruppe* von $E$ über $Z$, $H'$ heißt der *Fixpunktkörper* von $H$ (siehe auch Proposition 9.2.1.2).
Ein Körper $Z$ mit $K \leq Z \leq E$ heißt *Zwischenkörper* (bezüglich der Erweiterung $K \leq E$).
Die Körpererweiterung $K \leq E$ heißt *Galoissche Erweiterung*, und $E$ heißt *Galoissch* über $K$, wenn $K$ bezüglich der klassischen Galois-Korrespondenz Galois-abgeschlossen ist, d.h. wenn es zu jedem $\alpha \in E \setminus K$ ein $\sigma \in \mathrm{Aut}_K(E)$ mit $\sigma(\alpha) \neq \alpha$ gibt.[1]

Folgende einfache aber wichtige Beobachtungen halten wir fest:

**Proposition 9.2.1.2.** *Sei $K \leq E$ eine beliebige Körpererweiterung. Dann gilt mit den Notationen aus Definition 9.2.1.1:*

1. *Unter sämtlichen Automorphismen $\sigma \in \mathrm{Aut}(E)$ von $E$ sind die $K$-Automorphismen genau jene, die als Abbildungen des $K$-Vektorraumes $E$ auf sich selbst linear sind.*
2. *Ist $\sigma \in \mathrm{Aut}_K(E)$ und $f \in K[x]$, so gilt $\sigma(f(u)) = f(\sigma(u))$ für alle $u \in E$.*
3. *Die Galoisgruppe $\mathrm{Aut}_K(E)$ ist bezüglich der Komposition $\circ$ tatsächlich eine Gruppe.*
4. *Für eine (beliebige) Teilmenge $Z \leq E$ ist $Z' \leq \mathrm{Aut}_K(E)$.*

[1] Man erinnert sich an die Rolle der Punktetrennung zum Beispiel von Funktionen im Approximationssatz von Weierstraß oder von linearen Funktionalen in der Funktionalanalysis.

5. *Für eine (beliebige) Teilmengen $H \subseteq \mathrm{Aut}_K(E)$ ist $H'$ ein Zwischenkörper bezüglich der Erweiterung $K \leq E$, d.h. $K \leq H' \leq E$.*

6. *Bezeichne $K_1 := \mathrm{Aut}_K(E)'$ den Fixpunktkörper der Galoisgruppe $\mathrm{Aut}_K(E)$. Dann ist $K \leq K_1 \leq E$ und die Erweiterung $K_1 \leq E$ Galoissch mit Galoisgruppe $\mathrm{Aut}_{K_1}(E) = \mathrm{Aut}_K(E)$.*

**UE 475 ► Übungsaufgabe 9.2.1.3.** Beweisen Sie 9.2.1.2. **◄ UE 475**

Ein vertrautes Beispiel für die Begriffe aus Definition 9.2.1.1 ist die Körpererweiterung $K = \mathbb{R} \leq \mathbb{C} = E$. Aus Satz 1.2.4.3 folgt, dass die Galoisgruppe von $\mathbb{C}$ über $\mathbb{R}$ zwei Elemente hat, die Identität und die komplexe Konjugation. Die komplexe Konjugation lässt nur die Elemente des Grundkörpers $\mathbb{R}$ fest. Also ist $\mathbb{R} \leq \mathbb{C}$ eine Galoissche Erweiterung. Als zweielementige Gruppe hat die Galoisgruppe $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$ genau zwei Untergruppen, nämlich die einelementige Gruppe $\{\mathrm{id}_{\mathbb{C}}\}$ mit Fixpunktkörper $\mathbb{C}$ und sich selbst mit Fixpunktkörper $\mathbb{R}$. Bezüglich dieser Erweiterung gibt es genau zwei Zwischenkörper, nämlich die zugehörigen Fixpunktkörper $\{\mathrm{id}_{\mathbb{C}}\}' = \mathbb{C}$ und $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})' = \mathbb{R}$. Offenbar gilt auch $\mathbb{C}' = \{\mathrm{id}_{\mathbb{C}}\}$ und $\mathbb{R}' = \mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$.
Nicht Galoissch ist hingegen die Erweiterung $\mathbb{Q} \leq \mathbb{R}$. Laut Korollar 3.5.3.14 ist nämlich die Identität der einzige Automorphismus des Körpers $\mathbb{R}$, die Galoisgruppe $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{R})$ also einelementig.
Dass eine durch die Fixpunktrelation induzierte bijektive Galoiskorrespondenz zwischen den (abgeschlossenen) Untergruppen und den Zwischenkörpern wie im Beispiel $\mathbb{R} \leq \mathbb{C}$ ganz allgemein für jede algebraische Galoissche Erweiterung besteht, ist die wichtigste Aussage des Hauptsatzes der Galoistheorie 9.3.1.1 bzw. 9.3.4.2.

Wir wollen noch eine wichtige Folgerung aus der $K$-Linearität von $K$-Automorphismen von $E$ (siehe Aussage 1 in Proposition 9.2.1.2) ziehen, die wir sehr häufig verwenden werden. Sie lässt sich als Verallgemeinerung der bekannten Tatsache interpretieren, dass für jede komplexe Nullstelle $\alpha$ eines reellen Polynoms auch die konjugiert komplexe Zahl eine Nullstelle desselben Polynoms ist.

**Proposition 9.2.1.4.** *Sei $K \leq E$ eine Körpererweiterung mit Galoisgruppe $\mathrm{Aut}_K(E)$, $f \in K[x]$ ein Polynom über $K$ und $N$ die Menge aller Nullstellen von $f$ in $E$. Dann ist die Einschränkung $\sigma|_N$ jedes Automorphismus $\sigma \in \mathrm{Aut}_K(E)$ auf $N$ eine Permutation von $N$.*

*Beweis.* Sei $f(x) = \sum_{i=0}^{n} a_i x^i$. Wegen $f \in K[x]$ ist $a_i \in K$ für alle $i = 0, \ldots, n$. Ist $\alpha \in N$, also $f(\alpha) = 0$, so folgt aus der $K$-Linearität von $\sigma$ (siehe 9.2.1.2, Aussage 2):

$$f(\sigma(\alpha)) = \sum_{i=1}^{n} a_i \sigma(\alpha) = \sigma\left(\sum_{i=1}^{n} a_i \alpha\right) = \sigma(f(\alpha)) = \sigma(0) = 0.$$

Also ist $\sigma(\alpha) \in N$ und somit, weil $\alpha \in N$ beliebig war, $\sigma(N) \subseteq N$. Als Automorphismus ist $\sigma$ injektiv ist. Erst recht gilt das für die Einschränkung $\sigma|_N : N \to N$. Auf der

endlichen Menge $N$ zieht die Injektivität dieser Abbildung sogar Bijektivität nach sich. Insgesamt ist $\sigma|_N$ also eine Permutation von $N$. □

Somit liegt es in vielen Situationen nahe, Galoisgruppen als Permutationsgruppen auf endlichen Mengen zu interpretieren, was die Analyse vor allem bei endlichdimensionalen Erweiterungen in mancherlei Hinsicht einfacher machen kann. In 9.4 wird das der vorherrschende Standpunkt sein. Vorerst bevorzugen wir aber die allgemeine, abstrakte Sichtweise.

Wie bereits erwähnt, gilt der Hauptsatz der Galoistheorie nur für algebraische Galoissche Erweiterungen. Zwar ist es wegen Aussage 6 aus Proposition 9.2.1.2 bei einer beliebig vorgegebenen Körpererweiterung $K \leq E$ stets möglich, zu einer Galoisschen überzugehen, indem man den Grundkörper $K$ durch den Fixpunktkörper $K_1 := \mathrm{Aut}_K(E)'$ ersetzt. Auch führt dieser Schritt wieder zu einer algebraischen Erweiterung $K_1 \leq E$, sofern $K \leq E$ algebraisch ist. Trotzdem ist es von Interesse, Bedingungen dafür zu kennen, dass bereits $K \leq E$ Galoissch ist, also $K = K_1$ gilt.

### 9.2.2 Galoissch und algebraisch impliziert normal und separabel

Fragt man sich, ob eine Körpererweiterung $K \leq E$ Galoissch ist, hat man zu überlegen, ob es zu jedem $u \in E$ ein $\sigma \in \mathrm{Aut}_K(E)$ gibt mit $\sigma(u) \neq u$. Ist $u$ algebraisch über $K$ mit Minimalpolynom $f$, so kommen für $\sigma(u)$ laut Proposition 9.2.1.4 nur Nullstellen von $f$ in Frage. Enthält $E$ nur $u$ als einzige Nullstelle von $E$, so werden wir also sicher kein $\sigma(u) \neq u$ finden, und die Erweiterung ist sicher nicht Galoissch.
Auf den ersten Blick fallen zweierlei mögliche Gründe für diese Situation ins Auge: Es kann erstens sein, dass $E$ nicht sämtliche Nullstellen von $f$ enthält, oder dass $u$ in seinem Zerfällungskörper die einzige, also eine mehrfache Nullstelle von $f$ ist. Das folgende Resultat zeigt, dass so etwas bei Galoisschen Erweiterungen tatsächlich nicht auftreten kann.

**Proposition 9.2.2.1.** *Sei $K \leq E$ eine Galoissche Erweiterung, $u \in E$ algebraisch über $K$ und $f \in K[x]$ das Minimalpolynom von $u = u_1 \in E$. Dann zerfällt*

$$f(x) = \prod_{i=1}^{r}(x - u_i)$$

*über $E$ mit lauter verschiedenen Nullstellen $u_i \in E$.*

*Beweis.* Seien $u = u_1, u_2, \ldots, u_r$ sämtliche paarweise verschiedenen Wurzeln von $f$ in $E$. Insbesondere ist $\mathrm{grad}(f) \geq r$. (A priori muss $E$ keinen Zerfällungskörper von $f$ enthalten!) Wir definieren

$$g(x) := \prod_{i=1}^{r}(x - u_i) = \sum_{j=0}^{r} a_j x^j$$

Die $a_j$ sind bis auf das Vorzeichen die elementarsymmetrischen Polynome in den $u_i$. Alle $\tau \in Aut_K(E)$ permutieren die $u_i$ (Proposition 9.2.1.4), lassen also die $a_j$ und somit $g$

invariant, also gilt $a_i \in (Aut_K(E))' = K$, weil $K \leq E$ Galoissch ist. Es folgt $g \in K[x]$. Nach Voraussetzung ist $f$ das Minimalpolynom von $u$ über $K$. Wegen $g(u) = 0$ bedeutet das $f \mid g$. Da außerdem $\text{grad}(g) = r \leq \text{grad}(f)$ und $f$ wie auch $g$ normiert sind, folgt $f = g$. □

Proposition 9.2.2.1 motiviert zu den Definitionen 9.2.2.2 und 9.2.2.4:

**Definition 9.2.2.2.** Eine algebraische Körpererweiterung $K \leq E$ heißt *normal*, falls jedes irreduzible $f \in K[x]$ mit einer Nullstelle in $E$ sogar in Linearfaktoren über $E$ zerfällt.

Aus Proposition 9.2.2.1 folgt daher unmittelbar:

**Proposition 9.2.2.3.** *Ist die algebraische Körpererweiterung $K \leq E$ Galoissch, so ist sie auch normal.*

Die zweite Definition, zu der Proposition 9.2.2.1 Anlass gibt, lautet:

**Definition 9.2.2.4.** Ein Polynom $f \in K[x]$ heißt *separabel* über $K$, falls alle Nullstellen von $f$ im Zerfällungskörper von $f$ über $K$ einfach sind. Ist $E$ eine beliebige Körpererweiterung von $K$, so heißt ein Element $u \in E$ *separabel* über $K$, falls $u$ algebraisch ist über $K$ mit separablem Minimalpolynom. Die Körpererweiterung $K \leq E$ selbst heißt *separable Erweiterung*, falls alle $u \in E$ separabel über $K$ sind.
Ein Polynom $f \in K[x]$ heißt *(rein) inseparabel*, falls es im Zerfällungskörper $Z$ von der Form $f(x) = a(x-u)^n$ mit $a, u \in Z$ und $n \in \mathbb{N}$ ist. Ist $E$ eine beliebige Körpererweiterung von $K$, so heißt ein Element $u \in E$ *inseparabel* über $K$, falls $u$ algebraisch ist über $K$ mit inseparablem Minimalpolynom. Die Körpererweiterung $K \leq E$ selbst heißt *inseparable Erweiterung*, falls alle $u \in E$ inseparabel über $K$ sind.

Man beachte: Elemente des Grundkörpers $K$ sind sowohl separabel als auch inseparabel über $K$, während es für Elemente aus $E \setminus K$ auch möglich ist, keine der beiden Eigenschaften zu haben. „Inseparabel“ ist also nicht die Negation von „separabel“.

Separabilität betreffend entnehmen wir Proposition 9.2.2.1 ebenfalls unmittelbar:

**Proposition 9.2.2.5.** *Ist die algebraische Körpererweiterung $K \leq E$ Galoissch, so ist sie auch separabel.*

Wir fassen das Wichtigste zusammen: Für algebraische Körpererweiterungen $K \leq E$ folgen aus „Galoissch“ die Eigenschaften „normal“ und „separabel“. Es wird sich zeigen, dass auch umgekehrt für algebraische Körpererweiterungen „Galoissch“ aus „normal und separabel“ folgt. Um das zu sehen, wollen wir die beiden Eigenschaften „normal“ und „separabel“ besser verstehen.

### 9.2.3 Normale Erweiterungen

Genauere Beschreibungen normaler Erweiterungen ergeben sich aus der folgenden Äquivalenz.

**Satz 9.2.3.1.** *Sei $K \leq E$ eine algebraische Körpererweiterung. Dann sind äquivalent:*

*(i)* $K \leq E$ *ist normal.*

*(ii)* $E$ *ist Zerfällungskörper einer Menge* $S \subseteq K[x]$ *von Polynomen über* $K$*.*

*(iii) Bezeichne* $\overline{K}$ *einen algebraischen Abschluss von* $K \leq E \leq \overline{K}$ *und* $\sigma\colon E \to \overline{K}$ *irgendeine isomorphe Einbettung von* $E$ *in* $\overline{K}$*, die* $K$ *punktweise fest lässt. Dann ist* $\operatorname{Im}\sigma = E$*, d.h.* $\sigma \in Aut_K(E)$*.*

*Beweis.* (i) $\Rightarrow$ (ii): Sei $S$ die Menge aller irreduziblen Polynome über $K$, die in $E$ wenigstens eine Nullstelle haben. Wir behaupten, dass $E$ ein Zerfällungskörper von $S$ über $K$ ist. Weil $E$ nach Voraussetzung (i) normal über $K$ ist, enthält $E$ sogar die Menge $N$ sämtlicher Nullstellen von Polynomen aus $f \in S$. Der von $K$ und $N$ erzeugte Unterkörper $Z \leq E$ ist also ein Zerfällungskörper von $S$ über $K$. Zu zeigen bleibt die umgekehrte Inklusion $E \leq Z$. Sei dazu $u \in E$ beliebig. Weil $E$ laut Generalvoraussetzung algebraisch über $K$ ist, gibt es ein Minimalpolynom $f \in K[x]$ von $u$. Wegen $f(u) = 0$ und weil $f$ als Minimalpolynom irreduzibel ist, liegt $f$ in $S$. Somit liegt $u$ auch im Zerfällungskörper $Z$ von $S$.

(ii) $\Rightarrow$ (iii): Sei $E$ Zerfällungskörper einer Menge $S \subseteq K[x]$, wobei wir o.B.d.A. alle $f \in S$ als irreduzibel voraussetzen dürfen. (Andernfalls ersetzen wir in $S$ reduzible $f$ durch ihre irreduziblen Faktoren.) Zum Beweis von (iii) haben wir uns eine isomorphe Einbettung $\sigma\colon E \to \overline{K}$ mit $\sigma|_K = \mathrm{id}_K$ vorzugeben. Für den Nachweis von $\operatorname{Im}\sigma = E$ zeigen wir die beiden Mengeninklusionen.
$\operatorname{Im}\sigma \subseteq E$: Sei $u \in \operatorname{Im}\sigma$. Dann gibt es ein $v \in E$ mit $\sigma(v) = u$. Als Zerfällungskörper von $S$ wird $E$ von den Wurzeln aller $f \in S$ erzeugt. Es gibt also endlich viele $f_i \in S$ und $v_i \in E$ mit $f_i(v_i) = 0$, $i = 1, \ldots, n$, so dass $v \in K(v_1, \ldots, v_n)$ und somit eine gebrochen rationale Funktion $g \in K(x_1, \ldots, x_n)$ über $K$ in $n$ Variablen mit $v = g(v_1, \ldots, v_n)$. Nach Proposition 9.2.1.4 sind auch die $\sigma(v_i)$ Wurzeln der $f_i \in S$, liegen also im Zerfällungskörper von $S$, der ja $E$ ist, also $\sigma(v_i) \in E$. Daraus folgt schließlich

$$u = \sigma(v) = \sigma(g(v_1, \ldots, v_n)) = g(\sigma(v_1), \ldots, \sigma(v_n)) \in E,$$

wobei in der zweiten Gleichheit verwendet wurde, dass $\sigma$ den Grundkörper $K$ elementweise fest lässt.
$E \subseteq \operatorname{Im}\sigma$: Der Beweis verläuft ähnlich zu dem der ersten Inklusion. Sei $u \in E$, dann gibt es endlich viele $f_i \in S$ und $u_i \in E$ mit $f_i(u_i) = 0$, $i = 1, \ldots, n$, so dass $u \in K(u_1, \ldots, u_n)$, d.h. $u = g(u_1, \ldots, u_n)$ mit einer gebrochen rationalen Funktion $g \in K(x_1, \ldots, x_n)$. Weil $E$ Zerfällungskörper von $S$ ist, liegen alle Wurzeln der $f_i \in S$ in $E$, und der Automorphismus $\sigma$ kann diese für jedes $i$ nur untereinander permutieren. Das bedeutet, dass es $v_i \in E$ gibt mit $\sigma(v_i) = u_i$. Auch das Element $v := g(v_1, \ldots, v_n)$ liegt in $E$. Folglich ist

$$u = g(u_1, \ldots, u_n) = g(\sigma(v_1), \ldots, \sigma(v_n)) = \sigma(g(v_1, \ldots, v_n)) = \sigma(v) \in \operatorname{Im}\sigma.$$

(iii) $\Rightarrow$ (i): Sei $f \in K[x]$ irreduzibel, $f(u) = 0$ mit $u \in E$ und $v \in \overline{K}$ mit $f(v) = 0$ eine weitere Wurzel von $f$. Zu zeigen ist $v \in E$. Weil die Erweiterung $K \leq E$ algebraisch

ist, gibt es wegen der Eindeutigkeit von Zerfällungskörpern (siehe 6.2.3) eine Einbettung $\sigma : E \to \overline{K}$ in den algebraischen Abschluss, die $K$ punktweise fest lässt und $u$ auf $v$ abbildet. Nach Voraussetzung (iii) ist daher tatsächlich $v = \sigma(u) \in \operatorname{Im}\sigma = E$. □

**UE 476** ► **Übungsaufgabe 9.2.3.2.** Rekapitulieren Sie ausführlich das Argument im Beweis der Implikation (iii) ⇒ (i) in Satz 9.2.3.1, wo auf 6.2.3 Bezug genommen wurde. ◄ **UE 476**

**UE 477** ► **Übungsaufgabe 9.2.3.3.** Zeigen Sie, dass die Relation *normal über* nicht transitiv ist, d.h. geben Sie Körper $K \leq Z \leq E$ an derart, dass $Z$ normal über $K$ ist, $E$ normal über $Z$, $E$ aber nicht normal über $K$. ◄ **UE 477**

Immer wieder hilfreich ist auch die Beobachtung, dass sich für eine Körpererweiterung $K \leq E$ die Eigenschaften normal und separabel auch auf $Z \leq E$ für Zwischenkörper $Z$ übertragen. Hier halten wir das für Normalität fest:

**Proposition 9.2.3.4.** *Sei $K \leq E$ eine algebraische Körpererweiterung und $Z$ ein Zwischenkörper, also $K \leq Z \leq E$. Ist $K \leq E$ normal, so auch $Z \leq E$.*

*Beweis.* Mit zweimaliger Hilfe von Satz 9.2.3.1 schließt man sehr schnell: Ist $K \leq E$ normal, so gibt es eine Menge $S \subseteq K[x] \subseteq Z[x]$, so dass $E$ Zerfällungskörper von $S$ über $K$ ist. Dann ist $E$ Zerfällungskörper von $S$ auch über $Z$ und somit normal über $Z$. □

Der Begriff der normalen Erweiterung legt den des normalen Abschluss nahe:

**Definition 9.2.3.5.** Seien $K \leq E \leq N$ Körpererweiterungen. $N$ heißt *normaler Abschluss* von $E$ über $K$, wenn $N$ normal über $K$ ist und minimal mit dieser Eigenschaft, d.h.: Für jede normale Erweiterung $E \leq N'$ mit $E \leq N' \leq N$ gilt $N' = N$ gilt.

Die folgenden Eigenschaften des normalen Abschluss sind mit Hilfe des Bisherigen, insbesondere mit Satz 9.2.3.1 leicht einzusehen:

**Proposition 9.2.3.6.** *Sei die Körpererweiterung $K \leq E$ algebraisch, $S \subseteq K[x] \subseteq E[x]$ die Menge aller irreduziblen Polynome über $K$, welche in $E$ wenigstens eine Nullstelle haben und $N := Z_S$ ein Zerfällungskörper von $S$ über $E$ mit $K \leq E \leq N$. Dann gilt:*

*(i) $N$ ist ein normaler Abschluss von $E$ über $K$.*

*(ii) $[N : K]$ ist genau dann endlich, wenn $[E : K]$ endlich ist.*

*(iii) Jeder normale Abschluss $N'$ von $E$ über $K$ ist $E$-isomorph zu $N$.*

*Insbesondere gibt es also stets einen normalen Abschluss.*

**UE 478** ► **Übungsaufgabe 9.2.3.7.** Beweisen Sie Proposition 9.2.3.6. Hinweis: Verwenden Sie Satz 9.2.3.1. ◄ **UE 478**

### 9.2.4 Separable Erweiterungen

Wir erinnern an die Rolle der formalen Ableitung $f'(x) := \sum_{k=1}^{n} k a_k x^{k-1}$ eines Polynoms $f(x) = \sum_{k=0}^{n} a_k x^k$ im Zusammenhang mit der Mehrfachheit von Nullstellen aus 6.2.4:

**Proposition 9.2.4.1.** *Sei $K$ ein Körper und $f \in K[x]$. Dann gilt:*

1. *Ist $K \leq E$ eine Körpererweiterung und $u \in E$, so ist $u$ genau dann eine mehrfache Nullstelle von $f$, wenn $f(u) = f'(u) = 0$.*
2. *Ein Polynom $f \in K[x]$ ist genau dann separabel, wenn $f$ und sein formale Ableitung $f'$ teilerfremd sind.*
3. *Ist $f \in K[x]$ irreduzibel, so ist $f$ genau dann separabel, wenn die Ableitung $f'$ nicht das Nullpolynom ist.*
4. *Hat $K$ die Charakteristik $\operatorname{char} K = 0$, so ist jedes irreduzible Polynom $f \in K[x]$ separabel.*
5. *Jede Körpererweiterung mit $\operatorname{char} K = \operatorname{char} E = 0$ ist separabel.*
6. *Hat $K$ die Primzahlcharakteristik $\operatorname{char} K = p \in \mathbb{P}$, so ist $f$ genau dann separabel, wenn es nicht von der Gestalt $f(x) = g(x^p)$ mit einem $g \in K[x]$ ist (also genau dann, wenn $f$ mindestens einen Koeffizienten $a_k \neq 0$ mit einem nicht durch $p$ teilbaren $k$ hat).*

**UE 479** ► **Übungsaufgabe 9.2.4.2.** Beweisen Sie Proposition 9.2.4.1. Hinweis: Rekapitulieren Sie 6.2.4. ◄ **UE 479**

Folgende unmittelbare Konsequenz wollen wir besonders hervorheben:

**Satz 9.2.4.3.** *Sei $K \leq E$ algebraisch. Dann ist $E$ genau dann Galoissch über $K$, wenn $E$ separabel und normal über $K$ ist.*

*Beweis.* Dass jede algebraische Galoissche Erweiterung normal und separabel ist, war Inhalt von 9.2.2.3 bzw. 9.2.2.5 (beides unmittelbare Folgerungen aus 9.2.2.1).
Wir nehmen nun umgekehrt an, dass die algebraische Erweiterung $K \leq E$ sowohl separabel als auch normal ist. Um zu zeigen, dass sie Galoissch ist, müssen wir für ein beliebiges $u \in E \setminus K$ ein $\sigma \in \operatorname{Aut}_K(E)$ finden mit $\sigma(u) \neq u$. Weil $E$ algebraisch über $K$ ist, hat $u$ ein Minimalpolynom $f \in K[x]$. Wegen $u \notin K$ hat $f$ Grad $\geq 2$. Weil $E$ normal über $K$ ist, enthält $E$ einen Zerfällungskörper $Z$ von $f$ mit $K \leq Z \leq E$, insbesondere sämtliche Nullstellen von $f$. Weil $K \leq E$ separabel ist, sind diese Nullstellen paarweise verschieden. Es gibt also ein $v \in E \setminus K$, $v \neq u$, mit $f(v) = 0$. Weil $u$ und $v$ dasselbe Minimalpolynom $f$ haben, gibt es nach 6.1.3.4 einen $K$-Isomorphismus $\sigma_0 : K(u) \cong K(v)$ mit $\sigma_0(u) = v$. Als normale Erweiterung von $K$ ist $E$ nach Satz 9.2.3.1 Zerfällungskörper einer Menge $S \subseteq K[x]$. Wegen Satz 6.2.3.1 (mit $K_1 = K_2 = Z$, $\varphi = \sigma_0$, $P_1 = P_2 = S$, $Z_1 = Z_2 = E$) lässt sich $\sigma_0$ zu einem Automorphismus $\sigma$ von $E$, also $\sigma \in \operatorname{Aut}_K(E)$ mit $\sigma(u) = v \neq u$ fortsetzen, womit der Satz bewiesen ist. □

Für Körper der Charakteristik 0 erhalten wir die einfache Folgerung:

**Folgerung 9.2.4.4.** *Ist $K$ ein Körper mit* $\operatorname{char} K = 0$*, so ist jede algebraische Erweiterung $K \leq E$ genau dann Galoissch, wenn sie normal ist.*

*Beweis.* Nach Satz 9.2.4.3 folgt normal aus Galoissch. Ist umgekehrt $K \leq E$ algebraisch und normal, so wegen $\operatorname{char} K = 0$ nach Proposition 9.2.4.1, Aussage 5, separabel, also nach Satz 9.2.4.3 auch Galoissch. □

Jeder endliche Körper $E = \mathrm{GF}(p^n)$, $p \in \mathbb{P}$, $n \in \mathbb{N}^+$, ist als Zerfällungskörper des Polynoms $f(x) = x^{p^n} - x$ über dem Primkörper $K = \mathrm{GF}(p)$ gemäß Satz 9.2.3.1 normal. Auf die Separabilität können wir wegen $\operatorname{char} K = p \neq 0$ nicht unmittelbar schließen. Dennoch gilt (Beweis Übung):

**Theorem 9.2.4.5.** Sei $K \leq E$ eine Körpererweiterung mit endlichem $E$, so ist die Erweiterung Galoissch.

**UE 480** ► **Übungsaufgabe 9.2.4.6.** Beweisen Sie Theorem 9.2.4.5. Hinweis: Neben Satz 9.2.4.3 genügt die Theorie aus 6.3. ◄ **UE 480**

Folgende Frage ist noch offen: Erzeugt die Adjunktion separabler Elemente auch separable Körpererweiterungen? Die Antwort lautet „ja“. Das wird sich als Folgerung 9.2.4.8 aus der folgenden für sich sehr interessanten Charakterisierung Galoisscher Erweiterungen ergeben, die als Pendant des entsprechenden Satzes 9.2.3.1 über normale Erweiterungen aufgefasst werden kann:

**Satz 9.2.4.7.** *Eine algebraische Körpererweiterung $K \leq E$ ist Galoissch genau dann, wenn $E$ der Zerfällungskörper einer Menge $S \subseteq K[x]$ separabler Polynome ist.*

*Beweis.* (Clemens Schindler) Ist die algebraische Erweiterung $K \leq E$ Galoissch, so nach Satz 9.2.4.3 normal, woraus nach Satz 9.2.3.1 folgt, dass $E$ Zerfällungskörper einer Menge $S_0 \subseteq K[x]$ von Polynomen über $K$ ist. Sei $S$ die Menge aller irreduziblen Faktoren von Polynomen aus $S_0$. Dann ist $E$ auch Zerfällungskörper von $S$. Nochmals wegen Satz 9.2.4.3 ist $K \leq E$ als algebraische und Galoissche Erweiterung auch separabel, was nur möglich ist, wenn alle $f \in S$ separabel sind.

Sei nun umgekehrt vorausgesetzt, dass $E$ Zerfällungskörper einer Menge $S$ separabler Polynome ist, die wir o.B.d.A. als irreduzibel (Argument wie im ersten Teil des Beweises), normiert und vom Grad $\geq 2$ annehmen dürfen. Der Beweis des Satzes ist erbracht, wenn wir für ein beliebiges $u \in E \setminus K$ ein $\sigma \in \mathrm{Aut}_K(E)$ mit $\sigma(u) \neq u$ konstruieren können. Zunächst gehen wir ähnlich vor wie an der entsprechenden Stelle im Beweis von Satz 9.2.3.1: Als Zerfällungskörper wird $E$ von den Wurzeln sämtlicher $f \in S$ erzeugt, wobei für jedes Element von $E$ nur endlich viele nötig sind. Speziell für $u$ gibt es also endlich viele $v_1, \ldots, v_n \in E$ mit $u \in K(v_1, \ldots, v_n)$ und zugehörige Minimalpolynome $f_i \in S$ für die $v_i$. Wir dürfen annehmen, dass die $v_i$ so gewählt sind, dass ihre Anzahl $n$ minimal ist. Wir führen den Beweis mittels Induktion nach $n$.

Für $n = 0$ wäre $u \in K$, Widerspruch. In diesem Fall ist also nichts zu zeigen.
Sei $n = 1$, also $u \in K(v)$ mit $v = v_1$ und $f \in S$ das Minimalpolynom von $v$. Weil $E$ Zerfällungskörper von $S$ ist und $f \in S$ separabel, zerfällt $f$ über $E$ in paarweise verschiedene Linearfaktoren

$$f(x) = \prod_{j=1}^{m} (x - \alpha_j),$$

$\alpha_j \in E$, $\alpha_1 = v$, wobei $m \geq 2$ der Grad von $f$ ist. Nach Aussage 2 in 6.1.3.4 ist jedes Element aus $K(v)$ darstellbar als Polynom in $v$ mit Koeffizienten aus $K$ und einem Grad $< m$. Speziell sei

$$u = p_u(v) \quad \text{mit} \quad p_u(x) = \sum_{j=0}^{m-1} b_j x^j, \quad b_j \in K.$$

Wieder ähnlich wie im Beweis von Satz 9.2.4.3 schließen wir: Die einfachen Erweiterungen $K(\alpha_i)$ sind nach 6.1.3.4 alle zueinander $K$-isomorph, und jeder Isomorphismus dieser Art lässt sich nach Satz 6.2.3.1 zu einem Automorphismus des Zerfällungskörpers $E$ fortsetzen. Insbesondere gibt es für jedes $j = 1, \ldots, m$ ein $\sigma_j \in \mathrm{Aut}_K(E)$ mit $\sigma_j(v) = \alpha_j$. Wir wollen zeigen, dass wenigstens eines der $\sigma_j$ das Element $u$ nicht auf sich selbst abbildet. Wir gehen indirekt vor, indem wir $\sigma_j(u) = u$ für alle $j = 1, \ldots, m$ annehmen. Wir betrachten das Polynom $g(x) := p_u(x) - u \in E[x]$. Wegen $p_u \in K[x]$ und $u \notin K$ ist $g$ nicht das Nullpolynom und hat einen Grad $< m$. Für $j = 1, \ldots, m$ gilt

$$g(\alpha_j) = p_u(\alpha_j) - u = p_u(\sigma_j(v)) - u = \sigma_j(p_u(v)) - u = \sigma_j(u) - u = u - u = 0.$$

Also hat das Polynom $g \neq 0$ mehr Nullstellen als sein Grad beträgt, Widerspruch. Folglich gibt es ein $\sigma \in \mathrm{Aut}_K(E)$ mit $\sigma(u) \neq u$.
Induktionsschritt von $n$ auf $n + 1$: Es gelte die Induktionsvoraussetzung, dass für je $n$ Nullstellen $v_i \in E$ von irreduziblen Polynomen $f_i \in S$ auch die Erweiterung $K(v_1, \ldots, v_n)$ separabel ist. Wir haben die Separabilität von $u \in K(v_1, \ldots, v_n, v_{n+1})$ zu zeigen. Dabei ist $n + 1$ die minimale Anzahl von Nullstellen gewisser $f_i \in S$, die über $K$ das Element $u$ erzeugen, d.h. für die es ein gebrochen rationales $g \in K(x_1, \ldots, x_{n+1})$ mit $u = g(v_1, \ldots, v_{n+1})$ gibt (siehe 6.1.3.3). Wegen der Minimalität von $n + 1$ ist $u \notin K_0 := K(v_{n+1})$. $E$ ist Zerfällungskörper von $S$ auch über $K_0$ und $u \in K_0(v_1, \ldots, v_n)$. Da wir über den Grundkörper keine speziellen Voraussetzungen gemacht haben und die $v_i$ erst recht über $K_0$ separabel sind, können wir die Induktionsvoraussetzung auch auf $K_0$ statt auf $K$ anwenden. Also gibt es ein $\sigma \in \mathrm{Aut}_{K_0}(E) \subseteq \mathrm{Aut}_K(E)$ mit $\sigma(u) \neq u$. □

Hieraus schließen wir:

**Folgerung 9.2.4.8.** *Sei $K \leq E$ eine Körpererweiterung, und enthalte $T \subseteq E$ ausschließlich über $K$ separable Elemente. Dann ist auch die von $T$ erzeugte Erweiterung $K(T)$ von $K$ separabel über $K$.*

*Beweis.* Jedes $t \in T$ ist separabel über $K$, folglich algebraisch und hat deshalb ein separables Minimalpolynom $f_t \in K[x]$. Wir erweitern $E$ zu einem algebraischen Abschluss $\overline{E}$. Dieser enthält einen Zerfällungskörper $Z$ der Menge $S$ aller $f_t$, $t \in T$. Es gilt

$K \leq K(T) \leq Z$. Nach Satz 9.2.4.7 ist $Z$ und damit erst recht $K(T)$ separabel über $K$. □

Außerdem gilt analog zu Proposition 9.2.3.4 über Normalität auch die analoge Aussage für Separabilität und Galoissch:

**Proposition 9.2.4.9.** *Sei $K \leq E$ eine algebraische Körpererweiterung und $Z$ ein Zwischenkörper, also $K \leq Z \leq E$. Dann gilt:*

1. *Ist $K \leq E$ separabel, so ist auch $Z \leq E$ separabel.*
2. *Ist $K \leq E$ Galoissch, so ist auch $Z \leq E$ Galoissch.*

*Beweis.*
1. Sei $K \leq E$ separabel und $u \in E$ beliebig. Weil $K \leq E$ algebraisch ist, gibt es ein Minimalpolynom $f_K$ von $u$ über $K$. Nach Voraussetzung ist $f_K$ separabel. Das Minimalpolynom $f_Z$ von $u$ über $Z$ ist im Polynomring $Z[x]$ ein Teiler von $f_K$, also ebenfalls separabel. Somit ist $u$ auch separabel über $Z$.
2. Ist $K \leq E$ Galoissch, so nach Satz 9.2.4.3 sowohl separabel als auch normal. Daher ist nach Aussage 1 auch $Z \leq E$ separabel, nach Proposition 9.2.3.4 normal, wieder nach Satz 9.2.4.3 also auch Galoissch. □

**UE 481** ► **Übungsaufgabe 9.2.4.10.** Beweisen Sie den Satz vom primitiven Element 6.2.6.1 für beliebige Charakteristik, jedoch unter der Voraussetzung, dass die Erweiterung separabel ist: Jede endlichdimensionale und separable Körpererweiterung $K \leq E$ ist einfach, d.h. es gibt ein $u \in E$ mit $E = K(u)$. ◄ **UE 481**

## 9.3 Der Hauptsatz der Galoistheorie

Der Hauptsatz der Galoistheorie besagt im Fall endlichdimensionaler Galoisscher Körpererweiterungen, dass die Galois-abgeschlossenen Elemente genau die Untergruppen bzw. die Zwischenkörper sind. Darüber hinaus macht er noch interessante Aussagen über Dimension und Index sowie darüber, welche Untergruppen sogar Normalteiler sind. Die genaue Formulierung ist Gegenstand von 9.3.1. Die wichtigste technische Hürde wird mit dem Beweis zweier Ungleichungen über Dimension und Index in 9.3.2 genommen. Zusammen mit einigen weiteren Überlegungen über stabile Zwischenkörper gelingt damit in 9.3.3 der Beweis des Hauptsatzes für den endlichdimensionalen Fall. Verzichtet man auf Endlichdimensionalität, so sind bei Galoisschen Erweiterungen zwar weiterhin alle Zwischenkörper Galois-abgeschlossen, jedoch nicht mehr alle Untergruppen, sondern nur mehr jene, die abgeschlossen bezüglich einer natürlich auftretenden Topologie sind. Das ist Gegenstand von 9.3.4. Zwei interessante Korollare des Hauptsatzes für den endlichdimensionalen Fall (endliche Körper sind als Erweiterungen immer Galoissch und ein galoistheoretischer Beweis des Fundamentalsatzes der Algebra) bilden in 9.3.5 den Abschluss von Abschnitt 9.3.

### 9.3.1 Formulierung des Hauptsatzes für endlichdimensionale Erweiterungen

Die wichtigste Aussage des Hauptsatzes der Galoistheorie besteht in der Beschreibung der Galois-abgeschlossenen Elemente auf beiden Seiten der klassischen Galoiskorrespondenz. Sei dazu $K \leq E$ eine Körpererweiterung. Bei den in Definition 9.2.1.1 auftretenden Teilmengen $H' \subseteq E$ handelt es sich stets um Zwischenkörper, bei den $Z' \subseteq G$ um Untergruppen von $G_K(R)$ (siehe Proposition 9.2.1.2, Aussage 5 bzw. 4).
Die naheliegende Frage lautet, ob *alle* $H \leq \mathrm{Aut}_K(E)$ bzw. *alle* Zwischenkörper $Z$ Galois-abgeschlossen sind, d.h. ob sie $H'' = H$ und $Z'' = Z$ erfüllen.
Eine trivialerweise notwendige Bedingung dafür ist die Galois-Abgeschlossenheit wenigstens von $K$ selbst. Nach Definition 9.2.1.1 ist das gerade die definierende Bedingung dafür, dass man die Erweiterung $K \leq E$ Galoissch nennt.
Das wichtigste Ziel dieses Abschnitts ist der Beweis des Hauptsatzes der Galoistheorie. Für endlichdimensionale Erweiterungen besagt er, dass in diesem Fall die notwendige Bedingung auch hinreichend ist: In der Galoiskorrespondenz für eine endlichdimensionale und Galoissche Erweiterung sind alle Untergruppen und alle Zwischenkörper Galois-abgeschlossen. Darüber charakterisiert der Hauptsatz unter den Untergruppen die Normalteiler dadurch, dass sie selbst Galoisschen Erweiterungen des Grundkörpers entsprechen.
Zur Illustration für eine Situation mit $K \leq Z_1 \leq Z_2 \leq E$ (im allgemeinen Fall muss die Halbordnung der Zwischenkörper keine Kette bilden, immerhin aber einen Verband):

$$\begin{array}{ccc}
E & \longleftrightarrow & \{\mathrm{id}\} \\
\vdots & & \vdots \\
| \vee & & \wedge | \\
\vdots & & \vdots \\
H_2' = Z_2 & \overset{\widehat{=}}{\longleftrightarrow} & H_2 = Z_2' \\
\vdots & & \vdots \\
| \vee & & | \wedge \\
\vdots & & \vdots \\
H_1' = Z_1 & \overset{\widehat{=}}{\longleftrightarrow} & H_1 = Z_1' \\
\vdots & & \vdots \\
\vee | & & | \wedge \\
\vdots & & \vdots \\
K & \longleftrightarrow & G
\end{array}$$

Die qualitativen Aussagen des Hauptsatzes über die Galois-abgeschlossenen Elemente folgen aus quantitativen, nämlich aus den Identitäten zwischen einander entsprechenden Erweiterungsgraden und Gruppenindizes. In seiner ganzen Pracht lautet der Hauptsatz für endlichdimensionale Erweiterungen wie folgt.

**Satz 9.3.1.1** (Hauptsatz der Galoistheorie für endlichdimensionale Erweiterungen)**.** *Sei $K \leq E$ eine endlichdimensionale Galoissche Körpererweiterung und $G := \mathrm{Aut}_K(E)$ die Galoisgruppe von $E$ über $K$. Sei weiters*

$$\mathcal{Z} = \mathcal{Z}(K \leq E) := \{Z : \ K \leq Z \leq E\}$$

*die Menge aller Zwischenkörper von $K$ und $E$ sowie*

$$\mathrm{Sub}(G) := \{H : \ H \leq G\}$$

*die Menge aller Untergruppen von $G$. Dann gilt:*

*(a) Die Galois-abgeschlossenen Teilmengen von $E$ sind genau die Zwischenkörper $Z \in \mathcal{Z}$. Die Galois-abgeschlossenen Teilmengen von $G$ sind genau die Untergruppen $H \in \mathrm{Sub}(G)$. Insbesondere sind $Z \mapsto Z'$ und $H \mapsto H'$ zueinander inverse antitone Bijektionen zwischen $\mathcal{Z}$ und der Menge $Sub(G)$ der Untergruppen von $G$. Es gilt daher die Isomorphie*

$$(\mathcal{Z}, \subseteq) \cong (\mathrm{Sub}(G), \supseteq)$$

*von Halbordnungen.*

*(b) Ist $Z_1 \leq Z_2 \in \mathcal{Z}$, dann gilt sowohl*

$$\underbrace{[Z_2 : Z_1]}_{Grad} = \underbrace{[Z_1' : Z_2']}_{Index},$$

*also auch*

$$\underbrace{[H_2 : H_1]}_{Index} = \underbrace{[H_1' : H_2']}_{Grad}.$$

*für $H_1 \leq H_2 \leq G$.*

*(c) Für jedes $Z \in \mathcal{Z}$ ist $Z \leq E$ eine Galoissche Erweiterung.*

*(d) Für $Z \in \mathcal{Z}$ ist $K \leq Z$ genau dann eine Galoissche Erweiterung, wenn $Z'$ ein Normalteiler von $G$ ist. In diesem Fall ist $G/Z' \cong Aut_K(Z)$, wobei die Einschränkungsabbildung $\varphi : \sigma \mapsto \sigma|_Z$ ein surjektiver Homomorphismus $\varphi : \mathrm{Aut}_K(E) \to \mathrm{Aut}_K(Z)$ mit $\ker \varphi = \mathrm{Aut}_K(Z)$ ist.*

In Hinblick auf Aussage (b) des Hauptsatzes 9.3.1.1 erweist sich die Arbeit mit Erweiterungsgraden und Gruppenindizes als zielführend. Zwei Ungleichungen in Verbindung miteinander ermöglichen den entscheidenden Durchbruch.

### 9.3.2 Zwei Ungleichungen

Der technisch wesentliche Schritt im Beweis des Hauptsatzes der Galoistheorie besteht darin, die Dimension von Körpererweiterungen mit dem Index von Untergruppen in Beziehung zu setzen. Das ist in zwei Richtungen möglich, was sich in zwei Ungleichungen zwischen diesen beiden Größen manifestiert, die für beliebige Körpererweiterungen (Galoissch oder auch nicht) gelten. Aus beiden Ungleichungen gemeinsam folgen dann sehr rasch die ersten beiden Aussagen des Hauptsatzes. Zunächst zur Abschätzung von Erweiterungsdimension durch Gruppenindex:

**Lemma 9.3.2.1.** *Seien $K \leq Z_1 \leq Z_2 \leq E$ Körper und $[Z_2 : Z_1] < \infty$. Dann gilt*

$$[Z_1' : Z_2'] \leq [Z_2 : Z_1].$$

*Ist $K \leq E$ eine endlichdimensionale Erweiterung, so gilt $|Aut_K(E)| \leq [E : K]$.*

*Beweis.* Der Beweis erfolgt durch Induktion nach $n := [Z_2 : Z_1]$. Der Fall $n = 1$ ist trivial. Sei also $n > 1$ und gelte als Induktionsvoraussetzung (IV) die Behauptung für alle $i < n$. Sei $u \in Z_2 \setminus Z_1$ mit Minimalpolynom $f \in Z_1[x]$ vom Grad $k > 1$. Dann ist nach dem Gradsatz

$$[Z_1(u) : Z_1] = k \text{ und } [Z_2 : Z_1(u)] = \frac{n}{k}.$$

Ist $k < n$, so folgt

$$[Z_1' : Z_2'] = [Z_1' : Z_1(u)'] \cdot [Z_1(u)' : Z_2'] \overset{\text{IV}}{\leq} [Z_1(u) : Z_1] \cdot [Z_2 : Z_1(u)] = k \cdot \frac{n}{k} = n = [Z_2 : Z_1].$$

Im Fall $k = n$ ist $Z_1(u) = Z_2$. Wir konstruieren eine injektive Funktion $\varphi : S \to T$ von der Menge $S$ aller Linksnebenklassen von $Z_2'$ in $Z_1'$ in die Menge $T$ aller (verschiedenen) Wurzeln von $f$ in $E$ wie folgt:

$$\varphi : \tau Z_2' \mapsto \tau(u)$$

Wegen $\tau\sigma(u) = \tau(u)$ für alle $\sigma \in Z_2'$ hängt $\tau(u)$ nicht vom speziellen Repräsentanten $\tau$ der Linksnebenklasse $\tau Z_2'$ ab. Also ist $\varphi$ wohldefiniert. Wegen

$$\begin{aligned} \tau_1(u) = \tau_2(u) &\Rightarrow \tau_2^{-1}\tau_1(u) = u \\ &\Rightarrow \tau_2^{-1}\tau_1 \in Z_1(u)' = Z_2' \\ &\Rightarrow \tau_1 Z_2' = \tau_2 Z_2' \end{aligned}$$

ist $\varphi$ auch injektiv, und es folgt $[Z_1' : Z_2'] = |S| \leq |T| \leq n = [Z_2 : Z_1]$.

Für den Beweis der letzten Aussage des Lemmas ist lediglich speziell $Z_1 := K$ und $Z_2 := E$ zu setzen. Ist nämlich $K \leq E$ endlichdimensional, so ist die Voraussetzung $[Z_2 : Z_1] = [E : K] < \infty$ erfüllt. Somit liefert das bisher Bewiesene die Behauptung

$$|\operatorname{Aut}_K(E)| = [K' : E'] = [Z_1' : Z_2'] \leq [Z_2 : Z_1] = [E : K]. \quad \square$$

Und nun eine analoge Ungleichung in die umgekehrte Richtung:

**Lemma 9.3.2.2.** *Für die Körpererweiterung $K \leq E$ seien $H_1 \leq H_2 \leq \operatorname{Aut}_K(E)$ Untergruppen mit endlichem Index $[H_2 : H_1] < \infty$. Dann gilt*

$$[H_1' : H_2'] \leq [H_2 : H_1].$$

*Ist die Erweiterung Galoissch und $\operatorname{Aut}_K(E)$ endlich, so gilt $[E : K] \leq |\operatorname{Aut}_K(E)|$.*

*Beweis.* Sei indirekt $[H_1' : H_2'] > [H_2 : H_1] =: n$. Dann existieren $u_1, \ldots, u_{n+1} \in H_1'$, die linear unabhängig über $H_2'$ sind. Sei $\{\tau_1, \ldots, \tau_n\}$ ein vollständiges Vertretersystem für die Linksnebenklassen von $H_1$ in $H_2$, von denen es definitionsgemäß $[H_2 : H_1] = n$ Stück gibt. Das homogene System

$$\sum_{j=1}^{n+1} \tau_i(u_j)x_j = 0,\ i = 1, \ldots, n \tag{9.1}$$

aus $n$ linearen Gleichungen mit den Koeffizienten $\tau_i(u_j) \in E$ in $n+1$ Unbekannten hat nichttriviale Lösungen. Sei $a = (a_1, \ldots, a_{n+1}) \in (H_1')^{n+1}$ eine solche und o.B.d.A. (d.h. nach eventueller Permutation der $j$)

$$a_1 = 1,\ a_2 \neq 0,\ a_3 \neq 0, \ldots, a_r \neq 0, a_{r+1} = 0, \ldots, a_{n+1} = 0$$

mit minimalem $r$. Wir werden ein $\sigma \in H_2$ konstruieren mit $\sigma(a_2) \neq a_2$, für welches $b := (b_1, \ldots, b_{n+1})$ mit $b_j := \sigma(a_j)$ ebenfalls Lösung von (**??**) ist. Das liefert eine weitere nichttriviale Lösung $c = (c_1, \ldots, c_{n+1}) := a - b$, $c_j := a_j - b_j$, mit

$$c_1 = 0,\ c_2 \neq 0,\ c_{r+1} = 0, \ldots, c_{n+1} = 0,$$

was einen Widerspruch zur Minimalität von $r$ ergibt.
Zur Konstruktion von $\sigma$:
Sei o.B.d.A. $\tau_1 \in H_1$, also $\tau_1(u_j) = u_j$ für $j = 1, \ldots, n+1$. Setzt man die Lösung $a = (a_1, \ldots, a_{n+1})$ im System (**??**) in die Gleichung für $i = 1$ ein, erhält man

$$u_1a_1 + \ldots + u_{n+1}a_{n+1} = 0.$$

Da die $u_j$ linear unabhängig über $H_2'$ sind, muss es ein $i$ geben mit $a_i \notin H_2'$. Sei o.B.d.A. $i = 2$. Daher existiert ein $\sigma \in H_2$ mit $\sigma(a_2) \neq a_2$. Wenden wir nun $\sigma$ auf (**??**) an, erhalten wir das System

$$\sum_{j=1}^{n+1} \sigma\tau_i(u_j)x_j = 0,\ i = 1, \ldots, n, \tag{9.2}$$

das klarerweise von $b_j := \sigma(a_j),\ j = 1, \ldots, n+1$ gelöst wird. Weil $\sigma \in H_2$ die Nebenklassen von $H_1$ permutiert, folgt

$$\{\sigma\tau_1H_1, \ldots, \sigma\tau_nH_1\} = \{\tau_1H_1, \ldots, \tau_nH_1\}$$

und wegen der Implikationskette

$$\rho_1H_1 = \rho_2H_1 \Rightarrow \rho_2^{-1}\rho_1 \in H_1 \overset{u_j \in H_1'}{\Rightarrow} \rho_2^{-1}\rho_1(u_j) = u_j \Rightarrow \rho_1(u_j) = \rho_2(u_j)$$

sind die beiden Systeme (9.1) und (9.2) bis auf die Reihenfolge der Gleichungen identisch. Daher bilden die $b_j$ auch eine Lösung für (**??**) und $\sigma$ erfüllt das Gewünschte.

Für die letzte Aussage ist speziell $H_1 := \{\mathrm{id}_E\}$ und $H_2 := \mathrm{Aut}_K(E)$ zu setzen. Für eine Galoissche Erweiterung gilt dann $H_2' = \mathrm{Aut}_K(E)' = K$, außerdem in jedem Fall $H_1' = E$. Ist die Galoisgruppe $\mathrm{Aut}_K(E)$ endlich, so liefert das bisher Bewiesene daher die Behauptung

$$[E : K] = [H_1' : H_2'] \leq [H_2 : H_1] = [\mathrm{Aut}_K(E) : \{\mathrm{id}_E\}] = |\,\mathrm{Aut}_K(E)|. \quad \square$$

### 9.3.3 Beweis des Hauptsatzes für endlichdimensionale Erweiterungen

Wir wollen nun die Voraussetzungen des Hauptsatzes 9.3.1.1 annehmen und die dortigen Bezeichnungen verwenden. Dann folgt, wie wir gleich sehen werden, die Behauptung (b) und damit auch (a) durch geschicktes Zusammensetzen der beiden Ungleichungen aus Lemma 9.3.2.1 und Lemma 9.3.2.2.
Zunächst ergibt sich für eine Galois-abgeschlossene Untergruppe $H_1 = H_1'' \leq G$ und $[H_2 : H_1] < \infty$ sofort

$$[H_2 : H_1] \leq [H_2'' : H_1] = [H_2'' : H_1''] \overset{9.3.2.1}{\leq} [H_1' : H_2'] \overset{9.3.2.2}{\leq} [H_2 : H_1].$$

Wegen $[H_2 : H_1] < \infty$ lassen sich die Ungleichungen zu Gleichungen zwischen Mengen verschärfen. Insbesondere folgt $H_2'' = H_2$, also ist mit $H_1$ auch $H_2$ Galois-abgeschlossen. Speziell ist $H_1 = \{\mathrm{id}\}$ aus trivialen Gründen Galois-abgeschlossen, folglich sind alle $H_2 \leq G$ Galois-abgeschlossen, außerdem $[H_2 : H_1] = [H_1' : H_2']$.
Analog schließt man für einen Galois-abgeschlossenen Zwischenkörper $Z_1$ mit $Z_1 \leq Z_2 \leq E$ auf die Galois-Abgeschlossenheit von $Z_2$ und auf $[Z_2 : Z_1] = [Z_1' : Z_2']$. Für eine Galoissche Erweiterung $K \leq E$ ist neben $H_1 = \{\mathrm{id}\}$ auch $Z_1 = K$ Galois-abgeschlossen, also tatsächlich sogar alle Zwischenkörper $Z \geq Z_1 = K$ und alle $H = H_2 \leq G$. Zusammen mit dem allgemeinen Satz 9.1.3.3 über allgemeine Galoiskorrespondenzen sind damit die Aussagen (a) und (b) aus dem Hauptsatz 9.3.1.1 bewiesen.
Auch Aussage (c) folgt damit fast unmittelbar: Ein beliebiger Zwischenkörper $Z$ ist laut (a) Galois-abgeschlossen, d.h. $Z'' = Z$. Explizit bedeutet das: Die Automorphismen $\sigma \in Z' \leq \mathrm{Aut}_K(E)$ haben *nur* die Elemente aus $Z$ als gemeinsame Fixpunkte, mit anderen Worten: Zu jedem $u \in E \setminus Z$ gibt es ein $\sigma \in Z' \subseteq \mathrm{Aut}_K(E)$ mit $\sigma(u) \neq u$. Definitionsgemäß ist also die Erweiterung $Z \leq E$ Galoissch.

Zu beweisen bleibt noch Aussage (d) im Hauptsatz, wonach für einen Zwischenkörper $Z$ einer Galoisschen Erweiterung $K \leq E$ die Erweiterung $K \leq Z$ genau dann Galoissch ist, wenn $Z' = \mathrm{Aut}_Z(E)$ ein Normalteiler der Galoisgruppe $\mathrm{Aut}_K(E)$ ist. Außerdem wird behauptet, dass in diesem Fall die Einschränkung $\varphi : \mathrm{Aut}_K(E) \to \mathrm{Aut}_K(Z)$, $\sigma \mapsto \sigma|_Z$ ein surjektiver Homomorphismus ist. Ist letzteres der Fall, so ist offenbar $\ker \varphi = \mathrm{Aut}_Z(E)$, und es folgt die Normalteilereigenschaft. Damit die Einschränkung wohldefiniert ist, müssen alle $\sigma \in \mathrm{Aut}_K(E)$ den Zwischenkörper $Z$ zwar nicht punktweise aber als Menge invariant lassen. Diese Eigenschaft wollen wir nun näher untersuchen.

**Definition 9.3.3.1.** Sei $K \leq E$ eine Körpererweiterung. Ein Zwischenkörper $Z$, $K \leq Z \leq E$, heißt *stabil* bezüglich $K$ und $E$, wenn $\sigma(Z) \subseteq Z$ für alle $\sigma \in Aut_K(E)$ gilt.

Die Nützlichkeit dieses Begriffs wird an den folgenden Aussagen deutlich:

**Lemma 9.3.3.2.** *Für eine Körpererweiterung $K \leq E$ und einen Zwischenkörper $Z$, $K \leq Z \leq E$ gilt:*

*(i) Ist $Z$ stabil bzgl. $K$ und $E$, so ist*

$$\varphi : Aut_K(E) \to Aut_K(Z)$$
$$\varphi : \sigma \mapsto \sigma|_Z$$

*wohldefiniert und ein Gruppenhomomorphismus mit* $\ker\varphi = Z' \lhd Aut_K(E)$. *Ist zusätzlich* $K \leq E$ *Galoissch, so ist auch* $K \leq Z$ *Galoissch.*

*(ii) Ist* $H \lhd Aut_K(E)$, *so ist* $H'$ *stabil bzgl.* $K$ *und* $E$.

*(iii) Ist* $K \leq Z$ *algebraisch und Galoissch, so ist* $Z$ *stabil bzgl.* $K$ *und* $E$. *Der Homomorphismus* $\varphi$ *aus Aussage (i) ist in diesem Fall surjektiv.*

*Beweis.* (i): Wohldefiniertheit: Bei der Einschränkung von $\sigma$ von $E$ auf $Z$ bleiben Injektivität und Homomorphiebedingung von $\sigma$ erhalten. Für die Wohldefiniertheit von $\varphi$ haben wir $\sigma(Z) = Z$ zu zeigen. Dann ist nämlich $\varphi(\sigma) = \sigma|_Z$ bijektiv auf $Z$, folglich ein Element von $\mathrm{Aut}_K(Z)$. Tatsächlich, die Stabilität von $Z$ zeigt, angewandt auf $\sigma \in \mathrm{Aut}_K(E)$, die Inklusion $\sigma(Z) \subseteq Z$ und, angewandt auf den inversen Automorphismus $\sigma^{-1} \in \mathrm{Aut}_K(E)$, auch $\sigma^{-1}(Z) \subseteq Z$. Somit ist auch $Z = \sigma(\sigma^{-1}(Z)) \subseteq \sigma(Z)$, insgesamt also $\sigma(Z) = Z$ bewiesen.
Homomorphieeigenschaft und Kern: Klarerweise gilt die Homomorphiebedingung

$$\varphi(\sigma\tau) = (\sigma\tau)|_Z = \sigma|_Z\ \tau|_Z = \varphi(\sigma)\varphi(\tau),$$

also ist $\varphi$ ein Gruppenhomomorphismus. Der Kern von $\varphi$ besteht offenbar genau aus jenen $\sigma \in Aut_K(E)$, die $Z$ punktweise fest lassen, stimmt folglich mit $Z'$ überein.
Ist $K \leq E$ Galoissch, so auch $K \leq Z$: Unter der Voraussetzung, dass $K \leq E$ Galoissch ist, müssen wir für ein beliebiges $u \in Z \setminus K$ ein $\sigma_Z \in \mathrm{Aut}_K(Z)$ mit $\sigma(u) \neq u$ finden. Laut Voraussetzung gibt es ein $\sigma \in \mathrm{Aut}_K(E) = \mathrm{Aut}_K(E)$ mit dieser Eigenschaft. Wegen der Stabilität von $Z$ und dem Bisherigen ist $\sigma_Z := \sigma|_Z \in \mathrm{Aut}_K(Z)$ und hat die gewünschte Eigenschaft.

(ii): Sei $H \lhd \mathrm{Aut}_K(E)$, $\sigma \in \mathrm{Aut}_K(E)$ und $u \in H'$. Zun zeigen ist dann $\sigma(u) \in H'$, d.h. $\tau(\sigma(u)) = \sigma(u)$ für alle $\tau \in H$. Wegen $H \lhd \mathrm{Aut}_K(E)$ ist $\sigma^{-1}\tau\sigma \in \sigma^{-1}H\sigma \subseteq H$, wegen $u \in H'$ also $\sigma^{-1}\tau\sigma(u) = u$, d.h. tatsächlich $\tau\sigma(u) = \sigma(u)$.

(iii): Stabilität von $Z$: Sei $u \in Z$. Nach Proposition 9.2.2.1 zerfällt das Minimalpolynom $f(x) = \prod_{i=1}^{r}(x - u_i)$ von $u = u_1$ über $K$ in Linearfaktoren mit paarweise verschiedenen $u_i \in Z$. Ist nun $\sigma \in \mathrm{Aut}_K(E)$, dann ist $\sigma(u)$ eine Wurzel von $f$, also $\sigma(u) = u_i$ für ein $i$ und somit $\sigma(u) \in Z$.
Surjektivität von $\varphi$: Mit $K \leq E$ ist nach Proposition 9.2.4.9 auch $Z \leq E$ Galoissch, nach Proposition 9.2.2.3 also normal. Somit ist $E$ Zerfällungskörper über $Z$ (siehe Satz 9.2.3.1), und jeder Isomorphismus $Z \to Z$ lässt sich nach Satz 6.2.3.1 zu einem Isomorphismus $E \to E$ fortsetzen. Das bedeutet insbesondere: Jedes Element aus $\mathrm{Aut}_K(Z)$ tritt als Bild $\varphi(\sigma)$ eines $\sigma \in \mathrm{Aut}_K(E)$ unter $\varphi$ auf. □

Lemma 9.3.3.2 enthält offenbar auch Aussage (d) im Hauptsatz 9.3.1.1. Damit ist der Hauptsatz der Galoistheorie für den Fall einer endlichdimensionalen Körpererweiterung vollständig bewiesen.

### 9.3.4 Der allgemeine Hauptsatz

Ist die algebraische Erweiterung $K \leq E$ unendlichdimensional, so gilt der Hauptsatz nicht mehr in seiner ursprünglichen Form, sehr wohl jedoch in einer geeigneten Modifikation. Wieder treten alle Zwischenkörper als Galois-abgeschlossene Mengen auf, aber nicht alle Untergruppen. Und zwar erweisen sich nur jene Untergruppen als Galois-abgeschlossen, die auch abgeschlossen sind bezüglich jener Topologie, die $\mathrm{Aut}_K(E)$ als Spurtopologie von der punktweisen Topologie (schwachen Topologie, Produkttopologie) auf $E^E$ erbt, siehe Proposition 7.1.1.9.

**Theorem 9.3.4.1.** Ist $K \leq E$ eine algebraische Körpererweiterung, so ist die Galoisgruppe $\mathrm{Aut}_K(E)$ bezüglich der schwachen Topologie eine kompakte Hausdorffgruppe.

*Beweis.* Nach Proposition 7.1.1.9 ist die symmetrische Gruppe $\mathrm{Sym}(E)$ aller Permutationen von $E$ eine topologische Hausdorffgruppe. Klarerweise vererben sich diese Eigenschaften auf Untergruppen. Also ist auch $\mathrm{Aut}_K(E) \leq \mathrm{Sym}(E)$ eine topologische Hausdorffgruppe. Zu zeigen bleibt die Kompaktheit.
Für jedes $u \in E$ bezeichne $C_u$ die endliche Menge aller Konjugierten von $u$, d.h. die Menge aller Nullstellen des Minimalpolynoms von $u$ über $K$. Jeder $K$-Automorphismus $\sigma \in \mathrm{Aut}_K(E)$ bildet $u$ auf ein Element aus $C_u$ ab, ist daher ein Element des Produktes $P := \prod_{u \in E} C_u \subseteq E^E$. Weil sämtliche $C_u$ endlich sind, ist dieses Produkt $P$ nach dem Satz von Tychonow kompakt. Wir sind fertig, wenn wir zeigen können, dass $\mathrm{Aut}_K(E)$ als Teilmenge von $P$ abgeschlossen ist. Wir beweisen das, indem wir für jedes $f \in P \setminus \mathrm{Aut}_K(E)$ eine Umgebung $U \subseteq P$ finden, die disjunkt ist zu $\mathrm{Aut}_K(E)$. Man beachte zunächst, dass für alle $u \in K$ die Menge $C_u = \{u\}$ einelementig ist, also jedes $f \in P$ den Grundkörper $K$ punktweise fest lässt. Damit bleiben nur drei Möglichkeiten, die alle denkbaren Fälle für ein $f \in P$, das kein $K$-Automorphismus ist, abdecken: nicht bijektiv, nicht mit der Addition verträglich, nicht mit der Multiplikation verträglich. Wir untersuchen diese drei Fälle.
Sei $f$ nicht bijektiv. Jedes Element von $P$ nimmt auf jeder der Mengen $C_u$ ausschließlich Werte aus $C_u$ an. Ist $f$ insgesamt nicht bijektiv, so ist die Bijektivität auf wenigstens einem der $C_u$ verletzt. Weil $C_u$ endlich ist, gibt es $u_1 \neq u_2 \in C_u$ mit $f(u_1) = f(u_2) =: v$. Die Menge $U$ aller $g \in P$ mit $g(u_1) = g(u_2) = v$ ist eine zu $\mathrm{Aut}_K(E)$ disjunkte Umgebung von $f$.
Sei $f$ nicht verträglich mit der Addition, d.h. es gibt Elemente $u_1, u_2$ mit $f(u_1 + u_2) \neq f(u_1) + f(u_2)$. Die Menge $U$ aller $g \in P$ mit $g(u) = f(u)$ für $u = u_1, u_2, u_1 + u_2$ ist eine zu $\mathrm{Aut}_K(E)$ disjunkte Umgebung von $f$.
Ist $f$ nicht verträglich mit der Multiplikation, so verläuft das Argument völlig analog wie bei der Addition. □

Der allgemeine Hauptsatz der Galoistheorie lautet:

**Satz 9.3.4.2.** *Die (nicht notwendig endlichdimensionale) Körpererweiterung $K \leq E$ sei algebraisch und Galoissch. Dann gilt:*

1. *$E$ ist Galoissch über jedem Zwischenkörper $Z$ mit $K \leq Z \leq E$.*

2. *Die Galois-abgeschlossenen Teilmengen von $E$ sind genau die Zwischenkörper $Z$ mit $K \leq Z \leq E$.*

3. *Die Galois-abgeschlossenen Teilmengen der Galoisgruppe $\mathrm{Aut}_K(E)$ sind genau die topologisch abgeschlossenen Untergruppen von $\mathrm{Aut}_K(E)$.*

4. *Ein Zwischenkörper $Z$ ist genau dann Galoissch über $K$, wenn $Z' \lhd \mathrm{Aut}_K(E)$ ein Normalteiler der Galoisgruppe ist. In diesem Fall ist $\mathrm{Aut}_K(Z) \cong K'/Z' = \mathrm{Aut}_K(E)/\mathrm{Aut}_Z(E)$.*

*Beweis.* Wir halten fest, dass $E$ über $K$ wegen Satz 9.2.4.3 normal und separabel über $K$ ist.

1. Die erste Behauptung des Satzes ist gerade die zweite Aussage aus Proposition 9.2.4.9.

2. Nach Aussage 5 in Proposition 9.2.1.2 kommen nur Zwischenkörper als Galois-abgeschlossene Mengen in Frage. Somit bleibt zu zeigen, dass jeder Zwischenkörper $Z$ mit $K \leq Z \leq E$ auch Galois-abgeschlossen ist. Das ist aber gerade die bereits bewiesene erste Behauptung.

3. Wir zeigen zunächst, dass jede Galois-abgeschlossene Menge $H \subseteq \mathrm{Aut}_K(E)$ eine topologisch abgeschlossene Untergruppe ist. Für jedes $u$ aus dem Fixpunktkörper sei $H_u = \{u\}'$ die Menge aller $\sigma \in \mathrm{Aut}_K(E)$ mit $\sigma(u) = u$. Klarerweise ist $H_u$ eine Untergruppe von $\mathrm{Aut}_K(E)$. Nach der Definition der Topologie auf $\mathrm{Aut}_K(E)$ ist $H_u$ aber auch topologisch abgeschlossen. Damit ist jeder Durchschnitt von gewissen $H_u$ eine abgeschlossene Untergruppe von $\mathrm{Aut}_K(E)$. Als Galois-abgeschlossene Menge ist $H$ aber gerade der Durchschnitt all jener $H_u$ mit $u \in H'$, dem Fixpunktkörper von $H$.

   Sei nun umgekehrt vorausgesetzt, dass $H \leq \mathrm{Aut}_K(E)$ topologisch abgeschlossen ist. Wir haben die Galois-Abgeschlossenheit von $H$ zu beweisen. Dazu müssen wir von einem beliebigen $\sigma \in H''$ ausgehen und zeigen, dass es in $H$ liegt. Weil $H$ nach Voraussetzung topologisch abgeschlossen ist, genügt der Nachweis, dass $\sigma$ im topologischen Abschluss $\overline{H}$ von $H$ liegt. Dazu ist die endliche Interpolationseigenschaft zu beweisen: Für jede endliche Teilmenge $T = \{u_1, \ldots, u_n\} \subseteq E$ gibt es ein $\sigma_T \in H$ mit $\sigma_T(u_i) = \sigma(u_i)$ für $i = 1, \ldots, n$. So ein $T$ sei nun vorgegeben. Weil $E$ algebraisch über $K$ ist, hat jedes $u_i$ ein Minimalpolynom $f_i \in K[x]$. Als Galoissche Erweiterung ist $E$ sogar normal und separabel über $K$, enthält mit den $u_i$ also einen (innerhalb $E$ eindeutigen) Zerfällungskörper $Z_S$ von $S := \{f_1, \ldots, f_n\}$, wobei die $f_i$ separabel sind. Auch $Z_S$ ist normal (nach Satz 9.2.3.1) und separabel (nach Satz 9.2.4.7) über $K$, nach Satz 9.2.4.3 also Galoissch. Nach Lemma 9.3.3.2 ist $Z_S$ stabil bezüglich $K$ und $E$, und die Einschränkung $\sigma_{Z_S} := \sigma|_{Z_S}$ eines jeden $\sigma \in \mathrm{Aut}_K(E)$ ist ein Element von $\mathrm{Aut}_K(Z_S)$. Die Einschränkungen der Elemente von $H$ bilden eine Untergruppe $H_{Z_S}$ von $\mathrm{Aut}_K(Z_S)$. $K_1 := H' \cap Z_S$ enthält jedenfalls $K$, die Erweiterung $K_1 \leq Z_S$ ist Galoissch (nach Proposition 9.2.4), außerdem

endlichdimensional, erfüllt also den Hauptsatz 9.3.1.1 für endlichdimensionale Erweiterungen. Aus diesem folgt, dass der Fixpunktkörper $K_1$ *nur* von den Elementen in $H_{Z_S}$ punktweise fest gelassen wird. Wegen $\sigma \in H''$ folgt daraus $\sigma_{Z_S} \in H_{Z_S}$. Also stimmt $\sigma$ auf ganz $Z_S$ mit einem Element von $H$ überein, insbesondere also auf den Elementen $u_1, \ldots, u_n \in Z_S$. Damit ist der Beweis der dritten Behauptung erbracht.

4. Die vierte Behauptung folgt wie im endlichdimensionalen Fall 9.3.1.1. □

Reizvoll ist auch die folgende Sichtweise auf algebraische Galoissche Körpererweiterungen $K \leq E$. Bezeichne $\mathcal{Z}_0$ das System aller Zwischenkörper $Z$, die gleichzeitig Zerfällungskörper $Z_S$ einer endlichen Menge $S \subseteq K[x]$ von Polynomen sind. Solche $Z$ sind normal über $K$ und stabil bezüglich aller $K$-Automorphismen von Erweiterungen. Umgekehrt lässt sich für $Z_1, Z_2 \in \mathcal{Z}_0$ mit $Z_1 \leq Z_2$ jedes $\sigma_1 \in \mathrm{Aut}_K(Z_1)$ zu einem $\sigma_2 \in \mathrm{Aut}_K(Z_2)$ fortsetzen. Somit liegt ein projektives System vor. Trägermenge ist $\mathcal{Z}_0$, und für $Z_1 \leq Z_2$ ist die Einschränkungsabbildung $\varphi_{Z_2,Z_1} : \mathrm{Aut}_K(Z_2) \to \mathrm{Aut}_K(Z_1)$, $\sigma_2 \mapsto \sigma_2|_{Z_1}$ ein wohldefinierter Epimorphismus. Zusammen mit den $\psi_Z : \mathrm{Aut}_K(E) \to \mathrm{Aut}_K(Z)$, $\sigma \mapsto \sigma|_Z$, $Z \in \mathcal{Z}_0$, ist $\mathrm{Aut}_K(E)$ ein projektiver Limes dieses Systems. Weil alle $Z \in \mathcal{Z}_0$ endlichdimensional über $K$ sind, sind auch alle $\mathrm{Aut}_K(Z)$ endlich. Eine Gruppe, die projektiver Limes endlicher Gruppen ist, nennt man *proendlich*[2]. Wir haben also im Wesentlichen bewiesen:

**Theorem 9.3.4.3.** Ist $E$ eine algebraische und Galoissche Erweiterung von $K$, so ist $\mathrm{Aut}_K(E)$ proendlich.

**UE 482** ► **Übungsaufgabe 9.3.4.4.** Skizzenhaft wurde der Beweis von Satz 9.3.4.3 bereits erbracht. Führen Sie alle Argumente sorgfältig aus. Diskutieren Sie auch, was sich ändert, wenn für die algebraische Erweiterung $K \leq E$ nur Normalität vorausgesetzt wird, möglicherweise aber Inseparabilitäten auftreten. ◄ **UE 482**

Die bereits in Satz 9.3.4.1 bewiesene Kompaktheit von Galoisgruppen algebraischer Erweiterungen ließe sich auch aus der Proendlichkeit schließen. Es gilt nämlich:

**Theorem 9.3.4.5.** Jede proendliche Gruppe ist kompakt. (Der projektive Limes ist dabei auch im Sinne der Topologie zu verstehen.)

**UE 483** ► **Übungsaufgabe 9.3.4.6.** Beweisen Sie Satz 9.3.4.5. ◄ **UE 483**

Von besonderem Interesse sind maximale algebraische Erweiterungen $K \leq E$. Dann ist $E$ ein algebraischer Abschluss von $K$. In diesem Fall heißt $\mathrm{Aut}_K(E)$ die *absolute Galoisgruppe* des Körpers $K$. Die absolute Galoisgruppe eines algebraisch abgeschlossenen Körpers $K$ ist trivial, die des Körpers $\mathbb{R}$ ist zweielementig, die von $\mathbb{Q}$ ist ziemlich schwer zu überschauen. Ein interessantes Beispiel zwischen uninteressant und undurchschaubar sind die endlichen Körper, die wir im nächsten Unterabschnitt betrachten wollen.

[2] Sprich: pro-endlich

### 9.3.5 Zwei Folgerungen aus dem Hauptsatz

Wir wollen nun aus dem Hauptsatz der Galoistheorie (es genügt jeweils die endlichdimensionale Version) folgern, dass Erweiterungen endlicher Körper stets Galoissch sind. Danach präsentieren wir einen galoistheoretischen Beweis des Fundamentalsatzes der Algebra.
Zunächst zu den endlichen Körpern. Aus Theorem 9.2.4.5 wissen wir bereits, dass es sich stets um Galoissche Erweiterungen handelt. Die Galoisgruppe hat die einfachst denkbare Struktur:

**Satz 9.3.5.1.** *Die Galoisgruppe einer Erweiterung $K \leq E$ endlicher Körper ist zyklisch.*

*Beweis.* Sei $|E| = p^n$ mit $p \in \mathbb{P}$ und positivem $n \in \mathbb{N}$ und $P \leq K \leq E$ der Primkörper. Wegen $\mathrm{Aut}_K(E) \leq \mathrm{Aut}_P(E)$ und Aussage 9 in Satz **??** genügt es zu, dass $\mathrm{Aut}_P(E)$ zyklisch ist, Weil die Erweiterung $P \leq E$ nach Theorem 9.2.4.5 Galoissch ist, darf der Hauptsatz 9.3.1.1 angewendet werden. Folglich gilt $|\mathrm{Aut}_P(E)| = [E : P] = n$. Jedes Gruppenelement kann als Ordnung maximal die Gruppenordnung haben. Somit genügt es in diesem Fall einen Automorphismus der Ordnung $n$ zu finden. Der sogenannte Frobeniusautomorphismus $\sigma \in \mathrm{Aut}_K(E)$, $\sigma : u \mapsto u^p$ hat die gewünschte Eigenschaft. Dass es sich um einen Automorphismus handelt, sieht man mit Hilfe der Rechenregel $(a+b)^p = a^p + b^p$ unmittelbar ein. Da jeder Automorphismus den Primkörper punktweise fest lässt, liegt $\sigma$ auch in $\mathrm{Aut}_P(E)$. Zu zeigen verbleibt, dass $\sigma$ eine Ordnung $k \geq n$ hat. Denn dann ist $\sigma$ notgedrungen erzeugendes Element der Galoisgruppe und diese zyklisch. Nun zum Beweis dieser Behauptung: Für alle $i \in \mathbb{N}$ und $u \in E$ gilt $\sigma^i(u) = u^{p^i}$, wie man mittels Induktion und unter Verwendung der Beziehung

$$\sigma^{i+1}(u) = \sigma(\sigma^i(u)) = \sigma(u^{p^i}) = \sigma(u)^{p^i} = (u^p)^{p^i} = u^{p^{i+1}}$$

sofort verifiziert. Wir setzen speziell $i = k$. Wegen $u^{p^k} = \sigma^k(u) = \mathrm{id}_E(u) = u$ sind alle $u \in E$ (davon gibt es $p^n$ viele) Nullstellen des Polynoms $x^{p^k} - x$, welches den Grad $p^k$ besitzt. Folglich ist $p^n \leq p^k$ und somit tatsächlich $n \leq k$, wie behauptet. $\mathrm{Aut}_P(E)$ ist also tatsächlich zyklisch. □

Damit lässt sich nunmehr auch die absolute Galoisgruppe eines endlichen Körpers recht gut verstehen. Das zu erklären ist Gegenstand der folgenden Übungsaufgabe.

**UE 484** ► **Übungsaufgabe 9.3.5.2.** Sei $K$ ein endlicher Körper mit $p^n$ Elementen, $p \in \mathbb{P}$, $n \in \mathbb{N}$, $n \geq 1$. Geben Sie eine möglichst transparente Beschreibung der absoluten Galoisgruppe von $K$. ◄ **UE 484**
Hinweis: Verwenden Sie Satz 9.3.5.1, außerdem die Ergebnisse aus 6.3.5 und 9.3.4. Behandeln Sie zunächst den Fall $n = 1$.

Ist eine Körpererweiterungen $K \leq E$ nicht separabel, so muss $E$ also erstens unendlich sein und zweitens, wegen Aussage 5 in Proposition 9.2.4.1, von Primzahlcharakteristik.

**UE 485** ▶ **Übungsaufgabe 9.3.5.3.** Finden Sie ein Beispiel einer normalen aber nicht separablen Körpererweiterung. Finden Sie sogar eine mit endlichem $K$? ◀ **UE 485**

Zur Einstimmung die Wiederholung einer Übungsaufgabe:

**UE 486** ▶ **Übungsaufgabe 9.3.5.4.** Beweisen Sie den Satz vom primitiven Element 6.2.6.1 für beliebige Chrarakteristik, jedoch unter der Voraussetzung, dass die Erweiterung separabel ist: Jede endlichdimensionale und separable Körpererweiterung $K \leq E$ ist einfach, d.h. es gibt ein $u \in E$ mit $E = K(u)$. ◀ **UE 486**

Der Fundamentalsatz der Algebra lautet bekanntlich:

**Satz 9.3.5.5.** *Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.*

*Beweis.* Wir skizzieren einen galoistheoretischen Beweis des Fundamentalsatzes der Algebra. Es genügt zu zeigen, dass $\mathbb{C}$ keine echte endlichdimensionale Körpererweiterung $E_1$ besitzt. Wir gehen also von $\mathbb{C} \leq E_1$ mit $[E_1 : \mathbb{C}] < \infty$ aus. Es gibt eine Galoissche Erweiterung $F$ von $\mathbb{R}$ mit $\mathbb{R} \leq \mathbb{C} \leq E_1 \leq F$ mit $d := [F : \mathbb{R}] < \infty$ (zum Beispiel den normalen Abschluss von $E_1$ über $\mathbb{R}$ (siehe Proposition 9.2.3.6). Wir wollen $F = \mathbb{C}$ zeigen. Sei dazu $G$ die Galoisgruppe von $F$ über $\mathbb{R}$. Nach dem Hauptsatz 9.3.1.1 ist $G$ endlich, und alle Untergruppen und Zwischenkörper sind Galois-abgeschlossen. Sei $|G| = 2^n k$ mit $k$ ungerade und $n \in \mathbb{N}$. Nach dem ersten Sylowsatz gibt es eine 2-Sylowgruppe $H \leq G$, d.h. eine Untergruppe der Ordnung $|H| = 2^n$. Sei $E := H'$. $H$ hat in $G$ ungeraden Index $k$ mit $[E : \mathbb{R}] = [H' : G'] = [G : H] = k$. Wir wollen $E = \mathbb{R}$ und $G = H$ zeigen. Sei dazu $u \in E = H'$, $f \in \mathbb{R}[x]$ das Minimalpoynom von $u$ über $\mathbb{R}$ und $l := \operatorname{grad}(f)$. Dann ist $k = [H' : \mathbb{R}] = [H' : \mathbb{R}(u)] \cdot [\mathbb{R}(u) : \mathbb{R}] = [H' : \mathbb{R}(u)] \cdot l$. Also ist $l = \operatorname{grad}(f)$ als Teiler von $k$ ebenfalls ungerade. Als reelles Polynom dieses ungeraden Grades $l$ hat $f$ eine Nullstelle in $\mathbb{R}$. Weil $f$ überdies irreduzibel ist, folgt daraus $l = 1$, $u \in \mathbb{R}$ und somit tatsächlich $E = \mathbb{R}$ und $G = H$, also $|G| = 2^n$. Somit hat auch die Galoisgruppe $G_1 := \mathbb{C}'$ von $F$ über $\mathbb{C}$ als Untergruppe von $G$ eine Ordnung der Gestalt $2^m$ mit $m \in \mathbb{N}$. Nach Satz 8.3.1.2 ist jede Gruppe von Primzahlpotenzordnung nilpotent und hat zu jedem Teiler eine Untergruppe dieser Ordnung (siehe Übungsaufgabe 8.3.4.8). Wäre $m > 0$, so gäbe es folglich eine Untergruppe $U$ von $G_1$ vom Index 2. Für $E_0 := U'$ hätten wir $[E_0 : \mathbb{C}] = [\mathbb{C}' : E_0'] = [G_1 : U] = 2$. Das jedoch widerspricht der Tatsache, dass in $\mathbb{C}$ quadratische Gleichungen stets lösbar sind. □

## 9.4 Die Galoisgruppe eines Polynoms

Die historisch ersten Körpererweiterungen $K \leq E$, an denen Galoisgruppen untersucht wurden, waren (in moderner Terminologie) Zerfällungskörper $E$ eines Polynoms $f \in K[x]$. Man spricht in dieser Situation auch von der Galoisgruppe $G(f)$ des Polynoms $f$. Die Elemente von $G(f)$ lassen sich mit den auf der Menge der Wurzeln von $f$ induzierten Permutationen identifizieren. Galoisgruppen von Polynomen stehen im Zentrum des vorliegenden Abschnitts. Nach der Beobachtung einfacher allgemeiner Sachverhalte in

9.4.1 führt uns in 9.4.2 die bekannte Lösungsformel für die quadratische Gleichung zum Begriff der Diskriminante einer algebraischen Gleichung (siehe 9.4.3). Für Gleichungen vom Grad 3 (siehe 9.4.4) und 4 (siehe 9.4.5) steigt die Komplexität der Lösungstheorie schon beträchtlich, ist aber noch überschaubar. Für Grad 5 begnügen wir uns in Hinblick auf Abschnitt 9.5 im Wesentlichen mit einem Beispiel, wo die Galoisgruppe die volle symmetrische Gruppe $S_5$ ist (siehe 9.4.6) sowie mit kurzen Bemerkungen zur sogenannten allgemeinen Gleichung $n$-ten Grades.

### 9.4.1 Galoisgruppen als endliche Permutationsgruppen

**Definition 9.4.1.1.** Sei $K$ ein Körper, $f \in K[x]$ und $Z = Z_f$ ein Zerfällungskörper von $f$ über $K$, so heißt $G(f) := \mathrm{Aut}_K(Z)$ die *Galoisgruppe* von $f$ über $K$.

Es sei an Proposition 9.2.1.4 erinnert: Da die $\sigma \in G(f)$ alle Wurzeln $u_1, \ldots, u_n$ von $f$ permutieren und $Z = K(u_1, \ldots, u_n)$ von $K$ und den $u_i$ erzeugt wird, ist jedes $\sigma \in G(f)$ durch $\sigma|_{\{u_1,\ldots,u_n\}}$ eindeutig bestimmt. Daher kann jedes $\sigma \in G(f)$ mit jenem $\pi \in S_n$ identifiziert werden, welches $\sigma(u_i) = u_{\pi(i)}$ erfüllt, d.h. $G(f) \leq S_n$. Diese Auffassung wird im Folgenden sehr häufig stillschweigend vorausgesetzt. Insbesondere denken wir uns eine Nummerierung der Nullstellen von $f$ vorgegeben. Als Untergruppe der $S_n$ hat die Gruppe $G(f)$ eine Ordnung, die $|S_n| = n!$ teilt.
Ist $f$ irreduzibel, so können je zwei Nullstellen durch ein $\sigma \in G(f)$ aufeinander abgebildet werden. Das bedeutet, dass $G(f)$ auf $\{u_1, \ldots, u_n\}$ transitiv agiert. Nach Proposition 8.1.1.5 folgt daraus, dass $n$ ein Teiler von $|G(f)|$ ist. Ist $f$ separabel, so ist die Anzahl $n$ der Nullstellen gleich dem Grad von $f$ und der Dimension $[K(u_1) : K] = n$. Da auch für nicht separables $f$ die Anzahl der Nullstellen durch den Grad von $f$ beschränkt ist, können wir zusammenfassen:

**Proposition 9.4.1.2.** *Die Ordnung $|G(f)|$ der Galoisgruppe eines Polynoms vom Grad $n$ ist stets ein Teiler von $n! = |S_n|$. Ist $f \in K[x]$ außerdem separabel und irreduzibel, so ist $|G(f)|$ ein Vielfaches von $n$.*

Wir wollen die Situation für aufsteigenden Grad $n = 1, 2, 3, 4, \ldots$ von

$$f(x) = \sum_{k=0}^{n} a_k x^k$$

mit $a_n \neq 0$ eingehender studieren. Wir werden bei dieser Gelegenheit auch die berühmten Lösungsformeln behandeln, die gleichzeitig als die wichtigste historische Motivation der Galoistheorie gelten können. Weil sich durch Division der Gleichung durch eine Konstante $\neq 0$ die Nullstellen nicht ändern und somit auch die Galoisgruppe dieselbe bleibt, dürfen wir, wann immer es praktisch ist, zum normierten Polynom übergehen, das nach Division durch $a_n$ aus $f$ entsteht. Wir dürfen also o.B.d.A. $a_n = 1$ setzen.
Für $n = 1$ ist nichts weiter zu tun, weil Polynome vom Grad 1 ihre Nullstelle immer schon im Grundkörper haben, also $K = Z_f$ gilt und die Galoisgruppe $G(f) = \mathrm{Aut}_K(Z_f) = \mathrm{Aut}_K(K) = \{\mathrm{id}_K\}$ trivial ist. Für $n = 2$ ist die Situation ebenfalls noch sehr einfach, führt uns aber schon in natürlicher Weise zum verallgemeinerbaren Begriff der Diskriminante und verdient eine ausführlichere Diskussion.

### 9.4.2 Die quadratische Gleichung

Sei $f(x) = a_2x^2 + a_1x + a_0$ ein Polynom über dem Körper $K$ vom Grad $n = 2$, also $a_2 \neq 0$. Die symmetrische Gruppe $S_2$ hat nur die beiden trivialen zwei Untergruppen, die einelementige und $S_2 \cong C_2$ selbst, in Zyklenschreibweise $S_2 = \{e, (12)\} \cong C_2$. Wir wollen uns überlegen, wann für ein quadratisches Polynom $f \in K[x]$ die Galoisgruppe $G(f)$ einelementig und wann $G(f) \cong C_2$ ist.
Ein quadratisches Polynom ist genau dann reduzibel, wenn es in zwei Linearfaktoren zerfällt, von denen jeder einer Nullstelle entspricht, die schon in $K$ liegt. Die beiden Nullstellen können auch gleich sein (Doppelnullstelle). Für reduzibles $f$ ist jedenfalls $Z_f = K$ und die Galoisgruppe $G(f) = \mathrm{Aut}_K(Z_f) = \mathrm{Aut}_K(K) = \{\mathrm{id}_K\}$ trivial (einelementig).
Ist $f$ hingegen irreduzibel, dann liegt keine Nullstelle von $f$ in $K$. Liegt im Zerfällungskörper $Z_f$ eine doppelte Nullstelle $u$ von $f$, so muss diese durch jeden $K$-Automorphismus $\sigma$ von $Z_f$ auf sich selbst abgebildet werden. Da $Z_f = K(u)$ über $K$ von $u$ erzeugt wird, muss $\sigma$ auf ganz $Z_f$ die Identität sein. Also ist bei inseparablem $f$ die Galoisgruppe $G(f) = \{\mathrm{id}_{Z_f}\}$ ebenfalls trivial. Dieser Fall ist allerdings ziemlich speziell. Aus Proposition 9.2.4.1 wissen wir, dass er nur eintreten kann, wenn die Ableitung $f'(x) = 2a_2x + a_1$ das Nullpolynom ist. Wegen $a_2 \neq 0$ ist das nur der Fall, wenn $\mathrm{char}\, K = 2$ und $a_1 = 0$. Nach Normierung kommen also nur Polynome der Gestalt $x^2 - a$ über Charakterstik 2 in Frage. Ist $u$ eine Nullstelle von $f(x) = x^2 - a$, so gilt $u^2 = a$, also $f(x) = x^2 - a = x^2 - u^2 = (x - u)^2$. Es liegt also wirklich eine doppelte Nullstelle vor.
In allen anderen Fällen, d.h. wenn $f$ irreduzibel und separabel ist mit zwei verschiedenen Nullstellen $u_1 \neq u_2 \in Z_f$, so gibt es einen $K$-Isomorphismus $\sigma$, der $u_1$ und $u_2$ vertauscht. In diesem Fall ist $G(f)$, aufgefasst als Permutationsgruppe, ganz $S_2 \cong C_2$. Wir fassen zusammen:

**Satz 9.4.2.1.** *Ist $K$ ein Körper und $f(x) = a_2x^2 + a_1x + a_0$, $a_2 \neq 0$, ein quadratisches Polynom über $K$ mit Zerfällungskörper $Z_f$, so ist die Galoisgruppe $G(f)$ ein- oder zweielementig entsprechend der folgenden (vollständigen) Fallunterscheidung:*

1. *Hat $f$ eine Nullstelle in $K$, so ist $G(f) = \{\mathrm{id}_K\}$ einelementig.*
2. *Ist $\mathrm{char}\, K = 2$ und $a_1 = 0$, so ist $G(f) = \{\mathrm{id}_{Z_f}\}$ einelementig.*
3. *Habe $f$ keine Nullstelle in $K$. Außerdem sei $\mathrm{char}\, K \neq 2$ oder $a_1 \neq 0$. Dann hat $f$ zwei verschiedene Nullstellen $u_1, u_2 \in Z_f$, und $G(f) = \{\mathrm{id}_{Z_f}, \sigma\} \cong S_2 \cong C_2$ ist zweielementig. Dabei bezeichnet $\sigma$ den eindeutigen $K$-Automorphismus von $Z_f$, der $u_1$ mit $u_2$ vertauscht.*

Dieser Satz beantwortet noch nicht die Frage, wie man entscheidet, ob $f(x) = a_2x^2 + a_1x + a_0$ eine Nullstelle in $K$ hat und wie man die Nullstelle(n) von $f$ ermittelt. In endlichen Körpern ist das ein finitäres Problem, weil man nur endlich viele Elemente durchzuprobieren hat. Man kann aber anspruchsvoller sein und nach Formeln für die Nullstellen fragen.

Lässt man Quadratwurzelsymbole in gewohnter Weise zu (d.h. $\sqrt{a}$ bezeichnet eines von i.a. zwei Elementen, deren Quadrat $a$ ist), so kann man für $\operatorname{char} K \neq 2$ die Nullstellen eines quadratischen Polynoms $f(x) = a_2x^2 + a_1x + a_0$, $a_i \in K$, $a_2 \neq 0$, mit Hilfe der bekannten Lösungsformel für quadratische Gleichungen darstellen. Zunächst ändert sich die Lösungsmenge nicht, wenn man durch $a_2$ dividiert, also statt dem ursprünglichen Polynom nun $f(x) = x^2 + px + q$ mit $p = \frac{a_1}{a_2}$ und $q = \frac{a_0}{a_2}$ betrachtet und in bekannter Weise „auf ein vollständiges Quadrat ergänzt“:

$$f(x) = x^2 + px + q = (x + \frac{p}{2})^2 - \frac{p^2}{4} + q.$$

Für eine Nullstelle $u$ von $f$ muss daher $(u+\frac{p}{2})^2 = \frac{p^2}{4} - q$ gelten. Kürzen wir $D := p^2 - 4q$ ab, so ergeben sich zwei Nullstellen $u_1$ und $u_2$ von $f$:

$$u_1 = \frac{1}{2}(-p + \sqrt{D}), \quad \text{und} \quad u_2 = \frac{1}{2}(-p - \sqrt{D})$$

Aus

$$f(x) = x^2 + px + q = (x - u_1)(x - u_2) = x^2 - (u_1 + u_2)x + u_1u_2$$

können wir als Spezialfall des Satzes von Vieta für $n = 2$ die Beziehungen $-p = u_1 + u_2$ und $u_1u_2 = q$ ablesen. Damit gilt

$$D = p^2 - 4q = (u_1 + u_2)^2 - 4u_1u_2 = u_1^2 - 2u_1u_2 + u_2^2 = (u_1 - u_2)^2.$$

Dieser Wert $D$ heißt *Diskriminante* von $f$ und ist offenbar genau dann 0, wenn $u_1 = u_2$ eine Doppelnullstelle von $f$ ist. Wir fassen zusammen:

**Satz 9.4.2.2.** *Sei $K$ ein Körper mit* $\operatorname{char} K \neq 2$ *und $f(x) = x^2 + px + q \in K[x]$. Dann zerfällt $f$ über $K$ (bzw. über einem Erweiterungskörper $E$ von $K$) genau dann, wenn es ein $w \in K$ (bzw. $w \in E$) gibt mit $w^2 = D = p^2 - 4q$. Die Nullstellen von $f$ sind dann gegeben durch*

$$u_1 = \frac{1}{2}(-p + w), \quad \textit{und} \quad u_2 = \frac{1}{2}(-p - w)$$

*und stimmen genau dann überein, wenn $D = p^2 - 4q = 0$.*

Offenbar lässt sich die Definition der Diskriminante auf Polynome beliebigen Grades verallgemeinern.

### 9.4.3 Die Diskriminante

Sei $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ ein normiertes Polynom $n$-ten Grades über einem Körper $K$ und $f(x) = \prod_{i=1}^{n}(x - u_i)$ mit den Nullstellen $u_i$ von $f$ in einem Erweiterungskörper $E$ von $K$. Dann gilt nach dem Satz von Vieta 5.3.4.10 $s_{n,i}(u_1, \ldots, u_n) = (-1)^i a_{n-i}$, $i = 1, \ldots, n$, mit den elementarsymmetrischen Polynomen $s_{n,i} \in K[x_1, \ldots, x_n]$ aus 5.3.4. Wir betrachten das Polynom

$$\Delta_n(x_1, \ldots, x_n) := \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

Für $n = 1$ ist das Produkt leer und der allgemeinen Konvention entsprechend $\Delta_1 := 1$ zu setzen. Durch eine Permutation $\pi \in S_n$ der Indizes kann sich lediglich die Reihenfolge der Faktoren und das Vorzeichen ändern, letzteres je nachdem, ob $\pi$ gerade ($\operatorname{sgn}(\pi) = 1$) oder ungerade ($\operatorname{sgn}(\pi) = -1$) ist. Folglich gilt

$$\Delta_n(x_{\pi(1)}, \ldots, x_{\pi(n)}) = \operatorname{sgn}(\pi)\Delta_n(x_1, \ldots, x_n).$$

Wegen $\operatorname{sgn}(\pi)^2 = (\pm 1)^2 = 1$ gilt für $D_n(x_1, \ldots, x_n) := \Delta_n(x_1, \ldots, x_n)^2$ daher

$$D_n(x_{\pi(1)}, \ldots, x_{\pi(n)}) = (\Delta_n(x_{\pi(1)}, \ldots, x_{\pi(n)}))^2 = \Delta_n(x_1, \ldots, x_n)^2 = D_n(x_1, \ldots, x_n).$$

Folglich ist $D_n$ ein symmetrisches Polynom in den Variablen $x_1, \ldots, x_n$ und somit, nach dem Hauptsatz 5.3.4.4, selbst darstellbar als

$$D_n(x_1, \ldots, x_n) = g_n(s_{n,1}(x_1, \ldots, x_n), \ldots, s_{n,n}(x_1, \ldots, x_n))$$

mit einem eindeutig bestimmen Polynom $g_n$ über $K$ in $n$ Variablen. Man beachte, dass $g_n$ nur von $n$, nicht aber von $K$ abhängt. Motiviert durch die oben erwähnte Vieta-Beziehung $s_{n,i}(u_1, \ldots, u_n) = (-1)^i a_{n-i}$, $i = 1, \ldots, n$ definieren wir nun:

**Definition 9.4.3.1.** Mit den obigen Bezeichnungen heißt

$$D = D(f) := g_n(-a_{n-1}, a_{n-2}, \ldots, (-1)^{n-1}a_1, a_0) \in K$$

die *Diskriminante* eines normierten Polynoms $f$ vom Grad $n$. Ist $f(x) = \sum_{i=0}^{n} a_i x^i$ nicht normiert, so wird $D(f) := D(a_n^{-1} f)$ gesetzt.

**UE 487** ► **Übungsaufgabe 9.4.3.2.** Zeigen Sie, dass ein normiertes Polynom $f$ in seinem Zerfällungskörper genau dann eine mehrfache Nullstelle hat, wenn $D(f) = 0$. ◄ **UE 487**

**UE 488** ► **Übungsaufgabe 9.4.3.3.** Für drei Polynome $f, g, h \in K[x]$ gelte $f(x) = g(x + c) = ch(x)$ mit $c \in K \setminus \{0\}$. Dann stimmen die Diskriminanten $D(f) = D(g) = D(h)$ überein. ◄ **UE 488**

Wir wollen nun kontrollieren, ob die in 9.4.3.1 definierte Diskriminante für $n = 2$ denselben Wert liefert wie in Satz 9.4.2.2. Wir erhalten

$$\begin{aligned} D_2(x_1, x_2) = (x_1 - x_2)^2 = x_1^2 - 2x_1x_2 + x_2^2 = (x_1 + x_2)^2 - 4x_1x_2 = \\ = s_{2,1}(x_1, x_2)^2 - 4s_{2,2}(x_1, x_2), \end{aligned}$$

also ist $g_2(y_1, y_2) = y_1^2 - 4y_2$. Um $D(f)$ für $f(x) = x^2 + a_1x + a_0 = x^2 + px + q$ zu berechnen, müssen wir nach Definition 9.4.3.1 $y_1 = -a_1 = -p$ und $y_2 = a_0 = q$ einsetzen. Damit erhalten wir tatsächlich

$$D(f) = g_2(-p, q) = p^2 - 4q,$$

so wie in Satz 9.4.2.2.

Motiviert durch den Satz von Vieta 5.3.4.10, der den Zusammenhang zwischen Nullstellen und Koeffizienten eines Polynoms beschreibt, haben wir die Diskriminante eines Polynoms über den Umweg symmetrischer Polynome und unter Verwendung des Hauptsatzes 5.3.4.4 definiert. Wir hätten $D(f)$ auch direkt als das Produkt

$$D(f) := \prod_{1\leq i<j\leq n} (u_i - u_j)^2$$

über alle $(u_i - u_j)^2$ definieren können, wenn $u_1, \ldots, u_n$ die Nullstellen von $f$ in einem Zerfällungskörper $Z$ sind, wobei jede entsprechend ihrer Vielfachheit vorkommt. Diese Größe ist tatsächlich unabhängig von der speziellen Wahl des Zerfällungskörpers und der Nummerierung $u_i$ und liegt bereits im Grundkörper $K$:
Hat $f$ eine doppelte Nullstelle, also $u_i = u_j$ für $i \neq j$, dann ist trivialerweise $D(f) = 0$. Sind hingegen alle $u_i$ paarweise verschieden, so ist jeder der über $K$ irreduziblen Faktoren von $f$ separabel. $Z$ ist also der Zerfällungskörper einer Menge separabler Polynome. Nach Satz 9.2.4.3 (den wir bei der obigen Vorgangsweise nicht bemühen mussten) ist daher die Erweiterung $K \leq Z$ Galoissch. Wir wenden einen beliebigen $K$-Automorphismus $\sigma$ von $Z$ auf $D(f)$ an. Weil $\sigma$ die $u_i$ permutiert, liefert das ein Produkt mit denselben Faktoren, also $\sigma(D(f)) = D(f)$. $D(f)$ liegt also im Fixpunktkörper der vollen Galoisgruppe $\mathrm{Aut}_K(Z)$, also – die Erweiterung $K \leq Z$ ist Galoissch – in $K$.
Wenn wir hingegen

$$\Delta(f) := \prod_{1\leq i<j\leq n} (u_i - u_j)$$

definieren, so erhalten wir eine Größe, die nicht in $K$ liegen muss, somit vom speziellen Zerfällungskörper abhängt und auch dort nur bis auf das Vorzeichen eindeutig bestimmt ist, je nach der Nummerierung der $u_i$. Zum Beispiel kommen für das Polynom $f(x) := x^2 + 1$ über $K = \mathbb{Q}$ mit den Nullstellen $i$ und $-i$ im Zerfällungskörper $Z := \mathbb{Q}[i] \leq \mathbb{C}$ für $\Delta(f)$ die beiden Werte $i - (-i) = 2i$ und $-i - i = -2i$ in Frage, die nicht im Grundkörper$K = \mathbb{Q}$ liegen, weil dort $D(f) = p^2 - 4q = -4$ keine Quadratwurzel hat. In Hinblick auf die folgende Unterscheidung erweist sich diese Doppeldeutigkeit aber als unproblematisch, weil es nur darauf ankommt, ob $\Delta$ und somit auch $-\Delta$ im Grundkörper $K$ liegt.

**Satz 9.4.3.4.** *Sei* $\mathrm{char}\, K \neq 2$ *und habe das Polynom* $f \in K[x]$ *Grad* $n \geq 1$ *und in seinem Zerfällungskörper* $Z_f$ *nur einfache Nullstellen* $u_1, \ldots, u_n$*. Dann ist die Galoisgruppe* $G(f)$*, aufgefasst als Untergruppe von* $S_n$*, genau dann in der alternierenden Gruppe* $A_n \leq S_n$ *enthalten, wenn es in* $K$ *ein Element* $\Delta$ *gibt mit* $\Delta^2 = D(f)$*.*

*Beweis.* Sei $Z_f$ irgendein Zerfällungskörper von $f$. Es gilt $\Delta(f)^2 = D(f)$. Für ein beliebiges $\sigma \in G(f)$ sind zwei Fälle zu unterscheiden. Ist $\sigma$ als Permutation der $u_i$ gerade, so ist $\sigma(\Delta) = \Delta$, andernfalls $\sigma(\Delta) = -\Delta \neq \Delta$, letzteres wegen $\Delta \neq 0$ (weil die $u_i$ paarweise verschieden sind) und wegen $\mathrm{char}\, K \neq 2$. Also liegt $\Delta$ genau dann im Fixpunktkörper $K_0$ der Galoisgruppe $G(f)$, wenn diese nur gerade Permutationen enthält, also in $A_n$ enthalten ist. Zu zeigen bleibt $K_0 = K$, dass also die Erweiterung Galoissch ist. Nach Satz 9.2.4.7 ist das tatsächlich der Fall, weil $Z_f$ der Zerfällungskörper der Menge $S$ aller irreduziblen Faktoren von $f$ ist, die wegen der Einfachheit der Nullstellen $u_i$ separabel sind. □

### 9.4.4 Die kubische Gleichung

Ein Polynom $f(x) = a_3x^3+a_2x^2+a_1x+a_0 \in K[x]$ dritten Grades, also mit mit $a_3 \neq 0$ ist genau dann reduzibel, wenn es einen Linearfaktor, d.h. eine Nullstelle in $K$ hat. Im Fall $\operatorname{char} K = p \in \mathbb{P}$, also $K \cong \mathbb{Z}_p$ lässt sich das durch Einsetzen der endlich vielen Restklassen modulo $p$ in $f$ entscheiden. Ist $\operatorname{char} K = 0$, also $K \cong \mathbb{Q}$, so schränkt Satz 5.3.2.9 die Möglichkeiten ebenfalls auf eine endliche Menge ein. In jedem Fall ist die Suche nach einer Nullstelle von $f$ in $K$ also ein finitäres Problem. Ist eine Nullstelle gefunden, so ist $f$ das Produkt von Polynomen kleineren Grades und die Nullstellensuche auf die bereits behandelten Fälle $n = 1, 2$ zurückgeführt. Ähnliches gilt auch für die Bestimmung der Galoisgruppe $G(f)$. Denn entweder zerfällt $f = f_1f_2f_3$ in drei Linearfaktoren, in welchem Fall $Z_f = K$ und somit $G(f) = \{\mathrm{id}_K\}$ trivial ist; oder $f = f_1f_2$ mit linearem $f_1$ und quadratischem $f_2$, in welchem Fall $G(f) \cong G(f_2)$ gilt.

**UE 489** ▶ **Übungsaufgabe 9.4.4.1.** Geben Sie den Isomorphismus $G(f) \cong G(f_2)$ möglichst explizit an. ◀ **UE 489**

Zur Bestimmung von $G(f)$ dürfen wir uns daher auf irreduzible $f$ konzentrieren. Nach Satz 9.4.1.2 muss die Gruppenordnung $|G(f)|$ ein Vielfaches 3 und ein Teiler von $3! = 6$ sein. Als Untergruppe von $S_n$ kann es sich bei $G(f)$ also nur um die alternierende Gruppe $A_3 = \{\mathrm{id}, (123), (132)\}$ oder um die ganze symmetrische Gruppe $S_3$ handeln. Nach Satz 9.4.3.4 hängt das davon ab, ob die Diskriminante $D(f)$ Quadrat eines Elementes $\Delta \in K$ ist. Wegen Übungsaufgabe 9.4.3.3 ändert sich die Diskriminante nicht, wenn wir $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0 \in K[x]$ durch $a_3 \neq 0$ dividieren. Wir setzen daher o.B.d.A. $a_3 = 1$ voraus. Ebenso wegen 9.4.3.3 dürfen wir anschließend (sofern $\operatorname{char} K \neq 3$) $x$ durch $x - \frac{a_2}{3}$ ersetzen, wodurch das quadratische Glied wegfällt. Wir beschränken uns daher auf Polynome dritten Grades der Bauart $f(x) = x^3+px+q$. Nach etwas mühsamer Rechnung erhält man:

**Satz 9.4.4.2.** *Sei* $\operatorname{char} K \neq 2, 3$. *Die Diskriminante eines Polynoms* $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0 \in K[x]$ *dritten Grades ist gegeben durch*

$$D(f) = -4p^3 - 27q^2.$$

*Dabei sind* $p$ *und* $q$ *so zu wählen, dass* $a_3^{-1}f(x - \frac{a_2}{3a_3}) = x^3 + px + q$ *gilt.*
*Ist* $f$ *irreduzibel und* $D(f) = \Delta^2$ *mit einem* $\Delta \in K$, *so ist* $G(f) \cong A_3 \cong C_3$; *gibt es kein solches* $\Delta \in K$, *so ist* $G(f) \cong S_3$.

**UE 490** ▶ **Übungsaufgabe 9.4.4.3.** Beweisen Sie Proposition 9.4.4.2. Bedenken Sie weiterhin Übungsaufgabe 9.4.3.3. ◀ **UE 490**

Wir wollen weiterhin $\operatorname{char} K \neq 2, 3$ voraussetzen und unter dieser Bedingung die Lösungsformel von Cardano (siehe 9.4.4.4 weiter unten) herleiten.
Wir gehen aus vom Polynom $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0 \in K[x]$ mit $a_3 \neq 0$, dessen Nullstellen gesucht sind. Wie schon in Satz 9.4.4.2 gehen wir über zum normierten

Polynom $f_0 := a_3^{-1} f$ mit denselben Nullstellen wie $f$ und sodann zum Polynom $f_0(x - \frac{a_2}{3a_3})$, dessen Nullstellen gegenüber jenen von $f$ nur um $\frac{a_2}{3a_3}$ verschoben sind. Also genügt es, von vornherein nur kubische Polynome der speziellen Bauart $f(x) = x^3 + px + q$ zu untersuchen. Seien also $u = u_1, u_2, u_3$ die Nullstellen im Zerfällungskörper $Z_f$ von $f$. Der Rechentrick besteht darin, $u = a + b$ als Summe anzusetzen und nachträglich $a$ und somit $b$ geeignet zu wählen. Die dritte Potenz von $u$ ist

$$u^3 = (a+b)^3 = a^3 + 3ab(a+b) + b^3,$$

was wir unter nochmaliger Verwendung von $a + b = u$ zu

$$u^3 - 3abu - (a^3 + b^3) = 0$$

umschreiben. Sind $a$ und $b$ so gewählt, dass $-3ab = p$ gilt, so folgt daraus $-(a^3 + b^3) = -u^3 + 3abu = -u^3 - pu = -f(u) + q = q$. Nach Vieta sind dann $a^3$ und $b^3$ die beiden Lösungen der sogenannten *quadratischen Resolvente*

$$r(x) := x^2 + qx - \frac{p^3}{27} = x^2 - (a^3 + b^3)x + a^3 b^3$$

von $f$. Wegen $\operatorname{char} K \neq 2$ dürfen wir die Lösungsformel 9.4.2.2 für die quadratische Gleichung verwenden und erhalten

$$a^3, b^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

Für $u = a + b$ gilt folglich die sogenannte *Cardanosche Formel*:

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Zu beachten ist, dass es i.a. drei dritte Wurzeln gibt und nicht alle 9 Kombinationen zugelassen sind, sondern nur solche Paare aus $a$ und $b$, die $a^3 b^3 = -\frac{p^3}{27}$ erfüllen. Somit lässt sich die Formel korrekter in folgende Aussage kleiden.

**Satz 9.4.4.4.** *Sei $f(x) = x^3 + px + q \in K[x]$ ein normiertes Polynom dritten Grades über einem Körper $K$ mit $\operatorname{char} K \neq 2, 3$. Die Elemente $w, a, b \in K$ mögen die Beziehungen $w^2 = \frac{q^2}{4} + \frac{p^3}{27}$, $a^3 = -\frac{q}{2} + w$ und $b^3 = -\frac{q}{2} - w$ erfüllen. Außerdem sei $\zeta \in K$ eine primitive dritte Einheitswurzel, d.h. $\zeta^3 = 1$ aber $\zeta \neq 1$. Dann liegen sämtliche drei (nicht notwendig paarweise verschiedenen) Nullstellen $u_1, u_2, u_3$ von $f$ in $K$, und können als*

$$u_1 = a + b, \quad u_2 = \zeta a + \zeta^2 b, \quad u_3 = \zeta^2 a + \zeta b.$$

*erhalten werden.*

**UE 491** ► **Übungsaufgabe 9.4.4.5.** Sei $f \in K[x]$ ein separables kubisches Polynom mit Galoisgruppe $S_3$ und Wurzeln $u_1, u_2, u_3 \in E$. Zeigen Sie: Die Zwischenkörper dieser Erweiterung sind $E$, $K(\Delta)$, $K(u_1)$, $K(u_2)$, $K(u_3)$ und $K$. Die entsprechenden Untergruppen der Galoisgruppe sind $\{1\}$, $A_3$, $T_1 = \{\mathrm{id}, (23)\}$, $T_2 = \{\mathrm{id}, (13)\}$, $T_3 = \{\mathrm{id}, (12)\}$ und $S_3$. ◄ **UE 491**

**UE 492** ► **Übungsaufgabe 9.4.4.6.** 1. Für $f(x) = x^3 - 3x + 1 \in \mathbb{Q}[x]$ ist $G(f) \cong A_3$. ◄ **UE 492**

2. Für $g(x) = x^3 - 3x^2 - x - 1 \in \mathbb{Q}[x]$ ist $G(g) \cong S_3$.

### 9.4.5 Die Gleichung vierten Grades

Es überrascht wenig, dass sich die Dinge für Polynome vierten Grades komplizierter verhalten als bei kubischen. Immerhin lassen sich Galoisgruppe und Lösungen, wenn auch mit teilweise wesentlich mehr Aufwand, so doch grundsätzlich noch auf ähnliche Weise bestimmen. Das soll im Folgenden, teils nur skizzenhaft, ausgeführt werden.

Beginnen wir mit der Lösungsformel für Polynome vierten Grades über einem Körper $K$, von dem wir wie schon bei der kubischen Gleichung $\operatorname{char} K \neq 2, 3$ voraussetzen. Sei also

$$f(x) = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

mit $a_4 \neq 0$ ein Polynom vierten Grades über dem Körper $K$. Bei Bedarf dürfen wir uns von diesem allgemeinen Fall auf den vereinfachten Fall $a_4 = 1$ (nach Division der Gleichung durch $a_4$) und $a_3 = 0$ (nach der „Ergänzung auf ein vollständiges Biquadrat“) $f(x) = (x + \frac{a_3}{4})^4 + p(x + \frac{a_3}{4})^2 + q(x + \frac{a_3}{4}) + r$, also auf Polynome der Bauart

$$f(x) = x^4 + px^2 + qy + r$$

mit geeigneten Koeffizienten $p, q, r \in K$ beschränken. Wir gehen von der Faktorisierung

$$f(x) = (x - u_1)(x - u_2)(x - u_3)(x - u_4),$$

aus. Gemäß Vieta multiplizieren wir aus zu

$$f(x) = x^4 - (u_1 + u_2 + u_3 + u_4)x^3 + \left(\sum_{1\le i<j\le 4} u_iu_j\right)x^2 - \left(\sum_{1\le i<j<k\le 4} u_iu_j\right) + u_1u_2u_3u_4.$$

Nach Koeffizientenvergleich mit $f(x) = x^4 + px^2 + qy + r$ lesen wir für die vier elementarsymmetrischen Funktionen von $u_1, u_2, u_3, u_4$ ab:

$$u_1 + u_2 + u_3 + u_4 = 0, \quad \sum_{1\le i<j\le 4} u_iu_j = p, \quad \sum_{1\le i<j<k\le 4} u_iu_ju_k = -q, \quad u_1u_2u_3u_4 = r$$

Die entscheidende Idee besteht darin, die symmetrisch aufgebauten Elemente

$$v_1 := -(u_1 + u_2)(u_3 + u_4) \quad v_2 := -(u_1 + u_3)(u_2 + u_4), \quad v_3 := -(u_1 + u_4)(u_2 + u_3)$$

zu betrachten. Wegen $u_1+u_2+u_3+u_4=0$ sind in den Definitionen für die $v_i$ die beiden Faktoren bis auf das Vorzeichen gleich, also kann man auch schreiben

$$v_1=(u_1+u_2)^2=(u_3+u_4)^2 \quad v_2=(u_1+u_3)^2=(u_2+u_4)^2, \quad v_3=(u_1+u_4)^2=(u_2+u_3)^2.$$

Mit den anderen oben genannten Bedingungen kann man die elementarsymmetrischen Funktionen auch von $v_1, v_2, v_3$ auf die Koeffizienten der Gleichung zurückführen. Und zwar rechnet man nach:

$$v_1+v_2+v_3=-2p, \quad v_1v_2+v_1v_3+v_2v_3=p^2-4r, \quad v_1v_2v_3=q^2$$

Mit $v_1, v_2, v_3$ liegen folglich die drei Nullstellen der sogenannten *kubischen Resolvente*

$$R(x)=x^3+2px^2+(p^2-4r)x-q^2$$

von $f$ vor, die mit Hilfe der Cardanoschen Formel (siehe auch Satz 9.4.4.4) gefunden werden können. Wir werden nun die $u_i$ auf die $v_j$ zurückführen. Und zwar wählt man Quadratwurzeln $w_i$ der $v_i$, wobei nur noch auf das Vorzeichen der zusätzlichen Bedingung $w_1w_2w_3=-q$ zu achten ist. Dann kann man

$$u_1+u_2=-(u_3+u_4)=w_1, \quad u_1+u_3=-(u_2+u_4)=w_2, \quad u_1+u_4=-(u_2+u_3)=w_3$$

ablesen. Hieraus lassen sich die $u_i$ zurückrechnen: $u_1=\frac{1}{2}(w_1+w_2+w_3)$, $u_2=\frac{1}{2}(w_1-w_2-w_3)$, $u_3=\frac{1}{2}(-w_1+w_2-w_3)$, $u_4=\frac{1}{2}(-w_1-w_2+w_3)$. Wir fassen zusammen:

**Satz 9.4.5.1.** *Sei $K$ ein Körper der Charakteristik* $\operatorname{char} K\neq 2,3$ *und $f(x)=x^4+px^2+qx+r\in K[x]$. Seien $v_1, v_2, v_3$ die Nullstellen der sogenannten kubischen Resolvente $R(x):=x^3+2px^2+(p^2-4r)x-q^2$ (wie sie nach Elimination des quadratischen Gliedes mit Hilfe der Cardanoschen Formel, siehe auch Satz 9.4.4.4 gefunden werden können), weiters $w_1, w_2, w_3\in K$ mit $w_1^2=v_1$, $w^2=v_2$ und $w_3^2=v_3$ sowie $w_1w_2w_3=-q$. Dann sind*

$$u_1:=\frac{w_1+w_2+w_3}{2},\ u_2:=\frac{w_1-w_2-w_3}{2},\ u_3:=\frac{-w_1+w_2-w_3}{2},\ u_4:=\frac{-w_1-w_2+w_3}{2}$$

*die vier Nullstellen von $f$.*

**UE 493** ► **Übungsaufgabe 9.4.5.2.** Vervollständigen Sie die ausgelassenen Schritte in obiger Ableitung der Lösungsformel für die Gleichung vierten Grades und damit im Beweis von Satz 9.4.5.1. ◄ **UE 493**

Wir wollen uns auch noch der Bestimmung der Galoisgruppe eines Polynoms $f(x)=a_4x^4+a_3x^3+a_2x^2+a_1x+a_0$ mit $a_4\neq 0$ über einem Körper $K$ zuwenden. Eingangs wollen wir den Fall behandeln, dass sich das Polynom in irreduzible Faktoren kleineren Grades zerlegen lässt. Ist einer dieser Faktoren linear, so liegt die zugehörige Nullstelle in $K$, und es geht nur mehr um die Permutation der übrigen drei Nullstellen eines Polynoms dritten Grades. Damit ist die Bestimmung der Galoisgruppe auf früher bereits behandelte Fälle

zurückgeführt. Zerfällt $f = f_1 f_2$ hingegen in zwei quadratische irreduzible Faktoren $f_1$ und $f_2$, so sind zwei Fälle zu unterscheiden. Stimmen die Zerfällungskörper $Z_{f_1}$ und $Z_{f_2}$ von $f_1$ und $f_2$ überein, so ist $G(f) = G(f_1) = G(f_2)$, und diese Fälle wurden bereits behandelt. Andernfalls Ergibt sich der Zerfällungskörper $Z_f$ als Iteration zweier quadratischer Erweiterungen. Das führt maximal zu einer Erweiterung vierten Grades.

**UE 494** ► **Übungsaufgabe 9.4.5.3.** Welche Struktur kann die Galoisgruppe $G(f)$ eines Polynoms $f$ vom Grad 4 haben, das in zwei irreduzible quadratische Faktoren zerfällt? ◄ **UE 494**

Ebenso Gegenstand einer Übungsaufgabe sei die Frage, wie entschieden werden kann, ob ein Polynom $f$ vierten Grades irreduzibel ist.

**UE 495** ► **Übungsaufgabe 9.4.5.4.** Beschreiben Sie, wie für jedes Polynom $f$ vierten Grades über $\mathbb{Q}$ nach endlich vielen Schritten entschieden werden kann, ob es irreduzibel ist. Lässt sich Ihre Methode auf Polynome höheren Grades verallgemeinern? Wie sieht es mit Polynomen über endlichen Körpern (statt über $\mathbb{Q}$) aus? ◄ **UE 495**

Zu untersuchen bleibt als interessantester Fall der eines irreduziblen Polynoms $f$ vierten Grades über einem Körper $K$, dessen Galoisgruppe $G(f)$ gesucht ist. Wir beschränken uns auf den separablen Fall. Zunächst überlegen wir uns, welche Gruppen überhaupt in Frage kommen, und zwar aufgefasst als Untergruppen der symmetrischen Gruppe $S_4$. Aus Proposition 9.4.1.2 folgt, dass als Gruppenordnung $n := |G(f)|$ nur Teiler von $24 = 4! = |S_4|$ in Frage kommen, die (wegen irreduzibel) gleichzeitig ein Vielfaches von 4 sind, also $n = 4, 8, 12, 24$. Außerdem muss $G(f)$ als Permutationsgruppe auf $\{1, 2, 3, 4\}$ transitiv sein. Für $n = 4$ sind das einerseits die von einem Viererzyklus erzeugten zyklischen Untergruppen $\cong C_4$ von $S_4$ (davon gibt es drei Stück) sowie die Kleinsche Vierergruppe $V := \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \cong C_2 \times C_2$. Zur Ordnung $n = 8$: Die Diedergruppe $D_4$ (Symmetriegruppe des Quadrats, erzeugt z.B. von einem Viererzyklus (1234) und einer Transposition (13)) ist eine Gruppe der Ordnung 8, die sich in die $S_4$ einbetten lässt. Jede 8-elementige Untergruppe ist eine 2-Sylow-Untergruppe von $S_4$. Nach dem zweiten Sylowsatz 8.1.4.3 sind alle anderen zu dieser konjugiert. Innerhalb $S_4$ bedeutet Konjugation lediglich Umnummerierung der Symbole $1, 2, 3, 4$. Also kennen wir im Wesentlichen mit der gegebenen $D_4$ bereits alle. (Insgesamt gibt es in $S_4$ drei Kopien. Denn nach dem dritten Sylowsatz 8.1.4.5 ist ihre Anzahl ungerade und ein Teiler von 24, wobei die Anzahl 1 nicht in Frage kommt, weil $D_4$ kein Normalteiler von $S_4$ ist. Damit bleibt nur 3 als mögliche Anzahl.) Zu $n = 12$ und $n = 24$ gibt es jeweils nur eine Untergruppe, $A_4$ bzw. $S_4$.

**UE 496** ► **Übungsaufgabe 9.4.5.5.** Ergänzen Sie allfällige Lücken in der obigen Argumentation, um zu zeigen, dass als Galoisgruppe $G(f)$ eines irreduziblen separablen Polynoms $f$ vom Grad 4 über einem Körper $K$ nur fünf Typen von Permutationsgruppen $G(f) \leq S_4$ in Frage kommen: $C_4, V, D_4, A_4, S_4$. ◄ **UE 496**

Welcher dieser Fälle eintritt, lässt sich entscheiden, wenn man gewisse Hilfsgrößen kennt. Der folgende Satz beschreibt die Situation präzise:

**Satz 9.4.5.6.** *Sei $f$ ein irreduzibles separables Polynom über dem Körper $K$ mit Galoisgruppe $G(f)$ und mit paarweise verschiedenen Nullstellen $u_1, u_2, u_3, u_4$ in einem Zerfällungskörper $Z_f$ von $f$. Wir definieren in $Z_f$ die Elemente*

$$\alpha := u_1u_2 + u_3u_4, \quad \beta := u_1u_3 + u_2u_4, \quad \gamma := u_1u_4 + u_2u_3,$$

*das Polynom $\overline{R}(x) := (x-\alpha)(x-\beta)(x-\gamma)$, sowie $m := [K(\alpha,\beta,\gamma) : K]$, den Erweiterungsgrad des Zerfällungskörpers von $\overline{R}$ in $Z_f$. Dann gilt die folgende (vollständige) Fallunterscheidung:*

1. *$G(f) \cong S_4$ genau dann, wenn $m = 6$.*
2. *$G(f) \cong A_4$ genau dann, wenn $m = 3$.*
3. *$G(f) \cong V \cong C_2 \times C_2$ genau dann, wenn $m = 1$.*
4. *$G(f) \cong D_4$ genau dann, wenn $m = 2$ und $f$ irreduzibel ist über $K(\alpha,\beta,\gamma)$.*
5. *$G(f) \cong C_4$ genau dann, wenn $m = 2$ und $f$ reduzibel ist über $K(\alpha,\beta,\gamma)$.*

Das Polynom $\overline{R}$ nennt man, so wie $R$ weiter oben, ebenfalls *kubische Resolvente* von $f$. Im Unterschied zu $R$ muss $\overline{R}$ aber nicht in $K[x]$ liegen.
Nach unseren Vorüberlegungen bzw. wegen Übungsaufgabe 9.4.5.5 kommen genau die fünf genannten (paarweise nicht isomorphen) Gruppen $C_4, V, D_4, A_4, S_4$ für $G(f)$ in Frage. Somit genügt der Nachweis, dass für jeden dieser Fälle $m$ den in Satz 9.4.5.6 behaupteten Wert hat und, lediglich zur Unterscheidung der letzten beiden Fälle, $f$ die behauptete (Ir-)Reduzibilität aufweist. Das soll im Rahmen der folgenden Übungsaufgabe ausgeführt werden.

**UE 497** ► **Übungsaufgabe 9.4.5.7.** Beweisen Sie Satz 9.4.5.6. Hinweis: Zeigen Sie zunächst, dass in der Galoiskorrespondenz der Galoisschen Erweiterung $K \leq Z_f$ dem Körper $K(\alpha,\beta,\gamma)$ die Gruppe $G(f) \cap V$ entspricht. Eine der beiden dafür zu beweisenden Inklusionen ist offensichtlich, für die andere ist zu zeigen, dass jedes $\sigma \in G(f) \notin V$ wenigstens eines der Elemente $\alpha, \beta, \gamma$ nicht fest lässt. A priori kommen $24 - 4 = 20$ verschiedene $\sigma$ in Frage, man kann sich die Arbeit aber etwas erleichtern. ◄ **UE 497**

### 9.4.6 Die symmetrische Gruppe $S_5$ als Galoisgruppe

**UE 498** ► **Übungsaufgabe 9.4.6.1.** Sei $p$ eine Primzahl. Zeigen Sie, dass die beiden Permutationen $(12)$ und $(12\ldots p)$ (Zyklenschreibweise) die $S_p$ erzeugen. ◄ **UE 498**

**Satz 9.4.6.2.** *Sei $p \in \mathbb{P}$ und $f \in \mathbb{Q}[x]$ ein irreduzibles Polynom vom Grad $p$ mit genau zwei Wurzeln in $\mathbb{C} \setminus \mathbb{R}$. Dann ist $G(f) \cong S_p$.*

*Beweisskizze.* Wir betrachten $G(f)$ als Untergruppe von $S_p$. Nach Proposition 9.4.1.2 teilt $p$ die Gruppenordnung $|G(f)|$. Nach dem Satz von Cauchy 8.1.3.2 gibt es daher ein $\sigma \in G(f)$ mit Ordnung $p$. Wegen $p \in \mathbb{P}$ muss $\sigma = (1j_2 \dots j_p)$ als Permutation ein $p$-Zyklus sein. Die komplexe Konjugation $a+bi \mapsto a-bi$ ist ein $\mathbb{R}$-Automorphismus von $\mathbb{C}$. Daher vertauscht diese Abbildung die beiden komplexen Wurzeln von $f$ und hält alle anderen fest. Daraus folgt, dass $G(f)$ eine Transposition $\tau$ enthält, o.B.d.A. $\tau = (12)$. Für ein geeignetes $k$ gilt $\sigma^k = (12i_3 \dots i_p) \in G(f)$. Nach Übungsaufgabe 9.4.6.1 erzeugen $(12)$ und $(123 \dots p)$ schon ganz $S_p$, also muss $G(f) = S_p$ gelten. □

**UE 499** ▶ **Übungsaufgabe 9.4.6.3.** Zeigen Sie, dass das Polynom $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$ die Eigenschaften aus Satz 9.4.6.2 und somit eine Galoisgruppe $G(f) \cong S_5$ hat. Hinweis: Eisensteinsches Kriterium, Kurvendiskussion. ◀ **UE 499**

Das Polynom $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$ hat also eine nicht auflösbare Galoisgruppe $G(f) \cong S_5$. Andernfalls wäre ja auch $A_5 \leq S_5$ auflösbar (Aussage 2 in Proposition 8.3.2.3). Nach Satz 8.2.3.2 ist $A_5$ aber einfach, was sich nur im abelschen Fall mit Auflösbarkeit verträgt, Widerspruch. Mit den Ergebnissen aus Abschnitt 9.5, insbesondere 9.5.3 wird daraus folgen, dass es keine Lösungsformel für die Gleichung $f(x) = x^5 - 4x + 2 = 0$ gibt. Erst recht kann es daher keine allgemeine Lösungsformel für beliebige Polynome vom Grad 5 geben. Trotzdem ist es lehrreich, die Frage nach solch einer allgemeinen Formel begrifflich zu fassen. Das soll nun skizziert werden.
Für ein Polynom

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

wollen wir zu diesem Zweck nun neben $x$ auch die Koeffizienten $a_i$ als Unbestimmte auffassen. Wir betrachten also die rein transzendente Erweiterung $E := K(a_0, \dots, a_{n-1})$ von $K$ und $f$ als ein Element von $E[x]$. Ist $Z$ der Zerfällungskörper von $f$ über $E$, so heißt $\mathrm{Aut}_E(Z)$ die *Galoisgruppe der allgemeinen Gleichung n-ten Grades*.
Man überlegt sich dazu, dass der Fixpunktkörper von $\mathrm{Aut}_E(Z)$ aus den symmetrischen gebrochen rationalen Funktionen über $K$ in den Variablen $a_0, \dots, a_n$ besteht und dass $\mathrm{Aut}_E(Z)$ isomorph ist zur vollen symmetrischen Gruppe $S_n$.

**UE 500** ▶ **Übungsaufgabe 9.4.6.4.** Führen Sie diese Überlegungen durch. Hinweis: Man stößt kaum auf technische Schwierigkeiten. Das Interesse liegt vor allem auf einer begrifflich sauberen Durchführung. ◀ **UE 500**

## 9.5 Auflösung von Gleichungen durch Radikale

Dieser Abschnitt befasst sich mit jener Frage, aus der die Galoistheorie historisch ihren Ursprung nahm. Und zwar geht es um Lösungsformeln für algebraische Gleichungen in einer Variablen – das sind Gleichungen der Form $f(x) = 0$ für ein Polynom $f$ – durch Radikale. Das bedeutet, dass die gesuchte Formel die Koeffizienten von $f$ ausschließlich

mit Hilfe der vier Körperoperationen sowie Wurzelsymbolen verbindet. Die Schwierigkeit, eine solche Formel zu finden, hängt sehr stark vom Grad $n$ des Polynoms $f$ ab. Für $n = 1$ sind gar keine Wurzelsymbole nötig, und Lösungen der gesuchten Art – wenn auch natürlich nicht in moderner Symbolik – waren schon in der Antike bekannt. Die allgemeine Lösung für $n = 2$ stammt aus der frühmittelalterlichen Blüte des orientalischen Bagdad um das Jahr 800. Für $n = 3, 4$ waren italienische Mathematiker des 16. Jahrhunderts erfolgreich. Für $n \geq 5$ stand man dann etwa 300 Jahre lang an, bis Abel und Galois in der ersten Hälfte des 19. Jahrhunderts zeigten, dass und warum genau es für Gleichungen vom Grad $\geq 5$ keine allgemeine Formel der gesuchten Art geben kann. Wir beginnen in 9.5.1 mit der Präzisierung des Problems und der Definition der dafür hilfreichen Begriffe. Eine besondere Rolle spielt bei Radikalen die Adjunktion sogenannter reiner Wurzeln, d.h. Lösungen von Gleichungen der Gestalt $x^n - a = 0$. Die wichtigsten Aussagen dazu werden in 9.5.2 hergeleitet. Auf ihnen basiert der Beweis, dass radikale Erweiterungen stets auflösbare Galoisgruppen haben, siehe 9.5.3. Der (noch zu überarbeitende und mit * gekennzeichnete) Rest des Kapitels zielt auf den Beweis des Satzes von Galois ab, der (wenigstens für Charakteristik 0) auch die Umkehrung enthält: Ist die Galoisgruppe einer Gleichung auflösbar, so auch die Gleichung durch Radikale. Dieser Satz ist in 9.5.10 formuliert.

### 9.5.1 Problemanalyse

Gesucht ist eine Darstellung der Lösungen von

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 = 0$$

als Funktionen der Koeffizienten unter Einbeziehung von Grundrechnungsarten und „Radikalen“ $\sqrt[k]{c}$, d.h. von Lösungen von Gleichungen der Form $x^k - c = 0$. Derart dargestellte Elemente liegen also in einem Erweiterungskörper $E$ von $K$ mit $K = Z_0 \leq \ldots \leq Z_m = E$ wobei $Z_{i+1} = Z_i(u_i)$ und $u_i^{k_i} - c_i = 0$, $c_i \in Z_i$. Für $\mathrm{char}(K) = 0$ erweist sich die „Auflösbarkeit“ in diesem Sinn als äquivalent zur Auflösbarkeit der Galoisgruppe von $f$ im gruppentheoretischen Sinn (Satz von Galois 9.5.10.1).

**Definition 9.5.1.1.** $E$ heißt *radikale Erweiterung* von $K$, falls es endlich viele Elemente $u_i \in E$ und natürliche Zahlen $e_i$ gibt mit $E = K(u_1, \ldots, u_n)$ und $u_i^{e_i} \in K(u_1, \ldots, u_{i-1})$ für $i = 1, \ldots, n$.
Für $f \in K[x]$ heißt die Gleichung $f(x) = 0$ *auflösbar durch Radikale*, falls eine radikale Erweiterung $E$ existiert mit $K \leq Z_f \leq E$, wobei $Z_f$ der Zerfällungskörper von $f$ über $K$ ist.

**Proposition 9.5.1.2.** *Jede radikale Erweiterung ist endlichdimensional.*

**UE 501 ► Übungsaufgabe 9.5.1.3.** Beweisen Sie Proposition 9.5.1.2. **◄ UE 501**

Um zu zeigen, dass jede radikale Erweiterung eine auflösbare Galoisgruppe hat, werden wir uns zunächst überlegen, dass bei der Adjunktion einer einzigen reinen $n$-ten Wurzel,

das heißt einer Nullstelle eines Polynoms $f$ der Bauart $f(x) = x^n - a$, stets abelsche Galoisgruppen entstehen. Nach Definition setzen sich radikale Erweiterungen ausschließlich aus Adjunktionen reiner Wurzeln zusammen. Denken wir an die Galoiskorrespondenz aus dem Hauptsatz und an die Definition der Auflösbarkeit einer Gruppe über Subnormalreihen mit abelschen Faktoren, so scheint damit der Beweis im Wesentlichen schon erbracht. Obwohl bei genauerer Analyse der Situation noch einige weitere Komplikationen zu bedenken sind, kann man in diesen Überlegungen aber die wichtigsten Ideen für den gesuchten Beweis sehen. Es folgt nun die Ausführung des angedeuteten Programms.

### 9.5.2 Die Adjunktion reiner Wurzeln

Wir beginnen mit dem Spezialfall von Einheitswurzeln. Ohne bei jeder Einzelheit darauf zu verweisen, werden wir die Begriffsbildungen und Ergebnisse aus 6.2.5 über Einheitswurzeln und Kreisteilungspolynome verwenden.

**Proposition 9.5.2.1.** *Sei $K \leq E$ eine Körpererweiterung und $\zeta \in E$ eine primitive $n$-te Einheitswurzel. Dann ist $Z := K(\zeta)$ ein Zerfällungskörper für das Polynom $f(x) := x^n - 1$. Die Erweiterung $K \leq Z = K(\zeta)$ ist Galoissch mit abelscher Galoisgruppe.*

*Beweis.* In jedem Zerfällungskörper $Z_f$ des Polynoms $f(x) := x^n - 1$ bilden die $n$-ten Einheitswurzeln multiplikativ eine zyklische Untergruppe der Ordnung $n$, deren Erzeugende genau die primitiven $n$-ten Einheitswurzeln sind. Folglich ist $Z := K(\zeta)$ ein Zerfällungskörper von $f$ innerhalb $E$, auf den wir uns nun beziehen wollen. Die Erweiterung $K \leq Z$ ist sowohl normal (weil Zerfällungskörper) als auch separabel (wegen Satz 9.2.4.7, weil nach Satz 6.2.5.1 alle $\zeta^i$, $i = 0, \ldots, n-1$, paarweise verschieden sind). Nach Satz 9.2.4.3 ist $K \leq K(\zeta)$ also sogar Galoissch.
Jedes $\sigma \in \mathrm{Aut}_Z(K)$ bildet $\zeta$ wieder auf eine primitive Einheitswurzel ab, also auf ein $\zeta^i$ mit $i \in \mathbb{Z}_n^*$. Wegen $Z = K(\zeta)$ ist $\sigma$ durch den Wert $\sigma(\zeta)$ eindeutig bestimmt, also durch die Angabe von $i$. Wir schreiben für dieses $\sigma$ daher $\sigma = \sigma_i$. Entscheidend ist die Beziehung

$$\sigma_i\sigma_j(\zeta) = \sigma_i(\zeta^j) = \sigma_i(\zeta)^j = (\zeta^i)^j = \zeta^{ij} = \sigma_{ij}(\zeta),$$

aus der wir $\sigma_i\sigma_j = \sigma_{ij}$ ablesen. Weil $\zeta$ ein multiplikatives Erzeugendes der Ordnung $n$ ist, dürfen wir das Produkt $ij$ modulo $n$ interpretieren. Somit ist die Abbildung

$$\iota : G := G(f) \to \mathbb{Z}_n^*, \quad \sigma_i \mapsto i,$$

eine isomorphe Einbettung der Galoisgruppe $G(f)$ in die prime Restklassengruppe $\mathbb{Z}_n^*$. Diese ist abelsch, also ist auch $G(f)$ abelsch. □

Bemerkung zum obigen Beweis: Jede primitive $n$-te Einheitswurzel ist Nullstelle des $n$-ten Kreisteilungspolynoms $g_n$ über $K$. Dieses hat den Grad $\varphi(n) = |\mathbb{Z}_n^*|$ (Eulersche $\varphi$-Funktion). Über $K = \mathbb{Q}$ sind sämtliche Kreisteilungspolynome irreduzibel. (Das ist nicht trivial und wird hier nicht bewiesen. Dies Aussage ist Teil der späteren Proposition 9.5.8, deren Beweis in eine Übungsaufgabe ausgelagert wird.) In diesem Fall sind also genau die $n$-ten primitiven Einheitswurzeln die Konjugierten von $\zeta$. Folglich gibt

es zu jedem $i \in \mathbb{Z}_n^*$ auch ein $\sigma_i$, d.h. die Einbettung $\iota$ ist sogar surjektiv und somit ein Isomorphismus $G(f) \cong \mathbb{Z}_n^*$.

Ist eine primitive $n$-te Einheitswurzel $\zeta$ (und damit alle $n$-ten Einheitswurzeln) im Grundkörper vorhanden, so haben Erweiterungen um weitere reine $n$-te Wurzeln aus galoistheoretischer Sicht eine besonders einfache Struktur:

**Proposition 9.5.2.2.** *Sei $K$ ein Körper und $\zeta \in K$ eine $n$-te primitive Einheitswurzel. Weiters sei $K \leq E$ eine Körpererweiterung und $u \in E$ mit $u^n = a \in K$. Dann ist $Z = Z_f := K(u)$ ein Zerfällungskörper des Polynoms $f(x) := x^n - a$ über $K$. Die Galoisgruppe $G(f) = \mathrm{Aut}_K(Z)$ von $f$ ist zyklisch von einer Ordnung, die $n$ teilt, insbesondere also abelsch. Für* $\mathrm{char}\, K = 0$ *ist die Erweiterung $K \leq E$ Galoissch.*

*Beweis.* Die primitive Einheitswurzel $\zeta$ erzeugt multiplikativ eine zyklische Gruppe $\cong C_n$, bestehend aus den paarweise verschiedenen Potenzen $\zeta^i$, $i = 0, \ldots, n-1$. Folglich sind für diese Werte von $i$ auch die Elemente $u_i := \zeta^i u$ paarweise verschieden. Wegen $u_i^n = (\zeta^n)^i u^n = u^n = a$ sind die $u_i$ alle $n$ Nullstellen von $f$. Weil ihre Anzahl $n$ mit dem Grad von $f$ übereinstimmt, sind sie sogar sämtliche Nullstellen von $f$. Sie liegen alle in $K(\zeta, u) = K(\zeta)(u) = K(u)$, folglich ist $K(u) = Z$ bereits der Zerfällungskörper von $f(x) = x^n - a$.
Nach Proposition 9.2.1.4 permutiert jedes $\sigma \in \mathrm{Aut}_K(Z) = \mathrm{Aut}_K(K(u))$ die $u_i$ und ist durch den Wert $\sigma(u)$ beim Erzeuger $u$ bereits eindeutig festgelegt. Folglich gibt es eine injektive Abbildung

$$\iota : \mathrm{Aut}_K(E) \to \{0, 1, \ldots, n-1\}, \quad \sigma \mapsto i_\sigma = \iota(\sigma) \quad \text{mit} \quad \sigma(u) = u_{i_\sigma} = \zeta^{i_\sigma} u.$$

Identifizieren wir die $i \in \{0, 1, \ldots n-1\}$ mit den additiven Restklassen modulo $n$, so ist $\iota : \mathrm{Aut}_K(E) \to C_n$ also eine Abbildung in die zyklische Gruppe der Ordnung $n$. Wegen

$$\sigma_1\sigma_2(u) = \sigma_1(\zeta^{i_{\sigma_2}} u) = \zeta^{i_{\sigma_2}} \sigma_1(u) = \zeta^{i_{\sigma_2}} \zeta^{i_{\sigma_1}} u = \zeta^{i_{\sigma_1} + i_{\sigma_2}} u,$$

also $\iota(\sigma_1\sigma_2) = \iota(\sigma_1) + \iota(\sigma_2) \mod n$, ist $\iota$ ein Homomorphismus, aufgrund der Injektivität daher sogar eine isomorphe Einbettung in die zyklische Gruppe $C_n$. $\mathrm{Aut}_K(E)$ ist daher isomorph zu einer Untergruppe von $C_n$, also eine zyklische Gruppe (Proposition **??**) mit einer Ordnung, die $n$ teilt.
Für $\mathrm{char}\, K = 0$ ist die Erweiterung $K \leq E$ Galoissch: Denn erstens ist sie wegen Charakteristik 0 separabel (Proposition 9.2.4.1), und zweitens normal, weil $E = K(u)$ ja der Zerfällungskörper von $f(x) = x^n - a$ über $K$ ist (Satz 9.2.3.1). Beide Eigenschaften gemeinsam implizieren Galoissch (Satz 9.2.4.3). □

**UE 502** ► **Übungsaufgabe 9.5.2.3.** Was lässt sich im Sinne von Proposition 9.5.2.2 aussagen, wenn man auf die Voraussetzung $\zeta \in K$ verzichtet? ◄ **UE 502**

### 9.5.3 Radikale Erweiterungen haben auflösbare Galoisgruppen

Wir wollen nun zeigen: Die Galoisgruppe eines Polynoms $f$ über $\mathbb{Q}$, dessen Nullstellen sich durch Radikale ausdrücken lassen, ist stets auflösbar im Sinn von 8.3.2. Umgekehrt formuliert: Die Lösungen von Gleichungen $f(x) = 0$ mit einem Polynom $f \in \mathbb{Q}[x]$ mit nicht auflösbarer Galoisgruppe – wie etwa $f(x) = x^5 - 4x + 2$ über $K = \mathbb{Q}$ (siehe Übungsaufgabe 9.4.6.3) – lassen sich nicht durch Radikale im Sinn von 9.5.1 darstellen. Diese Behauptung ist in folgendem Satz enthalten:

**Theorem 9.5.3.1.** Ist $K \leq E$ eine radikale Erweiterung, dann ist $\mathrm{Aut}_K(Z)$ für jeden Zwischenkörper $Z$, $K \leq Z \leq E$, auflösbar. Insbesondere ist eine algebraische Gleichung $f(x) = 0$ mit einem Polynom $f \in \mathbb{Q}[x]$ nur dann durch Radikale auflösbar, wenn die Galoisgruppe von $f$ (= die Galoisgruppe des Zerfällungskörpers von $f$ über $\mathbb{Q}$) auflösbar ist.

*Beweis.* Der Einfachheit halber setzen wir $\mathrm{char}\, K = 0$ voraus, was ja der historisch interessante Fall ist. Die Komplikationen bei Primzahlcharakteristik sind Gegenstand von Übungsaufgabe 9.5.3.2.
In einem ersten Schritt wollen wir uns überlegen, dass für jede algebraische Galoissche Erweiterung $K \leq E$ mit auflösbarer Galoisgruppe $\mathrm{Aut}_K(E)$ auch sämtliche Zwischenkörper $Z$ eine auflösbare Galoisgruppe $\mathrm{Aut}_K(Z)$ über $K$ haben: Nach Proposition 9.2.2.3 ist $K \leq E$ als Galoissche Erweiterung auch normal. Somit lässt sich jedes $\sigma_0 \in \mathrm{Aut}_K(Z)$ zu einem $K$-Automorphismus $\sigma \in \mathrm{Aut}_K(E)$ fortsetzen, der notwendig $Z$ als Menge fest lässt. Derartige $\sigma$ bilden eine Untergruppe $H_Z \leq \mathrm{Aut}_K(E)$. Somit ist die Einschränkungsabbildung $\varphi : H_Z \to \mathrm{Aut}_K(Z)$ ein surjektiver Homomorphismus. Mit anderen Worten: $\mathrm{Aut}_K(Z)$ ist das homomorphe Bild einer Untergruppe der auflösbaren Gruppe $\mathrm{Aut}_K(E)$, nach Proposition 8.3.2.3 also selbst auflösbar.
Im zweiten Schritt zeigen wir, dass jede radikale Erweiterung in einer radikalen Erweiterung, die zusätzlich Galoissch ist, enthalten ist. Weil wir uns auf Charakteristik 0 beschränken, genügt es dafür laut Satz 9.2.4.4 zu einer radikalen Erweiterung $K \leq E$ eine Erweiterung $E \leq N$ zu finden, so dass $N$ über $K$ normal ist. Tatsächlich hat jeder normale Abschluss $N$ von $E$ über $K$ die gewünschten Eigenschaften: Mit $E$ sind auch alle $\sigma(E)$, $\sigma \in \mathrm{Aut}_K(N)$, radikal, durch iterierte Adjunktion der reinen Wurzeln also auch deren Erzeugnis. Dieses muss aber ganz $N$ sein, weil $N$ ja sämtliche über $K$ Konjugierte von Elementen von $E$ enthält.
Im dritten Schritt verschärfen wir die Aussage des zweiten Schritts: Zu jeder radikalen Erweiterung $K \leq E$ gibt es eine Erweiterung $K \leq N$, die zusätzlich nicht nur radikal und Galoissch ist, sondern außerdem eine primitive $n$-te Einheitswurzel $\zeta$ enthält, wobei wir $n$ später spezifizieren werden. Als Galoissche und somit normale Erweiterung ist $E$ nämlich Zerfällungskörper für eine Menge $S$ von Polynomen. Adjungieren wir zusätzlich $\zeta$, so erhalten wir mit $N(\zeta)$ einen Zerfällungskörper für $S \cup \{x^n - 1\}$, also wieder eine Galoissche radikale Erweiterung.
Wir resümieren die ersten drei Beweisschritte: Jede radikale Erweiterung $E$ von $K$ lässt sich zu einer Galoisschen radikalen Erweiterung $N$ von $K$ ausdehnen, die noch dazu eine beliebig vorgegebene $n$-te Einheitswurzel $\zeta$ enthält. Laut erstem Schritt genügt es, die

Auflösbarkeit der Galoisgruppe $\mathrm{Aut}_K(N)$ zu zeigen. Gemäß der Definition einer radikalen Erweiterung gibt es jedenfalls Elemente $u_1, \ldots, u_k$ mit

$$K \;\leq\; Z_0 := K(\zeta) \;\leq\; Z_1 := Z_0(u_1) \;\leq\; Z_2 := Z_1(u_2) \;\leq\; \ldots \;\leq\; Z_k := Z_{k-1}(u_k) = N$$

und $u_i^{n_i} \in Z_{i-1}$, $n_i \in \mathbb{N}$, $i = 1, \ldots, k$. Dabei steht es uns frei, $n$ als (kleinstes) gemeinsames Vielfaches der $n_i$ zu wählen. Weil $N$ Galoissch und endlichdimensional über $K$ ist, liefert der Hauptsatz 9.3.1.1 eine Zuordnung folgender Art:

$$\begin{array}{ccccccccccccc}
K & \leq & Z_0 & \leq & \ldots & \leq & Z_{i-1} & \leq & Z_i & \leq & \ldots & \leq & Z_k & = & N \\
\updownarrow & & \updownarrow & & & & \updownarrow & & \updownarrow & & & & \updownarrow & & \\
\mathrm{Aut}_K(N) & \geq & H_0 & \geq & \ldots & \geq & H_{i-1} & \geq & H_i & \geq & \ldots & \geq & H_k & = & \{\mathrm{id}\}
\end{array}$$

Alle Erweiterungen sind Galoissch, die erste laut Proposition 9.5.2.1, die übrigen laut Proposition 9.5.2.2. Mit Hilfe derselben Referenzen schließen wir auch, dass die Untergruppen eine Subnormalreihe mit abelschen Faktoren bilden. Also ist $\mathrm{Aut}_K(N)$ auflösbar. □

**UE 503** ► **Übungsaufgabe 9.5.3.2.** Der Beweis von Satz 9.5.3.1 wurde unter der Zusatzvoraussetzung $\mathrm{char}\, K = 0$ geführt. Welche Modifikationen sind für den Fall $\mathrm{char}\, K = p \in \mathbb{P}$ erforderlich? ◄ **UE 503**

Wir erinnern uns nochmals an Übungsaufgabe 9.4.6.3 (wonach das Polynom $f(x) = x^5 - 4x + 2$ eine nicht auflösbare Galoisgruppe $G(f) \cong S_5$ hat) sowie die daran anschließende Diskussion und resümieren:

**Folgerung 9.5.3.3** (Satz von Abel)**.** *Es gibt keine allgemeine Lösungsformel für algebraische Gleichungen vom Grad* $\geq 5$.

In Umgekehrung von Satz 9.5.3.1 kann man unter geeigneten Bedingungen von der Auflösbarkeit der Galoisgruppe auf die Auflösbarkeit der entsprechenden Gleichung durch Radikale schließen (siehe Satz 9.5.10.1 von Galois). Der Beweis dafür ist aber aufwendiger und erfordert einige weitere Begriffsbildungen, denen wir uns nun zuwenden.

### 9.5.4 Norm und Spur *

**Definition 9.5.4.1.** Sei $[E : K] < \infty$, $K \leq E \leq \overline{K}^{\mathrm{alg}}$ (algebraischer Abschluss von $K$). Seien $\sigma_1, \ldots, \sigma_r$ sämtliche $K$-Monomorphismen von $E$ nach $\overline{K}^{\mathrm{alg}}$. Für $u \in E$ heißt

$$N(u) = N_K^E(u) := \left( \prod_{j=1}^{r} \sigma_j(u) \right)^{[E:K]_i}$$

die *Norm* von $u$ über $K$,

$$T(u) = T_K^E(u) := [E : K]_i \cdot \sum_{j=1}^{r} \sigma_j(u)$$

die *Spur* von $u$. Hier ist $[E : K]_i = [E : S]$ der *„Inseparabilitätsgrad“* von $E$ über $K$, wobei $S$ die größte separable Erweiterung von $K$ in $E$ ist. $[S : K]$ heißt der *„Separabilitätsgrad“* von $E$ über $K$.

Ist $K \leq E$ separabel (was z.B. bei Charakteristik 0 stets der Fall ist), so ist $[E : K]_i = 1$, und die Formeln aus Definition 9.5.4.1 vereinfachen sich entsprechend.
Wir wollen uns auf Galoissche Erweiterungen konzentrieren. Sei also $E : K$ Galoissch und $Aut_K(E) = \{\sigma_1, \ldots, \sigma_r\}$. Man beachte, dass nach Satz 9.2.3.1 (iii) die Monomorphismen von $E$ nach $\overline{K}^{alg}$ genau die Elemente von $Aut_K(E)$ sind. Daher gilt im Galoisschen Fall

$$N(u) := N_K^E(u) = \prod_{j=1}^{r} \sigma_j(u) \quad \text{und} \quad T(u) := T_K^E(u) = \sum_{j=1}^{r} \sigma_j(u).$$

Man beachte

$$\sigma(N(u)) = \prod_{j=1}^{r} \sigma(\sigma_j(u)) = \prod_{j=1}^{r} \sigma_j(u) = N(u) \; \forall \sigma \in Aut_K(E)$$

und analog $\sigma(T(u)) = T(u)$. Es folgt:

(a) $N_K^E(u) \in (Aut_K(E))' = K$. Analog folgt $T_K^E(u) \in K$.

(b) $N_K^E(u \cdot v) = N_K^E(u) \cdot N_K^E(v)$, $T_K^E(u + v) = T_K^E(u) + T_K^E(v)$.

(c) Ist $u \in K$, so folgt $N_K^E(u) = u^{[E:K]}$ und $T_K^E(u) = [E : K] \cdot u$.

**Beispiel 9.5.4.2.** Ist $K = \mathbb{R}$ und $E = \mathbb{C}$, so sind Norm und Spur gegeben durch

$$N(u) = u \cdot \overline{u} = |u|^2 \text{ und } T(u) = u + \overline{u} = 2 \cdot \mathrm{Re}(u).$$

### 9.5.5 Zyklische und abelsche Erweiterungen *

**Lemma 9.5.5.1.** *Jede Menge paarweise verschiedener Automorphismen eines Körpers $K$, betrachtet als Elemente des $K$-Vektorraumes $K^K$, ist linear unabhängig.*

*Beweis.* [3] Angenommen, es wäre

$$\sum_{i=1}^{n} a_i \sigma_i = 0 \tag{9.3}$$

mit $(a_1, \ldots, a_n) \neq (0, \ldots, 0)$, $n \geq 2$ minimal (also $a_1, \ldots, a_n \neq 0$) und $\sigma_i \in Aut_K(E)$ paarweise verschieden. Dann gibt es ein $v$ mit $\sigma_1(v) \neq \sigma_2(v)$. Aus (9.3) folgt

$$0 = \sum_{i=1}^{n} a_i \sigma_i(u \cdot v) = \sum_{i=1}^{n} a_i (\sigma_i(u) \cdot \sigma_i(v))$$

[3] Man beachte die Ähnlichkeiten mit dem Beweis von Lemma 9.3.2.2.

mit $u \in K$ beliebig. Durch Anwendung auf $u$ und nach Multiplikation mit $\sigma_1(v)$

$$0 = \sum_{i=1}^{n} a_i \sigma_i(u)\sigma_1(v).$$

Zieht man diese beiden Gleichungen voneinander ab, erhält man

$$0 = \sum_{i=2}^{n} a_i \underbrace{(\sigma_i(v) - \sigma_1(v))}_{=:b_i} \cdot \sigma_i(u)$$

für alle $u \in K$. Das heißt aber

$$\sum_{i=2}^{n} a_i b_i \sigma_i = 0$$

mit $a_2 b_2 \neq 0$, was ein Widerspruch zur Minimalität von $n$ ist. □

**Satz 9.5.5.2** (Hilbert 90)**.** [4] *Sei $K \leq E$ Galoissch und $Aut_K(E) \cong C_n$ zyklisch mit Erzeuger $\sigma$. Dann ist*

$$N_K^E(u) = 1 \quad \textit{genau dann, wenn} \quad \exists v \in E^* = E \setminus \{0\} \textit{ mit } u = v\sigma(v)^{-1}.$$

*Analog gilt*

$$T_K^E(u) = 0 \quad \textit{genau dann, wenn} \quad \exists v \in E \textit{ mit } u = v - \sigma(v).$$

*Beweis.* Wir beweisen hier nur die erste Aussage. Die zweite kann sehr ähnlich bewiesen werden und wird im Folgenden nicht benötigt. Deshalb bleibt ihr Beweis einer Übungsaufgabe vorbehalten. Da $\sigma$ ein Erzeuger der Automorphismengruppe ist, gilt

$$N(u) = \prod_{j=0}^{n-1} \sigma^j(u) = u\sigma(u)\sigma^2(u) \cdot \ldots \cdot \sigma^{n-1}(u).$$

Angenommen, es existiert so ein $v \in E^*$ mit $u = v\sigma(v)^{-1}$. Dann ist (Teleskopprodukt)

$$\begin{aligned} N(u) &= \prod_{j=0}^{n-1} \sigma^j(v\sigma(v)^{-1}) = \\ &= (v\sigma(v)^{-1})(\sigma(v)\sigma^2(v)^{-1})(\sigma^2(v)\sigma^3(v)^{-1}) \ldots (\sigma^{n-1}(v)\sigma^n(v)^{-1}) = \\ &= v \underbrace{\sigma(v)^{-1}\sigma(v)}_{=1} \sigma^2(v)^{-1} \cdot \ldots \cdot \sigma^{n-2}(v) \underbrace{\sigma^{n-1}(v)^{-1}\sigma^{n-1}(v)}_{=1} \underbrace{\sigma^n(v)^{-1}}_{=v^{-1}} \\ &= 1 \end{aligned}$$

[4] Der Name dieses Satzes bezieht sich auf die Nummerierung in Hilberts berühmtem *Zahlbericht* aus dem Jahre 1897.

Sei nun umgekehrt $N(u) = 1$. Dann ist $u \neq 0$, folglich $a_j := \prod_{i=0}^{j} \sigma^i(u) \neq 0$ für $j = 0, \ldots, n-1$. Nach Lemma 9.5.5.1 gibt es ein $y \in E$, so dass

$$v := \sum_{i=0}^{n-1} a_j \sigma^j(y) = \sum_{j=0}^{n-1} \left( \prod_{i=0}^{j} \sigma^i(u) \right) \sigma^j(y) \neq 0.$$

Man rechnet nach, dass $\sigma(v) = u^{-1}v$ gilt. Das heißt aber gerade, dass $u = v\sigma(v)^{-1} \neq 0$. □

**UE 504** ► **Übungsaufgabe 9.5.5.3.** Beweisen Sie in Satz 9.5.5.2 (Hibert 90) die zweite, die Spur betreffende Aussage. ◄ **UE 504**

**Definition 9.5.5.4.** Ist $K \leq E$ Galoissch und algebraisch, so heißt die Erweiterung *zyklisch* bzw. *abelsch*, falls die Automorphismengruppe $\mathrm{Aut}_K(E)$ zyklisch bzw. abelsch ist.

### 9.5.6 Die Rolle der primitiven Einheitswurzeln *

Zur Erinnerung:

**Definition 9.5.6.1.** Ein Element $\zeta \in K$ heißt $n$-te *Einheitswurzel*, falls $\zeta^n = 1$. Hat $\zeta$ überdies die multiplikative Ordnung $n$, so nennt man $\zeta$ eine *primitive $n$-te Einheitswurzel*.

*Bemerkung* 9.5.6.2. Ist $\zeta$ eine $n$-te primitive Einheitswurzel und $d$ ein Teiler von $n$, so ist offenbar $\zeta^{\frac{n}{d}} =: \eta$ eine $d$-te primitive Einheitswurzel. Gilt $f(u) = 0$ für $f(x) = x^d - a$ mit $a \in K \setminus \{0\}$, so sind $u, \eta u, \eta^2 u, \ldots, \eta^{d-1} u$ sämtliche verschiedenen Wurzeln von $f$ und für $\eta \in K$ ist $K \leq K(u)$ der Zerfällungskörper von $f$ über $K$. Außerdem ist $K(u) : K$ separabel und normal, also Galoissch.

**Satz 9.5.6.3.** *Sei $\zeta \in K$ eine primitive $n$-te Einheitswurzel, $K \leq E$. Dann sind die folgenden Aussagen äquivalent:*

*(i) $E$ ist Zerfällungskörper von $f(x) = x^n - a \in K[x]$. (In diesem Fall ist $E = K(u)$ für ein $u$ mit $f(u) = 0$.)*

*(ii) $K \leq E$ ist zyklisch von einem Grad $d$ mit $d \mid n$.*

*(iii) $E$ ist Zerfällungskörper eines irreduziblen Polynoms der Gestalt $f(x) = x^d - b \in K[x]$ mit $d \mid n$. (In diesem Fall ist $E = K(v)$ mit $f(v) = 0$.)*

*Beweis.* (i) ⇒ (ii): Nach obiger Bemerkung 9.5.6.2 existiert eine Wurzel $u$ des Polynoms $f(x) = x^n - a$ mit $E = K(u)$, und $E : K$ ist Galoissch. Das heißt, jedes $\sigma \in Aut_K(E)$ ist durch $\sigma(u) = \zeta^{i_\sigma} u$ eindeutig festgelegt. Die Abbildung $\varphi : \sigma \mapsto \zeta^{i_\sigma}$ ist daher eine Einbettung von $\mathrm{Aut}_K(K(E)$ in die multiplikative Gruppe der $n$-ten Einheitswurzeln (zyklisch), also $Aut_K(E) \cong C_d$ mit $d \mid n$.

(ii) $\Rightarrow$ (iii): Sei $\sigma$ ein Erzeuger von $G = Aut_K(E)$ der Ordnung $d$, $\eta := \zeta^{\frac{n}{d}}$ ist primitive $d$-te Einheitswurzel. Da $\zeta$ ein Element von $K$ ist, ist $\sigma(\eta) = \eta$ für alle $\sigma \in G$. Daher ist

$$N_K^E(\eta) = \eta^{[E:K]} = \eta^d = 1.$$

Nach Satz 9.5.5.2 (Hilbert 90) gibt es ein $u \in E^\backslash\{0\}$ mit $\eta = u\sigma(u)^{-1}$. Sei $v := u^{-1}$, dann ist

$$\sigma(v) = \sigma(u)^{-1} = \eta u^{-1} = \eta v,$$

und deshalb

$$\sigma(v^d) = (\eta v)^d = \eta^d v^d = v^d =: b \in \langle\sigma\rangle' = Aut_K(E)' = K.$$

Es folgt, dass $v$ eine Wurzel des Polynoms $f(x) := x^d - b$ ist. Wir wollen noch zeigen, dass $f$ irreduzibel ist. Sämtliche Nullstellen von $f$ sind gegeben durch $\eta^i v = \sigma^i(v)$, $i = 0, \ldots, d-1$. $K(v) \cong K(\eta^i v)$, also sind $\eta^i v = \sigma^i(v)$, $i = 0, \ldots, d-1$, Nullstellen des selben irreduziblen Polynoms $g$ vom Grad $\geq d$. Daher muss $g = f$ irreduzibel sein.
(iii) $\Rightarrow$ (i): Sei $v$ eine Wurzel von $x^d - b \in K[x]$, dann ist $E = K(v)$. Nun ist

$$(\zeta v)^n = \zeta^n v^n = v^{d\frac{n}{d}} = b^{\frac{n}{d}} \in K,$$

daher ist $\zeta v$ eine Wurzel von $x^n - a \in K[x]$, wobei $a := b^{\frac{n}{d}}$. $K(\zeta v)$ ist Zerfällungskörper von $x^n - a$. Da aber $\zeta \in K$ ist $E = K(v) = K(\zeta v)$. □

### 9.5.7 Kreisteilungskörper und -polynome *

In diesem Unterabschnitt stehen jene Körpererweiterungen im Mittelpunkt, die den Einheitswurzeln entsprechen. Wegen ihrer Interpretation auf dem Einheitskreis im Fall Charakteristik 0 spricht man auch von Kreisteilungskörpern.

**Definition 9.5.7.1.** Ein Zerfällungskörper von $f(x) = x^n - 1$ über $K$ heißt *zyklotomische (Kreisteilungs-)Erweiterung* von $K$ oder der *Kreisteilungskörper* der Ordnung $n$ über $K$.

Aus der elementaren Zahlentheorie ist die Eulersche $\varphi$-Funktion bekannt. Dennoch wiederholen wir ihre Definition.

**Definition 9.5.7.2.** Die *Eulersche $\varphi$-Funktion* ist für $n = 1, 2, \ldots$ definiert als

$$\varphi(n) := |\{i : 1 \leq i \leq n \text{ mit } \mathrm{ggT}(i, n) = 1\}|.$$

Ihre Werte ergeben sich aus der folgenden Formel.

**Proposition 9.5.7.3.** *Seien $E \subseteq \mathbb{P}$ eine endliche Menge von Primzahlen und $e_p \geq 1$ natürliche Zahlen. Dann gilt*

$$\varphi\left(\prod_{p \in E} p^{e_p}\right) = \prod_{p \in E} (p-1)p^{e_p - 1}.$$

**UE 505 ► Übungsaufgabe 9.5.7.4.** Beweisen Sie die Formel aus Proposition 9.5.7.3 **◄ UE 505**

Im Unterschied zu Satz 9.5.6.3 wird von der Einheitswurzel $\zeta$ im folgenden Satz nicht vorausgesetzt, dass sie im Grundkörper $K$ liegt.

**Satz 9.5.7.5.** *Sei $E$ ein Kreisteilungskörper der Ordnung $n$ über $K$,* $\mathrm{char}(K) \nmid n$ *(z.B.* $\mathrm{char}(K) = 0$*). Dann gilt:*

*(a) $E = K(\zeta)$, wobei $\zeta$ eine primitive $n$-te Einheitswurzel ist.*

*(b) $K \leq E$ ist abelsch, $[E : K] = d$ mit $d \mid \varphi(n)$. Falls $n \in \mathbb{P}$, so ist $K \leq E$ auch zyklisch.*

*(c) $Aut_K(E) \cong A \leq (\mathbb{Z}_n^*, \cdot)$ (multiplikative Gruppe der primen Restklassen modulo $n$), $|A| = d$.*

*Beweis.* Punkt (a) ist klar. $E = K(\zeta)$ ist separabel und normal über $K$, also Galoissch. Ein Element $\sigma \in Aut_K(E)$ ist durch $\sigma(\zeta)$ eindeutig festgelegt, wobei $\sigma(\zeta)$ wieder eine primitive $n$-te Einheitswurzel sein muss. Für $\sigma_1, \sigma_2 \in Aut_K(E)$ gibt es also $i_1, i_2 \in \mathbb{Z}_n^*$, sodass

$$\sigma_1(\zeta) = \zeta^{i_1} \text{ und } \sigma_2(\zeta) = \zeta^{i_2}.$$

Deshalb, und wegen

$$\sigma_1\sigma_2(\zeta) = \sigma_1(\zeta^{i_2}) = \sigma_1(\zeta)^{i_2} = \left(\zeta^{i_1}\right)^{i_2} = \zeta^{i_1 \cdot i_2}$$

lässt sich die Automorphismengruppe in $\mathbb{Z}_n^*$ einbetten. Insbesondere ist also $[E : K] = |Aut_K(E)| = d$ ein Teiler der Gruppenordnung $\varphi(n)$ von $\mathbb{Z}_n^*$. Ist $n \in \mathbb{P}$, so ist $\mathbb{Z}_n^*$ zyklisch. Damit sind auch die Punkte (b) und (c) gezeigt. □

**Definition 9.5.7.6.** Seien $n \in \mathbb{N}$ und $\zeta_1, \ldots, \zeta_{\varphi(n)} \in E$ sämtlichen primitiven $n$-ten Einheitswurzeln, so heißt

$$\Phi_n(x) := \prod_{i=1}^{\varphi(n)} (x - \zeta_i)$$

das *$n$-te Kreisteilungspolynom* (über $K$ mit $\mathrm{char}(K) \nmid n$).

*Bemerkung* 9.5.7.7. Jede $n$-te Einheitswurzel ist genau für ein $d \mid n$ als $d$-te Einheitswurzel primitiv. Daher ist

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x),$$

wobei $\Phi_d(x) \in P[x]$ die Kreisteilungspolynome und $P$ den Primkörper von $K$ bezeichnen. Speziell im Fall $\mathrm{char}(K) = 0$ gilt sogar $\Phi_d(x) \in \mathbb{Z}[x]$. Um das zu sehen, betrachtet man

induktiv:

$$\begin{aligned}
\Phi_1(x) &= x-1\\
\Phi_2(x) &= \frac{x^2-1}{x-1} = x+1\\
\Phi_3(x) &= \frac{x^3-1}{x-1} = x^2+x+1\\
\Phi_4(x) &= \frac{x^4-1}{(x-1)(x+1)} = x^2+1\\
&\vdots\\
\Phi_n(x) &= \frac{x^n-1}{\prod\limits_{\substack{d\neq n\\ d\mid n}} \Phi_d(x)}.
\end{aligned}$$

**Proposition 9.5.7.8.** *Sei $E$ der Kreisteilungskörper der Ordnung $n$ über $\mathbb{Q}$ und $\Phi_n(x)$ das $n$-te Kreisteilungspolynom. Dann gilt:*

*(a) $\Phi_n(x)$ ist irreduzibel in $\mathbb{Q}[x]$ und $\Phi_n(x) \in \mathbb{Z}[x]$.*

*(b) $[E:\mathbb{Q}] = \varphi(n)$.*

*(c) $Aut_{\mathbb{Q}}(E) \cong (\mathbb{Z}_n^*, \cdot)$.*

**UE 506 ► Übungsaufgabe 9.5.7.9.** Beweisen Sie Proposition 9.5.7.8. Hinweis: [H]. **◄ UE 506**

### 9.5.8 Nochmals auflösbare Galoisgruppen *

**Lemma 9.5.8.1.** *Sei $K$ ein Körper mit $\mathrm{char}(K) = 0$. Ist $K \leq E$ radikal und Galoissch, so ist $\mathrm{Aut}_K(E)$ auflösbar.*

*Beweis.* Sei $E = E_n$, $E_i = K(u_1, \ldots, u_i)$, $u_i^{m_i} \in E_{i-1}$, $m = \prod_{i=1}^n m_i$ und $\zeta$ eine primitive $m$-te Einheitswurzel.
Zunächst sei zusätzlich $\zeta \in K$. In der Galoiskorrespondenz

$$\begin{array}{ccccccccccccc}
K & = & E_0 & \leq & \ldots & \leq & E_{i-1} & \leq & E_i & \leq & \ldots & \leq & E_n & = & E\\
 & & \updownarrow & & & & \updownarrow & & \updownarrow & & & & \updownarrow & & \\
G & = & H_0 & \geq & \ldots & \geq & H_{i-1} & \geq & H_i & \geq & \ldots & \geq & H_n & = & \{\mathrm{id}\}
\end{array}$$

sind nach 9.5.6.3 alle $E_i : E_{i-1}$ zyklisch, außerdem Galoissch. Nach dem Hauptsatz 9.3.1.1 sind dann alle $H_i \lhd H_{i-1}$ und $H_{i-1}/H_i \cong \mathrm{Aut}_{E_{i-1}} E_i$ abelsch. Da abelsche Gruppen auflösbar sind, ist die Subnormalreihe $G = H_0 \geq \ldots \geq H_{i-1} \geq H_i \geq \ldots \geq H_n = \{\mathrm{id}\}$ auflösbar. Daraus folgt, dass auch $G$ auflösbar ist.

Sei nun $\zeta \notin K$. $E(\zeta)$ ist Zerfällungskörper über $K$ und damit normal. Weil $\mathrm{char}(K) = 0$ ist, ist die Erweiterung $E(\zeta) : K$ Galoissch. Nochmals nach dem Hauptsatz 9.3.1.1 ist dann auch $E(\zeta) : K(\zeta)$ Galoissch. Aus dem bereits Bewiesenen folgt, dass $Aut_{K(\zeta)}(E(\zeta))$ auflösbar ist. Nach dem Hauptsatz gilt außerdem

$$\mathrm{Aut}_K(K(\zeta)) \cong \mathrm{Aut}_K(E(\zeta))/\mathrm{Aut}_{K(\zeta)}(E(\zeta))$$

und

$$\mathrm{Aut}_K(E) \cong \mathrm{Aut}_K(E(\zeta))/\mathrm{Aut}_E(E(\zeta)).$$

Satz 9.5.7.5 impliziert, dass $\mathrm{Aut}_K(K(\zeta))$ und $\mathrm{Aut}_E(E(\zeta))$ auflösbar sind. Wegen allgemeiner Eigenschaften auflösbarer Gruppen ist $\mathrm{Aut}_K(E(\zeta))$ und damit auch $\mathrm{Aut}_K(E)$ auflösbar. □

**Lemma 9.5.8.2.** *Ist $E$ eine radikale Erweiterung von $K$ und $N$ der normale Abschluss von $E$ über $K$, dann ist auch $N : K$ radikal.*

**UE 507 ► Übungsaufgabe 9.5.8.3.** Beweisen Sie Lemma 9.5.8.2 **◄ UE 507**

**Satz 9.5.8.4.** *Sei $K$ ein Körper mit $\mathrm{char}(K) = 0$, $K \leq Z \leq E$ und $E : K$ radikal. Dann ist $Aut_K(Z)$ auflösbar. Insbesondere ist die Galoisgruppe einer auflösbaren Gleichung auflösbar.*

*Beweis.* Sei $K_0$ der Fixpunktkörper von $Aut_K(Z)$. Wir müssen zeigen, dass $Aut_K(Z) = Aut_{K_0}(Z)$ auflösbar ist. Sei $N$ der normale Abschluss von $E$ über $K_0$ und $K_1$ der Fixpunktkörper von $Aut_{K_0}(N)$. Mit $E : K$ ist auch $E : K_0$ radikal. Nach Lemma 9.5.8.2 ist $N : K_0$ und damit auch $N : K_1$ radikal. Da $N : K_1$ nach Definition von $K_1$ auch Galoissch ist, folgt aus Lemma 9.5.8.1 die Auflösbarkeit von $Aut_{K_1}(N) = Aut_{K_0}(N)$. Nach Definition von $K_0$ ist $Z : K_0$ Galoissch und nach Lemma 9.3.3.2 ist $Z$ stabil bzgl. $K_0$ und $N$. Daher ist die Abbildung $\varphi\colon Aut_{K_0}(N) \to Aut_{K_0}(Z)$ definiert durch

$$\varphi(\sigma) := \sigma|_Z$$

wohldefiniert. Da sich jeder $K_0$-Automorphismus von $Z$ zu einem $K_0$-Automorphismus von $N$ fortsetzen lässt, ist $\varphi$ ein surjektiver Homomorphismus. Damit ist $Aut_K(Z) = Aut_{K_0}(Z) = \varphi(Aut_{K_0}(N))$ auflösbar. □

**UE 508 ► Übungsaufgabe 9.5.8.5.** Zeigen Sie, dass Satz 9.5.8.4 auch für beliebige Charakteristik von $K$ gilt. **◄ UE 508**

### 9.5.9 Auflösbare Galoisgruppen erzwingen Auflösbarkeit durch Radikale *

**Satz 9.5.9.1.** *Sei* $[Z : K] < \infty$, $Z : K$ *Galoissch,* $\mathrm{Aut}_K(Z)$ *auflösbar und* $\mathrm{char}(K) \nmid [Z : K]$. *Dann existiert ein Erweiterungskörper* $E \geq Z$, *sodass* $E : K$ *eine radikale Erweiterung ist.*

*Beweis.* Da $\mathrm{Aut}_K(Z) =: G$ auflösbar ist, gibt es einen Normalteiler $H \lhd G$ mit $[G : H] = p \in \mathbb{P}$. $Z$ ist Galoissch über $K$, daher $|G| = [Z : K]$, woraus $\mathrm{char}(K) \nmid p$ folgt. Sei $\zeta$ eine primitive $p$-te Einheitswurzel. Es genügt zu zeigen, dass eine radikale Erweiterung $E$ von $K(\zeta)$ mit $Z(\zeta) \leq E$ existiert, da $K(\zeta)$ klarerweise radikal über $K$ ist.
$Z$ ist Galoissch über $K$ und damit nach Lemma 9.3.3.2 stabil bezüglich $K$ und $Z(\zeta)$. Daher ist die Abbildung $\theta\colon\ \mathrm{Aut}_{K(\zeta)}(Z(\zeta)) \to G$ definiert durch

$$\theta(\sigma) := \sigma|_Z$$

wohldefiniert. $\theta$ ist ein injektiver Homomorphismus, denn ist $\theta(\sigma) = \mathrm{id}_Z$, dann gilt $\sigma|_{Z \cup K(\zeta)} = \mathrm{id}$, also $\sigma = \mathrm{id}_{Z(\zeta)}$. Da $G$ auflösbar ist und $\mathrm{Aut}_{K(\zeta)}(Z(\zeta))$ unter $\theta$ isomorph zu einer Untergruppe von $G$ ist, ist auch $\mathrm{Aut}_{K(\zeta)}(Z(\zeta))$ auflösbar.
Der Beweis erfolgt nun durch Induktion nach $n := [Z : K]$. Der Fall $n = 1$ ist trivial. Gelte nun die Behauptung für alle $k < n$.
1. Fall: $\theta$ ist ein Isomorphismus, also $Aut_{K(\zeta)}(Z(\zeta)) \cong G$. Definiere

$$J := \theta^{-1}(H) \lhd Aut_{K(\zeta)}(Z(\zeta)),$$

dann ist $[Aut_{K(\zeta)}(Z(\zeta)) : J] = p$. Sei weiters

$$P := J' = \mathrm{Aut}_P(Z(\zeta))' \leq Z(\zeta).$$

Wir betrachten die Galoisverbindung:

$$\begin{array}{ccccc} K(\zeta) & \subsetneq & P & \leq & Z(\zeta) \\ \updownarrow & & \updownarrow & & \updownarrow \\ Aut_{K(\zeta)}(Z(\zeta)) & \trianglerighteq & J & \trianglerighteq & \{\mathrm{id}\} \end{array}$$

Nach dem Hauptsatz 9.3.1.1 ist $P$ über $K(\zeta)$ Galoissch und

$$\mathrm{Aut}_{K(\zeta)}(P) \cong \mathrm{Aut}_{K(\zeta)}(Z(\zeta))/J.$$

$[\mathrm{Aut}_{K(\zeta)}(Z(\zeta)) : J] = p$ impliziert, dass $J = P' \cong C_p$. Also ist $P$ eine zyklische Erweiterung von $K(\zeta)$. Nach Satz 9.5.6.3 ist $P = K(\zeta)(u)$, dabei ist $u$ Wurzel eines irreduziblen Polynoms der Form $x^p - a \in K(\zeta)[x]$. Daher ist $P$ eine radikale Erweiterung von $K(\zeta)$ und

$$[Z(\zeta) : P] < [Z(\zeta) : K(\zeta)] = n.$$

Außerdem ist $\mathrm{Aut}_P(Z(\zeta))$ als Untergruppe von $\mathrm{Aut}_{K(\zeta)}(Z(\zeta))$ auflösbar und wieder nach dem Hauptsatz 9.3.1.1 ist $P \leq Z(\zeta)$ Galoissch. Die Induktionsvoraussetzung impliziert

die Existenz einer radikalen Erweiterung $E$ von $P$ mit $Z(\zeta) \leq E$. Diese Erweiterung liefert das Gewünschte.
2. Fall: $\theta$ ist nicht surjektiv, also $\mathrm{Aut}_{K(\zeta)}(Z(\zeta))$ ist isomorph zu einer echten Untergruppe von $G$. Dann gilt

$$[Z(\zeta) : K(\zeta)] = |\operatorname{Aut}_{K(\zeta)}(Z(\zeta))| < |\operatorname{Aut}_K(Z)| = [Z : K] = n.$$

Anwenden der Induktionsvoraussetzung liefert eine radikale Erweiterung $E$ von $K(\zeta)$ mit $Z(\zeta) \leq E$. □

### 9.5.10 Zusammenfassung: Der Satz von Galois

**Satz 9.5.10.1** (Satz von Galois)**.** *Sei $K$ ein Körper, $f \in K[x]$ vom Grad $n$ und* $\mathrm{char}(K) = 0$*. Die Gleichung $f(x) = 0$ lässt sich genau dann durch Radikale lösen, wenn die Galoisgruppe $G(f)$ von $f$ auflösbar ist.*

*Beweis.* Die Aussage ist die Synthese der Sätze 9.5.8.4 und 9.5.9.1. □

*Bemerkung* 9.5.10.2. Der Satz von Galois gilt auch für eine Charakteristik $\mathrm{char}(K) \neq 0$, sofern sie kein Teiler von $n!$ für $n := \mathrm{grad}(f)$ ist.

*Bemerkung* 9.5.10.3. Um die vorangegangenen Sätze auch für $\mathrm{char}(K) = p \in \mathbb{P}$ zu erhalten, kann der Begriff „radikale Erweiterung“ folgendermaßen umdefiniert werden. $E$ ist dann eine radikale Erweiterung von $K$, falls es eine endliche Folge von Erweiterungen

$$K = E_0 \leq E_1 \leq \ldots \leq E_n = E$$

gibt, so dass für jedes $1 \leq i \leq n$ gilt: $E_i = E_{i-1}(u_i)$ und eine der beiden folgenden Aussagen zutrifft:

(i) $u_i^{m_i} \in E_{i-1}$ für ein $m_i > 0$, oder

(ii) $\mathrm{char}(K) = p$ und $u_i^p - u_i \in E_{i-1}$.

**UE 509** ► **Übungsaufgabe 9.5.10.4.** (1) Rekapitulieren Sie die klassischen Unmöglichkeitsbeweise folgender Konstruktionsaufgaben mit Zirkel und Lineal: Würfelverdoppelung, Winkeldreiteilung, Quadratur des Kreises. ◄ **UE 509**

(2) Die Konstruktion des regelmäßigen $n$-Ecks mit Zirkel und Lineal ist genau dann möglich, wenn $n = 2^k \prod_{i=1}^{m} p_i$ mit $k \in \mathbb{N}$ und paarweise verschiedenen Primzahlen $p_i$ der Gestalt $p_i = 2^{2^{e_i}} + 1$ mit $e_i \in \mathbb{N}$ (Fermatsche Primzahlen). Im Gegensatz zu den Konstruktionen aus dem ersten Teil ist hier für den Beweis Galoistheorie substantiell erforderlich. Erläutern Sie dies.

# 10 Kommutative Ringe und Nullstellensatz

In diesem Kapitel stehen kommutative Ringe $R$ im Mittelpunkt, meist mit 1. Weil Ideale $I \lhd R$ auch als $R$-Moduln aufgefasst werden können, treten immer wieder auch Moduln in den Vordergrund. Ähnlich wie wir das schon an früheren Stellen gesehen haben, ermöglichen Kettenbedingungen interessante Ergebnisse. Noethersche Moduln und Ringe, die im Zentrum des ersten Abschnitts 10.1 stehen, sind explizit über die Kettenbedingung ACC an den Untermodul- bzw. an den Idealverband definiert. Auch der Begriff der Ganzheit von Ringerweiterungen und deren Elemente (siehe 10.2) hängt eng mit Kettenbedingungen zusammen. Mit seiner Hilfe lassen sich wichtige Hilfsresultate herleiten, die schließlich im Beweis des Hilbertschen Nullstellensatzes in 10.3 eine wichtige Rolle spielen. Dabei geht es um algebraische Gleichungssysteme in mehreren Variablen.

## 10.1 Noethersche Moduln und Ringe

In Hauptidealringen wird definitionsgemäß jedes Ideal von einem einzigen Element erzeugt. Schwächt man diese Eigenschaft etwas ab, so stößt man auf den Begriff eines Noetherschen Ringes, wo jedes Ideal endlich erzeugt ist. Wie schon aus allgemeinerem Kontext bekannt, hängen derartige Eigenschaften eng mit Ketten- und Maximalbedingungen an den Idealverband eines Ringes zusammen. Etwas allgemeiner ist der Gesichtspunkt, statt der Ideale in einem Ring $R$ Untermoduln von $R$-Moduln zu betrachten. Entsprechend beginnt der vorliegende Abschnitt in 10.1.1 mit Kettenbedingungen für Moduln, die in 10.1.2 auf Ringe übertragen werden. Im Zentrum stehen dabei kommutative Ringe mit 1, deren Idealverband die aufsteigende Kettenbedingung erfüllt, sogenannte Noethersche Ringe. Eine der fundamentalen Tatsachen in diesem Zusammenhang ist der Hilbertsche Basissatz (10.1.3): Der Polynomring in einer und folglich auch in endlich vielen Variablen über einem Noetherschen Ring ist wieder Noethersch. Nach einem kurzen Einschub über Primideale (SS-primideale) bietet 10.1.5 zum Abschluss weitgehend ohne Beweise, einen Überblick über die wichtigsten Konzepte und Ergebnisse der Idealtheorie über Noetherschen Ringen.

### 10.1.1 Kettenbedingungen für Moduln

Die folgende Definition ist eine Spezifikation allgemeiner ordnungstheoretischer Konzepte, die wir schon in 2.1.2 kennengelernt haben.

**Definition 10.1.1.1.** Ein Modul $A$ erfüllt die *aufsteigende Kettenbedingung ACC* (für „Ascending Chain Condition“) bezüglich Untermoduln (oder ist *Noethersch*), falls es zu jeder unendlich aufsteigenden Folge

$$A_0 \leq A_1 \leq A_2 \leq A_3 \leq \dots$$

von Untermoduln $A_n \leq A$ einen Index $n_0 \in \mathbb{N}$ gibt mit $A_{n_0} = A_n$ für alle $n \in \mathbb{N}$ mit $n \geq n_0$.
Ein Modul $A$ erfüllt die *absteigende Kettenbedingung DCC* (für „Descending Chain Condition“) bezüglich Untermoduln (oder ist *Artinsch*), falls es zu jeder unendlich absteigenden Folge

$$A_0 \geq A_1 \geq A_2 \geq A_3 \geq \dots$$

von Untermoduln $A_n \leq A$ einen Index $n_0 \in \mathbb{N}$ gibt mit $A_{n_0} = A_n$ für alle $n \in \mathbb{N}$ mit $n \geq n_0$.

Von folgender Charakterisierung werden wir wiederholt Gebrauch machen:

**Proposition 10.1.1.2.** *Für einen Modul $A$ sind folgende Bedingungen äquivalent:*

1. *$A$ ist Noethersch, d.h. definitionsgemäß: $A$ erfüllt die aufsteigende Kettenbedingung ACC für Untermodul.*
2. *$A$ erfüllt die Maximalbedingung für Untermoduln: Jede nichtleere Menge von Untermoduln von $A$ enthält ein bezüglich $\subseteq$ maximales Element.*
3. *Jeder Untermodul von $A$ ist endlich erzeugt.*

*Beweis.* Ergibt sich unmittelbar aus den Sätzen 2.1.2.12 und 2.3.1.24. □

Bei Moduln sind überdies folgende Aussagen über die Vererbung der Kettenbedingungen ACC und DCC nützlich:

**Proposition 10.1.1.3.** *Seien $A, B, C$ Moduln über einem Ring $R$. Dann gilt:*

1. *Sei $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ eine kurzexakte Sequenz von Moduln. Dann gilt ACC bzw. DCC in $B$ genau dann, wenn ACC bzw. DCC sowohl in $A$ als auch in $C$ gilt.*
2. *Sei $A$ Untermodul eines Moduls $B$. Dann gilt ACC bzw. DCC in $B$ genau dann, wenn ACC bzw. DCC sowohl in $B$ als auch in $A/B$ gilt.*
3. *Seien $A_1, \dots, A_n$ Moduln und $A = A_1 \oplus A_2 \oplus \dots \oplus A_n$. Dann gilt ACC bzw. DCC in $A$ genau dann, wenn ACC bzw. DCC in allen $A_i$, $i = 1, \dots, n$, gilt.*

*Beweis.* Die Beweise aller drei Aussagen verlaufen für aufsteigende und absteigende Kettenbedingung ACC und DCC völlig analog. Außerdem werden wir in diesem Kapitel nur die Versionen für ACC verwenden. Deshalb begnügen wir uns mit den Beweisen für ACC.

1. Wenn ACC für $B$ gilt, so folgt ACC für $A$ fast unmittelbar: Jede unendliche aufsteigende Kette von Untermoduln $A_n \leq A$ induziert eine unendliche Kette von Untermoduln $B_n := f(A_n)$ von $B$. Wäre sogar $A_n < A_{n+1}$ für alle $n$, so wegen der Injektivität von $f$ auch $B_n < B_{n+1}$, Widerspruch. Ein ähnliches Argument zeigt, dass auch $C$ Noethersch ist: Liegt eine unendliche Kette aus $C_n \leq C$ mit $C_n \leq C_{n+1}$ vor, so bilden die $B_n := g^{(-1)}(C_n)$ eine gleichfalls unendlich aufsteigende Kette von Untermoduln von $B$. Weil $g$ surjektiv ist, gilt $C_n = g(B_n)$ für alle $n$.

Nach Voraussetzung gibt es ein $n_0$ mit $B_n = B_{n_0}$, also $C_n = g(B_n) = g(B_{n_0}) = C_{n_0}$ für alle $n \geq n_0$. Damit ist die erste der beiden Implikationen gezeigt.

Für die umgekehrte Implikation setzen wir ACC für $A$ und $C$ voraus und gehen von einer unendlich aufsteigenden Kette von Untermoduln $B_n \leq B$, $n \in \mathbb{N}$, von $B$ aus. Eine solche induziert die gleichfalls aufsteigenden Ketten der Untermoduln $A_n := f^{(-1)}(f(A) \cap B_n)$ von $A$ und $C_n := g(B_n)$ von $C$. Laut Voraussetzung gibt es ein $n_0 \in \mathbb{N}$ mit $A_n = A_{n_0}$ und $C_n = C_{n_0}$ für alle $n \geq n_0$. Man überlegt sich unmittelbar, dass für jedes $n \in \mathbb{N}$ die Sequenz $0 \to A_n \xrightarrow{f_n} B_n \xrightarrow{g_n} C_n \to 0$ mit den Einschränkungen $f_n$ und $g_n$ auf $A_n$ bzw. $B_n$ exakt ist, außerdem für $n \geq n_0$ das Diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_{n_0} & \xrightarrow{f_{n_0}} & B_{n_0} & \xrightarrow{g_{n_0}} & C_{n_0} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_{A_{n_0}}} & & \downarrow{\scriptstyle \iota_{B_{n_0},B_n}} & & \downarrow{\scriptstyle \mathrm{id}_{C_{n_0}}} & & \\ 0 & \longrightarrow & A_{n_0} & \xrightarrow{f_n} & B_n & \xrightarrow{g_n} & C_{n_0} & \longrightarrow & 0 \end{array}$$

mit der Inklusionsabbildung $\iota_{B_{n_0},B_n} : B_{n_0} \to B_n$, $b \mapsto b$, kommutiert (Übung, siehe 10.1.1.4). Aus dem Kurzen Fünferlemma 7.2.3.7 folgt, dass mit $\mathrm{id}_{A_n}$ und $\mathrm{id}_{C_n}$ auch die Inklusionsabbildung $\beta$ surjektiv ist, also $B_n = B_{n_0}$.

2. Die erste Aussage angewandt auf die Sequenz $0 \to A \xrightarrow{\subseteq} B \to B/A \to 0$ liefert das Gewünschte.

3. Induktion nach $n$. Für $n = 2$ wendet man die erste Aussage auf die Sequenz $0 \to A_1 \xrightarrow{\iota_1} A_1 \oplus A_2 \xrightarrow{\pi_2} A_2 \to 0$ an. □

**UE 510** ▶ **Übungsaufgabe 10.1.1.4.** Überprüfen Sie die Exaktheit und Kommutativität der im Beweis der ersten Aussage von Proposition 10.1.1.3 auftretenden Sequenzen bzw. Diagramme. ◀ **UE 510**

So wie in Gruppen kann man auch in $R$-Moduln von Normalreihen und Subnormalreihen sprechen, wobei diese Begriffe offenbar zusammenfallen und schlicht endliche aufsteigende Ketten von Untermoduln bezeichnen. Ganz ähnlich den Sätzen von Jordan-Hölder und Schreier über Gruppen lässt sich dafür zeigen:

**Satz 10.1.1.5.** *Sei $R$ ein Ring und $A$ ein $R$-Modul. Dann gilt:*

1. *Je zwei Normalreihen von $A$ haben äquivalente Verfeinerungen.*
2. *Je zwei Kompositionsreihen von $A$ sind äquivalent.*
3. *$A$ hat genau dann eine Kompositionsreihe, wenn $A$ sowohl die aufsteigende als auch die absteigende Kettenbedingung bezüglich Untermoduln erfüllt.*

**UE 511** ▶ **Übungsaufgabe 10.1.1.6.** Beweisen Sie Satz 10.1.1.5. ◀ **UE 511**

### 10.1.2 Kettenbedingungen für Ringe

Betrachtet man einen Ring als Links- oder Rechts-Modul über sich selbst, so sind die Untermoduln gerade die Links- bzw. Rechtsideale, im kommutativen Fall die Ideale. Das legt die folgende Definition nahe.

**Definition 10.1.2.1.** Ein Ring $R$ heißt *links-* (bzw. *rechts-*) *Noethersch*, falls $R$ die aufsteigende Kettenbedingung ACC bezüglich Links- (bzw. Rechts-) Idealen erfüllt. $R$ heißt *Noethersch*, falls $R$ sowohl links- als auch rechts-Noethersch ist.
Ein Ring $R$ heißt *links-* (bzw. *rechts-*) *Artinsch*, falls $R$ die absteigende Kettenbedingung DCC bezüglich links- (bzw. rechts-) Idealen erfüllt. $R$ heißt *Artinsch*, falls $R$ sowohl links- als auch rechts-Artinsch ist.

Damit ergibt sich aus Proposition 10.1.1.2 unmittelbar:

**Folgerung 10.1.2.2.** *Ein kommutativer Ring $R$ mit 1 ist genau dann Noethersch, wenn jedes Ideal $I \lhd R$ endlich erzeugt ist. Insbesondere ist jeder Hauptidealring Noethersch.*

Wenig überraschend übertragen sich die Kettenbedingungen ACC und DCC von einem Ring $R$ auch auf endlich erzeugte $R$-Moduln:

**Satz 10.1.2.3.** *Ist $R$ ein links-Noetherscher bzw. links-Artinscher Ring und $A$ ein endlich erzeugter $R$-Linksmodul, so ist auch $A$ Noethersch bzw. Artinsch.*

*Beweis.* Sei $R$ Noethersch, der Beweis für Artinsch verläuft völlig analog. Werde $A$ von den Elementen $a_1, \ldots, a_n \in A$ erzeugt, und sei $F := \bigoplus_{i=1}^{n} Ra_i$ ein von $a_1, \ldots, a_n$ frei erzeugter $R$-Modul. Für jeden der Summanden gilt $Ra_i \cong R$ vermittels $ra_i \mapsto r$, also sind alle $Ra_i$ Noethersch bzw. Artinsch. In Proposition 10.1.1.3 garantiert die dritte Aussage, dass folglich auch $F$ ein Noetherscher $R$-Modul ist, die zweite, dass dies auch für das homomorphe Bild $A = f(F)$ unter dem (eindeutig bestimmten) Homomorphismus $f : F \to A$ mit $a_i \mapsto a_i$ für $i = 1, \ldots, n$ gilt. □

**UE 512** ► **Übungsaufgabe 10.1.2.4.** Sei $D$ ein Divisionsring und $R$ der Ring der $n \times n$-Matrizen über $D$. Untersuchen Sie $R$ in Hinblick auf die Eigenschaften (links-, rechts-) Noethersch und -Artinsch. ◄ **UE 512**

**UE 513** ► **Übungsaufgabe 10.1.2.5.** Finden Sie einen faktoriellen Ring an, der nicht Noethersch ist. ◄ **UE 513**

### 10.1.3 Der Basissatz

**Satz 10.1.3.1** (Hilbertscher Basissatz)**.** *Sei $R$ ein kommutativer Ring mit 1. Ist $R$ Noethersch, so ist auch $R[x_1, \ldots, x_n]$ Noethersch.*

*Beweisskizze.* Klarerweise reicht es, die Noethersche Eigenschaft für $n = 1$, d.h. für $R[x]$ zu beweisen, weil der Rest mittels Induktion nach $n$ folgt. Sei also $J \lhd R[x]$. Wegen Satz 10.1.2.3 genügt der Nachweis, dass $J$ endlich erzeugt ist. Sei

$$I_n := \{a_n \in R : \exists f \in R[x] : \ f(x) = a_n x^n + \ldots + a_1 x + a_0 \in J\}.$$

Offenbar ist $I_n \lhd R$ für alle $n$.
Wegen der Idealeigenschaft von $J$ liegt mit jedem $f \in J$ auch $xf$ in $J$, wobei der höchste Koeffizient $a_n \in I_n$ von $f$ zum höchsten Koeffizienten von $xf$ wird, also $a_n \in I_{n+1}$. Es liegt also eine aufsteigende Folge

$$I_1 \leq I_2 \leq I_3 \leq \ldots \lhd R$$

von Idealen in $R$ vor. Folglich gibt es ein $n_0 \in \mathbb{N}$ mit $I_{n_0} = I_{n_0+1} = I_{n_0+2} = \ldots$. Jedes Ideal im Noetherschen Ring $R$ ist endlich erzeugt, insbesondere die $I_n$, z.B. $I_n = \langle a_{n,i} : i = 1, \ldots, k_n \rangle$. Nach Wahl der $I_n$ existieren Polynome $f_{n,i} \in J$ mit $f_{n,i}(x) = a_{n,i}x^n + \ldots + a_0 \in J$. Man zeigt leicht (siehe Übungsaufgabe 10.1.3.2), dass dann

$$J = \langle f_{n,i} : n \leq n_0, i \leq k_n \rangle$$

gilt, womit ein endliches Erzeugendensystem von $J$ gefunden ist. □

**UE 514** ► **Übungsaufgabe 10.1.3.2.** Ergänzen Sie das im Beweis von Satz 10.1.3.1 nicht ausgeführte Argument, dass $J$ tatsächlich von den $f_{n,i}$, $n \leq n_0$, $i = 1, \ldots, k_n$, erzeugt wird. ◄ **UE 514**

Die Möglichkeit, ein beliebiges Polynomideal in mehreren Variablen durch endlich viele Erzeugende anzugeben, findet weitreichende praktische Anwendungen in der vom österreichischen Mathematiker Bruno Buchberger (geb. 1942) Mitte der 60er Jahre begründeten Theorie der *Gröbnerbasen*, die er nach seinem akademischen Lehrer Wolfgang Gröbner (1899-1980) benannte. Berühmt ist dabei der sogenannte *Buchberger-Agorithmus* zur Berechnung einer Gröbnerbasis eines gegebenen Ideals. Der Nutzen einer Gröbnerbasis zeigt sich im Kontext der allgemeinen Idealtheorie Noetherscher Ringe, siehe 10.1.5.

Der Hilbertsche Basissatz gilt analog auch für den Ring $R[[x]]$ der formalen Potenzreihen anstelle des Polynomrings:

**Satz 10.1.3.3.** *Ist $R$ ein kommutativer Noetherscher Ring, so auch der Ring $R[[x]]$ der formalen Potenzreihen über $R$.*

**UE 515** ► **Übungsaufgabe 10.1.3.4.** Beweisen Sie Satz 10.1.3.3. (Hinweis: Grundsätzlich führt eine ähnliche Vorgangsweise zum Ziel wie in Satz 10.1.3.1, Vorsicht ist aber geboten.) Gilt der entsprechende Satz auch für den Ring der formalen Laurentreihen über $R$? ◄ **UE 515**

### 10.1.4 Ein kurzer Einschub über Primideale

Folgender Satz erweist sich immer wieder als nützlich:

**Satz 10.1.4.1.** *Sei $R$ ein kommutativer Ring mit 1. $T \subseteq R$ multiplikativ abgeschlossen (d.h. $t_1, t_2 \in T \Rightarrow t_1 \cdot t_2 \in T$) und $I \lhd R$ mit $T \cap I = \varnothing$. Dann existiert ein maximales Ideal $P \lhd R$ mit den Eigenschaften $I \subseteq P$ und $T \cap P = \varnothing$. Jedes solche Ideal $P$ ist prim. Für $T = \varnothing$ bedeutet das, dass jedes Ideal in einem maximalen Ideal enthalten ist.*

*Beweis.* Eine Standardanwendung des Lemmas von Zorn liefert ein maximales Ideal $P$ mit den gewünschten Eigenschaften. Es bleibt zu beweisen, dass jedes derartige Ideal $P$ prim ist. Wir gehen dazu von Idealen $A, B \lhd R$ mit $AB \subseteq P$ aus und wollen zeigen, dass wenigstens eines der beiden in $P$ enthalten ist. Wir nehmen indirekt an, das wäre nicht der Fall. Dann wären $P + A$ und $P + B$ Ideale, die $P$ echt umfassen. Wegen der Maximalitätseigenschaft von $P$ folgt daraus $(P+A) \cap T \neq \emptyset \neq (P+B) \cap T$. Es gibt also Elemente $p_i \in P$, $a \in A$ und $b \in B$ mit $t_1 := p_1 + a \in T$ und $t_2 := p_2 + b \in T$. Weil $T$ multiplikativ ist, folgt einerseits $t_1 t_2 \in T$, andererseits

$$t_1 t_2 = p_1 p_2 + p_1 b + a p_2 + ab \in P + P + P + AB \subseteq P,$$

im Widerspruch zu $T \cap P = \emptyset$. □

Jedem Ideal $I$ in einem kommutativen Ring mit 1 wird das sogenannte Radikal $\mathrm{Rad}(I)$ zugeordnet. Die Definition lautet wie folgt.

**Definition 10.1.4.2.** Sei $R$ ein kommutativer Ring mit 1. Für $I \lhd R$ heißt

$$\mathrm{Rad}(I) := \bigcap \{P : I \subseteq P, P \lhd R \text{ prim}\}$$

das *Radikal* von $I$.

Wichtig ist die folgende alternative Beschreibung, die zeigt, dass es sich beim Radikal $\mathrm{Rad}(I)$ gewissermaßen um den Abschluss von $I$ bezüglich des Wurzelziehens handelt.

**Proposition 10.1.4.3.** *Sei $R$ ein kommutativer Ring mit 1 und $I \lhd R$. Dann gilt*

$$\mathrm{Rad}(I) = \{r \in R \mid \exists n \geq 1 : \ r^n \in I\}.$$

*Beweis.* Wir kürzen $M := \{r \in R \mid \exists n \geq 1 : \ r^n \in I\}$ ab und haben die beiden Inklusionen $M \subseteq \mathrm{Rad}(I)$ und $\mathrm{Rad}(I) \subseteq M$ zu zeigen.
$M \subseteq \mathrm{Rad}\, I$: Sei $r \in M$, dann ist $r^n \in I$ für ein $n \geq 1$. Für alle Primideale $P \lhd R$ mit $I \subseteq P$ folgt $r^n \in P$, also auch $r \in P$ und damit $r \in \mathrm{Rad}(I)$. Also ist $M \subseteq \mathrm{Rad}(I)$.
$\mathrm{Rad}(I) \subseteq M$: Sei $s \notin M$. Die Menge $S := \{s^n + r : n \in \mathbb{N} \setminus \{0\}, r \in I\}$ ist multiplikativ abgeschlossen, $S \cap I = \varnothing$ und $s \in S$. Nach Satz 10.1.4.1 existiert ein primes $P \lhd R$ mit $P \cap S = \varnothing$ und $I \subseteq P$. Also ist $s \notin P$ und damit auch $s \notin \mathrm{Rad}\, I$. □

### 10.1.5 Idealtheorie in Noetherschen Ringen

Die Idealtheorie für Noethersche Ringe (insbesondere also für Polynomringe in den Variablen $x_1, \ldots, x_n$ über einem Körper) ermöglicht die Darstellung eines beliebigen Ideals $I \lhd R$ in einem Noetherschen Ring als mengentheoretischer Schnitt von Primäridealen. Für derartige sogenannte *Primärzerlegungen* gelten auch gewisse Eindeutigkeitsaussagen. Noch etwas allgemeiner sind die entsprechenden Resultate für Moduln. Weitgehend ohne Beweise seien hier lediglich die Hauptergebnisse samt den für deren Würdigung notwendigen Begriffsbildungen und Hilfsresultaten wiedergegeben. Zunächst definieren wir Primärideale und primäre Moduln:

**Definition 10.1.5.1.** Sei $R$ ein kommutativer Ring mit 1. Ein Ideal $Q \lhd R$ mit $Q \neq R$ heißt *Primärideal* von $R$, wenn für alle $a, b \in R$ mit $ab \in Q$ und $a \notin Q$ folgt, dass $b^n \in Q$ für ein geeignetes positives $n \in \mathbb{N}$ gilt.
Sei nun $A$ ein $R$-Modul. Ein Untermodul $U \leq A$ heißt *primär*, wenn aus $r \in R$, $a \in A \setminus U$ und $ra \in U$ stets $r^n A \subseteq U$ für ein geeignetes positives $n \in \mathbb{N}$ folgt.

Ein wichtiger Zusammenhang zwischen Primär- und Primidealen ist der folgende:

**Proposition 10.1.5.2.** *Ist $R$ ein kommutativer Ring mit 1 und $Q \lhd R$ ein Primärideal in $R$, so ist $\mathrm{Rad}(Q) \lhd R$ ein Primideal.*

**UE 516** ► **Übungsaufgabe 10.1.5.3.** Beweisen Sie Proposition 10.1.5.2. ◄ **UE 516**

Man zeigt sehr leicht:

**Proposition 10.1.5.4.** *Ist $R$ ein kommutativer Ring mit 1 und $U \leq A$ ein primärer Untermodul eines $R$-Moduls $A$, dann ist $Q_U := \{r \in R : \ rA \subseteq U\}$ ein primäres Ideal.*

**UE 517** ► **Übungsaufgabe 10.1.5.5.** Beweisen Sie Proposition 10.1.5.4. ◄ **UE 517**

**Definition 10.1.5.6.** In der Konstellation aus Proposition 10.1.5.4 sei $P := \mathrm{Rad}\, Q_U$. Dann sagt man, *$U$ gehöre* zum Primideal $P$, und $U$ heißt dann *$P$-primärer Untermodul* oder auch nur *primärer Untermodul* von $A$.

Ziel ist es, beliebige Ideale als Schnitte von endlich vielen Primäridealen darzustellen und möglichst auch Eindeutigkeitsaussagen herzuleiten. Wenn man will, kann man darin eine Verallgemeinerung der eindeutigen Primfaktorzerlegung in Hauptidealringen sehen.
Für Noethersche Ringe erweist sich die folgende Definition als zweckmäßig:

**Definition 10.1.5.7.** Sei $R$ ein kommutativer Ring mit 1, $A$ ein $R$-Modul und $U \leq A$. Gilt $U = Q_1 \cap \ldots \cap Q_n$ mit primären Untermoduln $Q_i \leq A$, so nennt man diese Darstellung von $U$ als Schnitt eine *Primärzerlegung* von $U$. Wenn keines der $Q_i$ im Schnitt der übrigen enthalten ist (wenn also keines der $Q_i$ aus der Darstellung von $A$ als Schnitt gestrichen werden kann) und alle zugehörigen Primideale $P_i := \mathrm{Rad}\, Q_i$ paarweise verschieden sind, so heißt die Darstellung *reduziert*. Ein Primideal $P_i$ heißt in Bezug auf die Primärzerlegung *isoliert*, wenn es keines der übrigen $P_j$ enthält, andernfalls *eingebettet*.

Nicht sehr schwierig ist der Nachweis, dass Primärzerlegungen stets in reduzierte übergeführt werden können:

**Proposition 10.1.5.8.** *Sei $R$ ein kommutativer Ring mit 1, $A$ ein $R$-Modul. Hat der Untermodul $U \leq A$ eine Primärzerlegung, so auch eine reduzierte.*

**UE 518** ▶ **Übungsaufgabe 10.1.5.9.** Beweisen Sie Proposition 10.1.5.8. Hinweis: Zeigen Sie zunächst, dass der Schnitt von $P$-primären Untermoduln wieder $P$-primär zum selben Primideal ist. ◀ **UE 518**

Das angestrebte Hauptergebnis lautet nun:

**Satz 10.1.5.10.** *Für reduzierte Primärzerlegungen von Moduln und von Idealen gelten folgende Existenz- bzw. Eindeutigkeitsaussagen. Dabei sei $R$ ein kommutativer Ring mit 1, $A$ ein $R$-Modul und $U \leq A$ ein Untermodul.*

1. *Ist $A$ Noethersch, dann hat $U$ eine reduzierte Primärzerlegung. Insbesondere haben jeder Untermodul eines endlich erzeugten Moduls über einem Noetherschen Ring sowie jedes Ideal in einem Noetherschen Ring eine reduzierte Primärzerlegung.*

2. *Seien*
$$Q_1 \cap \ldots \cap Q_n = U = Q'_1 \cap \ldots \cap Q'_{n'}$$
*zwei reduzierte Primärzerlegungen von $U$ und $P_i$ sowie $P'_j$ Primideale von $R$ derart, dass die $Q_i$ alle $P_i$-primär und die $Q'_j$ alle $P'_j$-primär sind. Dann gilt $n = n'$ und, nach geeigneter Permutation der Indizes, $P_i = P'_i$ für $i = 1, \ldots, n$. Ist $P_i$ in Bezug auf die Primärzerlegung isoliert, so gilt sogar $Q_i = Q'_i$.*

**UE 519** ▶ **Übungsaufgabe 10.1.5.11.** Beweisen Sie Satz 10.1.5.10. (Achtung, nichttrivial!) ◀ **UE 519**

**UE 520** ▶ **Übungsaufgabe 10.1.5.12.** Finden Sie ein Beispiel einer Primärzerlegung, die nicht eindeutig ist. ◀ **UE 520**

## 10.2 Ganzheit in kommutativen Ringen

In diesem Abschnitt werden alle Ringe als kommutativ mit 1 vorausgesetzt.

In der Theorie der Ringerweiterungen spielt der Begriff der Ganzheit eine ähnliche Rolle wie jener der Algebraizität bei Körpererweiterungen. Im Fall von Körpern fallen die beiden Begriffe zusammen. Die Grundbegriffe werden in 10.2.1 bereitgestellt. Der ganze Abschluss eines Ringes $R$ ist Gegenstand von 10.2.2. Im Gegensatz zum algebraischen Abschluss eines Körpers wird der ganze Abschluss eines Ringes $R$ zunächst innerhalb

einer gegebenen Ringerweiterung $R \leq S$ definiert. Dedekindsche Ringe sind spezielle Noethersche Ringe, die besonders in der algebraischen Zahlentheorie eine wichtige Rolle spielen und auf sehr vielfältige Weise charakterisiert werden können, u.a. durch Ganzheitseigenschaften (siehe 10.2.3). Ebenfalls in den Kontext ganzer Ringerweiterungen fügt sich das Beispiel aus 10.2.4 eines Hauptidealringes, der nicht euklidisch ist. Damit wird ein bis dato offenes Desideratum aus 5.2.3 eingelöst.

### 10.2.1 Ganze Elemente und Ringerweiterungen

**Definition 10.2.1.1.** Ist $R$ ein kommutativer Ring mit 1 und $R \leq S$, so heißt $S$ eine *Ringerweiterung* von $R$. Für $X \subseteq S$ sei

$$R[X] := \{f(s_1, \ldots, s_n) : s_i \in X, f \in R[x_1, \ldots, x_n], n \in \mathbb{N}\}$$

der von $R \cup X$ erzeugte Unterring von $S$. Ein Element $s \in S$ heißt *ganz über* $R$, falls es ein monisches (d.h. normiertes, der führende Koeffizient ist 1) Polynom $f \in R[x]$ gibt mit $f(s) = 0$. $S$ heißt *ganz über* $R$, falls alle Elemente von $S$ ganz über $R$ sind.

Sind $R$ und $S$ Körper, so stimmt „ganz“ offenbar mit „algebraisch“ überein.

**Satz 10.2.1.2.** *Sei $R \leq S$ eine Ringerweiterung.*

*(a) Für $s \in S$ sind folgende Aussagen äquivalent.*

*(i) $s$ ist ganz über $R$.*

*(ii) $R[s]$ ist ein endlich erzeugter $R$-Modul.*

*(iii) Es existiert ein $T \leq S$, so dass $1 \in T$, $R[s] \subseteq T$ und $T$ ein endlich erzeugter $R$-Modul ist.*

*(b) Ist $S$ ein endlich erzeugter $R$-Modul, so ist $S$ ganz über $R$.*

*(c) Ist $S$ ein endlich erzeugter $R$-Modul und $T$ ein endlich erzeugter $S$-Modul, so ist $T$ auch als $R$-Modul endlich erzeugt.*

*(d) Sind $s_1, \ldots, s_n \in S$ ganz über $R$, so ist $R[s_1, \ldots, s_n]$ ein endlich erzeugter $R$-Modul und damit ganz über $R$.*

*(e) In den Ringerweiterungen $R \leq S \leq T$ sei $S$ ganz über $R$ und $T$ ganz über $S$. Dann ist $T$ ganz über $R$.*

*Beweis.* Wir zeigen nur die drei zyklischen Implikationen für (a). Der Rest folgt ähnlich wie die entsprechenden Aussagen über algebraische Körpererweiterungen in 6.1.4 und ist Inhalt einer Übungsaufgabe.
(i) $\Rightarrow$ (ii): Nach Voraussetzung gibt es ein normiertes Polynom $f(x) = x^n + r_{n-1}x^{n-1} + \ldots + r_1 x + r_0$ mit $r_i \in R$ und $f(s) = 0$. Wir behaupten, dass der von den Potenzen $s^0 = 1, s^1 = s, s^2, \ldots, s^{n-1}$ erzeugte $R$-Modul $A := \langle s^0 = 1, s, \ldots, s^{n-1}\rangle \subseteq R[s]$ bereits ganz $R[s]$ ist. Aus der Nullstellengleichung für $s$ lesen wir $s^n = -r_{n-1}s^{n-1} - \ldots - r_1 s^1 -$

$r_0 s^0 \in A$ ab. Der Induktionsschritt „$s^{m-1} \in A$ impliziert $s^m \in A$“ ergibt sich für $m \geq n$ aus der Rechnung

$$s^m = ss^{m-1} = s(r'_{n-1}s^{n-1} + \ldots + r'_1 s^1 + r'_0 s^0) = r'_{n-1}s^n + \ldots + r'_1 s^1 + r'_0 s^0 \in A + A = A.$$

Somit ist insgesamt $R[s] = \{g(s) : \ g \in R[x]\} \subseteq A$, also $R[s] = A$, wie behauptet.
(ii) $\Rightarrow$ (iii): Offenbar hat $T := R[s]$ die behauptete Eigenschaft.
(iii) $\Rightarrow$ (i): Werde $T$ von den Elementen $b_1, \ldots, b_n$ als $R$-Modul erzeugt. Dann gibt es Elemente $r_{i,j} \in R$ mit

$$sb_i = \sum_{j=1}^{n} r_{i,j} b_j \quad \text{für } i = 1, \ldots, n.$$

Wir setzen $r'_{i,j} := -r_{i,j}$ für $i \neq j$ und $r'_{i,i} := s - r_{i,i}$. Folglich gilt

$$\sum_{j=1}^{n} r'_{i,j} b_j = 0 \quad \text{für } i = 1, \ldots, n.$$

Daraus folgt $b_i \det(A') = 0$ für alle $i = 1, \ldots, n$ und die Matrix $A' := (r'_{i,j})_{1 \leq i,j \leq n}$ (Übungsaufgabe 10.2.1.3). Weil die $b_i$ ganz $T$ erzeugen, heißt das $t \det(A') = 0$ für alle $t \in T$. Setzen wir speziell $t = 1$, so folgt $\det(A') = 0$. Wir betrachten nun für die Matrix $A := (r_{i,j})_{1 \leq i,j \leq n}$ das monische Polynom $f(x) := \det(xI_n - A) \in R[x]$ (mit der $n$-dimensionalen Einheitsmatrix $I_n$). Wegen $f(s) = \det(sI_n - A) = \det A' = 0$ ist $s$ Nullstelle von $f$ und somit ganz über $R$. □

**UE 521** ▶ **Übungsaufgabe 10.2.1.3.** Zeigen Sie die im Beweis von Satz 10.2.1.2 (a), Implikation (iii) $\Rightarrow$ (i), verwendete Beziehung $b_i \det(A') = 0$ für $i = 1, \ldots, n$ unter den dort vorliegenden Bedingungen. ◀ **UE 521**

**UE 522** ▶ **Übungsaufgabe 10.2.1.4.** Beweisen Sie die noch offenen Behauptungen (b) bis (e) aus Satz 10.2.1.2. Hinweis: Ist (a) einmal bewiesen, folgen die verbleibenden Aussagen sehr ähnlich wie die entsprechenden Zusammenhänge zwischen „algebraisch“ und „endlichdimensional“ bei Körpererweiterungen. ◀ **UE 522**

### 10.2.2 Ganzer Abschluss

**Definition 10.2.2.1.** Sei $R \leq S$ eine Ringerweiterung. Der *ganze Abschluss von $R$ in $S$* ist definiert als

$$\widehat{R} := \{s \in S : s \text{ ganz über } R\} \geq R.$$

Ist $\widehat{R} = R$, so heißt $R$ *ganz abgeschlossen in $S$*. Ist $R$ ein Integritätsbereich, $S$ der Quotientenkörper von $R$ und $\widehat{R} = R$, so heißt $R$ (schlechthin) *ganz abgeschlossen*.

**Proposition 10.2.2.2.** *Für eine Ringerweiterung $R \leq S$ gilt:*

*(a) Der ganze Abschluss $\widehat{R}$ von $R$ ist ein Unterring von $S$.*

*(b) $\widehat{R}$ ist ganz über $R$.*

*(c) Die Bildung des ganzen Abschlusses ist idempotent, d.h.: $\widehat{\widehat{R}} = \widehat{R}$*

*(d) Der Ring der ganzen Zahlen $\mathbb{Z}$ ist ganz abgeschlossen (im Quotientenkörper $\mathbb{Q}$), aber nicht ganz abgeschlossen in $\mathbb{C}$.*

*(e) Ist $R$ ein faktorieller Ring, so ist $R$ ganz abgeschlossen. Insbesondere ist $K[x_1, \ldots, x_n]$ für jeden Körper $K$ und alle $n \in \mathbb{N}$ ganz abgeschlossen.*

**UE 523** ▶ **Übungsaufgabe 10.2.2.3.** Beweisen Sie Proposition 10.2.2.2. ◀ **UE 523**

### 10.2.3 Dedekindsche Ringe

Dedekindsche Ringe sind spezielle Integritätsbereiche und treten vor allem in der algebraischen Zahlentheorie auf. Sie bilden eine Teilklasse der Noetherschen Ringe und umfassen die Hauptidealringe. Dedekindsche Ringe lassen sich auf vielfältige Weise charakterisieren. Ohne Beweis werden wir einige Möglichkeiten angeben.
In der Idealtheorie Dedekindscher Ringe kann der mengentheoretische Schnitt durch das Produkt ersetzt werden. Es geht also um die Darstellung beliebiger Ideale als Produkt von Primär- und, sogar noch stärker, von Primidealen. Die Definition lautet:

**Definition 10.2.3.1.** Ein Integritätsbereich $R$ heißt *Dedekindscher Ring*, wenn jedes Ideal $I \lhd R$ mit $I \neq R$ das Produkt endlich vieler Primideale ist. Dabei ist das Produkt zweier Ideale $I, J \lhd R$ definiert als das von allen Produkten $ab$ mit mit $a \in I$ und $b \in J$ erzeugte Ideal, also die Menge aller endlichen Summen $\sum_{k=1}^{n} a_k b_k$ mit $n \in \mathbb{N}$, $a_k \in I$ und $b_k \in J$.

**UE 524** ▶ **Übungsaufgabe 10.2.3.2.** Zeigen Sie: Jeder Hauptidealring, aber nicht jeder faktorielle Ring ist Dedekindsch. ◀ **UE 524**

Für den Charakterisierungssatz 10.2.3.4 brauchen wir einige Begriffe.

**Definition 10.2.3.3.** Sei $R$ ein Integritätsbereich und $K$ sein Quotientenkörper. Ein $R$-Modul $I \subseteq K$ heißt ein *gebrochenes Ideal* von $R$, wenn es ein $r \in R$ mit $rI \subseteq R$ gibt. Unter dem *Produkt* $IJ$ zweier gebrochener Ideale versteht man den von den Produkten $ab$ mit $a \in I$ und $b \in J$ erzeugten $R$-Modul, also die Menge aller endlichen Summen $\sum_{k=1}^{n} a_k b_k$ mit $n \in \mathbb{N}$, $a_k \in I$ und $b_k \in J$. (Im Fall von Idealen $I, J \lhd$ stimmt diese Definition also mit jener aus 10.2.3.1 überein.)
Ein gebrochenes Ideal $I$ heißt *invertierbar*, wenn es ein gebrochenes Ideal $J$ mit $IJ = R$ gibt.

Es ist offensichtlich, dass die gebrochenen Ideale von $R$ ein kommutatives Monoid mit Einselement $R$ bilden, das sämtliche Ideale von $R$ enthält.
In der letzten der Charakterisierungen Dedekindscher Ringe, die wir bringen wollen, verwenden wir auch noch den Begriff der *Lokalisierung* $R_P$ eines Ringes $R$ bei einem Primideal $P$. Darunter versteht man den Quotientenring (Bruchring, siehe Definition 3.4.5.1) von $R$ bezüglich $S := R \setminus P$.
Damit können wir den angekündigten Charakterisierungssatz für Dedekindsche Ringe formulieren:

**Satz 10.2.3.4.** *Für einen Integritätsbereich $R$ sind die folgenden Bedingungen äquivalent:*

1. *$R$ ist ein Dedekindscher Ring, d.h. (definitionsgemäß) jedes Ideal $I \lhd R$, $I \neq R$, ist das Produkt endlich vieler Primideale.*
2. *Jedes Ideal $I \lhd R$, $I \neq R$, ist in eindeutiger Weise (bis auf die Reihenfolge der Faktoren) das Produkt endlich vieler Primideale.*
3. *Jedes Ideal $I \lhd R$ mit $I \neq \{0\}$ ist invertierbar.*
4. *Jedes gebrochene Ideal $I \lhd R$, $I \neq \{0\}$, ist invertierbar.*
5. *Die gebrochenen Ideale von $R$ bilden bezüglich der Multiplikation eine Gruppe.*
6. *Jedes Ideal ist als $R$-Modul projektiv.*
7. *Jedes gebrochene Ideal von $R$ ist als $R$-Modul projektiv.*
8. *$R$ ist Noethersch, ganz abgeschlossen und jedes Primideal $P \neq \{0\}$ ist maximal.*
9. *$R$ ist Noethersch und für jedes Primideal $P \neq \{0\}$ ist die Lokalisierung $R_P$ von $R$ bei $P$ ein Hauptidealring mit einem eindeutigen Primideal $P \neq \{0\}$.*

**UE 525** ► **Übungsaufgabe 10.2.3.5.** Beweisen Sie möglichst viele Implikationen zwischen den neun äquivalenten Bedingungen in Satz 10.2.3.4. ◄ **UE 525**

### 10.2.4 Ein Hauptidealring, der nicht euklidisch ist

In der algebraischen Zahlentheorie sind Zahlenringe der Form $\mathbb{Z}[\alpha] = \{f(\alpha) : \ f \in \mathbb{Z}[x]\}$, mit gewissen algebraischen Zahlen $\alpha \in \mathbb{C} \setminus \mathbb{Q}$ von besonderem Interesse. Wir haben schon gesehen, dass man für $\alpha = i$ einen euklidischen Ring erhält (den Ring der Gauß'schen Zahlen), für $\alpha = \sqrt{-5}$ hingegen einen Integritätsbereich, der nicht einmal faktoriell ist. Die Vielfalt der Möglichkeiten soll hier am Beispiel $\alpha := \frac{1+i\sqrt{19}}{2}$ weiter illustriert werden.

**Satz 10.2.4.1.** *Der Ring $\mathbb{Z}[\alpha]$ ist für $\alpha := \frac{1+i\sqrt{19}}{2}$ ein Hauptidealring aber nicht euklidisch.*

Einer Anleitung von H. W. Lenstra, Jr. und G. Bergman folgend soll ein Beweis dieser Behauptung im Wesentlichen im Rahmen von zwei Übungsaufgaben mit Anleitung skizziert werden.

**UE 526** ► **Übungsaufgabe 10.2.4.2.** Zeigen Sie, dass der Ring $\mathbb{Z}[\alpha]$ für $\alpha = \frac{1+i\sqrt{19}}{2}$ kein euklidischer Ring ist. Anleitung: Gehen Sie schrittweise vor, indem Sie die folgenden Behauptungen beweisen: ◄ **UE 526**

1. Die Zahl $\alpha$ ist Nullstelle des Polynoms $f(x) = x^2 - x + 5$.
2. $\mathbb{Z}[\alpha] = \{a + b\alpha : \ a, b \in \mathbb{Z}\} = \{a + b\overline{\alpha} : \ a, b \in \mathbb{Z}\}$.
3. Die Normfunktion $N : x \mapsto |x|^2 = x\overline{x}$ ist ein Homomorphismus bezüglich der Multiplikation, der auf $R$ nur nichtnegative ganzzahlige Werte annimmt.
4. Alle Einheiten $e$ von $\mathbb{Z}[\alpha]$ erfüllen $|e|^2 = 1$.
5. 1 und $-1$ sind die einzigen Einheiten in $\mathbb{Z}[\alpha]$. Anleitung: Man leite eine untere Abschätzung für den Betrag des Imaginärteils nicht reeller Elemente ab.
6. Die Annahme, $\mathbb{Z}[\alpha]$ sei euklidisch, führt zu einem Widerspruch. Anleitung: Gehen Sie indirekt von einer euklidischen Bewertung $H$ und einem $x \neq 0$, das keine Einheit ist, mit minimalem $H(x)$ aus. Zeigen Sie, dass 0 und die Einheiten alle Nebenklassen des von $x$ erzeugten Hauptideals repräsentieren. Also enthält dieser Faktorring höchstens 3 Elemente. Prüfen Sie nach, dass in keinem nichttrivialen solchen Ring das Polynom $f$ eine Nullstelle hat. Leiten Sie daraus den gesuchten Widerspruch ab.

$\mathbb{Z}[\alpha]$ ist für $\alpha := \frac{1+i\sqrt{19}}{2}$ also nicht euklidisch. Um zu zeigen, dass $\mathbb{Z}[\alpha]$ aber sehr wohl ein Hauptidealring ist, sei ein beliebiges Ideal $I \lhd \mathbb{Z}[\alpha]$ vorgegeben, von dem nachzuweisen ist, dass es ein Hauptideal ist. Wir dürfen annehmen, dass $I$ nicht das Nullideal ist und somit ein Element $x$ mit minimalem positiven Betrag enthält. Der Absolutbetrag ist, wie aus Übungsaufgabe 10.2.4.2 hervorgeht, keine euklidische Bewertung, wird aber ähnliche Dienste leisten, um $I = x\mathbb{Z}[\alpha]$, also die Hauptidealeigenschaft zu zeigen. Das würde den Beweis von Satz 10.2.4.1 vervollständigen. Nützlich wird dabei die Menge $J := x^{-1}I = \{x^{-1}r : \ r \in I\} \subseteq \mathbb{C}$ sein. Können wir $J = \mathbb{Z}[\alpha]$ zeigen, folgt $I = x\mathbb{Z}[\alpha]$. Dies wird gelingen, indem aus der Annahme $y_0 \in J \setminus \mathbb{Z}[\alpha]$ ein Widerspruch abgeleitet wird.

**UE 527** ► **Übungsaufgabe 10.2.4.3.** Vervollständigen Sie den Beweis, dass der Ring $\mathbb{Z}[\alpha]$ für $\alpha = \frac{1+i\sqrt{19}}{2}$ ein Hauptidealring ist. Anleitung: Gehen Sie in folgenden Schritten vor, wobei die oben eingeführten Notationen weiter verwendet werden: ◄ **UE 527**

1. $J$ ist ein $\mathbb{Z}[\alpha]$-Untermodul von $\mathbb{C}$, der $\mathbb{Z}[\alpha]$ enthält und in dem es außer 0 kein Element mit Absolutbetrag $< 1$ gibt.

2. Zeigen Sie: Aus $y \in J$ und $|y - r| < 1$ für ein $r \in \mathbb{Z}[\alpha]$ folgt $y \in \mathbb{Z}[\alpha]$.

3. Lassen Sie sich durch eine Skizze, die die geometrischen Verhältnisse in der komplexen Ebene wiedergibt, zu einem Beweis folgender Tatsache inspirieren: Ist $y \in J \setminus \mathbb{Z}[\alpha]$, $a$ der Imaginärteil von $y$ und $k \in \mathbb{Z}$, so folgt $|a - k\frac{\sqrt{19}}{2}| \geq \frac{\sqrt{3}}{2}$.

4. Wäre $J \setminus \mathbb{Z}[\alpha]$ nicht leer, so gäbe es darin ein Element $y_0$ mit Realteil im Intervall $(-\frac{1}{2}, \frac{1}{2}]$ und Imaginärteil im Intervall $[\frac{\sqrt{3}}{2}, \frac{\sqrt{19}}{2} - \frac{\sqrt{3}}{2}]$.

5. Für so ein $y_0$ läge der Imaginärteil von $2y_0$ zu nahe bei $\frac{\sqrt{19}}{2}$, als dass $y_0$ zu $J \setminus \mathbb{Z}[\alpha]$ gehören kann.

6. Zeigen Sie, dass nur mehr die Möglichkeiten $y_0 = \frac{\alpha}{2}$ und $y_0 = -\frac{\overline{\alpha}}{2}$ verbleiben.

7. Schließen Sie daraus, dass $\frac{\alpha\overline{\alpha}}{2} \in J$, berechnen Sie diese Zahl und leiten Sie daraus einen Widerspruch ab.

8. Wir wissen nun, dass $J \setminus \mathbb{Z}[\alpha]$ leer ist, mit anderen Worten $\mathbb{Z}[\alpha] = J$. Schließen Sie daraus $I = x\mathbb{Z}[\alpha]$.

Um besser zu verstehen, worauf es bei der Wahl von $\alpha$ ankommt, kann man sich auch noch die folgende Aufgabe vornehmen.

**UE 528** ▶ **Übungsaufgabe 10.2.4.4.** Untersuchen Sie, was schief geht, wenn man in den Übungsaufgaben 10.2.4.2 und 10.2.4.3 die Zahl 19 durch 17 oder durch 23 ersetzt. ◀ **UE 528**

## 10.3 Der Hilbertsche Nullstellensatz

Der Hilbertsche Nullstellensatz (HNS) befasst sich mit der Lösungsmenge von Systemen von algebraischen (d.h. von Polynom-) Gleichungen in endlich vielen Variablen $x_1, \ldots, x_n$ über einem Körper $K$. In seiner einfacheren Form (kleiner HNS) besagt der HNS grob gesprochen: Ist ein algebraisches Gleichungssystem in endlich vielen Variablen über einem Körper $K$ nicht widersprüchlich (d.h. kann daraus nicht durch die Bildung von Linearkombinationen die Gleichung $0 = 1$ abgeleitet werden), so gibt es auch Lösungen, die algebraisch über $K$ sind, also im algebraischen Abschluss von $K$ liegen. Die Vollversion des HNS nimmt zu einer gegebenen Menge $M \subseteq K[x_1, \ldots, x_n]$ von Polynomen mit gemeinsamer Lösungsmenge $L$ die (jedenfalls $M$ umfassende) Menge $I$ *aller* $f \in K[x_1, \ldots, x_n]$ in den Blick, die von ganz $L$ gelöst werden. Es ist fast trivial, dass $I$ ein Ideal ist. Der volle HNS besagt nun, dass unter sämtlichen Idealen $I \lhd K[x_1, \ldots, x_n]$ genau jene tatsächlich in der beschriebenen Weise auftreten, die $\mathrm{Rad}(I) = I$ erfüllen. Dabei besteht das sogenannte $\mathrm{Rad}(I)$ eines beliebigen Ideals $I$ definitionsgemäß aus jenen $f$, für die es ein positives $n \in \mathbb{N}$ mit $f^n \in I$ gibt. Man könnte also sagen: Radikale in diesem Sinn sind abgeschlossen unter der Bildung von Wurzeln.
Der Beweis des vollen HNS ist das Ziel in diesem Abschnitt. Erreichen werden wir es in 10.3.5. Der Beweis baut auf dem kleinen HNS aus 10.3.4 auf und greift außerdem auf die

eher technischen Ergebniss aus 10.3.2 zurück. Für den Beweis des kleinen HNS wiederum ist das sogenannte Noethersche Normalisierungslemma aus 10.3.3 das entscheidende Hilfsmittel. Eingeleitet wird der Abschnitt in 10.3.1 mit einführenden Bemerkungen zur algebraischen Geometrie, einem wichtigen Teilgebiet der Mathematik, als dessen Ausgangspunkt der HNS gelten kann. Den Anfang macht die Galoiskorrespondenz zwischen $K^n$ und $K[x_1, \ldots, x_n]$, die für $(a_1, \ldots, a_n) \in K^n$ und $f \in K[x_1, \ldots, x_n]$ durch die Relation $f(a_1, \ldots, a_n) = 0$ induziert wird.

### 10.3.1 Die Ausgangssituation in der algebraischen Geometrie

In der algebraischen Geometrie untersucht man Lösungsmengen algebraischer Gleichungssysteme in mehreren Variablen. Gegenstand ist daher die Relation $\perp$, definiert durch

$$f \perp (a_1, \ldots, a_n) \Leftrightarrow f(a_1, \ldots, a_n) = 0,$$

wobei $K$ ein Körper, $a_1, \ldots, a_n \in K$ und $f \in K[x_1, \ldots, x_n]$ sind. Die Relation $\perp$ induziert eine Galoisverbindung zwischen $K^n$ und $K[x_1, \ldots, x_n]$. Die Galois-abgeschlossenen Mengen in $K^n$ heißen *Varietäten* (= Lösungsmengen algebraischer Gleichungssysteme), jene in $K[x_1, \ldots, x_n]$ sind offensichtlich Ideale.
Für Polynome in einer einzigen Variablen über einem algebraisch abgeschlossenen Körper $K$ ist eine Gleichung $f(x) = 0$ genau dann lösbar, wenn $f$ kein konstantes Polynom $\neq 0$ ist, die Gleichung also nicht schon auf offensichtliche Weise widersprüchlich ist. Ähnliches wird sich auch für Gleichungssysteme in mehreren Variablen herausstellen. Dabei betrachten wir ein System

$$(*) \left\{ \begin{array}{rcl} f_1(x_1, \ldots, x_n) & = & 0 \\ & \vdots & \\ f_k(x_1, \ldots, x_n) & = & 0 \end{array} \right.$$

als offensichtlich widersprüchlich, falls eine geeignete Linearkombination der $f_j$ ein konstantes Polynom $c \neq 0$ darstellt:

$$\sum_{j=1}^{k} \lambda_j f_j \equiv c \neq 0$$

Das ist äquivalent dazu, dass das von den $f_j$ erzeugte Ideal ganz $K[x_1, \ldots, x_n]$ ist. Der Hilbertsche Nullstellensatz in seiner schwachen Form (kleiner Nullstellensatz 10.3.4.1) besagt, dass im Falle eines algebraisch abgeschlossenen Körpers diese offensichtliche Art von Widerspruch die einzige Möglichkeit ist, Lösungen des Gleichungssystems zu verhindern. Anders formuliert: Ein Ideal, das außer 0 keine Konstanten enthält, das also nicht bereits der ganze Polynomring $K[x_1, \ldots, x_n]$ ist, hat im algebraischen Abschluss gemeinsame Nullstellen. (Man beachte die Analogie zum Fall eines einzigen Polynoms in nur einer Variablen.) Oder, in der Sprache der Galoiskorrespondenzen: Ist $I \lhd K[x_1, \ldots, x_n]$ nicht der gesamte Polynomring, dann auch sein Galois-Abschluss. Der volle Nullstellensatz 10.3.5.1 verschärft diese Aussage, indem er den Galois-Abschluss von $I$ sehr explizit beschreibt als Radikal $\mathrm{Rad}(I)$ von $I$.

Zur Rechtfertigung des Schlagwortes *algebraische Geometrie* ist noch eine kurze Bemerkung angebracht. Zunächst induzieren Polynome $f \in K[x_1, \ldots, x_n]$ Polynomfunktionen, also $K$-wertige Funktionen auf $K^n$. Sei nun $V$ eine Varietät, d.h. die Nullstellenmenge eines Ideals $I$. Interessiert man sich für die Einschränkung von Polynomfunktionen auf $V$, so sind $f, g \in K[x_1, \ldots, x_n]$ genau dann zu identifizieren, wenn die zugehörigen Polynomfunktionen $f, g$ auf $V$ übereinstimmen. Offenbar ist das genau dann der Fall, wenn ihre Differenz$f - g$ im Ideal $J$ liegt, das durch die von der Nullstellenrelation $\perp$ induzierten Galoiskorrespondenz $V$ zugeordnet wird. Das ist aber gerade der Galois-Abschluss von $I$. Der Einschränkung der Polynomfunktionen auf $V$ entspricht algebraisch also der Übergang zum Faktorring $K[x_1, \ldots, x_n]/J$ mit dem Galois-abgeschlossenen Ideal $J$. Erinnert man sich an den Fall $K = \mathbb{R}$, die über $\mathbb{R}$ definierten euklidischen Vektorräume und an die dort auf der Hand liegende geometrische Interpretation von Lösungsmengen von Gleichungssystemen, so verwundert es nicht mehr, dass sich für jenes große Teilgebiet der Mathematik, das die hier angedeuteten Ansätze vertieft, die Bezeichnung „algebraische Geometrie“ eingebürgert hat. Wir werden diesen geometrisch orientierten Pfad allerdings nicht weiter verfolgen.

### 10.3.2 Ganze Erweiterungen und Ideale

Wir beginnen mit Hilfssätzen zu Satz 10.3.2.3, der im Beweis des Hilbertschen Nullstellensatzes eine wichtige Rolle spielen wird.

**Lemma 10.3.2.1.** *Sei $R \leq S$ ganz.*

1. *(Lying-over-Theorem): Sei $P \lhd R$ prim. Dann existiert ein $Q \lhd S$ prim mit $Q \cap R = P$.*

$$\begin{array}{lll} \exists Q & \lhd_{prim} & S \\ \downarrow \cap R & & \mid\!\vee \\ P & \lhd_{prim} & R \end{array}$$

2. *(Going-up-Theorem): Seien $P_1, P$ Primideale von $R$ mit $P_1 \subseteq P$, $Q_1 \lhd S$ prim mit $Q_1 \cap R = P_1$. Dann existiert ein $Q \lhd S$ prim mit $Q_1 \subseteq Q$ und $Q \cap R = P$.*

$$\begin{array}{lllll} & & \lhd_{prim} & & \\ Q_1 & \subseteq & \exists Q & \lhd_{prim} & S \\ \downarrow \cap R & & \downarrow \cap R & & \mid\!\vee \\ P_1 & \subseteq & P & \lhd_{prim} & R \\ & & \lhd_{prim} & & \end{array}$$

3. *(Eindeutigkeit von lying-over-Idealen, vgl. (a)): Sei $P \lhd R$ prim, seien $Q, Q_1 \lhd S$ beide prim mit $Q \supseteq Q_1$ und $Q \cap R = P = Q_1 \cap R$. Dann ist $Q = Q_1$.*

*Beweis.* 1. $T := R \setminus P$ ist multiplikativ, daher folgt aus Satz 10.1.4.1 die Existenz eines Primideals $Q \lhd S$, das als Ideal maximal ist mit der Eigenschaft $Q \cap (R \setminus P) = \varnothing$, also mit $Q \cap R \subseteq P$. Es bleibt zu zeigen, dass $P \subseteq Q$ und somit $P \subseteq Q \cap R$, insgesamt also $Q \cap R = P$.

Angenommen, es gäbe ein $u \in P \setminus Q$. Dann umfasst $Q + (u)$ (mit $(u) = Su$, weil das Erzeugnis in $S$ zu bilden ist) echt $Q$. Da $Q$ maximal mit $Q \cap (R \setminus P) = \varnothing$ ist, muss es ein $c \in (Q + (u)) \cap (R \setminus P)$ geben. Dieses Element lässt sich schreiben als $c = q + su$ mit $q \in Q, s \in S$. Weil $s$ ganz über $R$ ist, existieren $r_i \in R$ mit

$$s^n + r_{n-1}s^{n-1} + \ldots + r_1 s + r_0 = 0.$$

Multiplikation mit $u^n$ liefert

$$(su)^n + r_{n-1}u(su)^{n-1} + \ldots + r_1 u^{n-1}(su) + r_0 u^n = 0.$$

In dieser Gleichung verwenden wir nun $su = c - q$ und wenden darauf den binomischen Lehrsatz an. Alle Terme, wo $q$ vorkommt, liegen in $Q$, also auch die Summe der verbleibenden:

$$v := c^n + r_{n-1}uc^{n-1} + \ldots + r_1 u^{n-1}c + r_0 u^n \in Q.$$

Aus $c, u, r_i \in R$ folgt $v \in R$, also sogar $v \in R \cap Q \subseteq P$. Wegen $u \in P$ bedeutet das auch $c^n \in P$ und, da $P$ prim ist, $c \in P$, Widerspruch.

2. Ähnlich wie (a): Suche mittels $Q_1 \cap (R \setminus P) = \emptyset$ ein maximales Ideal $Q$ mit $Q_1 \subseteq Q$ und $Q \cap R = P$.

3. Es genügt zu zeigen, dass jedes Primideal $Q \lhd S$ mit $Q \cap R = P$ maximal ist unter allen Idealen $I \lhd S$ mit $I \cap (R \setminus P) = \emptyset$. Wir nehmen indirekt an, es gäbe ein solches $I$, das $Q$ echt umfasst, d.h. mit einem $u \in I \setminus Q$. Zunächst gilt $I \cap R \subseteq P$. Weil $S$ eine ganze Erweiterung von $R$ ist, ist $u$ Nullstelle eines monischen Polynoms, folglich gibt es auch ein monisches Polynom $f \in R[x]$ minimalen Grades mit $f(u) \in Q$. Sei $f(x) = \sum_{i=0}^{n} r_i x$ mit $r_n = 1$. Dann haben wir

$$u^n + r_{n-1}u^{n-1} + \ldots + r_1 u + r_0 = f(u) \in Q \subseteq I.$$

Es folgt $r_0 \in I \cap R \subseteq P = Q \cap R$, also

$$u(u^{n-1} + r_{n-1}u^{n-2} + \ldots + r_2 u + r_1) \in Q.$$

Weil $Q$ ein Primideal ist, muss einer der beiden Faktoren in $Q$ liegen. Der Klammerausdruck kann es wegen der minimalen Wahl von $n$ nicht sein, also $u \in Q$, was aber im Widerspruch zu $u \in I \setminus Q$ steht.

□

**UE 529 ► Übungsaufgabe 10.3.2.2.** Beweisen Sie Aussage 2 in Lemma 10.3.2.1(b). **◄ UE 529**

**Proposition 10.3.2.3.** *Sei $R \leq S$ eine ganze Ringerweiterung mit Primidealen $Q \lhd S$ und $P \lhd R$, die $Q \cap R = P$ erfüllen. Dann ist $Q$ ist genau dann maximal in $S$, wenn $P$ maximal in $R$ ist.*

*Beweis.* Sei zunächst $Q$ maximal in $S$. Wir erweitern $P$ zu einem in $R$ maximalen (und somit auch primen) Ideal $M$: $P \subseteq M \lhd R$. Laut der zweiten Aussage in Lemma 10.3.2.1gibt es ein Primideal $Q'$ von $S$ mit $Q \subseteq Q'$ und $Q' \cap R = M$. Wegen $Q' \neq S$ und der Maximalität von $Q$ folgt $Q = Q'$, also ist $P = Q \cap R = Q' \cap R = M$ maximal. Sei jetzt $P$ maximal in $R$. Wir erweitern $Q$ zu einem maximalen Ideal $N$ in $S$. Als echtes Ideal enthält $N$ sicher nicht das Einselement, folglich ist $R \cap N \neq R$. Wegen $P = R \cap Q \subseteq R \cap N$ und der Maximalität von $P$ folgt $P = R \cap N$. Nach der dritten Aussage in Lemma 10.3.2.1 folgt daraus $Q = N$. Also ist auch $Q$ maximal. □

**UE 530** ► **Übungsaufgabe 10.3.2.4.** Illustrieren Sie anhand geeigneter Beispiele, was sich verändert, wenn man in Proposition 10.3.2.3 gewisse Voraussetzungen ($R \leq S$ ganz, $P$ prim etc.) abschwächt. ◄ **UE 530**

### 10.3.3 Parametrisierung in Ringerweiterungen

Zur Motivation des folgenden, nach der großen Algebraikerin Emmy Noether (1882–1935) benannten Lemmas erinnern wir uns an Satz 6.1.5.6: Jede Körpererweiterung $K \leq E$ lässt sich interpretieren als eine Verkettung zweier Erweiterungen: einer rein transzendenten $K \subseteq Z = K(T)$ mit einer Transzendenzbasis $T$ von $E$, gefolgt von der rein algebraischen Erweiterung $Z \leq E$. Ersetzen wir die Körpererweiterung $K \leq E$ durch eine endliche Ringerweiterung $K \leq R$ des Körpers $K$ und „algebraisch“ durch „ganz“, so erhalten wir die Aussage des Normalisierungslemmas.

**Satz 10.3.3.1** (Noethersches Normalisierungslemma)**.** *Sei $R$ ein Integritätsbereich und eine endliche Ringerweiterung des Körpers $K$. Dann existieren algebraisch unabhängige $t_1, \ldots, t_r \in R$, sodass $R$ ganz ist über $K[t_1, \ldots, t_r]$. Dabei ist $r$ der Transzendenzgrad des Quotientenkörpers $E$ von $R$ über $K$.*

*Beweis.* Sei $R = K[u_1, \ldots, u_n]$, also $E = K(u_1, \ldots, u_n)$. Sind $u_1, \ldots, u_n$ algebraisch unabhängig über $K$, so ist $\{u_1, \ldots, u_n\}$ Transzendenzbasis von $E$ über $K$. Also folgt die Behauptung mit $r = n$ und $t_i = u_i$. Seien daher $u_1, \ldots, u_n$ algebraisch abhängig, also $r \leq n - 1$. Dann gilt eine Beziehung der Form

$$\sum_{(i_1,\ldots,i_n)\in I} k_{i_1\ldots i_n} u_1^{i_1} \ldots u_n^{i_n} = 0 \tag{10.1}$$

mit $\varnothing \neq I \subseteq \mathbb{N}^n$ endlich und $k_{i_1\ldots i_n} \in K \setminus \{0\}$ für alle $(i_1, \ldots, i_n) \in I$. Sei $c > i_s$, $c \in \mathbb{N}$ für alle $s$ mit $1 \leq s \leq n$ und $(i_1, \ldots, i_n) \in I$. Dann sind die ganzen Zahlen

$$i_1 + ci_2 + \ldots + c^{n-1} i_n,\ (i_1, \ldots, i_n) \in I,$$

paarweise verschieden (Darstellung zur Basis $c$). Daher gibt es ein eindeutiges Tupel $(j_1, \ldots, j_n) \in I$, so dass

$$e := j_1 + cj_2 + \ldots + c^{n-1} j_n$$

maximal ist. Wir definieren nun

$$\begin{aligned} v_2 &:= u_2 - u_1^c \\ v_3 &:= u_3 - u_1^{c^2} \\ &\vdots \\ v_n &:= u_n - u_1^{c^{n-1}}, \end{aligned}$$

also $u_i = v_i + u_1^{c^{i-1}}$ für $2 \leq i \leq n$. Mittels (10.1) erhält man

$$k_{j_1 \ldots j_n} u_1^e + f(u_1, v_2, \ldots, v_n) = 0,$$

wobei der Grad von $x_1$ in $f \in K[x_1, \ldots, x_n]$ kleiner ist als $e$. Das Polynom

$$g(x) := x^e + k_{j_1 \ldots j_n}^{-1} f(x, v_2, \ldots, v_n) \in K[v_2, \ldots, v_n][x]$$

ist monisch und hat $u_1$ als Nullstelle. Also ist $u_1$ ganz über $K[v_2, \ldots, v_n]$, und damit ist $K[u_1, v_2, \ldots, v_n] = K[v_2, \ldots, v_n][u_1]$ wegen Satz 10.2.1.2(d) ganz über $K[v_2, \ldots, v_n]$. Wegen $v_i = u_i - u_1^{c^{i-1}}$ sind außerdem $u_2, \ldots, u_n$ auf triviale Weise ganz über $K[u_1, v_2, \ldots, v_n]$. Nochmals nach Satz 10.2.1.2(d) ist daher auch $K[u_1, u_2, \ldots, u_n]$ ganz über $K[v_2, \ldots, v_n]$. Sind nun die $v_2, \ldots, v_n$ algebraisch unabhängig, so ist $\{v_2, \ldots, v_n\}$ Transzendenzbasis von $E$ über $K$ und die Behauptung ist mit $r = n - 1$ gezeigt. Sind die $v_2, \ldots, v_n$ algebraisch abhängig, so wiederholt man die obige Vorgangsweise und erhält, dass $K[v_2, \ldots, v_n]$ ganz ist über $K[w_3, \ldots, w_n]$, etc. Nach endlich vielen Schritten bricht dieser Prozess ab, und die Behauptung folgt. □

### 10.3.4 Der kleine Nullstellensatz

Eine „kleine“ (oder auch „schwache“) Version des Hilbertschen Nullstellensatzes besagt im Wesentlichen, dass über einem Körper $K$ jedes System aus polynomialen Gleichungen $f_i(x_1, \ldots, x_n) = 0$, $f_i \in K[x_1, \ldots, x_n]$, in den Variablen $x_1, \ldots, x_n$, aus dem sich nicht durch die Bildung von Linearkombinationen der Widerspruch $1 = 0$ ableiten lässt, eine Lösung $x_1 = a_1, \ldots, x_n = a_n$ mit Komponenten $a_i$ aus dem algebraischen Abschluss $\overline{K}$ von $K$ hat. Bevor wir den Beweis in aller Ausführlichkeit führen, ein paar Bemerkungen zur Beweisidee.

Denkt man an die Methoden der algebraischen Körpererweiterung bei der Nullstellensuche von Polynomen in einer Variablen aus Kapitel 6, so liegt folgende Konstruktion nahe: Die Voraussetzung an das Gleichungssystem besagt, dass das von den $f_i$ erzeugte Ideal $I$ nicht der gesamte Polynomring $K[x_1, \ldots, x_n]$ ist. Erweitert man $I$ zu einem maximalen Ideal $J \lhd K[x_1, \ldots, x_n]$, so ist der Faktorring $L := K[x_1, \ldots, x_n]/J$ ein Körper. Wenn $J$ nicht gerade das von $x_1, \ldots, x_n$ erzeugte Ideal ist, können wir $L$ vermittels $k \mapsto k + J$ als Körpererweiterung von $K$ auffassen. Die Elemente $a_i' := x_i + J$ bilden (analog zum Satz

von Kronecker für Polynome in einer Variablen) eine Lösung $(a'_1, \ldots, a'_n)$ des ursprünglich gegebenen Gleichungssystems. Wir wollen Lösungen aber in $\overline{K}$ finden und nicht in $L$. Wenn jedoch $L$ algebraisch über $K$ ist, so gibt es eine Einbettung $\iota : L \to \overline{K}$, so dass sich die gesuchte Lösung aus den Komponenten $a_i := \iota(a'_i)$ zusammensetzt. Tatsächlich lässt sich mit Hilfe des Noetherschen Normalisierungslemmas zeigen, dass gewisse Ringerweiterungen im Beweis ganz sind. Diese können dann durch eine geeignete Faktorisierung in eine algebraische Körpererweiterung $E$ von $K$ übergeführt werden. Dabei spielen die Ergebnisse aus 10.3.2 über das Zusammenspiel von Idealen mit ganzen Ringerweiterungen eine wesentliche Rolle. Doch nun zu Satz und Beweis in aller Ausführlichkeit (teilweise in modifizierter Notation).

**Satz 10.3.4.1** (Kleiner Hilbertscher Nullstellensatz)**.** *Sei $E$ ein algebraisch abgeschlossener Körper mit $K \leq E$ als Unterkörper, außerdem $I \lhd K[x_1, \ldots, x_n]$ ein echtes Ideal (also $I \neq K[x_1, \ldots, x_n]$). Dann ist*

$$I^{(\perp)} := \{(a_1, \ldots, a_n) \in E^n : f(a_1, \ldots, a_n) = 0 \text{ für alle } f \in I\} \neq \varnothing.$$

*Beweis.* Nach Satz 10.1.4.1 ist $I$ in einem primen Ideal $P \lhd K[x_1, \ldots, x_n]$ enthalten. Es folgt $P^{(\perp)} \subseteq I^{(\perp)}$. Es reicht daher zu zeigen, dass $P^{(\perp)} \neq \varnothing$ für alle Primideale $P$ von $K[x_1, \ldots, x_n]$. Man beachte, dass $P \cap K = \{0\}$ gelten muss, da sonst $P = K[x_1, \ldots, x_n]$ wäre. $S := K[x_1, \ldots, x_n]/P$ ist ein Integritätsbereich. Sei $\pi\colon K[x_1, \ldots, x_n] \to S$, $f \mapsto f + P$ der kanonische Homomorphismus und $u_i := \pi(x_i)$. Dann ist $S = \pi(K)[u_1, \ldots, u_n]$. $\pi|_K$ ist injektiv, also ein Isomorphismus zwischen $K$ und $\pi(K)$. Insbesondere ist $\pi(K)$ ein Körper. Nach dem Noetherschen Normalisierungslemma 10.3.3.1 existieren über $\pi(K)$ algebraisch unabhängige $t_1, \ldots, t_r \in S$, so dass $S$ ganz ist über $R := \pi(K)[t_1, \ldots, t_r]$. Bezeichne $M$ das von $t_1, \ldots, t_r$ in $R$ erzeugte Ideal. Dann ist

$$\begin{aligned} \varphi\colon \pi(K) &\to R/M \\ \pi(a) &\mapsto \pi(a) + M \end{aligned}$$

ein Isomorphismus, also ist $R/M$ ein Körper und daher muss $M$ ein maximales Ideal in $R$ sein. Nach Proposition 10.3.2.3 existiert ein maximales $N \lhd S$ mit $N \cap R = M$. Bezeichne $\tau\colon S \to S/N$, $s \mapsto s + N$, den kanonischen Homomorphismus, dann ist $\tau(S) = S/N$ ein Körper. Mit Obigem folgt aus dem zweiten Isomorphiesatz für den Isomorphismus $\psi := \tau\pi$:

$$\begin{array}{rcccccl} K & \cong & \pi(K) & \cong R/M = R/(N \cap R) & \cong & (R+N)/N = \tau(R) \\ \psi : a & \mapsto & \pi(a) & \mapsto \pi(a) + M & \mapsto & \pi(a) + N = \tau(\pi(a)). \end{array}$$

Sei $\overline{\tau(S)}$ ein algebraischer Abschluss von $\tau(S)$. Da $S$ ganz ist über $R$, ist $\tau(S)$ eine algebraische Körpererweiterung von $\tau(R)$, also ist $\overline{\tau(S)}$ auch ein algebraischer Abschluss von $\tau(R)$. $E$ enthält einen algebraischen Abschluss $\overline{K}$ von $K$. Nun besitzt $\psi$ eine Fortsetzung $\overline{\psi}\colon \overline{K} \to \overline{\tau(S)}$. Definiere

$$\sigma := \overline{\psi}^{-1}|_{\tau(S)}\colon \tau(S) \to \overline{K} \subseteq E$$

und

$$\rho := \sigma\tau\pi\colon K[x_1, \ldots, x_n] \xrightarrow{\pi} S \xrightarrow{\tau} \tau(S) \xrightarrow{\sigma} E.$$

Offensichtlich gilt $\rho|_K = \mathrm{id}_K$ und $\rho|_P \equiv 0$. Daher ist für alle $f \in P \lhd K[x_1, \ldots, x_n]$

$$f(\rho(x_1), \ldots, \rho(x_n)) = \rho(f(x_1, \ldots, x_n)) = 0,$$

wobei $\rho|_K = \mathrm{id}_K$ für die erste Gleichung verantwortlich ist, $\rho|_P \equiv 0$ für die zweite. Jedenfalls ist die gesuchte Nullstelle $(\rho(x_1), \ldots, \rho(x_n)) \in P^{(\perp)} \neq \varnothing$ gefunden. □

### 10.3.5 Der volle Nullstellensatz

Wir erinnern an die Definition 10.1.4.2 des Radikals $\mathrm{Rad}(I)$ eines Ideals $I \lhd R$ in einem kommutativen Ring $R$ mit 1 als Menge aller $r \in R$ mit $r^n \in I$ für ein $n > 0$ und an die Darstellung von $\mathrm{Rad}(I)$ aus Proposition 10.1.4.3 als Schnitt aller $I$ umfassender Primideale.
Der Hilbertsche Nullstellensatz besagt, dass $I \mapsto \mathrm{Rad}(I)$ der Abschlussoperator der von $\perp$ induzierten Galoiskorrespondenz ist. Daraus folgt sehr unmittelbar der Kleine Nullstellensatz 10.3.4.1: Ist nämlich $I$ ein echtes Ideal in $K[x_1, \ldots, x_n]$, so bedeutet das insbesondere $1 \notin I$. Weil es Primideale $P$ mit $I \subseteq P \neq K[x_1, \ldots, x_n]$, also $1 \notin P$ gibt, folgt daraus nach Definition des Radikals auch $1 \notin \mathrm{Rad}\, I = \left(I^{(\perp)}\right)^{(\perp)}$, woraus $I^{(\perp)} \neq \emptyset$ folgt.
Es ist bemerkenswert, dass auch umgekehrt der volle Nullstellensatz aus dem Kleinen hergeleitet werden kann, allerdings, wie wir gleich sehen werden, unter Verwendung eines sehr originellen Tricks, wo man an entscheidender Stelle den kleinen Nullstellensatz für $n+1$ statt für $n$ verwendet.

**Satz 10.3.5.1. (Hilbertscher Nullstellensatz)** *Sei $E$ ein algebraisch abgeschlossener Körper, $K \leq E$ und $I$ ein Ideal von $K[x_1, \ldots, x_n]$. Dann ist* $\mathrm{Rad}(I)$ *der Galois-Abschluss von $I$ bezüglich $\perp$, explizit: Die einzigen Polynome, die auf sämtliche Nullstellen von $I$ verschwinden, sind jene $f \in K[x_1, \ldots, x_n]$, für die eine Potenz $f^n$ mit positivem $n$ in $I$ liegt.*

*Beweis.* Für $I = K[x_1, \ldots, x_n]$ ist $\mathrm{Rad}(I)$ als Schnitt über die leere Menge wieder der ganze Polynomring, also gilt der Satz auf triviale Weise. Ab nun sei also $I$ ein echtes Ideal mit Galois-Abschluss $\overline{I}$. Wir haben die beiden Inklusionen $\mathrm{Rad}(I) \subseteq \overline{(I)}$ und $\overline{I} \subseteq \mathrm{Rad}(I)$ zu zeigen.

$\mathrm{Rad}(I) \subseteq \overline{I}$: Ist $f \in \mathrm{Rad}\, I$, dann ist $f^m \in I$ für ein $m \geq 0$. Ist $(a_1, \ldots, a_n) \in I^{(\perp)}$, dann ist $0 = f^m(a_1, \ldots, a_n) = (f(a_1, \ldots, a_n))^m$. Also ist $f(a_1, \ldots, a_n) = 0$. Daher ist $f \in \left(I^{(\perp)}\right)^{(\perp)} = \overline{I}$.

$\overline{I} \subseteq \mathrm{Rad}(I)$: Sei nun umgekehrt $f \in \overline{I}$, d.h. im Galois-Abschluss von $I$. Wegen $0 \in \mathrm{Rad}(I)$ dürfen wir $f \neq 0$ annehmen. Betrachte $K[x_1, \ldots, x_n] \leq K[x_1, \ldots, x_n, y]$. Sei $L$ das von $I$ und $y \cdot f - 1$ in $K[x_1, \ldots, x_n, y]$ erzeugte Ideal.
Wir behaupten: $L^{(\perp)} = \emptyset$. Denn wäre $(a_1, \ldots, a_n, b) \in L^{(\perp)} \subseteq E^{n+1}$, so auch $(a_1, \ldots, a_n) \in I^{(\perp)} \subseteq E^n$. Es gilt jedoch für alle $(a_1, \ldots, a_n) \in I^{(\perp)}$

$$(yf - 1)(a_1, \ldots, a_n, b) = bf(a_1, \ldots, a_n) - 1 = -1 \neq 0,$$

Widerspruch. Also gilt die Behauptung $L^{(\perp)} = \varnothing$.
Nach dem „Kleinen Nullstellensatz“ 10.3.4.1 kann daher $L$ kein echtes Ideal des Rings $K[x_1, \ldots, x_n, y]$ sein, also $L = K[x_1, \ldots, x_n, y]$. Insbesondere muss $1 \in L$ sein, also

$$1 = \sum_{i=1}^{t-1} g_i \cdot f_i + g_t \cdot (yf - 1),$$

wobei $f_1, \ldots, f_{t-1} \in I$, $g_1, \ldots, g_t \in K[x_1, \ldots, x_n, y]$. Wir definieren einen Einsetzungshomomorphismus $\varphi\colon K[x_1, \ldots, x_n, y] \to K(x_1, \ldots, x_n)$, der $K$ punktweise fest lässt, durch

$$x_j \mapsto x_j \text{ und } y \mapsto \frac{1}{f(x_1, \ldots, x_n)} = f^{-1} \in K(x_1, \ldots, x_n).$$

In obiger Darstellung des kontansten Polynoms 1 fällt bei dieser Ersetzung der letzte Summand weg:

$$1 = \sum_{i=1}^{t-1} g_i(x_1, \ldots, x_n, f^{-1}) \cdot f_i(x_1, \ldots, x_n).$$

Sei $m \in \mathbb{N}$ größer als alle Grade von $y$ in den $g_i$, dann ist

$$f^m(x_1, \ldots, x_n) \cdot g_i(x_1, \ldots, x_n, f^{-1}) \in K[x_1, \ldots, x_n]$$

für $i = 1, \ldots, t-1$, also

$$f^m = f^m \cdot 1 = \sum_{i=1}^{t-1} \underbrace{f^m(x_1, \ldots, x_n) g_i(x_1, \ldots, x_n, f^{-1})}_{\in K[x_1, \ldots, x_n]} \cdot \underbrace{f_i(x_1, \ldots, x_n)}_{\in I} \in I.$$

Damit ist $f \in \operatorname{Rad}(I)$, was zu zeigen war. □

# 11 Anhang: Mengentheoretische Grundlagen

## 11.1 Wohlordnungen

### 11.1.1 Grundbegriffe

**Definition 11.1.1.1.** Eine totale Ordnung (= lineare Ordnung = Kette)[1] $(W, <)$ heißt Wohlordnung (WO) :$\Leftrightarrow$

$$\forall T \subseteq W : [T \neq \emptyset \Rightarrow \exists \min(T)]$$

Die Ordnungsrelation $\leq_M$ in einem Modell $(M, 0_M, \nu_M, +_M, \cdot_M, \leq_M)$ der Peano-Axiome (siehe Abschnitt 1.1.3) ist nicht nur linear, sondern sogar eine Wohlordnung. Dies kann man mit Hilfe des Induktionsaxioms (siehe Definition 1.1.3.2) beweisen.

**Satz 11.1.1.2.** *Sei $(M, 0_M, \nu_M, +_M, \cdot_M, \leq_M)$ ein Modell der Peano-Arithmetik. Dann gilt*

(1) *Jede* beschränkte *nichtleere Teilmenge von $M$ hat ein kleinstes Element, das heißt: Für alle $n \in M$ gilt: Jede nichtleere Menge $A \subseteq \{k \in M : k \leq_M n\}$ hat ein kleinstes Element.*

(2) *Jede nichtleere Menge $B \subseteq \mathbb{N}$ hat ein kleinstes Element.*

Wir beweisen zunächst (1) mit Induktion nach $n$, und schließen dann daraus (2).

*Beweis von (1).* Sei $T$ die Menge aller Elemente $n \in M$, die die Bedingung (1) erfüllen. Man sieht leicht, dass $0 \in T$ gilt. Es gilt ja nach Definition $\{k \in M : k \leq_M 0\} = \{0\}$. Die einzige nichtleere Menge $A \subseteq \{0\}$ ist die Menge $\{0\}$ selbst, und die hat ein kleinstes Element.
Wir zeigen nun $n \in T \Rightarrow \nu_M(n) \in T$. Sei $A \subseteq \{k \in M : k \leq_M \nu_M(n)\}$ nicht leer. Wir definieren $A' := \{k \in A : k \neq \nu_M(n)\} = A \setminus \{\nu_M(n)\}$ und unterscheiden zwei Fälle:

Fall 1 $A'$ ist leer. Dann ist $A = \{\nu_M(n)\}$, und diese Menge hat sicher ein kleinstes Element.

Fall 2. $A'$ ist nicht leer. Für alle Elemente $k \in A'$ gilt $k \leq \nu_M(n)$, laut induktiver Definition von $\leq_M$ folgt also $k \leq n$ oder $k = \nu_M(n)$; der Fall $k = \nu_M(n)$ ist nach Definition von $A'$ unmöglich.

[1] Wenn kein Irrtum möglich ist, unterscheidet man oftmals nicht zwischen $W$ und $(W, <)$ und bezeichnet folglich $W$ als Wohlordnung. Wir unterscheiden auch nicht streng zwischen reflexiven und irreflexiven Wohlordnungen und deuten lediglich durch die Symbole $\leq$ bzw. $<$ (und ihre Varianten) an, ob wir gerade die reflexive oder irreflexive Version einer Wohlordnung meinen, dh. $\leq = <\uplus\{(\alpha, \alpha) \mid \alpha \in W\}$. Hierbei bezeichnet das Symbol $\uplus$ die disjunkte Vereinigung.

Somit ist $A'$ eine nichtleere Teilmenge von $\{k \in M : k \leq_M n\}$ und hat (wegen $n \in T$) ein kleinstes Element $k_0$. Aus $k_0 \leq n \leq \nu_M(n)$ ergibt sich, dass $k_0$ auch das kleinste Element von $A' \cup \{\nu_M(n)\} = A$ ist. □

*Beweis von (2).* Sei nun $B \subseteq M$ beliebig aber nicht leer. Sei also $b_1 \in B$. Wir betrachten die Menge $A := \{k \in B : k \leq_M b_1\}$. Diese Menge enthält $b_1$ und ist daher nicht leer. Laut (1) hat sie also ein kleinstes Element $b_0$, welches natürlich $b_0 \leq_M b_1$ erfüllen muss. Aus $b_0 = \min(A)$ erhält man (mit Transitivität der Relation $\leq_M$) wie in (1) die Beziehung $b_0 = \min(B)$. □

**Definition 11.1.1.3.** Seien $(W, <), (W_i, <_i), i \in \{1, 2\}$ Wohlordnungen.

- $(A, <)$ heißt Anfangsabschnitt von $(W, <) :\Leftrightarrow$

$$A \subseteq W \wedge \forall \alpha, \beta \in W : [\alpha \in A \wedge \beta < \alpha \Rightarrow \beta \in A]$$

- $W_\alpha := \{\beta \in W : \beta < \alpha\}$ heißt der von $\alpha$ induzierte Anfangsabschnitt (von $W$).
- $f \colon W_1 \to W_2$ heißt schwach monoton (bezüglich $(W_1, \leq_1), (W_2, \leq_2)) :\Leftrightarrow$

$$\forall \alpha, \beta \in W_1 : \alpha \leq_1 \beta \Rightarrow f(\alpha) \leq_2 f(\beta))$$

- $f \colon W_1 \to W_2$ heißt streng monoton (bezüglich $(W_1, \leq_1), (W_2, \leq_2)) :\Leftrightarrow$

$$\forall \alpha, \beta \in W_1 : \alpha <_1 \beta \Rightarrow f(\alpha) <_2 f(\beta))$$

- $f \colon W_1 \to W_2$ heißt Ordnungsisomorphismus wenn $f$ bijektiv und monoton ist.[2]

**Anmerkung 11.1.1.4.** Wenn $(L, R)$ eine lineare Ordnung ist, wird jede Teilmenge $T \subseteq L$ durch $R$ (genauer: durch die Einschränkung der Relation $R$ auf die Untermenge $T$, formal ist dies die Relation $R|T := R \cap (T \times T)$) auch linear geordnet. Wenn $(L, R)$ überdies eine Wohlordnung ist, sieht man leicht, dass auch $(T, R|T)$ eine Wohlordnung ist.
Statt $(T, R|T)$ schreiben wir oft der besseren Lesbarkeit halber nur $(T, R)$.

**Definition 11.1.1.5.** In Wohlordnungen unterscheidet man drei Arten von Elementen $\alpha$:

1. $\alpha = 0 := \min(W)$
2. $\exists \beta \in W : \alpha = \beta + 1$, wobei wir $\beta + 1$ als Abkürzung für $\min\{\gamma \in W : \beta < \gamma\}$ verstehen. $\alpha$ heißt dann Nachfolger[3] von $\beta$.
3. $\alpha \neq 0 \wedge \forall \beta \in W : \alpha \neq \beta + 1$. $\alpha$ heißt dann Limeselement. [4]

[2] Ordnungsisomorphismen übertragen ordnungstheoretische Eigenschaften.
[3] Um zu betonen, dass es um den Nachfolger im Sinne der Ordnung $(W, <)$ geht, kann man auch $\beta +_W 1$ oder $\beta +_{(W,<)} 1$ schreiben.
[4] Je nachdem, ob es praktisch ist, bezeichnet man manchmal auch 0 als Limeselement.

**Beispiele 11.1.1.6** (von Wohlordnungen)**.**

(a) Jede endliche Kette. (Insbesondere sind wird auch die leere Menge durch die einzig mögliche Ordnungsrelation wohlgeordnet, ebenso wie jede 1-elementige Menge.)

(b) $\mathbb{N} = \omega = \{0 < 1 < 2 < ...\}$

(c) $\omega + 1 = \omega \cup \{\omega\} = \{0 < 1 < 2 < \cdots < \omega\}$

**UE 531** ► **Übungsaufgabe 11.1.1.7.** Sei $(W_i, <_i)_{i\in I}$ eine Familie von Wohlordnungen, wobei $(I, <)$ ebenfalls eine Wohlordnung ist. Gib eine Wohlordnung auf $\bigcup_{i\in I}\{i\} \times W_i$ an. ◄ **UE 531**

## 11.1.2 Transfinite Induktion

**Lemma 11.1.2.1** (Prinzip der transfiniten Induktion)**.** *Eine Kette $(W, <)$ ist wohlgeordnet genau dann, wenn*

$$\forall T \subseteq W : \Big[(\forall \alpha \in W : (W_\alpha \subseteq T \Rightarrow \alpha \in T)) \;\Rightarrow\; T = W\Big]$$

*Beweis.* Die folgenden Aussagen sind äquivalent:

- $\forall T \subseteq W : (\forall \alpha \in W : (W_\alpha \subseteq T \Rightarrow \alpha \in T) \Rightarrow T = W)$
- $\forall T \subseteq W : (T \neq W \Rightarrow \neg\forall \alpha \in W : (W_\alpha \subseteq T \;\Rightarrow\; \alpha \in T))$
  (Diese Äquivalenz erhält man, weil allgemein die Aussagen $p \Rightarrow q$ und $\neg q \Rightarrow \neg p$ äquivalent sind.
- $\forall T \subseteq W : (T \neq W \Rightarrow \exists \alpha \in W : (W_\alpha \subseteq T \;\wedge\; \alpha \notin T))$
  (Die Negation von $p \Rightarrow q$ ist $(p \wedge \neg q)$.)
- $\forall S \subseteq W : (S \neq \emptyset \Rightarrow \exists \alpha \in W : (W_\alpha \subseteq W \setminus S \;\wedge\; \alpha \in S))$
  (Diese Äquivalenz erhält man, wenn man $S := W \setminus T$ bzw. $T := W \setminus S$ setzt.)
- $\forall S \subseteq W : (S \neq \emptyset \Rightarrow \exists \alpha \in W : (\alpha = \min(S)))$.
  (Denn $\alpha = \min(S)$ bedeutet, dass erstens $\alpha \in S$ gilt, aber zweitens kein $\beta < \alpha$ in $S$ liegt, also $W_\alpha \subseteq W \setminus S$.)
- $W$ ist Wohlordnung. (Nach Definition.) □

**Anmerkung 11.1.2.2.** Bei Anwendungen von 11.1.2.1 sprich man von einem Beweis durch transfinite Induktion. Der „Induktionsanfang“ entspricht dem Falle $\alpha = \min(W)$, $W_\alpha = \emptyset$. Im „Induktionsschritt“ unterscheidet man meist zwischen Nachfolger- und Limeselement, d.h. man überprüft die Implikation $W_\alpha \subseteq T \Rightarrow \alpha \in T$ für die Fälle „$\alpha$ ist Nachfolger, d.h. $\exists\beta : \alpha = \beta + 1$ und „$\alpha$ ist Limeselement, d.h. $\forall\beta < \alpha : \beta + 1 < \alpha$“.

**UE 532** ▶ **Übungsaufgabe 11.1.2.3.** Finden Sie eine nichtleere Teilmenge $T \subseteq \mathbb{Q}$ der rationalen Zahlen, die zwar ◀ **UE 532**

$$\forall \alpha \in \mathbb{Q} : (\mathbb{Q}_\alpha \subseteq T \Rightarrow \alpha \in T) \qquad (\text{mit } \mathbb{Q}_\alpha := \{x \in \mathbb{Q} : x < \alpha\})$$

erfüllt, aber trotzdem nicht $T = \mathbb{Q}$ erfüllt. Wenn möglich, finden Sie so eine Menge $T$, die alle negativen rationalen Zahlen enthält.

**Lemma 11.1.2.4.** *Sei $(W, <)$ eine Wohlordnung. Dann gilt:*

*(a1)* $A \subsetneqq W$ *echter Anfangsabschnitt* $\Rightarrow A = W_\alpha$, *wobei* $\alpha = \min(W \setminus A)$.

*(a2) Die Abbildung $\alpha \mapsto W_\alpha$ ist ein Isomorphismus zwischen $(W, \leq)$ und der Ordnung $(\{W_\alpha : \alpha \in W\}, \subseteq)$.*
*Ebenso ist $(W_\alpha, \leq)$ isomorph zu $(\{W_\beta : \beta < \alpha\}, \subseteq)$.*

*(b)* $f : W \to W$ *streng monoton* $\Rightarrow \forall \alpha \in W : \alpha \leq f(\alpha)$.

*(b') Die Identität ist der einzige Automorphismus von $(W, \leq)$.*
*(Dies folgt aus (b): Wenn $f$ Automorphismus ist, dann auch $f^{-1}$; wenn nun $f(x) = y$ und daher auch $f^{-1}(y) = x$ ist, muss $x \leq y \leq x$ gelten, also $x = y$.)*

*(c)* $(W, \leq) \cong (W', \leq')$ $\Rightarrow$ *der Isomorphismus $f : W \to W'$ ist eindeutig. Dies folgt leicht aus (b'): Wenn $f_1$, $f_2$ Isomorphismen sind, so ist $f_1^{-1} \circ f_2$ Automorphismus von $W$, also $f_1^{-1} \circ f_2 = id$.*

*(d)* $\alpha \in W \Rightarrow (\forall T \subseteq W_\alpha : T \ncong W)$*: Eine Wohlordnung ist niemals zu einem echten Anfangsabschnitt oder zu einer Teilmenge eines echten Anfangsabschnitts isomorph.*
*(Denn für einen Isomorphismus $f : W \to T$ müsste $f(\alpha) < \alpha$ gelten, was (b) widerspricht.)*

*(e)* $\alpha < \beta \in W \Rightarrow W_\alpha \ncong W_\beta$. *Dies folgt aus (d) für $W = W_\beta$.*

*(f) Für jede Kette $(K, <)$ gilt: $(K, <)$ ist Wohlordnung* $\Leftrightarrow \forall \alpha \in K : (W_\alpha, <)$ *ist Wohlordnung.*

**UE 533** ▶ **Übungsaufgabe 11.1.2.5.** Zeigen Sie 11.1.2.4 (a1) und (a2). ◀ **UE 533**

**UE 534** ▶ **Übungsaufgabe 11.1.2.6.** Zeigen Sie 11.1.2.4 (b). ◀ **UE 534**

**UE 535** ▶ **Übungsaufgabe 11.1.2.7.** Zeigen Sie 11.1.2.4 (f). ◀ **UE 535**

**Satz 11.1.2.8** (Vergleichbarkeit von Wohlordnungen)**.** *Seien $(W, <)$ und $(W', <')$ Wohlordnungen. Dann gilt genau eine der folgenden Aussagen*

*(i)* $(W, <) \cong (W', <')$

*(ii)* $\exists \alpha' \in W' : (W, <) \cong (W'_{\alpha'}, <')$. *Wir schreiben hierfür auch* $(W, <) < (W', <')$ *und sagen, dass* $W$ *kürzer als* $W'$ *ist.*

*(iii)* $\exists \alpha \in W : (W', <') \cong (W_\alpha, <)$. *Schreib- und Sprechweisen analog.*

*Beweis.* Sei $T := \{\alpha \in W : \exists \alpha' \in W' : W_\alpha \cong W'_{\alpha'}\}$ und $f := \{(\alpha, \alpha') \in W \times W' : W_\alpha \cong W'_{\alpha'}\}$. Dann ist $f$ eine Funktion $T \to W'$, denn zu jedem $\alpha \in T$ ist das $\alpha'$ eindeutig, weil aus $(\alpha, \alpha'), (\alpha, \tilde{\alpha}') \in f$ mit $\alpha' \neq \tilde{\alpha}'$ folgt, dass $W'_{\alpha'} \cong W'_{\tilde{\alpha}'}$ im Widerspruch zu 11.1.2.4(e). Offensichtlich gilt:

- $T$ ist Anfangsabschnitt von $W$.
- $f$ ist strikt monoton.
- $f(T)$ ist Anfangsabschnitt von $W'$.

Nun sind 4 Fälle denkbar:

- $T = W$ und $f(T) = W'$.
- $T = W$ und $f(T) \subsetneq W'$.
- $T \subsetneq W$ und $f(T) = W'$.
- $T \subsetneq W$ und $f(T) \subsetneq W'$.

Die ersten drei Fälle entsprechen genau den Punkten (i), (ii), (iii) in unserer Behauptung, und der vierte Fall ist unmöglich. Wäre nämlich $T \neq W \wedge f(T) \neq W'$, so gäbe es nach (a) Elemente $\alpha \in W, \alpha' \in W'$ mit $T = W_\alpha, f(T) = W'_{\alpha'}$. Daher $(\alpha, \alpha') \in f \Rightarrow \alpha \in T = W_\alpha$ aber $\alpha \notin W_\alpha$. Widerspruch. □

### 11.1.3 Die „Wohlordnung“ aller Wohlordnungen modulo $\cong$

Sei $W = \{(T, <_T) : T \in \mathcal{M}\}$ eine Menge von Wohlordnungen. Dann definiert

$$(S, <_S) \leq_W (T, <_T) :\Leftrightarrow \exists \text{ Anfangsabschnitt } A \text{ von } T \text{ mit } (S, <_S) \cong (A, <_T)$$

eine Quasiordnung, deren induzierte Halbordnung (Faktorisierung nach $\cong$, vergleiche auch 2.1.1.10) wegen 11.1.2.4 (f) eine Totalordnung ist. Diese ist sogar wohlgeordnet: Sei $\emptyset \neq \mathcal{T} \subseteq \mathcal{W}/_\cong$, $(T_1, <_1) \in \mathcal{T}$. Ist $[(T_1, <_1)]_\cong$ nicht selbst minimal in $\mathcal{T}$, so können wir ein minimales $t_0 \in T_1$ finden, sodass der Anfangsabschnitt $((T_1)_{t_0}, <_1)$ Repräsentant einer Klasse in $\mathcal{T}$ ist. Diese Klasse ist nun das gesuchte minimale Element.
In diesem Sinne ist die Klasse (nicht Menge!) aller Wohlordnungen selbst „wohlgeordnet“.

## 11.2 Definition durch transfinite Rekursion

### 11.2.1 Der Rekursionssatz

**Definition 11.2.1.1.** Für eine Funktion $f\colon A \to B$ und eine Teilmenge $T \subseteq A$ bezeichnet $f\restriction T$ oder $f|_T$ für die Einschränkung von $f$ auf $T$, d.h.

$$f\restriction T := f \cap (T \times B)$$

**Satz 11.2.1.2** (Rekursionssatz)**.** *Sei $S$ eine Menge, $(W, \leq)$ eine Wohlordnung, $\mathcal{F}_0 \subseteq \mathcal{F} := \bigcup_{\alpha \in W} S^{W_\alpha}$, $h\colon \mathcal{F}_0 \to S$, $* \notin S$. Dann gibt es genau ein $F\colon W \to S \cup \{*\}$ mit*

$$\forall \alpha \in W : F(\alpha) = \begin{cases} h(F\restriction W_\alpha) & \text{falls } F\restriction W_\alpha \in \text{ dom } h = \mathcal{F}_0 \\ * & \text{sonst} \end{cases}$$

*Ist $\mathcal{F}_0 = \mathcal{F}$, so tritt stets der erste, interessante Fall ein, und es gilt $F\colon W \to S$.*

**Anmerkung 11.2.1.3.** Der Satz gilt sinngemäß auch für $W = \mathbb{O}$ (= Klasse der Ordinalzahlen, vgl. 11.1.3).

*Beweis.* Die Eindeutigkeit folgt unmittelbar durch transfinite Induktion für $T := \{\alpha \in W : F_1(\alpha) = F_2(\alpha)\}$.
Wir fügen zu $W$ ein weiteres Element $\infty$ hinzu, für welches $(\forall w \in W : w < \infty)$ gelten soll; statt $W$ schreiben wir nun $W_\infty$, an den Mengen $W_\alpha$ ändert sich nichts.
Wir interessieren uns also für die Existenz von $F$: Sei $T$ die Menge aller $\alpha \in W \cup \{\infty\}$, sodass der Satz für $W_\alpha$ statt für $W$ gilt, und für $\alpha \in T$ sei $F_\alpha$ das dazugehörige $F_\alpha : W_\alpha \to S \cup \{*\}$. Offenbar ist mit $\beta < \alpha \in T$ auch $\beta \in T$ (weil die Einschränkung von $F_\alpha\colon W_\alpha \to S \cup \{*\}$ auf $W_\beta$ als $F_\beta$ dienen kann) und wegen der Eindeutigkeit $F_\beta = F_\alpha\restriction W_\beta$.
Behauptung: Es gilt $T = W \cup \{\infty\}$. Laut Lemma 11.1.2.1 müssen wir also aus der Annahme $W_\alpha \subseteq T$ die Folgerung $\alpha \in T$ ziehen können.

$$\text{1. Fall :} \quad \alpha_0 \text{ ist Limeselement } \Rightarrow F_{\alpha_0} := \bigcup_{\alpha < \alpha_0} F_\alpha \text{ zeigt } \alpha_0 \in T \tag{11.1}$$

$$\text{2. Fall :} \quad \alpha_0 = \beta + 1 \text{ ist Nachfolger } \Rightarrow F_{\alpha_0} := F_{\beta_0} \cup \{(\beta_0, h(F_{\beta_0})\} \text{ zeigt } \alpha_0 \in T \tag{11.2}$$

Also ist $T = W \cup \{\infty\}$ und $F_\infty$ ist die gewünschte Funktion. □

**Anmerkung 11.2.1.4.** Eine Anwendung des Rekursionssatzes werden wir zum Beispiel in Satz 6.2.3.1 (Eindeutigkeit des Zerfällungskörpers) sehen.

### 11.2.2 Vollständige Induktion auf $\mathbb{N}$

Für $W = \mathbb{N}$ reflektiert 11.2.1.2 die Definition durch „Ordnungsinduktion“, wo auf beliebige Vorgänger zurückgegriffen wird. Bei der „gewöhnlichen“ Rekursion $x_{n+1} = f(x_n)$ („Nachfolgerinduktion“) hängt $h$ immer nur von dem letzten Folgenglied ab.

## 11.3 Äquivalenzen des Auswahlaxioms

### 11.3.1 Präliminarien

**Satz 11.3.1.1** (Satz von Hartogs)**.** *Zu jeder Menge $M$ gibt es eine Wohlordnung $(W, \leq)$, sodass es keine injektive Funktion $f\colon W \to M$ gibt.*

**Anmerkung 11.3.1.2.** Man ist geneigt zu sagen, dass es zu jeder Menge $M$ eine Wohlordnung, die „größer“ als $M$ ist, gibt.
Der Satz verwendet das Auswahlaxiom nicht!

*Beweis.* Die Menge $W := \{\, (T, <_T) \,:\, T \subseteq M, (T, <_T) \text{ ist Wohlordnung} \,\}/_{\cong}$ ist nach 11.1.3 selbst wohlgeordnet durch $<_W$. Angenommen es gäbe eine injektive Funktion $f\colon W \to M$, dann sei $T := f(W)$.
Dann ist $f\colon W \to T$ eine Bijektion; es gibt daher eine (eindeutig bestimmte) Relation $<_T$ auf $T$, sodass $f\colon W, <) \to (T, <_T)$ zu einem Ordnungsisomorphismus wird.
Also ist $w_0 := [(T, <_T)]_{\cong} \in W$.
Die Abbildung $t \mapsto (T_t, <)$ ist ein Ordnungsisomorphismus zwischen $(T, <_T)$ und dem durch $w_0$ definierten Anfangsabschnitt $(W_{w_0}, <_W)$ von $W$. Daher gilt

$$(W, <_W) \overset{f}{\cong} (T, <_T) \cong (W_{w_0}, <_W).$$

Also müsste $W$ zu einem Anfangsabschnitt von sich selbst isomorph sein. Dies ist aber nach 11.1.2.4 (d) nicht möglich. □

**Definition 11.3.1.3** (Familie von endlichem Charakter)**.** Eine Menge $\mathcal{F}$ (von Mengen) hat *endlichen Charakter* wenn für alle Mengen $X$ die folgende Äquivalenz gilt:

$$X \in \mathcal{F} \;\Leftrightarrow\; [\forall T \subseteq X : (T \text{ endlich } \Rightarrow T \in \mathcal{F})].$$

Das heißt, dass eine Menge $X$ genau in $\mathcal{F}$ liegt, wenn es alle ihre endlichen Teilmengen tun.

**Anmerkung 11.3.1.4.** Jede Familie von endlichem Charakter ist unter Untermengen abgeschlossen. Wenn man zu überprüfen hat, dass eine vorgegebene Familie endlichen Charakter hat, dann ist die Implikation $X \in \mathcal{F} \;\Rightarrow\; [\forall T \subseteq X : (T \text{ endlich } \Rightarrow T \in \mathcal{F})]$ und sogar die stärkere Aussage $X \in \mathcal{F} \;\Rightarrow\; (\forall T \subseteq X : T \in \mathcal{F})$ meist aus trivialen Gründen erfüllt, und nur die Implikation

$$[\forall T \subseteq X : (T \text{ endlich } \Rightarrow T \in \mathcal{F})] \;\Rightarrow\; X \in \mathcal{F}$$

erfordert ein mathematisches Argument. Meist ist es übersichtlicher stattdessen die Kontraposition zu beweisen, also:

$$\forall X :\; [\; X \notin \mathcal{F} \;\Rightarrow\; \exists E \subseteq T : (E \text{ endlich } \;\wedge\; E \notin \mathcal{F}) \;]$$

**Lemma 11.3.1.5.** *Sei $\mathcal{F}$ eine Familie von endlichem Charakter. Dann hat jede Kette der Halbordnung $(\mathcal{F}, \subseteq)$ eine obere Schranke (in $\mathcal{F}$).*

*Beweis.* Sei $\mathcal{K} \subseteq \mathcal{F}$ eine Kette in $(\mathcal{F}, \subseteq)$ und sei $T \subseteq \bigcup \mathcal{K}$ beliebig aber endlich. Dann gibt[5] es ein $K \in \mathcal{K}$ mit $T \subseteq K \in \mathcal{F}$ und damit $T \in \mathcal{F}$. Also liegt $\bigcup \mathcal{K}$ in $\mathcal{F}$ und ist damit eine obere Schranke für $\mathcal{K}$. □

### 11.3.2 Formulierung der Äquivalenzen

**Definition 11.3.2.1** (Auswahlaxiom, Axiom of Choice, AC)**.** Sei $\mathcal{M}$ eine Menge nichtleerer, paarweise disjunkter Mengen. Dann gibt es ein $A \subseteq \bigcup \mathcal{M}$, sodass

$$\forall M \in \mathcal{M} : \exists m \in M : M \cap A = \{m\}$$

$A$ heißt in diesem Zusammenhang auch eine *Auswahlmenge.*

**Lemma 11.3.2.2** (Auswahlfunktion, AF)**.** *Sei $I$ eine Menge und $(M_i)_{i \in I}$ eine Familie[6] nichtleerer Mengen, dh. $M_i \neq \emptyset$ $\forall i \in I$. Dann gibt es ein $f \colon I \to \bigcup_{i \in I} M_i$, sodass $\forall i \in I : f(i) \in M_i$. In anderen Worten: Das kartesische Produkt nichtleerer Mengen ist nicht leer. Die Funktion $f$ heißt* Auswahlfunktion.

**Lemma 11.3.2.3** (Hausdorffsches Maximalitätsprinzip, Hausdorffscher Kettensatz, HMP)**.** *Sei $(H, \leq)$ eine Halbordnung, $K_0 \subseteq H$ eine Kette. Dann gibt es eine maximale Kette $K : K_0 \subseteq K \subseteq H$.*

**Lemma 11.3.2.4** (Lemma von Zorn, LVZ)**.** *Sei $(H, \leq)$ eine Halbordnung, in der jede Kette eine obere Schranke hat,[7] das heißt: $\forall K \subseteq H : K$ Kette $\Rightarrow \exists h_K \in H : k \leq h_K$. Dann gilt $\forall h \in H : \exists m_h \in H : h \leq m_h, m_h$ maximal in $(H, \leq)$.*

Häufig wendet man das Lemma von Zorn auf eine Teilmenge $\mathcal{F} \subseteq \mathfrak{P}(M)$, geordnet durch $\subseteq$ an. Für eine Kette $\mathcal{K} \subseteq \mathcal{F}$ gibt es einen natürlichen Kandidaten für eine obere Schranke, nämlich $S = \bigcup \mathcal{K}$. Kann man zeigen,[8] dass stets $S \in \mathcal{F}$ gilt, so sind die Voraussetzungen des Lemmas von Zorn erfüllt. Hat $\mathcal{F}$ endlichen Charakter, ist dies stets der Fall.

[5] Hier verwendet man Induktion nach der Größe von $T$.

[6] Es sei bemerkt, dass man jede Menge zu einer Familie machen kann, indem man sie mit sich selbst indiziert.

[7] Eine partielle Ordnung, in der jede Kette eine obere Schranke hat, kann nicht leer sein (weil die leere Menge eine Kette ist, und folglich eine obere Schranke haben müsste). Oft beginnt man in einer Anwendung des Zornschen Lemmas aber mit einem expliziten Beweis, dass die betrachtete bzw. gerade konstruierte Halbordnung nicht leer ist, um sich ab dann nur mit nichtleeren Ketten beschäftigen zu müssen.

[8] Achtung! Hier kann die üblicherweise verwendete schlampige Notation Verwirrung stiften. Wenn man von der Ordnung $(\mathcal{F}, \subseteq)$ spricht, meint man nämlich die Ordnung $(\mathcal{F}, \leq)$, wobei $\leq$ die Einschränkung der Teilmengenrelation auf $\mathcal{F}$ ist; dies wird durch die Notation aber verschleiert. Wenn man nun $S := \bigcup \mathcal{K}$ setzt, ist $Q \subseteq S$ für alle $Q \in \mathcal{K}$ zwar automatisch erfüllt, aber für $Q \leq S$ muss man erst $S \in \mathcal{F}$ zeigen.

**Lemma 11.3.2.5** (Lemma von Teichmüller/Tukey, LTT)**.** *Sei $\mathcal{F}$ eine Familie von endlichem Charakter. Dann hat $\mathcal{F}$ ein $\subseteq$-maximales Element.*

**Satz 11.3.2.6** (Wohlordnungssatz, WOS, Satz von Zermelo)**.** *Sei $W$ eine Menge. Dann gibt es eine Wohlordnung $\leq$ auf $W$, dh. es gibt eine Relation $\leq \subseteq W \times W$, sodass $(W, \leq)$ eine Wohlordnung ist.*

### 11.3.3 Beweis der Äquivalenz der Aussagen in 11.3.2

**Satz 11.3.3.1.** *Es sind äquivalent:*

*AC* *Das Auswahlaxiom, 11.3.2.1*

*AF* *Die Existenz einer Auswahlfunktion, 11.3.2.2*

*HMP* *Das Hausdorffsches Maximalitätsprinzip, 11.3.2.3*

*LVZ* *Das Lemma von Zorn, 11.3.2.4*

*LTT* *Das Lemma von Teichmüller/Tukey, 11.3.2.5*

*WOS* *Der Wohlordnungssatz von Zermelo, 11.3.2.6*

Der Beweis ergibt sich durch den Nachweis der folgenden Implikationen:

*Beweis von AC $\Rightarrow$ AF.* Seien die nichtleeren Mengen $M_i$ für $i \in I$ gegeben, und sei $M_i^* := \{i\} \times M_i$. Dann ist $\mathcal{M} := (M_i^*)_{i \in I}$ eine paarweise disjunkte Familie und erfüllt damit die Voraussetzungen des Auswahlaxioms, das heißt es gibt eine Auswahlmenge $f \subseteq \bigcup \mathcal{M}$ mit $\forall i \in I : \exists! m_i^* = (i, m_i) \in f \cap M_i^*$, wobei $m_i \in M_i$. Also ist

$$f\colon \begin{cases} I \to \bigcup_{i \in I} M_i \\ i \mapsto m_i \end{cases}$$

die gesuchte Auswahlfunktion. □

*Beweis von AF $\Rightarrow$ HMP.* Sei $(H, \leq)$ eine Halbordnung und $K_0 \subseteq H$ eine Kette. Angenommen, es gäbe keine maximale Kette $K$ mit $K_0 \subseteq K \subseteq H$. Das heißt, dass für jede Kette $K \supseteq K_0$ die Menge

$$R(K) := \{x \in H \mid x \notin K,\ K \cup \{x\} \text{ ist Kette in } (H, \leq)\}$$

nicht leer ist.
Mit Satz 11.3.1.1 finden wir eine Wohlordnung $(W, <)$, sodass es keine injektive Funktion $W \to H$ gibt. Sei weiters $g$ eine Auswahlfunktion auf $\mathfrak{P}(H) \setminus \{\emptyset\}$.
Durch Anwendung des Rekursionssatzes 11.2.1.2 erhalten wir eine Funktion $F\colon W \to B \cup \{*\}$, die für alle $\alpha \in W$ die Beziehung

$$F(\alpha) = \begin{cases} g(R(F[W_\alpha])), & \text{wenn } F[W_\alpha] \text{ Kette ist} \\ *, & \text{sonst} \end{cases}$$

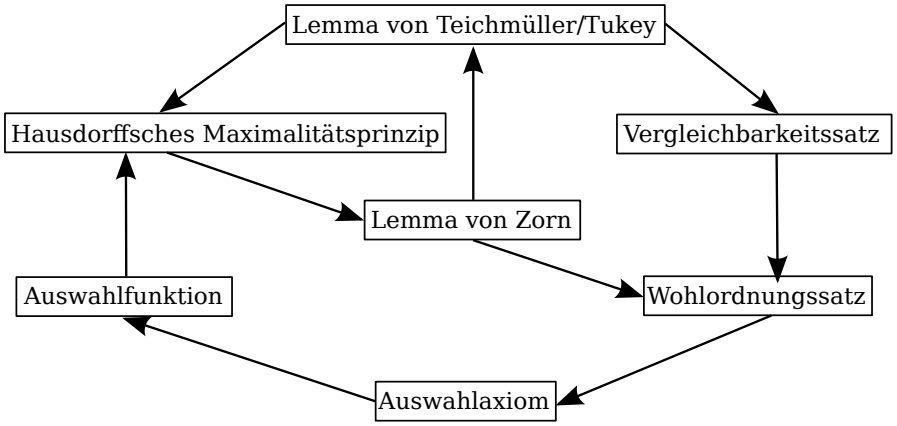



Abbildung 11.1: Die Pfeile symbolisieren die in diesem Abschnitt gezeigten Implikationen, mit Ausnahme des Vergleichbarkeitssatzes 11.4.3.3.

Mit transfiniter Induktion kann man zeigen, dass $F[W_\alpha]$ immer eine Kette ist, und dass daher $F$ nie den Wert $*$ annimmt. Da immer $R(K) \notin K$ gilt, sieht man auch, dass $F$ injektiv ist. Dies ist ein Widerspruch zur Definition von $W$. □

*Beweis von HMP ⇒ LVZ.* Sei $(H, \leq)$ eine Halbordnung, in der alle Ketten nach oben beschränkt sind und $h \in H$. Nach HMP gibt es eine maximale Kette $K$, $h \subseteq K \subseteq H$. Sei $m \in H$ eine obere Schranke von $K$. Wegen der Maximalität von $K$ folgt, dass $m \in K$ und $m$ maximal in $H$ ist. □

*Beweis von LVZ ⇒ LTT.* Sei $\mathcal{F}$ eine Familie von endlichem Charakter. Dann ist $(\mathcal{F}, \subseteq)$ eine Halbordnung, in der wegen 11.3.1.5 alle Ketten nach oben beschränkt sind. Also gibt es nach LVZ ein maximales Element. □

*Beweis von LTT ⇒ HMP.* Sei $(H, \leq)$ eine Halbordnung. Man sieht leicht, dass die Menge $\{K \subseteq H \mid K \text{ ist Kette}\}$ endlichen Charakter hat. In der Tat ist ein $K \subseteq H$ genau dann eine Kette, wenn je zwei (also endlich viele) Elemente aus $K$ vergleichbar (also eine Kette) sind. □

*Beweis von LVZ ⇒ WOS.* Sei $W$ eine beliebige Menge,
$H := \{(T, \leq) \mid T \subseteq W, (T, \leq) \text{ ist Wohlordnung}\}$ und

$$(T_1, \leq_1) \leq (T_2, \leq_2) :\Leftrightarrow T_1 \subseteq T_2 \quad \wedge \quad T_1 \text{ ist Anfangsabschnitt von } (T_2, \leq_2).$$

$(H, \leq)$ ist eine Halbordnung. Sei $K = \{(T_i, \leq_i) \mid i \in I\} \subseteq H$ eine Kette in $(H, \leq)$ und $T = \bigcup_{i \in I} T_i$, $\leq_T = \bigcup_{i \in I} \leq_i$. Dann ist $(T, \leq_T) \in H$ eine Wohlordnung und es gilt $\forall i \in I : (T_i, \leq_i) \leq (T, \leq_T)$. Wir können also LVZ anwenden und erhalten ein maximales Element $(T^*, \leq^*)$. Angenommen $T^* \neq W$ und $w \in W \setminus T^*$. Dann ist

$$(T^*, \leq^*) < (T^* \cup \{w\}, \leq^* \cup (T^* \times \{w\}) \cup \{(w, w)\}) \in H,$$

was der Maximalität von $(T^*, \leq^*)$ widerspricht. □

*Beweis von WOS ⇒ AC.* Sei $\mathcal{M}$ eine Menge nichtleerer, paarweise disjunkter Mengen. Dann Gibt es nach WOS eine Wohlordnung $(W, \leq)$ auf $W := \bigcup \mathcal{M}$ und $\{\min(M) \mid M \in \mathcal{M}\}$ ist die gesuchte Auswahlmenge. □

### 11.3.4 Anwendungen des Auswahlaxioms

**Satz 11.3.4.1** (Idealsatz)**.** *Sei $R$ ein kommutativer Ring mit 1, $I \lhd R, I \neq R$. Dann gibt es ein maximales Ideal $M \lhd R$ (dh. $M \neq R$) mit $I \subseteq M$.*

*Beweis.* Sei $\mathcal{M} := \{J \mid I \subseteq J \lhd R, J \neq R\}$, $I \in \mathcal{M} \neq \emptyset$. $(\mathcal{M}, \subseteq)$ ist eine Halbordnung und erfüllt die Voraussetzungen von LVZ (11.3.2.4), da $\emptyset \neq K \subseteq \mathcal{M}$ Kette $\Rightarrow \bigcup K \in \mathcal{M}$, weil $I \subseteq \bigcup K \lhd R$ und $1 \notin \bigcup K$, also $\bigcup K \neq R$. Es gibt also ein maximales Ideal in $\mathcal{M}$. □

**Satz 11.3.4.2** (Ultrafiltersatz[9])**.** *Sei $B$ eine Boolesche Algebra und $F_0$ ein echter Filter auf $B$. Dann gibt es einen echten Ultrafilter $U$ mit $F_0 \subseteq U \subseteq B$.*

**UE 536 ► Übungsaufgabe 11.3.4.3.** Beweisen Sie den Ultrafiltersatz... **◄ UE 536**

(1) ... indem Sie den Idealsatz auf Boolesche Ringe anwenden.

(2) ... indem Sie das Lemma von Teichmüller-Tukey auf die Menge aller $F \subseteq B$ anwenden, die

$$\forall x_1, \ldots, x_n \in F \; \forall y \in B : x_1 \wedge \cdots \wedge x_n \wedge y \neq 0$$

erfüllen.

**UE 537 ► Übungsaufgabe 11.3.4.4.** Sei $B$ eine höchstens abzählbare Boolesche Algebra mit mehr als einem Element. ($B$ ist also entweder endlich oder es gibt eine Bijektion $f : \mathbb{N} \to B$.) Zeigen Sie (ohne Verwendung des Auswahlaxioms, des Zornschen Lemmas etc), dass es einen Ultrafilter auf $B$ gibt. **◄ UE 537**

**Satz 11.3.4.5** (Vektorraum-Basis)**.** *Sei $V$ ein Vektorraum und $B_0 \subseteq V$ eine linear unabhängige Menge. Dann gibt es eine Basis $B \supseteq B_0$. Insbesondere hat jeder Vektorraum eine Basis (setze $B_0 = \emptyset$).*

**UE 538 ► Übungsaufgabe 11.3.4.6.** Beweisen Sie Satz 11.3.4.5. Hinweis: Man überlege sich, dass linear unabhängig zu sein eine Eigenschaft mit endlichem Charakter ist und wende LTT (11.3.2.5) an. **◄ UE 538**

[9] Dieser Satz wird oft mit BPI abgekürzt: „Boolean prime ideal theorem."

**Anmerkung 11.3.4.7.** Eine interessante Konsequenz dieses Ergebnisses ist, dass es auf $\mathbb{R}$ unstetige, jedoch additive Abbildungen $f\colon \mathbb{R} \to \mathbb{R}$ gibt (also Abbildungen für die $\forall x, y \in \mathbb{R} : f(x+y) = f(x)+f(y)$ gilt). Solche Abbildungen kann man finden, indem man sich auf einer Basis von $\mathbb{R}$, aufgefasst als Vektorraum über $\mathbb{Q}$, eine Abbildung geeignet vorgibt und diese dann auf $\mathbb{R}$ zu einer $\mathbb{Q}$-lineare (also insbesondere: additiven) Abbildung fortsetzt.

**Satz 11.3.4.8** (Algebraischer Abschluss)**.** *Jeder Körper hat einen algebraischen Abschluss.*

*Beweis.* Sei $K$ Körper, $X$ eine überabzählbare Menge mit $|X| > |K|$. Jede algebraische Erweiterung $E : K$ erfüllt $|E| \leq |X| + \aleph_0$ (siehe 11.4).
Wir definieren auf der Menge

$$H := \{(E, +, 0, -, \cdot, 1) \mid K \leq E \subseteq X,\ E \text{ algebraisch über } K\}$$

eine Halbordnung durch die Definition

$$(E_1, +_1, \cdot_1) \leq (E_2, +_2, \cdot_2) :\Leftrightarrow E_1 \leq E_2 \text{ (Körpererweiterung)}.$$

$(H, \leq)$ erfüllt die Voraussetzungen von LVZ, also gibt es ein maximales Element $(M, +, \cdot)$, welches algebraisch abgeschlossen sein muss. □

**Satz 11.3.4.9** (Satz von Tychonoff)**.** *Sei $(X_i)_{i\in I}$ eine Familie kompakter topologischer Räume. Dann ist $\prod_{i\in I} X_i$ in der Produkttopologie kompakt.*

**Anmerkung 11.3.4.10.** Im Beweis wendet man den Ultrafiltersatz **??** auf $B = \mathfrak{P}(X)$ an und verwendet, dass $X$ genau dann kompakt ist, wenn jeder Ultrafilter auf $X$ konvergiert.

**Satz 11.3.4.11** (Satz von Hahn-Banach)**.** *Sei $X$ ein Banachraum, $Y \leq X$ ein Untervektorraum, und $f\colon Y \to \mathbb{R}$ ein beschränktes lineares Funktional. Dann gibt es ein lineares $\bar{f}\colon X \to \mathbb{R}$ mit $\bar{f}\restriction Y = f$ und $\|\bar{f}\| = \|f\|$.*

## 11.4 Ordinal- und Kardinalzahlen

### 11.4.1 Ordnungstypen

**Anmerkung 11.4.1.1.** In diesem Abschnitt wollen wir, um Missverständnisse zu vermeiden, strikt zwischen Elementen und Teilmengen des Definitionsbereichs von Funktionen unterscheiden. Wie wir sehen werden, spielen Ordinalzahlen oft eine Doppelrolle, sie treten in natürlicher Weise sowohl als Elemente als auch als Teilmengen anderer Ordinalzahlen auf.
Für eine gegebene Funktion $f\colon A \to B$ und eine Teilmenge $T \subseteq A$ schreiben wir deshalb für die Menge $\{f(t) \mid t \in T\}$ nicht wie sonst oft $f(T)$, sondern $f[T]$. Der Ausdruck $f(T)$ ist in diesem Abschnitt nur dann definiert, wenn $T$ ein *Element* des Definitionsbereichs von $f$ ist.

Aus jeder Isomorphieklasse von Wohlordnungen möchten wir einen kanonischen Vertreter als *Ordnungstyp* wählen. Wir wollen also eine Klasse $\mathbb{O}$ von *Ordinalzahlen* so definieren, dass es eine natürliche Zuordnung $\mathrm{otp} : (W, <) \mapsto \mathrm{otp}(W, <) \in \mathbb{O}$ gibt, und zwar solcherart, dass

$$(W_1, <_1) \cong (W_2, <_2) \;\Leftrightarrow\; \mathrm{otp}(W_1, <_1) = \mathrm{otp}(W_2, <_2).$$

Genauso möchten wir eine Klasse $\mathbb{K}$ von *Kardinalzahlen* und eine natürliche Zuordnung $|\cdot| : M \mapsto |M| \in \mathbb{K}$ definieren, sodass für jede Menge $M$ gilt

$$M_1 \approx M_2 \text{ (d.h. } \exists f\colon M_1 \to M_2 \text{ bijektiv)} \;\Leftrightarrow\; |M_1| = |M_2|.$$

Sei $(W, <)$ eine Wohlordnung. Mittels transfiniter Induktion (siehe 11.1.2.1, bzw. auch Rekursionssatz 11.2.1.2) zeigt man, dass es ein $M$ und genau eine Funktion $\rho\colon W \to M$ mit $\forall \alpha \in W : \rho_W(\alpha) = \rho_W[W_\alpha]$ gibt. Diese Funktion $\rho$ (oder auch $\rho_W$ oder $\rho_{(W,<)}$) heißt *Rangfunktion* für $(W, <)$. Dies benötigt das Ersetzungsaxiom, siehe 11.5.2.

**Beispiel 11.4.1.2.** Sei $(W, <) = (\mathbb{N}, <)$. Dann ist

$$\begin{aligned}
&\rho(0) = \rho[\{n \in \mathbb{N} : n < 0\}] = \rho[\emptyset] = \emptyset,\\
&\rho(1) = \rho[\{n \in \mathbb{N} : n < 1\}] = \rho[\{0\}] = \{\rho(0)\} = \{\emptyset\},\\
&\rho(2) = \{\emptyset, \{\emptyset\}\}, \text{usw.}
\end{aligned}$$

**Definition 11.4.1.3.** Die Menge $\rho_W[W] = \{\rho(\alpha) : \alpha \in W\}$ heißt *Ordnungstyp* von $(W, <)$, und wird mit $\mathrm{otp}(W)$ oder $\mathrm{otp}(W, <)$ bezeichnet.

**Lemma 11.4.1.4.** *Für jede Wohlordnung $(W, <)$ ist $\rho_W$ ein Isomorphismus zwischen $(W, <)$ und $(\mathrm{otp}, \in)$.*

**UE 539** ► **Übungsaufgabe 11.4.1.5.** Beweisen Sie Lemma 11.4.1.4. (Beweisen Sie insbesondere, dass $\rho$ injektiv ist.) ◄ **UE 539**

**Definition 11.4.1.6.** $\alpha$ heißt *Ordinalzahl*, symbolisch $\alpha \in \mathbb{O}$ (wobei $\mathbb{O}$ die Klasse der Ordinalzahlen bezeichnet), wenn es eine Wohlordnung $(W, <)$ mit $\alpha = \mathrm{otp}(W, <)$ gibt.

**Definition 11.4.1.7.** Eine Menge $X$ heißt *transitiv*, wenn aus $z \in y \in X$ immer $z \in X$ folgt. Mit anderen Worten: wenn für alle $y \in X$ auch $y \subseteq X$ gilt.

**UE 540** ► **Übungsaufgabe 11.4.1.8.** Zeigen Sie, dass jede Ordinalzahl eine transitive Menge ist. Zeigen Sie, dass jede Ordinalzahl durch die Relation $\in$ (irreflexiv) wohlgeordnet wird. ◄ **UE 540**

**Satz 11.4.1.9.** *Sei $\alpha$ eine Menge. Dann gilt:*

$$\alpha \text{ ist Ordinalzahl } \Leftrightarrow \alpha \text{ ist transitiv und durch } \in \text{ wohlgeordnet.}$$

**UE 541** ▶ **Übungsaufgabe 11.4.1.10.** Beweisen Sie 11.4.1.9. Hinweis: Zeigen Sie, dass $\rho_{(\alpha,\in)}$ die Identität ist. ◀ **UE 541**

**Folgerungen 11.4.1.11.** Seien $\alpha$, $\beta$ Ordinalzahlen.

(i) $\beta \in \alpha \Rightarrow \beta \subseteq \alpha$.

(ii) $\beta \subsetneq \alpha \Rightarrow \beta \in \alpha$.

(iii) Genau einer der drei Fälle $\alpha \in \beta$, $\beta \in \alpha$, $\alpha = \beta$ trifft zu.

**UE 542** ▶ **Übungsaufgabe 11.4.1.12.** Beweisen Sie 11.4.1.11. ◀ **UE 542**

**Lemma 11.4.1.13.** *Seien $(W_i, \leq_i)$ Wohlordnungen, $\alpha_i = \mathrm{otp}(W_i, \leq_i)$, $i \in \{1, 2\}$.*

1. *Wenn $\alpha_1 = \alpha_2$, dann ist $W_1 \cong W_2$.*
2. *Wenn $f\colon W_1 \cong W_2$ ein Isomorphismus ist, dann ist $\rho_{W_1} = \rho_{W_2} \circ f$, und es folgt $\alpha_1 = \alpha_2$.*

**UE 543** ▶ **Übungsaufgabe 11.4.1.14.** Beweisen Sie 11.4.1.13. ◀ **UE 543**

**Definition 11.4.1.15.** Bezeichnungen wie in 11.4.1.11.

$$\alpha_1 < \alpha_2 :\Leftrightarrow \alpha_1 \in \alpha_2$$

bzw. äquivalent dazu $\alpha_1 \subsetneq \alpha_2$ oder $(W_1, \leq_1) < (W_2, \leq_2)$

## 11.4.2 Eigenschaften von Ordinalzahlen

Sei $\alpha$ Ordinalzahl. Dann gilt:

(a) $\alpha = \{\beta \in \mathbb{O} \mid \beta < \alpha\}$ und $(\alpha, \leq)$ ist Wohlordnung mit $\mathrm{otp}(\alpha, \leq) = \alpha$.

(b) $\beta \in \alpha \Rightarrow \beta = \alpha_\beta \subseteq \alpha$

(c) $M \subseteq \mathbb{O}$ Menge $\Rightarrow (M, \leq)$ ist Wohlordnung und $\bigcup M \in \mathbb{O}$

(d) Es gibt eine Ordinalzahl $\alpha + 1 := \min\{\beta \in \mathbb{O} \mid \beta > \alpha\} = \alpha \cup \{\alpha\}$. Man nennt $\alpha + 1$ die *Nachfolgerordinalzahl* bzw. den *Nachfolger* von $\alpha$.

(e) $\alpha \neq 0$ heißt *Limes(ordinal)zahl*, wenn es kein $\beta \in \mathbb{O}$ gibt, mit $\alpha = \beta + 1$. Dies ist äquivalent zu $\alpha = \sup \alpha (= \bigcup \alpha)$ bzw. $\beta < \alpha \Rightarrow \beta + 1 \in \alpha$. Die kleinste Limesordinalzahl ist $\omega = \mathrm{otp}(\mathbb{N}, \leq)$.

### 11.4.3 Größenvergleich von Mengen

Ohne Verwendung von Ordinalzahlen und des Auswahlaxioms lässt sich für Mengen $A, B$ definieren:

**Definition 11.4.3.1.**

- $|A| = |B| :\Leftrightarrow \exists f\colon A \to B$ bijektiv
- $|A| \leq |B| :\Leftrightarrow \exists f\colon A \to B$ injektiv
- $|A| \leq^* |B| :\Leftrightarrow \exists f\colon B \to A$ surjektiv $\vee\ A = \emptyset$

Dies versteht sich als Sprech- bzw. Schreibweise, d.h. noch ohne $|A|$ als mathematisches Objekt definiert zu haben.

**UE 544** ▶ **Übungsaufgabe 11.4.3.2.**

- Beweisen Sie: Wenn $|A| \leq |B|$, dann $|A| \leq^* |B|$. (Verwendet Ihr Beweis das Auswahlaxiom?) ◀ **UE 544**
- Beweisen Sie: Wenn $|A| \leq^* |B|$, dann $|A| \leq |B|$. (Verwendet Ihr Beweis das Auswahlaxiom?)

**Satz 11.4.3.3** (Vergleichbarkeitssatz)**.** *Für beliebige Mengen $A$ und $B$ gilt*

$$|A| \leq |B| \ \vee\ |B| \leq |A|.$$

*D.h. es gibt entweder eine Injektion von $A$ nach $B$ oder von $B$ nach $A$.*

**UE 545** ▶ **Übungsaufgabe 11.4.3.4.** Beweisen Sie Satz 11.4.3.3. Hinweis: Dies benötigt AC. Man überlegt sich, dass injektive partielle Funktion zu sein eine Eigenschaft von endlichem Charakter ist und wendet LTT (11.3.2.5) an. ◀ **UE 545**

**Korollar 11.4.3.5.** Satz 11.4.3.3 ermöglicht uns den folgenden, alternativen Beweis von WOS (11.3.2.6). Für eine Menge $M$ sei $W$ eine wohlgeordnete Menge, sodass es keine Injektion von $W$ nach $M$ gibt (Satz von Hartogs, 11.3.1.1). Also gibt es eine Injektion von $M$ nach $W$, die auf $M$ eine Wohlordnung induziert.

**Satz 11.4.3.6** (Cantor-Schröder-Bernstein)**.** *Für beliebige Mengen $A$, $B$ gilt*

$$|A| \leq |B| \wedge |B| \leq |A| \Rightarrow |A| = |B|.$$

*D.h.: Gibt es eine Injektion von $A$ nach $B$ und eine Injektion von $B$ nach $A$, so gibt es eine Bijektion zwischen $A$ und $B$.*

*Beweis.* Dies benötigt nicht AC. Seien $f\colon A \to B$ und $g\colon B \to A$ Injektionen. Wir definieren $C_0 = A \setminus g[B]$, $C_{n+1} = g[f[C_n]]$ für $n \in \omega$ und $C = \bigcup_{n\in\omega} C_n$. Sei $h := f\restriction C \cup g^{-1}\restriction(A \setminus C)$, dh. für $a \in A$ ist

$$h(a) = \begin{cases} f(a) & \text{falls } a \in C \\ g^{-1}(a) & \text{falls } a \notin C \end{cases}$$

Die Funktion $h$ ist wohldefiniert, denn für $a \notin C$ gilt insbesondere $a \notin C_0$, dh. $a$ hat ein Urbild unter $g$. Zu zeigen bleibt die Bijektivität.

- Surjektivität: Sei $b \in B$. Falls $b \in f[C]$ so gilt offensichtlich $b \in h[C]$. Für $b \notin f[C]$ sei $a := g(b)$. Es gilt für alle $n$:
  - $a \notin C_0$ (nach Definition);
  - für alle $n$: $b \notin f[C] \supseteq f[C_n]$, daher $b \notin f[C_n]$; also $a = g(b) \notin g[f[C_n]] = C_{n+1}$.
  - Also $a \notin C$, daher $b = g^{-1}(a) \in h[A]$.
- Injektivität: $f$ und $g^{-1}$ sind für sich genommen jeweils injektiv. Sei also $f(c) = g^{-1}(a)$ mit $c \in C$ und $a \in A \setminus C$. Also gibt es ein $n \in \omega$ sodass $c \in C_n$. Also ist $g(f(c)) \in C_{n+1} \subseteq C$ aber $g(f(c)) = g(g^{-1}(a)) = a \notin C$. □

**Folgerungen 11.4.3.7.** Zusammenfassend gilt:

- $=, \leq, \leq^*$ sind reflexiv und transitiv
- $|A| \leq |B| \Leftrightarrow |A| \leq^* |B|$ (Der Beweis von „⇐“ braucht ebenfalls AC.)
- $|A| \leq |B| \vee |B| \leq |A|$ (11.4.3.3)
- $|A| \leq |B| \wedge |B| \leq |A| \Rightarrow |A| = |B|$ (11.4.3.6)

Somit sind Kardinalitäten „totalgeordnet“.

### 11.4.4 Kardinalzahlen

**Definition 11.4.4.1.** Laut Wohlordnungssatz gibt es auf jeder Menge $M$ eine binäre Relation $\leq$ (eine Teilmenge von $M \times M$), so dass $(W, \leq)$ eine Wohlordnung ist. Also

$$\emptyset \neq \{\mathrm{otp}(W, \leq) \mid (W, \leq) \text{ Wohlordnung}\} =: O(W) \subseteq \mathbb{O}$$

und damit gibt es $\min O(W) =: |W| = \kappa(W)$. Dieses Minimum nennen wir die *Kardinalität* von W.
Alle $\kappa \in \mathbb{O}$, die als Kardinalitäten (d.h. minimale Ordinalzahlen gegebener Kardinalität) auftreten, heißen *Kardinalzahlen*.

Die Klasse $\mathbb{K}$ aller Kardinalzahlen ist als Teilklasse von $\mathbb{O}$ wohlgeordnet. Es gibt sogar eine kanonische Zuordnung (nicht Funktion) der Ordinalzahlen zu den unendlichen Kardinalzahlen $\alpha \mapsto \aleph_\alpha$, wobei[10] $\aleph_0$ die kleinste unendliche Kardinalzahl, $\aleph_{\alpha+1}$ die kleinste Kardinalzahl größer als $\aleph_\alpha$ und für eine Limeszahl $\lambda$ ist $\aleph_\lambda$ die kleinste Kardinalzahl die größer als alle $\aleph_\beta : \beta < \lambda$ ist.

**Beispiel 11.4.4.2.** $\mathrm{otp}(\mathbb{N}, \leq) = \omega =: \aleph_0 = |\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}|$ ist eine Kardinalzahl.
$2^{\aleph_0} = |2^\omega| = |\mathbb{R}| = |\mathbb{C}| =: \mathfrak{c}$ heißt *Kontinuum.*

**Anmerkung 11.4.4.3.** Die *Kontinuumshypothese* CH besagt, dass jede überabzählbare Teilmenge der reellen Zahlen gleichmächtig zu den reellen Zahlen ist. Unter AC ist das äquivalent dazu, dass die Kardinalität der reellen Zahlen die kleinste überabzählbare Kardinalität ist, also $\mathfrak{c} = \aleph_1$. Die Kontinuumshypothese ist in ZFC weder beweisbar noch widerlegbar.

### 11.4.5 Operationen für Ordinalzahlen

Summe und Produkt von Wohlordnungen $(W_1, \leq_1), (W_2, \leq_2)$ definiert man wie folgt:

**Definition 11.4.5.1.**

- $\underbrace{(W_1, \leq_1) + (W_2, \leq_2)}_{\text{Summe}} := (W_1 \uplus W_2, \leq)$ für $W_1 \cap W_2 = \emptyset$ mit
  $\alpha \leq \beta :\Leftrightarrow (\alpha \in W_1 \wedge \beta \in W_2) \vee (\exists i \in \{1,2\} : \alpha, \beta \in W_i \wedge \alpha \leq_i \beta)$
- $\underbrace{(W_1, \leq_1) \cdot (W_2, \leq_2)}_{\text{(lexikographisches) Produkt}} := (W_1 \times W_2, \leq)$ mit
  $(\alpha_1, \alpha_2) \leq (\beta_1, \beta_2) :\Leftrightarrow \alpha_2 < \beta_2 \vee (\alpha_2 = \beta_2 \wedge \alpha_1 \leq \beta_1)$

**Folgerung 11.4.5.2.** *Man überlegt sich leicht, dass aus* $(W_i, \leq_i) \cong (W_i', \leq_i')$ *(für* $i = 1, 2$*) die Beziehung* $(W_1, \leq_1) + (W_2, \leq_2) \cong (W_1', \leq_1') + (W_2', \leq_2')$ *folgt.*
*Also wird durch* $\mathrm{otp}(W_1, \leq_1) + \mathrm{opt}(W_2, \leq_2) := \mathrm{otp}((W_1, \leq_1) + (W_2, \leq_2))$ *(und analog für* $\cdot$*) auf* $\mathbb{O}$ *eine Operation wohldefiniert: die Ordinalzahl-Addition bzw. -Multiplikation. Achtung: Diese Operationen sind nicht kommutativ! z.B.* $\omega + \omega = \omega \cdot 2 \neq 2 \cdot \omega = \omega$

### 11.4.6 Operationen auf Kardinalzahlen

**Definition 11.4.6.1.** Seien $X, Y$ Mengen. Mit $Y^X$ (manchmal auch als ${}^X Y$ geschrieben) bezeichnet man die Menge aller Funktionen von $X$ nach $Y$.

**Beispiele 11.4.6.2.**

(a) Wenn $X = \{a\}$ einelementig ist, dann gibt es eine natürliche Bijektion zwischen $Y^X$ und $Y$, nämlich die Abbildung, die jeder Funktion $f \in Y^X$ ihren einzigen Wert $f(a)$ zuordnet.

[10] $\aleph$ (Aleph) ist der erste Buchstabe des hebräischen Alphabets.

(b) Wenn $X = \{a, b\}$ zwei Elemente hat, bieten sich zwei bijektive Abbildungen von $Y^X$ nach $Y \times Y$ an; die eine bildet $f$ auf das Paar $(f(a), f(b))$ ab.

(c) Wenn $X$ die leere Menge ist, dann gibt es genau eine Funktion $f\colon X \to Y$, nämlich $f = \emptyset$. (Als Funktion betrachtet, nennt man die leere Menge auch gelegentlich 0-Tupel.) In diesem Sinne gilt also $Y^\emptyset = \{\emptyset\}$ für alle Mengen $Y$, insbesondere auch für die leere Menge: $\emptyset^\emptyset = \{\emptyset\}$.

**Lemma 11.4.6.3.** *Für Mengen $A_i, B_i$, $i \in \{1, 2\}$ gilt*

$$|A_1| = |A_2|, |B_1| = |B_2| \Rightarrow \begin{cases} |A_1 \cup B_1| = |A_2 \cup B_2| & \text{sofern } A_1 \cap B_1 = \emptyset = A_2 \cap B_2 \\ |A_1 \times B_1| = |A_2 \times B_2| \\ |A_1^{B_1}| = |A_2^{B_2}| \end{cases}$$

Daher werden durch

**Definition 11.4.6.4.**

- $|A| + |B| := |A \cup B|$ (sofern $A \cap B = \emptyset$)
- $|A| \cdot |B| := |A \times B|$
- $|A|^{|B|} := |A^B|$

Operationen auf $\mathbb{K}$ wohldefiniert: Kardinalzahl-Addition, -Multiplikation und -Exponentation. Für endliche Mengen $A$, $B$ stimmen diese Funktionen mit den üblichen Operationen der Addition, Multiplikation und Exponentiation[11] überein.
Achtung: $\aleph_0 +_\mathbb{K} 1 = \aleph_0$ aber $\omega +_\mathbb{O} 1 \neq \omega$ (obwohl $\omega = \aleph_0$).

### 11.4.7 Von Neumanns Modell von $\mathbb{N}$

**Definition 11.4.7.1.** Eine Menge M heißt *induktiv*, wenn

- $\emptyset \in M$
- $\forall \alpha \in M : \alpha + 1 \in M$

wobei $\alpha + 1 := S(\alpha) := \alpha \cup \{\alpha\}$

**Definition 11.4.7.2.** $\mathbb{N} := \bigcap \underbrace{\{M \mid M \text{ ist induktiv}\}}_{\neq \emptyset \text{ laut Unendlichkeitsaxiom}}$

Also $0 := \emptyset, 1 = 0 + 1 = 0 \cup \{0\} = \{\emptyset\}, \ldots, n = \{0, 1, 2, \ldots, n-1\}$

[11] In der Analysis wird „$0^0$“ gelegentlich rein symbolisch als „unbestimmte Form“ verwendet; dies ist als Hinweis darauf zu verstehen, dass man einen Grenzwert zu betrachten hat. In der diskreten Mathematik erweist es sich als sinnvoll und praktisch, immer $0^0 := 1$ zu definieren. Siehe dazu auch Beispiel 11.4.6.2(c).

**UE 546 ► Übungsaufgabe 11.4.7.3.** Welche dieser Aussagen sind wahr? **◄ UE 546**

- $\mathbb{N} \subseteq \mathbb{O}$,
- $\mathbb{N} \in \mathbb{O}$,
- $\mathbb{N} = \mathbb{O}$.

**Folgerungen 11.4.7.4.**

- Mengen $M$ mit $|M| \in \mathbb{N}$ bzw. $|M| \notin \mathbb{N}$ heißen endlich bzw. unendlich.
- Auf $\mathbb{N}$ stimmen $+$ sowie $\cdot$ aus 11.4.5.2 und 11.4.6.4 überein.
- $\mathbb{N}$ ist abgeschlossen bezüglich $+$ und $\cdot$
- Wenn wir die Nachfolgeroperation $x \mapsto x+1$ mit $S$ bezeichnen, dann ist $(\mathbb{N}, 0, S, +, \cdot)$ eine Algebra vom Typ $(0, 1, 2, 2)$ (vergleiche Definition **??**) mit injektivem, aber nicht surjektivem $S$ (da $0 \notin \mathrm{Im}S$). $(\mathbb{N}, 0, S)$ enthält keine echte Unteralgebra.
  $\alpha + 0 = \alpha$, $\alpha + S(\beta) = S(\alpha + \beta)$
  $\alpha \cdot 0 = 0$, $\alpha \cdot S(\beta) = (\alpha \cdot \beta) + \alpha$

  Dieser Punkt entspricht den Peano-Axiomen. Damit gelten auch alle Folgerungen aus den Peano-Axiomen. Ein Vorteil der Deutung als Kardinalitäten ist, dass sie Anwendung auf die Kombinatorik rechtfertigt.

**UE 547 ► Übungsaufgabe 11.4.7.5.** Beweisen Sie, dass die von Neumannschen natürlichen Zahlen die Peano-Axiome erfüllen. (Achtung: Im Beweis ist kein „usw“ zulässig, sondern immer nur: „Wir zeigen, dass die folgende Menge induktiv ist“. **◄ UE 547**

### 11.4.8 Unendliche Kardinalzahlarithmetik

**Lemma 11.4.8.1.** *Die folgenden Rechengesetze gelten für alle endlichen und unendlichen Kardinalzahlen $\kappa$, $\lambda$:*

*(a)* $\kappa^{\lambda \cdot \mu} = (\kappa^{\lambda})^{\mu}$

*(b)* $(\kappa \cdot \lambda)^{\mu} = \kappa^{\mu} \cdot \lambda^{\mu}$

*(c)* $\kappa^{\lambda + \mu} = \kappa^{\lambda} \cdot \kappa^{\mu}$

*(d)* $\kappa < |\mathfrak{P}(\kappa)| = |2^{\kappa}| = 2^{\kappa}$

**UE 548 ► Übungsaufgabe 11.4.8.2.** Beweisen Sie 11.4.8.1 (a)-(c). Hinweis: Finden Sie kanonische Bijektionen. Das Auswahlaxiom muss hier nicht verwendet werden. **◄ UE 548**

**UE 549** ▶ **Übungsaufgabe 11.4.8.3.** Beweisen Sie 11.4.8.1 (d). ◀ **UE 549**

**Lemma 11.4.8.4.** *Sei $A$ eine unendliche Menge. Dann gibt es eine abzählbare Teilmenge $T \subseteq A$.*

**UE 550** ▶ **Übungsaufgabe 11.4.8.5.** Beweisen Sie Lemma 11.4.8.4. Anleitung: Dies benötigt AC. Wenden Sie den Vergleichbarkeitssatz auf $A$ und $\mathbb{N}$ an. (Fallunterscheidung!) ◀ **UE 550**

**Satz 11.4.8.6.** *Sei $A$ eine unendliche Menge, und sei $B$ ein nicht leere Menge mit $|B| \leq |A|$. Dann gilt:*

(1) $A \cup \{a\} \approx A$ *für alle $a$.*
(2) $A \cup E \approx A$ *für alle endlichen Mengen $E$.*
(3) $A \times \{0,1\} \approx A$.
(4) $A \cup B \approx A$.
(5) $A \times A \approx A$
(6) $A \times B \approx A$.
(7) $A^n \approx A$ *für $n > 0$.*

*In der Sprache der Kardinalzahlen lassen sich die obigen Aussagen so formulieren:*

(1) $\kappa + 1 = \kappa$ *für alle unendlichen $\kappa$.*
(2) $\kappa +$ *endlich* $= \kappa$ *für alle unendlichen $\kappa$.*
(3) $\kappa \cdot 2 = \kappa$ *oder* $\kappa + \kappa = \kappa$ *für alle unendlichen $\kappa$.*
(4) $\kappa + \lambda = \kappa$, *wenn $\kappa$ unendlich ist und $\kappa \geq \lambda$ gilt. Äquivalent: Für alle Kardinalzahlen $\kappa, \lambda$, von denen mindestens eine unendlich ist, gilt $\kappa + \lambda = \max(\kappa, \lambda)$.*
(5) $\kappa \cdot \kappa = \kappa$ *für alle unendlichen Kardinalzahlen $\kappa$.*
(6) $\kappa \cdot \lambda = \kappa$, *wenn unendlich ist und $\kappa \geq \lambda > 0$ gilt. Äquivalent: Für alle Kardinalzahlen $\kappa, \lambda > 0$, von denen mindestens eine unendlich ist, gilt $\kappa \cdot \lambda = \max(\kappa, \lambda)$.*
(7) $\kappa^n = \kappa$ *für alle positiven natürlichen Zahlen $n$.*

*Beweis von Satz 11.4.8.6.* 1. OBdA sei $a \notin A$. Laut Lemma 11.4.8.4 gibt es eine Bijektion $f\colon \mathbb{N} \to T \subseteq A$. Dann ist die Abbildung $g\colon A \to A$, die durch

$$g(f(n)) := f(n+1) \quad \text{und} \quad \forall x \in A \setminus T : g(x) = x$$

definiert ist, eine Bijektion zwischen $A$ und $A \setminus \{f(0)\}$; sie lässt sich zu einer Bijektion zwischen $A \cup \{a\}$ und $A$ fortsetzen.

2. Folgt aus (1) mit Induktion.

3. Wir definieren eine Halbordnung $\mathcal{F}$, deren Elemente gewisse Bijektionen sind:

$$\mathcal{F} := \{\, f \mid (\exists X \subseteq A)\ f\colon X \times \{0,1\} \to X \text{ ist Bijektion} \,\}.$$

Die Menge $\mathcal{F}$ wird durch die Relation $\subseteq$ partiell geordnet. (D.h. $f \leq g$ wenn $f$ von $g$ fortgesetzt wird). Die Halbordnung $\mathcal{F}$ enthält die Bijektion zwischen $\emptyset$ und $\emptyset \times \{0,1\}$, ist also nicht leer. Wir wenden das Lemma von Zorn an und erhalten eine maximale Bijektion $g\colon C \times \{0,1\} \to C$.

Es gilt also $C \times \{0,1\} \approx C$; wenn wir $A \approx C$ zeigen können, erhalten wir leicht $A \times \{0,1\} \approx A$.

Wir unterscheiden zwei Fälle:

**1.Fall** $A \setminus C$ ist unendlich. Dann enthält $A \setminus C$ eine abzählbare Teilmenge $D \subseteq A \setminus C$ und daher gibt es[12] eine Bijektion $h\colon D \times \{0,1\} \to D$. Dann ist $g \cup h\colon (C \cup D) \times \{0,1\} \to C \cup D$ eine Bijektion, was der Maximalität von $g$ widerspricht.

**2.Fall** $A \setminus C$ ist endlich. Wie wir in Punkt (2) bewiesen haben, gilt $|A| = |C| +$ endlich $= |C|$.

4. Es gilt $|A| \leq |A \cup B| \leq |A \times \{0,1\}| = |A|$; die zweite Ungleichung lässt sich durch injektive Abbildungen von $A$ nach $A \times \{0\}$ und von $B$ nach $A \times \{1\}$ belegen. Daher $|A| = |A \cup B|$ wegen Satz 11.4.3.6.

5. Wir gehen ähnlich wie bei $\kappa + \kappa = \kappa$ vor und definieren

$$\mathcal{F} := \{\, f \mid (\exists X \subseteq A)\ f\colon X \times X \to X \text{ ist Bijektion} \,\}.$$

Wir ordnen $\mathcal{F}$ durch Inklusion (=Fortsetzung), benutzen das Lemma von Zorn (11.3.2.4) und erhalten ein maximales $g\colon B \times B \to B$, wobei $|B| = |B \times B|$ nach Definition.

Wir unterscheiden zwei Fälle:

**1.Fall** Angenommen $|A \setminus B| > |B|$. Dann gibt es eine Teilmenge $C \subseteq A \setminus B$ mit $|C| = |B|$. Nun sind die Mengen

$$B \times B, B \times C, C \times B, C \times C$$

alle gleichmächtig mit $B$ bzw. $C$; nach zweimaliger Anwendung von (3) sehen wir, dass es eine Bijektion

$$h\colon (B \times C) \cup (C \times B) \cup (C \times C) \to C$$

geben muss. Nun ist aber $g \cup h$ eine Bijektion zwischen $B \cup C$ und $(B \cup C) \times (B \cup C)$, was der Maximalität von $g$ widerspricht.

**2.Fall** $|A \setminus B| \leq B$. Wir erhalten $|A| = |B \cup (A \setminus B| = |B| + |A \setminus B| = |B|$, wie wir in Punkt (4) gezeigt haben. Wegen $B \approx B \times B$ ergibt sich $A \approx A \times A$.

6. Wie oben mit Satz 11.4.3.6.

7. Mit Induktion. □

[12] wegen $\mathbb{N} \times \{0,1\} \approx \mathbb{N}$, bezeugt etwa durch die Bijektion $(n,i) \mapsto 2n + i$

**Folgerung 11.4.8.7.** (1) *Für alle unendlichen Kardinalzahlen $\kappa$ und alle natürlichen Zahlen $n > 0$ gilt $\kappa^n = \kappa$.*

(2) *Für alle unendlichen Mengen $A$ ist $A$ gleichmächtig mit der Menge $A^{<\omega} := A \cup A^2 \cup A^3 \cup \cdots$, denn die Mächtigkeit der Menge $A^{<\omega}$ ist durch $|A| \cdot \aleph_0 = |A|$ beschränkt.*

(3) *Sei $\kappa$ eine unendliche Kardinalzahl, und sei $(B_i : i \in I)$ eine Familie von Mengen für die $\forall i : |B_i| \leq \kappa$ und auch $|I| \leq \kappa$ gilt. Dann gilt auch $|\bigcup_{i\in I} B_i| \leq \kappa$.*
*(Denn sogar die Kardinalität der disjunkten Vereinigung $\bigcup_{i\in I} B_i \times \{i\}$ ist durch $|I| \times |I| = |I|$ beschränkt, und es gilt offensichtlich $|\bigcup_{i\in I} B_i| \leq^* |\bigcup_{i\in I} B_i \times \{i\}|$. Siehe Definition 11.4.3.1 und Aufgabe 11.4.3.2.)*

(4) *Insbesondere gilt: Wenn alle Mengen $B_i$ endlich sind, dann ist $|\bigcup_{i\in I} B_i| \leq |I|$.*

(5) *Sei $\mathfrak{A}$ eine Algebra endlichen oder abzählbar unendlichen Typs. (D.h., es gibt endlich oder abzählbar unendlich viele Operationen.)*
*Dann gibt es höchstens abzählbar viele Terme.*

(6) *Wenn $R$ ein unendlicher Ring ist, dann hat der Polynomring $R[x]$ die gleiche Kardinalität wie $R$.*
*(Allgemeiner: Wenn $\mathfrak{A}$ eine unendliche Algebra endlichen oder abzählbaren Typs ist, dann hat $A$ die gleiche Kardinalität wie die Polynomalgebra über $A$.)*

**Anmerkung 11.4.8.8.** Die obige Folgerung lässt sich nicht auf unendliche Exponenten verallgemeinern. Es gibt zwar (viele) unendliche Kardinalzahlen $\kappa$, die $\kappa^{\aleph_0} = \kappa$ erfüllen, es gibt aber auch (viele) unendliche Kardinalzahlen $\lambda$, die $\lambda^{\aleph_0} > \lambda$ erfüllen.

**Lemma 11.4.8.9.** *Für Kardinalzahlen $\kappa \in \mathbb{K} \setminus \mathbb{N}$ gilt:*

*(a)* $\kappa^\kappa \overset{(d)}{\leq} (2^\kappa)^\kappa \overset{11.4.8.1(a)}{=} 2^{\kappa\times\kappa} \overset{11.4.8.6}{=} 2^\kappa \leq \kappa^\kappa$, *also* $2^\kappa = \kappa^\kappa$.

*(b)* $|2^{\mathbb{N}}| = |\mathbb{R}|, |\mathbb{R}^{\mathbb{N}}| = |\mathbb{R}|$

## 11.5 Axiomatische Mengenlehre

### 11.5.1 Vorbemerkungen

Wozu braucht man Axiome? Es gibt unter den meisten Mathematikern[13] Einigkeit darüber, was ein gültiger Beweis ist. Wenn man also einen Beweis gefunden hat, kann man im Prinzip jede andere Mathematikerin[14] von dessen Gültigkeit überzeugen. Um aber

- Beweise selbst zum Objekt mathematischer Untersuchungen zu machen,
- insbesondere: um die Nichtexistenz gewisser Beweise zu beweisen,
- sowie: um Überlegungen wie „Ist Satz S auch ohne die Annahme A beweisbar?“ durchzuführen,

[13] Die Fußnote auf der Seite 121 ist hier sinnvoll zu modifizieren
[14] Nochmals.

- weiters: um wirkliche oder scheinbare Paradoxa (wie etwa das Russell-Paradoxon) zu analysieren/erklären/verstehen/aufzulösen

hat die mathematische Logik den Begriff des formalen Beweises entwickelt. Zunächst legt man in einem Beweissystem fest, welche (einfachen) logischen Wahrheiten, wie etwa $x = y \Rightarrow y = x$, $\forall x(x < 0) \to (7 < 0)$, $\varphi \Rightarrow \varphi$, etc) man als „logische Axiome“ akzeptiert, sowie welche einfachen Schlußformen, wie etwa

- „Modus ponens“: Aus $\varphi \Rightarrow \psi$ und $\varphi$ kann man $\psi$ schließen
- „Einführung von $\vee$“: Aus $(\varphi_1 \Rightarrow \psi)$ und $(\varphi_2 \Rightarrow \psi)$ kann man auf $(\varphi_1 \vee \varphi_2 \ \Rightarrow \ \psi)$ schließen

zulässig sind. Sodann wählt man „nichtlogische[15] Axiome“, die Information über die betrachteten Objekte enthalten, wie zum Beispiel „zu je zwei verschiedenen Punkten gibt es genau eine Gerade, die diese beiden Punkte enthält“ in der Geometrie, oder „Für alle Mengen $x, y$ gibt es eine Menge $P$ die sowohl $x$ als auch $y$ als Element enthält“.
Ein formaler Beweis besteht nun aus endlich[16] vielen Schritten; in jedem Schritt gibt man entweder ein logisches oder nichtlogisches Axiom an, oder man schließt aus früheren Schritten mit Hilfe der erlaubten Schlußformen auf einen neuen Satz.
Ob die so beschriebenen formalen Beweise eine adäquate Interpretation des informellen Begriffs „mathematischer Beweis“ sind, hängt natürlich davon ab, welche logischen Wahrheiten und Schlußformen man zulässt; für das von den meisten Mathematikern[17] betrachtete System der *klassischen Logik*, genauer: der klassischen Prädikatenlogik erster Stufe, gibt es Dutzende von Beweissystemen, die allerdings übereinstimmen, was die beweisbaren Sätze betrifft. Der Gödelsche Vollständigkeitssatz zeigt, dass diese Systeme tatsächlich alle allgemeingültigen Sätze der Prädikatenlogik erster Stufe beweisen.
Ob die so beschriebenen formalen Beweise auch wirklich nur Sätze beweisen, die „wahr“ sind, hängt davon ab, ob die nichtlogischen Axiome so gewählt sind, dass sie tatsächlich „wahr“ sind. (Eine zweite Frage ist, ob umgekehrt alle „wahren“ Sätze beweisbar sind; dies hängt davon ab, ob das gewählte System der nichtlogischen Axiome mächtig genug ist. Der Gödelsche Unvollständigkeitssatz verneint diese Frage in vielen Fällen.)

### 11.5.2 Die Axiome von ZFC

Als Beispiel eines sehr erfolgreichen Systems nichtlogischer Axiome geben wir ohne nähere Erklärung die ZFC-Axiome (Axiome von Zermelo und Fraenkel, mit Auswahlaxiom AC) an. Alle Sätze dieses Skriptums, sowie die meisten Sätze, denen Sie im Mathematikstudium begegnen werden, lassen sich in klassischer Prädikatenlogik mit Hilfe dieser ZFC-Axiome beweisen. (Dies gilt allerdings nur im Prinzip; so lässt sich etwa ein

[15] Beachten Sie den Unterschied zwischen den Begriffen „nichtlogisch“ und „unlogisch“. Die nichtlogischen Axiome wurden früher auch „Eigenaxiome“ genannt.
[16] In der Mathematischen Logik beschäftigt man sich auch mit Logiken, in denen infinitäre Formeln und/oder infinitäre Beweise zugelassen sind; in der Prädikatenlogik erster Stufe, die wir hier betrachten, bestehen aber Formeln aus endlich vielen Zeichen, und Beweise aus endlich vielen Formeln.
[17] Schon wieder.

Satz über die natürlichen Zahlen $0, 1, 2, \ldots$ zwar prinzipiell als Satz über die Mengen $\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \ldots$ interpretieren und auch beweisen, allerdings mit unverhältnismäßig großem Aufwand.)
Die folgenden Axiome sind informell formuliert. Für eine korrekte Formulierung müsste man noch einige Definition hinzufügen, die die verwendeten Begriffe (wie „Auswahlmenge“ oder „Funktion“) deutlicher in der Sprache der Mengenlehre erklären; statt der Existenz einer unendlichen Menge könnte man die Existenz einer induktiven Menge (siehe Definition 1.1.1.4) fordern. Die Begriffe „Menge“ und „Element“ bedürfen hingegen keiner weiteren Formalisierung; sie werden implizit durch die Axiome beschrieben.

1. *Extensionalitätsaxiom.* Wenn $X$ und $Y$ die selben Elemente haben, dann $X = Y$.

2. *Paarmengenaxiom.* Für alle Mengen $a$ und $b$ gibt es eine Menge $\{a, b\}$, die genau $a$ und $b$ enthält.

3. *Aussonderungsaxiom (Schema).* Wenn $P$ eine Eigenschaft (mit Parameter $p$) ist, dann gibt es für jedes $X$ und jedes $p$ eine Menge $Y = \{u \in X : P(u, p)\}$, die genau jene $u \in X$ enthält, die Eigenschaft $P$ haben.

4. *Vereinigungsmengenaxiom.* Für jedes $X$ gibt es eine Menge $Y = \bigcup X$, die Vereinigung aller Elemente aus $X$.

5. *Potenzmengenaxiom.* Für jedes $X$ gibt es eine Menge $Y = \mathfrak{P}(X)$, die Menge aller Teilmengen von $X$.

6. *Unendlichkeitsaxiom.* Es gibt eine unendliche Menge.

7. *Ersetzungsaxiom (Schema).* Wenn eine Klasse $F$ eine Funktion ist, dann gibt es für jede Menge $X$ eine Menge $Y = F[X] = \{F(x) : x \in X\}$.

8. *Regularitätsaxiom.* Jede nichtleere Menge hat ein $\in$-minimales Element.

9. *Auswahlaxiom.* Jede Familie nichtleerer Mengen hat eine Auswahlmenge.

# Index


≈ (\approx), 72
↾ (\upharpoonright), 8, A6
⊥ (\perp), 234

Abbildung, 41
Abelisierung, 151
abgeleitete Gruppe, 151
abgeleitete Untergruppen, 431
abgeschlossen bzgl. einer Operation, 97
abgeschlossen bzgl. einer Operationenfamilie, 97
Ableitung einer Gruppe, 431
Abschluss
  ganzer, 516
  normaler, 465
absolut freie Algebra, 250
Absolutbetrag, 28
absolute Galoisgruppe, 478
absorbierendes Element, 52
abzählbar erzeugt, 105
ACC, 47, 507
Adjunktion einer Nullstelle, 336
Aktion, 413, 414
algebraisch, 219, 322
  abhängig, 327
  unabhängig, 327
algebraisch abgeschlossen, 30, 336
algebraisch vom Grad $n$, 322
algebraische Geometrie, 522
algebraische Hülle, 328
algebraische Körpererweiterung, 325
algebraische Zahl, 341
algebraischer Abschluss, 336
algebraisches Erzeugendensystem, 328
algebraisches Körperelement, 322
allgemeine Algebra, 39, 51
allgemeine lineare Gruppe, 171
Allrelation, 113
alternierende Gruppe, 168, 422
Anfangsabschnitt, A2
angeordneter Körper, 58, 212
angeordneter Körper, 24, 214
angeordneter Ring, 212
Antikette, 46
antireflexiv (auch areflexiv oder irreflexiv), 42
antisymmetrisch, 42
antiton, 63, 454
≈ (\approx), 72
äquivalent (Zerfällungskörper), 339
äquivalente Körpererweiterung, 337
äquivalente lineare Abbildungen, 36
Äquivalenzklasse, 19, 43
Äquivalenzrelation, 43
archimedisch angeordnet, 212, 215
Artinsche Halbordnung, 47, 508
assoziativ, 51
Assoziativgesetz, 51, 83
assoziiert, 279
At, 238
Atom, 238
Atomformeln, 74
äußere Automorphismengruppe, 167
auflösbar, 151
  durch Radikale, 493
auflösbare
  Gruppe, 431
  Subnormalreihe, 432
aufsteigende Zentralreihe, 429
ausgezeichnetes Element, 51

Aussage, 75
äußere direkte Summe, 175
äußeres direktes Produkt, 154
äußeres semidirektes Produkt, 437
Auswahl
  axiom, A8
  funktion, A8
  menge, A8
Automorphismengruppe, 63
Automorphismengruppe einer Partition, 441
Automorphismus, 62
axiomatische Theorie, 76
Axiomensystem, 76

Basis, 32
  eines Vektorraums, 32, 377
Basisgruppe, 441
Baum, 69
Baumdiagramm, 69
bedingt vollständig, 58, 215, 225
Berechenbarkeitstheorie, 73
beschränkte Halbordnung, 46, 58
beschränkter Verband, 55
Beweistheorie, 73
Bidual, 373
bidualer Modul, 409
bijektiv, 41
Bild, 41
bilineare Abbildung, 410
Bimodul, 408
binäre Relation, 40
binäre Operation, 51
Binomialkoeffizienten, 193
binomische Formel, 193
binomischer Lehrsatz, 193
Boolesche Algebra, 55, 233
Boolescher Ring, 235
Boolescher Verband, 55
Bruch, 299
Bruchring, 195
Buchberger-Agorithmus, 511

$\mathbb{C}$, 28
Cardanosche Formel, 487
Cauchyfolge, 25
Cauchyprodukt, 200
CH, A17
Charakter
  endlicher, A7
Charakteristik, 192
charakteristischen Funktion, 245
Chinesischer Restsatz, 206
clopen, 262

Darstellungssatz von Cayley, 67
Darstellungssatz von Cayley für Monoide, 130
Darstellungssatz von Cayley für Gruppen, 165
Darstellungssatz von Stone, 245
Darstellungstheorie, 172
DCC, 47, 508
Dedekind-MacNeille-Vervollständigung, 214
Dedekindscher Ring, 517
Diedergruppe, 422, 423
Differenzengruppe, 139
Differenzenmonoid, 139
Dimension, 35
  eines freien Moduls, 379
dimensionsinvariant, 379
direkt unzerlegbare Gruppe, 443
direkt zerlegbare Gruppe, 443
direkter Limes, 375
direktes Produkt, 19
direktes Produkt von Algebren, 107
disjunkt, 43, 234
Diskriminante, 483, 484
distributiv, 51
distributiver Verband, 55, 61
Distributivgesetz, 51
Division mit Rest, 294
Divisionsalgebra, 411
Divisionsring, 54
dizyklische Gruppe, 425
duale Basis, 410
duale Relation, 42
dualer Filter, 238

dualer Verband, duale Aussage, 221
Dualitätsprinzip
für halbgeordnete Mengen, 46
für Boolesche Algebren, 234
für Verbände, 221

echter Teiler, 281
echtes Ideal, 190
eckige Klammer $[a, b]$, 223
eindeutige Zerlegbarkeit in irreduzible Elemente, 286
eindeutige Zerlegbarkeit in Primelemente, 286
eindeutiger Lesbarkeit, 69
einfache Algebra, 113
einfache Körpererweiterung, 319
eingebettetes Primideal, 513
Einheit, 126
Einheiten, 279
Einheitengruppe, 126, 279
Einheitswurzel, 344
Einschränkung, 41
einer Funktion, 8
$\restriction$ (`\upharpoonright`), 8, A6
Einselement, 51
Einsetzungshomomorphismus, 71, 205, 272, 322
Eisensteinsches Kriterium, 304
elementare Formeln, 74
elementarsymmetrische Polynome, 308
Elementarteiler, 398, 399
endlich erzeugt, 105
endlichdimensionale Erweiterung, 321
endliche Menge, 3
endlicher Körper, 349
Endomorphismenmonoid, 63
Endomorphismus, 62
Epimorphismus, 62
Erlanger Programm, 171
Erweiterung, 437
abelsche, 500
Galoissche, 460
inseparable, 463
normale, 463
radikale, 493
rein transzendente, 327
separable, 463
zyklische, 500
zyklotomische, 501
Erweiterungskörper, 319
Erweiterungskörper, 102, 318
Erzeugendensystem, 32, 100
erzeugendes Element, 144, 158, 243
erzeugte Unteralgebra, 100
von unten, von oben, 102
erzeugtes Ideal, 188
euklidische Bewertung, 294
Euklidischer Algorithmus, 295
euklidischer Ring, 285, 294
Eulersche $\varphi$-Funktion, 345
Eulersche $\varphi$-Funktion, 164
Eulersche $\varphi$-Funktion, 501
exakt, 381
Exponent, 172
extensiv, 454

Fünferlemma, 383
kurzes, 384
Faktoralgebra, 112
triviale, 113
faktorielle, 193
faktorieller Ring, 285, 287
Faktorisierung, 286
Fakultät, 193
Faltung, 274
Fastring, 209
Fehlstand, 168
Filter, 224
Fittings Lemma, 446
Fixpunktkörper, 460
Fixpunktrelation, 460
Folge, 10
Folgerung, 76
formale Ableitung, 342
formale Laurentreihe, 202
formale Laurentreihen, 368
formale Potenzreihe, 200
formale Sprache, 74

Formeln
elementare, 74
geschlossene, 75
frei
über $B$ in $\mathcal{K}$, 250
in $\mathcal{K}$, 250
freie Algebra
freie abelsche Gruppe, 252
freie Gruppe, 258
freies abelsches Monoid, 252
Termalgebra, 250
freie Halbgruppe, 129
freie Variable, 75
freier Ultrafilter, 244
freies Monoid, 129
freies Objekt, 250, 251
Frobenius-Automorphismus, 194
Frobeniusautomorphismus, 354
führender Koeffizient, 202
führender Koeffizient, 309
fundamentale Operation, 51
Fundamentalsatz der Algebra, 30, 306
Fundamentalsatz der Arithmetik, 132
Fundamentalsatz der Zahlentheorie, 132
Funktion, 41
Funktor, 88

Galois-abgeschlossen, 454
Galoisfeld, 283, 349
Galoisgruppe, 460
eines Polynoms, 481
Galoisgruppe der allgemeinen Gleichung $n$-ten Grades, 492
Galoiskorrespondenz, 454, 455
Galoisverbindung, 454, 455
ganz abgeschlossen in $S$, 516
ganz algebraisch, 326
ganz über einem Ring, 515
ganze $p$-adische Zahlen, 368
ganze $p$-adische Zahlen, 367
ganzes Element, 515
Gauß'scher Ring, 287
Gaus'sche Zahlen, 297
gebrochen rationale Funktion, 202, 300
gebrochen rationale Funktionen, 300
gebrochenes Ideal, 517
gebundene Variable, 75
gekürzte Darstellung, 299
geordnete Gruppe, 58, 212
geordnete Halbgruppe, 58
geordneter Körper, 58
geordnetes Paar, 40
gerade Permutation, 168
gerichtete Menge, 374
gerichteter Graph, 93
Gesetz, 72
Gleichheitsrelation, 113
Gleichung, 72
gleichungsdefinierte Klasse, 73
Going-up-Theorem, 522
Gröbnerbasis, 511
Grad, 201, 309
Grad einer Körpererweiterung, 321
Gradsatz, 321
Graph
gerichteter, 93
größter gemeinsamer Teiler, 134
größter gemeinsamer Teiler, 280
größtes Element, 46
Gruppe, 53
freie, 258
freie abelsche, 252
vom Typ (2), 57
vom Typ $(2, 0, 1)$, 57
Gruppen vom Lie-Typ, 426
Gruppenaktion, 414
Gruppenalgebra, 412
Gruppenordnung, 144
Gruppenring, 274
Gültigkeit von Gesetzen, 72

halbgeordnete Gruppe, 58
halbgeordnete Halbgruppe, 57
Halbgruppe, 53
Halbgruppenaktion, 414
Halbordnung, 43
Halbordnung(srelation), 43
Halbring, 54

Halbring mit Einselement, 54
Halbverband, 55
Hasse-Diagramm, 48
Hauptfilter, 243
Hauptideal, 189, 244
Hauptideale, 243
Hauptidealring, 189, 285, 292
Hauptsatz
der Galoistheorie endlichdimenional, 470
über endlich erzeugte abelsche Gruppen, 399
über endlich erzeugte $R$-Moduln, 398
Hauptsatz über endliche abelsche Gruppen, 183
Hauptsatz über symmetrische Polynome, 308
Hausdorffsches Maximalitatsprinzip, HMP, A8
Hilbert 90, 499
Hilbertsche Nullstellensatz, 206
Hilbertscher Basissatz, 510
Hom-Funktor, 405
Homomorphiebedingung, 20, 62
Homomorphiesatz, 114
Homomorphismus, 62

Ideal, 26, 186, 224
Idealsatz, A11
idempotent, 52
identifizieren, 20
Identität, 83
Identität, 113
$\Longrightarrow$ (Implikationsoperation)), 234
Index, 145
Induktion
transfinite, A3
induktive Menge, 2
induzierte Operation, 20
induzierte Sequenz, 406
induzierter Homomorphismus, 404
Infimum, 46
Infixnotation, 68
initiales Objekt, 87
injektiv, 41, 62
injektiver Limes, 375
injektiver Modul, 386
injektives System, 375
innere Automorphismus, 166
innere direkte Produkt, 152
innere direkte Summe, 176
innerer Automorphismus, 148
innerer Automorphismus, 166
inneres direktes Produkt, 154, 156
inneres semidirektes Produkt, 437, 438
inseparabel, 463
Separabilitätsgrad, 498
Integritätsbereich, 22
Integritätsbereich, 54
Interpolation nach Lagrange, 314
Interpolation nach Newton, 315
Interpolationspolynom, 314
Interpretation von Formeln, 75
Intervall, 223
invariante Faktoren, 399
inverse Relation, 42
Inversenbildung, 52
Inverses, 52
invertierbares Element, 52
invertierbares Ideal, 517
irreduzibel, 281, 284
irreduzibles Element, 284
isoliertes Primideal, 513
isomorph, 9
$\cong$ (isomorph), 62
isomorphe Einbettung, 20, 62, 64
Isomorphismus, 9, 62, 64

Juxtaposition, 167

$K$-Automorphismus, 460
Körper der $p$-adischen Zahlen, 368
Körpererweiterung, 318
$K$-Algebra, 411
kanonische Abbildung, 20
kanonische Darstellung, 299
kanonische Einbettungen, 152
kanonische Projektionen, 152

kanonischer Homomorphismus, 114
kanonischer Homomorphismus, 20
Kardinalzahl, A12
kartesische Produkt, 106
kartesisches Produkt, 40
Kategorie, 82
    konkrete, 83
Kategorientheorie, 81
Kern, 110, 114, 148, 174, 254
Kette, 43
Kettenbedingung
    absteigende, 443, 508
    aufsteigende, 443, 507
Klassen, 44, 81
Klassengleichung, 417
Klassifikation endlicher Körper, 349
klassische Galoiskorrespondenz, 460
klassische Logik, A23
kleine Kategorie, 83
kleinstes Element, 45
kleinstes gemeinsame Vielfache, 134
kleinstes gemeinsames Vielfaches, 280
Klon, 79
Koeffizient, 200
koendliche Menge, 240
Kolimes, 375
Komma-Kategorie, 86
kommutativ, 51
kommutativer Halbring, 54
kommutativer Ring, 54
Kommutativgesetz, 51
Kommutator, 151, 431
Kommutatorgruppe, 151, 431
kompakt-offene Topologie, 372
Komplement, 52
komplementäres Element, 52
komplexe Zahlen, 28
Komplexprodukt, 50, 129
komponentenweise, 19
Komposition, 79, 82
Kompositionsreihe, 432
kongruent modulo $m$, 160, 161
Kongruenz, 110
    triviale, 113
Kongruenzrelation, 13, 110
Konjugation, 166
konjugiert, 28, 323
Konjugierte, 166
Konjugiertenklassen, 416
Konkatenation, 129
konstante Operation, 51
Konstantensymbol, 67
konstanter Koeffizient, 202
konstruierbar (mit Zirkel und Lineal), 331
Konstruktion (mit Zirkel und Lineal), 330
Konstruktion von Gruppen mittels Erzeuger und Relation, 422
Kontinuum, A17
Kontinuumshypothese, A17
kontravarianter Funktor, 88
kontravarianter Hom-Funktor, 91
kontravarianter Hom-Funktor, 405
konvexe Teilmenge, 223
Koprodukt, 266
Körper, 54
Körper der gebrochen rationalen Funktionen, 199
kouniverselles Objekt, 87
kovarianter Funktor, 88
kovarianter Hom-Funktor, 91
kovarianter Hom-Funktor, 405
Kranzprodukt, 437, 442
Kreisteilungskörper, 344
Kreisteilungskörper, 501
Kreisteilungspolynom, 502
Kreisteilungspolynome, 344
kubische Resolvente, 489, 491
Kürzbarkeit, 52
kurzexakte Sequenz, 437
$\mathfrak{K}$-Vektorraum, 55

Länge eines Zyklus, 167
leere Menge, 51
leeres Wort, 129
Lemma
    von Fitting, 446
    von Teichmüller/Tukey, A8
    von Zassenhaus, 434

von Zorn, A8
lexikographische Ordnung, 213
Limeselement, A2
linear abhängig, 32, 377
linear unabhängig, 32, 377
lineare Hülle, 32
lineare Ordnung, 43
linearer Koeffizient, 202
Linearkombinationen, 174
Links-Modul, 54
Linksdistributivität, 51
Linksideal, 188
Linksinverses, 52
linksinvertierbares Element, 52
linkskürzbar, 52
Linkskürzbarkeit, 52
Linksnebenklasse, 144
linksneutrales Element, 51
Linksnullteiler, 54
linksregulär, 52
Lokalisierung, 518
Lying-over-Theorem, 522

$M_3$, 225
Maximalbedingung, 47
maximaler Filter, 242
maximales Element, 46
maximales Ideal, 190, 191, 243
Menge
endliche, A19
induktive, A18
unendliche, A19
Mengen und Klassen, 44, 81
Mengenalgebra, 240
Mengenlehre, 73
Minimalbedingung, 47
minimales Element, 45
Minimalpoynom, 322
miteinander verträglich, 62
mittellineare Abbildung, 410
Modell, 76
Modell von John von Neumann, 11, 12
Modelltheorie, 73
Modul, 54
dualer, 409
injektiver, 390
$p$-primärer, 395
projektiver, 391
torsionsfreier, 395
Modul über einem Ring, 174
modularer Verband, 228
modulo, 136, 161
monisch, 202
monisches Polynom, 281
Monoid, 53
Monoidring, 273
Monom, 274
Monomorphismus, 62, 64
monoton, 63
schwach, 45, A2
streng, A2
monoton fallend, 63
monoton wachsend, 63
Monotoniegesetz, 58, 211
Monotoniegesetz für die Multiplikation, 58
Monotoniegesetze, 24
Morphismus, 82
Morphismus von Diagrammen, 94

$N_5$, 225
nach oben beschränkt, 46
nach unten beschränkt, 46
Nachfolgeelement, A2
Nachfolger, 48
$n$-äre Operation, 51
natürliche Abbildung, 409
natürliche Transformation, 94, 95
natürlicher Homomorphismus, 114
Nebenklasse, 186
Nebenklassenzerlegung einer Gruppe nach einer Untergruppe, 144
Negativteil, 212
Nenner, 299
neutrales Element, 51
$\mathbb{N}_I$, 4
nichttrivialer Teiler, 281
nilpotente Gruppe, 429

Noethersch, 507
Noethersche Halbordnung, 47
Noethersches Normalisierungslemma, 524
Nonstandardmodell, 78
Nonstandardmodelle, 8
Norm, 498
normaler Endomorphismus, 445
Normalform, 17, 256
Normalisator, 416
Normalreihe, 432
Normalteiler, 146
Normalteilerverband, 148
Normfunktion, 282
normiert, 202, 281, 299
normierte Darstellung, 300
normiertes Polynom, 281
Normierungsfunktion, 299
$n$-stellige Operation, 51
$n$-stellige Relation, 40
Nullelement, 51
Nullstellen, 206
Nullstellenkörper, 336
Nullteiler, 54, 195
nullteilerfrei, 22, 54

obere Schranke, 46
Oberkörper, 318
Objekt, 82
Operationssymbol, 67
Orbit, 415
Ordinalzahl, A12
Ordinalzahlen, A13
Ordnung, 201, 202
Ordnung einer Gruppe, 144
Ordnung eines Elements, 144
Ordnungsideal, 395
Ordnungsisomorphismus, A2
Ordnungstyp, A13
$\perp$, 234
orthogonale Gruppe, 172
otp, A13

$P$-primärer Untermodul, 513

$p$-Anteil, 172, 180
paradoxe Zerlegung, 260
Paradoxon von Hausdorff-Banach-Tarski, 260
Partialbruchzerlegung, 312, 313
partielle Operation, 51
partielle Ordnung, 43
Partition, 43
Peano-Axiome, 8, A19
Peano-Struktur, 8
$p$-Element, 144, 172, 400
Permutationsgruppe, 165
$\perp$ (`\perp`), 234
$\to$ (Implikationsoperation), 234
$p$-Gruppe, 144, 418
$p$-Komponente, 180
planarer Wurzelbaum, 69
Polynom, 200, 202
Polynomalgebra, 270
Polynome, 200, 270
Polynomfunktion, 205, 272
Polynomfunktionen, 80
Polynomring, 200
Pontrjaginsches Dual, 372
positives Element, 212
Positivteil, 212
Postfixnotation, 68
Potenz, 125
Potenzkategorie, 96
Potenzmenge, 43
$p$-Prüfergruppe, 181
Prüfergruppe, 366
Prädikatenlogik erster Stufe, 74, 77
Prädikatenlogik zweiter Stufe, 77
Präfixnotation, 68
Präordnung, 44
primärer Modul, 513
$P$-primärer Untermodul, 513
Primärideal, 513
Primärzerlegung, 513
prime Restklasse, 164
Primelement, 283
Primfaktorzerlegung, 132
Primfilter, 224, 242

Primideal, 190, 191, 224, 243
primitive Einheitswurzel, 344
primitive $n$-te Einheitswurzel, 500
primitives Polynom, 352
primitives Polynom, 301
Primkörper, 318, 320
Primkörper, 283, 317
Primzahl, 132
Prinzip der isomorphen Einbettung, 20
Prinzip der transfiniten Induktion, A3
Produkt, 125, 126
    semidirektes, 440
Produkt in einer Kategorie, 108
Produkt von Idealen, 517
proendlich, 478
Projektion, 78, 106
projektive lineare Gruppe, 172
projektiver Modul, 386
%, 136
Prüfergruppe, 181
$p$-Sylow-Gruppe, 418

quadratische Resolvente, 487
quadratischer Zahlring, 282
Quadratwurzelerweiterung, 332
Quasiordnung, 44
Quaternionen, 31
Quaternionengruppe, 422
Quelle, 82
Quotient, 136
Quotientengruppe, 139
Quotientenkörper, 24, 196
Quotientenmonoid, 139
Quotientenmonoid im eigentlichen Sinn, 139
Quotientenmonoid im weiteren Sinn, 137
Quotientenring, 195

$R$-lineare Abbildung, 174
$R$-Modul, 174
Radikal, 512
Rang, 399
    einer linearen Abbildung, 36
    eines freien Moduls, 379
Rangfunktion, A13
Rechts-Modul, 54
Rechtsdistributivität, 51
Rechtsideal, 188
Rechtsinverses, 52
rechtsinvertierbares Element, 52
Rechtskürzbarkeit, 52
rechtskürzbar, 52
Rechtsnebenklasse, 144
rechtsneutrales Element, 51
Rechtsnullteiler, 54
rechtsregulär, 52
reduzierte Darstellung eines Ideals, 513
reduziertes Wort, 258
reflexiv (auf $A$), 42
reflexiver Raum, 92
reguläre Darstellung, 131
rein algebraische relationale Struktur, 57
rein relationale Struktur, 57
Rekursionssatz, 9, A6
Rekursionstheorie, 73
relationale Struktur, 57
Relationenmonoid, 53
Relationenprodukt, 41
Rest, 136
Restklasse, 161
Restklassengruppe, 161
Restklassenring, 115, 189
Ring, 54
Ring der formalen Potenzreihen, 200
Ring der ganzen Gaus'schen Zahlen, 297
Ring mit 1, 54
Ring mit eindeutiger Primfaktorzerlegung, 287
Ring mit Einselement, 54
Ringerweiterung, 515
    ganze, 515
Ringerzeugnis, 319

Satz
    von Birkhoff, 248, 264
    von Cantor-Schröder-Bernstein, A15
    von Schröder-Bernstein, 379
    von Cauchy, 417

von Cayley, 414
von Hartogs, A7
von Jordan-Hölder, 435
von Krull-Schmidt, 444
von Lagrange, 417
von Schreier, 435
von Stone, 239, 245
von Wedderburn, 421
Wohlordnungs-, A9
Satz vom primitiven Element, 345
Satz von Feit-Thompson, 436
Satz von Kronecker, 335
Satz von Lüroth, 346
Satz von Vieta, 312
Schiefkörper, 31
Schiefkörper, 54
Schmetterlingslemma, 434
Schnitt-Halbverband im ordnungstheoretischen Sinn, 58
schwach monoton, 45
schwach strukturverträgliche Abbildung, 63
schwaches Produkt, 155
semidirektes Produkt, 437
separabel, 463
Separabilitätsgrad, 498
Sequenz
kurzexakte, 381
zerfallende, 383
Signatur, 57
Signum einer Permutation, 168
spezielle lineare Gruppe, 172
sporadische Gruppen, 426
Spur, 498
stabil, 474
Stabilisator, 415
Standardkranzprodukt, 442
stark strukturverträgliche Abbildung, 63
strikt monoton, 45
strikte Halbordnung(srelation), 43
strukturverträgliche Abbildung, 63
Stützstellen, 314
subdirektes Produkt, 139, 263
Subnormalreihe, 432
Supremum, 27, 46
surjektiv, 41, 62
Syllogismen, 40
Sylow-Sätze, 419
symmetrisch, 42
symmetrische Funktion, 308
symmetrische Gruppe, 53
symmetrische Halbgruppe, 53
symmetrische Monoid, 130
symmetrisches Monoid, 53, 365
symmetrisches Polynom, 308

teilbar, 136, 278
teilbar durch $n$, 386
Teilbarkeit, 278, 386
Teilbarkeitshalbordnung, 279
Teiler, 132, 278
teilerfremde Restklasse, 164
Teilerkettenbedingung, 287
Teilerverband, 59, 291
Tensorprodukt, 410
Termalgebra, 68
als freie Algebra, 250
Terme, 67
Termfunktionen, 80
terminales Objekt, 87
Theorie der reell abgeschlossenen Körper, 78
Topologie der gleichmäßigen Konvergenz auf kompakten Teilmengen, 372
topologische Algebra, 362
topologische Gruppe, 362, 363
topologische Halbgruppe, 362
topologischer Isomorphismus, 366
topologischer Ring, 362
Torsionsanteil, 172
Torsionselement, 144, 172, 395, 400
Torsionsgruppe, 144
Torsionsmodul, 395
totalgeordnete Gruppe, 212
Totalordnung, 43
Träger, 155
Trägermenge, 51, 57
transitiv, 42, 415

transitive Hülle, 48
transitive Menge, A13
Transposition, 167
Transversale, 281
transzendent, 322
transzendente Zahl, 341
transzendentes Körperelement, 322
Transzendenzbasis, 327
Transzendenzgrad, 330
triviale Erweiterung, 438
triviale Faktoralgebren, 113
triviale homomorphe Bilder, 113
triviale Ideale, 186
triviale Kongruenzen, 113
triviale Normalteiler, 149
triviale Varietät, 120
trivialer Teiler, 281
Tupel, 106
Typ, 51, 57

Ultrafilter, 242
Ultrafiltersatz, 243, A11
unäre Operation, 51
Unbestimmten, 270
unechter Teiler, 281
uneigentlicher Filter, 224
uneigentliches Ideal, 224
unendlichdimensionale Erweiterung, 321
unendliche Menge, 3
ungerade Permutation, 168
unitäre Gruppe, 172
unitärer Modul, 54
universell, 130
universelle Algebra, 39, 51
universelle Eigenschaft, 70
universelle Prüfergruppe, 181
universelles Objekt, 87
Universum, 83
Unteralgebra, 97
untere Schranke, 45
Untergruppe, 98
Unterhalbgruppe, 98
Unterkörper, 99
Unterkörper, 102, 318
Unterraum, 99
Unterring, 99
Untervektorraum, 99
Unvollständigkeitssatz, 77
Urbild, 41

Variablen, 67, 270
Variablenbelegung, 71
Varietät, 521
Varietät, 72
Vektorraum, 55
verallgemeinerte Polynome, 270
verallgemeinerte Quaternionengruppe, 425
Verband, 58
    distributiver, 55, 61
    im algebraischen Sinn, 55
    vollständiger, 49, 58
Vereinigungs-Halbverband im ordnungstheoretischen Sinn, 58
Vergissfunktor, 84, 89
vergleichbar, 42
Vergleichbarkeitssatz, A15
Verschmelzungsgesetze, 52
verträglich, 19
Verträglichkeit, 9
verträglich, 62, 110
Vielfaches, 278
Vielfachheit, 305
vollständig angeordneter Körper, 27, 215
vollständige partielle Ordnung, 225
vollständiger Verband, 49
vollständiger Verband, 58
Vollständigkeitssatz, 76
Von Neumanns Modell, A18

Wert, 72, 272
Wert eines Polynoms, 272
Wirkung, 413, 414
wohldefiniert, 20
Wohldefiniertheit, 13, 112
Wohlordnung, 43, A1
Wurzelbaum, 69

Zähler, 299
Zentralisator, 416

Zentrum, 166
Zerfällungskörper, 336
Zerlegbarkeit in irreduzible Elemente, 286
Zerlegbarkeit in Primelemente, 286
Zerlegung, 286
ZFC-Axiome, A23
Ziel, 82
ZPE-Ring, 287
zugehörige rein relationale Struktur, 57
Zwischenkörper, 460
Zyklenschreibweise, 167
zyklisch, 144, 376
zyklische Gruppe, 158
zyklische Permutation, 167
Zyklus, 167