Inhaltsverzeichnis

Kapitel 1

Algebraische Strukturen

1.1 Operationen

1.1.A Stelligkeit und Typ

1.1.1 Definition. Sei A eine Menge, $n \in \mathbb{N}_0$, dann heißt eine Abbildung $\omega : A^n \to A$ eine *n-stellige*[1] (oder *n-äre*) *Operation auf A*, d. h.,
für $n \in \mathbb{N}$:

$$\omega : \begin{cases} A^n \to A \\ (x_1, \ldots, x_n) \mapsto \omega x_1 \ldots x_n \text{ oder } \omega(x_1, \ldots, x_n) \end{cases}$$

für $n = 0$:

$$\omega : \begin{cases} A^0 = \{\emptyset\} \to A \\ \emptyset \mapsto \omega\emptyset =: \omega. \end{cases}$$

Wichtigster Fall: $n = 2$. Eine 2-stellige oder binäre Operation ist eine Abbildung

$$\omega : \begin{cases} A^2 \to A \\ (x, y) \mapsto \omega xy \text{ oder } \omega(x, y). \end{cases}$$

Meist bezeichnen wir 2-stellige Operationen mit Symbolen wie $\circ$, $+$, $*$, $\star$ statt mit Buchstaben wie ω; für diese Symbole verwenden wir dann meist „Infixnotation“ statt Präfixnotation (siehe Abschnitt 1.2), also

$$\circ : \begin{cases} A^2 \to A \\ (x, y) \mapsto x \circ y. \end{cases}$$

1.1.2 Beispiele. 1) $+$ und $\cdot$ sind 2-stellige Operationen auf $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}^+$, $\mathbb{R}$, $\mathbb{R}^+$ und $\mathbb{C}$, $-$ ist 2-stellige Operation auf $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$, $\div$ auf $\mathbb{Q}^+$, $\mathbb{R}^+$, $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$, $\mathbb{C} \setminus \{0\}$.

2) $+$ und $\cdot$ (im üblichen Sinn) sind 2-stellige Operationen auf $M_n(\mathbb{C})$, der Menge aller quadratischen $n \times n$-Matrizen über $\mathbb{C}$ (analog mit $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ statt $\mathbb{C}$).

3) Seien M und N Mengen. Mit N^M bezeichnen wir die Menge aller Abbildungen von M nach N: $N^M := \{f \mid f : M \to N\}$.
Für $M = N$ ist die binäre Operation $\circ$ auf N^M wie folgt definiert: $(f \circ g)(x) := f(g(x))$ für alle $x \in M$ (Komposition oder Verkettung von Funktionen). Wir erhalten also:

$$\circ : \begin{cases} M^M \times M^M \to M^M \\ (f, g) \mapsto f \circ g. \end{cases}$$

4) M sei eine Menge und $\mathfrak{P}(M) := \{T \mid T \subseteq M\}$ die Potenzmenge von M. $\cap$, $\cup$ sind binäre Operationen auf $\mathfrak{P}(M)$.

[1] n heißt auch „Stelligkeit“ oder „Arität“ der Operation, englisch „arity“

Weiterer wichtiger Fall: $n = 1$. Eine einstellige (unäre) Operation ist eine Abbildung

$$\omega : \begin{cases} A \to A \\ x \mapsto \omega x. \end{cases}$$

1.1.3 Beispiele. 1) $- : \begin{cases} \mathbb{C} \to \mathbb{C} \\ x \mapsto -x \end{cases}$ ist einstellige Operation auf $\mathbb{C}$.

2) $-$ ist auch einstellige Operation auf $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $M_n(\mathbb{C})$.

3) $x \mapsto 1/x$ ist einstellige Operation auf $\mathbb{Q} \setminus \{0\}$, $\mathbb{Q}^+$, $\mathbb{R} \setminus \{0\}$, $\mathbb{R}^+$, $\mathbb{C} \setminus \{0\}$.

4) $T \mapsto M \setminus T =: T'$ ist einstellige Operation auf der Potenzmenge $\mathfrak{P}(M)$.

1.1.4 Anmerkung. Das Symbol „$-$“ wird sowohl für die einstellige Operation des „Negativmachens“ (oft: Multiplikation mit -1) als auch für die zweistellige Operation „Differenz“ verwendet. Der Kontext entscheidet, ob die einstellige oder zweistellige Operation gemeint ist.
In den Gleichungen

$$x - y = x + (-y), \qquad x - (-y) = x + y$$

bezeichnet das erste „$-$“ jeweils die zweistellige Operation, das zweite die einstellige.

1.1.5 Definition. Sei A eine Menge, $n \in \mathbb{N}_0$, $D \subseteq A^n$, dann heißt eine Abbildung $\omega : D \to A$ eine *n-stellige partielle Operation auf A*.
1) $-$ ist eine zweistellige partielle Operation auf $\mathbb{N}$.

2) $x \mapsto 1/x$ ist einstellige partielle Operation auf $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ($D = \mathbb{Q} \setminus \{0\}, \ldots$).

Sei $A = \{a_1, \ldots, a_n\}$ eine endliche Menge und $\circ$ eine binäre Operation auf A. Dann kann diese durch eine Operationstafel, die sog. *Cayley-Tafel* angegeben werden. Die Tafel weist im Schnittpunkt der i-ten Zeile mit der j-ten Spalte das Element $a_i \circ a_j$ auf.

1.1.6 Definition. Sei A Menge, I (Index-)Menge. Für $i \in I$ sei ω_i eine n_i-stellige Operation auf A, $n_i \in \mathbb{N}_0$. Dann heißt $\mathfrak{A} := (A, (\omega_i)_{i \in I})$ eine (*universelle*) *Algebra* mit der *Grundmenge* A und der *Operationenfamilie* $(\omega_i)_{i \in I} =: \Omega$.

Häufig ist I endlich, etwa $I = \{1, \ldots, n\}$. In diesem Fall schreibt man

$$(A, \Omega) = (A, (\omega_i)_{i \in \{1, \ldots, n\}}) =: (A, \omega_1, \ldots, \omega_n).$$

Die Familie $(n_i)_{i \in I}$ heißt der *Typ* der Algebra (A, Ω). Algebren desselben Typs heißen „ähnlich“. Oft[2] verwenden wir für eine Algebra und ihre Grundmenge dasselbe Symbol, also $A = (A, \Omega)$, sofern keine Verwechslung möglich ist.

1.1.7 Beispiel. $(\mathbb{Z}, +, -, 0)$ ist eine Algebra vom Typ $(2, 1, 0)$, $(\mathbb{Z}, +, -, 0, \cdot, 1)$ ist eine Algebra vom Typ $(2, 1, 0, 2, 0)$.

[2] In der Logik und auch in der universellen Algebra verwendet man oft ein Symbol (A, B, …, oder auch einen komplizierteren Ausdruck wie A', B_1, …) für die Grundmenge einer Algebra und ein entsprechendes Symbol aus einem anderen Zeichensatz ($\mathfrak{A}$, $\mathcal{A}$, $\mathscr{A}$, analog $\mathfrak{B}_1$, …) für die Algebra. Man kann auch die Algebra selbst als das fundamentale Objekt betrachten, und bezeichnet dann die Algebra z.B. mit A, die Grundmenge mit $|A|$ oder $univ(A)$, die Operationen mit ω_i^A.

1.1.B Kommutativität, Assoziativität, Distributivität

1.1.8 Definition. Sei A Menge, $\circ$ binäre Operation. $\circ$ heißt *assoziativ* genau dann, wenn das so genannte *Assoziativgesetz* gilt:

$$\forall x, y, z \in A : (x \circ y) \circ z = x \circ (y \circ z).$$

1.1.9 Beispiel. $+, \cdot$ auf $\mathbb{C}$ und $M_n(\mathbb{C})$ sind assoziativ, ebenso $\circ$ auf M^M und $\cap, \cup$ auf $\mathfrak{P}(M)$. Dagegen sind $-, \div$ im allgemeinen *nicht* assoziativ![3]

1.1.10 Definition. Die binäre Operation $\circ$ auf A heißt *kommutativ* $:\Leftrightarrow$

$$\forall x, y \in A : x \circ y = y \circ x \quad (\textit{Kommutativgesetz})$$

1.1.11 Beispiel. *Nicht* kommutativ sind: $-$ auf $\mathbb{C}$, $\div$ auf $\mathbb{C} \setminus \{0\}$, $\cdot$ auf $M_n(\mathbb{C})$ für $n \geq 2$, $\circ$ auf M^M für $|M| \geq 2$.

1.1.12 Definition. Sind $+, \cdot$ binäre Operationen auf A, dann heißt $\cdot$ *distributiv über* $+ :\Leftrightarrow$ es gelten die *Distributivgesetze*:

$$\forall x, y, z \in A : x \cdot (y + z) = x \cdot y + x \cdot z \quad (\textit{Linksdistributivgesetz})$$
$$\forall x, y, z \in A : (y + z) \cdot x = y \cdot x + z \cdot x \quad (\textit{Rechtsdistributivgesetz})$$

1.1.13 Anmerkung. Um Klammern zu sparen, verwenden wir die Konvention: „Punktrechnung wird vor Strichrechnung ausgeführt."

1.1.14 Beispiel. $\cdot$ ist distributiv über $+$ in $\mathbb{C}$, $M_n(\mathbb{C})$. In $\mathfrak{P}(M)$ ist $\cup$ distributiv über $\cap$ und $\cap$ distributiv über $\cup$.

1.1.C Neutrale und inverse Elemente

1.1.15 Definition. Sei A Menge, $\circ$ eine binäre Operation auf A. Sei $e \in A$, dann heißt e

- ein *Linkseinselement* oder *linksneutrales Element* bezüglich $\circ :\Leftrightarrow \forall x \in A : e \circ x = x$,
- ein *Rechtseinselement* oder *rechtsneutrales Element* bezüglich $\circ :\Leftrightarrow \forall x \in A : x \circ e = x$,
- ein *Einselement* oder *neutrales Element* bezüglich $\circ :\Leftrightarrow \forall x \in A : e \circ x = x \circ e = x$.

1.1.16 Anmerkung. Universell quantifizierte Gleichungen zwischen Termen (also Gleichungen, die die Form $t_1(x, y, z, \ldots) = t_2(x, y, z, \ldots)$ mit geeigneten Termen t_1, t_2 haben und für alle Elemente einer Algebra erfüllt sein sollen, wie z. B. „$\forall x \in A : e \circ x = x$"), heißen *Gesetze*.
Um deutlich zu machen, dass nicht die Terme t_1 und t_2 qua[4] formale Objekte gleich sind, sondern nur ihre Auswertungen an allen Elementen der betrachteten Algebra (zum Beispiel enthält der Term $x \cdot x^{-1}$ die Variable x zwei Mal, der Term 1 enthält sie gar nicht), schreibt man Gesetze oft nicht in der Form $t_1 = t_2$ sondern verwendet die Notation $t_1 \approx t_2$.

[3] Ein weiteres Beispiel aus der Umgangssprache: Nach dem 2.Weltkrieg waren Lebensmittel in Österreich rationiert, und man konnte sie offiziell nur gegen Marken oder „Punkte" eintauschen, die man am Anfang des Monats von einer Behörde erhielt. Diese (Lebensmittel)punkte standen für viele im Lebens(mittelpunkte).

[4] qua=in ihrer Eigenschaft als

1.1.17 Beispiele. 1) Sei $A = \mathbb{C}$ mit der Operation $\circ = +$. Dann ist 0 neutrales Element.
2) Sei $A = \mathbb{C}$ mit der Operation $\circ = \cdot$. Dann ist 1 ist neutrales Element. (Wir sagen: „1 ist neutral *bezüglich* Multiplikation, 0 ist neutral bezüglich Addition.“)

3) Sei $A = M_n(\mathbb{C})$. Dann ist $\begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}$ neutrales Element bezüglich Addition, $\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$ ist neutrales Element bezüglich (Matrizen-)Multiplikation.

4) Sei $A = M^M$ mit $\circ =$ Komposition. Dann ist id_M (die identische Abbildung) neutrales Element.

5) Sei $A = \mathfrak{P}(M)$. Dann ist M ist neutrales Element bezüglich der Operation $\cap$, denn $X \cap M = X$ für alle $X \in \mathfrak{P}(M)$. Die leere Menge $\emptyset$ ist neutrales Element bezüglich $\cup$.

1.1.18 Satz. *Sei $\circ$ binäre Operation auf A, e_1 Linkseinselement und e_2 Rechtseinselement. Dann gilt: $e_1 = e_2$, und $e_1 (= e_2)$ ist Einselement.*

Beweis. $e_1 = e_1 \circ e_2 = e_2$. □

1.1.19 Folgerung. Es gibt höchstens ein Einselement.

1.1.20 Definition. Sei A Menge, $\circ$ binäre Operation, e Einselement, $x \in A$; dann heißt ein Element $y \in A$ *linksinvers* zu $x :\Leftrightarrow y \circ x = e$, *rechtsinvers* zu $x :\Leftrightarrow x \circ y = e$, *invers* zu $x :\Leftrightarrow x \circ y = y \circ x = e$.

1.1.21 Beispiel.

Menge	Operation	Element	Inverses
$\mathbb{C}$	$+$	x	$-x$
$\mathbb{C}$	$\cdot$	$x \neq 0$	$1/x$
$M_n(\mathbb{C})$	$+$	(a_{ij})	$(-a_{ij})$
$M_n(\mathbb{C})$	$\cdot$	(a_{ij}) mit $\det(a_{ij}) \neq 0$	$(a_{ij})^{-1}$
M^M	$\circ$	bijektives f	f^{-1}
$\mathfrak{P}(M)$	$\cap$	M	M
$\mathfrak{P}(M)$	$\cup$	$\emptyset$	$\emptyset$
$\mathbb{Z}$	$\cdot$	± 1	± 1

1.1.22 Definition. x heißt *invertierbar* $:\Leftrightarrow$ es gibt ein Inverses zu x.

1.1.23 Satz. *$\circ$ sei assoziative binäre Operation auf A, $x \in A$, y_1 linksinvers zu x, y_2 rechtsinvers zu x bezüglich des neutralen Elementes e. Dann gilt: $y_1 = y_2$.*

Beweis. $y_2 = e \circ y_2 = (y_1 \circ x) \circ y_2 = y_1 \circ (x \circ y_2) = y_1 \circ e = y_1$. □

1.1.24 Folgerung. Bei einer assoziativen Operation gibt es zu jedem Element x höchstens ein Inverses.

Schreibweise für das Inverse von x: x^{-1} (bezüglich $\circ, \cdot$) oder $-x$ (bezüglich $+$). Ein neutrales Element bezüglich $+$ wird meist mit 0 bezeichnet.

1.1.D Reguläre und invertierbare Operationen

1.1.25 Definition. $\circ$ heißt *invertierbar* auf $A :\Leftrightarrow$

$$\forall (a,b) \in A^2 \; \exists (x,y) \in A^2 : a \circ x = b \text{ und } y \circ a = b.$$

1.1.26 Satz. *Sei $A \neq \emptyset$ und $\circ$ eine assoziative Operation auf A. Dann sind folgende Aussagen äquivalent:*

a) $\circ$ ist invertierbar auf A.

b) Es gibt ein neutrales Element e bezüglich $\circ$, und jedes $x \in A$ ist invertierbar, d. h., $\exists y \in A : x \circ y = y \circ x = e$.

Beweis. b) $\Rightarrow$ a): Für $x \in A$ bezeichne x^{-1} das Inverse von x. Seien $a, b \in A$. Dann gilt: $a \circ (a^{-1} \circ b) = (a \circ a^{-1}) \circ b = e \circ b = b$ und $(b \circ a^{-1}) \circ a = b \circ (a^{-1} \circ a) = b \circ e = b$.

a) $\Rightarrow$ b): Sei $a \in A$ beliebig, aber fest. Dann gilt: $\exists e_1, e_2 \in A : e_1 \circ a = a = a \circ e_2$ (setze $b = a$, $y = e_1$, $x = e_2$). Für beliebiges $b \in A$ gilt dann:

$$\exists x \in A : b = a \circ x \Rightarrow e_1 \circ b = e_1 \circ (a \circ x) = (e_1 \circ a) \circ x = a \circ x = b,$$
$$\exists y \in A : b = y \circ a \Rightarrow b \circ e_2 = (y \circ a) \circ e_2 = y \circ (a \circ e_2) = y \circ a = b.$$

Also ist e_1 Linkseinselement, e_2 Rechtseinselement und daher $e_1 = e_1 \circ e_2 = e_2 =: e$ Einselement.

Nun ist noch zu zeigen, dass zu jedem $x \in A$ ein Inverses y existiert. Da $\circ$ invertierbar, gilt:

$$\exists y_1, y_2 \in A : x \circ y_1 = e \text{ und } y_2 \circ x = e.$$

Also ist y_1 Rechtsinverses, y_2 Linksinverses von x, woraus $y_1 = y_2 =: y$ folgt und somit y invers zu x ist. □

1.1.27 Anmerkung. In dem eben bewiesenen Satz haben die Gleichungen $a \circ x = b$ und $y \circ a = b$ genau eine Lösung x, y. Aus $a \circ x_1 = b = a \circ x_2$ folgt nämlich $a^{-1} \circ (a \circ x_1) = a^{-1} \circ (a \circ x_2)$ und daraus (mit Hilfe des Assoziativgesetzes) $x_1 = x_2$. Analog für die zweite Gleichung.

1.1.28 Definition. Die Operation $\circ$ auf A heißt *regulär* oder *kürzbar* $:\Leftrightarrow \forall a, x_1, x_2, y_1, y_2 \in A : (a \circ x_1 = a \circ x_2 \Rightarrow x_1 = x_2)$ und $(y_1 \circ a = y_2 \circ a \Rightarrow y_1 = y_2)$.

Die Gleichungen $a \circ x = b$ und $y \circ a = b$ haben also bei einer kürzbaren Operation $\circ$ *höchstens* eine Lösung, bei einer invertierbaren assoziativen Operation $\circ$ *genau* eine Lösung.

In der Operationstafel: kürzbar $\Leftrightarrow$ jede Zeile (Spalte) enthält jedes Element *höchstens* einmal, invertierbar $\Leftrightarrow$ jede Zeile (Spalte) enthält jedes Element *mindestens* einmal.

Für endliches A gilt: $\circ$ invertierbar $\Leftrightarrow$ $\circ$ regulär (Übung).

Nach obiger Anmerkung gilt: $\circ$ ist invertierbar und assoziativ $\Rightarrow$ $\circ$ ist regulär.

1.1.29 Beispiel. $+, \cdot$ auf $\mathbb{N}$ sind regulär, aber *nicht* invertierbar.

1.1.E Abschluss

1.1.30 Definition. Sei A eine Menge, und sei ω eine partielle (möglicherweise auch totale) einstellige Operation auf A, also eine partielle Funktion von A nach A.
Eine Teilmenge $B \subseteq A$ heißt *abgeschlossen* unter ω, wenn aus $b \in B$ stets $\omega(b) \in B$ folgt.
Sei allgemeiner $\omega : A^n \to A$ eine n-stellige Operation ($n \geq 1$), dann nennen wir B „*abgeschlossen unter* ω“, wenn für alle $b_1, \ldots, b_n \in B$ auch $\omega(b_1, \ldots, b_n) \in B$ gilt.
B heißt *abgeschlossen* unter der nullstelligen Operation ω, wenn der (einzige) Wert von ω in B liegt.

1.1.31 Lemma.

1. *A ist unter jeder partiellen Operation auf A abgeschlossen.*
2. *Für $n \geq 1$ ist die leere Menge unter jeder partiellen n-stelligen Operation abgeschlossen (aber unter keiner nullstelligen Operation).*
3. *Der Durchschnitt von beliebig vielen unter ω abgeschlossenen Mengen ist selbst unter ω abgeschlossen.*
4. *Zu jeder Menge $S \subseteq A$ gibt es eine kleinste Obermenge, den „Abschluss von S unter ω“[5] $\bar{S} \subseteq A$, die unter ω abgeschlossen ist, nämlich den Durchschnitt aller abgeschlossenen Mengen, die S enthalten.*

Der Abschluss $\bar{S}$ von S kann auch so konstruiert werden: Sei $S_0 := S$. Induktiv definieren wir nun eine aufsteigende Folge von Mengen so:

$$S_{k+1} := S_k \cup \{\omega(b_1, \ldots, b_n) \mid b_1, \ldots, b_n \in S_k, (b_1, \ldots, b_k) \in dom(\omega)\}.$$

Wir setzen $S_\infty := \bigcup_{k=0}^{\infty} S_k$. Dann kann man einerseits (induktiv) zeigen, dass $S_k \subseteq \bar{S}$ gelten muss, somit auch $S_\infty \subseteq \bar{S}$, andererseits sieht man leicht, dass S_∞ unter ω abgeschlossen ist, somit $\bar{S} \subseteq S_\infty$. Daher ist S_∞ der Abschluss von S.
Dieses Argument zeigt auch den folgenden Satz:

1.1.32 Satz. *Sei $S \subseteq A$ höchstens abzählbar, das heißt: endlich oder abzählbar. Dann ist der Abschluss von S unter ω auch höchstens abzählbar (weil nämlich die Mengen S_k alle höchstens abzählbar sind und die Vereinigung von abzählbar vielen höchstens abzählbaren Mengen wieder höchstens abzählbar ist).*

Sei nun Ω eine Familie von (partiellen) Operationen auf der Menge A. Dann definieren wir die Begriffe „$S \subseteq A$ ist *abgeschlossen* unter Ω“ und „*Abschluss* von S unter Ω“ ganz analog: S heißt *abgeschlossen* unter Ω, wenn S unter jeder Operation $\omega \in \Omega$ abgeschlossen ist; der *Abschluss* von S ist die kleinste Menge $\bar{S} \subseteq A$, die S als Untermenge enthält und unter Ω abgeschlossen ist.

1.2 Präfix und Postfix

1.2.A Präfix, Infix, Postfix

Es gibt verschiedene Arten, binäre Operationen anzuschreiben.
Sei $\circ$ eine binäre Operation auf der Menge A, also $\circ : A \times A \to A$. Die Operation $\circ$ ordnet jedem Element von $A \times A$ (d.h., jedem geordnetem Paar (x, y) mit $x, y \in A$) ein Element z aus A zu.

[5] Diese Menge nennen wir auch „die von S erzeugte Unteralgebra von (A, ω)“ und schreiben sie als $\langle S \rangle$ oder $\langle S \rangle_\omega$ an, siehe Abschnitt 2.1.

- Wenn wir *Infixnotation* verwenden, schreiben wir das Ergebnis z dieser Operation als $x \circ y$ oder $(x \circ y)$ an.
  Diese Notation wird vor allem dann verwendet, wenn wir die zweistellige Operation als ein abstraktes Symbol (wie $\circ$, $+$, $*$, etc.) anschreiben.

- Wenn wir *Präfixnotation* (auch „polnische Notation“, Łukasiewicz-Notation) verwenden, schreiben wir das Ergebnis z dieser Operation als $\circ xy$ oder $\circ(x, y)$ an.
  Diese Notation wird vor allem dann verwendet, wenn wir die zweistellige Operation durch einen Buchstaben (wie f oder g) oder eine Buchstabengruppe (wie ggT) repräsentieren. Insbesondere werden daher benutzerdefinierte Funktionen in Programmiersprachen meist in Präfixform geschrieben. Auch für einstellige Funktionen wird meistens Präfixnotation verwendet (z.B. $\sin x$). Die Programmiersprache LISP betont diese Notation (z.B. `(cons a b)`).

- Wenn wir *Postfixnotation* (auch „umkehrte polnische Notation“, „reverse Polish notation“, RPN) verwenden, schreiben wir das Ergebnis z dieser Operation als $xy\circ$ an.
  Diese Notation wird in manchen Programmiersprachen verwendet (FORTH, PostScript) sowie auf manchen Taschenrechnern.

Kompliziertere Terme lassen sich ebenfalls in Infix-, Präfix- oder Postfixnotation schreiben. Den Term $(x \cdot y) + (a \cdot b)$ kann man

- in Präfixnotation als $+\cdot xy \cdot ab$ ausdrücken, das kann man von links nach rechts so lesen:

  $+$ die Summe von
  - $\cdot$ erstens dem Produkt aus
    - x
    - y
  - $\cdot$ und zweitens dem Produkt aus
    - a
    - b

- in Postfixnotation als $xy \cdot ab \cdot +$ ausdrücken, das kann man von links nach rechts als einen Algorithmus für die Berechnung des Terms lesen. „Man nehme x, y und bilde das Produkt; dann nehme man a und b und bilde das Produkt. Schließlich bilde man die Summe der beiden letzten Zwischenresultate.“

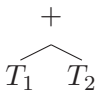
Auch Terme, in denen nicht nur binäre Operationen sondern auch Operationen mit anderen Stelligkeiten vorkommen, lassen sich in Präfix- oder Postfixnotation schreiben. Der Term $(-x) * (-y)$ (wo „$-$“ eine unäre Operation ist) sieht in Präfix- bzw Postfixnotation so aus:

$$*-x-y \qquad x-y-*$$

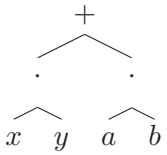
Terme in Präfix- und Postfixnotation lassen sich ohne Verwendung von Klammern anschreiben. Natürlich muss hier die Stelligkeit der Operationen vorgegeben sein. Wenn etwa f und g zweistellig sind, dann ist mit $f\,x\,g\,y\,z$ der Term $f(x, g(y, z))$ gemeint. Wenn hingegen f dreistellig und g einstellig ist, so ist mit $f\,x\,g\,y\,z$ der Term $f(x, g(y), z)$ gemeint.

1.2.B Baumdarstellung

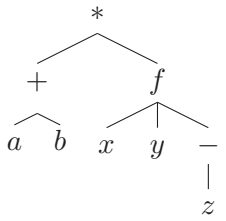
Terme in Präfix- und Postfixnotation lassen sich leicht in Baumdiagramme übersetzen. Ein Term t, der eine Summe darstellt (also t_1+t_2, bzw $+(t_1,t_2)$ bzw $t_1\,t_2+$), wird in einen Baum transformiert, dessen Wurzel (die traditionell oben geschrieben wird) mit dem Symbol $+$ markiert ist; von der 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 $(x \cdot y) + (a \cdot b)$ wird durch den Baum



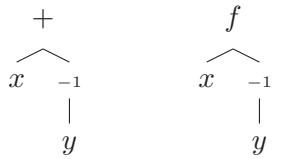
dargestellt, der Term $(a + b) * f(x, y, -z)$ durch den folgenden Baum:



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.

1.2.C Gemischte Darstellung

Ein Element y, das (bezüglich einer zweistelligen Operation $*$) invers zu x ist (also $x * y = y * x = e$ erfüllt, mit e neutral), bezeichnet man oft mit x^{-1}. Das Symbol $^{-1}$ kann man hier als einstelliges Operationssymbol auffassen, das *immer* in Postfixnotation geschrieben wird. Es ist üblich, die Postfixnotation für $^{-1}$ auch dann anzuwenden, wenn für die anderen Symbole Präfix- oder Infixnotation verwendet wird. Die Terme mit Baumnotation



schreiben wir also $x+y^{-1}$ (Infix, gemischt mit Postfix) bzw. $f(x, y^{-1})$ (Präfix, gemischt mit Postfix).
Ähnliches gilt für manche anderen einstelligen Operationen, wie z.B. die Operation $x \mapsto x^2$.

1.2.D Terme

Im vorigen Abschnitt haben wir öfters den Ausdruck „Term“ verwendet, aber was genau bedeutet das? Statt einer formalen Definition geben wir eine informelle Beschreibung:

1.2.1 Definition. Ein „Term“ (in Präfixnotation) ist ein Ausdruck, der sich in sinnvoller Weise aus Variablen und/oder Operationssymbolen zusammensetzt. Jede Variable ist bereits ein Term; wenn $t_1, \ldots, t_k$ Terme sind und ω ein k-stelliges Operationssymbol ist, dann ist auch der „String“[6]

$$\omega t_1 \cdots t_k$$

wiederum ein Term. Überdies entstehen alle Terme durch wiederholte Anwendung (endlich oft) der gerade genannten Regeln.

Analog kann man einen Term in Postfix- oder Infix-Notation definieren. Auch Terme in Baumdarstellung lassen sich ähnlich beschreiben.

1.3 Einige wichtige Typen von Algebren

1.3.1 Definition. Eine Algebra $(A, \cdot)$ vom Typ (2) heißt ein *Gruppoid*.

Schreibweise: $a \cdot b =: ab, a, b \in A$.

1.3.2 Definition. Ein Gruppoid $(H, \cdot)$ heißt eine *Halbgruppe*[7] $:\Leftrightarrow \cdot$ ist assoziativ.

1.3.3 Beispiel. $(M^M, \circ)$ ist eine Halbgruppe, die so genannte *symmetrische* Halbgruppe von M.

1.3.4 Definition. a) Eine Halbgruppe $(H, \cdot)$ heißt *Monoid* vom Typ (2) $:\Leftrightarrow$ es existiert ein neutrales Element e. (Es kann höchstens ein neutrales Element geben.)

b) Eine Algebra $(H, \cdot, e)$ vom Typ $(2, 0)$ heißt *Monoid* vom Typ $(2, 0) :\Leftrightarrow$ die folgenden Gesetze gelten für alle $x, y, z \in H$:

1) $x(yz) = (xy)z$,

2) $ex = x$, $xe = x$.

Oft sprechen wir einfach von einem Monoid, ohne festzulegen, ob wir nun ein Monoid vom Typ (2) oder ein Monoid vom Typ (2,0) meinen. Dadurch können aber kaum Missverständnisse entstehen, da sich jedes Monoid vom Typ (2) in eindeutiger Weise als Monoid vom Typ (2,0) interpretieren lässt, und umgekehrt.

1.3.5 Definition. a) Ein Monoid $(G, \cdot)$ mit neutralem Element e heißt eine *Gruppe* vom Typ (2) $:\Leftrightarrow$ jedes $x \in G$ ist invertierbar, d. h., $\forall x \in G\ \exists x^{-1} \in G : xx^{-1} = x^{-1}x = e$.

b) Eine Algebra $(G, \cdot, e, {}^{-1})$ vom Typ $(2, 0, 1)$ heißt eine *Gruppe* vom Typ $(2, 0, 1) :\Leftrightarrow$ die folgenden Gesetze gelten für alle $x, y, z \in G$:

1) $x(yz) = (xy)z$,

[6] Wir begnügen uns hier mit der anschaulichen Vorstellung eines Strings oder einer Zeichenkette: Strings bestehen aus Symbolen, die aneinander gereiht werden; Strings können miteinander „verkettet“ werden und ergeben so einen neuen String. Aus der Verkettung von *abc* und *xyz* entsteht *abcxyz*. Wenn wir uns mit freien Halbgruppen beschäftigen, werden wir dieses Konzept noch genauer untersuchen.

[7] englisch: *semigroup*

2) $ex = x$, $xe = x$,

3) $xx^{-1} = e$, $x^{-1}x = e$.

c) Eine Gruppe $(G, \cdot)$ bzw. $(G, \cdot, e, ^{-1})$ heißt *kommutativ* oder *abelsch* $:\Leftrightarrow \forall x, y \in G : xy = yx$.

1.3.6 Anmerkung. $(G, \cdot)$ ist Gruppe $\Leftrightarrow G \neq \emptyset$, $\cdot$ assoziativ und invertierbar.

1.3.7 Definition. a) Eine Algebra $(R, +, \cdot)$ vom Typ $(2, 2)$ heißt ein *Ring* vom Typ $(2, 2)$ $:\Leftrightarrow$

1) $(R, +)$ ist eine abelsche Gruppe,

2) $(R, \cdot)$ ist eine Halbgruppe,

3) $\cdot$ ist distributiv über $+$.

b) Eine Algebra $(R, +, 0, -, \cdot)$ vom Typ $(2, 0, 1, 2)$ heißt ein *Ring* vom Typ $(2, 0, 1, 2)$ $:\Leftrightarrow$

1) $(R, +, 0, -)$ ist eine abelsche Gruppe,

2) $(R, \cdot)$ ist eine Halbgruppe,

3) $\cdot$ ist distributiv über $+$.

Das Element 0 heißt „Nullelement“ des Ringes. Weiters vereinbaren wir die Schreibweise: $x - y := x + (-y)$.

Ähnlich wie bei Monoiden „identifizieren“[8] wir oft eine Gruppe vom Typ (2) mit der entsprechenden Gruppe vom Typ $(2, 0, 1)$, ebenso einen Ring vom Typ $(2, 2)$ mit dem entsprechenden Ring vom Typ $(2, 0, 1, 2)$.

1.3.8 Lemma. *Sei $(R, +, 0, -, \cdot)$ ein Ring. Dann gilt für alle $x, y, z \in R$:*

a) $x0 = 0 = 0x$,

b) $x(-y) = (-x)y = -(xy)$,

c) $(-x)(-y) = xy$,

d) $x(y - z) = xy - xz$, $(x - y)z = xz - yz$.

[8]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)) oder von der Gruppe $(\mathbb{Z}, +, 0, -)$ (vom Typ $(2, 0, 1)$) sprechen. Auch hat eine Gruppe vom Typ (2) dieselben Untergruppen wie die entsprechende Gruppe vom Typ $(2, 0, 1)$.

Allerdings hat die algebraische Struktur $(\mathbb{Z}, +)$ mehr „Unteralgebren“ (siehe Abschnitt 2.1, Seite 25ff) als die Struktur $(\mathbb{Z}, +, 0, -)$, denn die natürlichen Zahlen bilden eine Unteralgebra (=Unterhalbgruppe) von $(\mathbb{Z}, +)$, nicht aber eine Unteralgebra (=Untergruppe) von $(\mathbb{Z}, +, 0, -)$, weil sie ja nicht unter der unären Operation „$-$“ abgeschlossen sind. Wenn es also um Unter*gruppen* geht, dürfen wir $(\mathbb{Z}, +, 0, -)$ mit $(\mathbb{Z}, +)$ „identifizieren“; wenn es um Unter*algebren* geht (was selten der Fall ist), nicht.

Beweis. a) $0 = 0 + 0 \Rightarrow x0 = x(0 + 0) = x0 + x0 \Rightarrow x0 - x0 = x0 + x0 - x0 \Rightarrow 0 = x0$. Analog für $0 = 0x$.

b) $y + (-y) = 0 \Rightarrow xy + x(-y) = x0 = 0 \Rightarrow xy + (-(xy)) + x(-y) = 0 + (-(xy))$ $\Rightarrow x(-y) = -(xy)$. Analog für $(-x)y = -(xy)$.

c) folgt aus b) und $-(-x) = x$.

d) $x(y - z) = x(y + (-z)) = xy + x(-z) = xy + (-(xz)) = xy - xz$. Analog für $(x - y)z = xz - yz$. □

1.3.9 Beispiele. $(\mathbb{Z}, +, 0, -, \cdot)$ und $(M_n(\mathbb{C}), +, 0, -, \cdot)$ sind Ringe.

1.3.10 Definition. a) Eine Algebra $(R, +, 0, -, \cdot, 1)$ vom Typ $(2, 0, 1, 2, 0)$ heißt ein *Ring mit Einselement* (oder auch *unitärer Ring*) :⇔

1) $(R, +, 0, -, \cdot)$ ist ein Ring,

2) 1 ist neutrales Element bezüglich $\cdot$, d. h., $\forall x \in R : 1 \cdot x = x \cdot 1 = x$. (1 heißt „Einselement“ des Ringes.)

b) Ein Ring $(R, +, 0, -, \cdot)$ heißt *kommutativ* :⇔ $\forall x, y \in R : xy = yx$.

c) Eine Algebra $(R, +, 0, -, \cdot, 1)$ heißt ein *kommutativer Ring mit Einselement* :⇔

1) $(R, +, 0, -, \cdot)$ ist ein kommutativer Ring,

2) 1 ist neutrales Element bezüglich $\cdot$.

1.3.11 Beispiel. $(\mathbb{Z}, +, 0, -, \cdot, 1)$ ist kommutativer Ring mit Einselement; ebenso jeder Körper (s. u.).

1.3.12 Definition. Ein kommutativer Ring mit Einselement $(R, +, 0, -, \cdot, 1)$ heißt ein *Integritätsbereich*[9] :⇔

1) $R \setminus \{0\} \neq \emptyset$ (d. h., $0 \neq 1$),

2) $\forall x, y \in R$: Wenn $x \neq 0$ und $y \neq 0$, dann $xy \neq 0$. Oder in äquivalenter Form: Wenn $xy = 0$ ist, dann muss $x = 0$ oder $y = 0$ gelten.

1.3.13 Lemma. *Ist* $(R, +, 0, -, \cdot, 1)$ *ein Integritätsbereich, dann ist* $\cdot$ *regulär auf* $R \setminus \{0\}$.

Beweis. Es seien $x, y, z \neq 0$. Dann gilt: $xy = xz \Rightarrow xy - xz = 0 \Rightarrow x(y - z) = 0 \Rightarrow y - z = 0$ $\Rightarrow y = z$. □

1.3.14 Anmerkung. In einem Integritätsbereich ist $(R \setminus \{0\}, \cdot, 1)$ ein kommutatives Monoid.

1.3.15 Beispiel. $(\mathbb{Z}, +, 0, -, \cdot, 1)$ ist ein Integritätsbereich.

[9] englisch: *integral domain*

1.3.16 Definition. a) Ein Ring mit Einselement $(R, +, 0, -, \cdot, 1)$ heißt ein *Schiefkörper*[10] :⇔

1) $0 \neq 1$,

2) $(R \setminus \{0\}, \cdot)$ ist eine Gruppe.

b) Ein kommutativer Ring mit Einselement $(R, +, 0, -, \cdot, 1)$ heißt ein *Körper*[11] :⇔

1) $0 \neq 1$,

2) $(R \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe.

1.3.17 Beispiele. 1) $(\mathbb{Q}, +, 0, -, \cdot, 1)$, $(\mathbb{R}, +, 0, -, \cdot, 1)$, $(\mathbb{C}, +, 0, -, \cdot, 1)$ sind Körper.

2) Ohne Beweis: Jeder endliche Schiefkörper ist Körper (Satz von Wedderburn).

3) Ist p Primzahl, dann ist $(\mathbb{Z}_p, +, 0, -, \cdot, 1)$ Körper (mit p Elementen). (Zur genauen Definition des Restklassenrings $(\mathbb{Z}_n, +, 0, -, \cdot, 1)$ modulo n siehe Abschnitt 2.2.B)

1.3.18 Anmerkung. $\mathbb{Z}_n$ Körper $\Leftrightarrow$ n prim $\Leftrightarrow$ $\mathbb{Z}_n$ Integritätsbereich. (Siehe Abschnitt 5.3.)

1.3.19 Satz. *Jeder Körper ist ein Integritätsbereich. Jeder endliche Integritätsbereich ist ein Körper.*

Beweis. Die erste Aussage ist klar.

Sei nun $R = \{a_1, \ldots, a_n\}$ endlicher Integritätsbereich $\Rightarrow \cdot$ ist eine assoziative, reguläre Operation auf der endlichen Menge $R \setminus \{0\}$ $\Rightarrow \cdot$ ist invertierbar $\Rightarrow (R \setminus \{0\}, \cdot)$ ist abelsche Gruppe. □

1.3.20 Definition. Sei $(K, +, 0, -, \cdot, 1)$ ein Körper, $I = \{a, b, c\} \cup K$ mit $a, b, c \notin K$, a, b, c paarweise verschieden. Eine Algebra $(V, (\omega_i)_{i \in I})$ vom Typ $(2, 0, 1, (1)_{\lambda \in K})$ heißt *Vektorraum über*[12] K :⇔

1) $(V, \omega_a, \omega_b, \omega_c) =: (V, +, 0, -)$ ist eine abelsche Gruppe,

2) $\forall x, y \in V, \lambda, \mu \in K$:
$\omega_\lambda(x + y) = \omega_\lambda(x) + \omega_\lambda(y)$,
$\omega_{\lambda+\mu}(x) = \omega_\lambda(x) + \omega_\mu(x)$,
$\omega_{\lambda\mu}(x) = \omega_\lambda(\omega_\mu(x))$,
$\omega_1(x) = x$.

Im folgenden schreiben wir statt $\omega_\lambda(x)$ einfach $\lambda \cdot x$ oder nur[13] λx. setzen wir $\omega_\lambda =: \lambda$ und schreiben für den Vektorraum $(V, +, 0, -, K)$. Die Gesetze unter 2) lauten dann: $\lambda(x+y) = \lambda x + \lambda y$, $(\lambda + \mu)x = \lambda x + \mu x$, $(\lambda\mu)x = \lambda(\mu x)$, $1x = x$.

[10] englisch: *skew field oder division ring*
[11] englisch: *field*
[12] englisch: *vector space*
[13] Dadurch wird also eine Abbildung $(\lambda, x) \mapsto \omega_\lambda(x)$ von $K \times V$ nach V definiert, die „Multiplikation mit Skalaren“. Man beachte, dass diese (so genannte „externe“) Verknüpfung zwar ähnlich notiert wird wie die Multiplikation in K, nämlich durch das Symbol $\cdot$ oder durch Nebeneinanderschreiben, aber dennoch keine „Operation“ (in unserem Sinne) auf der Menge V ist, denn Operationen müssen von einer endlichen Potenz von V (z.B. von V oder von V^2) nach V abbilden. In der Gleichung $(\lambda \cdot \mu) \cdot x = \lambda \cdot (\mu \cdot x)$ kommt links zunächst die Operation $\cdot$ des Körpers und dann die externe Verknüpfung vor, rechts zweimal die externe Verknüpfung.

1.4 Die komplexen Zahlen

Es gibt verschiedene Möglichkeiten, die komplexen Zahlen zu definieren; sie führen alle auf isomorphe Strukturen. Im Kapitel 6 werden wir die komplexen Zahlen als Faktorring des Polynomrings $\mathbb{R}[x]$ nach dem von x^2+1 erzeugten Ideal wiederfinden. In diesem Abschnitt skizzieren wir eine Konstruktion, die sich auf Vorkenntnisse aus der linearen Algebra stützt.

1.4.1 Definition. Sei $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ die 2×2-Einheitsmatrix über den reellen Zahlen, und sei $I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

Sei $\mathbb{C} := \{aE + bI \mid a, b \in \mathbb{R}\} = \{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{R}\}$.

Für $a, b \in \mathbb{R}$ nennen wir die Wurzel aus der Determinante von $z := aE + bI$, also die nichtnegative Zahl $\sqrt{a^2+b^2}$, den „absoluten Betrag“ von z, abgekürzt $|z|$. Offenbar gilt $|z| = 0$ genau dann, wenn $z = \mathbf{0}$. Weiters ist $|aE|$ der absolute Betrag (im üblichen Sinn) der reellen Zahl a.

1.4.2 Satz. *1. $\mathbb{C}$ (mit der üblichen Addition und Multiplikation von Matrizen) ist ein Unterring (siehe Abschnitt 2.1) des Rings der 2×2-Matrizen.*

2. Die Nullmatrix $\mathbf{0}$ ist neutral bezüglich Addition, die Matrix E ist neutral bezüglich Multiplikation. Weiters gilt $I^2 = -E$.

3. $\mathbb{C}$ ist Körper; wenn $aE + bI \neq \mathbf{0}$, dann ist $(aE + bI)(aE - bI) = (a^2 + b^2)E$, somit ist $\frac{a}{a^2+b^2}E + \frac{-b}{a^2+b^2}I$ das multiplikative Inverse zu $aE + bI$.

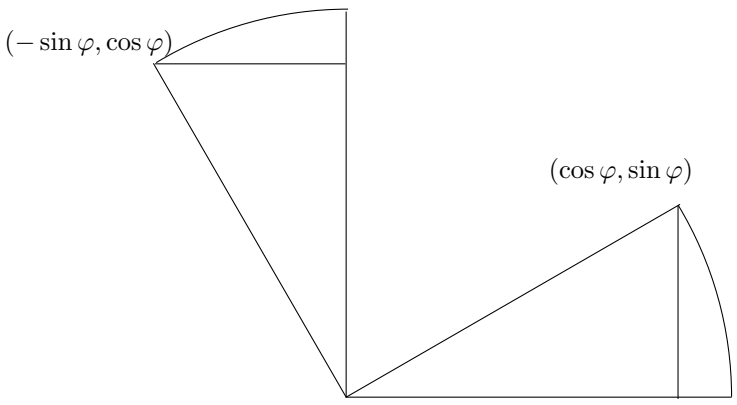
4. Die Abbildung $a \mapsto aE$ ist ein Isomorphismus zwischen $\mathbb{R}$ und einem Unterkörper von $\mathbb{C}$.

Wir schreiben ab jetzt statt $aE + bI$ einfach $a + bi$; das heißt, wir identifizieren ab jetzt jede reelle Zahl a mit der Matrix aE, und wir verwenden für die Matrix I einen Kleinbuchstaben, um von der Tatsache abzulenken, dass I eine Matrix ist, und um zu betonen, dass man mit i wie mit einer Zahl rechnen kann. In dieser Schreibweise übersetzt sich $I^2 = -E$ in $i^2 = -1$.

1.4.3 Satz.

(1) *Der absolute Betrag ist multiplikativ: $|x \cdot y| = |x| \cdot |y|$ für alle $x, y \in \mathbb{C}$.*

(2) *Wenn $|a + bi| = 1$, dann gibt es einen eindeutig bestimmten Winkel $\varphi \in [0, 2\pi)$ mit $a = \cos\varphi$, $b = \sin\varphi$. Die Matrix $aE + bI$, also $\begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}$, stellt in diesem Fall eine Drehung um den Winkel φ dar.*



(3) *Matrizenmultiplikation entspricht einer Hintereinanderausführung von Drehungen, das heißt:* $(\cos\varphi + i\,\sin\varphi) \cdot (\cos\psi + i\,\sin\psi) = \cos(\varphi + \psi) + i\,\sin(\varphi + \psi)$.
Insbesondere ist die Multiplikation auf der Menge $\mathbb{C}$ kommutativ.

(4) *φ verhält sich also wie ein Logarithmus der Zahl $\cos\varphi + i\sin\varphi$. Da die Funktion $f(\varphi) = \cos\varphi + i\sin\varphi$ die Differentialgleichung $f'(\varphi) = -\sin\varphi + i\cos\varphi = i \cdot f(\varphi)$ mit der Anfangsbedingungs $f(0) = 1$ erfüllt — ebenso[14] wie die Funktion $\varphi \mapsto e^{i\varphi}$ — ist die Schreibweise $e^{i\varphi}$ für $\cos\varphi + i\sin\varphi$ sinnvoll.*[15]

(5) *$e^{\frac{\pi}{2}i} = i$, $e^{\pi i} = -1$, $e^{2\pi i} = 1$. Weiters gilt $e^{i\varphi} = e^{i\psi}$ genau dann, wenn die Differenz $\varphi - \psi$ ein ganzzahliges Vielfaches von 2π ist.*

(6) *Jedes Element $z \in \mathbb{C} \setminus \{0\}$ lässt sich eindeutig in der Form $z = r \cdot e^{i\varphi}$ mit $r \in \mathbb{R}$, $r > 0$, $\varphi \in [0, 2\pi)$ darstellen.*
Für die Multiplikation gilt $re^{i\varphi} \cdot se^{i\psi} = (rs) \cdot e^{i(\varphi+\psi)}$.

(7) *Sei $n \geq 1$ eine natürliche Zahl. Dann hat die Gleichung $z^n = 1$ genau n Lösungen in den komplexen Zahlen:*

$$z^n = 1 \;\Leftrightarrow\; z \in \{\, 1 = e^{\frac{2\pi i 0}{n}},\, e^{\frac{2\pi i}{n}},\, \ldots,\, e^{\frac{2\pi i(n-1)}{n}} \,\}.$$

Die Lösungen dieser Gleichungen heißen n-te Einheitswurzeln.

(8) *Sei $s \cdot e^{i\psi}$ eine beliebige komplexe Zahl $\neq 0$, s eine positive reelle Zahl, $\psi \in [0, 2\pi)$. Dann hat die Gleichung $x^n = s\,e^{i\psi}$ genau n Lösungen in $\mathbb{C}$; eine Lösung ist die Zahl $\sqrt[n]{s}\,e^{i\frac{\psi}{n}}$, die weiteren Lösungen erhält man durch Multiplikation dieser Lösung mit den Einheitswurzeln:*

$$x^n = s\,e^{i\psi} \;\Leftrightarrow\; \exists k \in \{0, \ldots, n-1\}\; x = \sqrt[n]{s}\,e^{i\frac{\psi+2\pi k}{n}}.$$

Beweis. (1) ist leicht nachzurechnen. (2) setzen wir als aus der Analysis bekannt voraus.
(3) folgt direkt aus der geometrischen Anschauung oder aus den Additionstheoremen für die trigonometrischen Funktionen.
(5) ergibt sich durch Einsetzen, z.B. $e^{i\pi} = \cos\pi + i\sin\pi = -1 + 0 \cdot i = -1$.
Die Beziehung $e^{i\varphi} = e^{i\psi}$ gilt genau dann, wenn $e^{i\varphi}\,e^{-i\psi} = 1$ ist, also wenn $\cos(\varphi - \psi) = 1$ ist.
(6) Man muss offenbar $r := |z|$ wählen; Existenz und Eindeutigkeit von φ folgt aus (2) und (5).
(7) Jede Lösung der Gleichung $z^n = 1$ in den komplexen Zahlen muss $|z|^n = 1$, also $|z| = 1$ erfüllen, hat also die Form $e^{i\varphi}$. Weiters gilt $z^n = e^{i\varphi n} = 1$, daher muss $i\varphi n$ von der Form $2\pi ik$ mit $k \in \mathbb{Z}$ sein, also $\varphi = \frac{2\pi k}{n}$. Für $\varphi \in [0, 2\pi)$ muss $k \in \{0, \ldots, n-1\}$ gelten.
(8) folgt aus (6) und (7). □

1.5 Äquivalenzrelationen und Klasseneinteilungen

1.5.1 Definition. Für Mengen A, B bezeichnen wir mit $A \times B$ die Menge aller „geordneten Paare“ (a, b), die $a \in A$ und $b \in B$ erfüllen.
Insbesondere ist $A \times A$ die Menge aller geordneten Paare (a, b) mit $a, b \in A$.

Wenn A und B endliche Mengen mit k bzw. n Elementen sind, dann hat $A \times B$ $n \cdot k$ Elemente.

[14] Die Frage, wie diese Funktion definiert ist, und ob die Ableitung erstens existiert und zweitens die üblichen Regeln erfüllt, überlassen wir der Analysis

[15] Je nach Zugang bzw. nach Geschmack kann man die Beziehung $e^{i\varphi} = \cos\varphi + i\sin\varphi$ als abkürzende *Schreibweise*, als wichtige *Eigenschaft* der Exponentialfunktion (die man etwa mit Hilfe der Reihendarstellung beweisen kann) oder als Teil der *Definition* der Exponentialfunktion auf den komplexen Zahlen sehen.

1.5.2 Definition. Ist M eine Menge, dann heißt jede Teilmenge R von $M \times M$ eine *binäre* oder *zweistellige Relation* auf M. (Eine binäre Relation ist also eine Menge von geordneten Paaren.)
Statt $(x, y) \in R$ schreibt man meist xRy.
Eine *einstellige* (*unäre*) Relation ist einfach eine Teilmenge von M.

Spezielle Relationen: $\alpha_M := M \times M$ heißt *Allrelation*, $\iota_M := \{(x, x) \mid x \in M\}$ heißt *identische Relation*, *Gleichheitsrelation* oder *Diagonale*.[16]
Die leere Menge ist eine Relation (auf jeder Menge M).[17]

1.5.3 Definition. Eine Relation $R \subseteq M \times M$ heißt:

1) *reflexiv (auf M)* $:\Leftrightarrow \iota_M \subseteq R$, d. h., $\forall x \in M : xRx$.

2) *symmetrisch* $:\Leftrightarrow \forall x, y \in M : xRy \Rightarrow yRx$.

3) *antisymmetrisch* $:\Leftrightarrow \forall x, y \in M : (xRy \text{ und } yRx) \Rightarrow x = y$.

4) *transitiv* $:\Leftrightarrow \forall x, y, z \in M : (xRy \text{ und } yRz) \Rightarrow xRz$.

Eine Relation mit 1), 2) und 4) heißt *Äquivalenzrelation*, eine mit 1), 3) und 4) *Halbordnung* oder *partielle Ordnung*.

1.5.4 Beispiele. α_M und ι_M sind stets Äquivalenzrelationen. $\leq$ auf $\mathbb{R}$, $\subseteq$ auf $\mathfrak{P}(M)$ und $|$ („teilt“) auf $\mathbb{N}$ sind Halbordnungen.

Für Äquivalenzrelationen verwenden wir meistens die griechischen Buchstaben θ, π, ρ, σ, oder aber Symbole wie $\sim$, $\equiv$, $\approx$, etc. Die Symbole sind vor allem dann praktisch, wenn wir die Äquivalenzrelation als *Prädikat* betrachten, also uns dafür interessieren, welche Elemente zu einander in Relation stehen: $a \sim b$, $a \not\sim c$, etc. Buchstaben sind hingegen dann typographisch passender, wenn wir uns für die Äquivalenzrelationen als *Objekte* und für die Beziehungen zwischen diesen Relationen interessieren, z.B. $\theta \neq \omega_A$, $\rho \subseteq \sigma$, etc.
Wenn θ eine Äquivalenzrelation auf der Menge M ist, a ein Element von M, dann nennen wir die Menge

$$[a]_\theta := \{x \in M \mid x \,\theta\, a\}$$

die „(Äquivalenz-)Klasse von a“. Statt $[a]_\theta$ schreibt man manchmal nur $[a]$, manchmal auch a/θ.

1.5.5 Definition. Sei M eine Menge. $\mathcal{P} \subseteq \mathfrak{P}(M)$ heißt *Klasseneinteilung* oder *Partition* $:\Leftrightarrow$

1) $\bigcup_{C \in \mathcal{P}} C = M$,

2) $\emptyset \notin \mathcal{P}$,

3) $A, B \in \mathcal{P} \Rightarrow A = B$ oder $A \cap B = \emptyset$ (d. h., die Mengen in $\mathcal{P}$ sind paarweise disjunkt).

Die Elemente der Partition P (die also alle nichtleere Teilmengen von M sein müssen) heißen *Klassen* von P.

[16] Die Allrelation bezeichnet man manchmal auch mit ω_A oder ∇_A, die Gleichheitsrelation mit „=“ oder Δ_A.

[17] Der leeren Menge wird entweder keine Stelligkeit zugeordnet, oder aber eine Stelligkeit, die sich aus dem Kontext ergibt. Gelegentlich wird auch zwischen der „einstelligen“ leeren Menge $\emptyset \subseteq M$ und der „zweistelligen“ leeren Menge $\emptyset \subseteq M^2$ unterschieden.

1.5.6 Satz. *Sei π Äquivalenzrelation auf der Menge M, $a \in M$ und $M/\pi := \{[a]_\pi \mid a \in M\}$ die Menge aller Äquivalenzklassen bezüglich π. (M/π heißt auch* Faktor- *oder* Quotientenmenge *von M nach π.)*
Dann ist M/π Klasseneinteilung von M.

Ist umgekehrt $\mathcal{P}$ eine Klasseneinteilung von M und π definiert durch $a \,\pi\, b :\Leftrightarrow \exists C \in \mathcal{P} : a, b \in C$, dann ist π eine Äquivalenzrelation auf M, und es gilt $M/\pi = \mathcal{P}$.

$\pi \mapsto M/\pi$ ist eine bijektive Abbildung von der Menge aller Äquivalenzrelationen von M auf die Menge aller Klasseneinteilungen von M. Die Umkehrabbildung ist gegeben durch obige Vorschrift $\mathcal{P} \mapsto \pi$.

Beweis. Übungsaufgabe. □

1.5.7 Satz. *Seien M, N Mengen, $f : M \to N$ eine Abbildung und $x \,\pi_f\, y :\Leftrightarrow f(x) = f(y)$. Dann gilt:*

a) π_f ist eine Äquivalenzrelation auf M, genannt der Kern von f.

b) Die Abbildung

$$\begin{cases} M/\pi_f \to f(M) := \{f(x) \mid x \in M\} \subseteq N \\ [x]_{\pi_f} \mapsto f(x) \end{cases}$$

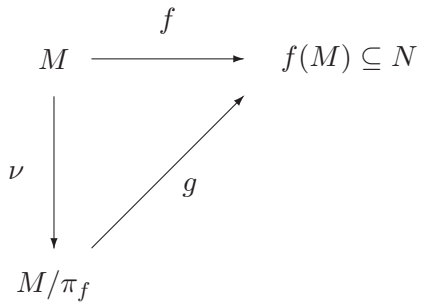
ist wohldefiniert und bijektiv.

Umgekehrt gilt: Sei θ eine beliebige Äquivalenzrelation auf M. Dann gibt es eine Menge N (nämlich M/θ) und eine Abbildung $f : M \to N$ (die so genannte kanonische Abbildung) sodass $\theta = \pi_f$.

Kurz gesagt: Jede Abbildung induziert eine Äquivalenzrelation, ihren Kern; umgekehrt wird jede Äquivalenzrelation durch ihre kanonische Abbildung induziert.

Beweis. Übungsaufgabe. □

1.5.8 Anmerkung. Der in obigem Satz beschriebene Sachverhalt lässt sich durch das folgende *kommutative Diagramm* veranschaulichen:



Hier ist

$$\nu : \begin{cases} M \to M/\pi_f \\ x \mapsto [x]_{\pi_f} \end{cases}$$

die *kanonische* oder *natürliche* Abbildung und g die Abbildung

$$\begin{cases} M/\pi_f \to f(M) \\ [x]_{\pi_f} \mapsto f(x). \end{cases}$$

Es gilt: $f = g \circ \nu$.

1.6 Partielle Ordnungen und Verbände

1.6.1 Definition. Eine „partielle Ordnung“ ist eine Menge P zusammen mit einer zweistelligen Relation R auf P, die antisymmetrisch, transitiv und reflexiv ist (siehe 1.5.3).

Für die Relation R verwendet man meistens eines der Symbole $\leq$, $\sqsubseteq$, $\precsim$, ...; damit ergibt sich die übliche Schreibweise $x \leq y$ (statt $(x, y) \in \leq$ oder $\leq(x, y)$).

1.6.2 Definition. Sei $(P, \leq)$ partielle Ordnung, $A \subseteq P$, $s \in P$. s heißt *obere Schranke* für A, wenn $a \leq s$ für alle $a \in A$ gilt. s heißt „*größtes Element* von A“, wenn s erstens obere Schranke für A und zweitens sogar Element von A ist.
Analog sind die Begriffe „*untere Schranke*“ und „*kleinstes Element*“ definiert.
Die kleinste obere Schranke einer Menge A (so etwas muss nicht existieren; es kann zum Beispiel sein, dass A gar keine obere Schranken hat, oder auch, dass die Menge der oberen Schranken kein kleinstes Element hat) nennen wir $\sup A$. Die größte untere Schranke heißt $\inf A$.

Man beachte: Eine obere Schranke für A kann (muss aber nicht) in A liegen. Weiters gilt: Jedes Element $s \in P$ ist obere Schranke für die leere Menge, und jede einelementige Menge ist (durch ihr einziges Element) beschränkt.

1.6.3 Beispiel. Sei $P = \{1, 2, 3, 4, 6\}$. Die Relation

$$| \;:=\; \{(1,1),(2,2),(3,3),(4,4),(6,6)\} \cup \{(1,2),(1,3),(1,4),(1,6),\ (2,4),(2,6),(3,6)\},$$

die man üblicherweise als „Teilbarkeitsrelation“ bezeichnet, ist eine partielle Ordnung auf P. Bezüglich dieser Ordnung gilt: Die Menge $\{1, 2\}$ ist nach oben beschränkt, sowohl durch 2 als auch durch 4 als auch durch 6. (2 ist die kleinste aller dieser oberen Schranken.)
Die einzige (und daher auch kleinste) obere Schranke der Menge $\{2, 3\}$ ist die Zahl 6.
Die Menge $\{3, 4\}$ hat keine obere Schranke.

1.6.4 Definition. Sei $(P, \leq)$ partielle Ordnung. P heißt „*Verband*“,[18,19] wenn jede zweielementige Teilmenge von P sowohl eine kleinste obere als auch eine größte untere Schranke hat.
Schreibweise: $x \vee y := \sup\{x, y\}$. $x \wedge y := \inf\{x, y\}$.
P heißt *vollständiger Verband*, wenn jede Teilmenge von P sowohl eine kleinste obere als auch eine größte untere Schranke hat.

1.6.5 Satz. *Sei P eine partielle Ordnung, in der jede Teilmenge eine größte untere Schranke hat. Dann hat in P auch jede Teilmenge eine kleinste obere Schranke.*

Beweis. Übungsaufgabe. □

1.6.6 Beispiel. Sei X eine Menge, und sei V eine Familie von Teilmengen von X, die unter beliebigen Schnitten abgeschlossen ist, mit $X \in V$. Dann ist $(V, \subseteq)$ ein vollständiger Verband, denn für jede[20] Teilmenge $T \subseteq V$ ist $Z := \bigcap T := \bigcap_{Y \in T} Y$ in V. Nach Definition ist Z untere Schranke für T (d.h., $Z \subseteq Y$ für alle $Y \in T$, und es ist auch klar, dass Z die größte untere Schranke ist.
Konkrete Beispiele für diese Situation: V könnte die Menge aller Untergruppen einer Gruppe sein (siehe Abschnitt 2.1) oder die Menge aller abgeschlossenen Teilmengen eines topologischen oder metrischen Raums auf der Grundmenge X.

[18] englisch: *lattice*

[19] Genauer: Verband im ordnungstheoretischen Sinn. Später werden wir eine algebraische Version dieser Definition kennenlernen.

[20] Für $T = \emptyset$ definieren wir $\bigcap T := X$; mit dieser Definition treffen die nun folgenden Überlegungen auch auf diesen Fall zu.

1.7 Grundbegriffe der Gruppentheorie

1.7.1 Definition. Sei $(G, \cdot)$ ein Gruppoid, $a_1, \ldots, a_n \in G$ $(n \in \mathbb{N})$, dann ist das *Produkt* $a_1 \cdots a_n$ induktiv definiert durch $a_1 \cdots a_n := (a_1 \cdots a_{n-1})a_n$.

1.7.2 Beispiel. $a_1a_2a_3a_4 = (a_1a_2a_3)a_4 = ((a_1a_2)a_3)a_4$.

1.7.3 Definition. Sei $(G, \cdot)$ ein Gruppoid, $a \in G$, dann sind die *Potenzen*[21] von a definiert durch: $a^1 := a$, $a^{n+1} := (a^n)a$ $(n \in \mathbb{N})$.

1.7.4 Anmerkungen. 1) Beim Rechnen mit Produkten in einer Halbgruppe dürfen Klammern beliebig eingeführt werden. (Übungsbeispiel)

2) In einer kommutativen Halbgruppe gilt: $a_1 \cdots a_n = a_{\pi(1)} \cdots a_{\pi(n)}$, wann immer π eine Permutation der Menge $M = \{1, \ldots, n\}$ ist.

1.7.5 Satz. *Sei $(G, \cdot, e, {}^{-1})$ eine Gruppe, $a, b \in G$. Dann gilt $(ab)^{-1} = b^{-1}a^{-1}$.*

Beweis. $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = a(ea^{-1}) = aa^{-1} = e$. □

1.7.6 Folgerung. $(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$ (Induktion nach n).

1.7.7 Definition. Sei $(G, \cdot, e, {}^{-1})$ eine Gruppe, $a \in G$. Für $n \in \mathbb{N}$ sei a^n wie oben definiert. Weiters sei $a^0 := e$ und $a^{-n} := (a^{-1})^n$, $n \in \mathbb{N}$.

1.7.8 Satz (Rechenregeln für Potenzen in Gruppen)**.** *Für alle $a, b \in G$, $n, m \in \mathbb{Z}$ gilt:*

a) $a^n a^m = a^{n+m}$,

b) $(a^m)^n = a^{mn}$,

c) $(ab)^n = a^n b^n$, *falls $\cdot$ kommutativ ist.*

Beweis. Durch Fallunterscheidungen. Z. B. b) für $n > 0$:

$$(a^m)^n = \underbrace{a^m \cdots a^m}_{n \text{ mal}} = a^{\overbrace{m+\cdots+m}^{n \text{ mal}}} = a^{nm}.$$

□

1.7.9 Anmerkung. Diese Regeln gelten für $m, n \in \mathbb{N}$ auch in Halbgruppen.

1.7.10 Definition. Sei $(G, \cdot, e, {}^{-1})$ eine Gruppe, $a \in G$. Dann heißt

$$|\{a^0 = e, a^1, a^{-1}, a^2, a^{-2}, \ldots\}| = |\{a^k \mid k \in \mathbb{Z}\}|$$

die *Ordnung*[22] *von* a, symbolisch $\mathrm{o}(a)$.

1.7.11 Anmerkung. $\mathrm{o}(a) \in \mathbb{N}$ oder $\mathrm{o}(a) = |\mathbb{N}| = \aleph_0 (= \infty)$.

1.7.12 Beispiele. 1) In $(\mathbb{Z}, +, 0, -)$ schreiben wir (ebenso wie in allen Gruppen, bei denen „+“ als Operationszeichen verwendet wird) na anstelle von a^n. Die obigen Rechenregeln lauten dann: (i) $ma + na = (m + n)a$, (ii) $n(ma) = (mn)a$, (iii) $n(a + b) = na + nb$. („Additive Schreibweise“.) Es gilt $\mathrm{o}(0) = 1$, $\mathrm{o}(k) = \infty$ für alle $k \in \mathbb{Z}$, $k \neq 0$. (In jeder Gruppe gilt $\mathrm{o}(e) = 1$.)

[21] englisch: *power*
[22] englisch: *order*

2) In der Gruppe $(\mathbb{C} \setminus \{0\}, \cdot, 1, ^{-1})$ gilt: $o(1) = 1$, $o(-1) = 2$, $o(i) = o(-i) = 4$.

1.7.13 Anmerkung. Die additive Schreibweise $(G, +, 0, -)$ wird meist nur für kommutative Gruppen verwendet, die multiplikative Schreibweise $(G, \cdot, 1, ^{-1})$ für beliebige Gruppen.

1.7.14 Definition. Sei $(G, \cdot, e, ^{-1})$ eine Gruppe. Dann heißt $|G|$ (die Mächtigkeit von G) die *Ordnung* der Gruppe. Allgemeiner heißt für eine Algebra $(A, (\omega_i)_{i \in I})$ die Mächtigkeit $|A|$ die *Ordnung* der Algebra.

Für alle $a \in G$ gilt: $o(a) \leq |G|$.

1.7.15 Lemma (Division mit Rest)**.**

$$\forall k, l \in \mathbb{Z} : \Big(l \neq 0 \Rightarrow \exists q, r \in \mathbb{Z} : 0 \leq r < |l| \text{ und } k = lq + r \Big).$$

Beweis. Wir betrachten zunächst den Fall $k \geq 0$, $l > 0$. Die Menge

$$\{n \in \mathbb{N}_0 \mid l \cdot n \leq k\}$$

kann nur Zahlen $n \leq k$ enthalten (weil für $n > k$ auch $l \cdot n > k$ gilt). Daher ist diese Menge endlich (und sicher nicht leer), hat also ein maximales Element $q := \max\{n \in \mathbb{N}_0 \mid l \cdot n \leq k\}$. Dann ist $l \cdot q \leq k < l \cdot (q + 1)$, also $0 \leq k - lq < l$. Sei $r := k - lq$, dann ist $k = lq + r$ mit $0 \leq r < l$.

Die anderen Fälle ($k < 0$, und/oder $l < 0$) können auf den ersten Fall zurückgeführt werden. Wenn zum Beispiel $k < 0$ und $l > 0$ gilt, dann können wir das Ergebnis des ersten Falls auf $-k$ und l anwenden und erhalten $-k = lq + r$; wenn $r = 0$ ist, dann erhalten wir die Darstellung $k = -lq = lq' + r'$ mit $q' := -q$, $r' := 0$; wenn $0 < r < l$, dann erhalten wir $k = -lq - r = l(-q - 1) + l - r = lq' + r'$ mit $q' := -q - 1$, $r' := l - r$. □

1.7.16 Definition. Für $n \in \mathbb{N}_0$, $r, s \in \mathbb{Z}$ ist $r \equiv s \bmod n$ („r kongruent s modulo n“) :⇔ $n|(r - s)$ (n teilt $(r - s)$).

Es gilt: 1) $r \equiv s \bmod n \Leftrightarrow r = s + kn$, $k \in \mathbb{Z} \Leftrightarrow r, s$ haben denselben Rest bei Division durch n.

2) $\equiv \bmod n$ ist eine Äquivalenzrelation (siehe später).

1.7.17 Satz. *Sei $(G, \cdot, e, ^{-1})$ eine Gruppe und $a \in G$.*

a) Ist $o(a) = \infty$, so sind die Potenzen von a paarweise verschieden.

b) Ist $o(a) = n \in \mathbb{N}$, dann gilt $n = \min\{m \in \mathbb{N} \mid a^m = e\}$ und $\{a^k \mid k \in \mathbb{Z}\} = \{a^0 = e, a^1, \ldots, a^{n-1}\}$. Weiters ist $a^r = a^s \Leftrightarrow r \equiv s \bmod n$.

Beweis. a) Sei $o(a) = \infty$. Annahme: $\exists r, s \in \mathbb{Z} : r > s$ und $a^r = a^s$. Für $m := r - s \in \mathbb{N}$ gilt dann $a^m = e$. Sei $k \in \mathbb{Z}$. Dann ist $k = mq + l$ mit $q \in \mathbb{Z}$, $l \in \mathbb{N}_0$ und $0 \leq l < m$. Daraus folgt $a^k = a^{mq+l} = (a^m)^q a^l = e^q a^l = a^l$, also $\{a^k \mid k \in \mathbb{Z}\} = \{e, a, \ldots, a^{m-1}\}$. Widerspruch!

b) Ist $o(a) = n \in \mathbb{N}$, dann gibt es nach a) ein $m \in \mathbb{N}$ mit $a^m = e$, und weiters gilt $\{a^k \mid k \in \mathbb{Z}\} = \{e, a, \ldots, a^{m-1}\}$. Sei $n_0 = \min\{m \in \mathbb{N} \mid a^m = e\}$. Dann ist $a^{n_0} = e$ und $n \leq n_0$. Die Elemente $e, a, \ldots, a^{n_0-1}$ sind paarweise verschieden. Denn wäre dies nicht der Fall, also $a^r = a^s$ für $0 \leq s < r < n_0$, dann würde gelten $a^{r-s} = e$ für $0 < r - s < n_0$

— Widerspruch zur Minimalität von n_0. Also gilt auch $n \geq n_0$ und damit $n = n_0$. Es gilt somit $\{a^k \mid k \in \mathbb{Z}\} = \{e, a, \ldots, a^{n-1}\}$.

Wir zeigen nun noch $a^r = a^s \Leftrightarrow r \equiv s \bmod n$.

$\Rightarrow$: $a^r = a^s$, $r > s \Rightarrow a^{r-s} = e$, $r - s > 0$, $r - s = nq + l$, $0 \leq l < n \Rightarrow e = a^{r-s} = (a^n)^q a^l = e^q a^l = a^l \Rightarrow l = 0 \Rightarrow r - s = nq \Rightarrow r \equiv s \bmod n$.
$\Leftarrow$: $r \equiv s \bmod n \Rightarrow r - s = nq \Rightarrow a^{r-s} = a^{nq} = (a^n)^q = e \Rightarrow a^r = a^s$. □

1.7.18 Beispiel. Sei M Menge und $S_M := \{f : M \to M \mid f \text{ bijektiv}\}$. $(S_M, \circ, \mathrm{id}_M, {}^{-1})$ ist eine Gruppe, die *symmetrische Gruppe auf* M (Übungsbeispiel). Die Elemente von S_M heißen auch *Permutationen* von M. Ist $M = \{1, 2, \ldots, n\}$, schreibt man S_n anstelle von S_M. Es gilt: $|S_n| = n!$. So ist z. B.

$$S_3 = \left\{ \begin{pmatrix} 1\,2\,3 \\ 1\,2\,3 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 3\,1\,2 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 1\,3\,2 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 3\,2\,1 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix} \right\},$$

in *Zyklenschreibweise*:

$$S_3 = \{(1), (123), (132), (23), (13), (12)\}.$$

Die geraden Permutationen bilden die *alternierende* Gruppe A_n. So ist z. B.

$$A_3 = \{(1), (123), (132)\}.$$

(Zur Definition von geraden und ungeraden Permutationen siehe die Vorlesung „Lineare Algebra I“.)

Die Ordnungen der Elemente der S_3:

π	$\mathrm{o}(\pi)$
(1)	1
(123)	3
(132)	3
(23)	2
(13)	2
(12)	2

Es gilt: Jedes Element der S_n lässt sich als Produkt elementfremder Zyklen darstellen. Diese Darstellung ist bis auf die Reihenfolge der Zyklen eindeutig. Z. B. besitzt die Permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 9 & 8 & 5 & 4 & 1 & 3 & 2 & 7 \end{pmatrix}$$

aus der S_9 die Zyklendarstellung $(16)(29738)(45)$. Es ist $\mathrm{o}(\pi) = 2 \cdot 5 = \mathrm{kgV}(2, 5, 2)$. Allgemein: Ein Zyklus der Länge k hat die Ordnung k. Die Ordnung eines Produkts elementfremder Zyklen ist das kleinste gemeinsame Vielfache der Ordnungen der Faktoren.

Kapitel 2

Grundlegende algebraische Methoden

2.1 Unteralgebren

2.1.1 Definition. Sei A eine Menge, $\omega : A^n \to A$ eine n-stellige Operation auf A ($n \in \mathbb{N}_0$), $T \subseteq A$, dann heißt T *abgeschlossen* bezüglich $\omega :\Leftrightarrow \omega(T^n) \subseteq T$ (d. h., $t_1, \ldots, t_n \in T \Rightarrow \omega t_1 \ldots t_n \in T$; im Fall $n = 0$: $\omega \in T$).

2.1.2 Definition. Sei $\mathfrak{A} = (A, (\omega_i)_{i\in I})$ eine Algebra vom Typ $(n_i)_{i\in I}$, $T \subseteq A$, dann heißt T *abgeschlossen* bezüglich $(\omega_i)_{i\in I} :\Leftrightarrow T$ abgeschlossen bezüglich ω_i für alle $i \in I$. In diesem Fall wird durch $\omega_i^* x_1 \ldots x_{n_i} := \omega_i x_1 \ldots x_{n_i}$, $(x_1, \ldots, x_{n_i}) \in T^{n_i}$, eine n_i-stellige Operation ω_i^* auf T definiert: $\omega_i^* = \omega_i \restriction T^{n_i}$. Die Algebra $(T, (\omega_i^*)_{i\in I})$ heißt dann eine *Unteralgebra* von $\mathfrak{A}$. Meist schreiben wir: $\omega_i^* =: \omega_i$, das heißt, wir identifizieren[1] die Operation ω_i mit ihrer Einschränkung ω_i^*.

2.1.3 Anmerkung. Oft heißt auch nur die Menge T selbst eine Unteralgebra von $\mathfrak{A}$.

2.1.A Unteralgebren spezieller algebraischer Strukturen

1) Sei $(H, \cdot)$ eine Halbgruppe. $T \subseteq H$ ist eine Unteralgebra von $(H, \cdot) \Leftrightarrow (x, y \in T \Rightarrow xy \in T)$. Es ist dann $\cdot = \cdot \restriction T \times T$ eine binäre Operation auf T, und $(T, \cdot)$ ist eine Halbgruppe, denn das Assoziativgesetz gilt in H und damit erst recht in T. (Allgemein: Wenn in einer Algebra eine Operation ein *Gesetz* erfüllt, so hat die auf eine Unteralgebra eingeschränkte Operation natürlich auch diese Eigenschaft.)

$(T, \cdot)$ heißt *Unterhalbgruppe* von $(H, \cdot)$.

2) Sei $(G, \cdot)$ eine Gruppe vom Typ (2) und $(T, \cdot)$ Unterhalbgruppe von $(G, \cdot)$. Dann ist im allgemeinen $(T, \cdot)$ *keine* Gruppe!

2.1.4 Beispiel. $(G, \cdot) = (\mathbb{Z}, +)$, $(T, \cdot) = (\mathbb{N}, +)$.

3) Sei $(G, \cdot, e, {}^{-1})$ eine Gruppe vom Typ $(2, 0, 1)$. $T \subseteq G$ ist Unteralgebra

$$\Leftrightarrow \left\{ \begin{array}{l} x, y \in T \Rightarrow xy \in T \\ e \in T \\ x \in T \Rightarrow x^{-1} \in T \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} T \neq \emptyset \\ x, y \in T \Rightarrow xy^{-1} \in T \end{array} \right\}.$$

[1] Siehe Fußnote auf Seite 14.

Da die definierenden Gesetze einer Gruppe vom Typ $(2,0,1)$ in G und damit auch in T gelten, ist die Unteralgebra $(T,\cdot,e,^{-1})$ wieder eine Gruppe, genannt *Untergruppe* von $(G,\cdot,e,^{-1})$.

4) Ist $(R,+,0,-,\cdot)$ ein Ring vom Typ $(2,0,1,2)$, dann ist jede Unteralgebra $(T,+,0,-,\cdot)$ wieder ein Ring, genannt *Unterring* von $(R,+,0,-,\cdot)$. Dies gilt nicht für Ringe vom Typ $(2,2)$.

2.1.5 Beispiel. $(\mathbb{N},+,\cdot)$ ist Unter*algebra* von $(\mathbb{Z},+,\cdot)$, aber nicht Unter*ring*.

5) Sei $(K,+,0,-,\cdot,1)$ ein Körper vom Typ $(2,0,1,2,0)$ und $(T,+,0,-,\cdot,1)$ eine Unteralgebra (d. h. ein Unterring mit demselben Einselement). Ist $(T,+,0,-,\cdot,1)$ selbst ein Körper, so heißt dieser ein *Unterkörper* von $(K,+,0,-,\cdot,1)$. Es gilt: T ist Unterkörper

$$\Leftrightarrow \begin{cases} x,y\in T \Rightarrow x+y\in T \\ 0\in T \\ x\in T \Rightarrow -x\in T \\ x,y\in T \Rightarrow xy\in T \\ 1\in T \\ x\in T, x\neq 0 \Rightarrow x^{-1}\in T. \end{cases}$$

2.1.6 Beispiel. $(\mathbb{R},+,0,-,\cdot,1)$ ist Unterkörper von $(\mathbb{C},+,0,-,\cdot,1)$, aber $(\mathbb{Z},+,0,-,\cdot,1)$ ist *kein* Unterkörper.

6) Sei $(V,+,0,-,K)$ ein Vektorraum über K und $(T,+,0,-,K)$ eine Unteralgebra, d. h.,

$$\begin{array}{l} x,y\in T \Rightarrow x+y\in T \\ 0\in T \\ x\in T \Rightarrow -x\in T \\ \lambda\in K, x\in T \Rightarrow \lambda x\in T. \end{array}$$

Dann ist auch $(T,+,0,-,K)$ ein Vektorraum über K, genannt ein *Unter-(Vektor-)Raum*.

7) Betrachten wir das Monoid $M=(\{0,1\},\cdot)$. Jede Teilmenge von $\{0,1\}$ (insbesondere also auch die leere Menge) ist eine Unterhalbgruppe der Halbgruppe $(\{0,1\},\cdot)$. Die Unterhalbgruppen $(\{0\},\cdot)$, $(\{1\},\cdot)$ und natürlich $(\{0,1\},\cdot)$ sind überdies Monoide. Allerdings bezeichnen wir nur die Unterhalbgruppen $(\{1\},\cdot)$ und $(\{0,1\},\cdot)$ als *Untermonoide*, weil nur diese dasselbe neutrale Element wie M haben. Wenn wir von Untermonoiden eines Monoids M sprechen, interpretieren wir M immer als Monoid vom Typ $(2,0)$.

2.1.7 Satz. *Sei (A,Ω) eine Algebra und $(T_j)_{j\in J}$ eine Familie von Unteralgebren. Dann ist $\bigcap_{j\in J} T_j$ ebenfalls eine Unteralgebra.*

2.1.8 Anmerkung. Der in diesem Satz auftretende allgemeine Durchschnitt ist definiert durch $\bigcap_{j\in J} T_j := \{\, x\in A \mid \forall j\in J : x\in T_j \,\}$. Für $J=\emptyset$ ist $\bigcap_{j\in J} T_j = A$.

Beweis. Sei $\Omega=(\omega_i)_{i\in I}$, ω_i eine n_i-stellige Operation und $T:=\bigcap_{j\in J} T_j$. Sei $i\in I$ mit $n_i>0$, und seien $x_1,\ldots,x_{n_i}\in T$. Dann gilt: $\forall j\in J : x_1,\ldots,x_{n_i}\in T_j \Rightarrow \omega_i x_1\ldots x_{n_i}\in T_j$ $\Rightarrow \omega_i x_1\ldots x_{n_i}\in T$. Für $n_i=0$ gilt: $\forall j\in J:\omega_i\in T_j\Rightarrow\omega_i\in T$. □

2.1.9 Satz. *Sei (A,Ω) eine Algebra und $S\subseteq A$, dann ist*

$$\langle S\rangle := \bigcap\{T \mid T\supseteq S \text{ und } T \text{ ist Unteralgebra von } (A,\Omega)\}$$

die kleinste *Unteralgebra von (A,Ω), die S enthält.*
($\langle S\rangle$ ist der Abschluss von S unter allen Operationen in Ω, siehe 1.1.E.)

2.1.10 Definition. $\langle S\rangle$ heißt die *von S erzeugte Unteralgebra* von (A,Ω). S heißt ein *Erzeugendensystem* von $\langle S\rangle$.

2.1.11 Satz. *Sei $(G,\cdot,e,^{-1})$ eine Gruppe, $x\in G$, $S=\{x\}$ dann gilt:*

$$\langle x\rangle := \langle S\rangle = \{x^k \mid k\in\mathbb{Z}\}.$$

Beweis. Zu zeigen: $\langle x\rangle = \{x^k \mid k\in\mathbb{Z}\} =: T$.
$\subseteq$: T ist eine Untergruppe von $(G,\cdot,e,^{-1})$, denn seien $x^k, x^l \in T$, $k,l\in\mathbb{Z}$. Dann gilt: $x^k x^l = x^{k+l}\in T$ (wegen $k+l\in\mathbb{Z}$); $x^0\in T$ (wegen $0\in\mathbb{Z}$); $(x^k)^{-1}=x^{-k}\in T$ (wegen $-k\in\mathbb{Z}$). Weiters gilt $x=x^1\in T$, also $\{x\}\subseteq T$, woraus $\langle x\rangle\subseteq T$ folgt.
$\supseteq$: Sei U eine Untergruppe von $(G,\cdot,e,^{-1})$ mit $\{x\}\subseteq U$, d. h., $x\in U$. Dann gilt: $x^n\in U$ $(n\in\mathbb{N})$, $e=x^0\in U$, $x^{-n}=(x^n)^{-1}\in U \Rightarrow T\subseteq U \Rightarrow T\subseteq\langle x\rangle$. □

2.1.12 Definition. $\langle x\rangle$ heißt die *von x erzeugte Untergruppe* von $(G,\cdot,e,^{-1})$.

2.1.13 Anmerkungen. 1. Analog gilt[2] für Vektorräume:

$$\langle\{x_1,\ldots,x_n\}\rangle = \{\sum_{1\le i\le n}\lambda_i x_i \mid \lambda_1,\ldots,\lambda_n\in K\}.$$

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:

$$\langle\{x_1,\ldots,x_n\}\rangle = \{k_1x_1+k_2x_2+\cdots+k_nx_n \mid k_i\in\mathbb{Z} \text{ für alle } i\}.$$

3. Für *nichtabelsche* Gruppen gilt z. B.:

$$\langle\{x_1,x_2\}\rangle = \{x_1^{k_{11}}x_2^{k_{12}}x_1^{k_{21}}x_2^{k_{22}}\cdots x_1^{k_{n1}}x_2^{k_{n2}} \mid n\in\mathbb{N},\ k_{ij}\in\mathbb{Z}\}.$$

4. Allgemein gilt:

$$\langle\{x_1,\ldots,x_n\}\rangle = \{t(x_1,\ldots,x_n) \mid t \text{ ist ein beliebiger } n\text{-stelliger } \textit{Term} \text{ in der Algebra } (A,\Omega)\}.$$

2.1.14 Definition. Eine Gruppe $(G,\cdot,e,^{-1})$ heißt *zyklisch* $:\Leftrightarrow \exists x\in G: G=\langle x\rangle$. x heißt dann *erzeugendes Element.*

2.1.15 Lemma. *Sei $(G,\cdot,e,^{-1})$ eine zyklische Gruppe und $\langle x\rangle = G$. Dann gibt es zwei Fälle:*

a) Ist $\mathrm{o}(x)=\infty$*, dann ist auch G unendlich, und es gilt $G=\{e,x,x^{-1},x^2,x^{-2},\ldots\}$.*

b) Ist $\mathrm{o}(x)=n\in\mathbb{N}$*, dann ist $|G|=n$, und es gilt $G=\{e,x,x^2,\ldots,x^{n-1}\}$.*

In beiden Fällen sind die angeführten Potenzen paarweise verschieden.

2.1.16 Beispiel. Zu a): Für $(\mathbb{Z},+,0,-)$ gilt $\mathbb{Z}=\langle 1\rangle=\langle -1\rangle$.

Zu b): Für $(\mathbb{Z}_m,+,0,-)$ (Operationen modulo m, siehe Abschnitt 2.4) gilt $\mathbb{Z}_m=\langle 1\rangle=\langle k\rangle$ mit $\mathrm{ggT}(m,k)=1$ (Übungsbeispiel).

[2]Die leere Summe $\sum_{i\in\{\}} x_i$ 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: $\langle\{\}\rangle=\{0\}$.

2.1.B Nebenklassenzerlegung einer Gruppe nach einer Untergruppe

Bezeichnung: Falls kein Irrtum möglich ist, setzen wir im folgenden häufig $G := (G, \cdot, e, ^{-1})$ bzw. $G := (G, \cdot)$, d. h., wir bezeichnen eine Gruppe mit demselben Symbol wie ihre Grundmenge. In weiterer Folge wird dies auch für Ringe getan.

2.1.17 Satz. *Sei $(G, \cdot, e, ^{-1})$ eine Gruppe und $(H, \cdot, e, ^{-1})$ eine Untergruppe von G. Sei weiters π auf G definiert durch $x \,\pi\, y :\Leftrightarrow x^{-1}y \in H$, $x, y \in G$. Dann ist π eine Äquivalenzrelation auf G.*

Beweis. 1) π ist reflexiv: $\forall x : x \,\pi\, x$, denn $x^{-1}x = e \in H$.
2) π ist symmetrisch: $x \,\pi\, y \Rightarrow x^{-1}y \in H \Rightarrow (x^{-1}y)^{-1} = y^{-1}x \in H \Rightarrow y \,\pi\, x$.
3) π ist transitiv: $x \,\pi\, y$, $y \,\pi\, z \Rightarrow x^{-1}y \in H$, $y^{-1}z \in H \Rightarrow (x^{-1}y)(y^{-1}z) = x^{-1}z \in H \Rightarrow x \,\pi\, z$. □

2.1.18 Anmerkung. Analog gilt: durch $x \varrho y :\Leftrightarrow xy^{-1} \in H$ ist ebenfalls eine Äquivalenzrelation auf G definiert.

2.1.19 Definition (Komplexprodukt)**.** Sei $(G, \cdot, e, ^{-1})$ Gruppe, $A, B \subseteq G$. Dann heißt $AB := \{ab \mid a \in A, b \in B\}$ das *Komplexprodukt* von A und B.
Spezialfälle: $A = \{a\}$: $AB =: aB = \{ab \mid b \in B\}$, $B = \{b\}$: $AB =: Ab = \{ab \mid a \in A\}$.
Für eine Untergruppe H von G heißt aH eine *Linksnebenklasse* von G nach H und Ha eine *Rechtsnebenklasse* von G nach H ($a \in G$ fest, aber beliebig).

2.1.20 Lemma. *Sei G Gruppe, $H \subseteq G$, $a \in G$.*
Dann gilt für alle $x \in G$: $ax \in aH \Leftrightarrow x \in H$.
Weiters gilt für alle $y \in G$: $y \in aH \Leftrightarrow a^{-1}y \in H$.

Beweis. Wenn $x \in H$ ist, dann ist (nach Definition von aH) $ax \in aH$. Wenn umgekehrt $ax \in aH$ ist, muss $ax = ah$ für ein $h \in H$ gelten; durch Multiplikation mit a^{-1} (oder: weil die Gruppenmultiplikation regulär ist) erhalten wir $x = h \in H$.
Für die zweite Folgerung schreiben wir $y = aa^{-1}y = ax$ mit $x := a^{-1}y$.
Dann gilt $y \in aH \Leftrightarrow ax \in aH \Leftrightarrow x \in H \Leftrightarrow a^{-1}y \in H$. □

2.1.21 Satz. *Seien π, ϱ die oben definierten Äquivalenzrelationen. Dann gilt für alle $a \in G$: $[a]_\pi = aH$ (also $b \,\pi\, a \Leftrightarrow b \in aH$) und $[a]_\varrho = Ha$.*

Beweis. $b \in [a]_\pi \Leftrightarrow a \,\pi\, b \Leftrightarrow a^{-1}b \in H \Leftrightarrow b \in aH$.

Der Beweis von $[a]_\varrho = Ha$ verläuft analog. □

2.1.22 Folgerung. $\{aH \mid a \in G\}$ ist eine Klasseneinteilung von G, genannt *Linksnebenklassenzerlegung* von G nach H. Entsprechend nennt man $\{Ha \mid a \in G\}$ die *Rechtsnebenklassenzerlegung* von G nach H.

2.1.23 Beispiel. $G = S_3 = \{(1), (123), (132), (12), (23), (13)\}$, $H = \{(1), (23)\}$.

$(1)H{=}H$	$H(1){=}H$
$(123)H{=}\{(123), (12)\}$	$H(123){=}\{(123), (13)\}$
$(132)H{=}\{(132), (13)\}$	$H(132){=}\{(132), (12)\}$

Im allgemeinen gilt also $Ha \neq aH$! Für $a = e$ gilt jedoch stets $He = eH = H$. In abelschen Gruppen gilt $Ha = aH$ für alle $a \in G$.

2.1.24 Satz. *Sei $(G, \cdot, e, ^{-1})$ eine Gruppe, H eine Untergruppe, $a, b \in G$, dann ist durch*

$$i : \begin{cases} aH \to bH \\ ax \mapsto bx \end{cases}$$

eine bijektive Abbildung definiert.

Beweis. 1) i ist wohldefiniert: $ax_1 = ax_2 \Rightarrow x_1 = x_2$.
2) i ist injektiv: $i(ax_1) = i(ax_2) \Rightarrow bx_1 = bx_2 \Rightarrow x_1 = x_2$.
3) i ist surjektiv: jedes $bx \in bH$ ist Bild von $ax \in aH$. □

2.1.25 Folgerung. $\forall a, b \in G : |aH| = |bH| = |H|$. (Analog: $\forall a \in G : |Ha| = |H|$.)

2.1.26 Satz. *Durch $aH \mapsto Ha^{-1}$, $a \in G$, ist eine bijektive Abbildung φ von der Linksnebenklassenzerlegung auf die Rechtsnebenklassenzerlegung von G nach H definiert.*

Beweis. 1) φ ist wohldefiniert: $aH = bH \Rightarrow a \,\pi\, b \Rightarrow a^{-1}b \in H \Rightarrow a^{-1} \varrho b^{-1} \Rightarrow Ha^{-1} = Hb^{-1}$.
2) φ ist surjektiv: $\forall a \in G : \varphi(a^{-1}H) = Ha$.
3) φ ist injektiv: $\varphi(aH) = \varphi(bH) \Rightarrow Ha^{-1} = Hb^{-1} \Rightarrow a^{-1} \varrho b^{-1} \Rightarrow a^{-1}b \in H \Rightarrow a \,\pi\, b \Rightarrow aH = bH$. □

2.1.27 Definition. Die Anzahl aller verschiedenen Linksnebenklassen (Rechtsnebenklassen) von G nach H heißt der *Index von H in G*, in Zeichen: $[G : H] := |\{aH \mid a \in G\}| = |\{Ha \mid a \in G\}|$.

2.1.28 Satz (von Lagrange)**.** *Sei $(G, \cdot, e, ^{-1})$ eine endliche Gruppe, H eine Untergruppe, dann gilt:*

$$[G : H] \cdot |H| = |G|.$$

2.1.29 Anmerkung. Der Satz von Lagrange gilt auch für unendliche Gruppen.

2.1.30 Folgerung. a) $|H|$ teilt $|G|$.

b) $x \in G \Rightarrow \mathrm{o}(x) = |\{x^n \mid n \in \mathbb{Z}\}| = |\langle x \rangle|$ teilt $|G|$. „Die Ordnung jedes Elements ist Teiler der Gruppenordnung."

c) $|G| = p$ Primzahl, H Untergruppe $\Rightarrow H = \{e\}$ oder $H = G$. Für $x \in G$, $x \neq e$, ist daher $\langle x \rangle = G$, also G zyklisch.

2.2 Isomorphismen und Homomorphismen

2.2.1 Definition. Seien $\mathfrak{A} = (A, (\omega_i)_{i \in I})$ und $\mathfrak{A}^* = (A^*, (\omega_i^*)_{i \in I})$ Algebren vom selben Typ $(n_i)_{i \in I}$. Eine Abbildung $f : A \to A^*$ heißt *Homomorphismus von $\mathfrak{A}$ nach $\mathfrak{A}^*$* :⇔

1) für $i \in I$ mit $n_i > 0$ gilt $\forall x_1, \ldots, x_{n_i} \in A : f(\omega_i x_1 \ldots x_{n_i}) = \omega_i^* f(x_1) \ldots f(x_{n_i})$,

2) für $i \in I$ mit $n_i = 0$ gilt $f(\omega_i) = \omega_i^*$.

2.2.2 Lemma. *Seien $(G, \cdot, e, ^{-1})$ und $(H, \cdot, e, ^{-1})$ Gruppen, $f : G \to H$. Dann gilt: f ist Homomorphismus von $(G, \cdot, e, ^{-1})$ nach $(H, \cdot, e, ^{-1})$ ⇔ f ist Homomorphismus von $(G, \cdot)$ nach $(H, \cdot)$.*

Beweis. ⇒: trivial.
⇐: Voraussetzung: $f(xy) = f(x)f(y)$. Zu zeigen: $f(e) = e$, $f(x^{-1}) = (f(x))^{-1}$.
$ee = e \Rightarrow f(e)f(e) = f(e) \Rightarrow f(e) = e$.
$xx^{-1} = e \Rightarrow f(x)f(x^{-1}) = f(e) = e = f(x)(f(x))^{-1} \Rightarrow f(x^{-1}) = (f(x))^{-1}$. □

2.2.3 Folgerung. 1) Seien $\mathfrak{V} = (V, +, 0, -, K)$ und $\mathfrak{W} = (W, +, 0, -, K)$ Vektorräume über demselben Körper K und $f : V \to W$. Dann gilt: f ist Homomorphismus von $\mathfrak{V}$ nach $\mathfrak{W} \Leftrightarrow$ f ist lineare Abbildung, d. h., $\forall x, y \in V : f(x + y) = f(x) + f(y)$, $\forall \lambda \in K, x \in V : f(\lambda x) = \lambda f(x)$.
2) Seien $(R, +, 0, -, \cdot)$ und $(S, +, 0, -, \cdot)$ Ringe, $f : R \to S$, dann gilt: f ist Homomorphismus von $(R, +, 0, -, \cdot)$ nach $(S, +, 0, -, \cdot) \Leftrightarrow f$ ist Homomorphismus von $(R, +, \cdot)$ nach $(S, +, \cdot)$.

2.2.4 Definition. 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 $f : A \to A^*$ ein Homomorphismus von $\mathfrak{A}$ nach $\mathfrak{A}^*$. f heißt

1) *Isomorphismus*, falls f bijektiv (in diesem Fall sagt man: $\mathfrak{A}$ ist *isomorph* zu $\mathfrak{A}^*$, in Zeichen: $\mathfrak{A} \cong \mathfrak{A}^*$),

2) *Endomorphismus*, falls $\mathfrak{A} = \mathfrak{A}^*$,

3) *Automorphismus*, falls $\mathfrak{A} = \mathfrak{A}^*$ und f Isomorphismus,

4) *Epimorphismus*, falls f surjektiv (in diesem Fall heißt $\mathfrak{A}^*$ *homomorphes Bild* von $\mathfrak{A}$),

5) *Monomorphismus*, falls f injektiv (in diesem Fall heißt $\mathfrak{A}$ *isomorph eingebettet in* $\mathfrak{A}^*$).

2.2.5 Lemma. *a) Seien $\mathfrak{A}$, $\mathfrak{A}^*$, $\mathfrak{A}^{**}$ Algebren vom selben Typ, f Homomorphismus von $\mathfrak{A}$ nach $\mathfrak{A}^*$, g Homomorphismus von $\mathfrak{A}^*$ nach $\mathfrak{A}^{**}$. Dann ist $g \circ f$ Homomorphismus von $\mathfrak{A}$ nach $\mathfrak{A}^{**}$. Sind f, g beide Isomorphismen, so ist auch $g \circ f$ ein Isomorphismus.*

b) Ist f Isomorphismus von $\mathfrak{A}$ nach $\mathfrak{A}^*$, so ist f^{-1} Isomorphismus von $\mathfrak{A}^*$ nach $\mathfrak{A}$.

Beweis. Übung. □

Bilder und (vollständige) Urbilder von Unteralgebren bei Homomorphismen sind wieder Unteralgebren (Übung). (Ist $f : A \to A^*$ Abbildung, $U^* \subseteq A^*$, so heißt $f^{-1}(U^*) := \{x \in A \mid f(x) \in U^*\}$ *vollständiges Urbild* von U^*.)

2.2.A Homomorphismen und Gesetze

2.2.6 Satz. *Sei $(H, \cdot)$ eine Halbgruppe, $(H^*, \cdot)$ ein Gruppoid und $f : H \to H^*$ ein Homomorphismus. Dann ist die Unteralgebra $(f(H), \cdot)$ von $(H^*, \cdot)$ eine Halbgruppe.*

Beweis. Seien $x, y, z \in f(H)$. Dann gibt es $a, b, c \in H$ mit $f(a) = x$, $f(b) = y$ und $f(c) = z$. Da $(H, \cdot)$ Halbgruppe, gilt $a(bc) = (ab)c$ und damit $f(a)(f(b)f(c)) = (f(a)f(b))f(c)$, also $x(yz) = (xy)z$. □

2.2.7 Anmerkung. Seien $(A, (\omega_i)_{i\in I})$ und $(A^*, (\omega_i^*)_{i\in I})$ Algebren vom selben Typ, $f : A \to A^*$ ein Epimorphismus (d. h., A^* ist homomorphes Bild von A). Gilt mit geeigneten Termen t_1, t_2 in A eine Gleichung (ein Gesetz) $\forall a, b, c, \ldots : t_1(a, b, c, \ldots) = t_2(a, b, c, \ldots)$, so ist wegen $t_1(f(a), f(b), f(c), \ldots) = f(t_1(a, b, c, \ldots)) = f(t_2(a, b, c, \ldots)) = t_2(f(a), f(b), f(c), \ldots)$ das Gesetz auch in A^* gültig. Die Terme sind dabei aus endlich vielen Variablen und Operationssymbolen (für A bzw. A^*) aufgebaut.

2.2.8 Anmerkung. Ist $(A, (\omega_i)_{i\in I})$ Algebra, so nennt man $(\omega_i)_{i\in I}$ die *fundamentalen* Operationen, Terme dagegen *abgeleitete* Operationen.

Interpretation des letzten Satzes: Jedes homomorphe Bild einer Halbgruppe ist eine Halbgruppe. Analog zeigt man: Jedes homomorphe Bild
1) einer (abelschen) Gruppe ist eine (abelsche) Gruppe,
2) eines (kommutativen) Ringes ist ein (kommutativer) Ring,
3) eines Ringes mit Einselement ist ein Ring mit Einselement,
4) eines Verbandes ist ein Verband[3],
5) einer Booleschen Algebra ist eine Boolesche Algebra,
6) eines Vektorraumes über K ist ein Vektorraum über K.

Sei $(A, \cdot)$, $A = \{a_1, \ldots, a_n\}$, ein Gruppoid, $(A^*, \circ)$ ein weiteres Gruppoid mit $|A^*| = n$, $f : A \to A^*$ Isomorphismus, $A^* = \{a_1^*, \ldots, a_n^*\}$ mit $a_i^* = f(a_i)$, $1 \leq i \leq n$. Die Operationstafeln der beiden Algebren sehen dann so aus:

$\cdot$	a_1	$\ldots$	a_n
a_1	a_1a_1	$\ldots$	a_1a_n
$\vdots$	$\vdots$	$\ddots$	$\vdots$
a_n	a_na_1	$\ldots$	a_na_n

$\circ$	a_1^*	$\ldots$	a_n^*
a_1^*	$a_1^* \circ a_1^*$	$\ldots$	$a_1^* \circ a_n^*$
$\vdots$	$\vdots$	$\ddots$	$\vdots$
a_n^*	$a_n^* \circ a_1^*$	$\ldots$	$a_n^* \circ a_n^*$

Ist (links) $a_ia_j = a_k$ so ist (rechts) $a_i^* \circ a_j^* = a_k^*$. Vom Standpunkt der Algebra ist daher ein Isomorphismus lediglich eine „Umbezeichnung“. Isomorphe Algebren sind „als gleich zu betrachten“.

Algebraische Eigenschaften sind solche, die bei Isomorphismen erhalten bleiben. So sind etwa alle Gesetze algebraische Eigenschaften, da sie nach obiger Anmerkung sogar bei Epimorphismen erhalten bleiben.

Oft ist es möglich, algebraische Strukturen „bis auf Isomorphie“ zu charakterisieren. So sind z. B. alle endlich-dimensionalen Vektorräume über K bis auf Isomorphie gegeben durch K^n, $n \in \mathbb{N}_0$ (mit den üblichen Operationen). Analoge Aussagen werden wir für endliche Körper und endliche Boolesche Algebren kennenlernen. Ein weiteres Ergebnis in diese Richtung ist der folgende

2.2.9 Satz (Darstellungssatz von Cayley)**.** *Sei $(G, \cdot, e, ^{-1})$ eine Gruppe, dann ist G isomorph zu einer Untergruppe der symmetrischen Gruppe $(S_G, \circ, \mathrm{id}_G, ^{-1})$.*
Kurz: *Jede Gruppe ist isomorph zu einer Permutationsgruppe.*

Beweis. Wir konstruieren eine Einbettung (Monomorphismus) $\pi : G \to S_G$, $a \mapsto \pi_a$, auf folgende Weise:

$$\forall g \in G : \pi_a(g) := ag.$$

1) $\pi_a \in S_G$, d. h., π_a ist injektiv und surjektiv (injektiv: $\pi_a(g_1) = \pi_a(g_2) \Rightarrow ag_1 = ag_2 \Rightarrow g_1 = g_2$; surjektiv: $h \in G \Rightarrow h = \pi_a(a^{-1}h)$).
2) π ist injektiv: $\pi_{a_1} = \pi_{a_2} \Rightarrow \pi_{a_1}(e) = \pi_{a_2}(e) \Rightarrow a_1e = a_2e \Rightarrow a_1 = a_2$.
3) $\pi_{ab} = \pi_a \circ \pi_b$: $\pi_{ab}(g) = (ab)g = a(bg) = \pi_a(bg) = \pi_a(\pi_b(g)) = (\pi_a \circ \pi_b)(g)$. □

2.2.10 Anmerkung. Ein analoger Satz gilt auch für Monoide.

[3]Verbände und Boolesche Algebren werden wir in einem späteren Kapitel als algebraische Strukturen kennen lernen.

2.2.B Kongruenzrelationen und Faktoralgebren

2.2.11 Definition. Sei $\mathfrak{A} = (A, (\omega_i)_{i\in I})$ eine Algebra vom Typ $(n_i)_{i\in I}$; weiters sei π Äquivalenzrelation auf A. π heißt *Kongruenz(relation)* auf $\mathfrak{A} :\Leftrightarrow$
für alle $i \in I$ mit $n_i > 0$, $a_1, \dots, a_{n_i}, b_1, \dots, b_{n_i} \in A$ gilt:

$$a_1 \,\pi\, b_1, \dots, a_{n_i} \,\pi\, b_{n_i} \Rightarrow \omega_i a_1 \dots a_{n_i} \,\pi\, \omega_i b_1 \dots b_{n_i}.$$

2.2.12 Beispiel. Sei $\mathfrak{A} = (\mathbb{Z}, +, 0, -, \cdot, 1)$ der Integritätsbereich der ganzen Zahlen und $n \in \mathbb{N}_0$ fest (n heißt Modul). π sei definiert durch:

$$a \,\pi\, b :\Leftrightarrow \exists c \in \mathbb{Z} : a - b = cn, \qquad a, b \in \mathbb{Z}.$$

Im folgenden schreiben wir — wie bereits in Abschnitt 1.3 — $a \equiv b \bmod n$ anstelle von $a \,\pi\, b$. Es gilt: $\equiv \bmod n$ ist Kongruenzrelation, denn:
1) $\equiv \bmod n$ ist Äquivalenzrelation: $a \equiv a \bmod n$ wegen $a - a = 0 = 0n$; $a \equiv b \bmod n \Rightarrow a - b = cn \Rightarrow b - a = (-c)n \Rightarrow b \equiv a \bmod n$; $a \equiv b \bmod n$ und $b \equiv c \bmod n \Rightarrow a - b = d_1 n$ und $b - c = d_2 n \Rightarrow a - c = (d_1 + d_2)n \Rightarrow a \equiv c \bmod n$.
2) Operation $+$: $a_1 \equiv b_1 \bmod n$ und $a_2 \equiv b_2 \bmod n \Rightarrow a_1 - b_1 = c_1 n$ und $a_2 - b_2 = c_2 n \Rightarrow (a_1 + a_2) - (b_1 + b_2) = (c_1 + c_2)n \Rightarrow (a_1 + a_2) \equiv (b_1 + b_2) \bmod n$.
3) Operation $-$: $a \equiv b \bmod n \Rightarrow a - b = cn \Rightarrow (-a) - (-b) = (-c)n \Rightarrow (-a) \equiv (-b) \bmod n$.
4) Operation $\cdot$: $a_1 \equiv b_1 \bmod n$ und $a_2 \equiv b_2 \bmod n \Rightarrow a_1 = b_1 + c_1 n$ und $a_2 = b_2 + c_2 n \Rightarrow a_1 a_2 = b_1 b_2 + (b_1 c_2 + b_2 c_1 + c_1 c_2 n)n \Rightarrow a_1 a_2 \equiv b_1 b_2 \bmod n$.

Zugehörige Klasseneinteilung: Es ist $[a] = \{a + kn \mid k \in \mathbb{Z}\}$. Für $n = 0$ gilt $[a] = \{a\}$ für alle $a \in \mathbb{Z}$ ($\equiv \bmod n$ ist dann die Gleichheitsrelation). Für $n \neq 0$ gilt: $\mathbb{Z}_n := \mathbb{Z}/\equiv \bmod n = \{[a] \mid a \in \mathbb{Z}\} = \{[0], \dots, [n-1]\}$.

2.2.13 Satz. *Sei $\mathfrak{A} = (A, (\omega_i)_{i\in I})$ eine Algebra und π eine Kongruenz auf $\mathfrak{A}$. Dann sind durch*

$$\omega_i^*[a_1]_\pi \dots [a_{n_i}]_\pi := [\omega_i a_1 \dots a_{n_i}]_\pi, \quad n_i > 0,\ a_1, \dots, a_{n_i} \in A,$$
$$\omega_i^* := [\omega_i]_\pi, \quad n_i = 0,$$

Operationen auf der Quotientenmenge A/π definiert.

Beweis. Die Operationen sind wohldefiniert:[4]

$$\left.\begin{array}{c} [a_1]_\pi = [b_1]_\pi \\ \vdots \\ [a_{n_i}]_\pi = [b_{n_i}]_\pi \end{array}\right\} \Rightarrow \left\{\begin{array}{c} a_1 \pi b_1 \\ \vdots \\ a_{n_i} \pi b_{n_i} \end{array}\right\} \Rightarrow \omega_i a_1 \dots a_{n_i} \pi \omega_i b_1 \dots b_{n_i}.$$

Daher ist $[\omega_i a_1 \dots a_{n_i}]_\pi = [\omega_i b_1 \dots b_{n_i}]_\pi$. □

[4] Was heißt es, dass eine Funktion wohldefiniert ist? Wenn wir eine Funktion f auf einer Menge X 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 tatsächlich für jede Eingabe x ein Resultat $t(x)$ ausgibt.
Wenn wir aber f durch eine Formel

$$(*) \qquad f(t_1(x)) := t_2(x)$$

definieren, enthält diese „Definition“ implizit die Behauptung, dass es tatsächlich eine Funktion gibt, die jedem Element der Form $t_1(x)$ das Element $t_2(x)$ zuordnet. Notwendig und hinreichend für die Gültigkeit dieser Behauptung ist die Implikation

$$(**) \qquad \forall x, y\ (t_1(x) = t_1(y) \Rightarrow t_2(x) = t_2(y)).$$

Wenn wir also eine Funktion f durch eine Vorschrift $(*)$ definieren, müssen wir uns immer erst vergewissern, dass $(**)$ erfüllt ist.

2.2.14 Definition. Die so erhaltene Algebra $\mathfrak{A}/\pi := (A/\pi, (\omega_i^*)_{i\in I})$ heißt *Faktoralgebra* von $\mathfrak{A}$ nach der Kongruenz π. Oft setzt man $\omega_i := \omega_i^*$.

2.2.15 Beispiel. $\mathfrak{A} = (\mathbb{Z}, +, 0, -, \cdot, 1)$, $\pi = \equiv \bmod n$. Die Faktoralgebra $\mathfrak{A}/\pi$ ist dann gegeben durch $(\mathbb{Z}_n, +^*, 0^*, -^*, \cdot^*, 1^*)$ mit $[a]+^*[b] = [a+b]$, $0^* = [0]$, $-^*[a] = [-a]$, $[a]\cdot^*[b] = [ab]$, $1^* = [1]$ (d. h., man rechnet mit den Repräsentanten der Klassen). Im folgenden wird „*“ bei den Operationen weggelassen. Es gilt (siehe folgender Satz): $(\mathbb{Z}_n, +, 0, -, \cdot, 1)$ ist ein kommutativer Ring mit Einselement, genannt der *Restklassenring modulo n*.

2.2.16 Satz. *Sei $\mathfrak{A} = (A, (\omega_i)_{i\in I})$ eine Algebra, π eine Kongruenz auf $\mathfrak{A}$. Dann ist die Abbildung*

$$\nu : \begin{cases} A \to A/\pi \\ a \mapsto [a]_\pi \end{cases}$$

ein surjektiver Homomorphismus von $\mathfrak{A}$ auf $\mathfrak{A}/\pi$, der so genannte natürliche Homomorphismus.

Beweis.

$$\nu(\omega_i a_1 \dots a_{n_i}) = [\omega_i a_1 \dots a_{n_i}]_\pi = \omega_i [a_1]_\pi \dots [a_{n_i}]_\pi = \omega_i \nu(a_1) \dots \nu(a_{n_i}), \quad n_i > 0,$$
$$\nu(\omega_i) = [\omega_i]_\pi = \omega_i, \quad n_i = 0.$$

□

2.2.17 Folgerung. a) $\mathfrak{A}/\pi$ ist ein homomorphes Bild von $\mathfrak{A}$.

b) Jedes Gesetz, welches in $\mathfrak{A}$ gilt, gilt auch in $\mathfrak{A}/\pi$, insbesondere ist also

i) jede Faktoralgebra einer Halbgruppe eine Halbgruppe,

ii) jede Faktoralgebra einer (abelschen) Gruppe eine (abelsche) Gruppe,

iii) jede Faktoralgebra eines Vektorraumes ein Vektorraum (vgl. den Begriff „Quotientenraum“ aus der Linearen Algebra),

iv) jede Faktoralgebra eines (kommutativen) Ringes ein (kommutativer) Ring,

v) jede Faktoralgebra eines Ringes mit Einselement ein Ring mit Einselement,

vi) jede Faktoralgebra eines Verbandes (bzw. einer Booleschen Algebra) ein Verband (bzw. eine Boolesche Algebra).

2.2.18 Anmerkung. Eine Faktoralgebra eines Integritätsbereiches braucht kein Integritätsbereich zu sein, wie das Beispiel $(\mathbb{Z}_n, +, 0, -, \cdot, 1)$ zeigt.

2.2.19 Satz (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 $f : A \to A^*$ ein Homomorphismus. Dann ist der Kern π_f eine Kongruenz auf $\mathfrak{A}$, und es gibt* genau einen *injektiven Homomorphismus g von $\mathfrak{A}/\pi_f$ nach $\mathfrak{A}^*$, sodass $f = g \circ \nu$ (ν ist die natürliche Abbildung).*

Beweis. 1) π_f ist eine Äquivalenzrelation, und es gibt eine injektive Abbildung $g : A/\pi_f \to A^*$ mit $f = g \circ \nu$ (siehe Abschnitt 1.5).

2) π_f ist Kongruenz: Sei $i \in I$, $n_i > 0$. Wir haben:

$$\left.\begin{matrix} a_1 \pi_f b_1 \\ \vdots \\ a_{n_i} \pi_f b_{n_i} \end{matrix}\right\} \Rightarrow \left\{\begin{matrix} f(a_1) = f(b_1) \\ \vdots \\ f(a_{n_i}) = f(b_{n_i}) \end{matrix}\right\} \Rightarrow \omega_i^* f(a_1) \dots f(a_{n_i}) = \omega_i^* f(b_1) \dots f(b_{n_i})$$

$\Rightarrow f(\omega_i a_1 \dots a_{n_i}) = f(\omega_i b_1 \dots b_{n_i})$ (f Homomorphismus!) $\Rightarrow \omega_i a_1 \dots a_{n_i}\ \pi_f\ \omega_i b_1 \dots b_{n_i}$. Die Eindeutigkeit von g ist trivial: $g([a]_{\pi_f}) = g(\nu(a)) = (g \circ \nu)(a) = f(a)$.

3) g ist ein Homomorphismus: Sei $i \in I$, $n_i > 0$, dann gilt:

$$\begin{aligned} &g(\omega_i [a_1]_{\pi_f} \dots [a_{n_i}]_{\pi_f}) = g([\omega_i a_1 \dots a_{n_i}]_{\pi_f}) = f(\omega_i a_1 \dots a_{n_i}) \\ &= \omega_i^* f(a_1) \dots f(a_{n_i}) = \omega_i^* g([a_1]_{\pi_f}) \dots g([a_{n_i}]_{\pi_f}). \end{aligned}$$

Analog gilt für $n_i = 0$: $g(\omega_i) = g([\omega_i]_{\pi_f}) = f(\omega_i) = \omega_i^*$. □

2.2.20 Folgerung. Für die Unteralgebra $(f(A), (\omega_i^*)_{i\in I})$ von $\mathfrak{A}^*$ gilt $(f(A), (\omega_i^*)_{i\in I}) \cong \mathfrak{A}/\pi_f$, also ist jedes homomorphe Bild einer Algebra isomorph zu einer Faktoralgebra.

2.2.21 Anmerkung. Die Gleichheitsrelation $\iota = \{(x, x) \mid x \in A\}$ und die Allrelation $\alpha = A \times A$ sind stets Kongruenzen auf $\mathfrak{A}$, genannt die *trivialen* Kongruenzen auf $\mathfrak{A}$. Es gilt: $\mathfrak{A}/\iota \cong \mathfrak{A}$ und $|\mathfrak{A}/\alpha| \leq 1$. $\mathfrak{A}/\iota$ und $\mathfrak{A}/\alpha$ sind die *trivialen* Faktoralgebren.

2.2.22 Definition. Eine Algebra $\mathfrak{A}$ heißt *einfach*[5], wenn sie nur die trivialen Kongruenzen besitzt.

2.2.23 Anmerkung. Die Algebra $\mathfrak{A}$ ist einfach genau dann, wenn sie nur *triviale* homomorphe Bilder hat (d. h., jeder Homomorphismus $h : A \to B$ ist entweder konstant oder injektiv).

2.2.C Kongruenzrelationen auf Gruppen

2.2.24 Satz. *Sei $(G, \cdot, e, ^{-1})$ eine Gruppe und π eine Äquivalenzrelation auf G. Dann gilt:*

a) π ist Kongruenz auf $(G, \cdot, e, ^{-1}) \Leftrightarrow \pi$ ist Kongruenz auf $(G, \cdot)$.

b) Ist π Kongruenz auf $(G, \cdot)$ und $[e]_\pi =: N$, dann gilt:

i) N ist Untergruppe von $(G, \cdot, e, ^{-1})$.

ii) $xNx^{-1} = \{xnx^{-1} \mid n \in N\} \subseteq N$ für alle $x \in G$.

iii) $x\pi y \Leftrightarrow x^{-1}y \in N$ für alle $x, y \in G$ (d. h., $[x]_\pi = xN$ für alle $x \in G$).

Beweis. a) $\Rightarrow$: trivial. $\Leftarrow$:

$$\left.\begin{matrix} x\pi y \\ x^{-1}\pi x^{-1} \end{matrix}\right\} \Rightarrow \left\{\begin{matrix} e = xx^{-1}\pi yx^{-1} \\ y^{-1}\pi y^{-1} \end{matrix}\right\} \Rightarrow y^{-1}\pi y^{-1} yx^{-1} = x^{-1}.$$

b) i) $e \in N$ wegen $e\pi e$. $x, y \in N \Rightarrow x\pi e$ und $y\pi e \Rightarrow xy\pi ee = e \Rightarrow xy \in N$.
$x \in N \Rightarrow x\pi e \Rightarrow x^{-1}\pi e^{-1} = e \Rightarrow x^{-1} \in N$.
ii) $y \in N \Rightarrow y\pi e \Rightarrow xyx^{-1}\pi xex^{-1} = e \Rightarrow xyx^{-1} \in N$.
iii) $\Rightarrow$: $x\pi y \Rightarrow e = x^{-1}x\pi x^{-1}y \Rightarrow x^{-1}y \in N$.
$\Leftarrow$: $x^{-1}y \in N \Rightarrow x^{-1}y\pi e \Rightarrow y = xx^{-1}y\pi xe = x$. □

2.2.25 Lemma. *Sei $(G, \cdot, e, ^{-1})$ Gruppe und $x \in G$. Dann ist die Abbildung*[6]

$$\varphi_x : \left\{\begin{matrix} G \to G \\ g \mapsto xgx^{-1} \end{matrix}\right.$$

ein Automorphismus von $(G, \cdot, e, ^{-1})$, genannt ein innerer *Automorphismus von G. Wir nennen diese Abbildung* Konjugation *mit x.*

[5] englisch: *simple*

[6] Statt $\varphi_{x^{-1}}(g)$ schreibt man oft g^x. In dieser Schreibweise gilt dann: $(g^x)^y = g^{xy}$.

Beweis. Übung. □

2.2.26 Anmerkung. Die Eigenschaft ii) in obigem Satz ist dann gleichbedeutend mit: $\varphi_x(N) \subseteq N$ für alle $x \in G$.

2.2.27 Definition. Zwei Elemente $g, h \in G$ heißen „konjugiert“ zu einander, wenn es ein x mit $x^{-1}gx = h$ gibt; Konjugiertheit ist offenbar eine Äquivalenzrelation.

2.2.28 Definition. Sei N eine Untergruppe von $(G, \cdot, e, ^{-1})$, dann heißt N eine *invariante* Untergruppe oder ein *Normalteiler*[7] von G:$\Leftrightarrow xNx^{-1} \subseteq N$ für alle $x \in G$.
Statt „U ist Untergruppe von G“ schreiben wir $U \leq G$; die Notation $N \lhd G$ bedeutet, dass U Normalteiler von G ist.

2.2.29 Anmerkung. In einer abelschen Gruppe ist jede Untergruppe Normalteiler. Für nicht abelsche Gruppen ist dies nicht der Fall. Z. B. gibt es Untergruppen der S_3, die nicht Normalteiler sind, nämlich: $\{(1), (12)\}$, $\{(1), (13)\}$ und $\{(1), (23)\}$.

2.2.30 Lemma. *Für eine Untergruppe N einer Gruppe G sind folgende Aussagen äquivalent:*

a) N ist Normalteiler von G.

b) $\forall x \in G : \varphi_x(N) = N$.

c) $\forall x \in G : xNx^{-1} = N$.

d) $\forall x \in G : Nx = xN$, d. h., Rechtsnebenklasse = Linksnebenklasse.

Beweis. a) $\Rightarrow$ b): N Normalteiler $\Rightarrow \forall x \in G : xNx^{-1} \subseteq N \Rightarrow \forall x \in G : x^{-1}Nx \subseteq N \Rightarrow$
$\forall x \in G : N = xx^{-1}Nxx^{-1} \subseteq xNx^{-1} \Rightarrow \forall x \in G : \varphi_x(N) = xNx^{-1} = N$. □

b) $\Rightarrow$ a) und b) $\Leftrightarrow$ c) sind trivial.

c) $\Leftrightarrow$ d): $xNx^{-1} = N \Rightarrow xN = xNx^{-1}x = Nx \Rightarrow xNx^{-1} = Nxx^{-1} = N$ für alle $x \in G$.

2.2.31 Satz. *Sei $(G, \cdot, e, ^{-1})$ eine Gruppe, $N \lhd G$ und π durch $x\pi y :\Leftrightarrow x^{-1}y \in N$, $x, y \in G$ definiert. Dann ist π eine Kongruenzrelation auf G mit $[e]_\pi = N$.*

Beweis. π ist eine Äquivalenzrelation und $[x]_\pi = xN = Nx$. π ist Kongruenz:

$$\left.\begin{array}{l} x_1\pi y_1 \\ x_2\pi y_2 \end{array}\right\} \Rightarrow \left\{\begin{array}{l} x_1 = y_1n_1 \text{ mit } n_1 \in N \text{ (da } x_1 \in y_1N) \\ x_2 = n_2y_2 \text{ mit } n_2 \in N \text{ (da } x_2 \in Ny_2) \end{array}\right\} \Rightarrow$$
$$\Rightarrow x_1x_2 = y_1n_1n_2y_2 \in y_1Ny_2 = y_1y_2N \Rightarrow x_1x_2\pi y_1y_2.$$

Weiters gilt $[e]_\pi = eN = N$. □

2.2.32 Satz. *Durch $\pi \mapsto [e]_\pi$ ist eine bijektive Abbildung von der Menge der Kongruenzen auf der Gruppe G auf die Menge aller Normalteiler von G definiert. Die Umkehrabbildung ist gegeben durch $N \mapsto \pi$ mit $x\pi y :\Leftrightarrow x^{-1}y \in N$.*

Beweis. Die beiden Zuordnungen sind invers: $\pi \mapsto [e]_\pi =: N \mapsto \pi_1$ mit $x\pi_1 y :\Leftrightarrow x^{-1}y \in N \Leftrightarrow x\pi y$, d. h., $\pi = \pi_1$. Umkehrung: $N \mapsto \pi \mapsto [e]_\pi = N$. □

[7] englisch: *normal subgroup*

Um — bis auf Isomorphie — alle homomorphen Bilder einer Gruppe G zu finden, kann man daher alle Normalteiler N von G bestimmen und mit den entsprechenden Kongruenzen die Faktoralgebren G/π bilden. Entspricht dem Normalteiler N die Kongruenz π, so schreiben wir $G/N := G/\pi = \{xN \mid x \in G\}$. Eine solche Faktoralgebra heißt *Faktorgruppe* von G.

In der Faktorgruppe G/N wird wie folgt gerechnet: $(xN)(yN) = (xy)N$, $eN = N$ ist Einselement, $(xN)^{-1} = x^{-1}N$.

Den trivialen Kongruenzen $\iota = \{(x,x) \mid x \in G\}$ und $\alpha = G \times G$ entsprechen die so genannten *trivialen* Normalteiler $\{e\}$ und G. Daher gilt: G ist einfach $\Leftrightarrow$ G hat nur die beiden trivialen Normalteiler.

2.2.33 Beispiele.

1. Jede zyklische Gruppe $G = \langle x \rangle$ mit $\mathrm{o}(x) = p$ (Primzahl) ist einfach (Satz von Lagrange). Umgekehrt gilt: Jede einfache abelsche Gruppe G mit $|G| > 1$ ist zyklisch und von Primzahlordnung (Übung).
2. Die alternierende Gruppe $A_n = \{\pi \in S_n \mid \mathrm{sign}(\pi) = 1\}$ ist einfach für $n \neq 4$. (Wichtig für die Theorie der algebraischen Gleichungen.)
3. Die symmetrische Gruppe S_n ist für $n \geq 3$ nicht einfach, denn es gilt: $A_n \lhd S_n$. Die Links(Rechts)nebenklassenzerlegung von S_n nach A_n ist gegeben durch $\{A_n, S_n \setminus A_n\}$, und es ist $[S_n : A_n] = 2$ (Index von A_n in S_n).

2.2.34 Satz. *Sei G Gruppe, U Untergruppe mit $[G : U] = 2$. Dann gilt $U \lhd G$.*

Beweis. $x \in U \Rightarrow xU = Ux = U$. $x \notin U \Rightarrow xU = Ux = G \setminus U$. □

2.2.35 Anmerkung. Auch für Vektorräume gilt ein ähnliches Ergebnis wie für Gruppen: Durch $\pi \mapsto [0]_\pi$ ist eine umkehrbar eindeutige Zuordnung von der Menge aller Kongruenzrelationen des Vektorraumes $(V, +, 0, -, K)$ auf die Menge aller Unterräume von V definiert (Beweis wie bei Gruppen).

Ist U Unterraum von V, so ist $V/U = \{x + U \mid x \in V\}$ (*Faktorraum*) mit den Operationen $(x + U) + (y + U) = (x + y) + U$, $0 + U = U$ (neutrales Element), $-(x + U) = (-x) + U$, $\lambda(x + U) = (\lambda x) + U$, $x, y \in V$, $\lambda \in K$.

2.2.36 Anmerkung. Wir haben für eine beliebige Abbildung $f : A \to B$ den *Kern* von f als die von f induzierte Äquivalenzrelation $\sim_f := \{(x,y) \mid f(x) = f(y)\}$ definiert.

Wenn $f : G \to H$ aber ein Gruppenhomomorphimus ist, mit $N_f := f^{-1}(e)$, dann wissen wir, dass die durch f induzierte Partition genau die Nebenklassenzerlegung von G modulo N_f ist; es gilt nämlich

$$x \sim_f y \Leftrightarrow x^{-1}y \in N_f.$$

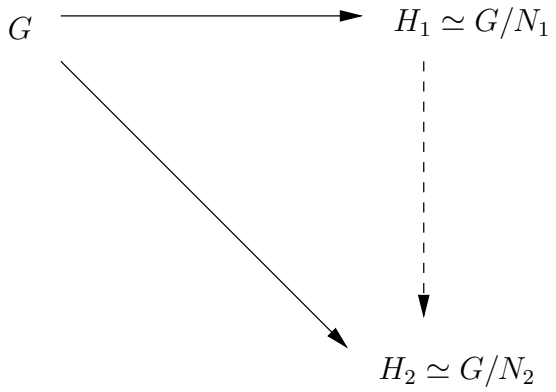
Da also N_f (zusammen mit den Gruppenoperationen) den Kern $\sim_f$ von f definiert, nennt man auch meistens die Menge N_f selbst den Kern von f; statt N_f schreibt man oft $\ker(f)$. Dies ist einerseits praktisch, weil Normalteiler (als Teilmengen von G) einfachere Objekte sind als Kongruenzrelationen (als Teilmengen von $G \times G$), ist aber andererseits eben nur auf Gruppen (somit auch auf Ringe und Vektorräume) anwendbar, nicht aber auf andere algebraische Strukturen (wie z.B. Verbände).
In dieser Notation lässt sich der Homomorphiesatz also so schreiben:

2.2.37 Satz. *Seien G, H Gruppen, $f : G \to H$ ein Epimorphismus. Sei N der Kern von f, und sei $k : G \to G/N$ die kanonische Abbildung $g \mapsto gN$.*
Dann gibt es einen eindeutig bestimmten Isomorphismus $h : G/N \to H$ mit $h \circ k = f$. Für jedes $y \in H$ ist $f^{-1}(y) \in G/N$ (d.h. Nebenklasse von N in G), und h bildet diese Nebenklasse auf y ab.

2.2.D Isomorphiesätze für Gruppen

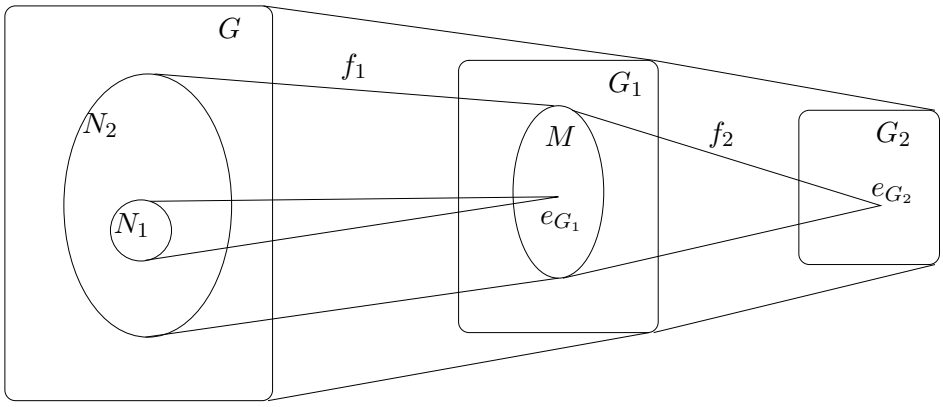
Wir zeigen zunächst die folgende Verschärfung des Homomorphiesatzes:

2.2.38 Satz. *Seien G, H_1, H_2 Gruppen, $f_1 : G \to H_1$ und $f_2 : G \to H_2$ Epimorphismen, mit Kernen N_1 und N_2. Dann gilt $N_1 \subseteq N_2$ genau dann, wenn es einen Homomorphismus (oder sogar: Epimorphismus) $h : H_1 \to H_2$ gibt mit $h \circ f_1 = f_2$.*



Beweis. Die Richtung „⇐“ ist klar.
Wir definieren $h(f_1(x)) = f_2(x)$. Wir müssen nun nur zeigen, dass h wohldefiniert ist; die Homomorphie-Eigenschaft von h und die Eigenschaft $h \circ f_1 = f_2$ folgen dann direkt aus der Definition und der Homomorphiebedingung für f_1 und f_2 (etwa $h(f_1(x) \cdot f_1(y)) = h(f_1(x \cdot y)) = f_2(x \cdot y) = f_2(x) \cdot f_2(y) = h(f_1(x)) \cdot h(f_1(y))$), ebenso die Surjektivität von h. Die Wohldefiniertheit ist ebenfalls leicht: Für alle x, x' mit $f_1(x) = f_1(x')$ gilt nämlich $f_1(x^{-1}x') = e$, also $x^{-1}x' \in N_1 \subseteq N_2$, also $f_2(x^{-1}x') = e$, somit $f_2(x) = f_2(x')$. □

Wenn G, G_1, G_2 Gruppen sind und $f_1 : G \to G_1$, $f_2 : G_1 \to G_2$ surjektive Homomorphismen, dann ist auch $f_2 \circ f_1$ surjektiver Homomorphismus.



Sei $N_1 := f_1^{-1}(e_{G_1})$, $M := f_2^{-1}(e_{G_2})$, $N_2 := f_1^{-1}(f_2^{-1}(e_{G_2})) = f_1^{-1}(M) = (f_2 \circ f_1)^{-1}(e_{G_2})$. Dann sind N_1 und N_2 Normalteiler von G, und $N_1 \subseteq N_2$ ist überdies Normalteiler von N_2. Aus dem Homomorphiesatz wissen wir, dass G_1 zu G/N_1 isomorph ist, daher nehmen wir zur Vereinfachung der Notation $G_1 = G/N_1$ an. Da der Normalteiler $M \lhd G_1$ genau aus jenen Klassen xN_1 mit $x \in N_2$ besteht, gilt $M = N_2/N_1$.
Die Gruppe G_2 ist nun einerseits zu G_1/M isomorph, andererseits zu G/N_2. Daher gilt $G_1/M \cong G/N_2$, also:

$$(G/N_1)/(N_2/N_1) \cong G/N_2.$$

Der *zweite*[8] *Isomorphiesatz* beschreibt diesen Sachverhalt, ohne die Abbildungen f_i explizit zu erwähnen, nur mit Hilfe der Normalteiler:

2.2.39 Satz. *Sei G eine Gruppe, und seien N_1, N_2 Normalteiler von G mit $N_1 \subseteq N_2$. Dann gilt:*

1. *N_1 ist Normalteiler von N_2.*
2. *N_2/N_1 (die Menge der Nebenklassen von N_1 in der Gruppe N_2) ist eine Untermenge von G/N_1.*
3. *N_2/N_1 ist nicht nur Teilmenge, sondern Untergruppe und sogar Normalteiler von G/N_1.*
4. *$G/N_2 \cong (G/N_1)/(N_2/N_1)$.*

Beweis.

1. $N_1 \lhd G$ bedeutet $x^{-1}N_1x \subseteq N_1$ für alle $x \in G$. $N_1 \lhd N_2$ bedeutet $x^{-1}N_1x \subseteq N_1$ für alle $x \in N_2$. Daher gilt $N_1 \lhd G \Rightarrow N_1 \lhd N_2$.
2. Die Elemente von N_2/N_1 sind von der Form xN_1, mit $x \in N_2$. Jedes solche Element ist eine Nebenklasse von N_1 in G.
3. Seien f_1 und f_2 die kanonischen Abbildungen von G nach G/N_1 bzw G/N_2. (Also $f_i(x) = xN_i$ für $i = 1, 2$.) Nach der gerade bewiesenen Verschärfung des Homomorphiesatzes gibt es einen Homomorphismus $h : G/N_1 \to G/N_2$ mit $h \circ f_1 = f_2$. Sei $M \lhd G/N_1$ der Kern dieses Homomorphismus. Dann ist für $g \in G$:

   $$gN_1 \in M \Leftrightarrow f_1(g) \in M \Leftrightarrow h(f_1(g)) = N_2 \Leftrightarrow f_2(g) = N_1 \Leftrightarrow g \in N_2 \Leftrightarrow gN_1 \in N_2/N_1.$$

   Also ist $N_2/N_1 = M \lhd G/N_1$.
4. Folgt aus der obigen Rechnung und aus dem Homomorphiesatz (weil $N_2/N_1 = \ker(h)$). □

Wir erinnern an das auf Seite 28 definierte Komplexprodukt: Für beliebige Untermengen $A, B \subseteq G$ einer Gruppe (oder Halbgruppe) G ist das „Komplexprodukt“ $A \cdot B$, oft auch durch AB abgekürzt, durch

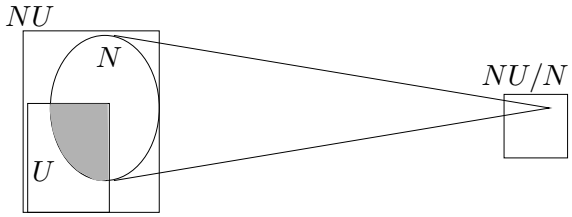
$$AB := \{ab \mid a \in A, b \in B\}$$

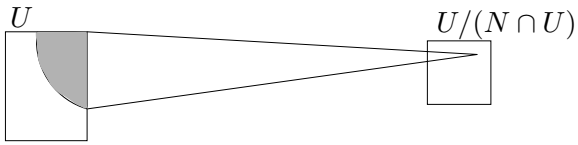
definiert. Man sieht leicht, dass das Komplexprodukt das Assoziativgesetz erfüllt. (Im Allgemeinen aber nicht das Kommutativgesetz, denn zum Beispiel ist $\{a\} \cdot \{b\} = \{ab\}$.)

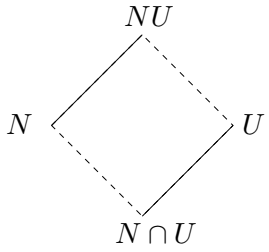
2.2.40 Satz. *Sei G Gruppe, $U \leq G$ Untergruppe und $N \lhd G$ Normalteiler. Dann gilt:*

1. *$NU = UN$.*
2. *Die Mengen NU und $N \cap U$ sind Untergruppen von G. (NU ist die kleinste Untergruppe, die N und U umfasst, $N \cap U$ die größte, die in N und U enthalten ist.)*
3. *$N \lhd NU$.*
4. *$N \cap U \lhd U$.*
5. *$NU/N \cong U/(N \cap U)$.*

[8] Diese Nummerierung ist nicht kanonisch. Der Satz 2.2.40, insbesondere Teil 2.2.40(5), heißt manchmal „erster Isomorphiesatz“, der hier angeführte Satz „zweiter“. Manchmal wird auch der Homomorphiesatz 2.2.19 als „erster“ Isomorphiesatz bezeichnet, unsere beiden Isomorphiesätze bekommen dann die Nummern 2 und 3.







Beweis. [9]

1. $NU = \bigcup_{u \in U} Nu = \bigcup_{u \in U} uN = UN$.

2. Für $u \in U$, $n \in N$ ist $(nu)^{-1} = u^{-1}n^{-1} \in UN = NU$, daher ist NU unter Inversen abgeschlossen.

   Für $u, u' \in U$, $n, n' \in N$ ist $(n'u')(nu) \in (NU)(NU) = (NU)(UN) \subseteq NUN = NNU \subseteq NU$, daher ist NU unter Multiplikation abgeschlossen. Also ist NU Untergruppe von G.

   Es ist klar, dass $N \cap U$ Untergruppe von G (und ebenso von N und U) ist.

3. Für alle $g \in G$, somit erst recht für alle $g \in NU$, gilt $g^{-1}Ng = N$, daher ist $N \lhd NU$.

4. Für $u \in U$, $n \in N$ ist $u^{-1}nu \in u^{-1}Nu = N$. Wenn n überdies noch in u liegt, gilt $u^{-1}nu \in N \cap U$. Daher gilt $N \cap U \lhd U$.

5. Sei $f : G \to G/N$ die kanonische Abbildung. Wegen $U \subseteq NU$ ist die Identität id_U auf U ein Homomorphismus von U nach NU. Die Abbildung $h := f \circ id_U : U \to NU/N$ ist surjektiv auf NU/N, denn für jede Klasse $(nu)N$ gilt $(nu)N = uN = h(u)$.

   Nach dem Homomorphiesatz (sowie seiner Folgerung) gilt also $NU/N \cong U/kern(h)$. Nun ist aber $kern(h) = \{u \in U \mid h(u) = N\} = \{u \in U \mid u \in N\} = N \cap U$. Also $NU/N \cong U/(N \cap U)$.

□

[9] Die wichtigste Aussage des Satzes ist die Isomorphie $NU/N \cong U/(N \cap U)$. Der tiefere Grund für diese Isomorphie ist einfach zu verstehen: Die „Vergrößerung“ der Gruppe U zur Gruppe NU wird durch die Wegfaktorisierung von N annulliert.

2.2.41 Beispiel. Sei V endlichdimensionaler Vektorraum, und seien N und U Unterräume. Dann ist $(N+U)/N$ zu $U/(N\cap U)$ isomorph. (Als Gruppe, und sogar als Vektorraum.) Wenn nämlich $\dim N = n$, $\dim U = u$, $\dim(N\cap U) = d$, dann hat $N+U$ Dimension $n+u-d$; $(N+U)/N$ und $U/(N\cap U)$ haben Dimension $u-d$ und sind daher isomorph.

2.2.E Kongruenzrelationen auf Ringen

2.2.42 Definition. Sei $(R,+,0,-,\cdot)$ ein Ring und I Unterring von R. Dann heißt I

- ein *Linksideal* von $R :\Leftrightarrow \forall r\in R : rI := \{ri \mid i\in I\}\subseteq I$,
- ein *Rechtsideal* von $R :\Leftrightarrow \forall r\in R : Ir := \{ir \mid i\in I\}\subseteq I$,
- ein *Ideal* von R (in Zeichen: $I \lhd R$) $:\Leftrightarrow \forall r\in R : rI\subseteq I$ und $Ir\subseteq I$.

2.2.43 Beispiele. 1) $\{0\}$ und R sind stets Ideale von R, die so genannten *trivialen* Ideale.

2) In $(\mathbb{Z},+,0,-,\cdot)$ ist $\{nk \mid k\in\mathbb{Z}\}$, $n\in\mathbb{Z}$, ein Ideal. Dies sind bereits alle Ideale in $\mathbb{Z}$. (Beweis siehe Abschnitt 5.4.)

2.2.44 Lemma. *Sei $(R,+,0,-,\cdot,1)$ ein Ring mit Einselement und I ein Ideal von R. Dann gilt: $1\in I \Leftrightarrow I = R$.*

Beweis. trivial. □

2.2.45 Satz. *Jeder Körper hat nur die trivialen Ideale.*

Beweis. Sei I Ideal des Körpers $(K,+,0,-,\cdot,1)$ und $I\neq\{0\}$. Dann gibt es $x\in I$ mit $x\neq 0$ und wegen $1 = x^{-1}x\in x^{-1}I\subseteq I$ ist $I = K$. □

2.2.46 Satz. *Sei $(R,+,0,-,\cdot,1)$ ein kommutativer Ring mit Einselement, der nur die trivialen Ideale besitzt. Dann ist R ein Körper oder $R=\{0\}$.*

Beweis. $x\in R$, $x\neq 0 \Rightarrow xR = \{xr \mid r\in R\}$ ist ein Ideal von R (analog zu $\mathbb{Z}$) mit $x = x1\in xR \Rightarrow xR\neq\{0\} \Rightarrow xR = R \Rightarrow \exists r\in R : 1 = xr \Rightarrow x$ besitzt ein Inverses. □

2.2.47 Folgerung. Ein kommutativer Ring R mit Einselement und $R\neq\{0\}$ ist ein Körper $\Leftrightarrow$ R besitzt nur die trivialen Ideale.

2.2.48 Satz. *Sei $(R,+,0,-,\cdot)$ ein Ring.*

a) Ist π eine Kongruenz auf R, dann ist $I := [0]_\pi$ ein Ideal von R, und es gilt: $R/\pi = R/I = \{x+I \mid x\in R\}$.

b) Ist I Ideal von R und π definiert durch $x\pi y :\Leftrightarrow y-x\in I$, $x,y\in R$, dann ist π Kongruenz auf R und $[0]_\pi = I$.

c) $\pi\mapsto[0]_\pi$ definiert eine bijektive Abbildung von der Menge aller Kongruenzen auf R auf die Menge aller Ideale von R. Die Umkehrabbildung ist definiert durch $I\mapsto\pi$ gemäß b).

Beweis. a) $i\in I$ und $r\in R \Rightarrow i\pi 0$ und $r\pi r \Rightarrow ir\pi 0r = 0$ und $ri\pi r0 = 0 \Rightarrow ir, ri\in I$.

b) $x_1\pi y_1$ und $x_2\pi y_2 \Rightarrow y_1 = x_1+i_1$ und $y_2 = x_2+i_2$, $i_1,i_2\in I \Rightarrow y_1y_2 = x_1x_2+i$ mit $i = x_1i_2+i_1x_2+i_1i_2\in I$ (I Ideal!) $\Rightarrow x_1x_2\pi y_1y_2$.

c) $\pi\mapsto[0]_\pi = I\mapsto\pi$, $I\mapsto\pi\mapsto[0]_\pi = I$ (analog zum entsprechenden Beweis für Normalteiler). □

Ist I Ideal von R, dann ist die Faktoralgebra $(R/I, +, I, -, \cdot)$ ein Ring, genannt der *Faktor- oder Restklassenring* von R modulo I. Die Operationen in R/I sind: $(x+I)+(y+I) = (x+y)+I$ (deckt sich mit der Komplexsumme $A+B = \{a+b \mid a \in A,\ b \in B\}$), $(x+I)(y+I) = xy+I$ (deckt sich *nicht* mit dem Komplexprodukt $AB = \{ab \mid a \in A,\ b \in B\}$), $-(x+I) = (-x)+I$, $0+I = I$ ist Nullelement.

2.2.49 Beispiel. $\mathbb{Z}_n = \mathbb{Z}/I$ mit $I = \{kn \mid k \in \mathbb{Z}\}$, denn: $x \in I \Leftrightarrow x \equiv 0 \bmod n \Leftrightarrow x - 0 = x = kn$, $k \in \mathbb{Z}$. Also entspricht das angegebene Ideal I der Relation $\equiv \bmod n$. Schreibweise: $I =: (n)$.

2.2.50 Anmerkung. Ein Ring R ist einfach $\Leftrightarrow$ R besitzt nur die trivialen Kongruenzen $\Leftrightarrow$ R besitzt nur die trivialen Ideale $\{0\} =: (0)$ und R.

2.2.51 Satz. *Ein kommutativer Ring R mit Einselement und $R \neq \{0\}$ ist einfach genau dann, wenn er ein Körper ist.*

2.2.52 Beispiel. Jeder Matrizenring $M_n(K)$ über einem Körper K ist einfach (Übung).

2.3 Direkte Produkte von Algebren

2.3.1 Definition. 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 $A := \prod_{k\in K} A_k = \{(a_k)_{k\in K} \mid a_k \in A_k\}$ das cartesische Produkt aller Mengen A_k. Die Elemente von A sind K-Tupel; wir bezeichnen Elemente von A auch manchmal als Vektoren $\vec{a} = (a_k : k \in K)$.
Für alle $i \in I$ sei die Operation ω_i auf A „komponentenweise“ so definiert:

- Wenn $n_i = 0$ ist (d.h. die Abbildungen $\omega_i^{(k)}$ sind nullstellige Operationen bzw. Konstante), dann kennen wir bereits die ausgezeichneten Elemente $\omega_i^{(k)} \in A_k$ und können sie zu einem K-Tupel in A zusammenfassen:

$$\omega_i := (\omega_i^{(k)})_{k\in K}.$$

- Wenn $n_i = n > 0$ ist, dann ist jede Operation $\omega_i^{(k)}$ auf A_k n-stellig. Für Vektoren

$$\begin{aligned} \vec{a}^{(1)} &= (a_k^{(1)} : k \in K) \in A \\ \vdots \qquad &\qquad \vdots \\ \vec{a}^{(n)} &= (a_k^{(n)} : k \in K) \in A \end{aligned}$$

  definieren wir

$$\omega_i(\vec{a}^{(1)}, \ldots, \vec{a}^{(n)}) := \vec{b} = (b_k : k \in K) \in A,$$

  wobei $b_k := \omega_i^{(k)}(a_k^{(1)}, \ldots, a_k^{(n)})$ ist.

In der k-ten Komponente wenden wir also die Operation $\omega_i^{(k)}$ auf Elemente von A_k an.
Die Algebra $(A, (\omega_i)_{i\in I})$ heißt das *direkte Produkt* der Algebren $\mathfrak{A}_k$ und wird mit $\prod_{k\in K} \mathfrak{A}_k$ bezeichnet.

2.3.2 Beispiel. $K = \{1,2\}$, $\mathfrak{A}_1 = (A_1, \cdot, e, {}^{-1})$, $\mathfrak{A}_2 = (A_2, +, 0, -)$ seien Gruppen. Dann wird in $\mathfrak{A}_1 \times \mathfrak{A}_2 = (A_1 \times A_2, \circ, (e,0), \overline{\ \ })$ folgendermaßen gerechnet:

$$(a_1, a_2) \circ (b_1, b_2) = (a_1 b_1, a_2 + b_2),$$

$\overline{(a_1, a_2)} = (a_1^{-1}, -a_2)$.

Es gilt: $\mathfrak{A}_1 \times \mathfrak{A}_2$ ist eine Gruppe. Assoziativgesetz: $((a_1, a_2) \circ (b_1, b_2)) \circ (c_1, c_2) = (a_1 b_1 c_1, a_2 + b_2 + c_2) = (a_1, a_2) \circ ((b_1, b_2) \circ (c_1, c_2))$; $(e, 0)$ ist neutrales Element: $(e, 0) \circ (a_1, a_2) = (ea_1, 0 + a_2) = (a_1, a_2) = (a_1 e, a_2 + 0) = (a_1, a_2) \circ (e, 0)$; $\overline{(a_1, a_2)}$ ist Inverses von (a_1, a_2): $(a_1, a_2) \circ \overline{(a_1, a_2)} = (a_1, a_2) \circ (a_1^{-1}, -a_2) = (a_1 a_1^{-1}, a_2 + (-a_2)) = (e, 0)$, analog $\overline{(a_1, a_2)} \circ (a_1, a_2) = (e, 0)$.

2.3.3 Satz. *Gilt mit geeigneten Termen t_1, t_2 ein Gesetz der Form $\forall x_1, \ldots, x_n : t_1(x_1, \ldots, x_n) = t_2(x_1, \ldots, x_n)$ in allen Algebren $\mathfrak{A}_k$, $k \in K$, so gilt es auch in $\prod_{k \in K} \mathfrak{A}_k$.*

Beweis. Induktion nach der „Stufe“ der Terme t_1, t_2. □

2.3.4 Folgerung. Direkte Produkte von Halbgruppen (Gruppen, Vektorräumen über dem selben Körper K, Ringen, Booleschen Algebren) sind wieder Halbgruppen (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: $0 \neq 1$.)

2.3.5 Anmerkungen.

1. Das direkte Produkt $\prod_{k \in K} \mathfrak{A}_k$ ist — bis auf Isomorphie — unabhängig von der Reihenfolge. Z. B.: $\mathfrak{A}_1 \times \mathfrak{A}_2 \cong \mathfrak{A}_2 \times \mathfrak{A}_1$.

2. Man kann Produkte „zusammenfassen“. Z. B.: $\mathfrak{A}_1 \times \mathfrak{A}_2 \times \mathfrak{A}_3 \cong (\mathfrak{A}_1 \times \mathfrak{A}_2) \times \mathfrak{A}_3 \cong \mathfrak{A}_1 \times (\mathfrak{A}_2 \times \mathfrak{A}_3)$.
   Allgemein: Wenn die Indexmenge I eine disjunkte Vereinigung $I = \bigcup_{k \in K} J_k$ ist, dann ist das Produkt über I kanonisch isomorph zu einem Produkt (über der Indexmenge K) von Produkten:
   $$\prod_{i \in I} A_i \cong \prod_{k \in K} B_k \quad \text{mit } B_k := \prod_{j \in J_k} A_j.$$

3. Wenn die Indexmenge K nur ein einziges Element k_0 enthält, dann ist $\prod_{k \in K} A_k$ formal die Menge aller Funktionen $f : \{k_0\} \to A_{k_0}$. Die Abbildung, die jeder solchen Funktion ihren Wert an der Stelle k_0 zuordnet, ist eine Bijektion zwischen den Mengen $\prod_{k \in \{k_0\}} A_k$ und A_{k_0}, bzw. ein Isomorphismus zwischen den Algebren $\prod_{k \in \{k_0\}} \mathfrak{A}_k$ und $\mathfrak{A}_{k_0}$.

4. Wenn die Indexmenge K zwei Elemente hat, sagen wir $K = \{3, 5\}$ dann ist $\prod_{k \in K} A_k$ formal die Menge aller Funktionen f auf $\{3, 5\}$, die $f(3) \in A_3$ und $f(5) \in A_5$ erfüllen. Die Abbildung, die jeder solchen Funktion f das Paar $(f(3), f(5))$ zuordnet, ist ein Isomorphismus zwischen $\prod_{k \in \{3,5\}} \mathfrak{A}_k$ und $\mathfrak{A}_3 \times \mathfrak{A}_5$.[10]

5. Wenn die Indexmenge K leer ist, dann definieren wir $\prod_{k \in \emptyset} \mathfrak{A}_k$ als die einelementige Algebra.

2.3.6 Satz. *Seien C_n bzw. C_m zyklische Gruppen der Ordnungen n bzw. m. Dann gilt: $C_n \times C_m$ ist zyklisch $\Leftrightarrow \mathrm{ggT}(m, n) = 1$.*

[10] Oft wird zwischen $A_3 \times A_5$, $A_5 \times A_3$ und $\prod_{i \in \{3,5\}} A_i$ nicht unterschieden, da es kanonische Isomorphismen zwischen diesen Strukturen gibt, und daher diese Strukturen insbesondere die selben algebraischen Eigenschaften haben.

Beweis. Sei $C_n = \langle x \rangle$, $C_m = \langle y \rangle$.
$\Rightarrow$ (indirekt): $\mathrm{ggT}(n,m) > 1 \Rightarrow k := \mathrm{kgV}(n,m) < nm$ (wegen $\mathrm{kgV}(n,m) = nm/\mathrm{ggT}(n,m)$) und $(x^i, y^j)^k = (x^{ki}, y^{kj}) = (e,e)$ (wegen $n|ki$ und $m|kj$) $\Rightarrow \mathrm{o}(x^i, y^j)|k < nm \Rightarrow$ die Ordnung aller Elemente von $C_n \times C_m$ ist kleiner als $nm = |C_n \times C_m| \Rightarrow C_n \times C_m$ ist nicht zyklisch.
$\Leftarrow$: Wir zeigen, dass $C_n \times C_m = \langle (x,y) \rangle$ gilt. $(x,y)^t = (e,e) \Rightarrow x^t = e$ und $y^t = e \Rightarrow n|t$ und $m|t \Rightarrow \mathrm{kgV}(n,m) = nm|t$ (wegen $\mathrm{ggT}(n,m) = 1$). Andererseits gilt: $(x,y)^{nm} = (x^{nm}, y^{nm}) = ((x^n)^m, (y^m)^n) = (e,e)$. Also ist $\mathrm{o}(x,y) = nm$. □

2.3.7 Folgerung. Ist $n = p_1^{e_1} \cdots p_k^{e_k}$ die Primfaktorzerlegung von $n \in \mathbb{N}$, dann gilt $C_n \cong C_{p_1^{e_1}} \times \cdots \times C_{p_k^{e_k}}$.

2.3.8 Satz (Hauptsatz über endlich erzeugte abelsche Gruppen)**.** *Ist $G = \langle \{x_1, \ldots, x_m\} \rangle$ eine von den Elementen $x_1, \ldots, x_m$ erzeugte* abelsche *Gruppe, dann gilt:*

$$G \cong C_\infty^k \times C_{n_1} \times \cdots \times C_{n_r},$$

wobei $k \geq 0$ ($C_\infty^0 := \{e\}$), $n_i \in \mathbb{N}$, $r \geq 0$. Dabei gilt: G endlich $\Leftrightarrow k = 0$.

(C_∞ bezeichnet eine unendliche zyklische Gruppe; sie ist isomorph zur additiven Gruppe $\mathbb{Z}$.)

Den Beweis dieses Satzes werden wir später kennenlernen.

2.3.9 Beispiel. 1) Alle abelschen Gruppen mit 12 Elementen sind — bis auf Isomorphie — gegeben durch C_{12} ($\cong C_3 \times C_4$) und $C_2 \times C_6$ ($\cong C_2 \times C_2 \times C_3$).

2) Alle abelschen Gruppen mit 8 Elementen sind — bis auf Isomorphie — gegeben durch C_8, $C_2 \times C_4$ und $C_2 \times C_2 \times C_2$.

Zur nächsten Definition vgl. den Begriff „direkte Summe“ $V = U_1 \oplus U_2 \oplus \cdots \oplus U_n$ aus der Linearen Algebra ($U_1, U_2, \ldots, U_n$ Unterräume eines Vektorraumes V).

2.3.10 Definition. Sei G Gruppe, und seien U, V Untergruppen von G. G heißt *inneres direktes Produkt* von U und V genau dann, wenn die Abbildung

$$\varphi : \begin{cases} U \times V \to G \\ (u,v) \mapsto uv \end{cases}$$

ein Isomorphismus von $U \times V$ auf G ist.

2.3.11 Beispiel. Seien G_1 und G_2 Gruppen mit neutralem Element e_1 bzw e_2. Dann sind $U := G_1 \times \{e_2\}$ und $V := \{e_1\} \times G_2$ Untergruppen von $G := G_1 \times G_2$, und G ist das direkte Produkt von U und V.

Wir verallgemeinern diese Definition auf das Produkt von endlich vielen Gruppen.

2.3.12 Definition. Sei G Gruppe, $U_1, \ldots, U_n$ Untergruppen von G. Dann heißt G *inneres direktes Produkt* von $U_1, \ldots, U_n$ genau dann, wenn die Abbildung

$$\varphi : \begin{cases} U_1 \times \cdots \times U_n \to G \\ (u_1, \ldots, u_n) \mapsto u_1 \cdots u_n \end{cases}$$

ein Isomorphismus von $U_1 \times \cdots \times U_n$ auf G ist.

2.3.13 Anmerkung. $G \cong G_1 \times \cdots \times G_n \Leftrightarrow$ es gibt Untergruppen U_i von G mit $U_i \cong G_i$, $i = 1, \ldots, n$, sodass G inneres direktes Produkt von $U_1, \ldots, U_n$ ist. (Beweis: Übung.)

2.3.14 Anmerkung. Je nachdem, ob wir die Gruppe G additiv oder multiplikativ schreiben, verwenden wir die Notation $G = U_1 \oplus U_2$ oder $G = U_1 \otimes U_2$ für die Aussage „G ist inneres direktes Produkt von U_1 und U_2."

2.3.15 Definition. Sei I eine endliche oder unendliche Menge, und sei $(G_i)_{i\in I}$ eine Familie von abelschen Gruppen. Dann schreiben wir $\bigoplus_{i\in I} G_i$ für die Menge aller $\vec{x} = (x_i)_{i\in I} \in \prod_{i\in I} G_i$, die

$$supp(\vec{x}) := \{i \in I \mid x_i \neq 0_i\} \text{ endlich}$$

erfüllen (wobei 0_i das neutrale Element der Gruppe G_i bezeichnet). Man sieht leicht (Übung), dass $\bigoplus_{i\in I} G_i$ eine Untergruppe von $\prod_{i\in I} G_i$ ist.
Sei $(G, +, 0, -)$ eine abelsche Gruppe, und seien U_i (für $i \in I$) Untergruppen von G. Für jedes Element $\vec{x} = (x_i)_{i\in I} \in \bigoplus_{i\in I} U_i$ bezeichnen wir mit $\sum \vec{x}$ die Summe aller x_i mit $i \in supp(\vec{x})$; für $\vec{x} = (0)_{i\in I}$ sei $\sum \vec{x} = 0$. Wir sagen, dass G die *direkte Summe der Untergruppen* U_i ist, wenn die Abbildung $\vec{x} \mapsto \sum \vec{x}$ eine Isomorphismus von $\bigoplus_{i\in I} U_i$ auf G ist.

2.3.16 Anmerkung. Wenn I endlich ist, dann ist $\bigoplus_{i\in I} U_i = \prod_{i\in I} U_i$, und die gerade gegebene Definition des inneren direkten Produkts stimmt mit der vorigen überein.

2.3.17 Satz. *Sei G Gruppe, $U_1, \ldots, U_n$ Untergruppen von G. Dann sind die folgenden Aussagen äquivalent:*

a) G ist inneres direktes Produkt von $U_1, \ldots, U_n$.

b) i) Die oben definierte Abbildung $\varphi : U_1 \times \cdots \times U_n \to G$, $(u_1, \ldots, u_n) \mapsto u_1 \cdots u_n$, ist bijektiv und

ii) für $1 \leq i < j \leq n$, $x \in U_i$, $y \in U_j$ gilt stets $xy = yx$.

Beweis. a) $\Rightarrow$ b): i) gilt, da φ Isomorphismus.
Zu ii): Für $x \in U_i$, $y \in U_j$, $1 \leq i < j \leq n$ gilt

$$\begin{aligned}
xy &= \varphi(e, \ldots, e, \underbrace{x}_{i-\text{te Stelle}}, e, \ldots, e) \cdot \varphi(e, \ldots, e, \underbrace{y}_{j-\text{te Stelle}}, e, \ldots, e) = \\
&= \varphi((e, \ldots, e, \underbrace{x}_{i-\text{te Stelle}}, e, \ldots, e) \cdot (e, \ldots, e, \underbrace{y}_{j-\text{te Stelle}}, e, \ldots, e)) = \\
&= \varphi(e, \ldots, e, \underbrace{x}_{i-\text{te Stelle}}, e, \ldots, e, \underbrace{y}_{j-\text{te Stelle}}, e, \ldots, e) = \\
&= \varphi((e, \ldots, e, \underbrace{y}_{j-\text{te Stelle}}, e, \ldots, e) \cdot (e, \ldots, e, \underbrace{x}_{i-\text{te Stelle}}, e, \ldots, e)) = \\
&= \varphi(e, \ldots, e, \underbrace{y}_{j-\text{te Stelle}}, e, \ldots, e) \cdot \varphi(e, \ldots, e, \underbrace{x}_{i-\text{te Stelle}}, e, \ldots, e) = \\
&= yx.
\end{aligned}$$

b) $\Rightarrow$ a): Da φ bijektiv ist, muss nur mehr gezeigt werden, dass φ Homomorphismus ist. Für $\vec{a} := (a_1, \ldots, a_n)$, $\vec{b} := (b_1, \ldots, b_n) \in U_1 \times \cdots \times U_n$ gilt:

$$\varphi(\vec{a}\vec{b}) = \varphi(a_1b_1, \ldots, a_nb_n) = a_1b_1 \cdots a_nb_n \overset{*}{=} a_1 \cdots a_nb_1 \cdots b_n = \varphi(\vec{a})\varphi(\vec{b}).$$

Die mit * bezeichnete Gleichheit gilt wegen ii). □

2.3.18 Satz. *Sei G Gruppe, $U_1, \ldots, U_n$ Untergruppen von G. Dann sind die folgenden Aussagen äquivalent:*

a) G ist inneres direktes Produkt von $U_1, \ldots, U_n$.

b) I) $G = U_1 \cdots U_n = \{u_1 \cdots u_n \mid u_i \in U_i\}$ *(d. h., φ ist surjektiv),*
II) $(U_1 \cdots U_i) \cap U_{i+1} = \{e\}$ *für* $i = 1, \ldots, n-1$,
III) $U_i \lhd G$ *für* $i = 1, \ldots, n$.

Beweis. a) $\Rightarrow$ b): I) ist erfüllt.
Zu II): $a \in (U_1 \cdots U_i) \cap U_{i+1} \Rightarrow a = a_1 \cdots a_i e \cdots e = e \cdots e a_{i+1} e \cdots e$ mit $a_k \in U_k \Rightarrow$ $a_1 = \cdots = a_i = a_{i+1} = e$ (da φ injektiv).
Zu III): Für $g \in G$, $g = a_1 \cdots a_n$, $a_i \in U_i$, gilt:

$$gU_i = a_1 \cdots a_n U_i \overset{*}{=} a_1 \cdots a_i U_i a_{i+1} \cdots a_n \overset{**}{=} a_1 \cdots a_{i-1} U_i a_i \cdots a_n \overset{*}{=} U_i a_1 \cdots a_n = U_i g$$

(dabei gilt * wegen ii) im vorigen Satz und **, weil $a_i \in U_i$).

b) $\Rightarrow$ a): Wegen I) ist φ surjektiv. Wir zeigen nun ii) (im vorigen Satz): Für $1 \leq i < j \leq n$, $a_i \in U_i$, $a_j \in U_j$, gilt

$$a_i a_j (a_j a_i)^{-1} = a_i a_j a_i^{-1} a_j^{-1} = a_i \cdot \underbrace{(a_j a_i^{-1} a_j^{-1})}_{\in U_i, \text{ da } U_i \lhd G} = \underbrace{(a_i a_j a_i^{-1})}_{\in U_j, \text{ da } U_j \lhd G} \cdot a_j^{-1} \in U_i \cap U_j.$$

Wegen $U_i \cap U_j \subseteq (U_1 \cdots U_i \cdots U_{j-1}) \cap U_j = \{e\}$ ist $a_i a_j (a_j a_i)^{-1} = e$ woraus $a_i a_j = a_j a_i$ folgt.
Abschließend zeigen wir i) (im vorigen Satz), d. h., dass φ injektiv ist: Sei $a_1 \cdots a_n = b_1 \cdots b_n$, $a_i, b_i \in U_i$. Dann gilt $b_{n-1}^{-1} \cdots b_1^{-1} a_1 \cdots a_{n-1} = b_n a_n^{-1}$, woraus (mit ii)) $b_1^{-1} a_1 \cdots b_{n-1}^{-1} a_{n-1} = b_n a_n^{-1} \in (U_1 \cdots U_{n-1}) \cap U_n = \{e\}$ folgt. Damit ist $a_n = b_n$. Analog erhält man $a_{n-1} = b_{n-1}$, $\ldots$, $a_1 = b_1$. □

Spezialfall: Seien U, V Normalteiler von G. Dann ist G genau dann das innere direkte Produkt von U und V, wenn $UV = G$ und $U \cap V = \{1\}$ gilt.

2.3.19 Definition. Sei R ein Ring, $U_1, \ldots, U_n$ Unterringe von R. Dann heißt R *innere direkte Summe* von $U_1, \ldots, U_n$ genau dann, wenn die Abbildung

$$\varphi : \begin{cases} U_1 \times \cdots \times U_n \to R \\ (u_1, \ldots, u_n) \mapsto u_1 + \cdots + u_n \end{cases}$$

ein Ring-Isomorphismus ist.

2.3.20 Satz. *Sei R ein Ring, $U_1, \ldots, U_n$ Unterringe von R. Dann sind folgende Aussagen äquivalent:*

a) R ist innere direkte Summe von $U_1, \ldots, U_n$.

b) i) φ (von oben) ist bijektiv und
ii) für $1 \leq i \neq j \leq n$, $x \in U_i$, $y \in U_j$ gilt stets $xy = 0$.

c) I) $R = U_1 + \cdots + U_n$,
II) $(U_1 + \cdots + U_i) \cap U_{i+1} = \{0\}$ *für* $i = 1, \ldots, n-1$,
III) Jedes U_i ist Ideal, d. h., $U_i \lhd R$ für $i = 1, \ldots, n$.

Beweis. a) $\Rightarrow$ b): i) ist erfüllt.

Zu ii): Für $x \in U_i$, $y \in U_j$, $i \neq j$ gilt

$$(0,\dots,0,\underbrace{x}_{i-\text{te Stelle}},0,\dots,0)\cdot(0,\dots,0,\underbrace{y}_{j-\text{te Stelle}},0,\dots,0)=(0,\dots,0),$$

woraus — nach Anwendung von φ — $xy=0$ folgt.

b) $\Rightarrow$ c): I) und II) folgen aus dem zweiten Satz über Gruppen. Zu III): Für $b_i \in U_i$, $r = a_1 + \cdots + a_n \in R$ gilt

$$rb_i = (a_1+\cdots+a_n)b_i = a_1b_i+\cdots+a_ib_i+\cdots+a_nb_i = 0+\cdots+0+a_ib_i+0+\cdots+0 = a_ib_i \in U_i.$$

Analog zeigt man $b_ir \in U_i$.

c) $\Rightarrow$ a): Da φ nach I) und II) bijektiv ist (folgt aus dem Satz über Gruppen), muss nur mehr gezeigt werden, dass φ Homomorphismus ist. Bezüglich $+$ folgt dies ebenfalls aus dem Satz über Gruppen, bezüglich $\cdot$ gilt:

$$\begin{aligned}\varphi((a_1,\dots,a_n)(b_1,\dots,b_n)) &= \varphi(a_1b_1,\dots,a_nb_n) = \\ &= a_1b_1+\cdots+a_nb_n = (a_1+\cdots+a_n)(b_1+\cdots+b_n) = \\ &= \varphi(a_1,\dots,a_n)\varphi(b_1,\dots,b_n).\end{aligned}$$

Die hierbei verwendete Beziehung $a_1b_1+\cdots+a_nb_n = (a_1+\cdots+a_n)(b_1+\cdots+b_n)$ folgt aus II) und III): Für $i<j$ ist $a_ib_j \in U_i$ (wegen $U_i \lhd R$) und $a_ib_j \in U_j$ (wegen $U_j \lhd R$), d. h., $a_ib_j \in (U_1+\cdots+U_{j-1}) \cap U_j = \{0\}$, woraus $a_ib_j = 0$ folgt. Analog erhält man $a_ib_j = 0$ für $i > j$. □

2.4 Aufsteigende Vereinigungen und direkter Limes

Wir betrachten in diesem Abschnitt nur nichtleere[11] Algebren eines festen Typs. Um die Notation zu vereinfachen, betrachten wir hier nur Algebren $(A,+,',c)$ vom Typ $(2,1,0)$ (aber die Definitionen und Überlegungen lassen sich in offensichtlicher Weise verallgemeinern).

2.4.A Aufsteigende Vereinigungen

2.4.1 Definition. Sei $(I,\leq)$ eine lineare Ordnung; für jedes $i \in I$ sei $\mathfrak{A}_i = (A_i,+_i,'^i,c_i)$ eine Algebra, wobei die Beziehung

$$i \leq j \;\Rightarrow\; \mathfrak{A}_i \leq \mathfrak{A}_j$$

gelten möge. (Das heißt: Für $i \leq j$ ist $\mathfrak{A}_i$ Unteralgebra von $\mathfrak{A}_j$, also $A_i \subseteq A_j$, $c_i = c_j$, $x'^i = x'^j$ für alle $x \in A_i$, und $x +_i y = x +_j y$ für alle $x,y \in A_i$.)
Wir definieren den „*direkten Limes*“ (auch „*injektiven Limes*“ oder „*Vereinigung*“) $\lim_{i\in I}\mathfrak{A}_i$ oder $\varinjlim_{i\in I}\mathfrak{A}_i$ der Familie $(\mathfrak{A}_i)_{i\in I}$ so:

- Die Grundmenge von $\lim_i \mathfrak{A}_i$ ist die Menge $\bigcup_{i\in I} A_i$.
- Die Operationen $+,',c$ sind auf $\bigcup_{i\in I} A_i$ in „natürlicher Weise“ definiert, das heißt:

[11] Wir könnten auch leere Algebren zulassen, das würde nur einige notationelle Modifikationen verlangen; auch müsste man dann Satz 2.4.3 umformulieren, indem wir die leeren Faktoren vom Produkt ausnehmen.

– c sei der gemeinsame Wert aller c_i.
– Wenn $x \in \bigcup_{i\in I} A_i$, dann muss es ein i_0 geben[12] mit $x \in A_{i_0}$. Alle Werte x'^j, die auch definiert sind (d.h., für die $x \in A_j$ gilt), stimmen mit dem Wert x'^{i_0} überein; diesen gemeinsamen Wert definieren wir als x'.
– Wenn $x, y \in \bigcup_{i\in I} A_i$, dann ist wiederum die Menge $\{j \mid x, y \in A_j\}$ nicht leer. Für alle j in dieser Menge stimmen die Werte $x +_j y$ überein; den gemeinsamen Wert definieren wir als $x + y$.

2.4.2 Lemma. *Für die gerade definierte Algebra* $\varinjlim_{i\in I} \mathfrak{A}_i = (A, +, ', c) = \mathfrak{A}$ *gilt* $\mathfrak{A}_i \leq \mathfrak{A}$ *für alle* i.
Weiters gilt: Wenn ein Gesetz in allen Algebren $\mathfrak{A}_i$ *gilt, dann gilt es auch in* $\mathfrak{A}$.

2.4.3 Satz. $\varinjlim_{i\in I} \mathfrak{A}_i$ *ist isomorph zu einer Unteralgebra von* $\prod_{i\in I} \mathfrak{A}_i/\!\sim$, *mit einer geeigneten Kongruenzrelation* $\sim$.

Beweis. Auf der Menge $\prod_{i\in I} A_i$ definieren wir die folgende Äquivalenzrelation:

$$(a_i)_{i\in I} \sim (b_i)_{i\in I} \Leftrightarrow \exists i_0 \forall j \geq i_0 (a_j = b_j).$$

Man sieht leicht (Übung), dass diese Relation sogar eine Kongruenzrelation ist.
Wir definieren eine Abbildung $\psi : \varinjlim_{i\in I} A_i \to \prod_{i\in I} A_i$ wie folgt: $\psi(b) = (a_i)_{i\in I}$, wobei gilt

- wenn $b \in A_i$, dann $a_i = b$,
- wenn $b \notin A_i$, dann $a_i = c_i$ (oder ein beliebiges Element von A_i).

Weiters sei $k : \prod_{i\in I} A_i \to \prod_{i\in I} A_i/\!\sim$ die kanonische Abbildung, die jeder Familie $(a_i)_{i\in I}$ ihre $\sim$-Äquivalenzklasse zuordnet.
Für $b_1 \neq b_2$ gibt es ein i mit $b_1, b_2 \in A_i$, daher stimmen $\psi(b_1)$ und $\psi(b_2)$ an der Stelle i (sowie auch an allen folgenden $j \geq i$) nicht überein, somit ist $\psi(b_1) \not\sim \psi(b_2)$, also $(k \circ \psi)(b_1) \neq (k \circ \psi)(b_2)$. Also ist $k \circ \psi$ injektiv. Man rechnet leicht nach, dass $k \circ \psi$ ein Homomorphismus ist.[13]
Das Bild von $\varinjlim_{i\in I} A_i$ in $\prod_{i\in I} A_i/\!\sim$ ist also eine Unteralgebra von $\prod_{i\in I} A_i/\!\sim$, die zu $\varinjlim_{i\in I} A_i$ isomorph ist. □

Nach dem gerade bewiesenen Satz lässt sich also ein direkter Limes als Kombination von Produkt, Quotient und Unteralgebra schreiben.

2.4.B Direkter Limes eines Systems kommutierender Abbildungen

In den Übungen werden wir eine Verallgemeinerung des gerade betrachteten Begriffs betrachten (die man auch „direkten Limes“ nennt). Der vorhin betrachtete Fall der aufsteigenden Vereinigung ergibt sich als Spezialfall, wenn alle vorkommenden Homomorphismen Inklusionsabbildungen sind (also die Identität auf ihrem Definitionsbereich).

2.4.4 Definition. Sei $(I, \leq)$ eine lineare Ordnung[14]; für jedes $i \in I$ sei $\mathfrak{A}_i = (A_i, +_i, '^i, c_i)$ eine Algebra. Weiters sei $(h_{ij})_{i,j\in I, i\leq j}$ eine Familie von Abbildungen, die die folgenden Bedingungen erfüllen möge:

[12] Achtung: es muss nicht unbedingt ein kleinstes oder größtes solches i_0 geben.
[13] Achtung! ψ ist im Allgemeinen kein Homomorphismus.
[14] Oder allgemeiner: eine nach oben gerichtete partielle Ordnung, das heißt: eine partielle Ordnung, in der jede zweielementige (und daher jede endliche) Teilmenge nach oben beschränkt ist.

- $h_{ij} : A_i \to A_j$ ist ein Homomorphismus.
- Für $i \leq j \leq k$ gilt immer $h_{jk} \circ h_{ij} = h_{ik}$.

Das System aller Algebren $(\mathfrak{A}_i)_{i\in I}$ zusammen mit den Homomorphismen $(h_{ij})_{i\leq j,\, i,j\in I}$ bezeichnen wir mit $\mathscr{A}$. Wir definieren den „*direkten*“ („*injektiven*“) *Limes* $\varinjlim \mathscr{A}$ so:
Sei $B := \{(i,x) \mid x \in A_i, i \in I\}$. Auf der Menge B definieren wir eine Äquivalenzrelation $\sim$ durch

$$(i,x) \sim (j,y) \;\Leftrightarrow\; \exists k\,(i \leq k \text{ und } j \leq k \text{ und } h_{ik}(x) = h_{jk}(y).$$

(Dies bedeutet anschaulich, dass wir ein Element $x \in A_i$ mit seinem Bild $h_{ik}(x) \in A_k$ identifizieren.)
Die Klasse von (i,x) bezeichnen wir mit $[i,x]_\sim$.

- Die Grundmenge von $\varinjlim \mathscr{A}$ sei $B/\!\sim$.
- Die Operationen $+, ', c$ sind auf $B/\!\sim$ in „natürlicher Weise“ definiert, das heißt:
  - Für alle $i \leq j$ gilt $(i, c_i) \sim (j, c_j)$. Daher liegen alle (i, c_i) in der selben Klasse. Diese Klasse definieren wir nun als den Wert von c.
  - Die Operation $'$ definieren wir durch $[i,x]' := [i, x'^i]_\sim$. (Hier muss man nachprüfen, dass die Operation $'$ tatsächlich wohldefiniert ist: Wenn $(i,x) \sim (j,y)$, dann $(i, x'^i) \sim (j, x'^j)$.)
  - Schließlich definieren wir die Operation $+$: Seien $[i,x]_\sim$ und $[j,y]_\sim$ Elemente von $B/\!\sim$. Wir finden zunächst ein k mit $i, j \leq k$; dann gilt $(i,x) \sim (k, h_{ik}(x))$ und $(j,y) \sim (k, h_{jk}(y))$; wir definieren also die Summe in natürlicher Weise als

    $$[i,x]_\sim + [j,y]_\sim = [k, h_{ik}(x)]_\sim + [k, h_{jk}(y)]_\sim := [k, h_{ik}(x) + h_{jk}(y)]_\sim.$$

    Man muss nun nachprüfen, dass diese Definition nicht von der Wahl von k abhängt.

2.4.5 Satz. *Sei $\mathscr{A} = (\,(\mathfrak{A}_i)_{i\in I}, (h_{ij})_{i\leq j}\,)$ ein System wie in der Definition 2.4.4. Dann gilt:*

1. *$\varinjlim \mathscr{A}$ ist wohldefiniert.*
2. *Jedes Gesetz, das in allen Algebren $\mathfrak{A}_i$ gilt, gilt auch in $\varinjlim \mathscr{A}$.*
3. *Für jedes i ist die Abbildung $h_i : \mathfrak{A}_i \to \varinjlim \mathscr{A}$, die durch $h_i(x) = [i,x]$ definiert ist, ein Homomorphismus.*
4. *Für alle $i \leq j$ gilt $h_i = h_j \circ h_{ij}$.*

Kapitel 3

Freie Algebren

Wir betrachten in diesem Kapitel Algebren eines beliebigen (aber festen) Typs $\vec{n} = (n_i)_{i\in I}$. Wenn wir also von einer Algebra sprechen, meinen wir immer eine Algebra vom Typ $\vec{n}$. Wir unterscheiden in der Notation oft nicht zwischen einer Algebra und ihrer Grundmenge; eine Algebra $(A, (\omega_i)_{i\in I})$ bezeichnen wir also auch mit A.

Für jedes $i \in I$ verwenden wir nun ein Symbol ω_i. In jeder Algebra A wird das Symbol ω_i durch eine n_i-stellige Operation interpretiert; diese Operation bezeichnet man meist ebenfalls mit ω_i. Um aber die Funktion vom reinen Symbol zu unterscheiden, bezeichnen wir sie manchmal auch mit ω_i^A; um zu betonen, dass ω_i nur ein Symbol ist, schreiben wir statt ω_i gelegentlich $\dot{\omega}_i$.

Wir beginnen mit einem mengentheoretischen Lemma:

3.0.6 Lemma.

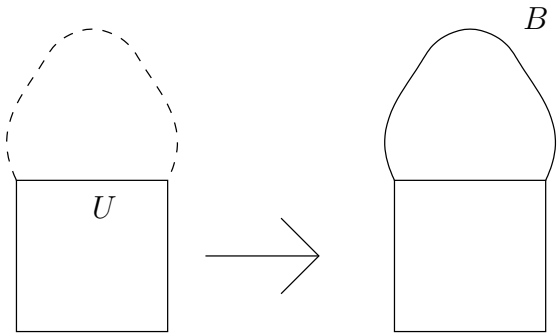
1. *Für jede Menge A gibt es eine Menge B, die zu A disjunkt ist, aber gleichmächtig mit A.*
2. *Für alle Mengen A_1, A_2 gibt es eine Menge B und eine Bijektion $f : A_1 \to B$ mit $B \cap A_2 = \emptyset$.*

Beweis. (1) Den Beweis überlassen wir den Mengentheoretikern.[1]
(2) Sei $C \cap (A_1 \cup A_2) = \emptyset$, $g : A_1 \cup A_2 \to C$ eine Bijektion (laut (1)), dann können wir $B := g(A_1)$ wählen. □

3.0.7 Satz (Prinzip der isomorphen Einbettung)**.** *Seien $\mathfrak{U} = (U, (\omega_i^U)_{i\in I})$, $\mathfrak{B} = (B, (\omega_i^B)_{i\in I})$ Algebren vom selben Typ $(n_i)_{i\in I}$, und sei f ein Monomorphismus von $\mathfrak{U}$ nach $\mathfrak{B}$.*
Dann gibt es eine Algebra $\mathfrak{A} = (A, (\omega_i^A)_{i\in I})$ und einen Isomorphismus $g : \mathfrak{A} \to \mathfrak{B}$, sodass $\mathfrak{U}$ Unteralgebra von $\mathfrak{A}$ und g eine Fortsetzung von f ist.

Statt einer Einbettung von $\mathfrak{U}$ in die Algebra $\mathfrak{B}$ haben wir also $\mathfrak{U}$ als Unteralgebra einer zu $\mathfrak{B}$ isomorphen Algebra realisiert. Aus der Einbettung $f : U \to B$ wird dann die identische Einbettung $id|U : U \to A$.
Wenn wir zusätzlich noch voraussetzen, dass U zu B disjunkt ist, dann können wir $A \setminus U = B \setminus f(U)$ verlangen, und g als die Identitätsabbildung auf der Menge $A \setminus U$ wählen. In diesem Fall wird also in der Algebra $\mathfrak{B}$ einfach die Unteralgebra $f(U)$ durch ihre isomorphe Kopie U ersetzt.

[1] Beweisskizze: Es gibt eine Menge C, die nicht injektiv nach A eingebettet werden kann, zum Beispiel $C = \mathfrak{P}(A)$. Für jedes $a \in A$ kann die Menge $\{a\} \times C$ keine Teilmenge von A sein, es gibt also ein $c_a \in C$ mit $(a, c_a) \notin A$. Sei nun $B := \{(a, c_a) \mid a \in A\}$. (Die Anwendung des Auswahlaxioms kann bei geschickterer Wahl von C auch vermieden werden.)



Beweis. Sei D eine zu $B \setminus f(U)$ gleichmächtige Menge, die zu U disjunkt ist, und sei $A := U \cup D$. Sei $h : D \to B \setminus f(U)$ Bijektion, dann definieren f und h zusammen eine Bijektion $g := f \cup h$ von $A = U \cup D$ auf $B = f(U) \cup h(D)$. Auf A gibt es eine eindeutig bestimmte Algebra $\mathfrak{A} = (A, (\omega_i^A)_{i \in I})$, sodass g ein Isomorphismus von $\mathfrak{A}$ nach $\mathfrak{B}$ ist. In dieser Algebra $\mathfrak{A}$ ist $\mathfrak{U}$ Unteralgebra. □

3.0.8 Beispiel. Sei $(\mathbb{R}, +, \cdot)$ der Körper der reellen Zahlen, und seien die Operationen $+$ und $\cdot$ auf $\mathbb{R} \times \mathbb{R}$ definiert durch:

$$(a_1, a_2) + (b_1, b_2) := (a_1 + b_1, a_2 + b_2), \quad (a_1, a_2) \cdot (b_1, b_2) := (a_1 b_1 - a_2 b_2, a_1 b_2 + a_2 b_1).$$

Dann ist auch $(\mathbb{R} \times \mathbb{R}, +, \cdot)$ ein Körper und $f : \mathbb{R} \to \mathbb{R} \times \mathbb{R}$, $f(x) := (x, 0)$, ein Monomorphismus. Wendet man auf diese Situation das Prinzip der isomorphen Einbettung an, so erhält man den Körper $(\mathbb{C}, +, \cdot)$ der komplexen Zahlen, der isomorph ist zu $(\mathbb{R} \times \mathbb{R}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ als Unterkörper enthält. Nach Konstruktion ist daher: $\mathbb{C} := ((\mathbb{R} \times \mathbb{R}) \setminus f(\mathbb{R})) \cup \mathbb{R}$, und mit $i := (0, 1)$ gilt $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$.

3.1 Termalgebra

Sei X eine Menge von „Variablen“. Ein Term (in den Variablen aus X) ist ein formaler Ausdruck, den man durch sinnvolles Kombinieren von Operationssymbolen $\dot{\omega}_i$ mit den Variablen $x \in X$ bekommt. Anders ausgedrückt: Ein Term baut sich aus Variablen und Konstantensymbolen (=Symbolen für 0-stellige Operationen) mit Hilfe der anderen Operationssymbole auf.
Diese informelle Definition kann man wie folgt formal fassen:

3.1.1 Definition. Sei $S = S(X)$ die Menge aller „Strings“ (Zeichenketten), die man durch Aneinanderreihen von Variablen und Operationssymbolen erhält.[2]
Für jedes Operationssymbol $\dot{\omega}_i$ definieren wir eine n_i-stellige Funktion auf S, die jedem n_i-Tupel $(s_1, \ldots, s_{n_i})$ den neuen String $\dot{\omega}_i s_1 \cdots s_{n_i}$ zuordnet. (Für $n_i = 0$ ist das einfach der String $\dot{\omega}_i$.) Diese Funktion bezeichnen wir mit ω_i^S oder einfach mit ω_i.
Die Menge S wird dadurch zu einer Algebra vom Typ $\vec{n}$.
Die Menge $\mathbb{T}(X)$ aller Terme ist nun die durch die Menge X erzeugte Unteralgebra von $S(X)$. Meistens ist X eine endliche Menge $\{x_1, \ldots, x_n\}$. Statt $\mathbb{T}(\{x_1, \ldots, x_n\})$ schreiben wir dann $\mathbb{T}(x_1, \ldots, x_n)$.

[2]Formal ist ein „String“ der Länge n eine Funktion von $\{0, \ldots, n-1\}$ in die Menge aller Variablen und Operationssymbole. Wir werden im Allgemeinen aber nicht zwischen einem String der Länge 1 und dem in diesem String verwendeten Symbol unterscheiden.

Da man bei gewissen Symbolen (wie $+$, $\cdot$) traditionellerweise Infixnotation verwendet, vereinbaren wir, dass der Ausdruck $x + y$ eine inoffizielle Schreibweise für den Term $+xy$ ist; bei komplizierteren Termen müssen wir in der Infixnotation Klammern einführen.
Die Menge X ist meistens eine „genügend große“ endliche Menge, gelegentlich auch die abzählbare Menge $\{x_1, x_2, \dots\}$. Jeder Term verwendet natürlich nur endlich viele dieser Variablen. Wenn es nur endlich viele oder höchstens abzählbar viele Operationssymbole gibt (d.h., wenn die Menge I höchstens abzählbar ist), dann ist die Menge $\mathbb{T}(X)$ eine abzählbare[3] Menge.

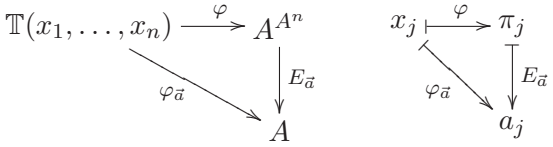
3.1.2 Lemma (Einsetzungshomomorphismus mit festem Parameter)**.** *Sei A Algebra, und sei $\vec{a} = (a_1, \dots, a_n) \in A^n$.*
Dann gibt es einen (eindeutig bestimmten) Homomorphismus $\varphi_{\vec{a}} : \mathbb{T}(x_1, \dots, x_n) \to A$, der jeder Variablen x_k das Element a_k zuordnet.

3.1.3 Schreibweise. Wenn $t \in \mathbb{T}(x_1, \dots, x_n)$ ein Term ist, schreiben wir oft statt t den Ausdruck $t(x_1, \dots, x_n)$, um zu betonen, dass in t nur die Variablen $x_1, \dots, x_n$ (möglicherweise aber nicht alle) vorkommen. Das Element $\varphi_{\vec{a}}(t)$ bezeichnet man dann meist mit $t(a_1, \dots, a_n)$ oder $t(\vec{a})$.

3.1.4 Definition. Sei A eine Algebra. Für jede Menge J ist die Menge A^J aller Funktionen von J nach A (oder „J-Tupel“) ebenfalls eine Algebra. Die Operationen $\omega_i^{A^J}$ sind komponentenweise definiert.
Wenn J die Menge A^n aller n-Tupel ist, nennen wir $A^J = A^{A^n}$ die „n-stellige Funktionenalgebra auf A“.
Die Abbildung $\pi_k^n : A^n \to A$, die durch $\pi_k^n(a_1, \dots, a_n) = a_k$ definiert ist, heißt „k-te Projektion“. Sie ist ein Element von A^{A^n}.

3.1.5 Lemma (Auswertung bei $\vec{a}$)**.** *Sei $\vec{a} = (a_1, \dots, a_n) \in A^n$. Dann ist die Abbildung $E_{\vec{a}} : A^{A^n} \to A$, $f \mapsto f(\vec{a})$ ein Homomorphismus.*

3.1.6 Lemma (Einsetzungshomomorphismus mit variablem Parameter)**.** *Sei A Algebra, A^{A^n} die n-stellige Funktionenalgebra.*
Dann gibt es einen (eindeutig bestimmten) Homomorphismus $\varphi : \mathbb{T}(x_1, \dots, x_n) \to A^{A^n}$, der jeder Variable x_k die k-te Projektion π_k^n zuordnet.



3.1.7 Anmerkung. $\varphi(t)$ ist in A^{A^n}, d.h. eine Funktion von A^n nach A. Sei $\vec{a} \in A^n$. Dann können wir $\varphi(t)$ an der Stelle $\vec{a} = (a_1, \dots, a_n)$ auswerten und erhalten $\varphi(t)(\vec{a}) = \varphi_{\vec{a}}(t)$.

Dies kann man mit Induktion nach Aufbau des Terms t zeigen; wir begnügen uns hier mit dem Induktionsanfang:

> Wenn t der Term x_k ist, dann ist $\varphi(t) = \pi_k^n$, also ist $\varphi(t)(\vec{a}) = a_k$.
> Aber $\varphi_{\vec{a}}(x_k)$ ist (nach Definition) ebenfalls a_k.

[3] Nur in den folgenden beiden Fällen, die aber so gut wie nie auftreten, ist $\mathbb{T}(X)$ endlich: wenn X endlich ist und es nur endlich viele nullstelligen Operationen und keine Operationen ω_i mit $n_i > 0$ gibt, dann besteht $\mathbb{T}(X)$ nur aus den Variablen und den nullstelligen Operationen; wenn X leer ist und es keine nullstelligen Operationen gibt, dann ist $\mathbb{T}(X) = \emptyset$.

3.1.8 Anmerkung. Den Einsetzungshomomorphismus φ („mit variablem Parameter“) können wir auch als Spezialfall des Einsetzungshomomorphismus mit festem Parameter sehen; A^{A^n} ist ja eine Algebra, die unter anderem die Projektionen $\pi^n_1, \dots, \pi^n_n$ enthält. Wenn wir das n-Tupel $(\pi^n_1, \dots, \pi^n_n)$ mit $\vec{\pi}$ bezeichnen, dann ist φ genau die Abbildung $\varphi_{\vec{\pi}}$.

3.1.9 Schreibweise. Statt $\varphi(t)$ schreibt man meistens t^A; wir nennen $t^A \in A^{A^n}$ die „durch $t(x_1, \dots, x_n)$ induzierte n-stellige Termfunktion“.
Statt $\varphi_{\vec{a}}(t)$ schreiben wir $t^A(\vec{a})$ oder $t^A(a_1, \dots, a_n)$; dieses Element von A heißt „der Wert von t an der Stelle $\vec{a}$.“

3.1.10 Lemma. *Sei $h : A \to B$ eine Homomorphismus (zwischen zwei Algebren desselben Typs), und sei $t(x_1, \dots, x_n)$ ein Term. Dann gilt für alle $a_1, \dots, a_n \in A$:*

$$h(t^A(a_1, \dots, a_n)) = t^B(h(a_1), \dots, h(a_n))$$

Beweis. Sei $b_i := h(a_i)$. Die Abbildung $\varphi_{\vec{b}}$ ist ein Homomorphismus von $\mathbb{T}(x_1, \dots, x_n)$ nach B, ebenson wie die Abbildung $h \circ \varphi_{\vec{a}}$. Da diese beiden Homomorphismen auf der Erzeugendenmenge von $\mathbb{T}(x_1, \dots, x_n)$ übereinstimmen, stimmen sie auf der ganzen Termalgebra überein, insbesondere an der Stelle t: $h(\varphi_{\vec{a}}(t)) = \varphi_{\vec{b}}(t)$. □

3.2 Varietäten

3.2.1 Definition. Ein „Gesetz“ ist eine allquantifizierte[4] Gleichung zwischen Termen. (Die Terme müssen aus Variablen und den Operationen des betrachteten Typs aufgebaut sein.)

Sei Γ eine Menge von Gesetzen. Mit $\mathrm{Mod}(\Gamma)$ bezeichnen wir die Klasse aller Algebren, die alle Gesetze in Γ erfüllen.

3.2.2 Definition. Jede Klasse der Form $\mathrm{Mod}(\Gamma)$ bezeichnen wir als *gleichungsdefinierte Klasse.*[5]

3.2.3 Satz. *Sei $\mathbb{V}$ eine gleichungsdefinierte Klasse, und sei $A = (A, (\omega_i)_{i \in I})$ ein Objekt in $\mathbb{V}$. Dann gilt:*

- *Jede Unteralgebra von A ist ebenfalls in $\mathbb{V}$.*
- *Jede zu A isomorphe Algebra ist in $\mathbb{V}$.*
- *Jedes homomorphe Bild von A ist ebenfalls in $\mathbb{V}$. (D.h., wenn $f : A \to B$ surjektiver Homomorphismus ist, dann ist auch B in $\mathbb{V}$. Anders gesagt: Für jede Kongruenzrelation θ auf A gilt $A/\theta \in \mathbb{V}$.)*

Weiters gilt:

- *Sei $(A_j)_{j \in J}$ eine Familie von Algebren in $\mathbb{V}$. Dann ist auch $\prod_{j \in J} A_j$ in $\mathbb{V}$. (Dies gilt für beliebige Mengen J; insbesondere muss J nicht unbedingt endlich oder abzählbar sein.)*
- *Sei $(J, \leq)$ eine lineare Ordnung. Sei $(A_j)_{j \in J}$ eine Familie von Algebren in $\mathbb{V}$, die $i \leq j \Rightarrow A_i \leq A_j$ erfüllt. Dann ist auch die Vereinigung $\bigcup_i A_i$ (das heißt, der direkte Limes dieser Algebren, siehe 2.4.1) in $\mathbb{V}$.*

[4] Oft schreibt man die Allquantoren nicht explizit an; statt $\forall x \forall y\, (xy = yx)$ oder $\forall x\, (x * x^{-1} = e)$ schreibt man also kürzer $xy = yx$ bzw $x * x^{-1} = e$, auch wenn man das allgemeine Gesetz und keine konkrete Instanz meint.

[5] englisch: *equationally defined class*

Beweis. Man rechnet leicht nach, dass alle Gesetze, die in A gelten, „erst recht“ in Unteralgebren und in homomorphen Bildern gelten.
Die Gültigkeit von Gesetzen in einem direkten Produkt rechnet man komponentenweise nach. Da jede aufsteigende Vereinigung von Algebren homomorphes Bild einer Unteralgebra des direkten Produkts dieser Algebren ist, überträgt sich die Gültigkeit von Gesetzen auch auf aufsteigende Vereinigungen. □

3.2.4 Definition. Wir nennen[6] eine Klasse von Algebren *Varietät*[7], wenn sie unter homomorphen Bildern (speziell also auch unter Isomorphie), Unteralgebren und Produkten[8] abgeschlossen ist.[9]

3.2.5 Anmerkung. Nach dem obigen Satz gilt also: Jede gleichungsdefinierte Klasse ist eine Varietät. Es gilt aber auch die Umkehrung: Jede Varietät $\mathbb{K}$ ist eine gleichungsdefinierte Klasse. (Satz von Birkhoff) [10]

Die einelementige Algebra

Zu jedem Typ gibt es eine (bis auf Isomorphie eindeutige) einelementige Algebra dieses Typs. Diese Algebra liegt in jeder Varietät. Sie tritt als Produkt der leeren Familie (d.h., einer Familie $(A_j)_{j\in J}$ mit $J = \emptyset$) auf.
Wenn die Menge Γ das Gesetz $x = y$ enthält, dann enthält $\mathrm{Mod}(\Gamma)$ nur einelementige Algebren. Solche Varietäten nennen wir *ausgeartet*.[11]
Gelegentlich werden wir „ohne Beschränkung der Allgemeinheit“ solche Varietäten von unseren Überlegungen ausschließen, oder genauer: nur nicht-ausgeartete Varietäten betrachten, und den (meist uninteressanten) Fall der ausgearteten Varietäten dem Leser überlassen.
Sobald eine Varietät nicht nur einelementige Algebren enthält, enthält sie bereits beliebig große Algebren. Wenn nämlich A mindestens 2 Elemente hat, dann hat $\prod_{j\in J} A = A^J$ mehr Elemente als die Menge J.

3.3 Beispiele von freien Algebren

3.3.A Die frei von einem Element erzeugte Gruppe

Die Gruppe $\mathbb{Z}$ wird vom Element 1 erzeugt, ist also zyklisch.
Sei G eine beliebige zyklische Gruppe, d.h., G wird von einem Element g erzeugt: $G = \langle g\rangle$. Dann lässt sich jedes Element von G als g^n (mit einem $n \in \mathbb{Z}$) darstellen, und die Abbildung $n \mapsto g^n$ ist ein Homomorphismus von $(\mathbb{Z}, +)$ auf G, wobei der Erzeuger 1 der Gruppe $\mathbb{Z}$ auf den Erzeuger g der Gruppe G abgebildet wird.
In gewissem Sinn ist also $\mathbb{Z}$ die allgemeinste zyklische Gruppe.

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

[7] englisch: *variety*

[8] Das leere Produkt $\prod_{i\in I} A_i$ wird als die einelementige Menge $\{\emptyset\}$ definiert, die nur das leere $\emptyset$-Tupel enthält; sie ist Element jeder Varietät. Gelegentlich wird auch explizit gefordert, dass Varietäten nicht leer sind; als homomorphes Bild jeder Algebra sind die einelementigen Algebren dann Elemente jeder Varietät.

[9] Für eine Klasse $\mathbb{K}$ von Algebren bezeichnet man mit $H\mathbb{K}$ die Menge aller homomorphen Bilder von Elementen von $\mathbb{K}$, analog sei $S\mathbb{K}$ die Menge aller Unteralgebren von Elementen von $\mathbb{K}$, und $P\mathbb{K}$ die Menge aller Produkte von Algebren in $\mathbb{K}$. Eine Varietät ist also eine Klasse von Algebren, die unter H, S und P abgeschlossen ist.

[10] Die Nomenklatur ist nicht immer eindeutig. Das Wort „Varietät“ wird manchmal für gleichungsdefinierte Klassen verwendet, und umgekehrt werden gleichungsdefinierte Klassen manchmal als Klassen von Algebren definiert, die unter H, S und P abgeschlossen sind.

[11] englisch: *degenerate*

3.3.B Die frei von zwei Elementen erzeugte kommutative Gruppe

Die kommutative Gruppe $\mathbb{Z} \times \mathbb{Z}$ wird von den beiden Elementen $(1,0)$ und $(0,1)$ erzeugt. Sei nun $(G,+)$ eine kommutative Gruppe, die von 2 Elementen g_1 und g_2 erzeugt wird: $G = \langle\{g_1, g_2\}\rangle$. Dann ist die Menge $\{n_1g_1 + n_2g_2 \mid n_1, n_2 \in \mathbb{Z}\}$ unter $+$ und $-$ abgeschlossen, also eine Untergruppe von G. Da diese Menge g_1 und g_2 enthält, muss sie ganz G sein.
Die Abbildung $(n_1, n_2) \in \mathbb{Z} \times \mathbb{Z} \mapsto n_1g_1 + n_2g_2$ ist also surjektiv von $\mathbb{Z} \times \mathbb{Z}$ auf G. Man sieht leicht, dass diese Abbildung ein Homomorphismus ist, wobei die beiden Erzeuger $(1,0)$ und $(0,1)$ der Gruppe $\mathbb{Z} \times \mathbb{Z}$ auf die Erzeuger g_1 und g_2 der Gruppe G abgebildet werden.
Eine nichtkommutative Gruppe H lässt sich natürlich nicht als homomorphes Bild von $\mathbb{Z} \times \mathbb{Z}$ schreiben, weil das Bild einer kommutativen Gruppe wieder kommutativ sein muss.
Allgemein gelten im homomorphen Bild einer Algebra A immer zumindest alle Gesetze, die auch in A gelten — möglicherweise aber mehr. Wenn $h : A \to B$ ein surjektiver Homomorphismus ist, dann ist also A in dem Sinn „freier“ als die Algebra B, dass in A eher weniger Gesetze als in B gelten. In dieser Sprechweise ist also $\mathbb{Z} \times \mathbb{Z}$ die freieste aller 2-erzeugten kommutativen Gruppen.
Analog kann man zeigen, dass $\mathbb{Z}^n$ von den n „Einheitsvektoren“ $(1,0,\ldots,0), \ldots, (0,\ldots,0,1)$ frei erzeugt wird.

3.4 Definition der freien Algebra

Ab jetzt betrachten wir in diesem Kapitel immer nur Klassen $\mathbb{K}$ von Algebren, die **unter Unteralgebren abgeschlossen** sind: Wenn $A \in \mathbb{K}$ und $B \leq A$, dann $B \in \mathbb{K}$.

3.4.1 Definition. Sei $\mathbb{K}$ eine Klasse von Algebren des gleichen Typs. Sei $B \subseteq F$ und $F \in \mathbb{K}$. Wir sagen, dass F „frei (in $\mathbb{K}$)“ über B ist, wenn gilt:

- Für jede Algebra $C \in \mathbb{K}$ lässt sich jede **Abbildung** $j : B \to C$ zu einem eindeutigen **Homomorphismus** $h : F \to C$ fortsetzen.

3.4.2 Anmerkung. Die obige Definition besagt, dass für jede Abbildung $j : B \to C$ zwei Bedingungen erfüllt sein müssen:

(1) Es gibt mindestens einen Homomorphismus von F nach C, der j fortsetzt.

(2) Es gibt höchstens einen Homomorphismus von F nach C, der j fortsetzt.

Oft verwendet man die folgende äquivalente Definition (wir werden die Äquivalenz gleich nachprüfen, siehe 3.4.3 und 3.4.6):
Die Algebra $F \in \mathbb{K}$ ist genau dann frei[12] über $B \subseteq F$, wenn die folgenden Bedingungen erfüllt sind:

(1) Für alle Algebren $C \in \mathbb{K}$ und alle Abbildungen $j : B \to C$ gibt es mindestens einen Homomorphismus von F nach C, der j fortsetzt.

(2') $\langle B\rangle = F$, d.h. B erzeugt F.

Die Eigenschaft (2') ist leichter nachzuprüfen als (2), da (2') sich nur auf die Algebra F bezieht. Aus (2') folgt sofort (2), wie aus dem folgenden Hilfssatz hervorgeht:

3.4.3 Hilfssatz. *Wenn A_1, A_2 Algebren in $\mathbb{K}$ sind, $E \subseteq A_1$ ein Erzeugendensystem, dann ist jeder Homomorphismus $f : A_1 \to A_2$ durch $f{\restriction}E$ eindeutig bestimmt.*

[12] Wegen dieser Charakterisierung sagen wir statt „F ist in $\mathbb{K}$ frei über B“ auch oft: „F wird in $\mathbb{K}$ von B frei erzeugt“.

Beweis. Sei $g : A_1 \to A_2$ ein Homomorphismus mit $g{\restriction}E = f{\restriction}E$. Dann ist $\{x \in A_1 \mid g(x) = f(x)\}$ eine Unteralgebra von A_1, die ganz E enthält, muss also ganz A_1 sein. □

3.4.4 Beispiel. Sei K ein Körper, und sei $\mathbb{V}$ die Klasse der K-Vektorräume. (Wir verwenden eine nullstellige Operation 0, eine einstellige Operation $-$, eine zweistellige Operation $+$, und für jedes Element $k \in K$ eine einstellige Operation, die Skalarmultiplikation mit k.) Sei $V \in \mathbb{V}$, $B \subseteq V$. Dann gilt:

$$V \text{ ist frei über } B \quad \Leftrightarrow \quad B \text{ ist Basis von } V.$$

Beweis. Sei B Basis von V. Dann lässt sich jeder Vektor $v \in V$ eindeutig als Linearkombination $v = \sum_i \lambda_i b_i$ von Elementen von B darstellen. Sei $f : B \to W$ eine Abbildung von B in einen beliebigen K-Vektorraum W, dann ist die Abbildung

$$\sum_i \lambda_i b_i \mapsto \sum_i \lambda_i f(b_i)$$

erstens wohldefiniert auf ganz V, zweitens linear, daher drittens ein Homomorphismus von V nach W, und viertens eine Fortsetzung der Abbildung f. Die Eindeutigkeit ist ebenfalls leicht einzusehen.
Daher ist V frei über B.
Sei nun V frei über B. Wir wollen zeigen, dass B linear unabhängig ist und ganz V aufspannt.
Sei W ein Vektorraum mit einer genügend großen Basis (oder jedenfalls linear unabhängigen Menge) C; „genügend groß“ heißt hier, dass es eine injektive Abbildung $f : B \to C$ geben soll. (So einen Vektorraum gibt es, z.B. K^B, die Menge aller Abbildungen von B nach K.)
Da V von B frei erzeugt wird, gibt es eine lineare Abbildung $h : V \to W$, die f fortsetzt. Weil h linear und $h{\restriction}B$ injektiv ist, übersetzt h jede nichttriviale Linearkombination von Elementen von B in eine nichttriviale Linearkombination von Elementen von C. Da C linear unabhängig ist, muss B es also auch sein.
Wir zeigen nun, dass B bereits ganz V_1 erzeugt. (Dies folgt ganz allgemein im Lemma 3.4.6, aber für den konkreten Spezialfall geben wir einen Beweis hier.)
Sei V_1 der von B aufgespannte Unterraum von V, und sei V_2 ein Komplement von V_1 (d.h., V_2 ist ein Unterraum mit $V_1 \cap V_2 = \{0\}$, und $V_1 \cup V_2$ spannt ganz V auf). Wenn V_2 nicht trivial wäre, dann hätte die Identitätsabbildung id_B mehr als eine Fortsetzung zu einer linearen Abbildung $V \to V$, nämlich zum Beispiel die Identität und die Projektion auf V_1; also muss $V_1 = V$ gelten, und B ist tatsächlich eine Basis. □

3.4.5 Lemma (Eindeutigkeit der freien Algebra)**.** *Sei $\mathbb{K}$ eine Klasse von Algebren. Mit „frei“ meinen wir im Folgenden immer „frei in $\mathbb{K}$“ (gemäß 3.4.1).*

(*a*) *Sei F frei über B. Dann gibt es außer der Identität auf F keinen Homomorphismus $h : F \to F$, der auf B die Identität ist.*

(*b*) *Sei F_1 frei über B_1, F_2 frei über B_2, und sei $j : B_1 \to B_2$ eine Bijektion. Dann gibt es einen (eindeutig bestimmten) Isomorphismus $h : F_1 \to F_2$ mit $h{\restriction}B_1 = j$.*

(*c*) *Wenn F_1 und F_2 beide frei über B sind, dann gibt es einen Isomorphismus $h : F_1 \to F_2$, der auf B die Identität ist.*
Kurz gesagt: Wenn F frei über B ist, dann ist F bis auf Isomorphie eindeutig bestimmt.

Beweis. (a) Nach Definition gibt es genau einen Homomorphismus von F nach F, der die Identität auf B fortsetzt, und die Identität auf F ist so ein Homomorphismus.
(b) Sei $h : F_1 \to F_2$ der eindeutig bestimmte Homomorphismus, der j fortsetzt, und sei $h' : F_2 \to F_1$ der eindeutig definierte Homomorphismus, der $j^{-1} : B_2 \to B_1$ fortsetzt.
Dann setzen sowohl $h' \circ h : F_1 \to F_1$ als auch id_{F_1} die Identität auf B_1 fort; weil F_1 frei über B_1 ist, muss $h' \circ h = id_{F_1}$ sein. Analog zeigt man $h \circ h' = id_{F_2}$. Daher ist h Isomorphismus.
(c) Spezialfall von (b) mit $B_1 = B_2$. □

3.4.6 Lemma. *Sei F in $\mathbb{K}$ frei über B. Dann wird F von B erzeugt, d.h., es gibt keine echte Unteralgebra von F, die B enthält. (Damit haben wir gezeigt, dass (2') aus (1) und (2) folgt.)*
(Statt „F ist frei über B" sagen wir daher auch: „F wird durch B frei erzeugt".)

Beweis. Sei $F_0 := \langle B \rangle$ die von B erzeugte Unteralgebra. F_0 liegt in $\mathbb{K}$. Wir wollen zeigen, dass F_0 frei über B ist.
Sei $C \in \mathbb{K}$, und sei $j : B \to C$ eine beliebige Abbildung.
Sei $h : F \to C$ ein Homomorphismus, der j auf ganz F fortsetzt, dann ist $h{\restriction}F_0$ Homomorphismus von F_0 nach C, der j fortsetzt; daher gibt es mindestens einen solchen Homomorphismus.
Nach dem Hilfssatz 3.4.3 gibt es höchstens einen solchen Homomorphismus. Daher schließen wir, dass auch F_0 frei über B ist.
Nach dem vorigen Lemma 3.4.5 gibt es einen Isomorphismus $h : F_0 \to F$, der die Identität auf B und somit — wieder auf Grund der Eindeutigkeit — die Identität auf F_0 ist. Also ist $F_0 = F$. □

3.4.7 Lemma. *Sei F in $\mathbb{K}$ frei über B, und sei $B_0 \subseteq B$.*
Sei $F_0 := \langle B_0 \rangle$ die von B_0 in F erzeugte Unteralgebra.
Dann ist F_0 von B_0 frei erzeugt.

Beweis. Sei $C \in \mathbb{K}$, und sei $j_0 : B_0 \to C$. Gesucht ist ein Homomorphismus $h : F_0 \to C$ (die Eindeutigkeit folgt aus dem Hilfssatz 3.4.3: $F_0 = \langle B_0 \rangle$, daher ist jeder auf F_0 definierte Homomorphismus bereits durch seine Einschränkung auf B_0 eindeutig bestimmt).
Der Fall, dass $C = \emptyset$ ist, kann nur dann eintreten, wenn auch $B_0 = \emptyset$ ist und der Typ der betrachteten Algebren keine nullstelligen Operationen enthält. In diesem Fall ist B_0 bereits Unteralgebra von F, also $F_0 = B_0 = \emptyset$, und $j_0 : B_0 \to C$ ist bereits Homomorphismus.
Wir betrachten nun den (interessanteren) Fall, dass $C \neq \emptyset$ gilt. Dann können wir j_0 zu einer Abbildung $j : B \to C$ fortsetzen (j ist im Allgemeinen nicht eindeutig). Die Abbildung j lässt sich zu einem Homomorphismus $h : F \to C$ fortsetzen; $h_0 := h{\restriction}F_0$ ist nun ein Homomorphismus von F_0 nach C, der j_0 fortsetzt. □

3.4.8 Beispiel. Sei G_n die Gruppe $\mathbb{Z}^n$, und sei $B_n := \{b_1, \ldots, b_n\}$ die Menge der n „Einheitsvektoren", d.h., $b_1 := (1, 0, \ldots, 0)$, $\ldots$, $b_n := (0, \ldots, 0, 1)$. Dann ist G_n die von B_n frei erzeugte kommutative Gruppe.

Beweis. Sei H eine Gruppe, und sei $f : B \to H$ eine beliebige Abbildung. Wir behaupten, dass die Abbildung $h : G_n \to H$, die durch

$$h(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i f(b_i)$$

definiert ist[13], erstens ein Homomorphismus von G_n nach H ist, zweitens f fortsetzt, und drittens der einzige Homomorphismus ist, der diese Bedingungen erfüllt. Alle drei Behauptungen sind leicht nachzurechnen; die dritte folgt aus der Tatsache, dass $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ sich als

$$(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i b_i$$

schreiben lässt. □

3.4.9 Lemma (Charakterisierung der freien Algebra)**.** *Sei $\mathbb{K}$ Klasse von Algebren.*

1. *Sei $F \in \mathbb{K}$ von der n-elementigen Menge $\{a_1, \ldots, a_n\}$ in $\mathbb{K}$ frei erzeugt. Dann gilt*

   $(*)_n$ *Für alle Terme $s, t \in \mathbb{T}(x_1, \ldots, x_n)$ und alle Algebren $C \in \mathbb{K}$:*
   Wenn $s^F(a_1, \ldots, a_n) = t^F(a_1, \ldots, a_n)$,
   dann gilt das Gesetz $s \approx t$ in C.
   (Das heißt: für alle $c_1, \ldots, c_n \in C$ gilt $s^C(c_1, \ldots, c_n) = t^C(c_1, \ldots, c_n)$.)

2. *Sei $F \in \mathbb{K}$ und $F = \langle\{a_1, \ldots, a_n\}\rangle$. Wenn $(*)_n$ gilt, dann wird F von $\{a_1, \ldots, a_n\}$ frei erzeugt.*

3. *Analoges gilt für Algebren in $\mathbb{K}$, die von unendlichen Mengen erzeugt werden: Wenn $F = \langle\{a_i \mid i \in I\}\rangle \in \mathbb{K}$ (und alle a_i verschieden sind), dann sind folgenden Bedingungen äquivalent:*

   - *Für alle n, alle Terme $s, t \in \mathbb{T}(x_1, \ldots, x_n)$, alle $i_1, \ldots, i_n \in I$ und alle Algebren $C \in \mathbb{K}$:*
     Wenn $s^F(a_{i_1}, \ldots, a_{i_n}) = t^F(a_{i_1}, \ldots, a_{i_n})$, dann gilt das Gesetz $s \approx t$ in C.
   - *F wird von $\{a_i \mid i \in I\}$ in $\mathbb{K}$ frei erzeugt.*

Beweis. 1. Seien $c_1, \ldots, c_n \in C$. Da F frei ist, gibt es einen Homomorphismus $h : F \to C$ mit $h(a_i) = c_i$. Wegen Lemma 3.1.10 gilt

$$s^C(\vec{c}) = s^C(h(a_1), \ldots, h(a_n)) = h(s^F(a_1, \ldots, a_n)) = h(t^F(a_1, \ldots, a_n)) = \cdots = t^C(\vec{c}).$$

2. Sei $j : \{a_1, \ldots, a_n\} \to C$ eine beliebige Abbildung; sei $\vec{c} := (j(a_1), \ldots, j(a_n))$.
Wir definieren einen Abbildung $h : F \to C$ durch $h(t^F(\vec{a})) := t^C(\vec{c})$. Aus der Voraussetzung $(*)_n$ folgt, dass h tatsächlich wohldefiniert ist. Wenn man für t speziell den Term x_i einsetzt, der ja in jeder Algebra durch die i-te Projektion interpretiert wird, erhält man $h(a_i) = c_i = j(a_i)$.
Zu zeigen ist noch, dass h Homomorphismus ist. Dazu verwenden wir $h \circ \varphi_{\vec{a}} = \varphi_{\vec{c}}$ und das folgende Lemma 3.4.10.

3. Ähnlich. □

3.4.10 Lemma. *Seien A, B, C Algebren eines festen Typs, seien $f : A \to B$ und $g : A \to C$ Homomorphismen, und sei $h : B \to C$ eine Abbildung, die $h \circ f = g$ erfüllt. Wenn f surjektiv ist, dann muss h Homomorphismus sein.*

Beweis. Sei ω eine k-stellige Operation, für die wir $h(\omega^B(b_1, \ldots, b_k)) = \omega^C(h(b_1), \ldots, h(b_k))$ überprüfen müssen. Wir können $\vec{a} = (a_1, \ldots, a_k)$ mit $f(a_i) = b_i$ finden; sei weiters $\vec{c} := (h(b_1), \ldots, h(b_k))$.
Dann ist $\omega^B(\vec{b}) = f(\omega^A(\vec{a}))$, weil f Homomorphismus ist. Weiters gilt $h(\omega^B(\vec{b})) = h(f(\omega^A(\vec{a})))$ $= g(\omega^A(\vec{a})) = \omega^C(\vec{c})$, da auch g Homomorphismus ist. □

[13] Man beachte, dass die auf der rechten Seite auftretende Multiplikation $x_i f(b_i)$ die in 1.3 definierte Kurzschreibweise für wiederholte Addition ist.

3.5 Die freie Halbgruppe

Sei B eine Menge von „Buchstaben“. Mit B^+ bezeichnen wir die Menge aller nichtleeren „Worte“ (oder „Zeichenketten“) aus diesen Buchstaben, d.h. die Menge aller endlichen Folgen von Elementen aus B der Länge > 0. (Eine Folge von Elementen von B der Länge n kann man entweder naiv als „Aneinanderreihung“ (oder „Konkatenation“) von n Buchstaben verstehen[14], oder als Abbildung von der Menge $\{0, \dots, n-1\}$ in die Menge B.)
Mit ε bezeichnen wir die leere Folge, oder Folge der Länge 0. (Als Abbildung ist ε die leere Menge.) Wir setzen $B^* := B^+ \cup \{\varepsilon\}$.
Oft unterscheidet man nicht zwischen dem Buchstaben x und dem einbuchstabigen Wort x.
Auf der Menge B^* ist eine natürliche zweistellige Operation erklärt, die „Verkettung“ oder Aneinanderreihung. Diese Operation ist assoziativ[15], mit neutralem Element ε.
B^+ ist also eine Halbgruppe, B^* ein Monoid. Tatsächlich ist B^+ die von B frei erzeugte Halbgruppe, und B^* ist das von B frei erzeugte Monoid. Jedes Element von B^+ lässt sich nämlich eindeutig als Produkt von Elementen von B schreiben, dadurch ergibt sich für jede Abbildung $f : B \to H$ in eine beliebige Halbgruppe H eine natürliche Fortsetzung $h : B^+ \to H$, von der man leicht zeigen kann, dass sie ein Homomorphismus ist.
Spezialfall: Sei $B = \{x\}$. Dann besteht die frei von B erzeugte Halbgruppe aus den Strings $\{x, xx, xxx, \dots\} = \{x^n \mid n = 1, 2, \dots\}$, und das freie Monoid enthält zusätzlich das Leerwort.

3.6 Die Termalgebra als freie Algebra

Sei $\mathbb{K}$ die Klasse aller Algebren eines fixen Typs. Dann ist die Termalgebra $\mathbb{T}(x_1, \dots, x_n)$ in $\mathbb{K}$ frei von $\{x_1, \dots, x_n\}$ erzeugt.
Dies ist bloß eine Umformulierung von Lemma 3.1.2.

Ebenso[16] ist $\mathbb{T}(x_1, \dots, x_n, \dots)$ frei von $\{x_1, \dots, x_n, \dots\}$ erzeugt. Die Algebra $\mathbb{T}(x_1, \dots, x_n, \dots)$ heißt manchmal auch „absolut freie Algebra“.

3.7 Die freie Gruppe

3.7.A 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 ist die Menge aller Zeichenfolgen, die man mit den „Buchstaben“ aus B und $\bar{B}$ bilden kann (inklusive der leeren Folge).
Auf dem Monoid M definieren wir eine Relation $\sim$, von der wir zeigen werden:

[14] Stillschweigend wird hier immer vereinbart, dass Buchstaben selbst keine Folgen sind, und dass sich jedes Wort eindeutig aus Buchstaben zusammensetzt; wenn nämlich zum Beispiel die Buchstaben x, y, z in Wirklichkeit die Folgen a, b, ab wären, dann könnte man nicht zwischen dem 2-buchstabigen Wort xy und dem 1-buchstabigen Wort z unterscheiden.

[15] Wenn wir die Worte v und w als Funktionen von $\{0, \dots, n-1\}$ bzw $\{0, \dots, k-1\}$ nach B auffassen, dann ist vw, die Verkettung von v und w, eine Funktion von $\{0, \dots, n+k-1\}$ nach B. Für $i < n$ ist ihr Wert $v(i)$, für $n \leq i < n+k$ ist er $w(i-n)$. Mit dieser Definition lässt sich die Assoziativität auch formal beweisen, wir ziehen aber hier den anschaulichen Zugang vor.

[16] Man könnte die Termalgebra auch über einer überabzählbaren Menge von Variablen definieren und würde dann eine Algebra erhalten, die in $\mathbb{K}$ frei über einer überabzählbaren Menge ist. Meistens beschränkt man sich aber auf abzählbare Mengen von Variablen, weil für Resultate über Gleichungen und Terme meistens nur endlich oder abzählbar erzeugte Algebren eine Rolle spielen.

1. $\sim$ ist Kongruenzrelation.

2. $M/\sim$ ist nicht nur Monoid sondern sogar Gruppe.

3. Die kanonische Abbildung k von M nach $M/\sim$ ist auf der Menge B injektiv. (Äquivalent: Für alle $b \neq b'$ in B gilt $b \not\sim b'$.)

4. $M/\sim$ ist die von $k(B)$ frei erzeugte Gruppe.

Für zwei Worte $w, w' \in M$ definieren wir $w \rightsquigarrow w'$ genau dann, wenn w' aus w hervorgeht, indem man in w einen Buchstaben x gegen sein „Inverses“ $\bar{x}$ „kürzt“. Genauer: $w \rightsquigarrow w'$ gilt genau dann, wenn man $w = ux\bar{x}v$ (oder $w = u\bar{x}xv$) schreiben kann, und $w' = uv$ ist.
Mit $\sim$ bezeichnen wir die reflexive symmetrische transitive Hülle von $\rightsquigarrow$, also die kleinste Äquivalenzrelation, die $\rightsquigarrow$ enthält.
(Genauer: $w \sim w'$ gilt genau dann, wenn $w = w'$ ist, oder es eine endliche Folge $(w_0, \ldots, w_n)$ gibt, für die $w = w_0$ gilt, $w' = w_n$, und für alle $i < n$: $w_i \rightsquigarrow w_{i+1}$ oder $w_{i+1} \rightsquigarrow w_i$.)

3.7.B Freiheit

Da $\rightsquigarrow$ mit der Konkatenation verträglich ist, ist es auch $\sim$ (Beweis mit Induktion), daher ist $\sim$ eine Halbgruppenkongruenz, somit ist $M/\sim$ eine Halbgruppe (und sogar ein Monoid).
Da $x\bar{x} \sim \varepsilon \sim \bar{x}x$ gilt, gibt es in $M/\sim$ zu jedem Element von $B \cup \bar{B}$ ein Inverses. Es hat sogar jedes Element ein Inverses; das Inverse erhält man, indem man die Reihenfolge der Buchstaben umdreht und jedes b mit dem entsprechenden $\bar{b}$ vertauscht. Z.B. ist $(b_1\bar{b}_2\bar{b}_2\bar{b}_1b_2)^{-1} = \bar{b}_2b_1b_2b_2\bar{b}_1$.
Daher ist $M/\sim$ eine Gruppe.
Zu zeigen ist nun, dass für $b \neq b'$ niemals $b \sim b'$ gelten kann. Dazu „zählen“ wir einfach, wie oft b in jedem Wort vorkommt.
Genauer: Für jedes b definieren wir eine Abbildung $\|\cdot\|_b$: $(B \cup \bar{B})^* \to \mathbb{Z}$, via Hilfsfunktionen $\mathbf{n}_b^+$ und $\mathbf{n}_b^-$:

- $\mathbf{n}_b^+(w)$ = Anzahl der Vorkommnisse von b in w
- $\mathbf{n}_b^-(w)$ = Anzahl der Vorkommnisse von $\bar{b}$ in w
- $\|w\|_b := \mathbf{n}_b^+(w) - \mathbf{n}_b^-(w)$

Insbesondere ist $\|b\|_b = 1$, $\|\varepsilon\|_b = 0$.
Offenbar sind die Abbildungen $\mathbf{n}_b^+$, $\mathbf{n}_b^-$ (und daher auch $\|\cdot\|_b$) mit der Verkettung verträglich, d.h. Monoidhomomorphismen von $(B \cup \bar{B})^*$ nach $(\mathbb{Z}, +)$. Für $w \rightsquigarrow w'$ gilt aber $\|w\|_b = \|w'\|_b$, denn entweder ist $\mathbf{n}_b^+(w) = \mathbf{n}_b^+(w')$ und $\mathbf{n}_b^-(w) = \mathbf{n}_b^-(w')$, oder beide Werte $(\mathbf{n}_b^+, \mathbf{n}_b^-)$ werden beim Übergang von w zu w' um 1 kleiner.
Daher gilt (Induktion) auch $w \sim w' \;\Rightarrow\; \|w\|_b = \|w'\|_b$. Für $b \neq c$ kann also nicht $b \sim c$ gelten, denn $\|b\|_b = 1$, $\|c\|_b = 0$.
Die Abbildung $k : B \to M/\sim$, definiert durch $k(b) = b/\sim$, ist also injektiv. Wir werden zeigen, dass $M/\sim$ frei über $k(B)$ ist. Mit dem Prinzip der isomorphen Einbettung erhalten wir dann eine Gruppe, die B enthält und frei über B ist.
Zu zeigen ist also, dass die definierende Eigenschaft der „Freiheit“ erfüllt ist. Sei $j : k(B) \to G$ eine beliebige Abbildung von $k(B)$ in eine Gruppe G:

1. Zuerst definieren wir eine Abbildung $j' : B \cup \bar{B} \to G$ so:
   $j'(b) = j(k(b))$, $j'(\bar{b}) = j(k(b))^{-1}$.

2. j' können wir zu einem Monoidhomomorphismus $j'' : (B \cup \bar{B})^*$ nach G fortsetzen.

3. j'' erfüllt die Bedingung $w \rightsquigarrow w' \Rightarrow j''(w) = j''(w')$.
   Wenn nämlich $w = ub\bar{b}v$ und $w' = uv$ ist, dann ist $j''(b)j''(\bar{b}) = 1$, also

$$j''(w) = j''(u)j''(b)j''(\bar{b})j''(v) = j''(u)j''(v) = j''(w').$$

   Daher gilt auch $w \sim w' \Rightarrow j''(w) = j''(w')$.

4. Also ist die Abbildung $j^* : (B \cup \bar{B})/\sim \to G$, die durch $j^*([w]_\sim) = j''(w)$ definiert ist, wohldefiniert.

5. j^* ist ein Gruppenhomomorphismus. Die Eigenschaften $j^*(w_1w_2) = j^*(w_1)j^*(w_2)$ und $j^*(w^{-1}) = j^*(w)^{-1}$ zeigt man zunächst für den Spezialfall, dass w_1, w_2, w in $(B \cup \bar{B})$ sind, dann mit Induktion für alle Elemente von $(B \cup \bar{B})^*$.

6. Nach Definition ist $j^*(k(b)) = j''(b) = j'(b) = j(k(b))$ für alle $b \in B$.

3.7.C Normalform

Die Elemente der freien Gruppe sind Äquivalenzklassen von Elementen des freien Monoids. Im Fall der Gruppen sind wir in der glücklichen Lage, aus jeder Äquivalenzklasse einen kanonischen Repräsentanten wählen zu können, nämlich den kürzesten. Eine solche Wahl ist von der Theorie her nicht notwendig, erleichtert aber viele Rechnungen.
Wir nennen eine Element $w \in (B \cup \bar{B})^*$ „reduziert“, wenn in w keine aufeinander folgenden zu einander inversen Buchstaben vorkommen, d.h., wenn w weder die Form $(\cdots)b\bar{b}(\cdots)$ noch $(\cdots)\bar{b}b(\cdots)$ hat; anders ausgedrückt: wenn es kein w' mit $w \rightsquigarrow w'$ gibt.
Man kann zeigen, dass es in jeder Äquivalenzklasse ein eindeutiges reduziertes Wort gibt, und dass der folgende Algorithmus zu jedem $w \in (B \cup \bar{B})^*$ das eindeutig bestimmte reduzierte w' mit $w \sim w'$ liefert.

1. Eingabe: w.

2. Wenn w reduziert ist, dann STOP. Ausgabe w.

3. Finde ein beliebiges[17] Paar $(b, \bar{b})$, sodass sich w als $vb\bar{b}v'$ oder $v\bar{b}bv'$ schreiben lässt.

4. Ersetze w durch $w' := vv'$. (Es gilt $w \rightsquigarrow w'$.)

5. Gehe zu 2.

3.8 Freie Algebren in Varietäten

3.8.1 Satz. *Sei $\mathbb{V}$ eine Klasse von Algebren, die unter Unteralgebren, beliebigen Produkten und isomorphen Kopien abgeschlossen ist. Nehmen wir an, dass es in $\mathbb{V}$ Algebren mit mehr als einem Element gibt, d.h. dass $\mathbb{V}$ „nicht ausgeartet“ ist.*[18]
Dann gibt es für jede Menge B eine Algebra $F \in \mathbb{V}$, die (in $\mathbb{V}$) frei über B ist.

3.8.2 Notation. Wir bezeichnen die von B frei erzeugte Algebra mit $Fr(B)$, oder genauer $Fr_{\mathbb{V}}(B)$. (Sie ist durch B bis auf Isomorphie eindeutig bestimmt.)
Für die über einer n-elementigen Menge freie Algebra schreiben wir auch $Fr(n)$.

[17] oder z.B.: das erste von links

[18] Der Satz gilt auch dann, wenn $\mathbb{V}$ ausgeartet ist; allerdings muss man für diesen Fall die Definition der „freien Algebra“ etwas modifizieren.

3.8.3 Anmerkung. Wenn $\mathbb{V}$ die Klasse aller Gruppen (aller abelschen Gruppen, aller Monoide, aller Ringe, aller Ringe mit 1) ist, dann gilt für alle natürlichen Zahlen $n \neq k$: $Fr(n) \ncong Fr(k)$ (Übung; dies gilt in jeder Varietät, in der es endliche Algebren mit mehr als einem Element gibt).
Es gibt aber Varietäten $\mathbb{V}$, in denen $Fr_{\mathbb{V}}(1) \cong Fr_{\mathbb{V}}(2)$ ist (Übung). In diesen Varietäten gilt $Fr_{\mathbb{V}}(1) \cong Fr_{\mathbb{V}}(n)$ für alle natürlichen Zahlen $n > 0$.

3.8.4 Beispiel. Sei $\mathbb{V}$ die Klasse aller Gruppen, oder allgemeiner: die Klasse aller Algebren von einem festen Typ, die eine feste Menge von Gesetzen erfüllen.
Dann ist $\mathbb{V}$ unter Unteralgebren, Produkten und homomorphen Bildern abgeschlossen, also eine Varietät, und es gibt in $\mathbb{V}$ viele freie Algebren.

Zunächst überlegen wir, dass wir, um die Freiheit einer Algebra F über einer Menge B zu überprüfen, nicht alle Algebren $C \in \mathbb{K}$ betrachten müssen, sondern nur Repräsentanten jeder Isomorphieklasse brauchen.

3.8.5 Lemma. *Sei $\mathbb{K}$ eine Klasse von Algebren, und sei $I\mathbb{K}$ die Klasse aller Algebren, die zu einer Algebra in $\mathbb{K}$ isomorph sind. Wenn F in $\mathbb{K}$ frei von B erzeugt wird, dann auch in $I\mathbb{K}$.*

Beweis. Sei $C \in I\mathbb{K}$, und sei $j : B \to C$ eine Abbildung. Dann gibt es eine Algebra $C' \in \mathbb{K}$, $C' \cong C$. Sei $k : C \to C'$ ein Isomorphismus.
Sei $j' : B \to C'$ durch $j' = k \circ j$ definiert. Weil F in $\mathbb{K}$ frei über B ist, und C' in $\mathbb{K}$ liegt, lässt sich j' zu einen Homomorphismus $h' : F \to C'$ fortsetzen, der $h' \supseteq j'$ erfüllt.
Sei nun $h := k^{-1} \circ h' : B \to C$. Als Verknüpfung von Homomorphismen ist h selbst Homomorphismus, und für $b \in B$ gilt $h(b) = k^{-1}(h'(b)) = k^{-1}(j'(b)) = k^{-1}(\,(k \circ j)(b)\,) = j(b)$. □

Als nächstes zeigen wir, dass eine von einer Menge B erzeugte Algebra nicht viel größer sein kann als B selbst.

3.8.6 Lemma. *Sei $A = \langle B \rangle$ eine Algebra, und sei $\mathbb{T}$ die Menge aller Terme in den Variablen $x_1, x_2, \ldots$, und sei $B^* = \bigcup_{n=1}^{\infty} B^n$ die Menge aller endlichen Tupel aus B.*
Dann ist A isomorph zu einer Algebra, deren Trägermenge Teilmenge von $\mathbb{T} \times B^*$ ist.

Beweis. Die Menge aller Elemente von A der Form $\varphi_{\vec{b}}(t) = t^A(b_1, \ldots, b_n)$ (mit $t \in \mathbb{T}$, $n \in \{0, 1, \ldots\}$, $b_1, \ldots, b_n \in B$) ist Unteralgebra von A, die ganz B enthält, also ganz A. Für jedes $a \in A$ können wir einen Term $t_a = t_a(x_1, \ldots, x_n)$ und ein n-Tupel $\vec{b}^a = (b_1^a, \ldots, b_n^a) \in B^n$ mit $t_a(\vec{b}^a) = a$ wählen. Dadurch erhalten wir eine Bijektion zwischen A und $\{(t_a, \vec{b}^a) \mid a \in A\}$ und somit eine zu A isomorphe Algebra A', deren Trägermenge Teilmenge von $\mathbb{T} \times B^*$ ist. □

Nun schließen wir, dass bei der Überprüfung der Freiheit einer von B erzeugten Algebra F die Fortsetzungseigenschaft nur für Abbildungen j relevant ist, die B in „wenige“ und „relativ kleine“ Algebren abbilden, genauer: In Algebren, deren Trägermenge Teilmenge einer festen Menge $Z = Z(B)$ ist.

3.8.7 Korollar. Sei $\mathbb{K}$ eine Klasse von Algebren, $F = \langle B \rangle \in \mathbb{K}$. Sei Z eine genügend große Menge, das soll heißen:

$\mathbb{T} \times B^* \subseteq Z$, oder es gibt zumindest eine injektive Abbildung von $\mathbb{T} \times B^*$ nach Z.

Dann ist F genau dann frei über B, wenn für alle $D \in \mathbb{K}$, deren Trägermenge eine Teilmenge von Z ist, gilt: Jede Abbildung $j : B \to D$ lässt sich zu einem Homomorphismus $f : B \to D$ fortsetzen.

Beweis. Sei C in $\mathbb{K}$ beliebig, $j : B \to C$. Wir suchen einen Homomorphismus $h : F \to C$, der j fortsetzt. Sei $C_0 := \langle j(B)\rangle$. Es genügt, j zu einem Homomorphismus $h : F \to C_0$ fortzusetzen, dieses h ist dann auch Homomorphismus von F nach C. Wegen unserer Annahme, dass $\mathbb{K}$ unter Unteralgebren abgeschlossen ist, ist $C_0 \in \mathbb{K}$.
Laut 3.8.6 gibt es einen Isomorphismus $k : C_0 \to C_0'$ zu einer Algebra C_0', deren Universum Teilmenge von Z ist. Nach unserer Annahme lässt sich $k \circ j : B \to C_0'$ zu einem Homomorphismus $h : F \to C_0'$ fortsetzen; wie in 3.8.5 ist dann $k^{-1} \circ h$ Homomorphismus von F nach C_0. □

Beweis von Satz 3.8.1

Sei B eine Menge; gesucht ist eine über B freie Algebra.
Sei Z eine genügend große Menge (siehe 3.8.7). Sei $\mathscr{Z}$ die Menge aller Algebren in $\mathbb{V}$, deren Trägermenge eine Teilmenge von Z ist. Wir betrachten nun die Menge aller Paare (A, j), sodass $A \in \mathscr{Z}$ ist und $j : B \to A$; wir indizieren diese Menge mit einer geeigneten Indexmenge K:

$$\{(A, j) \mid A \in \mathscr{Z},\ j : B \to A\} = \{(A_k, j_k) \mid k \in K\}.$$

Sei nun $P := \prod_{k\in K} A_k$. Da $\mathbb{V}$ unter Produkten abgeschlossen ist, ist $P \in \mathbb{V}$.
Wir definieren nun eine Abbildung $g : B \to P$ so: $g(b) = (j_k(b))_{k\in K}$. Wenn wir mit $\pi_k : P \to A_k$ die Projektion aus dem Produkt P auf den Faktor A_k bezeichnen, dann gilt also $\pi_k \circ g = j_k : B \to A_k$.
Sei $F := \langle g(B)\rangle$ die von $g(B)$ erzeugte Unteralgebra von P. Wir behaupten, dass F von $g(B)$ frei erzeugt wird, und dass $g : B \to g(B)$ injektiv ist. Mit Hilfe des Prinzips der isomorphen Einbettung erhalten wir somit eine von B frei erzeugte Algebra.
Da F Unteralgebra von P ist und $P \in \mathbb{V}$, ist auch $F \in \mathbb{V}$.

Injektivität von g

Sei $b_1 \neq b_2$. In $\mathbb{V}$ gibt es eine Algebra C mit mindestens zwei Elementen; wir können sogar $C \in \mathscr{Z}$ finden. Sei $j : B \to C$ eine Abbildung mit $j(b_1) \neq j(b_2)$.
Das Paar (C, j) kommt in unserer Aufzählung als $(C, j) = (A_{k^*}, j_{k^*})$ vor. Nun ist

$$\pi_{k^*}(g(b_1)) = j_{k^*}(b_1) = j(b_1) \neq j(b_2) = \pi_{k^*}(g(b_2)),$$

daher $g(b_1) \neq g(b_2)$.

Freiheit von F über $g(B)$

Sei C eine beliebige Algebra in $\mathbb{V}$, und $j : g(B) \to C$ eine Abbildung. Gesucht ist ein Homomorphismus $h : F \to C$.
Nach Korollar 3.8.7 dürfen wir annehmen, dass die Trägermenge von C eine Teilmenge von Z ist. (Z ist „genügend groß“ im Bezug auf B, also auch im Bezug auf $g(B)$.)
Wir betrachten nun die Abbildung $j \circ g : B \to C$. Das Paar $(C, j \circ g)$ kommt in $\mathscr{Z}$ vor, sagen wir $(C, j \circ g) = (A_{k_0}, j_{k_0})$.
Sei $h := \pi_{k_0} \restriction F : F \to A_{k_0}$. Als Einschränkung des Homomorphismus $\pi_{k_0} : P \to A_{k_0}$ auf die Unteralgebra F ist auch h ein Homomorphismus.
Sei nun $b \in B$. Dann ist

$$h(g(b)) = \pi_{k_0}(g(b)) = j_{k_0}(b) = (j \circ g)(b) = j(g(b)),$$

also setzt h die Abbildung j auf $g(B)$ fort.

3.9 Freie Algebren aus Termen

Sei $\mathbb{V}$ eine Varietät. Für zwei Terme $t_1, t_2 \in \mathbb{T}(x_1, \ldots, x_n)$ definieren wir $t_1 \approx_{\mathbb{V}} t_2$, wenn t_1 und t_2 in allen Algebren $A \in \mathbb{V}$ dieselbe Funktion liefern, d.h. (siehe Ende von Abschnitt 3.1): $t_1^A = t_2^A$. Expliziter formuliert:

$$t_1 \approx_{\mathbb{V}} t_2 \;\Leftrightarrow\; \forall A \in \mathbb{V}\; \forall a_1, \ldots, a_n \in A\; t_1(a_1, \ldots, a_n) = t_2(a_1, \ldots, a_n)$$

3.9.1 Beispiel. Betrachten wir Algebren vom Typ (2), und sei $t_1 = (x + y) + z$, $t_2 = (y + x) + z$ (beides sind Terme in den Variablen x, y, z, d.h. Elemente von $\mathbb{T}(x, y, z)$). Wenn $\mathbb{G}$ die Varietät aller Gruppen ist, dann gilt $t_1 \not\approx_{\mathbb{G}} t_2$. Wenn aber $\mathbb{A}$ die Varietät aller abelschen Gruppen ist, dann ist $t_1 \approx_{\mathbb{A}} t_2$.

Man sieht leicht, dass für jede Varietät $\mathbb{V}$ von Algebren die Relation $\approx_{\mathbb{V}}$ eine Äquivalenzrelation ist, und sogar eine Kongruenzrelation auf der Algebra[19] $\mathbb{T}(x_1, \ldots, x_n)$.
Der folgende Satz zeigt, dass wir die Elemente der freien Algebra auch als Klassen von äquivalenten Termen verstehen können.

3.9.2 Satz. *Sei $\mathbb{V}$ eine Varietät. Für $n \in \{0, 1, 2, \ldots\}$ sei F_n die über $b_1, \ldots, b_n$ freie Algebra, und sei $\mathbb{T}_n := \mathbb{T}(x_1, \ldots, x_n)$.*
Dann gilt $F_n \cong \mathbb{T}_n/{\approx_{\mathbb{V}}}$.

Beweis. Jedes Element $c \in F_n$ ist von der Form $c = t(b_1, \ldots, b_n)$ für einen Term $t \in \mathbb{T}_n$. Sei $h : F_n \to \mathbb{T}_n/{\approx_{\mathbb{V}}}$ durch $h(t(b_1, \ldots, b_n)) := t(x_1, \ldots, x_n)/{\approx_{\mathbb{V}}}$ definiert.
Im Folgenden schreiben wir abkürzend $\vec{b}$ für $(b_1, \ldots, b_n)$, und analog $\vec{x} := (x_1, \ldots, x_n)$.
Wir überprüfen nun die folgenden Punkte:

- h ist wohldefiniert.
  Wenn $t(\vec{b}) = t'(\vec{b})$ in der freien Algebra F gilt, dann gilt auch für alle Homomorphismen $g : F \to C$ in eine beliebige Algebra $C \in \mathbb{V}$:

  $$t(g(b_1), \ldots, g(b_n)) = t'(g(b_1), \ldots, g(b_n)).$$

  Da $g(b_1), \ldots, g(b_n)$ in C frei wählbar sind, gilt $t(\vec{c}) = t'(\vec{c})$ für alle $\vec{c} = (c_1, \ldots, c_n)$ in C, daher $t \approx_{\mathbb{V}} t'$, also $t/{\approx_{\mathbb{V}}} = t'/{\approx_{\mathbb{V}}}$.

- h ist Homomorphismus: leicht nachzurechnen.

- h ist surjektiv: $\mathbb{T}_n$ wird von den Termen $x_1, \ldots, x_n$ generiert; alle $x_i/{\approx_{\mathbb{V}}}$ treten im Bild von h auf, daher wird ganz $\mathbb{T}_n/{\approx_{\mathbb{V}}}$ erreicht.

- h ist injektiv: Wenn $t(\vec{x}) \approx_{\mathbb{V}} t'(\vec{x})$, dann gilt die Gleichheit zwischen diesen beiden Termen in allen Algebren in $\mathbb{V}$, also insbesondere auch in F_n. Daher ist $t(\vec{b}) = t'(\vec{b})$.

□

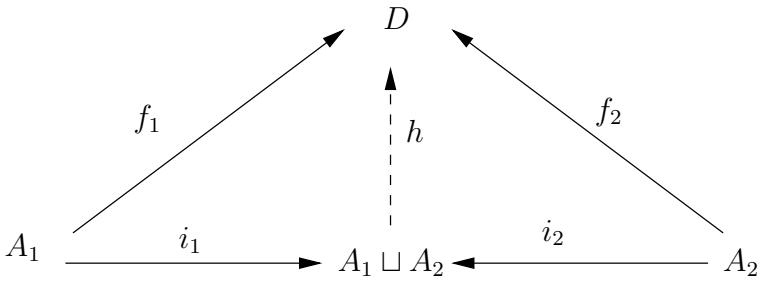
Im Fall der Gruppen und Halbgruppen ist es möglich, aus jeder Klasse einen kanonischen Repräsentanten zu wählen; mit solchen Repräsentanten lässt sich oft leichter rechnen als mit den Elementen der im vorigen Abschnitt konstruierten „abstrakten“ freien Algebra (da diese Elemente ja typischerweise Tupel mit einer sehr großen Indexmenge sind). Die Konstruktion der freien Algebra als Untermenge eines großen Produkts war aber dennoch sinnvoll, da wir in der Konstruktion $\mathbb{T}/{\approx}$ nicht (oder jedenfalls nicht in offensichtlicher Weise) garantieren können, dass $\mathbb{T}/{\approx}$ tatsächlich in $\mathbb{V}$ liegt.

[19] Man beachte, dass die Termalgebra zwar denselben Typ hat wie alle Algebren von $\mathbb{V}$, aber im allgemeinen nicht in $\mathbb{V}$ liegt. Wenn wir etwa Algebren vom Typ (2) betrachten, ist die Termalgebra zwar ein Gruppoid, aber nie Gruppe.

3.10 Koprodukte; Untergruppen von freien Gruppen

Eine Algebra A in einer Klasse $\mathbb{K}$ heißt *frei*, wenn es eine Teilmenge $B \subseteq A$ gibt, sodass A frei über B ist.
Der Satz von Nielsen-Schreier besagt, dass jede Untergruppe einer freien Gruppe selbst frei ist. Wir werden in diesem Abschnitt eine einfachere Variante dieses Satzes beweisen: Jede Untergruppe einer freien abelschen Gruppe ist eine freie abelsche Gruppe.
Für den Beweis des Satzes wird der Begriff des Koprodukts nützlich sein.

3.10.1 Definition. Sei $\mathbb{K}$ eine Klasse von Algebren, A_1, $A_2 \in \mathbb{K}$. Ein Tripel (C, i_1, i_2) heißt *Koprodukt in* $\mathbb{K}$[20] der Algebren A_1, A_2, wenn $i_1 : A_1 \to C$ und $i_2 : A_2 \to C$ Homomorphismen sind, $C \in \mathbb{K}$ gilt, und es für jede Algebra $D \in \mathbb{K}$ und für alle Homomorphismen $f_1 : A_1 \to D$ und $f_2 : A_2 \to D$ genau einen Homomorphismus $h : C \to D$ gibt, der die Bedingungen $h \circ i_\ell = f_\ell$ für $\ell = 1, 2$ erfüllt.

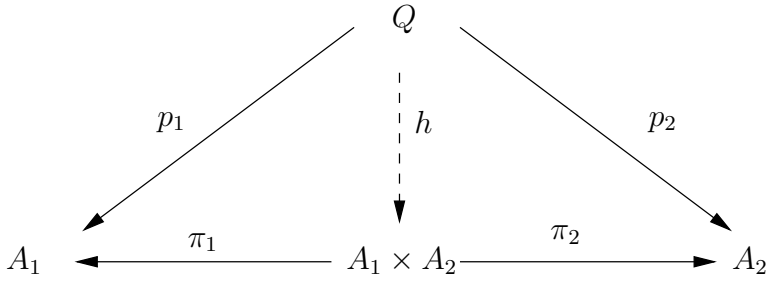


Liegt ein Koprodukt vor, so schreiben wir für die Algebra C (bzw. ihre Trägermenge) $A_1 \sqcup A_2$, auch die Schreibweise $A_1 \oplus A_2$ ist üblich. Die Abbildungen i_1 und i_2 werden oft nicht angegeben, wenn sie aus dem Kontext erschlossen werden können.

3.10.2 Anmerkung. Wenn $\mathbb{K}$ zum Beispiel die Klasse der Gruppen ist, dann müssen die in der Definition des Koprodukts vorkommenden Abbildungen i_1, i_2 injektiv sein (Übung). Es gibt aber auch Klassen, in denen Koprodukte zwar existieren, aber die entsprechenden Abbildungen nicht injektiv sind (Übung).

3.10.3 Anmerkung. Analog kann man ein Koprodukt von beliebig vielen Algebren definieren. Man kann zeigen, dass in jeder Varietät das Koprodukt beliebig vieler Algebren existiert (und bis auf Isomorphie eindeutig ist).

3.10.4 Anmerkung. Man beachte, dass ein „Umdrehen“ aller Pfeile in dieser Definition eine Charakterisierung des Produkts liefert. Sei nämlich $P := A_1 \times A_2$, und seien π_ℓ $(\ell = 1, 2)$ die beiden Projektionen von P, dann gibt es für jede Algebra Q und alle Homomorphismen $p_\ell : Q \to A_\ell$ $(\ell = 1, 2)$ genau einen Homomorphismus $h : Q \to P$ mit $\pi_\ell \circ h = p_\ell$ $(\ell = 1, 2)$, nämlich den Homomorphisms $h(q) := (p_1(q), p_2(q))$.



[20] manchmal auch Summe oder „freies Produkt“

3.10.5 Satz. *Sei $\mathbb{K}$ eine Klasse von Algebren, und seien F_1, F_2 frei (in $\mathbb{K}$) über B_1 bzw B_2. Sei (C, i_1, i_2) ein Koprodukt von F_1 und F_2 (in $\mathbb{K}$). Dann ist C frei über $i(B_1) \cup i(B_2)$.*

Im speziellen Fall der abelschen Gruppen ist es leicht, das Koprodukt zu konstruieren.

3.10.6 Lemma. *Seien $(G_1, +)$, $(G_2, +)$ abelsche Gruppen. Sei $i_1 : G_1 \to G_1 \times G_2$ die natürliche Einbettung $x \mapsto (x, 0)$, analog $i_2(y) = (0, y)$.*
Dann ist $(G_1 \times G_2, i_1, i_2)$ Koprodukt von G_1 und G_2 (in der Klasse aller abelschen Gruppen).

Beweis. Offensichtlich sind i_1 und i_2 Homomorphismen. Sei D eine abelsche Gruppe, und seien $f_\ell : G_\ell \to D$ Homomorphismen.
Wenn es überhaupt einen Homomorphismus $h : G_1 \times G_2 \to D$ gibt, der die Bedingungen $h \circ i_\ell = f_\ell$ erfüllt, dann muss $h(x, y) = h(x, 0) + h(0, y) = h(i_1(x)) + h(i_2(y)) = f_1(x) + f_2(y)$ gelten; es kann also höchstens einen solchen Homomorphismus geben.
Man sieht aber leicht, dass die durch $h(x, y) := f_1(x) + f_2(y)$ definierte Abbildung ein Homomorphismus ist. (Beim Nachrechnen muss das Kommutativgesetz in D verwendet werden.) □

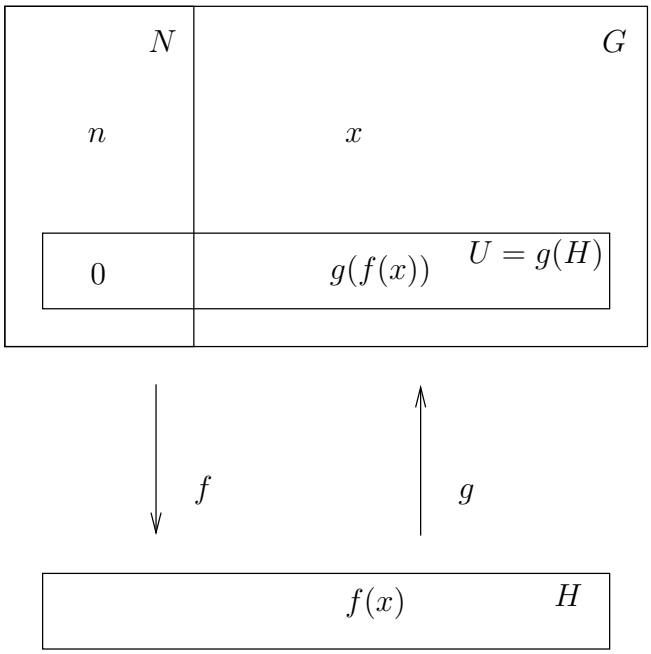
3.10.7 Anmerkung. Ein Analogon des folgenden Lemmas ist aus der linearen Algebra bekannt: Wenn $\pi : U \to V$ lineare Abbildung zwischen Vektorräumen ist, dann ist $U \cong \ker(\pi) \oplus \pi(U)$.

3.10.8 Lemma. *Seien $(G, +)$, $(H, +)$ abelsche Gruppen, $f : G \to H$ surjektiver Homomorphismus mit Kern N. Wenn f ein Rechtsinverses hat (genauer: wenn es einen Homomorphismus $g : H \to G$ mit $f \circ g = id_H$ gibt), dann gibt es eine Untergruppe $U \leq G$, $U \cong H$, sodass $G = N \oplus U$ inneres direktes Produkt von N und U ist (also insbesondere: $G \cong \ker(f) \times f(G)$).*

Beweis. Sei $g : H \to G$ Homomorphismus mit $f \circ g = id_H$. Sei $U := g(H)$. g ist injektiv, also Isomorphismus von H nach U. Wir müssen $N + U = G$ und $N \cap U = \{0\}$ überprüfen:

- Sei $x \in G$. Dann ist $f(x) = f(g(f(x)))$, daher $n := x - g(f(x)) \in \ker(f) = N$, und $u := g(f(x)) \in g(H) = U$; also können wir x in der Form $x = n + u$ mit $n \in N$, $u \in U$ schreiben.
- Sei $x \in N \cap U$, sagen wir $x = g(y)$ mit $y \in H$. Dann ist $f(x) = 0$ wegen $x \in N$, und $f(x) = f(g(y)) = y$, also $y = 0$, daher $x = g(y) = 0$.

□



3.10.9 Anmerkung. Die Bedingung, dass f ein Rechtsinverses hat, ist sicher dann erfüllt, wenn H frei ist, sagen wir über einer Menge $W \subseteq H$. Dann kann man nämlich eine Abbildung j finden, die $j(w) \in f^{-1}(w)$ für alle $w \in W$ erfüllt, somit $f(j(w)) = w$; diese Abbildung lässt sich dann zu einem Homomorphismus h fortsetzen, der dann $f(h(y)) = y$ für alle $y \in H$ erfüllen muss.

3.10.10 Lemma (Nachfolgerschritt)**.** *Sei $G = G_1 \oplus G_2$ inneres direktes Produkt der Untergruppen G_1 und G_2, wobei $G_2 \cong \mathbb{Z}$ gelten möge. Sei $V \leq G$.*
Dann gilt entweder $V \leq G_1$, oder es gibt Untergruppen $V_1, V_2 \leq V$, sodass Folgendes gilt:

1. *$V_1 = V \cap G_1$,*
2. *$V_2 \cong \mathbb{Z}$,*
3. *$V = V_1 \oplus V_2$.*

Wenn überdies V_1 frei über einer Menge W_1 ist, dann gibt es ein $c \in V$, sodass V frei über $W_1 \cup \{c\}$ ist.

Beweis. Sei $\varphi : G \to G_1 \times G_2$ der zur Abbildung

$$(x, y) \in G_1 \times G_2 \mapsto x + y \in G$$

inverse Isomorphismus, seien $\pi_\ell : G_1 \times G_2 \to G_\ell$ $(\ell = 1, 2)$ die beiden Projektionen, und sei $\pi : V \to G_2$ die Einschränkung von $\pi_2 \circ \varphi$ auf V: $\pi := (\pi_2 \circ \varphi) \restriction V$.
Es gilt $\ker(\pi_2) = G_1$, daher $\ker(\pi) = V \cap G_1$.
Im Fall $V \leq G_1$ ist nichts zu beweisen, also können wir annehmen $V \not\subseteq G_1$, also $\ker(\pi) \neq V$, daher hat $V_2 := \pi(V) \subseteq G_2$ mehr als ein Element. Also ist V_2 isomorph zu $\mathbb{Z}$.
Nach Anmerkung 3.10.9 können wir einen zu π rechtsinversen Homomorphismus $k : V_2 \to V$ finden; nach Lemma 3.10.8 folgt $V = V_1 \oplus k(V_2)$. □

3.10.11 Folgerung. Sei $b \notin B$, $U \leq Fr(B \cup \{b\})$. Wenn $U \cap Fr(B)$ frei ist, dann ist auch U frei. Überdies kann jedes freie Erzeugendensystem von $U \cap Fr(B)$ zu einem freien Erzeugendensystem von U erweitert werden.

Beweis. $Fr(B \cup \{b\}) = Fr(B) \oplus Fr(b)$, und $Fr(b) \cong \mathbb{Z}$. Daher können wir das vorige Lemma anwenden. □

3.10.12 Satz. *Sei F freie abelsche Gruppe mit freier Erzeugendenmenge B. Sei $U \leq F$ Untergruppe. Dann ist U frei.*

Beweis für B endlich. Wir verwenden vollständige Induktion.
Für $B = \emptyset$ muss $F = U = \{0\}$ sein. Für $B = \{b\}$ ist $F \cong (\mathbb{Z}, +)$, und wir wissen, dass jede Untergruppe von $\mathbb{Z}$ entweder $\{0\}$ oder von der Form $\{n_0 z \mid z \in \mathbb{Z}\}$ für ein $n_0 > 0$ ist. Jede Untergruppe von $\mathbb{Z}$ (somit auch jede von F) ist frei.
Sei nun $F = Fr(B \cup \{c\})$, wobei $c \notin B$ und B genau n Elemente hat. Sei $U \leq F$. Nach Induktionsvoraussetzung ist $U \cap Fr(B)$ frei, nach der Folgerung 3.10.11 also auch U. □

3.10.13 Anmerkung. Der Beweis zeigt eigentlich mehr:

(a) Sei F freie abelsche Gruppe mit freier Erzeugendenmenge der Größe n. Sei $U \leq F$ Untergruppe. Dann ist U frei, mit höchstens n Erzeugenden.

(b) Sei G eine von n Elementen erzeugte abelsche Gruppe. Dann hat jede Untergruppe von G ein Erzeugendensystem mit höchstens n Elementen.

Beweis. Für (a) muss man nur den gerade gefundenen Beweis des Satzes 3.10.12 (für endliche Erzeugendenmengen) wiederholen. (Übungsaufgabe)
Für (b): Sei $G = \langle \{g_1, \ldots, g_n\} \rangle$. Sei F frei von der n-elementigen Menge $\{x_1, \ldots, x_n\}$ erzeugt, und sei $h : F \to G$ der (eindeutig bestimmte) Homomorphismus mit $h(x_i) = g_i$ für alle i.
Sei $U \leq G$, und sei $V := h^{-1}(U)$. Dann ist $V \leq F$, wird also von höchstens n Elementen erzeugt: $V = \{v_1, \ldots, v_k\}$, $k \leq n$. Dann ist aber $\{h(v_1), \ldots, h(v_k)\}$ ein Erzeugendensystem für $h(V) = U$. □

3.10.14 Anmerkung. Für nichtabelsche Gruppen gilt die vorige Anmerkung nicht. Zum Beispiel hat die von zwei Elementen frei erzeugte Gruppe eine Untergruppe, die von keiner endlichen Menge erzeugt wird.

Das Nachfolger-Lemma 3.10.10 hat uns gezeigt, wie wir unser Wissen über eine freie Gruppe verwenden können, um eine etwas größere freie Gruppe (mit einem zusätzlichen freien Erzeuger) zu verstehen. Um diesen Beweis auf Untergruppen von beliebigen freien Gruppen verallgemeinern zu können, müssen wir verstehen, was passiert, wenn wir unendlich oft einen neuen Erzeuger zu unserer Gruppe hinzufügen.

3.10.15 Lemma (Limesschritt)**.** *Sei $(I, \leq)$ eine linear geordnete Menge, seien $(G_i)_{i \in I}$ abelsche Gruppen und $(W_i)_{i \in I}$ Mengen, sodass gilt:*

1. *G_i ist frei über W_i.*
2. *Für $i_1 \leq i_2$ ist $W_{i_1} \subseteq W_{i_2}$ und $G_{i_1} \leq G_{i_2}$.*

Sei $W_\infty := \bigcup_{i \in I} W_i$, und $G_\infty := \bigcup_{i \in I} G_i$ (direkter Limes). Dann ist G_∞ frei über W_∞.

Beweis. Es ist klar, dass G_∞ eine Gruppe ist, und alle G_i Untergruppen von G_∞ sind. Für alle $x \in G_\infty$ gibt es ein $i \in I$ mit $x \in G_i$, daher ist $x \in \langle W_i \rangle_{G_i} = \langle W_i \rangle_{G_\infty} \subseteq \langle W_\infty \rangle_{G_\infty}$, also wird G_∞ durch W_∞ erzeugt.
Sei $j : W_\infty \to H$ eine Abbildung von W_∞ in irgend eine abelsche Gruppe H. Für alle i sei $j_i := j \restriction W_i$. Dann lässt sich j_i zu einem Homomorphismus $h_i : G_i \to H$ fortsetzen.
Für $i_1 \leq i_2$ ist h_{i_2} eine Fortsetzung der Abbildung j_{i_2}, also auch eine Fortsetzung der

Abbildung j_{i_1}. Daher sind sowohl h_{i_1} als auch $h_{i_2} \restriction G_{i_1}$ Homomorphismen, die j_{i_1} fortsetzen, müssen also übereinstimmen.
Daher ist $h := \bigcup_{i \in I} h_i$ eine Abbildung. Man sieht leicht, dass h Homomorphismus ist und j fortsetzt. □

Die Situation, die durch das Limes-Lemma 3.10.15 und das Nachfolger-Lemma 3.10.10 beschrieben wird, ist typisch für eine Anwendung des Zornschen Lemmas. Um zu zeigen, dass eine vorliegende Untergruppe U einer freien Gruppe selbst frei ist, approximieren wir U von innen durch freie Gruppen. Das Limes-Lemma kann verwendet werden, um zu zeigen, dass es eine maximale Approximation gibt, und das Nachfolger-Lemma zeigt, dass diese maximale Approximation schon ganz U sein muss.

Beweis von Satz 3.10.12 für beliebige Mengen B. Sei F frei über B, und sei $G \leq F$. Jedes Element von F (also auch jedes Element von G) lässt sich in eindeutiger Weise als Summe $\sum_{b \in B_0} z_b b$ (mit $B_0 \subseteq B$ endlich, alle z_b in $\mathbb{Z} \setminus \{0\}$) schreiben.
Für jede Menge $E \subseteq B$ sei $G_E := G \cap \langle E \rangle$. Wir wollen eine möglichst große Menge E finden (eigentlich wollen wir sogar $E = B$), sodass G_E frei ist. Dazu verwenden wir das Lemma von Zorn.

Auf der Menge $P := \{(E, W) \mid G_E \text{ frei über } W\}$ definieren wir eine Halbordnung durch die Definition

$$(E_1, W_1) \leq (E_2, W_2) \;\Leftrightarrow\; E_1 \subseteq E_2 \text{ und } W_1 \subseteq W_2.$$

Wir zeigen nun, dass diese Halbordnung die Voraussetzung im Lemma von Zorn erfüllt. Sei also $\mathcal{K} \subseteq P$ eine Kette; wir suchen eine obere Schranke für $\mathcal{K}$. Wir definieren $E^* := \bigcup_{(E,W) \in \mathcal{K}} E$, und $W^* := \bigcup_{(E,W) \in \mathcal{K}} W$. Aus dem Limes-Lemma folgt, dass $(E^*, W^*) \in P$ ist; daher ist (E^*, W^*) obere Schranke.

Da in P also jede Kette beschränkt ist, gibt es in P ein maximales Element $(\bar{E}, \bar{W})$. Die Gruppe $G_{\bar{E}}$ ist frei über $\bar{W}$; wir wollen $G_{\bar{E}} = G$ zeigen.
Wenn $\bar{E} = B$ ist, dann ist $G_{\bar{E}} = G$, und wir sind fertig.
Sei also $\bar{E} \subsetneqq B$, und sei $b \in B \setminus \bar{E}$. Dann gilt $G_{\bar{E}} \subseteq G_{\bar{E} \cup \{b\}}$; Gleichheit kann hier nicht gelten, sonst wäre $(\bar{E}, \bar{W}) < (\bar{E} \cup \{b\}, W) \in P$, was einen Widerspruch zur Maximalität von $(\bar{E}, \bar{W})$ bedeuten würde.
Die Gruppe $G_{\bar{E} \cup \{b\}}$ ist eine Untergruppe von $Fr(E \cup \{b\}) = Fr(E) \oplus Fr(\{b\})$; weiters gilt

$$G_{\bar{E}} = G_{\bar{E} \cup \{b\}} \cap Fr(E).$$

Es gilt $G_{\bar{E} \cup \{b\}} \subseteq \langle \bar{E} \cup \{b\} \rangle = Fr(\bar{E} \cup \{b\})$, und $G_{\bar{E}} = G_{\bar{E} \cup \{b\}} \cap \langle \bar{E} \rangle$. Außerdem ist $G_{\bar{E}}$ frei über $\bar{W}$; wegen der Folgerung aus dem Nachfolger-Lemma können wir schließen, dass es eine Menge $\tilde{W} \supseteq \bar{W}$ gibt, sodass $G_{\bar{E} \cup \{b\}}$ frei über $\tilde{W}$ ist. Damit ist $(\bar{E}, \bar{W}) < (\bar{E} \cup \{b\}, \tilde{W}) \in P$, im Widerspruch zur Maximalität $(\bar{E}, \bar{W})$. □

3.11 Endlich erzeugte abelsche Gruppen

Der Hauptsatz über endlich erzeugte abelsche Gruppen besagt, dass jede endlich erzeugte abelsche Gruppe ein Produkt von endlich vielen zyklischen Gruppen ist; die im Produkt vorkommenden zyklischen Gruppen sind entweder isomorph zu $\mathbb{Z}$ oder selbst endlich.

Der Beweis sieht grob so aus:

1. *Jede endlich erzeugte abelsche Gruppe G lässt sich als inneres Produkt $G = G_1 \oplus G_2$ schreiben, wobei G_1 endlich und G_2 endlich erzeugt und torsionsfrei ist (also außer 0 nur Elemente der Ordnung ∞ hat).*
   (Satz 3.11.16(3))

2. *Jede endliche abelsche Gruppe ist inneres direktes Produkt von p-Gruppen (siehe Definition 3.11.1).*
   (Satz 3.11.9)

3. *Jede endliche abelsche p-Gruppe, ist inneres direktes Produkt von zyklischen (endlichen) Gruppen.*
   (Korollar 3.11.7)

4. *Jede endlich erzeugte torsionsfreie abelsche Gruppe ist freie abelsche Gruppe. Insbesondere trifft dies auf G_2 zu.*
   (Satz 3.11.15)

5. *Die endlich erzeugten freien abelschen Gruppen sind genau die Gruppen $\mathbb{Z}^n$ ($n = 0, 1, 2, \ldots$).*
   (Korollar 3.11.12)

Sei G eine Gruppe. Wir schreiben $G = 1$, wenn G nur aus dem neutralen Element besteht. In diesem Abschnitt betrachten wir (abgesehen von einigen Anmerkungen) nur abelsche Gruppen; wir schreiben alle Gruppen additiv.

3.11.A p-Gruppen

3.11.1 Definition. Sei p eine Primzahl. G heißt p-Gruppe, wenn die Ordnung jedes Elements eine Potenz von p ist.

3.11.2 Lemma. *Sei G eine zyklische Gruppe der Ordnung $n > 0$. Dann gibt es für jeden Teiler d von n genau eine Untergruppe der Ordnung d, nämlich $(\frac{n}{d})G := \{\frac{n}{d}g \mid g \in G\} = \{x \in G \mid dx = 0\}$.*
Insbesondere gilt: Wenn $|G| = p^n$ für eine Primzahl p, dann gibt es für jede natürliche Zahl k mit $0 \leq k \leq n$ genau eine Untergruppe der Ordnung p^k.

Beweis. Übung. □

3.11.3 Lemma. *Wenn $ord(x) = m$, dann $ord(kx) = m/ggT(k, m)$.*

Beweis. Übung. □

3.11.4 Lemma. *Sei G endliche p-Gruppe, $G \neq 1$. Dann hat G eine Untergruppe der Ordnung p.*

Beweis. Sei $g \in G \setminus \{0\}$. Die Gruppe $\langle g \rangle$ ist zyklisch von der Ordnung p^k, mit einem $k \geq 1$. Nach dem vorigen Lemma hat $p^{k-1}g$ die Ordnung p. □

3.11.5 Lemma. *Sei G endliche p-Gruppe, $|G| > 1$. Wenn G genau eine Untergruppe der Ordnung p enthält, dann ist G zyklisch.*

Beweis. Sei U die einzige Untergruppe der Ordnung p. Sei $|G| = p^n$. Für $n = 1$ ist die Aussage wahr. Wir verwenden Induktion nach n.
Sei nun $n > 1$.

Sei $h : G \to pG \leq G$ die Abbildung $x \mapsto px$. Die Abbildung h ist ein Homomorphismus. Jedes Element im Kern von h (ausgenommen 0) erzeugt eine Gruppe der Ordnung p, also ist U genau der Kern von h.
$pG \simeq G/U$ ist eine Gruppe der Ordnung p^{n-1} (nach dem Satz von Lagrange). pG hat genau eine Untergruppe der Ordnung p (höchstens eine, weil $pG \leq G$; mindestens eine wegen des vorigen Lemmas).
Nach Induktionsannahme ist also pG zyklisch. Sei $g \in G$ so, dass $h(g) = pg$ die Ordnung p^{n-1} hat. Dann hat g die Ordnung p^n.

□

3.11.6 Lemma. *Sei G endliche abelsche p-Gruppe. Sei $a \in G$ Element mit größtmöglicher Ordnung. Dann gibt es eine Untergruppe $U \leq G$ sodass $G = \langle a \rangle + U$ als inneres direktes Produkt.*
Als Folgerung sehen wir, dass sich G als direktes Produkt von zyklischen Gruppen darstellen lässt.

Beweis. Wir verwenden Induktion nach $|G|$.
Wenn G zyklisch ist, dann ist $\langle a \rangle = G$, und wir können $U = 1$ wählen. Andernfalls gilt einerseits, dass es in $\langle a \rangle$ eine Untergruppe der Ordnung p gibt, und andererseits laut dem gerade bewiesenen Lemma 3.11.5, dass diese nicht die einzige Untergruppe von G der Ordnung p sein kann. Es gibt also eine Untergruppe P der Ordnung p, $P \not\subseteq \langle a \rangle$, daher $P \cap \langle a \rangle = 1$.
Sei $k : G \to G/P$ die kanonische Abbildung. k ist injektiv auf $\langle a \rangle$, also hat die Nebenklasse $a + P$ in G/P noch immer die selbe Ordnung wie in G; da die Ordnungen von anderen Elementen entweder gleich bleiben oder kleiner werden, hat $a + P$ in G/P maximale Ordnung.
Nach Induktionsvoraussetzung gibt es eine Untergruppe $V \leq G/P$ sodass $\langle a+P \rangle \oplus V = G/P$ als inneres direktes Produkt; jedes Element von G/P lässt sich also eindeutig als Summe $b + v$ schreiben, wobei b ein Vielfaches von $a + P$ ist, und $v \in V$.
Sei nun $U = k^{-1}(V)$. Wir behaupten $\langle a \rangle \oplus U = G$, also $\langle a \rangle + U = G$ und $\langle a \rangle \cap U = 1$. Aus $\langle aP \rangle + V = G/P$ erhalten wir $\langle a \rangle + U + P = G$. [Genauer: Sei $g \in G$. Dann können wir $g + P$ in der Form $(ka + P) + (u + P)$ mit $k \in \mathbb{Z}$, $u \in U$ darstellen, also liegt $g - ka - u$ in P, d.h. $g = ka + u + q$ mit $q \in P$.] Wegen $P \leq U$ gilt also $\langle a \rangle + U = G$.
Wenn $x \in \langle a \rangle \cap U$ ist, dann gilt in G/P: $k(x) \in \langle a + P \rangle \cap V$, daher $k(x) = 0$, also $x \in P$. Wegen $P \cap \langle a \rangle = \{0\}$ ist $x = 0$. Daher $\langle a \rangle \cap U = \{0\}$.

□

3.11.7 Korollar. Jede endlich erzeugte p-Gruppe ist endliches Produkt von zyklischen Gruppen.

Beweis. Sei $G = \langle a_1, \ldots, a_n \rangle$, und $p^k = \max(o(a_1), \ldots, o(a_n))$ die maximale Ordnung aller Erzeugenden. Jedes Element von G lässt sich dann in der Form $\sum_{i=1}^{n} \lambda_i a_i$ darstellen, mit $0 \leq \lambda_i \leq p^k$. Also ist G endlich.
Durch induktive Anwendung von Lemma 3.11.6 können wir G als inneres direktes Produkt von endlichen zyklischen Gruppen schreiben. □

3.11.8 Anmerkung. Eine endlich erzeugte *nichtkommutative* Gruppe, deren Erzeuger alle endliche Ordnung haben, muss nicht endlich sein. (Siehe Übungen.)
Es gibt sogar endlich erzeugte unendliche Gruppen, in denen alle Elemente endliche Ordnung haben. (Diese sind unter dem Stichwort „Burnside-Gruppen“ zu finden.)

3.11.B Endliche abelsche Gruppen

3.11.9 Satz. *Jede endliche abelsche Gruppe G ist*

1. *isomorph zu einem Produkt von p-Gruppen (d.h., es gibt Primzahlen $p_1, \dots, p_k$ und Gruppen $H_1, \dots, H_k$, sodass $G \cong H_1 \times \cdots \times H_k$ ist, wobei H_i eine p_i-Gruppe ist);*

2. *isomorph zu einem Produkt von zyklischen Gruppen.*

Beweis. Da sich jede p-Gruppe als Produkt von zyklischen Gruppen schreiben lässt, folgt (2) aus (1).
Sei $|G| = n$. Für jeden Primteiler p von n sei

$$G_p := \{x \in G \mid \exists k : \ o(x) = p^k\} = \{x \in G \mid \exists k : \ p^k x = 0\}.$$

Allgemeiner schreiben wir für jeden Teiler d von n:

$$G_d := \{x \in G \mid \exists k : \ d^k x = 0\}.$$

Wenn d und d' teilerfremd sind, dann ist $G_d \cap G_{d'} = 1$, denn: Sei $d^k x = 0$, $d'^{k'} x = 0$, dann sind auch d^k und $d'^{k'}$ teilerfremd, also gibt es ganze Zahlen a, a' mit $ad^k + a'd'^{k'} = 1$, daher $x = 1x = (ad^k + a'd'^{k'})x = 0 + 0 = 0$.
G_p ist eine Untergruppe von G, denn wenn $p^k x = 0$ und $p^l y = 0$ ist, und oBdA $k \le l$ gilt, dann ist $p^l(x + y) = 0$, also ist $o(x + y)$ ein Teiler von p^l.
Seien nun $p_1, \dots, p_k$ alle verschiedenen Primteiler von n. Mit Induktion zeigt man leicht:

$$\langle G_{p_1} \cup \cdots \cup G_{p_i} \rangle \le G_{p_1 \cdot \dots \cdot p_i}, \text{ daher } \langle G_{p_1} \cup \cdots \cup G_{p_i} \rangle \cap G_{p_{i+1}} = 1.$$

Daher ist $G_{p_1} + \cdots + G_{p_k}$ ein inneres direktes Produkt, und offensichtlich sind alle G_{p_i} p_i-Gruppen.
Zu zeigen ist noch, dass die G_{p_i} gemeinsam ganz G erzeugen. Sei $g \in G$ beliebig, mit Ordnung $o(g) = p_1^{e_1} \cdots p_k^{e_k}$. Für $i = 1, \dots, k$ definieren wir $p_i^* := o(g)/p_i^{e_i}$. Die Zahlen p_1^*, $\dots$, p_k^* haben nun keinen gemeinsamen Teiler, daher gibt es ganze Zahlen $n_1, \dots, n_k$ mit

$$n_1 p_1^* + \cdots + n_k p_k^* = 1.$$

Daher ist

$$g = 1g = (n_1 p_1^* + \cdots + n_k p_k^*)g = n_1(p_1^* g) + \cdots + n_k(p_k^* g),$$

und die Ordnung von $p_i^* g$ ist $p_i^{e_i}$, also $p_i^* g \in G_{p_i}$. □

3.11.C Freie endlich erzeugte abelsche Gruppen

Wir haben bereits erwähnt, dass die Gruppe $\mathbb{Z}^n$ von den n Einheitsvektoren frei erzeugt wird. Hier geben wir einen Beweis.

3.11.10 Definition. Sei $(G, +)$ abelsche Gruppe. Wir nennen ein Tupel $(g_1, \dots, g_n)$ von Elementen von G *linear unabhängig*, wenn aus $\sum_{i=1}^n \lambda_i g_i = 0$ (mit $\lambda_i \in \mathbb{Z}_i$) folgt, dass alle λ_i verschwinden.

3.11.11 Lemma. *Sei $(G, +)$ abelsche Gruppe, die von $\{g_1, \dots, g_n\}$ erzeugt wird, wobei die g_i linear unabhängig sind. Dann ist ist G frei über $\{g_1, \dots, g_n\}$.*

Beweis. Jedes Element von G lässt sich in als endliche Summe der Form $\sum_i \lambda_i g_i$ (mit $\lambda_i \in \mathbb{Z}$) darstellen, weil G von den g_i erzeugt wird. Diese Darstellung ist überdies eindeutig, weil aus $\sum_i \lambda_i g_i = \sum_i \mu_i g_i$ ja $\sum_i (\lambda_i - \mu_i) g_i = 0$ folgt, also $\forall i : \lambda_i = \mu_i$.
Sei nun $j : \{g_1, \ldots, g_n\} \to H$ eine Abbildung in eine beliebige abelsche Gruppe, dann ist die durch $h(\sum_i \lambda_i g_i) := \sum_i \lambda_i j(g_i)$ definierte Abbildung erstens wohldefiniert, zweitens ein Homomorphismus, und setzt drittens die Abbildung j fort. Daher ist G frei über $\{g_1, \ldots, g_n\}$. □

3.11.12 Korollar. $\mathbb{Z}^n$ wird frei von den Einheitsvektoren erzeugt.

Beweis. Sei g_i der i-te Einheitsvektor. Offensichtlich ist $(\lambda_1, \ldots, \lambda_n)$ eindeutig als $\sum \lambda_i g_i$ darstellbar. Aus dem Lemma folgt, dass $\mathbb{Z}^n$ frei ist. □

3.11.D Torsionsfreie Gruppen

3.11.13 Definition. Sei G Gruppe. $x \in G$ heißt *Torsionselement*, wenn die von x erzeugte Untergruppe endlich ist, d.h., wenn x endliche Ordnung hat. Mit G^T bezeichen wir die Menge aller Torsionselemente von G. Die Gruppe G heißt *torsionsfrei*, wenn $G^T = 1$. Die Gruppe G heißt Torsionsgruppe, wenn $G^T = G$ ist.

3.11.14 Lemma. *Sei G abelsche Gruppe. Dann ist G^T Untergruppe von G, und G/G^T ist torsionsfrei.*

Beweis. $G^T \leq G$ folgt leicht aus der Kommutativität.
Sei $x+G^T$ ein Torsionselement in G/G^T, sagen wir $n(x+G^T) = G^T$ mit $n \in \{1, 2, \ldots\}$. Dann gilt $nx \in G^T$, sagen wir $k(nx) = 0$, also ist x Torsionselement, daher $x + G^T = G^T$. □

3.11.15 Lemma. *Sei G eine endlich erzeugte torsionsfreie abelsche Gruppe. Dann ist G freie abelsche Gruppe.*

Beweis. Sei $\{g_1, \ldots, g_n\}$ eine minimale Erzeugendenmenge von G. (Insbesondere seien alle $g_i \neq 0$.)
Wir ordnen die (paarweise verschiedenen) g_i so an, dass $g_1, \ldots, g_k$ unter den Erzeugern eine maximale linear unabhängige Menge sind, d.h.: $\{g_1, \ldots, g_k\}$ sind linear unabhängig, aber für alle $i \in \{k+1, \ldots, n\}$ gilt, dass $\{g_1, \ldots, g_k, g_i\}$ linear abhängig ist.
Sei $\mu_i g_i = \sum_{j=1}^{k} \mu_{i,j} g_j$ für $i = k+1, \ldots, n$, wobei alle $\mu_i \neq 0$ sind. Sei $\mu \neq 0$ ein gemeinsames Vielfaches der μ_i, dann gilt

$$\forall i \in \{k+1, \ldots, n\} : \ \mu g_i \in \langle g_1, \ldots, g_k \rangle$$

(Für $i \in \{1, \ldots, k\}$ gilt natürlich erst recht $\mu g_i \in \langle g_1, \ldots, g_k \rangle$.)
Wir betrachten nun die Abbildung $f : G \to G$, die durch $x \mapsto \mu x$ definiert ist. Weil G torsionsfrei ist, hat f trivialen Kern, daher ist

$$f(G) \cong G/\ker(f) \cong G.$$

Nun ist $f(G) \leq \langle g_1, \ldots, g_k \rangle$. Die Gruppe $\langle g_1, \ldots, g_k \rangle$ ist (nach Lemma 3.11.11) frei.
Als Untergruppe einer freien abelschen Gruppe ist $f(G)$ also auch frei.
Daher ist G frei. □

Hauptsatz über endlich erzeugte abelsche Gruppen

3.11.16 Satz. *Sei G endlich erzeugte abelsche Gruppe. Dann gilt:*

1. *G^T ist endlich erzeugte Torsionsgruppe.*
2. *G^T ist endlich.*
3. *G/G^T ist endlich erzeugte torsionsfreie Gruppe (daher frei).*
4. *$G \cong G^T \times (G/G^T)$.*

Insbesondere ist also jede endlich erzeugte abelsche Gruppe isomorph zu einem endlichen Produkt von zyklischen Gruppen.

Beweis. (1) G^T ist Untergruppe einer endlich erzeugten abelschen Gruppe, also ebenfalls endlich erzeugt, nach Anmerkung 3.10.13.
(2) folgt aus (1).
(3) Wenn G von $g_1, \ldots, g_n$ erzeugt wird, dann wird G/G^T von $g_1 + G^T, \ldots, g_n + G^T$ erzeugt. Wir wissen bereits, dass G/G^T torsionsfrei ist.
(4) Sei $f : G \to G/G^T$ die kanonische Abbildung. G/G^T ist freie abelsche Gruppe, sagen wir mit Erzeugern $b_1, \ldots, b_k$. Daher gibt es einen Homomorphismus $h : G/G^T \to G$, der jedem b_i eines seiner Urbilder unter f zuordnet, d.h. $h(b_i) \in f^{-1}(b_i)$, also $f(h(b_i)) = b_i$.
Da die b_i ganz G/G^T erzeugen, gilt $f \circ h = id$ auf ganz G/G^T. Daher ist $G \cong G^T \times (G/G^T)$. □

Kapitel 4

Polynome

4.1 Konstruktion des Potenzreihenrings und des Polynomrings

4.1.1 Definition. Sei $(R, +, 0, -, \cdot, 1)$ ein kommutativer Ring mit Einselement. Wir betrachten $R^{\mathbb{N}_0} = \{(a_n)_{n\in\mathbb{N}_0} = (a_0, a_1, a_2, \ldots) \mid a_n \in R\}$ und setzen $(a_n)_{n\in\mathbb{N}_0} =: \sum_{n=0}^{\infty} a_n x^n$ ($\sum_{n=0}^{\infty} a_n x^n$ heißt *formale Potenzreihe*). Wir wollen nun die Operationen $+, 0, -, \cdot, 1$ auf $R^{\mathbb{N}_0}$ so definieren, dass $(R^{\mathbb{N}_0}, +, 0, -, \cdot, 1)$ wieder ein kommutativer Ring mit Einselement ist:

$$\begin{aligned}
\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n &:= \sum_{n=0}^{\infty} (a_n + b_n) x^n, & 0 &:= \sum_{n=0}^{\infty} 0 \cdot x^n, \\
\sum_{n=0}^{\infty} a_n x^n \cdot \sum_{n=0}^{\infty} b_n x^n &:= \sum_{n=0}^{\infty} \big(\sum_{k=0}^{n} a_k b_{n-k}\big) x^n, & 1 &:= \sum_{n=0}^{\infty} \delta_{0n} x^n = (1, 0, 0, 0, \ldots), \\
-\big(\sum_{n=0}^{\infty} a_n x^n\big) &:= \sum_{n=0}^{\infty} (-a_n) x^n.
\end{aligned}$$

4.1.2 Satz. *(a)* $(R^{\mathbb{N}_0}, +, 0, -, \cdot, 1)$ *ist ein kommutativer Ring mit Einselement.*

(b) $\varphi : R \to R^{\mathbb{N}_0}$, $r \mapsto \sum_{n=0}^{\infty} \delta_{0n} r x^n = (r, 0, 0, 0, \ldots)$ *ist ein Monomorphismus (injektiver Homomorphismus).*

(c) Mit $x := (0, 1, 0, 0, 0, \ldots) = \sum_{n=0}^{\infty} \delta_{1n} x^n$ *gilt:* $(a_0, a_1, \ldots, a_n, 0, 0, 0, \ldots) = \varphi(a_0) + \varphi(a_1)x + \ldots + \varphi(a_n)x^n$.

Beweis. a) Z. B. Assoziativgesetz für die Multiplikation:

$$\begin{aligned}
&\big(\sum_{n=0}^{\infty} a_n x^n \sum_{n=0}^{\infty} b_n x^n\big) \sum_{n=0}^{\infty} c_n x^n = \sum_{n=0}^{\infty} \big(\sum_{k=0}^{n} a_k b_{n-k}\big) x^n \sum_{n=0}^{\infty} c_n x^n = \\
&= \sum_{n=0}^{\infty} \big(\sum_{k=0}^{n} \big(\sum_{j=0}^{k} a_j b_{k-j}\big) c_{n-k}\big) x^n = \sum_{n=0}^{\infty} \big(\sum_{\substack{0\le i,j,k\le n,\\ i+j+k=n}} a_i b_j c_k\big) x^n = \\
&= \ldots = \sum_{n=0}^{\infty} a_n x^n \big(\sum_{n=0}^{\infty} b_n x^n \sum_{n=0}^{\infty} c_n x^n\big).
\end{aligned}$$

Analog rechnet man die anderen Gesetze nach. Anmerkung: Das Symbol $\sum_{n=0}^{\infty} \cdots$ ist nur ein formaler Ausdruck; in der Algebra (genauer: in dieser Vorlesung) betrachten wir keine

unendlichen Summen. Das Symbol $\sum_{n=0}^{k} \cdots$ bezeichnet hingegen die gewöhnliche Summe[1] im Ring R.

b) φ ist offenbar injektiv: $r \neq s \Rightarrow \varphi(r) \neq \varphi(s)$. Weiters gilt: $\varphi(r+s) = (r+s, 0, 0, \ldots) = (r, 0, 0, \ldots) + (s, 0, 0, \ldots) = \varphi(r) + \varphi(s)$, $\varphi(rs) = (rs, 0, 0, \ldots) = (r, 0, 0, \ldots)(s, 0, 0, \ldots) = \varphi(r)\varphi(s)$ und $\varphi(1) = (1, 0, 0, \ldots)$.

c) Es gilt $x = (0, 1, 0, 0, \ldots)$, $x^2 = (0, 0, 1, 0, \ldots)$, $\ldots$, allgemein: $x^m = \sum_{n=0}^{\infty} \delta_{mn} x^n$, woraus c) folgt. □

4.1.3 Definition. Ist $p(x) = \sum_{k=0}^{\infty} a_k x^k \in R[[x]]$, so heißen die Ringelemente a_k die *Koeffizienten* der Potenzreihe $p(x)$; insbesondere heißt a_0 der „konstante Term“ von $p(x)$, und a_k heißt „Koeffizient“ von x^k.

$0 \in R[x]$ ist das *Nullpolynom*.

4.1.4 Definition. Wir fassen nun nach dem Prinzip der isomorphen Einbettung den Ring R als Unterring von $R[[x]]$ auf, indem wir Elemente von $r \in R$ mit den entsprechenden konstanten Potenzreihen $(r, 0, 0, \ldots)$ identifizieren. Insbesondere sind Null- und Einselement von R auch Null- und Einselement von $R[[x]]$. Der Ring $R[[x]]$ heißt der *Ring der formalen Potenzreihen* in x über R.

4.1.5 Definition. Wir definieren nun den *Polynomring* in x über R als die Menge aller formalen Potenzreihen mit nur endlich vielen nichtverschwindenden Koeffizienten, also

$$R[x] := \{\sum_{n=0}^{\infty} a_n x^n \mid \exists m \, \forall n > m : \ a_n = 0\},$$

also $R[x] := \{a_0 + a_1 x + \cdots + a_n x^n \mid n \in \mathbb{N}_0, \ a_i \in R\}$.

Man sieht leicht: $(R[x], +, 0, -, \cdot, 1)$ ist genau der von $R \cup \{x\}$ erzeugte Unterring von $(R[[x]], +, 0, -, \cdot, 1)$. Man zeigt dazu:

1) $R[x]$ ist abgeschlossen bezüglich $+, 0, -, \cdot, 1$. (Bezüglich $\cdot$ beachte man: $a_k = 0$ für alle $k > n$, $b_k = 0$ für alle $k > m \Rightarrow \sum_{j=0}^{k} a_j b_{k-j} = 0$ für alle $k > n + m$.)

2) Ist S Unterring von $R[[x]]$ mit $R \cup \{x\} \subseteq S$, so gilt $R[x] \subseteq S$.

x heißt auch „Unbestimmte“.[2] Die Elemente von $R[x]$ heißen *Polynome* und werden als $f(x)$, $p(x)$, $\ldots$ geschrieben.

---

[1] Formal ist diese induktiv definiert: $\sum_{n=0}^{0} f(n) := f(0)$, und $\sum_{n=0}^{k+1} f(n) := (\sum_{n=0}^{k} f(n)) + f(k+1)$. Es ist üblich und auch sinnvoll, $\sum_{n=0}^{-1} f(n) := 0$ zu setzen.

[2] Die Grenzen zwischen „Unbestimmten“, „Variablen“, „Unbekannten“, „Konstanten“, und „Parametern“ sind oft etwas unscharf — unter anderem deshalb, weil derselbe Buchstabe in einem mathematischen Argument oft mehr als eine Rolle spielen kann. *Variable* sind heißen Symbole dann, wenn man vorhat, die Variable irgendwann durch Werte, und zwar durch beliebige Werte in einer vorgegebenen Menge, zu ersetzen – Variable stehen daher oft hinter einem Allquantor oder Existenzquantor. Das Symbol x in einer formalen Potenzreihe heißt *Unbestimmte*, weil man damit rechnen kann, ohne einen bestimmten Wert einzusetzen. (Das x in einem Polynom spielt abwechselnd die Rolle einer Unbestimmten und einer Variablen.) *Unbekannte* sind jene Variable, deren Wert eigentlich schon fest liegt, aber noch gesucht wird — etwa beim Lösen einer Gleichung. *Konstante* behalten im Verlauf eines mathematischen Arguments meist ihren Wert; allerdings kann z.B. das nullstellige Funktionssymbol oder Konstantensymbol e für das neutrale Element einer Gruppe durchaus in verschiedenen Gruppen mit verschiedenen Werten belegt werden, etwa mit 0 in $(\mathbb{Z}, +)$ und mit 1 in $(\mathbb{Q} \setminus \{0\}, \cdot)$. *Parameter* sind Variable, die länger konstant gehalten werden als die eigentlichen Variablen; wenn man etwa alle Gleichungen der Form $Ax + By = C$ betrachtet, sind x, y für jedes fest A, B, C variabel (und definieren eine Gerade $G_{A,B,C} := \{(x, y) \mid Ax + By = C\}$); durch Variieren der Parameter A, B und C bekommt man alle Geradengleichungen.

Jedes $p(x) \in R[x]$ hat die Gestalt $p(x) = \sum_{k=0}^{n} a_k x^k$ mit $n \in \mathbb{N}_0$. Sei weiters $q(x) = \sum_{k=0}^{m} b_k x^k$ mit $m \leq n$. Wann gilt $p(x) = q(x)$? Wir schreiben $q(x) = \sum_{k=0}^{n} b_k x^k$, wobei $b_k = 0$ für $m < k \leq n$. Dann gilt: $p(x) = q(x) \Leftrightarrow a_k = b_k$ für $k = 0, \ldots, n$.

Mit Polynomen wird nach den Gesetzen des kommutativen Ringes $R[x]$ mit Einselement gerechnet.

4.1.6 Definition. Ist $p(x) = \sum_{k=0}^{n} a_k x^k$ mit $a_n \neq 0$, so heißt n der *Grad* von $p(x)$ ($n = \operatorname{grad} p(x)$).
Wenn n der Grad des Polynoms p ist, dann heißt a_n (der Koeffizient von x^n) auch „Koeffizient des höchsten Terms“.

Es gilt:

$$\operatorname{grad}(p(x) + q(x)) \leq \max(\operatorname{grad} p(x), \operatorname{grad} q(x))$$
$$\operatorname{grad}(p(x)q(x)) \leq \operatorname{grad} p(x) + \operatorname{grad} q(x)$$

falls $p(x)$, $q(x)$, $p(x)+q(x)$ und $p(x)q(x) \neq 0$ sind. Dem Polynom 0 wird oft kein Grad zugeordnet. Gelegentlich setzt man auch $\operatorname{grad}(0) = -\infty$, dann gelten die obigen Abschätzungen auch dann, wenn p oder q oder $p + q$ oder pq das Nullpolynom sind (sofern man die Rechenregeln $(-\infty) + k = -\infty = (-\infty) + (-\infty)$ vereinbart).

4.1.7 Definition. Gilt $\operatorname{grad} p(x) = n$ und $a_n = 1$, so heißt $p(x)$ ein *normiertes* (oder auch „monisches“) Polynom. Polynome der Gestalt $ax + b$ mit $a \neq 0$ heißen *lineare* Polynome.

4.1.8 Satz. *Ist R ein Integritätsbereich, dann ist auch $R[x]$ ein Integritätsbereich, und für $p(x), q(x) \in R[x] \setminus \{0\}$ gilt:* $\operatorname{grad}(p(x)q(x)) = \operatorname{grad} p(x) + \operatorname{grad} q(x)$.

Beweis. $p(x) = \sum_{k=0}^{n} a_k x^k$, $a_n \neq 0$, $q(x) = \sum_{k=0}^{m} b_k x^k$, $b_m \neq 0 \Rightarrow p(x)q(x) = \sum_{k=0}^{n+m} c_k x^k$ mit $c_k = \sum_{j=0}^{k} a_j b_{k-j}$, insbesondere: $c_{n+m} = a_n b_m \neq 0$. □

4.1.9 Anmerkung. Ist R kein Integritätsbereich, so ist auch $R[x]$ keiner, da R Unterring von $R[x]$ ist.

4.1.10 Anmerkung. Wenn R Integritätsbereich ist, dann ist auch $R[[x]]$ Integritätsbereich. (Beweis: Übung.)

4.1.A Potenzreihen und Polynome in n Unbestimmten $x_1, \ldots, x_n$

Wenn es bereits ein Element von R gibt, das wir mit x bezeichnen, dann wählen wir einen anderen Namen für die Unbestimmte[3] im Polynomring bzw. im Ring der formalen Potenzreihen über R, z.B. y.
Sei R Ring, $R[x]$ Polynomring über R. Den Polynomring über $R[x]$ bezeichnen wir mit $R[x][y]$ oder einfach $R[x, y]$. Elemente von $R[x, y]$ kann man entweder (gemäß der Definition) als Polynome über $R[x]$ in der Unbestimmten y auffassen, oder auch als Polynome über dem Polynomring $R[y]$ (welcher in natürlicher Weise zu $R[x]$ isomorph ist) in der Variablen x.
Unter dem „Grad“ eines solchen Polynoms versteht man je nach Kontext bzw. nach Auffassung etwas anderes. Zum Beispiel hat das Polynom $3x^2y + xy - 5x \in \mathbb{Z}[x, y]$, als Element von $\mathbb{Z}[y][x]$ aufgefasst, den Grad 2 („quadratisch in der Variablen x“); die Koeffizienten von

$$3y \cdot x^2 + (y - 5) \cdot x^1 + 0 \cdot x^0$$

[3] formal: für die Folge $(0, 1, 0, 0, \ldots)$.

sind $3y$, $y-5$ und 0. Wenn wir das Polynom aber als Element von $\mathbb{Z}[x][y]$ auffassen, ist es linear: Das Polynom

$$(3x^2+x)\cdot y^1 - 5x\cdot y^0$$

hat die Koeffizienten $3x^2+x$ und -5.
Oft ist es auch sinnvoll, einem Polynom in den Variablen x, y einen gemeinsamen Grad zuzuweisen; dieser gemeinsame Grad ist als die maximale vorkommende Summe der Exponenten von x und y definiert. Im Polynom $3x^2y^1 + x^1y^1 - 5x^1y^0$ kommen als Summen von Exponenten $2+1$, $1+1$, $1+0$ vor, der gemeinsame Grad ist also 3. Das Polynom $xy+1$ hat dann gemeinsamen Grad $1+1=2$; es ist aber „linear in x“ und auch „linear in y“.

Allgemeiner definieren wir induktiv:

$$R[[x_1]] := R[[x]], \qquad R[[x_1,\ldots,x_n]] := (R[[x_1,\ldots,x_{n-1}]])[[x_n]],\ n>1,$$

und entsprechend:

$$R[x_1] := R[x], \qquad R[x_1,\ldots,x_n] := (R[x_1,\ldots,x_{n-1}])[x_n],\ n>1.$$

Dann gilt (Beweis durch vollständige Induktion nach n):

$$R[x_1,\ldots,x_n] = \{\sum_{0\le i_1,\ldots,i_n\le m} a_{i_1\ldots i_n} x_1^{i_1}\cdots x_n^{i_n} \mid m\in\mathbb{N}_0,\ a_{i_1\ldots i_n}\in R\}.$$

Z. B. hat ein Element aus $R[x_1,x_2]$ die allgemeine Form: $p(x_1,x_2) = a_{00} + a_{10}x_1 + a_{01}x_2 + a_{20}x_1^2 + a_{11}x_1x_2 + a_{02}x_2^2 + \cdots + a_{jk}x_1^jx_2^k$.

4.2 Polynome und Funktionen

4.2.1 Satz. *[Einsetzungsprinzip] Sei $(R,+,0,-,\cdot,1)$ ein kommutativer Ring mit Einselement und $p(x) = a_nx^n+\cdots+a_1x+a_0 \in R[x]$. Für $a\in R$ ist dann $p(a) := a_na^n+\cdots+a_1a+a_0$ wieder ein Element von R, genannt der* Wert des Polynoms an der Stelle a. *Die Funktion*

$$\begin{cases} R\to R \\ a\mapsto p(a)\end{cases}$$

heißt die durch das Polynom $p(x)$ induzierte Polynomfunktion *und wird oft ebenfalls mit p bezeichnet.*

Der folgende Satz betrachtet eine etwas allgemeinere Situation.

4.2.2 Satz. *Seien R und S kommutative Ringe mit Einselement, und sei $f: R\to S$ ein Homomorphismus. Sei c ein Element von S.*
Dann ist die Abbildung $\varphi_c: R[x]\to S$, die durch

$$\varphi_c(\sum_{k=1}^{n} a_kx^k) = \sum_{k=1}^{n} f(a_k)c^k$$

definiert ist, ein Homomorphismus. Überdies ist φ_c der einzige Homomorphismus ψ, der f fortsetzt und $\psi(x)=c$ erfüllt.

Beweis. Die Eindeutigkeit ist klar, weil $R[x]$ von $R \cup \{x\}$ erzeugt wird.
Sei $p(x) = \sum_{k=0}^{n} a_k x^k$ und $q(x) = \sum_{k=0}^{n} c_k x^k$. Dann gilt:

$$\begin{aligned}\varphi_c(p(x) + q(x)) &= \sum_{k=0}^{n} (f(a_k + b_k))c^k \\ &= \sum_{k=0}^{n} (f(a_k) + f(b_k))c^k \\ &= \sum_{k=0}^{n} f(a_k)c^k + \sum_{k=0}^{n} f(b_k)c^k \\ &= \varphi_c(p(x)) + \varphi_c(q(x)).\end{aligned}$$

Analog sieht man: $\varphi_c(p(x)q(x)) = \varphi_c(p(x))\varphi_c(q(x))$. □

Im Spezialfall $S = R$ erhalten wir den Einsetzungshomomorphismus $p(x) \mapsto p(c)$.
Im Spezialfall $S = R^R$ (das heißt, S ist die Menge aller Funktionen von R nach R) und $c = id_R$ erhalten wir eine Abbildung $\varphi : R[x] \to R^R$, die jedem Polynom $p(x) = \sum_{n=0}^{k} a_n x^n$ die Funktion $\varphi(p) : r \mapsto \varphi_r(p) = \sum_{n=0}^{k} a_n r^n$ zuordnet. Diese Funktion $\varphi(p)$ ist dann die „durch $p(x)$ induzierte“ Funktion.

4.2.3 Anmerkung. In der Analysis ist es üblich, nicht zwischen einem Polynom p und der durch p induzierten Polynomfunktion zu unterscheiden. Diese Identifikation kann man durch Satz 4.2.12 rechtfertigen. Wenn wir aber endliche Strukturen oder Ringe mit Nullteilern betrachten, ist die gerade definierte Abbildung φ nicht injektiv, zwei verschiedene Polynome können also dieselbe Funktion induzieren; mit $p(x) = q(x)$ meinen wir im Allgemeinen die Gleichheit der Polynome (d.h., die Gleichheit aller einander entsprechenden Koeffizienten), und nicht die Gleichheit der Polynomfunktionen.

4.2.4 Beispiel. Die Polynome $p(x) = x^2 + x$ und $q(x) = 0$ induzieren auf dem zweielementigen Ring $\mathbb{Z}_2$ dieselbe Polynomfunktion. Es gilt also $p(x) \neq q(x)$, aber $\varphi(p(x)) = \varphi(q(x))$

4.2.5 Beispiel. Gilt etwa $f(x)^2 - g(x)h(x) + k(x) = f(x)^4 + k(x)^2$ mit $f(x), g(x), h(x), k(x) \in R[x]$ und ist $a \in R$, so gilt auch $f(a)^2 - g(a)h(a) + k(a) = f(a)^4 + k(a)^2$.

4.2.6 Definition. Sei $p(x) \in R[x]$ (R kommutativer Ring mit Einselement). Dann heißt $a \in R$ *Nullstelle* von $p(x) :\Leftrightarrow p(a) = 0$. $p(x)$ heißt *teilbar* durch $q(x) \in R[x]$ (in Zeichen: $q(x)|p(x)) :\Leftrightarrow p(x) = q(x)r(x)$ mit $r(x) \in R[x]$.

4.2.7 Satz. *Ist a Nullstelle von $p(x)$, so ist $p(x)$ teilbar durch das lineare Polynom $x - a$ (und umgekehrt).*

Beweis. Sei $p(x) = a_n x^n + \cdots + a_1 x + a_0$. Man bildet

$$\begin{aligned}q(x) &:= p(x) - a_n x^{n-1}(x - a) = b_{n-1}x^{n-1} + \cdots + b_1 x + b_0, \\ r(x) &:= q(x) - b_{n-1}x^{n-2}(x - a) = c_{n-2}x^{n-2} + \cdots + c_1 x + c_0, \\ s(x) &:= r(x) - c_{n-2}x^{n-3}(x - a) = d_{n-3}x^{n-3} + \cdots + d_1 x + d_0 \text{ usw.}\end{aligned}$$

und erhält $p(x) = a_n x^{n-1}(x - a) + q(x) = a_n x^{n-1}(x - a) + b_{n-1}x^{n-2}(x - a) + r(x) = a_n x^{n-1}(x - a) + b_{n-1}x^{n-2}(x - a) + c_{n-2}x^{n-3}(x - a) + s(x) = \ldots = a_n x^{n-1}(x - a) + \cdots + k_1(x - a) + k_0$. Wegen $0 = p(a) = a_n a^{n-1}(a - a) + \cdots + k_1(a - a) + k_0 = k_0$ ist $k_0 = 0$ und $p(x) = (x - a)(a_n x^{n-1} + \cdots + k_1)$. Also gilt: $x - a$ teilt $p(x)$. (Wir haben praktisch $p(x)$ durch $x - a$ dividiert und den Rest $k_0 = 0$ erhalten!) □

Von nun an sei R ein Integritätsbereich (z. B. $R = \mathbb{Z}$ oder R Körper). In Integritätsbereichen kann man Gleichungen „kürzen“, das heißt:

> Sei $a \neq 0$. Dann[4] gilt: $ab = ac \Rightarrow b = c$.
> (Wenn nämlich $ab = ac$, dann $ab - ac = a(b - c) = 0$, also $b - c = 0$.)

Ist $\operatorname{grad} p(x) = n$ und gilt $(x-a)^k | p(x)$, d. h., $p(x) = (x-a)^k q(x)$, dann ist $k + \operatorname{grad} q(x) = \operatorname{grad} p(x) = n$, woraus $k \leq n$ folgt.

4.2.8 Definition. Sei $p(x) \in R[x] \setminus \{0\}$ und $a \in R$ Nullstelle von $p(x)$. Dann heißt das größte k mit $(x-a)^k | p(x)$ die *Vielfachheit* der Nullstelle a. (Nach der eben gemachten Bemerkung ist $k \leq n$.)

4.2.9 Satz. *Seien $a_1, \ldots, a_r$ paarweise verschiedene Nullstellen von $p(x) \in R[x]$ mit den Vielfachheiten $k_1, \ldots, k_r$. Dann gilt:*

$$(x-a_1)^{k_1} \cdots (x-a_r)^{k_r} | p(x).$$

Beweis. Für $r = 1$ ist nichts mehr zu zeigen. Für $r > 1$ ist aufgrund der Voraussetzung $p(x) = (x-a_1)^{k_1} q_1(x) = (x-a_2)^{k_2} q(x)$. Da $p(a_2) = (a_2-a_1)^{k_1} q_1(a_2) = 0$ und $(a_2-a_1)^{k_1} \neq 0$, muss $q_1(a_2) = 0$ und damit $q_1(x) = (x-a_2)q_2(x)$ gelten.
Also ist $p(x) = (x-a_1)^{k_1}(x-a_2)q_2(x) = (x-a_2)^{k_2} q(x)$. Durch „Kürzen“ dieser Gleichung durch $x - a_2$ (dieses Polynom ist ja $\neq 0$) erhalten wir daraus $(x-a_1)^{k_1} q_2(x) = (x-a_2)^{k_2-1} q(x)$. Falls $k_2 - 1 > 0$ ist, erhält man analog $p(x) = (x-a_1)^{k_1}(x-a_2)^2 q_3(x) = (x-a_2)^{k_2} q(x)$, d. h., $(x-a_1)^{k_1} q_3(x) = (x-a_2)^{k_2-2} q(x)$. Nach k_2 Schritten erhält man so $p(x) = (x-a_1)^{k_1}(x-a_2)^{k_2} q_{k_2+1}(x)$, d. h., $(x-a_1)^{k_1}(x-a_2)^{k_2} | p(x)$. Mit den restlichen Nullstellen $a_3, \ldots, a_r$ verfährt man ebenso und erhält schließlich die Behauptung. □

4.2.10 Folgerung. Seien $a_1, \ldots, a_r$ paarweise verschiedene Nullstellen von $p(x) \in R[x]$ mit den Vielfachheiten $k_1, \ldots, k_r$. Dann gilt: $k_1 + \cdots + k_r \leq \operatorname{grad} p(x)$.

Ein Polynom vom Grad n über einem Integritätsbereich hat also höchstens n Nullstellen, wobei jede Nullstelle mit ihrer Vielfachheit gezählt wird.

4.2.11 Satz. *Seien $p(x), q(x) \in R[x]$, $\operatorname{grad} p(x), \operatorname{grad} q(x) \leq n$ und $p(b_i) = q(b_i)$ für $n+1$ paarweise verschiedene Elemente $b_0, \ldots, b_n$ von R. Dann gilt $p(x) = q(x)$.*

Beweis. $(p-q)(b_i) = 0$ für $0 \leq i \leq n \Rightarrow p-q$ hat $n+1$ Nullstellen $\Rightarrow p-q = 0 \Rightarrow p = q$. □

4.2.12 Satz. *Sei R ein unendlicher Integritätsbereich, und seien $p(x), q(x) \in R[x]$ Polynome. Dann gilt: $p(x) = q(x)$ gilt genau dann, wenn $\varphi(p(x)) = \varphi(q(x))$, das heißt, wenn $p(r) = q(r)$ für alle $r \in R$ gilt.*

4.2.13 Anmerkung. Sei S ein Ring, $R \leq S$ ein Unterring von S. Dann kann jedes Polynom $p(x) \in R[x]$ auch als Element von $S[x]$ aufgefasst werden. Mit $\varphi^S(p)$ bezeichnen wir jene Funktion von S nach S, die jedes $s \in S$ auf $p(s)$ abbildet; $\varphi^R(p)$ ist die Einschränkung dieser Funktion auf R.
Es gilt nun (für beliebige Ringe R; diese Ringe dürfen auch endlich sein und Nullteiler haben) für beliebige Polynome $p, q \in R[x]$, dass die folgenden Aussagen äquivalent sind:

[4] Achtung! Die hier betrachtete „Kürzbarkeit“ bezieht sich nur auf die Multiplikation in R, nicht aber auf Multiplikation mit Elementen von $\mathbb{Z}$, d.h. auf iterierte Addition. Zum Beispiel kann man aus $2b = 2c$ (also $b + b = c + c$) im Allgemeinen nicht auf $b = c$ schließen, auch nicht in nullteilerfreien Ringen. Man betrachte etwa den nullteilerfreien Ring — sogar Körper — $\mathbb{Z}_2$.

(a) $p = q$

(b) Für alle S mit $R \leq S$ gilt $\varphi^S(p) = \varphi^S(q)$.

(c) Für den Ring $S := R[x]$ (den wir als Oberring von R auffassen) gilt $\varphi^S(p) = \varphi^S(q)$.

(d) Für den Ring $S := R[x]$ und das Element $s := x$ gilt $\varphi_s(p) = \varphi_s(q)$.

Zum Beweis genügt es, sich zu überlegen, dass $\varphi_s(p) = p$ ist. (Etwa mit Induktion nach dem Grad von p, oder indem man zeigt, dass die Menge aller p, die diese Gleichung erfüllen, ein Ring ist, der $R \cup \{x\}$ enthält.)

Ein Polynom braucht keine Nullstellen zu besitzen.

4.2.14 Beispiele. 1) $x^2 - 2 \in \mathbb{Q}[x]$ hat keine Nullstellen in $\mathbb{Q}$, wohl aber in $\mathbb{R} \supset \mathbb{Q}$, nämlich $\pm\sqrt{2}$.

2) $x^2 + 1 \in \mathbb{R}[x]$ hat keine Nullstellen in $\mathbb{R}$, wohl aber in $\mathbb{C} \supset \mathbb{R}$, nämlich $\pm i$.

4.2.15 Definition. Ein Körper K heißt *algebraisch abgeschlossen*, wenn jedes $p(x) \in K[x] \setminus K$ mindestens eine Nullstelle besitzt.

4.2.16 Anmerkung. Hat in einem Integritätsbereich jedes lineare Polynom eine Nullstelle, so ist dieser bereits ein Körper ($ax - 1$ ($a \neq 0$) habe die Nullstelle $c \Rightarrow ac = 1 \Rightarrow c = a^{-1}$).

4.2.17 Satz (Fundamentalsatz der Algebra von Gauß)**.** $\mathbb{C}$ *ist algebraisch abgeschlossen.*

Der Beweis wird später geführt (Kapitel 7). □

4.2.18 Satz. *Ist K ein Körper, dann sind folgende Aussagen äquivalent:*

a) K ist algebraisch abgeschlossen.

b) Für alle $p(x) \in K[x]$ mit $\operatorname{grad} p(x) = n > 0$ gilt: $p(x) = c(x - b_1)^{k_1} \cdots (x - b_r)^{k_r}$ mit $b_1, \ldots, b_r, c \in K$ und $k_1 + \cdots + k_r = n$.

Beweis. b) $\Rightarrow$ a): trivial.
a) $\Rightarrow$ b): Sei $p(x) \in K[x]$, $\operatorname{grad} p(x) > 0$. Dann gibt es ein $a_1 \in K$ mit $p(a_1) = 0$, d. h., $p(x) = (x - a_1)p_1(x)$. Ist $\operatorname{grad} p_1(x) > 0$, erhält man analog $p_1(x) = (x - a_2)p_2(x)$, also $p(x) = (x - a_1)(x - a_2)p_2(x)$. Fortgesetzte Anwendung dieser Überlegung ergibt schließlich $p(x) = (x - a_1)(x - a_2) \cdots (x - a_n)c$. Faßt man gleiche Faktoren $(x - a_i)$ zu Potenzen zusammen, erhält man die behauptete Darstellung. □

Berechnung von Nullstellen von Polynomen über Körpern.
1) $\operatorname{grad} p(x) = 1$: trivial.
2) $\operatorname{grad} p(x) = 2$: $p(x) = ax^2 + bx + c$ ($a \neq 0$) hat die Nullstellen $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ („2“ bzw. „4“ steht hier für $1 + 1$ bzw. $1 + 1 + 1 + 1$; der Wurzelausdruck muss existieren und $1 + 1 \neq 0$ sein).
3) $\operatorname{grad} p(x) = 3, 4$: Formeln von Cardano (Tartaglia).
4) $\operatorname{grad} p(x) > 4$: Hier gibt es keine allgemeinen „Formeln“ (bestehend aus Grundrechnungsarten und Wurzelausdrücken) mehr.

4.3 Interpolation durch Polynome

Sei K ein Körper und $f : K \to K$ eine Funktion.
Gegeben: $b_i = f(a_i)$ für paarweise verschiedene $a_i \in K$, $1 \le i \le n$ (z. B.: Messreihe).
Gesucht: $p(x) \in K[x]$ mit $p(a_i) = b_i = f(a_i)$, $1 \le i \le n$ und $\operatorname{grad} p(x) < n$. (Es kann höchstens ein solches Polynom $p(x)$ geben: aus $p(a_i) = q(a_i)$, $1 \le i \le n$, mit $\operatorname{grad} p(x), \operatorname{grad} q(x) < n$ folgt nämlich $p = q$.)

4.3.A Interpolationsformel von Lagrange

Sei

$$q_i(x) := \prod_{\substack{1 \le j \le n, \\ j \ne i}} (x - a_j) = (x - a_1) \cdots (x - a_{i-1})(x - a_{i+1}) \cdots (x - a_n).$$

Dann gilt:

$$q_i(a_k) = \begin{cases} 0 & \text{für } i \ne k, \\ \prod_{1 \le j \le n,\, j \ne i} (a_k - a_j) \ne 0 & \text{für } i = k. \end{cases}$$

Für

$$p(x) := \sum_{i=1}^{n} b_i \frac{q_i(x)}{q_i(a_i)}$$

gilt dann $p(a_j) = b_j$, $1 \le j \le n$.

4.3.1 Folgerung. Ist K ein *endlicher* Körper (z. B. $K = \mathbb{Z}_p$, p Primzahl), $f : K \to K$, dann gibt es ein Polynom $p(x) \in K[x]$ mit $f(a) = p(a)$ für alle $a \in K$.

4.3.2 Beispiel. Um ein quadratisches Polynom $p(x) \in \mathbb{Q}[x]$ zu erhalten, das an den Stellen 1, 2, 3 die Werte 10, 41, 62 hat, definiert man einfach

$$p(x) := 10\frac{(x-2)(x-3)}{(1-2)(1-3)} + 41\frac{(x-1)(x-3)}{(2-1)(2-3)} + 62\frac{(x-1)(x-2)}{(3-1)(3-2)} = (-5)x^2 + 46x^1 + (-31)x^0$$

4.3.B Interpolationsformel von Newton

Sei K ein Körper, $n \in \mathbb{N}$, $K_{n-1}[x] := \{p(x) \in K[x] \mid \operatorname{grad} p(x) < n\} \cup \{0\}$. Dann gilt: $K_{n-1}[x] = \{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \mid a_i \in K\}$ ist n-dimensionaler Vektorraum über K mit der Basis $\{1, x, \ldots, x^{n-1}\}$.

Man sieht leicht: Ist $\varphi_i(x) \in K[x]$, $\operatorname{grad} \varphi_i(x) = i-1$, $1 \le i \le n$, dann ist $\{\varphi_1(x), \ldots, \varphi_n(x)\}$ ebenfalls Basis von $K_{n-1}[x]$. (Die Matrix, die den Basiswechsel beschreibt, ist nämlich eine Dreiecksmatrix, in deren Diagonale genau die höchsten Koeffizienten der Polynome φ_i stehen.)

Sei nun $f : K \to K$, $a_1, \ldots, a_n \in K$, $f(a_i) = b_i$, $1 \le i \le n$. Setzt man $\varphi_1(x) := 1$ und

$$\varphi_i(x) := \prod_{j=1}^{i-1} (x - a_j), \qquad 2 \le i \le n,$$

so ist $\{\varphi_1(x), \ldots, \varphi_n(x)\}$ nach der eben gemachten Bemerkung Basis von $K_{n-1}[x]$. Für das gesuchte Interpolationspolynom $p(x)$ mit $p(a_i) = b_i$, $1 \le i \le n$, muss daher gelten:

$$p(x) = \sum_{i=1}^{n} \lambda_i \varphi_i(x)$$

für geeignete $\lambda_i \in K$. Diese lassen sich aus dem folgenden Gleichungssystem in Halbdiagonalform berechnen:

$$\begin{aligned} p(a_1) &= b_1 = \lambda_1 \\ p(a_2) &= b_2 = \lambda_1 + \lambda_2(a_2 - a_1) \\ p(a_3) &= b_3 = \lambda_1 + \lambda_2(a_3 - a_1) + \lambda_3(a_3 - a_1)(a_3 - a_2) \\ &\vdots \end{aligned}$$

Vorteil dieser Interpolationsmethode: bei Hinzufügen einer neuen Stützstelle $b_{n+1} = f(a_{n+1})$ bleiben $\lambda_1, \ldots, \lambda_n$ unverändert, nur λ_{n+1} muss neu berechnet werden.

Kapitel 5

Integritätsbereiche und Teilbarkeit

5.1 Einfache Teilbarkeitsregeln

5.1.1 Definition. Sei $(I, +, 0, -, \cdot, 1)$ ein Integritätsbereich. Sind $a, b \in I$, dann heißt a durch b *teilbar* und b ein *Teiler* von a (b „teilt“ a, in Zeichen: $b|a$) $:\Leftrightarrow \exists c \in I : a = bc$.

Elementare Teilbarkeitsregeln:

1) $\forall a \in I : a|0$,

2) $\forall a \in I : 1|a$,

3) $\forall a \in I : a|a$,

4) $\forall a, b, c \in I : a|b$ und $b|c \Rightarrow a|c$,

5) $\forall a, b, c \in I : a|b \Rightarrow a|bc$,

6) $\forall a, b, c \in I : a|b$ und $a|c \Rightarrow a|b + c$,

7) $\forall a, b, c \in I, c \neq 0 : a|b \Leftrightarrow ac|bc$,

8) $\forall a, b, c, d \in I : a|b$ und $c|d \Rightarrow ac|bd$,

9) $\forall a, b \in I, n \in \mathbb{N} : a|b \Rightarrow a^n|b^n$.

5.1.2 Definition. Sei $(I, +, 0, -, \cdot, 1)$ ein Integritätsbereich. Jeder Teiler von 1 heißt *Einheit* von I. Sei $E(I)$ die Menge aller Einheiten von I. $a, b \in I$ heißen *assoziiert* (in Zeichen: $a \sim b$) $:\Leftrightarrow \exists e \in E(I) : a = be$.

5.1.3 Beispiele. 1) $I = \mathbb{Z}$: $E(I) = \{\pm 1\}$, also $a \sim b \Leftrightarrow a = \pm b$.

2) $I = K$ (K Körper): $E(I) = K \setminus \{0\}$, also $a \sim b \Leftrightarrow a, b \neq 0 \vee a = b = 0$.

3) $I = K[x]$ (K Körper): $E(I) = K \setminus \{0\}$ (wegen $\operatorname{grad} p(x)q(x) = \operatorname{grad} p(x) + \operatorname{grad} q(x)$), also gilt: $p(x) \sim q(x) \Leftrightarrow \exists a \in K \setminus \{0\} : p(x) = aq(x)$.

5.1.4 Satz. *a) $e \in I$ ist eine Einheit von $I \Leftrightarrow \exists f \in I : ef = 1$.*

b) $(E(I), \cdot)$ ist eine abelsche Gruppe, genannt die Einheitengruppe *von I.*

c) $\sim$ ist eine Kongruenzrelation auf $(I, \cdot)$.

d) $\forall a, b \in I : a \sim b \Leftrightarrow a|b$ und $b|a$.

Beweis. a) folgt unmittelbar aus der Definition.

b) $1 \in E(I)$; $e_1, e_2 \in E(I) \Rightarrow \exists f_1, f_2 : e_1 f_1 = e_2 f_2 = 1 \Rightarrow (e_1 e_2)(f_1 f_2) = 1 \cdot 1 = 1 \Rightarrow e_1 e_2 \in E(I)$; $e \in E(I) \Rightarrow \exists f : ef = 1 \Rightarrow f \in E(I)$, und f ist Inverses zu e.

c) $a \sim a$, denn $a = a \cdot 1$; $a \sim b \Rightarrow a = be \Rightarrow b = ae^{-1}$ $(e, e^{-1} \in E(I)) \Rightarrow b \sim a$; $a \sim b$, $b \sim c \Rightarrow a = be$, $b = cf \Rightarrow a = c(ef) \Rightarrow a \sim c$ (wegen $ef \in E(I)$). Also ist $\sim$ eine Äquivalenzrelation. Weiters gilt: $a \sim b$, $c \sim d \Rightarrow a = be$, $c = df \Rightarrow ac = (bd)(ef) \Rightarrow ac \sim bd$.

d) $\Rightarrow$: $a \sim b \Rightarrow a = be$, $b = ae^{-1} \Rightarrow b|a$ und $a|b$.
$\Leftarrow$: $b|a$ und $a|b \Rightarrow a = bc$ und $b = ad \Rightarrow a = adc$. Für $a = 0$ ist auch $b = 0$. Für $a \neq 0$ ist $1 = dc$, also $d, c \in E(I)$, d. h., $a \sim b$. □

5.1.5 Beispiele. Äquivalenzklassen bezüglich $\sim$:

1) $I = \mathbb{Z}$: $\{0\}$, $\{\pm 1\}, \{\pm 2\}, \ldots, \{\pm n\}, \ldots$, $n \in \mathbb{N}$.

2) $I = K$: $\{0\}, K \setminus \{0\}$.

3) $I = K[x]$: $\{0\}$, $\{ap(x) \mid a \in K \setminus \{0\}\}$, $p(x)$ normiert.

5.1.6 Definition. Sei $(I, +, 0, -, \cdot, 1)$ ein Integritätsbereich, $a \in I$.

Triviale Teiler von a: alle $e \in E(I)$ und alle b mit $b \sim a$.
Echte Teiler von a: alle b mit $b|a$ und $b \not\sim a$.

5.1.7 Definition. $a \in I \setminus E(I)$, $a \neq 0$, heißt *irreduzibel* $:\Leftrightarrow a$ hat nur triviale Teiler.

5.1.8 Beispiele. 1) $I = \mathbb{Z}$: $a \in I$ irreduzibel $\Leftrightarrow a = \pm p$, p Primzahl.

2) $I = K[x]$ (K Körper): Die irreduziblen Elemente heißen *irreduzible Polynome*. Z. B. ist ein lineares Polynom $ax + b$, $a \neq 0$, stets irreduzibel. In einem algebraisch abgeschlossenen Körper ist jedes irreduzible Polynom auch linear.

3) $I = \mathbb{R}[x]$: Irreduzibel sind hier alle linearen Polynome sowie alle Polynome $ax^2 + bx + c$ mit $a \neq 0$ und $b^2 - 4ac < 0$. (Aus dem Fundamentalsatz der Algebra folgt, dass es keine weiteren gibt.)

4) $I = K[x]$, K endlicher Körper: Zu jedem $n \in \mathbb{N}$ gibt es ein $p(x) \in K[x]$ mit $\operatorname{grad} p(x) = n$ und $p(x)$ irreduzibel. (Siehe Abschnitt 6.6.)

5.1.9 Definition. $p \in I \setminus E(I)$, $p \neq 0$, heißt *primes Element* oder *Primelement* $:\Leftrightarrow p|ab \Rightarrow p|a \vee p|b$.

5.1.10 Beispiel. Für $I = \mathbb{Z}$, $K[x]$ (K Körper) gilt: p irreduzibel $\Leftrightarrow p$ prim (folgt aus Abschnitt 5.3 und 5.4).

5.1.11 Anmerkungen. 1) a irreduzibel und $b \sim a \Rightarrow b$ irreduzibel.

2) p prim und $q \sim p \Rightarrow q$ prim.

3) p prim $\Rightarrow p$ irreduzibel, denn: $a|p \Rightarrow \exists b \in I : p = ab \Rightarrow p|ab \Rightarrow p|a \vee p|b$ und $a|p$ und $b|p$. Also gilt $p \sim a \vee p \sim b$. Im Falle $p \sim b$ ist $p = eb = ab$ für eine Einheit e. Wegen $p \neq 0$ ist $b \neq 0$ und daher $a = e$. Also ist in jedem Falle a ein trivialer Teiler von p. (Die Umkehrung von 3) gilt im allgemeinen nicht!)

5.2 ZPE-Ringe

5.2.1 Definition. Ein Integritätsbereich I heißt ein *ZPE-Ring* (Ring mit Primelementzerlegung, Ring mit eindeutiger Primelementzerlegung, Gauß'scher Ring, faktorieller Ring) :$\Leftrightarrow$ Zu jedem $a \in I \setminus E(I)$, $a \neq 0$, gibt es Primelemente $p_1, \ldots, p_r$ mit $a = p_1 \cdots p_r$.

5.2.2 Satz (Eindeutigkeit der Primelementzerlegung)**.** *Sei I ein ZPE-Ring, $a \in I \setminus E(I)$, $a \neq 0$, $a = p_1 \cdots p_r = q_1 \cdots q_s$ mit Primelementen $p_1, \ldots, p_r, q_1, \ldots, q_s$. Dann ist $r = s$, und es gibt eine Permutation π von $\{1, \ldots, r\}$ mit $p_i \sim q_{\pi(i)}$, $i = 1, \ldots, r$.*

Beweis. Da $p_1 | q_1 \cdots q_s$, gibt es ein $\pi(1)$, $1 \leq \pi(1) \leq r$ mit $p_1 | q_{\pi(1)}$, d. h., $p_1 \sim q_{\pi(1)}$. Für eine geeignete Einheit e_1 gilt daher $e_1 p_2 \cdots p_r = q_1 \cdots q_{\pi(1)-1} \cdot q_{\pi(1)+1} \cdots q_s$. Durch wiederholte Anwendung dieser Überlegung erhält man schließlich die Behauptung. □

5.2.3 Satz (Teilerkettenbedingung)**.** *Sei I ein ZPE-Ring. Dann gibt es keine unendliche Folge $(a_n)_{n \in \mathbb{N}}$ von Elementen von I, sodass für alle $n \in \mathbb{N}$ das Element a_{n+1} ein echter Teiler von a_n ist.*

Beweis. Es genügt, zu zeigen, dass es in $I \setminus \{0\}$ keine solche Folge geben kann. Nach dem gerade bewiesenen Satz gibt es zu jedem Element $a \in I \setminus \{0\}$ eine eindeutig bestimmte Zahl $r = r(a)$, sodass sich a als Produkt von r Primelementen schreiben lässt. (Für Einheiten a setzen wir $r(a) = 0$.)
Wenn b ein echter Teiler von a ist, dann ist $r(b) < r(a)$.
Wenn also $r(a_1) = k$ ist, dann kann es keine Folge $(a_n)_{n=1,\ldots,k+1,k+2}$ von Elementen von $I \setminus \{0\}$ geben, sodass für alle $n \leq k+1$ das Element a_{n+1} ein echter Teiler von a_n ist; erst recht kann es keine unendliche solche Folge geben. □

5.2.4 Beispiele. $\mathbb{Z}$ und $K[x]$ (K Körper) sind ZPE-Ringe (Beweis folgt aus Abschnitt 5.4).

5.2.5 Definition. Sei I Integritätsbereich, $a_1, \ldots, a_n \in I$.

1) $d \in I$ heißt ein *größter gemeinsamer Teiler (ggT)* von $a_1, \ldots, a_n \in I$:$\Leftrightarrow$ (i) $d | a_i$, $i = 1, \ldots, n$ und (ii) $\forall t \in I : t | a_i$, $i = 1, \ldots, n \Rightarrow t | d$.

2) $v \in I$ heißt ein *kleinstes gemeinsames Vielfaches (kgV)* von $a_1, \ldots, a_n \in I$:$\Leftrightarrow$ (i) $a_i | v$, $i = 1, \ldots, n$ und (ii) $\forall w \in I : a_i | w$, $i = 1, \ldots, n \Rightarrow v | w$.

5.2.6 Anmerkung. Sei d ein ggT von $a_1, \ldots, a_n$ und $d_1 \in I$. Dann gilt: d_1 ist ein ggT von $a_1, \ldots, a_n \Leftrightarrow d_1 \sim d$. Eine entsprechende Aussage gilt für das kgV.

5.2.7 Satz. *In einem ZPE-Ring I ist jedes irreduzible Element prim.*

Beweis. $a \in I$, a irreduzibel $\Rightarrow a \notin E(I)$, $a \neq 0 \Rightarrow a = p_1 \cdots p_r$ mit p_i prim $\Rightarrow p_1 | a$, $p_1 \notin E(I)$, d. h., $p_1 \sim a \Rightarrow a$ prim. □

Wir betrachten die Quotientenmenge $I/\!\sim = \{[a]_\sim \mid a \in I\}$ und denken uns aus jeder Klasse $[a]_\sim = \{b \in I \mid b \sim a\}$ ein festes Element $\mathbf{n}([a]_\sim)$ herausgegriffen (Auswahlaxiom!), d. h.,

$$\mathbf{n} : \begin{cases} I/\!\sim \to I \\ [a]_\sim \mapsto \mathbf{n}([a]_\sim) \in [a]_\sim. \end{cases}$$

Die Elemente der Menge $\mathbf{n}(I/\!\sim)$ heißen *normierte Elemente* (bezüglich $\mathbf{n}$).

Jede Klasse $[a]_\sim$ mit a prim besteht zur Gänze aus Primelementen. Die Elemente $\mathbf{n}([a]_\sim)$ mit a prim heißen *normierte Primelemente*.

5.2.8 Beispiele. 1) $I = \mathbb{Z}$, $\mathbf{n}([a]_\sim) = \mathbf{n}(\{\pm a\}) = |a|$.

2) $I = K[x]$, $\mathbf{n}(\{0\}) = 0$, $\mathbf{n}([p(x)]_\sim) = q(x)$, wobei $p(x) = a_n x^n + \cdots + a_1 x + a_0$, $a_n \neq 0$, $q(x) = (1/a_n)p(x)$. Wir wählen also aus jeder $\sim$-Klasse das Polynom mit höchstem Koeffizienten 1 aus.

5.2.9 Satz. *Ist I ein ZPE-Ring, $a \in I \setminus E(I)$, $a \neq 0$, dann gilt $a = ep_1^{e_1} \cdots p_r^{e_r}$, wobei $e \in E(I)$, $p_1, \ldots, p_r$ normierte, paarweise verschiedene Primelemente, $e_i \in \mathbb{N}$.* □

5.2.10 Lemma. *Sei I ein ZPE-Ring, $a, b \in I \setminus \{0\}$, $a = fp_1^{f_1} \cdots p_r^{f_r}$, $b = gp_1^{g_1} \cdots p_r^{g_r}$ (p_j prim, normiert und paarweise verschieden, $f_j, g_j \in \mathbb{N}_0$, $f, g \in E(I)$). Dann gilt: $a|b \Leftrightarrow f_j \leq g_j$ für $j = 1, \ldots, r$.*

Beweis. $a|b \Rightarrow \exists c \in I : b = ac \Rightarrow c = hp_1^{h_1} \cdots p_r^{h_r}$, $h_j \in \mathbb{N}_0$, $h \in E(I)$ (da I ZPE-Ring) $\Rightarrow f_j + h_j = g_j$, $j = 1, \ldots, r \Rightarrow f_j \leq g_j$, $j = 1, \ldots, r$.
Umkehrung: Ist $f_j \leq g_j$, $j = 1, \ldots, r$, so gilt mit $h_j := g_j - f_j \in \mathbb{N}_0$, $c := f^{-1}gp_1^{h_1} \cdots p_r^{h_r}$: $ac = b$, d. h., $a|b$. □

5.2.11 Satz. *Sei I ein ZPE-Ring, $a_1, \ldots, a_n \in I$, $a_i \neq 0$, $a_i = e_i p_1^{e_{1i}} \cdots p_r^{e_{ri}}$, $e_i \in E(I)$, p_j paarweise verschiedene normierte Primelemente, $e_{ji} \in \mathbb{N}_0$. Dann gilt:*

$$\mathrm{ggT}(a_1, \ldots, a_n) = p_1^{\min_{1 \leq i \leq n}(e_{1i})} \cdots p_r^{\min_{1 \leq i \leq n}(e_{ri})}$$

und

$$\mathrm{kgV}(a_1, \ldots, a_n) = p_1^{\max_{1 \leq i \leq n}(e_{1i})} \cdots p_r^{\max_{1 \leq i \leq n}(e_{ri})}.$$

Sind einige $a_i = 0$, so ist $\mathrm{ggT}(a_1, \ldots, a_n) = \mathrm{ggT}(a_i \mid a_i \neq 0)$, sind alle $a_i = 0$, so ist $\mathrm{ggT}(a_1, \ldots, a_n) = 0$. Sind einige $a_i = 0$, so ist $\mathrm{kgV}(a_1, \ldots, a_n) = 0$.

Beweis. Sei $d := p_1^{\min_{1 \leq i \leq n}(e_{1i})} \cdots p_r^{\min_{1 \leq i \leq n}(e_{ri})}$.
(i) $\min_i(e_{ji}) \leq e_{jk}$ für alle $k \in \{1, \ldots, n\} \Rightarrow d|a_k$, $k = 1, \ldots, n$.
(ii) $t|a_k$ für alle $k \in \{1, \ldots, n\} \Rightarrow t = fp_1^{f_1} \cdots p_r^{f_r}$ mit $f \in E(I)$, $f_j \leq e_{jk}$, $k = 1, \ldots, n$, $j = 1, \ldots, r \Rightarrow f_j \leq \min_i(e_{ji})$, $j = 1, \ldots, r \Rightarrow t|d$.
Die Sonderfälle (einige oder alle $a_i = 0$) sind trivial.
Die Aussage über das kgV beweist man analog zum ggT. □

5.2.12 Satz. *Sei I ein ZPE-Ring, und $\wedge, \vee$ auf $I/\sim = \{[a]_\sim \mid a \in I\}$ definiert durch*

$$[a]_\sim \wedge [b]_\sim := [\mathrm{ggT}(a, b)]_\sim, \qquad [a]_\sim \vee [b]_\sim := [\mathrm{kgV}(a, b)]_\sim.$$

Dann sind $\wedge$ und $\vee$ wohldefiniert (d. h., vom Repräsentanten unabhängig) und $(I/\sim, \wedge, \vee)$ ist ein Verband mit Nullelement $[1]_\sim = E(I)$ und Einselement $[0]_\sim = \{0\}$ („Teilerverband“). Die zugehörige Ordnung $\leq$ ist gegeben durch: $[a]_\sim \leq [b]_\sim :\Leftrightarrow a|b$.

Der Beweis dieses Satzes folgt unschwer aus den Definitionen. □

5.2.13 Beispiel. $(\mathbb{Z}/\sim, \wedge, \vee) \cong (\mathbb{N}_0, \mathrm{ggT}, \mathrm{kgV})$.

5.2.A Charakterisierung von ZPE-Ringen

5.2.14 Satz. *Ein Integritätsbereich I ist genau dann ZPE-Ring, wenn die folgenden Bedingungen erfüllt sind:*

(*a*) *Jedes irreduzible Element ist prim.*

(*b*) *Teilerkettenbedingung: es gibt keine unendliche Folge $(a_n)_{n\in\mathbb{N}}$ von Elementen von I, sodass für alle $n \in \mathbb{N}$ das Element a_{n+1} ein echter Teiler von a_n ist.*

Beweis. Wir wissen bereits, dass jeder ZPE-Ring die Bedingungen (a) und (b) erfüllt. Zu zeigen ist die Umkehrung.
Sei also I ein Integritätsbereich, der die Bedingungen (a) und (b) erfüllt. Sei $a \in I$, $a \neq 0$, $a \notin E(I)$. Wir haben zu zeigen, dass a eine Primelementzerlegung besitzt.
Indirekt: Angenommen, es gibt keine Primelementzerlegung von a. Dann ist a kein Primelement, wegen (a) also nicht irreduzibel. Somit existiert ein nichttrivialer Teiler a_1 von a, d. h., $a = a_1b_1$, wobei a_1, b_1 beide echte Teiler sind. (Denn: $b_1 \sim a \Rightarrow b_1 = ae$, $e \in E(I) \Rightarrow a = a_1ae \Rightarrow 1 = a_1e \Rightarrow a_1 \in E(I)$, Widerspruch!)
Einer der beiden Teiler (o. B. d. A. a_1) hat keine Primelementzerlegung (sonst hätte ja a eine solche). Daher existiert ein echter Teiler a_2 von a_1, welcher ebenfalls keine Primelementzerlegung besitzt. Auf diese Weise wäre es möglich, eine unendliche echte Teilerkette $a, a_1, a_2, \ldots$ zu konstruieren, was der Bedingung (b) widerspricht. □

5.3 Hauptidealringe

5.3.1 Satz. *Sei R ein kommutativer Ring mit Einselement, $a \in R$, $(a) := \{ar \mid r \in R\}$. Dann ist (a) das kleinste Ideal von R, welches a enthält.*

Beweis. (a) ist Ideal: $0 = a0 \in (a)$; $ar_1, ar_2 \in (a) \Rightarrow ar_1 + ar_2 = a(r_1 + r_2) \in (a)$; $-ar_1 = a(-r_1) \in (a)$; für beliebiges $r \in R$ ist $r(ar_1) = a(rr_1) \in (a)$. Weiters ist $a = a \cdot 1 \in (a)$. Da jedes Ideal, welches a enthält, alle ar, $r \in R$, und damit (a) enthalten muss, ist (a) das kleinste Ideal, welches a enthält. □

5.3.2 Definition. (a) heißt das *von a erzeugte Hauptideal* von R. Ein Ideal heißt Hauptideal, wenn es von der Form (a) für ein $a \in R$ ist.

5.3.3 Definition. Ein Integritätsbereich I heißt *Hauptidealring* :⇔ Jedes Ideal von I ist ein Hauptideal.

5.3.4 Beispiele. 1) Jeder Körper ist ein Hauptidealring: $\{0\} = (0)$ und $K = (1)$ sind die einzigen Ideale, da K einfach ist.

2) $\mathbb{Z}$, $K[x]$ (K Körper) sind Hauptidealringe (siehe Abschnitt 5.4).

3) $\mathbb{Q}[x, y]$ ist kein Hauptidealring. Das von der Menge $\{x, y\}$ erzeugte Ideal (anders gesagt: der Kern des Homomorphismus $h : \mathbb{Q}[x, y] \to \mathbb{Q}$, der jedem Polynom seinen konstanten Term zuordnet) ist kein Hauptideal.

4) $\mathbb{Z}[x]$ ist kein Hauptidealring. (Übungsbeispiel: Wenn R ein Integritätsbereich ist, und $a \in R$ kein multiplikatives Inverses hat, dann ist das von $\{a, x\}$ erzeugte Ideal kein Hauptideal.)

5.3.5 Lemma. *Sei I ein Integritätsbereich, dann gilt:*

1) $a|b \Leftrightarrow (a) \supseteq (b)$.

2) $a \sim b \Leftrightarrow (a) = (b)$.

Beweis. Folgt aus den Definitionen. □

5.3.6 Definition. Sei R ein kommutativer Ring mit Einselement, $J \lhd R$ (d. h. J Ideal von R), $J \neq R$. Dann heißt J

1) *maximales Ideal* $:\Leftrightarrow \forall K\,(K \lhd R, J \subseteq K \subseteq R \;\Rightarrow\; K = J \text{ oder } K = R)$,

2) *Primideal* $:\Leftrightarrow (ab \in J \Rightarrow a \in J \text{ oder } b \in J)$.

5.3.7 Satz. *Sei R ein kommutativer Ring mit Einselement und $J \lhd R$, dann gilt:*

a) R/J Körper $\Leftrightarrow$ J maximales Ideal,

b) R/J Integritätsbereich $\Leftrightarrow$ J Primideal.

Beweis. Übung. □

5.3.8 Folgerung. Jedes maximale Ideal ist ein Primideal.

5.3.9 Satz. *Sei I ein Integritätsbereich, $p \in I$, $p \neq 0$, $p \notin E(I)$. Dann gilt:*

a) (p) maximal in der Menge aller Hauptideale $\neq I \Leftrightarrow p$ irreduzibel,

b) (p) Primideal $\Leftrightarrow p$ prim.

Beweis. a) $\Rightarrow$: $a|p \Rightarrow (a) \supseteq (p) \;\Rightarrow\; (a) = (p)$ oder $(a) = I = (1) \;\Rightarrow\; a \sim p$ oder $a \sim 1 \;\Rightarrow$ p irreduzibel.
$\Leftarrow$: analog.

b) $\Rightarrow$: $p|ab \Rightarrow ab \in (p) \Rightarrow a \in (p)$ oder $b \in (p) \Rightarrow p|a$ oder $p|b$.
$\Leftarrow$: analog. □

5.3.10 Folgerung. Sei I ein Hauptidealring, $p \in I$, $p \neq 0$, $p \notin E(I)$. Dann gilt:

a) p prim $\Leftrightarrow$ p irreduzibel,

b) $I/(p)$ Körper $\Leftrightarrow$ p irreduzibel.

5.3.11 Beispiel. $\mathbb{Z} = \mathbb{Z}/(n)$ ist Körper $\Leftrightarrow n = \pm p$, p Primzahl.

5.3.12 Satz. *Sei I Hauptidealring, $a_1, \ldots, a_n \in I$. Dann existiert* $\mathrm{ggT}(a_1, \ldots, a_n) =: d$, *und es gibt $x_1, \ldots, x_n \in I$ mit $d = a_1x_1 + \cdots + a_nx_n$.*

Beweis. Sei $M := \{a_1r_1 + \cdots + a_nr_n \mid r_i \in I\}$. Dann gilt $M \lhd I$ (analog wie für das Hauptideal (a) einzusehen). Somit gibt es ein $d \in I$ mit $M = (d)$. Wir zeigen: $d = \mathrm{ggT}(a_1, \ldots, a_n)$: wegen $a_1, \ldots, a_n \in M = (d)$ gilt $d|a_1, \ldots, d|a_n$; aus $t|a_1, \ldots, t|a_n$ folgt $t|a_1r_1 + \cdots + a_nr_n$, $\forall r_1, \ldots, r_n \in I$, und daraus $t|d$ (denn $d \in M$). □

5.3.13 Lemma (Teilerkettensatz)**.** *Sei I Hauptidealring. Dann gibt es* keine *unendliche Folge $(a_n)_{n\in\mathbb{N}}$ von Elementen von I, sodass für alle $n \in \mathbb{N}$ das Element a_{n+1} ein echter Teiler von a_n ist.*

Beweis. Angenommen, es gibt eine solche Folge $(a_n)_{n\in\mathbb{N}}$. Dann muss $(a_1) \subset (a_2) \subset \ldots \subset (a_n) \subset (a_{n+1}) \subset \ldots$ gelten, wobei alle auftretenden Inklusionen echt sind. Für $J := \bigcup_{n=1}^{\infty}(a_n)$ gilt dann $J \lhd I$, denn: $0 \in J$; $a, b \in J \Rightarrow \exists n, m \in \mathbb{N}$ (o. B. d. A. $n \geq m$): $a \in (a_n)$, $b \in (a_m) \Rightarrow a, b \in (a_n) \Rightarrow a + b, -a, ra \in (a_n)$, $r \in I$, $\Rightarrow a + b, -a, ra \in J$. Also gibt es ein $d \in I$ mit $J = (d)$. Wegen $d \in J$ ist $d \in (a_n)$ für ein $n \in \mathbb{N}$ und damit $(d) \subseteq (a_n) \subseteq (d)$, woraus $(a_n) = (a_{n+1}) = \ldots$ folgt. Widerspruch zur Annahme! □

5.3.14 Folgerung. Jeder Hauptidealring ist ein ZPE-Ring.

5.4 Euklidische Ringe

5.4.1 Definition. Ein Integritätsbereich I heißt ein *Euklidischer Ring* $:\Leftrightarrow$ Es gibt eine Abbildung $H : I \setminus \{0\} \to \mathbb{N}_0$ („Euklidische Bewertung“) mit folgender Eigenschaft: für alle $a \in I \setminus \{0\}$, $b \in I$ gibt es $q, r \in I$, sodass $b = aq + r$ mit $r = 0$ oder $H(r) < H(a)$ („Division mit Rest“).

5.4.2 Beispiele. 1) $\mathbb{Z}$ ist ein Euklidischer Ring mit $H(a) := |a|$. (Siehe Abschnitt 1.3.)

2) Jeder Körper ist ein Euklidischer Ring ($q = a^{-1}b$, $r = 0$).

5.4.3 Satz. *$K[x]$ (K Körper) ist ein Euklidischer Ring mit $H(p(x)) := \operatorname{grad} p(x)$, d. h., für $p(x) \neq 0$, $p_1(x)$ beliebig, gibt es Polynome $q(x)$ und $r(x)$ mit $p_1(x) = p(x)q(x) + r(x)$, wobei $r(x) = 0$ oder $\operatorname{grad} r(x) < \operatorname{grad} p(x)$.*

Beweis. Sei $p(x) = a_m x^m + \cdots + a_1 x + a_0$, $a_m \neq 0$, $m = \operatorname{grad} p(x)$, $p_1(x) = b_n x^n + \cdots + b_1 x + b_0$. Für $n < m$ kann $q(x) = 0$ und $r(x) = p_1(x)$ gewählt werden. Für $n \geq m$ sei $p_2(x) := p_1(x) - b_n a_m^{-1} x^{n-m} p(x)$. Wir haben $p_2(x) = c_k x^k + \cdots + c_1 x + c_0$ mit $k \leq n-1$. Für $k < m$ kann $q(x) = b_n a_m^{-1} x^{n-m}$ und $r(x) = p_2(x)$ gewählt werden. Für $k \geq m$ sei $p_3(x) := p_2(x) - c_k a_m^{-1} x^{k-m} p(x)$. Wir haben $p_3(x) = d_l x^l + \cdots + d_1 x + d_0$ mit $l \leq k-1$. Für $l < m$ kann $q(x) = b_n a_m^{-1} x^{n-m} + c_k a_m^{-1} x^{k-m}$ und $r(x) = p_3(x)$ gewählt werden. Für $l \geq m$ wird das Verfahren fortgesetzt, und man erhält nach endlich vielen Schritten ein Polynom $p_t(x)$ mit $p_t(x) = 0$ oder $\operatorname{grad} p_t(x) < m$. □

5.4.4 Satz. *Jeder Euklidische Ring I ist ein Hauptidealring.*

Beweis. Sei $J \lhd I$, $J \neq (0) = \{0\}$. Zu zeigen: $\exists a \in I : J = (a) = \{aq \mid q \in I\}$. Sei $a \in J \setminus \{0\}$ so gewählt, dass $H(a) = \min\{H(x) \mid x \in J \setminus \{0\}\}$. Wir behaupten, dass dann $J = (a)$ gilt. Trivialerweise gilt $(a) \subseteq J$. Sei umgekehrt $b \in J$. Wegen $a \neq 0$ gibt es $q, r \in I$ mit $b = aq + r$ und $r = 0 \vee H(r) < H(a)$. Es ist $r = b - aq \in J$ (wegen $J \lhd I$), woraus (wegen der Minimalität von $H(a)$) $r = 0$ und damit $b = aq \in (a)$ folgt. Somit gilt auch $J \subseteq (a)$, also $J = (a)$. □

5.4.5 Folgerung. Jeder Euklidische Ring ist ein ZPE-Ring.

5.4.A Euklidischer Algorithmus

Der Euklidische Algorithmus ist ein Algorithmus zur Berechnung des ggT in Euklidischen Ringen.

Sei I Euklidischer Ring und $a, b \in I$. Für $a = b = 0$ ist $\operatorname{ggT}(a, b) = 0$. 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:

$$\begin{aligned} r_{k-2} = r_{k-1}q_k + 0 &\Rightarrow r_{k-1}|r_{k-2}, \\ r_{k-3} = r_{k-2}q_{k-1} + r_{k-1} &\Rightarrow r_{k-1}|r_{k-3}, \\ r_{k-4} = r_{k-3}q_{k-2} + r_{k-2} &\Rightarrow r_{k-1}|r_{k-4}, \\ &\vdots \\ r_1 = r_2q_3 + r_3 &\Rightarrow r_{k-1}|r_1, \\ a = r_1q_2 + r_2 &\Rightarrow r_{k-1}|a, \\ b = aq_1 + r_1 &\Rightarrow r_{k-1}|b, \end{aligned}$$

also gilt $r_{k-1}|a \wedge r_{k-1}|b$. Gilt umgekehrt $t|a \wedge t|b$, dann folgt analog: $t|r_1$, $t|r_2$, $t|r_3$, $\ldots$, $t|r_{k-1}$.

Wir haben für Hauptidealringe gezeigt: $\mathrm{ggT}(a, b) = ax + by$ mit $x, y \in I$. In Euklidischen Ringen kann man x, y berechnen:

$$\begin{aligned} \mathrm{ggT}(a,b) = r_{k-1} &= r_{k-3} + r_{k-2}(-q_{k-1}) = r_{k-3} + (r_{k-4} - r_{k-3}q_{k-2})(-q_{k-1}) = \\ &= r_{k-4}\underbrace{(-q_{k-1})}_{\in I} + r_{k-3}\underbrace{(1 + q_{k-2}q_{k-1})}_{\in I} = \ldots = ax + by. \end{aligned}$$

Kapitel 6

Körpertheorie

6.1 Quotientenkörper eines Integritätsbereiches

6.1.A Quotientenhalbgruppe

Sei $\mathfrak{M} = (M, \cdot, 1)$ ein kommutatives Monoid, dann heißt ein Element $a \in M$ *kürzbar* (*regulär*) $:\Leftrightarrow \forall x, y \in M : ax = ay \Rightarrow x = y$. $R(\mathfrak{M})$ sei die Menge aller kürzbaren Elemente von $\mathfrak{M}$. Wegen $1 \in R(\mathfrak{M})$ ist $R(\mathfrak{M}) \neq \emptyset$.

In vielen wichtigen Fällen ist $R(\mathfrak{M}) = M$.

6.1.1 Beispiele. 1) $\mathfrak{M} = (\mathbb{N}_0, +, 0)$.

2) $\mathfrak{M} = (\mathbb{Z} \setminus \{0\}, \cdot, 1)$.

3) $\mathfrak{M} = (I \setminus \{0\}, \cdot, 1)$, I Integritätsbereich.

Sei $S := M \times R(\mathfrak{M}) = \{(a, b) \mid a \in M,\ b \in R(\mathfrak{M})\}$ und $\sim$ auf S definiert durch

$$(a, b) \sim (c, d) :\Leftrightarrow ad = bc, \quad a, c \in M,\ b, d \in R(\mathfrak{M}).$$

Dann ist $\sim$ eine Äquivalenzrelation auf S (reflexiv, symmetrisch: klar; transitiv: $(a, b) \sim (c, d) \sim (e, f) \Rightarrow ad = bc \wedge cf = ed \Rightarrow adf = bcf = bed \Rightarrow af = be \Rightarrow (a, b) \sim (e, f)$).

Wir setzen $S/\sim =: S_1$, $[(a, b)]_\sim =: \frac{a}{b}$, $a \in M$, $b \in R(\mathfrak{M})$, und definieren

$$\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}, \qquad \frac{a}{b}, \frac{c}{d} \in S_1.$$

Die Operation $\cdot$ (auf S_1) ist wohldefiniert, denn: 1) $bd \in R(\mathfrak{M})$, da $b, d \in R(\mathfrak{M})$, 2) $(a, b) \sim (a_1, b_1) \wedge (c, d) \sim (c_1, d_1) \Rightarrow (ac, bd) \sim (a_1c_1, b_1d_1)$ (Übung). Weiters sei $1 := \frac{1}{1}$. Damit ist $(S_1, \cdot, 1)$ ein kommutatives Monoid.

Die Abbildung

$$\begin{cases} M \to S_1 \\ a \mapsto \frac{a}{1} \end{cases}$$

ist ein injektiver Homomorphismus (d. h., ein Monomorphismus) von $\mathfrak{M}$ in $(S_1, \cdot, 1)$. Nach dem Prinzip der isomorphen Einbettung erhalten wir damit ein kommutatives Monoid $\mathfrak{T} = (T, \cdot, 1) \cong (S_1, \cdot, 1)$, sodass $\mathfrak{M}$ Unteralgebra von $\mathfrak{T}$ ist. $\mathfrak{T}$ heißt *Quotientenhalbgruppe* von $\mathfrak{M}$ und hat folgende Eigenschaften (Übung):

a) Jedes $a \in R(\mathfrak{M})$ ist in $\mathfrak{T}$ invertierbar und hat das Inverse $a^{-1} = \frac{1}{a}$.

b) $E(\mathfrak{T}) = R(\mathfrak{T}) = \{\frac{a}{b} \mid a, b \in R(\mathfrak{M})\}$, und für $a, b \in R(\mathfrak{M})$ gilt: $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$. Dabei ist — analog zu Abschnitt 5.1 — $E(\mathfrak{T})$ definiert als die Menge der invertierbaren Elemente des Monoids $\mathfrak{T}$. (Einheitengruppe von $\mathfrak{T}$)

Für $a \in M$ setzen wir dabei $a =: \frac{a}{1} =: \frac{ae}{e}$ mit $e \in R(\mathfrak{M})$ beliebig.

Es gilt nach a):

$$T = \{ab^{-1} \mid a \in M,\ b \in R(\mathfrak{M})\}.$$

6.1.B Quotientenring, Quotientenkörper

Sei $(R, +, 0, -, \cdot, 1)$ ein kommutativer Ring mit Einselement $1 \neq 0$. Ein Element $a \in R$ heißt ein *Nullteiler* von $R :\Leftrightarrow \exists b \in R \setminus \{0\} : ab = 0$. Dann ist $\mathfrak{M} := (R, \cdot, 1)$ ein kommutatives Monoid, und es gilt

$$R(\mathfrak{M}) = \{a \in R \mid a \text{ ist } \textit{kein} \text{ Nullteiler von } R\}.$$

Mit der Bezeichnung von oben haben wir also $S_1 = \{\frac{a}{b} \mid a, b \in R,\ b \text{ kein Nullteiler}\}$ und definieren auf S_1 folgende weiteren Operationen:

$$\begin{aligned} &\tfrac{a}{b} + \tfrac{c}{d} := \tfrac{ad+bc}{bd} && a, b, c, d \in R,\ b, d \text{ keine Nullteiler},\\ &0 := \tfrac{0}{1}, \\ &-\tfrac{a}{b} := \tfrac{-a}{b} && a, b \in R,\ b \text{ kein Nullteiler}. \end{aligned}$$

Man kann zeigen, dass auch diese Operationen wohldefiniert sind (Übung).

Die Abbildung

$$\begin{cases} R \to S_1 \\ a \mapsto \frac{a}{1} \end{cases}$$

ist ein Monomorphismus von $(R, +, 0, -, \cdot, 1)$ in $(S_1, +, 0, -, \cdot, 1)$, und S_1 ist wieder ein kommutativer Ring mit Einselement. Nach dem Prinzip der isomorphen Einbettung erhalten wir damit einen kommutativen Ring mit Einselement $(T, +, 0, -, \cdot, 1) \cong (S_1, +, 0, -, \cdot, 1)$ mit folgenden Eigenschaften:

a) $(R, +, 0, -, \cdot, 1)$ ist Unteralgebra von $(T, +, 0, -, \cdot, 1)$.

b) Jedes $a \in R$, welches kein Nullteiler ist, ist in T invertierbar und hat das Inverse $a^{-1} = \frac{1}{a}$.

c) $T = \{ab^{-1} \mid a, b \in R, b \text{ kein Nullteiler}\}$.

d) In $(T, \cdot, 1)$ sind genau die Elemente $\frac{a}{b}$ invertierbar, bei denen a, b beide keine Nullteiler sind, und es gilt $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$.

Spezialfall: Ist R ein Integritätsbereich, dann ist $(T, +, 0, -, \cdot, 1)$ ein Körper, genannt der *Quotientenkörper* von R.

6.1.2 Beispiele. 1) Die Quotientenhalbgruppe von $(\mathbb{N}_0, +, 0)$ ist isomorph zu $(\mathbb{Z}, +, 0)$.

2) Der Quotientenkörper von $(\mathbb{Z}, +, 0, -, \cdot, 1)$ ist isomorph zu $(\mathbb{Q}, +, 0, -, \cdot, 1)$.

3) Ist K ein Körper, so ist der Quotientenkörper von K gleich K.

4) Der Quotientenkörper von $K[x_1, \ldots, x_n]$ (K Körper) heißt *Körper der rationalen Funktionen in $x_1, \ldots, x_n$ über K* und wird mit $K(x_1, \ldots, x_n)$ bezeichnet. Es gilt

$$K(x_1, \ldots, x_n) = \{\frac{p(x_1, \ldots, x_n)}{q(x_1, \ldots, x_n)} \mid p, q \in K[x_1, \ldots, x_n],\ q \neq 0\},$$

insbesondere

$$K(x) = \{\frac{p(x)}{q(x)} \mid p, q \in K[x],\ q \neq 0\}.$$

Der folgenden Satz zeigt, dass die Konstruktion des Quotientenkörpers kanonisch ist.

6.1.3 Satz. *Sei R Integritätsbereich, K sein Quotientenkörper. Sei L ein beliebiger Körper, der R als Unterring enthält. Dann gibt es genau einen (Ring)Homomorphismus $f : K \to L$ mit $f\restriction R = id$. Wenn $L = \langle R \rangle$ (das soll heißen: kein echter Unterkörper von L enthält R), dann ist f ein Isomorphismus.*

Beweis. Jeder Ringhomomorphismus von Körpern (der nicht konstant 0 ist), ist mit der Inversenbildung verträglich. Daher muss

$$\forall r \in R\ \forall s \in R \setminus \{0\}\ f(\frac{r}{s}) = \frac{f(r)}{f(s)}$$

gelten, daher gibt es höchstens ein solches f. Man rechnet leicht nach, dass das so definierte f wohldefiniert und Homomorphismus ist. □

Später werden wir die folgende Variante dieses Satzes brauchen:

6.1.4 Satz. *Sei R Integritätsbereich, K sein Quotientenkörper, und sei $f : R \to \tilde{R}$ ein Isomorphismus. Sei L ein beliebiger Körper, der $\tilde{R}$ als Unterring enthält. Dann gibt es genau einen (Ring)Homomorphismus $\bar{f} : K \to L$ mit $\bar{f}\restriction R = f$.*
Wiederum gilt: Wenn $L = \langle R \rangle$, dann ist f ein Isomorphismus.

6.2 Primkörper

6.2.1 Definition. Ein Körper $(K, +, 0, -, \cdot, 1)$ heißt *Primkörper*, wenn er nur sich selbst als Unterkörper besitzt.

6.2.2 Satz. *Jeder beliebige Körper besitzt stets genau einen Unterkörper, welcher Primkörper ist.*

Beweis. Sei L beliebiger Körper und $K := \bigcap\{M \subseteq L \mid M \text{ ist Unterkörper von } L\}$, d. h., K ist der kleinste Unterkörper von L. Offensichtlich ist K Primkörper. Sind $K_1, K_2 \subseteq L$ zwei Primkörper, so ist $K_1 \cap K_2$ Unterkörper von K_1 und von K_2 und daher $K_1 = K_1 \cap K_2 = K_2$. □

6.2.3 Lemma. *Sei $(R, +, 0, -, \cdot, 1)$ ein Ring mit Einselement. Dann wird durch*

$$\varphi : \mathbb{Z} \to R, \qquad n \mapsto n \cdot 1 := \begin{cases} \overbrace{1 + 1 + \cdots + 1}^{n \text{ mal}}, & n > 0, \\ 0, & n = 0, \\ \underbrace{(-1) + (-1) + \cdots + (-1)}_{|n| \text{ mal}}, & n < 0, \end{cases}$$

ein Homomorphismus von $(\mathbb{Z}, +, \cdot)$ nach $(R, +, \cdot)$ definiert.

Beweis. $\varphi(n+m) = (n+m)\cdot 1 = n\cdot 1 + m\cdot 1 = \varphi(n)+\varphi(m)$ (vgl. Potenzrechnung in Gruppen, Abschnitt 1.3); für $n, m > 0$ ist $\varphi(nm) = (nm)\cdot 1 = \underbrace{1+\cdots+1}_{nm \text{ mal}} = \underbrace{1\cdot 1+\cdots+1\cdot 1}_{nm \text{ mal}} = (\underbrace{1+\cdots+1}_{n \text{ mal}})(\underbrace{1+\cdots+1}_{m \text{ mal}}) = (n\cdot 1)(m\cdot 1) = \varphi(n)\varphi(m)$, alle anderen Fälle werden analog gezeigt. □

6.2.4 Folgerung. $\{n\cdot 1 \mid n \in \mathbb{Z}\}$ ist ein kommutativer Unterring von R mit demselben Einselement 1, nämlich der von 1 erzeugte Unterring.

6.2.5 Definition. Sei $(R, +, 0, -, \cdot, 1)$ ein Ring mit Einselement. Dann ist die *Charakteristik* von R (in Zeichen: $\operatorname{char} R$) definiert durch

$$\operatorname{char} R := \begin{cases} |\{n\cdot 1 \mid n \in \mathbb{Z}\}|, & \text{falls diese Mächtigkeit endlich ist,} \\ 0 & \text{sonst.} \end{cases}$$

Sei o(1) die Ordnung von 1 in der abelschen Gruppe $(R, +)$ (siehe Abschnitt 1.3), dann gilt:

$$\operatorname{char} R = \begin{cases} \text{o}(1), & \text{falls o}(1) \in \mathbb{N}, \\ 0, & \text{falls o}(1) = \infty. \end{cases}$$

6.2.6 Beispiele. 1) Für den Restklassenring $(\mathbb{Z}_n, +, 0, -, \cdot, 1)$ gilt $\operatorname{char} \mathbb{Z}_n = n$ $(n \in \mathbb{N}_0)$.

2) $\operatorname{char} \mathbb{Z} = \operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{R} = \operatorname{char} \mathbb{C} = 0$.

6.2.7 Lemma. *Sei $(R, +, 0, -, \cdot, 1)$ ein Ring mit Einselement. Dann gilt:*

a) $\forall n \in \mathbb{Z} : \Big(n\cdot 1 = 0 \Leftrightarrow \operatorname{char} R | n \Leftrightarrow n \in (\operatorname{char} R) \lhd \mathbb{Z}\Big)$.

b) $\forall a \in R : \Big(\operatorname{char} R \cdot a = 0$, *d. h.,* $\text{o}(a) | \operatorname{char} R\Big)$.

c) $\{n\cdot 1 \mid n \in \mathbb{Z}\} \cong \mathbb{Z}_m$, *wobei* $m := \operatorname{char} R$.

Beweis. a) Folgt aus Abschnitt 1.3.
b) Sei $m = \operatorname{char} R$. Für $m = 0$ ist die Aussage trivial. Für $m > 0$ gilt: $m\cdot a = \underbrace{a+\cdots+a}_{m \text{ mal}} = \underbrace{a\cdot 1+\cdots+a\cdot 1}_{m \text{ mal}} = a\cdot(\underbrace{1+\cdots+1}_{m \text{ mal}}) = a\cdot 0 = 0$.
c) Wir betrachten den Homomorphismus $\varphi : \mathbb{Z} \to R$, $n \mapsto n\cdot 1$. Aus dem Homomorphiesatz folgt $\varphi(\mathbb{Z}) = \{n\cdot 1 \mid n \in \mathbb{Z}\} \cong \mathbb{Z}/\ker\varphi$ und $\ker\varphi = \{n \in \mathbb{Z} \mid \varphi(n) = 0\} \overset{\text{a)}}{=} (\operatorname{char} R)$. Setzen wir $m = \operatorname{char} R$, so ist also $\varphi(\mathbb{Z}) \cong \mathbb{Z}/(m) = \mathbb{Z}_m$. □

6.2.8 Lemma. *1) Ist R Integritätsbereich, dann ist auch $\{n\cdot 1 \mid n \in \mathbb{Z}\}$ und damit $\mathbb{Z}_m$ mit $m = \operatorname{char} R$ Integritätsbereich, und es gilt $m = 0$ oder $m \in \mathbb{P}$ (d. h. m ist Primzahl).*
2) Ist R Integritätsbereich und $\operatorname{char} R \in \mathbb{P}$, dann ist $\{n\cdot 1 \mid n \in \mathbb{Z}\}$ ein Körper.

Beweis. Nach Abschnitt 5.3 gilt: $\mathbb{Z}_m = \mathbb{Z}/(m)$ Integritätsbereich $\Leftrightarrow m = 0$ oder $m \in \mathbb{P}$; $\mathbb{Z}_m$ Körper $\Leftrightarrow m \in \mathbb{P}$. □

6.2.9 Satz. *Sei $(K, +, 0, -, \cdot, 1)$ ein Körper mit $\operatorname{char} K \in \mathbb{P}$. Dann ist $\{n\cdot 1 \mid n \in \mathbb{Z}\}$ der Primkörper von K. In diesem Fall gilt also: Der Primkörper von K ist isomorph zu $\mathbb{Z}_m$ mit $m = \operatorname{char} K$.*

Beweis. Folgt unmittelbar aus dem letzten Lemma. □

6.2.10 Satz. *Sei* $(K, +, 0, -, \cdot, 1)$ *ein Körper mit* $\operatorname{char} K = 0$. *Dann ist* $\{\frac{n\cdot 1}{m\cdot 1} \mid n \in \mathbb{Z},\ m \in \mathbb{Z} \setminus \{0\}\}$ *der kleinste Unterkörper und damit der Primkörper von* K. *Dieser Primkörper ist isomorph zu* $\mathbb{Q}$. *Dabei haben wir* $\frac{n\cdot 1}{m\cdot 1} := (n \cdot 1)(m \cdot 1)^{-1}$ *gesetzt.*

Beweis. Sei L ein Unterkörper von K. Dann gilt: $1 \in L \Rightarrow \forall n \in \mathbb{Z} : n \cdot 1 \in L \Rightarrow \forall n, m \in \mathbb{Z},\ m \neq 0 : \frac{n\cdot 1}{m\cdot 1} \in L \Rightarrow P := \{\frac{n\cdot 1}{m\cdot 1} \mid n \in \mathbb{Z},\ m \in \mathbb{Z} \setminus \{0\}\} \subseteq L$.
Wir zeigen nun, dass die Abbildung $\varphi : \mathbb{Q} \to P,\ \frac{n}{m} \mapsto \frac{n\cdot 1}{m\cdot 1}$, wohldefiniert und ein Isomorphismus ist:
φ ist wohldefiniert und bijektiv: $\frac{n\cdot 1}{m\cdot 1} = \frac{p\cdot 1}{q\cdot 1} \Leftrightarrow (n\cdot 1)(m\cdot 1)^{-1} = (p\cdot 1)(q\cdot 1)^{-1} \Leftrightarrow (n\cdot 1)(q\cdot 1) = (m \cdot 1)(p \cdot 1) \Leftrightarrow (nq) \cdot 1 = (mp) \cdot 1 \Leftrightarrow nq = mp \Leftrightarrow \frac{n}{m} = \frac{p}{q}$.
φ ist ein Homomorphismus: $\varphi(\frac{n}{m} \cdot \frac{p}{q}) = \varphi(\frac{np}{mq}) = \frac{(np)\cdot 1}{(mq)\cdot 1} = \frac{(n\cdot 1)(p\cdot 1)}{(m\cdot 1)(q\cdot 1)} = \frac{(n\cdot 1)}{(m\cdot 1)} \cdot \frac{(p\cdot 1)}{(q\cdot 1)} = \varphi(\frac{n}{m})\varphi(\frac{p}{q})$; analog folgt $\varphi(\frac{n}{m} + \frac{p}{q}) = \varphi(\frac{n}{m}) + \varphi(\frac{p}{q})$. □

6.2.11 Folgerung. Bis auf Isomorphie sind alle Primkörper gegeben durch $\mathbb{Z}_p$ $(p \in \mathbb{P})$ und $\mathbb{Q}$.

6.2.12 Schreibweise. Statt $n \cdot 1$ schreiben wir meistens nur n. Der Kontext[1] entscheidet, ob etwa mit „3“ die natürliche Zahl 3 gemeint ist, oder das Ringelement $1 + 1 + 1$. Man beachte, dass die natürliche Zahl 3 verschieden von der Zahl 0 ist, aber das Ringelement $1 + 1 + 1$ durchaus gleich dem neutralen Element 0 sein kann.

6.2.13 Satz. *Sei* $(K, +, 0, -, \cdot, 1)$ *ein Körper mit* $\operatorname{char} K = p \in \mathbb{P}$. *Dann gilt für alle* $a, b \in K$: $(a + b)^p = a^p + b^p$.

Beweis. Es gilt:

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i} + a^p.$$

Für $i = 1, \ldots, p-1$ gilt $p | \binom{p}{i}$ (wegen $\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{1\cdot 2\cdots i} \in \mathbb{Z}$). Daher ist $\binom{p}{i} a^i b^{p-i} = 0$ für $1 \leq i \leq p-1$. □

6.2.14 Folgerung. Für alle $a, b \in K$ und $k \in \mathbb{N}$ gilt

$$(a \pm b)^{p^k} = a^{p^k} \pm b^{p^k}.$$

6.3 Nullstellenkörper

6.3.1 Definition. Seien K, L Körper und K Unterkörper von L. Dann heißt L ein *Oberkörper* oder *Erweiterungskörper* von K.

Problem.

> Gegeben: K Körper, $f(x) \in K[x]$, $f(x) \neq 0$, $\operatorname{grad} f(x) = n$.
> Gesucht: Erweiterungskörper L von K, in dem $f(x)$ genau n Nullstellen (gezählt mit ihren Vielfachheiten) besitzt, d. h., in dem gilt: $f(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$ mit $\alpha_i \in L$. Anders ausgedrückt: $f(x)$ zerfällt ganz in Linearfaktoren.

[1] Der Exponenten der Unbestimmten in einem Polynom wird immer als natürliche Zahl interpretiert. So ist etwa im Polynom $2x^3$ die Zahl 2 Abkürzung für $1+1$ („+“ ist hier die Ringaddition), während die Zahl 3 tatsächlich die natürliche Zahl 3 ist. Formal ist dieses Polynom ja eine Potenzreihe $0+0x+0x^2+2x^3+0x^4+\cdots$, also ganz formal die Folge $(0, 0, 0, 1+1, 0, \ldots)$; die Zahl 3 kommt hier nur als Index des Elements $1+1$ vor.

Ein solcher Körper L heißt ein *Nullstellenkörper* von $f(x)$ bezüglich K.

Sei L so ein Nullstellenkörper von $f(x)$ bezüglich K. Dann ist

$$K(\alpha_1, \ldots, \alpha_n) := \bigcap \{M \subseteq L \mid M \text{ Unterkörper von } L,\ K \subseteq M,\ \alpha_1, \ldots, \alpha_n \in M\}$$

der kleinste Unterkörper von L, der K und $\alpha_1, \ldots, \alpha_n$ enthält. $K(\alpha_1, \ldots, \alpha_n)$ heißt ein *Zerfällungskörper* von $f(x)$ bezüglich K.

Es gilt: Ist M Unterkörper von L und $K \subseteq M \subseteq K(\alpha_1, \ldots, \alpha_n)$, so ist entweder $M = K(\alpha_1, \ldots, \alpha_n)$, oder M ist — da $f(x)$ in L genau die Nullstellen $\alpha_1, \ldots, \alpha_n$ besitzt — *kein* Nullstellenkörper von $f(x)$ bezüglich K. Die Zerfällungskörper sind somit genau die minimalen Nullstellenkörper.

6.3.2 Satz (von Kronecker)**.** *Zu jedem $f(x) \in K[x]$, $f(x) \neq 0$, gibt es einen Nullstellenkörper, also auch einen Zerfällungskörper von $f(x)$ bezüglich K.*

Den Beweis dieses Satzes führen wir in 4 Schritten (Lemma 6.3.3–6.3.7) durch:

6.3.3 Lemma. *Sei $p(x) \in K[x]$, $p(x)$ irreduzibel,* $\operatorname{grad} p(x) = k$, *$I := (p(x)) = \{p(x)q(x) \mid q(x) \in K[x]\}$, dann ist der Restklassenring $K[x]/I$ ein Körper, und es gilt:*

$$\begin{aligned} K[x]/I &= \{b_0 + b_1 x + \cdots + b_{k-1}x^{k-1} + I \mid b_i \in K\} = \\ &= \{g(x) + I \mid g(x) = 0 \vee \operatorname{grad} g(x) < k\}. \end{aligned}$$

Weiters gilt: $g_1(x) + I = g_2(x) + I$ mit $g_i(x) = 0 \vee \operatorname{grad} g_i(x) < k \Rightarrow g_1(x) = g_2(x)$.

Beweis. Wir wissen aus Folgerung 5.3.10, dass $K[x]/I$ ein Körper ist.
$h(x) + I \in K[x]/I \Rightarrow h(x) = q(x)p(x) + r(x)$ mit $r(x) = 0 \vee \operatorname{grad} r(x) < \operatorname{grad} p(x) = k$ $\Rightarrow h(x) + I = r(x) + I$. Ist $g_1(x) + I = g_2(x) + I$ mit $g_i(x) = 0 \vee \operatorname{grad} g_i(x) < k$, so gilt $g_1(x) - g_2(x) \in I$ und damit $g_1(x) = g_2(x)$. □

6.3.4 Lemma. *Sei $p(x) \in K[x]$, $p(x)$ irreduzibel mit $k := \operatorname{grad}(p) \geq 1$. Dann gibt es einen Erweiterungskörper $L \supseteq K$, sodass ein $\alpha \in L$ mit $p(\alpha) = 0$ existiert.*

Beweis. Sei y eine neue Variable. Wegen Lemma 6.3.3 ist $K[y]/(p(y))$ Körper, und die Abbildung $\varphi : K \to K[y]/(p(y))$, $a \mapsto a + (p(y))$ ist ein injektiver Homomorphismus. Nach dem Prinzip der isomorphen Einbettung identifizieren wir K mit seinem Bild $\varphi(K) \subseteq K[y]/(p(y))$, somit ist $L := (K[y]/(p(y))$ ein Oberkörper von K.
Sei $k := \operatorname{grad} p(x)$.
Fall 1: Sei $k = 1$. Dann gilt $L = K$, und in K gibt es schon eine Nullstelle von $p(x)$.
Fall 2: Sei $k > 1$ und $(p(y)) =: I$. Dann ist $\alpha := y + I$ Nullstelle des Polynoms $p(x) \in K[x] \subseteq L[x]$, denn:
Sei $p(x) = a_0 + a_1 x + \cdots + a_k x^k$. In $K[y]/I$ gilt: $p(y+I) = (a_0+I) + (a_1+I)(y+I) + \cdots + (a_k + I)(y+I)^k = a_0 + a_1 y + \cdots + a_k y^k + I = p(y) + I = I$, also $p(\alpha) = a_0 + a_1\alpha + \cdots + a_k\alpha^k = 0$. □

6.3.5 Anmerkung. Nach Lemma 6.3.3 ist $L = \{b_0 + b_1\alpha + \cdots + b_{k-1}\alpha^{k-1} \mid b_i \in K\}$.

6.3.6 Lemma. *Zu jedem $f(x) \in K[x]$, $f(x) \neq 0$, $\operatorname{grad} f(x) = n \in \mathbb{N}$, gibt es einen Oberkörper $L \supseteq K$, sodass ein $\alpha \in L$ mit $f(\alpha) = 0$ existiert.*

Beweis. Sei $f(x) = p(x)q(x)$, wobei $p(x)$ irreduzibel ist. Nach Lemma 6.3.4 gibt es dann einen Oberkörper L von K, sodass ein $\alpha \in L$ mit $p(\alpha) = 0$ existiert. Für dieses α gilt dann auch $f(\alpha) = p(\alpha)q(\alpha) = 0$. □

6.3.7 Lemma. *Zu jedem $f(x) \in K[x]$, $f(x) \neq 0$, $\operatorname{grad} f(x) = n \in \mathbb{N}$, gibt es einen Oberkörper $L \supseteq K$, sodass in $L[x]$ gilt: $f(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$ mit $\alpha_1, \ldots, \alpha_n \in L$.*

Beweis. Induktion nach n: Für $n = 1$ kann $L = K$ gewählt werden.
Sei $\operatorname{grad} f(x) = n+1$. Nach Lemma 6.3.6 gibt es $L^* \supseteq K$ und $\alpha \in L^*$ mit $f(\alpha) = 0$. In $L^*[x]$ gilt daher $f(x) = (x-\alpha)f_1(x)$ mit $\operatorname{grad} f_1(x) = n$. Nach Induktionsvoraussetzung gibt es $L \supseteq L^*$, sodass in $L[x]$ gilt: $f_1(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$ mit $\alpha_1, \ldots, \alpha_n \in L$. Dann gilt in $L[x]$ auch $f(x) = (x-\alpha)f_1(x) = c(x-\alpha)(x-\alpha_1)\cdots(x-\alpha_n)$. □

Der Begriff des Zerfällungskörpers kann auf beliebige Mengen von Polynomen verallgemeinert werden:

6.3.8 Definition. Seien $K \leq L$ Körper, $P \subseteq K[x]$ eine Menge von Polynomen. L heißt „Nullstellenkörper“ für P (über K), wenn jedes Polynom $p(x) \in P$ im Ring $L[x]$ in Linearfaktoren zerfällt. L heißt „Zerfällungskörper“ für P über K, wenn L minimaler Nullstellenkörper ist, d.h., wenn L Nullstellenkörper ist aber wenn es keinen echten Unterkörper von L gibt, der Nullstellenkörper ist.

Ohne Beweis geben wir den folgenden Satz an:

6.3.9 Satz. *Sei K Körper, $P \subseteq K[x]$. Dann gibt es einen Zerfällungskörper L von P, und L ist im Wesentlichen eindeutig.*
(Genauer: Wenn L_1, L_2 Zerfällungskörper für P über K sind, dann gibt es einen Isomorphismus $f : L_1 \to L_2$ mit $f \restriction K = id$.)

Für den Beweis verwendet man den Satz von Kronecker und das Zornsche Lemma (oder eine Wohlordnung von $K[x]$).

6.4 Erweiterungskörper

Ist L Oberkörper von K, dann ist L auch Vektorraum über K mit den Operationen

$$\begin{aligned} a+b &\ldots \text{Summe in } L \ (a, b \in L), \\ \lambda a &\ldots \text{Produkt in } L \ (a \in L, \lambda \in K). \end{aligned}$$

Es existiert daher eine Vektorraumbasis von L über K. Diese bestimmt die Dimension $\dim_K L =: [L : K]$, den so genannten *Grad der Körpererweiterung L von K*. Ist $[L : K] < \infty$, so heißt L eine *endliche Erweiterung von K*.

6.4.1 Anmerkungen. 1) $[L : K] = 1 \Leftrightarrow L = K$.

2) In Lemma 6.3.4 gilt $L = \{b_0 + b_1\alpha + \cdots + b_{k-1}\alpha^{k-1} \mid b_i \in K\}$, und $\{1, \alpha, \ldots, \alpha^{k-1}\}$ ist eine Basis von L über K. Also gilt $[L : K] = k$.

3) Wenn $K \leq E \leq L$, dann ist $[L : K] \leq [L : E]$, weil jedes Erzeugendensystem des K-Vektorraums L auch den E-Vektorraum L erzeugt. Überdies ist $[E : K] \leq [L : K]$, weil E Untervektoraum des K-Vektorraums L ist.

6.4.2 Satz (Gradsatz)**.** *Ist L Oberkörper von K, E Oberkörper von L und $[E : K] < \infty$, so gilt:*

$$[E : K] = [E : L] \cdot [L : K].$$

Beweis. Übungsbeispiel. (Man zeigt: Ist $\{a_1, \ldots, a_m\}$ eine Basis des Vektorraumes L über K und $\{b_1, \ldots, b_n\}$ eine Basis des Vektorraumes E über L, so ist $\{a_i b_j \mid i = 1, \ldots, m, \ j = 1, \ldots, n\}$ eine Basis des Vektorraumes E über K.) □

6.4.3 Definition. Seien $K \leq L$ Körper, und sei $\alpha \in L$. Sei $\varphi_\alpha : K \to L$ der in 4.2.1, 4.2.2 definierte Einsetzungshomomorphismus, der jedem Polynom $a_0 + a_1 x + \cdots + a_n x^n$ das Körperelement $a_0 + a_1\alpha + \cdots + a_n\alpha^n$ zuordnet. Die Wertemenge von φ_α bezeichnen wir mit $K[\alpha]$.

Offenbar ist $K[\alpha]$ der kleinste Unterring von L, der $K \cup \{\alpha\}$ enthält.
Aus dem Homomorphiesatz für Ringe wissen wir, dass der Kern des Einsetzungshomomorphismus ein Ideal von $K[x]$ ist, und dass $K[\alpha] \cong K[x]/\ker(\varphi_\alpha)$. Wir untersuchen also den Kern von φ_α:

6.4.4 Definition. Sei L Oberkörper von K und $\alpha \in L$.

- α heißt *algebraisch* über $K :\Leftrightarrow \exists f(x) \in K[x] \setminus \{0\} : f(\alpha) = 0$.
- α heißt *transzendent* über $K :\Leftrightarrow \nexists f(x) \in K[x] \setminus \{0\} : f(\alpha) = 0$.

Mit anderen Worten: α ist transzendent über K, wenn $\ker(\varphi_\alpha) = \{0\}$, und algebraisch, wenn $\ker(\varphi_\alpha) \neq \{0\}$.

6.4.5 Beispiele. 1) $\sqrt{2}$ ist algebraisch über $\mathbb{Q}$ ($f(x) = x^2 - 2$, $L = \mathbb{R}$).

2) $\sqrt[3]{3}$ ist algebraisch über $\mathbb{Q}$ ($f(x) = x^3 - 3$, $L = \mathbb{R}$).

3) i ist algebraisch über $\mathbb{R}$ ($f(x) = x^2 + 1$, $L = \mathbb{C}$).

4) e, π sind transzendent über $\mathbb{Q}$ (ohne Beweis).

6.4.6 Definition. 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 $S = \{u_1, \ldots, u_r\}$ endlich, so schreiben wir $K(S) =: K(u_1, \ldots, u_r)$. Ist insbesondere $S = \{\alpha\}$ einelementig, so schreiben wir $K(S) =: K(\alpha)$ („einfache Erweiterung von K“).

6.4.7 Definition. Sei K Körper. Den Quotientenkörper des Polynomrings $K[x]$ bezeichnen wir mit $K(x)$.

6.4.8 Anmerkung. Wir verwenden die Schreibweise $K(\cdot)$ für zwei scheinbar verschiedene Operationen. Tatsächlich ergibt sich aber, dass die zweite ein Speziallfall der ersten 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 $K[x]$; jedes Element aus $K\langle x\rangle$ lässt sich als Quotient $p(x)/q(x)$ mit $p(x) \in K[x]$, $q(x) \in K[x]$, $q(x) \neq 0$ 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.

Daher ist die Schreibweise $K(x)$ an Stelle von $K\langle x\rangle$ gerechtfertigt.

6.4.9 Satz (Einfache transzendente Erweiterungen)**.** *Sei $K \leq L$, $\alpha \in L$ transzendent über K. Dann ist $K(\alpha) \cong K(x)$ (wobei $K(x)$ wieder der Quotientenkörper des Polynomrings $K[x]$ ist). Es gibt einen (einzigen) Isomorphismus $\varphi : K(x) \to K(\alpha)$, der auf K die Identität ist, und x auf α abbildet.*
Insbesondere gilt: Seien α, β beide transzendent über K, dann ist $K(\alpha) \cong K(\beta)$, mit einem Isomorphismus, der α auf β abbildet.

Beweis. Da α transzendent über K ist, ist der Einsetzungshomomorphismus $\varphi_\alpha : K[x] \to K[\alpha]$ ein Ringisomorphismus. Nach Satz 6.1.4 lässt sich φ_α zu einem Körperisomorphismus $\bar{\varphi} : K(x) \to K(\alpha)$ fortsetzen. □

6.4.10 Anmerkung. Sei α transzendent über K. Dann ist der Körpergrad $[K(\alpha) : K]$ unendlich, denn die Potenzen α^n sind linear unabhängig über K.
Wenn K endlich ist, dann ist $K(\alpha)$ abzählbar unendlich und hat daher abzählbar unendliche Dimension über K. Wenn K unendlich ist, so kann in $K(\alpha)$ eine über K linear unabhängige Menge finden, die gleichmächtig mit K ist, zum Beispiel $\{\frac{1}{q-\alpha} \mid q \in K\}$. Daraus kann man schließen, dass die Dimension von $K(\alpha)$ über K genau die Kardinalität von K ist, d.h., dass es eine Basis des K-Vektorraumes $K(\alpha)$ gibt, die zu K gleichmächtig ist.

Jedes Ideal in $K[x]$ ist Hauptideal, also von der Form $(p(x))$ mit einem „Erzeuger“ $p(x) \in K[x]$. Offenbar gibt es (wenn $I \neq \{0\}$) genau einen normierten Erzeuger.

6.4.11 Definition. Sei α algebraisch über K, und sei $I \subseteq K[x]$ der Kern des Einsetzungshomomorphismus, also $I := \{p(x) \in K[x] \mid p(\alpha) = 0\}$. Sei $m(x)$ normierter Erzeuger von I, dann heißt $m(x)$ „Minimalpolynom“ von α über K.

6.4.12 Beispiele. 1) Für $\alpha \in K$ ist $x - \alpha$ Minimalpolynom von α bezüglich K.

2) $x^2 - 2$ ist Minimalpolynom von $\sqrt{2}$ bezüglich $\mathbb{Q}$.

3) $x^3 - 3$ ist Minimalpolynom von $\sqrt[3]{3}$ bezüglich $\mathbb{Q}$.

4) $x^2 + 1$ ist Minimalpolynom von i bezüglich $\mathbb{R}$.

5) Sei $\alpha := \frac{\sqrt{2}}{2}(1 + i)$. Dann ist $\alpha^2 = i$, $\alpha^4 = -1$. Das Minimalpolynom von α über $\mathbb{R}$ ist $x^2 - \sqrt{2}x + 1$, über $\mathbb{Q}$ ist es $x^4 + 1$.

6) Das Minimalpolynom von π über $\mathbb{Q}(\pi^2)$ ist $x^2 - \pi^2$, über $\mathbb{Q}(\pi)$ ist es $x - \pi$, und über $\mathbb{Q}$ hat π kein Minimalpolynom.

Es gilt: $[K(\alpha) : K] = \operatorname{grad} p(x)$, wobei $p(x)$ das Minimalpolynom von α bezüglich K ist. Eine Basis von $K(\alpha)$ (als Vektorraum über K gesehen) ist dann gegeben durch $\{1, \alpha, \ldots, \alpha^{k-1}\}$ mit $k = \operatorname{grad} p(x)$.

6.4.13 Lemma. *Sei α algebraisch über K, $m(x) \in K[x]$ das Minimalpolynom von α über K. Dann ist $m(x)$ in $K[x]$ irreduzibel.*
Sei umgekehrt $p(x) \in K[x]$ ein irreduzibles normiertes Polynom mit $p(\alpha) = 0$, dann muss $p(x) = m(x)$ sein.

Beweis. Nach dem Homomorphiesatz ist $K[\alpha] \cong K[x]/(m(x))$. Da $K[\alpha]$ Integritätsbereich ist, ist das Ideal $(m(x))$ ein Primideal, daher ist $m(x)$ prim und irreduzibel.
Wenn $p(\alpha) = 0$ ist, dann gilt $m(x)|p(x)$. Wenn aber p irreduzibel ist, muss $m(x) \sim p(x)$ gelten. Da $m(x)$ und $p(x)$ beide normiert sind, schließen wir $m(x) = p(x)$. □

6.4.14 Satz (Einfache algebraische Erweiterungen)**.** *Sei $K \leq L$, $\alpha \in L$ algebraisch über K. Sei $m(x)$ das Minimalpolynom von α über K, $k = \operatorname{grad} m(x)$. Dann gilt:*

(a) $K[\alpha] \simeq K[x]/I$, wobei I das von $m(x)$ erzeugte Ideal in $K[x]$ ist. Es gibt einen Isomorphismus, der auf K die Identität ist, und der α auf die Nebenklasse $x + I$ abbildet.

(b) $K(\alpha) = K[\alpha]$.

(c) 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.

(d) $[K(\alpha) : K] = n$.

Insbesondere gilt:

(e) Wenn $\alpha, \beta \in L$ *dasselbe Minimalpolynom* $m(x)$ *über* K *haben, dann gibt es einen Isomorphismus* $\varphi : K(\alpha) \to K(\beta)$ *mit* $\varphi(\alpha) = \beta$, $\varphi \restriction K = id$.

Beweis. (a) Sei $\varphi : K[x] \to K[\alpha]$ der Einsetzungshomomorphismus, $j : K[x] \to K[x]/I$ die kanonische Abbildung $p \mapsto p + I$. Der Homomorphiesatz liefert einen Isomorphismus $h : K[\alpha] \to K[x]/I$ mit $k \circ \varphi_\alpha = j$. Insbesondere ist $x + I = j(x) = k(\varphi_\alpha(x)) = k(\alpha)$. Die Abbildung j ist injektiv auf $K \subseteq K[x]$; wir identifizieren alle $b \in K$ mit $j(b)$. Dann gilt $b = j(b) = k(\varphi_\alpha(b)) = k(b)$.

(b) $K[x]/I$ ist ein Körper wegen 6.3.3. Wegen (a) ist also auch $K[\alpha]$ ein Körper. Also $K[\alpha] = K(\alpha)$.

(c) Siehe 6.3.3.

(d) Aus (c) folgt, dass $1, \alpha, \ldots, \alpha^{k-1}$ eine Basis von des K-Vektorraums $K[\alpha]$ ist.

□

6.4.15 Satz. *Sei* $K \leq L$, *und seien* $\alpha_1, \ldots, \alpha_n, \beta \in L$. *Wenn* $\alpha_1, \ldots, \alpha_n$ *algebraisch über* K *sind, und* β *algebraisch über* $K(\alpha_1, \ldots, \alpha_n)$, *dann ist* β *algebraisch über* K.

Beweis. Die Erweiterungsgrade

$$[K(\alpha_1, \ldots, \alpha_n, \beta) : K(\alpha_1, \ldots, \alpha_n)],\ [K(\alpha_1, \ldots, \alpha_n) : K(\alpha_1, \ldots, \alpha_{n-1})],\ \ldots,\ [K(\alpha_1) : K]$$

sind alle endlich. Durch wiederholte Anwendung des Gradsatzes schließen wir, dass der K-Vektorraum $K(\alpha_1, \ldots, \alpha_n, \beta)$ und sein Unterraum $K(\beta)$ endliche Dimension haben. Wenn nun $[K(\beta) : K] = n$ ist, dann sind $\{1, \beta, \ldots, \beta^n\}$ über K linear abhängig, und wir erhalten ein Polynom $p(x) \in K[x] \setminus \{0\}$ mit Nullstelle β. □

6.4.16 Lemma. *Sei* K *ein Körper mit* $\operatorname{char} K = 0$ *und* $f(x) \in K[x]$ *irreduzibel,* L *ein Erweiterungskörper von* K *und* α *Nullstelle von* $f(x)$ *in* L, *dann ist* α *eine einfache Nullstelle.*

Beweis. Wäre α eine mehrfache Nullstelle, so wäre α auch Nullstelle von $f'(x)$ (siehe Übungen), also wäre in $L[x]$

$$\operatorname{grad} \operatorname{ggT}(f(x), f'(x)) \geq 1.$$

Nun ist aber — nach dem Euklidischen Algorithmus — der ggT von $f(x)$ und $f'(x)$ in $K[x]$ derselbe wie in $L[x]$. Da $f(x)$ in $K[x]$ irreduzibel ist, muss daher $\operatorname{ggT}(f(x), f'(x)) = f(x)$ gelten. Also muss $f'(x) = 0$ sein (sonst wäre ja $\operatorname{grad} f'(x) \geq \operatorname{grad} f(x)$). Ist $f(x) = \sum_{i=0}^{n} a_i x^i$, so gilt $f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$, also muss $i a_i = 0$ sein für $i = 1, \ldots, n$. Wegen $\operatorname{char} K = 0$ folgt daraus $a_i = 0$ für $i = 1, \ldots, n$, also $f(x) = a_0$, Widerspruch! □

6.4.17 Satz (Satz vom primitiven Element)**.** *Ist* L *Oberkörper von* K *mit* $\operatorname{char} K = 0$ *(also auch* $\operatorname{char} L = 0$*), und sind* $u_1, \ldots, u_r \in L$ *alle algebraisch über* K, *so gibt es ein* $\alpha \in L$ *mit* $K(u_1, \ldots, u_r) = K(\alpha)$.

Beweis. Induktion nach r. Für $r = 1$ ist die Aussage trivial.
Annahme: Die Aussage stimmt für $r - 1$ $(r > 1)$. Wir haben dann: $K(u_1, \ldots, u_r) = K(u_1, \ldots, u_{r-1})(u_r) = K(\alpha)(u_r) = K(\alpha, \beta)$ für ein geeignetes $\alpha \in L$ und für $\beta = u_r$. Wegen $[K(\alpha, \beta) : K] < \infty$ sind α, β algebraisch über K. Wir zeigen: $\exists \delta \in L$ mit $K(\alpha, \beta) = K(\delta)$.

Seien $f(x)$ bzw. $g(x)$ die Minimalpolynome von α bzw. β. Wir betrachten einen Erweiterungskörper M von K, der zugleich Nullstellenkörper von $f(x)$ und $g(x)$ ist, d. h., $\exists \alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_t \in M$ 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 dem vorhergehenden Lemma 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

$$K(\alpha, \beta) = K(\delta) \text{ mit } \delta := \alpha + c\beta.$$

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 β 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 $\alpha = \delta - c\beta \in K(\delta)$. □

6.5 Zerfällungskörper

Gemäß Abschnitt 6.3 ist ein minimaler Nullstellenkörper von $f(x) \in K[x]$ mit $f(x) \neq 0$ ein Zerfällungskörper von $f(x)$ bezüglich K.

Die Existenz wurde bereits in Abschnitt 6.3 gezeigt: Ist L Nullstellenkörper von $f(x)$ bezüglich K, dann gilt $f(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$ mit $c \in K$, $\alpha_1, \ldots, \alpha_n \in L$, und $K(\alpha_1, \ldots, \alpha_n)$ ist ein Zerfällungskörper von $f(x)$ bezüglich K.

6.5.1 Definition. Sei $K_1 \cong K_2$ (K_1, K_2 Körper), $\varphi : K_1 \to K_2$ Isomorphismus und L_i Erweiterungskörper von K_i, $i = 1, 2$. Dann heißen L_1, L_2 *äquivalent* bezüglich $\varphi :\Leftrightarrow$ Es gibt einen Isomorphismus $\bar{\varphi} : L_1 \to L_2$ mit $\bar{\varphi}\restriction K_1 = \varphi$.
Spezialfall: $K_1 = K_2 = K$, $\varphi = \mathrm{id}_K$. In diesem Fall sind L_1, L_2 äquivalent bezüglich $\varphi \Leftrightarrow$ es gibt einen Isomorphismus $\psi : L_1 \to L_2$ mit $\psi(a) = a$ für alle $a \in K$. Solche Erweiterungskörper L_1, L_2 heißen *äquivalent* bezüglich K.

6.5.2 Anmerkung. „äquivalent bezüglich K“ ist eine Äquivalenzrelation.

6.5.3 Lemma. *Sind R, S kommutative Ringe mit Einselement und ist $\varphi : R \to S$ Homomorphismus, so gibt es* genau einen *Homomorphismus von $R[x] \to S[x]$, der φ fortsetzt und x auf x abbildet. Wir bezeichnen diesen Homomorphismus mit $\varphi_{[x]}$ und nennen $\varphi_{[x]}$ die „natürliche Fortsetzung“ von φ.*
Ist φ Isomorphismus, so auch $\varphi_{[x]}$.

Beweis. $\varphi_{[x]}$ ist gegeben durch die Zuordnung

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \mapsto \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n.$$

Die angegebenen Eigenschaften von $\varphi_{[x]}$ rechnet man leicht nach. □

6.5.4 Satz. *Sei Z ein Zerfällungskörper von $f(x) \in K[x]$ bezüglich K und Z_1 äquivalent zu Z bezüglich K. Dann ist auch Z_1 ein Zerfällungskörper von $f(x) \in K[x]$ bezüglich K.*

Beweis. In $Z[x]$ gilt: $f(x) = c(x-\alpha_1)^{k_1}\cdots(x-\alpha_r)^{k_r}$ mit $c \in K$, $\alpha_1, \ldots, \alpha_r \in Z$. Sei $\varphi : Z \to Z_1$ ein Isomorphismus mit $\varphi(a) = a$ für alle $a \in K$ und $\varphi_{[x]} : Z[x] \to Z_1[x]$ die Fortsetzung von φ nach obigem Lemma. Dann ist $\varphi_{[x]}$ Isomorphismus und $\varphi_{[x]}(f(x)) = c(x-\varphi(\alpha_1))^{k_1}\cdots(x-\varphi(\alpha_r))^{k_r} = f(x)$, da ja $\varphi_{[x]}\restriction K[x] = \mathrm{id}$. Somit ist Z_1 Nullstellenkörper.

Ist U Unterkörper von Z_1 mit $U \supseteq K \cup \{\varphi(\alpha_1), \ldots, \varphi(\alpha_r)\}$, so ist $\varphi^{-1}(U) \supseteq K \cup \{\alpha_1, \ldots, \alpha_r\}$, $\varphi^{-1}(U) \subseteq Z$ und $\varphi^{-1}(U)$ Unterkörper von Z. Wegen $Z = K(\alpha_1, \ldots, \alpha_r)$ ist $Z = \varphi^{-1}(U)$ und damit $Z_1 = U$. □

Wir wollen nun zeigen (siehe 6.5.11), dass je zwei Zerfällungskörper Z_1, Z_2 desselben Polynoms (oder derselben Menge von Polynomen) in $K[x]$ äquivalent bezüglich K sind.
Das folgende Lemma ist eine Verallgemeinerung von 6.4.14(e):

6.5.5 Lemma. *Sei $\varphi : K \to \tilde{K}$ Isomorphismus. Sei α algebraisch über K mit Minimalpolynom $m(x)$, und sei $\tilde{\alpha}$ algebraisch über $\tilde{K}$ mit Minimalpolynom $\tilde{m}(x)$, wobei $\tilde{m}(x) = \varphi_{[x]}(m(x))$ (vergleiche 6.5.3). Wenn $\varphi_{[x]}(m(x)) = \tilde{m}(x)$, dann gibt es einen Isomorphismus $\bar{\varphi} : K(\alpha) \cong K(\tilde{\alpha})$, der φ fortsetzt und $\bar{\varphi}(\alpha) = \tilde{\alpha}$ erfüllt.*

Beweis. Nach 6.4.14 wissen wir, dass es einen Isomorphismus $\iota : K(\alpha) \to K[x]/I$ gibt (wobei I das von $m(x)$ erzeugte Ideal in $K[x]$ ist), der K fest lässt und α auf die Nebenklasse $x + I$ abbildet.
Ebenso gibt es einen Isomorphismus $\tilde{\iota} : \tilde{K}(\tilde{\alpha}) \to \tilde{K}[x]/\tilde{I}$, wobei $\tilde{I}$ das von $\tilde{m}(x)$ erzeugte Ideal in $\tilde{K}[x]$ ist, und $\tilde{\iota}(\tilde{\alpha}) = x + \tilde{I}$.
Der Isomorphismus $\varphi_{[x]}$ bildet $K[x]$ auf $K^*[x]$ und I auf I^* ab (wobei $\varphi_{[x]}(x) = x$ gilt) und vermittelt daher einen Isomorphismus von $K[x]/I$ nach $\tilde{K}[x]/\tilde{I}$.
Insgesamt erhalten wir die folgenden Kette von Isomorphismen:

$$K(\alpha) \xrightarrow{\ \iota\ } K[x]/I \xrightarrow{\ \varphi_{[x]}\ } \tilde{K}[x]/\tilde{I} \xrightarrow{\ \tilde{\iota}^{-1}\ } \tilde{K}(\tilde{\alpha}),$$

wobei der erste und der dritte Isomorphismus die Identität auf K bzw $\tilde{K}$ induzieren, und der mittlere Isomorphismus den Isomorphismus φ fortsetzt. □

6.5.6 Lemma. *Sei $\varphi : K \to \tilde{K}$ ein Körperisomorphismus; seien $E, \tilde{E}$ Körper mit $K \leq E$, $\tilde{K} \leq \tilde{E}$. Sei $p(x) \in K[x]$, $\alpha \in E$, $p(\alpha) = 0$. Mit $\tilde{p}(x)$ bezeichnen wir das Bild von $p(x)$ unter der natürlichen Fortsetzung von $\varphi : K \to \tilde{K}$ zu $\varphi_{[x]} : K[x] \to \tilde{K}[x]$.*
Wenn $\tilde{p}(x)$ in $\tilde{E}$ in Linearfaktoren zerfällt, dann gibt es ein $\tilde{\alpha} \in \tilde{E}$, sodass sich φ zu einem Isomorphismus $\bar{\varphi} : K(\alpha) \to \tilde{K}(\tilde{\alpha})$ fortsetzen lässt.

Beweis. Sei $p(x) = p_1(x) \cdot p_2(x) \cdots$ Produkt von irreduziblen Faktoren $p_i(x) \in K[x]$, dann ist α Nullstelle eines Faktors, sagen wir $p_1(\alpha) = 0$. Sei $\tilde{p}_i := \varphi_{[x]}(p_i)$, dann sind die Polynome $\tilde{p}_i(x) \in \tilde{K}[x]$ irreduzibel (siehe Lemma 6.5.3), und es gilt $\tilde{p}(x) = \tilde{p}_1(x) \cdot \tilde{p}_2(x) \cdots$.
Da E Nullstellenkörper von $\tilde{p}(x)$ ist, zerfällt $\tilde{p}_1(x)$ in E in Linearfaktoren. Sei nun $\tilde{\alpha} \in \tilde{E}$ eine beliebige Nullstelle des irreduziblen Polynoms $\tilde{p}_1(x)$. Dann können wir nach Lemma 6.5.5 einen Isomorphismus $\bar{\varphi} : K(\alpha) \to \tilde{K}(\tilde{\alpha})$ mit $\bar{\varphi}(\alpha) = \tilde{\alpha}$ finden, der φ fortsetzt. □

6.5.7 Lemma. *Seien $K \leq E$, $\tilde{K} \leq \tilde{E}$ Körper, $\varphi : K \to \tilde{K}$ ein Isomorphismus. Sei $p(x) \in K[x]$, $\tilde{p}(x) := \varphi_{[x]}(p(x))$ das entsprechende Polynom in $\tilde{K}[x]$. Dann gilt:*

(a) Wenn E ein Zerfällungskörper von $p(x)$ über K ist, und $\tilde{E}$ ein Nullstellenkörper von $\tilde{p}(x)$, dann lässt sich φ zu einem Monomorphismus $\bar{\varphi} : E \to \tilde{E}$ fortsetzen.

(b) Wenn überdies $\tilde{E}$ Zerfällungskörper von $\tilde{p}(x)$ über $\tilde{K}$ ist, dann ist $\bar{\varphi}$ ein Isomorphismus zwischen E und $\tilde{E}$.

Beweis von (a). Seien $\alpha_1, \ldots, \alpha_n$ die Nullstellen von $p(x)$ in E, dann ist $E = K(\alpha_1, \ldots, \alpha_n)$. Wir werden Elemente $\tilde{\alpha}_1, \ldots, \tilde{\alpha}_n \in \tilde{E}$ sowie eine aufsteigende Kette $\varphi = \varphi_0 \subseteq \varphi_1 \subseteq \cdots \subseteq \varphi_n$ finden, sodass $\varphi_k : K(\alpha_1, \ldots, \alpha_k) \to \tilde{K}(\tilde{\alpha}_1, \ldots, \tilde{\alpha}_k)$ ein Isomorphismus mit $\varphi_k(\alpha_i) = \tilde{\alpha}_i$ für $1 \leq i \leq k$ ist. Die Abbildung φ_n ist dann der gewünschte Monomorphismus $\bar{\varphi}$, der $E = K(\alpha_1, \ldots, \alpha_n)$ auf $K(\bar{\alpha}_1, \ldots, \bar{\alpha}_n) \subseteq \tilde{E}$ abbildet.
$\varphi = \varphi_0$ ist bereits gegeben. Wenn wir φ_k bereits kennen, können wir das vorige Lemma auf das Polynom $p(x)$ mit der Nullstelle α_{k+1} (und den Körper $K(\alpha_1, \ldots, \alpha_k)$) anwenden und erhalten $\tilde{\alpha}_{k+1}$ und φ_{k+1}. □

Beweis von (b). Da $p(x)$ in E bereits in Linearfaktoren zerfällt, zerfällt auch $\tilde{p}(x)$ in $\bar{\varphi}(E) \subseteq \tilde{E}$ in Linearfaktoren. Daher ist $\bar{\varphi}(E)$ bereits Nullstellenkörper für $\tilde{p}(x)$, also muss $\bar{\varphi}(E) = \tilde{E}$ sein. □

6.5.8 Anmerkung. Im Beweis von 6.5.6 bzw. 6.5.7(a) sieht man, dass die Fortsetzung $\bar{\varphi}$ von φ im Allgemeinen nicht eindeutig ist, denn als Bild $\tilde{\alpha} = \varphi(\alpha)$ kann man eine beliebige Nullstelle des irreduziblen Polynoms $\tilde{p}_1(x)$ wählen.

6.5.9 Anmerkung. Sei $p(x)$ in $K(x)$ irreduzibel ist, und seien α, β, γ Nullstellen von $p(x)$ in einem Nullstellenkörper E (wobei wir hier nicht annehmen, dass α, β, γ verschieden sind). Es gibt einen Monomorphismus $\varphi : K(\alpha) \to E$ mit $\varphi \restriction K = id$, $\varphi(\alpha) = \beta$; φ ist Isomorphismus zwischen $K(\alpha)$ und $K(\beta)$.
Nach dem bereits Bewiesenen gibt es eine Fortsetzung $\varphi' : K(\alpha, \gamma) \to E$. Um eine solche Fortsetzung zu finden, muss man $p(x)$ in $K(\alpha)[x]$ in irreduzible Faktoren zerlegen; einer dieser Faktoren hat dann die Nullstelle γ, und γ kann dann auf eine beliebige andere Nullstelle dieses Faktors abgebildet werden. Über den Grad dieses Faktors, und somit über die Anzahl der möglichen Fortsetzungen, wissen wir nur, dass er kleiner als der Grad von $p(x)$ sein muss. Es kann durchaus der Fall eintreten, dass γ bereits in $K(\alpha)$ liegt, dann ist $\varphi(\gamma)$ bereits definiert und es muss $\varphi' = \varphi$ gelten.

6.5.10 Lemma. *Seien $K \leq E$, $\tilde{K} \leq \tilde{E}$ Körper, $\varphi : K \to \tilde{K}$ ein Isomorphismus. Sei $\mathscr{P} \subseteq K[x]$ eine Menge von Polynomen, $\tilde{\mathscr{P}} := \varphi_{[x]}(\mathscr{P})$. Dann gilt:*
Wenn $E, \tilde{E}$ Zerfällungskörper von $\mathscr{P}$ bzw. $\tilde{\mathscr{P}}$ über K bzw $\tilde{K}$ sind, dann lässt sich φ zu einem Isomorphismus $\bar{\varphi} : E \to \tilde{E}$ fortsetzen.

Beweis. Betrachten wir zunächst den Fall, dass $\mathscr{P} = \{p_0(x), p_1(x), \ldots\}$ abzählbar ist. Sei $K_0 := K$, und sei K_{n+1} der Zerfällungskörper von $p_n(x)$ über K_n. Mit Hilfe des vorigen Lemmas erhalten wir eine Folge von Monomorphismen $\varphi_n : K_n \to \tilde{E}$ mit $\varphi = \varphi_0 \subseteq \varphi_1 \subseteq \cdots$.
Die Abbildung $\bar{\varphi} := \varphi_0 \cup \varphi_1 \cup \cdots$ ist dann ein Monomorphismus von E nach $\tilde{E}$, und ähnlich wie vorhin können wir schließen, dass $\bar{\varphi}(E) = \tilde{E}$ sein muss.
Wenn $\mathscr{P}$ überabzählbar ist, verwenden wir eine Wohlordnung von $\mathscr{P}$ und konstruieren durch transfinite Induktion eine transfinite Folge von Approximationen an $\bar{\varphi}$, deren Vereinigung schließlich $\bar{\varphi}$ ergibt.

□

6.5.11 Folgerung. Sei $\mathscr{P} \subseteq K[x]$. Seien Z_1 und Z_2 Zerfällungskörper von $\mathscr{P}$ (bezüglich K). Dann sind Z_1 und Z_2 bezüglich K äquivalent.

6.6 Endliche Körper (Galois-Felder)

Sei K ein endlicher Körper. Dann ist $\operatorname{char} K = p \in \mathbb{P}$, und der Primkörper P von K ist isomorph zu $\mathbb{Z}_p$. Da K Vektorraum über dem Unterkörper P ist, gibt es eine Basis

$\{a_1, \ldots, a_n\}$ von K über P ($[K : P] = n \in \mathbb{N}$). Daher ist $K = \{\lambda_1 a_1 + \cdots + \lambda_n a_n \mid \lambda_i \in P\}$ und $|K| = p^n$, da jeder Koeffizient λ_i auf $|P| = p$ Arten gewählt werden kann.

Frage: Gegeben $p \in \mathbb{P}$ und $n \in \mathbb{N}$. Gibt es einen Körper K mit $|K| = p^n$?

Wenn es einen solchen Körper gibt, dann mit $\operatorname{char} K = p$. Wir gehen daher von $\mathbb{Z}_p$ aus und betrachten das Polynom $f(x) = x^{p^n} - x = x(x^{p^n-1} - 1) \in \mathbb{Z}_p[x]$. Sei K ein Zerfällungskörper von $f(x)$ über $\mathbb{Z}_p$. Dann hat $f(x)$ in K genau p^n Nullstellen $\alpha_1, \ldots, \alpha_{p^n}$, welche alle einfach sind, denn: $f'(x) = p^n x^{p^n-1} - 1 = -1 \neq 0$ ($p^n x^{p^n-1} = 0$ wegen $\operatorname{char} \mathbb{Z}_p[x] = p$). Wir behaupten nun, dass $K = \{\alpha_1, \ldots, \alpha_{p^n}\} =: N$ gilt. Dazu müssen wir nur zeigen, dass N Unterkörper von K ist:
$0, 1 \in N$, denn $f(0) = f(1) = 0$.
$\alpha, \beta \in N \Rightarrow f(\alpha+\beta) = (\alpha+\beta)^{p^n} - (\alpha+\beta) = (\alpha^{p^n} - \alpha) + (\beta^{p^n} - \beta) = f(\alpha) + f(\beta) = 0 + 0 = 0$ $\Rightarrow \alpha + \beta \in N$.
$\alpha \in N \Rightarrow f(-\alpha) = (-1)^{p^n}\alpha^{p^n} - (-1)\alpha = (-1)f(\alpha) = (-1)0 = 0 \Rightarrow -\alpha \in N$. (Beachte, dass für $p = 2$ die Gleichung $1 = -1$ gilt.)
$\alpha, \beta \in N \Rightarrow f(\alpha\beta) = (\alpha\beta)^{p^n} - \alpha\beta = \alpha^{p^n}\beta^{p^n} - \alpha\beta = \alpha\beta - \alpha\beta = 0 \Rightarrow \alpha\beta \in N$.
$\alpha \in N$, $\alpha \neq 0 \Rightarrow f(\alpha) = 0 \Rightarrow \alpha^{p^n} = \alpha \Rightarrow (\alpha^{p^n})^{-1} = \alpha^{-1} \Rightarrow (\alpha^{-1})^{p^n} = \alpha^{-1} \Rightarrow f(\alpha^{-1}) = 0$ $\Rightarrow \alpha^{-1} \in N$.

Sind K_1, K_2 endliche Körper mit $|K_1| = |K_2| = p^n$ ($p \in \mathbb{P}$, $n \in \mathbb{N}$) und P_1, P_2 die Primkörper von K_1, K_2, so gilt: $P_1 \cong P_2 \cong \mathbb{Z}_p$.

Wir zeigen nun, dass K_i Zerfällungskörper von $f(x) = x^{p^n} - x \in P_i[x]$ über P_i, $i = 1, 2$ ist: Es gilt $|K_1 \setminus \{0\}| = p^n - 1$ und $(K_1 \setminus \{0\}, \cdot)$ ist eine Gruppe. Sei $\alpha \in K_1 \setminus \{0\}$. Dann ist $\alpha^{p^n-1} = 1$ und damit $\alpha^{p^n} - \alpha = f(\alpha) = 0$, wobei letzteres auch für $\alpha = 0$ gilt. Somit sind die Elemente von K_1 genau die p^n Nullstellen von $f(x)$. Die Aussage für K_2 folgt analog. Wegen der Eindeutigkeit des Zerfällungskörpers (Lemma 6.5.7) gilt dann $K_1 \cong K_2$.

6.6.1 Satz. *Die Ordnung 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 $|K| = p^n$.* □

Schreibweise für K mit $|K| = p^n$: $K = \mathrm{GF}(p^n)$ (*Galois-Feld*).

6.6.2 Satz. *Ist K endlicher Körper, so ist die Gruppe $(K \setminus \{0\}, \cdot)$ zyklisch.*

Beweis. Sei $a \in K \setminus \{0\}$ mit maximaler Ordnung r. Zu zeigen: $r = p^n - 1$ (wobei $|K| = p^n$). Sei $b \in K \setminus \{0\}$ beliebig, $\mathrm{o}(b) = s$. Wir betrachten die Primfaktorzerlegungen von r und s: $r = p_1^{e_1} \cdots p_k^{e_k}$, $s = p_1^{f_1} \cdots p_k^{f_k}$. Es gilt:

$$\mathrm{kgV}(r, s) \quad = \quad \prod_{i=1}^{k} p_i^{\max(e_i, f_i)} \quad \overset{\text{o.B.d.A.}}{=} \quad \underbrace{p_1^{e_1} \cdots p_j^{e_j}}_{=: \tilde{r}} \underbrace{p_{j+1}^{f_{j+1}} \cdots p_k^{f_k}}_{=: \tilde{s}}, \qquad 1 \leq j \leq k.$$

Es gilt: $\mathrm{ggT}(\tilde{r}, \tilde{s}) = 1$ und $\mathrm{kgV}(\tilde{r}, \tilde{s}) = \tilde{r}\tilde{s} = \mathrm{kgV}(r, s)$. Sei $\tilde{a} := a^{r/\tilde{r}}$ und $\tilde{b} := b^{s/\tilde{s}}$. Dann gilt $\mathrm{o}(\tilde{a}) = \tilde{r}$ (denn: $\tilde{a}^{\tilde{r}} = a^r = 1$ und $\mathrm{o}(a) = r$) und $\mathrm{o}(\tilde{b}) = \tilde{s}$ (analog).

Wir behaupten nun: $\mathrm{o}(\tilde{a}\tilde{b}) = \tilde{r}\tilde{s} = \mathrm{o}(\tilde{a})\mathrm{o}(\tilde{b})$. Wegen $(\tilde{a}\tilde{b})^{\tilde{r}\tilde{s}} = (\tilde{a}^{\tilde{r}})^{\tilde{s}}(\tilde{b}^{\tilde{s}})^{\tilde{r}} = 1 \cdot 1 = 1$ gilt $\mathrm{o}(\tilde{a}\tilde{b}) | \tilde{r}\tilde{s}$. Weiters gilt: $(\tilde{a}\tilde{b})^m = 1$ für ein $m \in \mathbb{N} \Rightarrow \tilde{a}^m = \tilde{b}^{-m} \Rightarrow 1 = \tilde{a}^{m\tilde{r}} = \tilde{b}^{-m\tilde{r}} \Rightarrow$ $\mathrm{o}(\tilde{b}) = \tilde{s} | -m\tilde{r} \Rightarrow \tilde{s} | m$. Analog: $\tilde{r} | m$. Aus $\mathrm{ggT}(\tilde{r}, \tilde{s}) = 1$ folgt somit $\tilde{r}\tilde{s} | m$.

Also haben wir: $\mathrm{o}(\tilde{a}\tilde{b}) = \tilde{r}\tilde{s} = \mathrm{kgV}(r, s) = \frac{rs}{\mathrm{ggT}(r,s)} \leq r$, da r maximal. Daraus erhält man: $s \leq \mathrm{ggT}(r, s) \Rightarrow s = \mathrm{ggT}(r, s) \Rightarrow s | r$. Da b beliebig war, gilt also $b^r = 1$ für alle $b \in K \setminus \{0\}$.

$f(x) = x^r - 1 \in K[x]$ hat $p^n - 1$ Nullstellen, somit gilt $p^n - 1 \leq r$. Klarerweise gilt $r | p^n - 1$, also $r \leq p^n - 1$. Daraus folgt: $r = p^n - 1$. □

Jedes erzeugende Element von $(K \setminus \{0\}, \cdot)$ heißt ein *primitives Element* von K (für $K = \mathbb{Z}_p$: *Primitivwurzel* mod p). Ist a primitives Element von K, so gilt $K = \{0, 1, a, a^2, \ldots, a^{|K|-2}\}$ und $K \setminus \{0\} = \langle a \rangle = \langle a^t \rangle$ mit $\mathrm{ggT}(t, |K| - 1) = 1$.

Weiters gilt $K \cong \mathbb{Z}_p(a)$ für ein beliebiges primitives Element a von K. Sei $q(x)$ das Minimalpolynom von a über $\mathbb{Z}_p$. Dann ist $q(x)$ irreduzibel, und es gilt

$$\mathbb{Z}_p(a) \cong \mathbb{Z}_p[x]/(q(x)) = \{\alpha_0 + \alpha_1 x + \cdots + \alpha_{m-1} x^{m-1} + (q(x)) \mid \alpha_i \in \mathbb{Z}_p\}$$

mit $m = \operatorname{grad} q(x)$. Aus $|K| = p^n$ folgt dann $n = m = \operatorname{grad} q(x)$, also: zu beliebigem $n \in \mathbb{N}$ gibt es ein irreduzibles Polynom $q(x) \in \mathbb{Z}_p[x]$ mit $\operatorname{grad} q(x) = n$.

Um einen endlichen Körper K mit $|K| = p^n$ ($p \in \mathbb{P}$, $n \in \mathbb{N}$) zu bestimmen, d. h., seine Operationstafeln zu ermitteln, kann man daher so vorgehen:

1) Der Primkörper von K wird als $\mathbb{Z}_p$ angenommen.

2) Bestimme ein Polynom $q(x) \in \mathbb{Z}_p[x]$ mit $q(x)$ normiert, irreduzibel und $\operatorname{grad} q(x) = n$ (in endlich vielen Schritten möglich).

3) Bilde $\mathbb{Z}_p[x]/(q(x))$ — dies ist der gesuchte Körper K.

Es gilt: $\alpha := x + (q(x))$ ist (nach Einbettung von $\mathbb{Z}_p$) Nullstelle von $q(x)$. Aber nicht immer muss dieses α ein primitives Element von K sein.

α ist primitives Element $\Leftrightarrow \alpha^r \neq 1$ für $0 < r < |K| - 1 = p^n - 1 \Leftrightarrow \alpha$ ist nicht Nullstelle von $x^r - 1$ für $0 < r < p^n - 1 \;\Leftrightarrow\; q(x) \nmid x^r - 1$ für $0 < r < p^n - 1$.

Irreduzible Polynome $q(x)$ mit dieser Eigenschaft heißen *primitive Polynome*.

6.6.3 Beispiel. Bestimmung von $\mathrm{GF}(9) = \mathrm{GF}(3^2)$: 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. 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	$(0, 0)$
$\alpha^0 = 1$	$(1, 0)$
$\alpha^1 = \alpha$	$(0, 1)$
$\alpha^2 = 1 + \alpha$	$(1, 1)$
$\alpha^3 = 1 + 2\alpha$	$(1, 2)$
$\alpha^4 = 2$	$(2, 0)$
$\alpha^5 = 2\alpha$	$(0, 2)$
$\alpha^6 = 2 + 2\alpha$	$(2, 2)$
$\alpha^7 = 2 + \alpha$	$(2, 1)$
$\alpha^8 = 1$	$(1, 0)$

Die Potenzen α^j, $0 \leq j < 8$, sind somit alle verschieden, α ist ein primitives Element von GF(9) und $x^2 - x - 1$ ein primitives Polynom in $\mathbb{Z}_3[x]$. Damit können die Operationstafeln angegeben werden.

Multiplikation: $0 \cdot \alpha^i = 0$, $\alpha^i \alpha^j = \alpha^{(i+j) \bmod 8}$ ($(\mathrm{GF}(9) \setminus \{0\}, \cdot)$ ist eine zyklische Gruppe).
Addition: z. B.:

$$\begin{array}{ccccc} \alpha^2 & + & \alpha^4 & = & \alpha \\ \downarrow & & \downarrow & & \uparrow \\ (1,1) & + & (2,0) & = & (0,1) \end{array}$$

Praktische Vorgangsweise: 1) Wähle normiertes, irreduzibles Polynom $q(x) \in \mathbb{Z}_p[x]$ vom Grad n. Sei etwa $q(x) = x^n - a_{n-1}x^{n-1} - \cdots - a_1 x - a_0$ mit $a_i \in \mathbb{Z}_p$.

2) Setze $q(\alpha) = 0$ und betrachte die Basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ von $\mathrm{GF}(p^n)$ über $\mathbb{Z}_p$. Berechne unter Verwendung von $q(\alpha) = 0$ (d. h., $\alpha^n = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$) die Potenzen von α. Gilt erstmals $\alpha^{p^n-1} = 1$ (d. h., $\alpha^j \neq 1$ für $1 \leq j < p^n - 1$), so ist das gewählte $q(x)$ primitiv. Andernfalls versuche es mit einem neuen $q(x)$.

6.6.A Unterkörper von endlichen Körpern

Sei p eine feste Primzahl.

6.6.4 Satz. *Für jeden Teiler k von n hat $GF(p^n)$ genau einen Unterkörper der Kardinalität p^k.*
Umgekehrt: Wenn $GF(p^k)$ ein Unterkörper von $GF(p^n)$ ist, dann muss k ein Teiler von n sein.

Beweis. Wir überlegen zuerst, dass $x^{p^k} - x$ in $GF(p^n)$ in Linearfaktoren zerfällt:

- Wenn $a, b \in \mathbb{Z}$, $a|b$, dann gilt in $\mathbb{Z}[x]$ (und auch in $\mathbb{Z}_p[x]$): $x^a - 1 | x^b - 1$, denn $x^b - 1 = (x^a - 1)(x^{b-a} + x^{b-2a} + \cdots + x^a + 1)$.
- Sei $n = km$. Dann gilt $x^k - 1 | x^n - 1$ in $\mathbb{Z}[x]$, also $p^k - 1 | p^n - 1$ in $\mathbb{Z}$.
- Daher $x^{p^k-1} - 1 | x^{p^n-1} - 1$ in $\mathbb{Z}[x]$ (und auch in $\mathbb{Z}_p[x]$), daher $x^{p^k} - x | x^{p^n} - x$ in $\mathbb{Z}_p[x]$.
- $x^{p^n} - x$ zerfällt in $GF(p^n)$ in Linearfaktoren, also auch $x^{p^k} - x$.

Sei $K \leq GF(p^n)$ der kleinste Körper, der alle Nullstellen von $x^{p^k} - x$ enthält; K ist Zerfällungskörper von $x^{p^k} - x$ über $\mathbb{Z}_p$, hat also p^k Elemente, und zwar alle Nullstellen von $x^{p^k} - x$.
Damit ist der erste Teil des Satzes bewiesen.
Wenn nun $GF(p^k)$ Unterkörper von $GF(p^n)$ ist, dann ist $GF(p^n)$ Vektorraum über $GF(p^k)$; sei $d := [GF(p^n) : GF(p^k)]$. Dann ist $p^n = (p^k)^d$, also $k|n$. □

6.7 Algebraisch abgeschlossene Körper

6.7.1 Satz. *Sei K Körper. Dann sind die folgenden Aussagen äquivalent:*

1. *Jedes nichtkonstante Polynom $p(x) \in K[x]$ hat eine Nullstelle in K.*
2. *Jedes nichtkonstante irreduzible Polynom in $K[x]$ hat eine Nullstelle in K.*
3. *Jedes nichtkonstante irreduzible Polynom in $K[x]$ hat einen linearen Faktor $x - \alpha \in K[x]$ (ist also linear).*
4. *Jedes nichtkonstante Polynom $p(x) \in K[x]$ zerfällt in Linearfaktoren.*

5. *Für jede algebraische Erweiterung $L \geq K$ gilt $L = K$.*

Jede der obigen Eigenschaften lässt sich also als Definition für den Begriff „K ist algebraisch abgeschlossen“ verwenden.

Beweis. $4 \Rightarrow 1 \Rightarrow 2$: trivial.
$2 \Leftrightarrow 3$: $p(\alpha) = 0$ genau dann, wenn $x - \alpha$ Teiler von p ist.
$3 \Rightarrow 4$: Jedes Polynom zerfällt in irreduzible Faktoren, diese müssen laut 3 alle linear sein.
$1 \Rightarrow 5$: Sei $\alpha \in L$. Da α algebraisch ist, hat α ein Minimalpolynom in $K[x]$. Dieses muss linear sein, also $\alpha \in K$.
$5 \Rightarrow 2$: Sei $p(x)$ irreduzibel und nicht konstant. Dann ist das von $p(x)$ in $K[x]$ erzeugte Ideal $(p(x))$ maximal, und $L := K[x]/(p(x))$ ist eine algebraische Körpererweiterung von K, in der $p(x)$ eine Nullstelle hat. Wegen $L = K$ hat p auch schon in K eine Nullstelle. □

6.7.2 Satz. *Sei K Körper, und sei L der Zerfällungskörper von ganz $K[x]$ über K. Dann ist L algebraisch abgeschlossen.*

Bemerkung: Jedes Polynom $p(x) \in K[x]$ hat eine Nullstelle in L; wir wollen zeigen, dass auch jedes Polynom aus $L[x]$ eine Nullstelle hat.

Beweis. Sei $L \leq L(\beta)$, β algebraisch über L. Zu zeigen ist $\beta \in L$.
β ist Nullstelle eines Polynoms $a_0 + \ldots + a_n x^n \in L[x]$. Alle Koeffizienten a_i sind in L, daher algebraisch über K.
Es ist also β algebraisch über $K(a_0, \ldots, a_n)$, und jedes a_i algebraisch über K. Nach einem bereits bewiesenen Satz ist dann auch β algebraisch über K. Sei $q(x)$ Minimalpolynom von β über K, dann zerfällt q in $L[x]$ in Linearfaktoren, einer davon muss $x - \beta$ sein, also $\beta \in L$. □

6.7.3 Folgerung. Zu jedem Körper K gibt es eine algebraisch abgeschlossene Erweiterung L. Insbesondere gilt: Der Zerfällungskörper von $K[x]$ ist der „algebraische Abschluss“ von K, das ist der (bis auf Isomorphie eindeutige) kleinste algebraisch abgeschlossene Körper $L \geq K$.

6.7.A Beispiele

Sei p eine Primzahl. Die Körper $GF(p^{n!})$ $(n = 1, 2, \ldots)$ bilden eine aufsteigende Kette:

$$GF(p) \leq GF(p^2) \leq GF(p^6) \leq GF(p^{24}) \leq GF(p^{120}) \leq \cdots$$

Die Vereinigung aller dieser Körper bezeichnen wir mit $GF(p^\infty)$. Offenbar ist $GF(p^\infty)$ Körper. Für jede Zahl $k \geq 1$ gilt $GF(p^k) \leq GF(p^{k!}) \leq GF(p^\infty)$, also enthält $GF(p^\infty)$ alle endlichen Körper der Charakteristik p.

6.7.4 Satz. *$GF(p^\infty)$ ist algebraisch abgeschlossen. $GF(p^\infty)$ ist sogar der kleinste algebraisch abgeschlossene Körper der Charakteristik p.*

Beweis. Sei $q(x) \in GF(p^\infty)[x]$ Polynom. Dann liegen alle Koeffizienten von q in einem geeigneten $GF(p^{k!})$, daher gibt es ein gemeinsames k mit $q(x) \in GF(p^{k!})[x]$.
Sei nun K der Zerfällungskörper von q über $GF(p^{k!})$. K ist eine endliche Erweiterung von $GF(p^{k!})$, ist also isomorph zu einem geeigneten $GF(p^n)$, $n \geq k$. In $GF(p^n)$ (und erst recht in $GF(p^{n!})$ und in $GF(p^\infty)$) zerfällt $q(x)$ in Linearfaktoren.
Für die Umkehrung: Sei L ein algebraisch abgeschlossener Körper der Charakteristik p. Dann zerfällt $x^{p^n} - x$ in $L[x]$ in Linearfaktoren, also enthält L den Körper $GF(p^n)$. □

Kapitel 7

Fundamentalsatz der Algebra

7.1 Der Fundamentalsatz

Dieser Satz lautet: Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen, d. h., jedes Polynom $f(x) \in \mathbb{C}[x]$, $f(x) \neq 0$, mit $\operatorname{grad} f(x) = n$ hat genau n Nullstellen, sofern man jede Nullstelle mit ihrer Vielfachheit zählt.

Anders ausgedrückt: Jedes $f(x) \in \mathbb{C}[x]$, $f(x) \neq 0$, mit $\operatorname{grad} f(x) = n$ kann in der Form

$$f(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$$

dargestellt werden mit $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$.

Der Körper $\mathbb{C}$ der komplexen Zahlen kann algebraisch definiert werden als $\mathbb{C} := \mathbb{R}(i)$, wobei i Nullstelle des in $\mathbb{R}[x]$ irreduziblen Polynoms $x^2+1 \in \mathbb{R}[x]$ ist. Es gilt somit $\mathbb{C} \cong \mathbb{R}[x]/(x^2+1)$ sowie $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}$, wobei $i^2 = -1$.

Der erste Beweis des Fundamentalsatzes stammt von Gauß. Bevor wir hier den Fundamentalsatz beweisen können, benötigen wir zunächst einige Ergebnisse über Polynome in mehreren Unbestimmten.

7.2 Polynome in n Unbestimmten

Sei I ein Integritätsbereich. Nach Abschnitt 4.1 haben wir

$$I[x_1, \ldots, x_n] = \{ \sum_{(i_1,\ldots,i_n) \in \mathbb{N}_0^n} a_{i_1 \ldots i_n} x_1^{i_1} \cdots x_n^{i_n} \mid a_{i_1 \ldots i_n} \in I, \text{ fast alle } = 0\}.$$

Homogene Polynome: alle auftretenden $a_{i_1 \ldots i_n} x_1^{i_1} \cdots x_n^{i_n}$ haben den gleichen Grad $i_1 + \cdots + i_n$.

Anderer Ausdruck für homogenes Polynom: *Form*. Z. B. hat eine quadratische Form in 2 Variablen die Gestalt: $a_{20}x_1^2 + a_{11}x_1x_2 + a_{02}x_2^2$. Jedes Polynom aus $I[x_1, \ldots, x_n]$ ist als Summe von Formen darstellbar.

$h(ax_1^{i_1} \cdots x_n^{i_n}) := (i_1, \ldots, i_n)$ $(a \neq 0)$ heißt *Höhe* von $ax_1^{i_1} \cdots x_n^{i_n}$.

$(i_1, \ldots, i_n) \geq (k_1, \ldots, k_n) :\Leftrightarrow (i_1, \ldots, i_n) = (k_1, \ldots, k_n)$ oder unter den Differenzen $i_1 - k_1, \ldots, i_n - k_n$ ist die erste von 0 verschiedene positiv („lexikographische Ordnung“).

$(\mathbb{N}_0^n, \leq)$ ist eine Wohlordnung, d. h., jede nichtleere Teilmenge hat ein kleinstes Element.

Induktionsbeweise in wohlgeordneten Mengen $(M, \leq)$:

1) Aussage gilt für das kleinste Element von M.

2) Aussage gilt für alle $b < a \Rightarrow$ Aussage gilt für a $(a, b \in M)$.

(Dieses Induktionsprinzip folgt unmittelbar aus der Definition der Wohlordnung.)

Ist $f(x_1, \ldots, x_n) \in I[x_1, \ldots, x_n]$, $f \neq 0$, so bezeichne $\mathrm{HG}(f)$ (in Worten: „höchstes Glied von f“) das höchste Element $a_{i_1 \ldots i_n} x_1^{i_1} \cdots x_n^{i_n}$ mit $a_{i_1 \ldots i_n} \neq 0$ in der obigen Darstellung von f.

7.2.1 Satz. $\mathrm{HG}(f \cdot g) = \mathrm{HG}(f) \cdot \mathrm{HG}(g)$, $f, g \in I[x_1, \ldots, x_n] \setminus \{0\}$.

Beweis. Übungsbeispiel. □

7.2.2 Satz. *Ist I unendlich und $f(a_1, \ldots, a_n) = 0$ für alle $(a_1, \ldots, a_n) \in I^n$, so ist $f(x_1, \ldots, x_n)$ das Nullpolynom.*

Beweis. Übungsbeispiel. □

Dies gilt nicht für endliches I: z. B. hat in $\mathrm{GF}(p^n)$ das vom Nullpolynom verschiedene Polynom $f(x) = x^{p^n} - x$ jedes Element als Nullstelle.

7.3 Symmetrische Polynome

Sei z. B. $x^3 + ax^2 + bx + c \in \mathbb{C}[x]$ mit den 3 Nullstellen x_1, x_2, x_3, d. h., $x^3 + ax^2 + bx + c = (x - x_1)(x - x_2)(x - x_3)$. Dann gilt $a = -(x_1 + x_2 + x_3) =: -s_1$, $b = x_1x_2 + x_1x_3 + x_2x_3 =: s_2$, $c = -x_1x_2x_3 =: -s_3$ (elementarsymmetrische Polynome).

7.3.1 Definition. $f(x_1, \ldots, x_n) \in I[x_1, \ldots, x_n]$ heißt *symmetrisch* $:\Leftrightarrow \forall \pi \in S_n : f(x_1, \ldots, x_n) = f(x_{\pi(1)}, \ldots, x_{\pi(n)})$.

Beispiele symmetrischer Polynome. 1) Potenzsummen $x_1^k + \cdots + x_n^k$ $(k \in \mathbb{N})$.

2) Wronski-Funktionen: $\sum_{i_1 + \cdots + i_n = k} x_1^{i_1} \cdots x_n^{i_n}$, z. B. für $k = 3$ und $n = 2$: $x_1^3 + x_1^2 x_2 + x_1 x_2^2 + x_2^3$.

3) Diskriminante: $\prod_{1 \leq i < k \leq n} (x_i - x_k)^2$.

4) Elementarsymmetrische Polynome $s_1, \ldots, s_n$: $(z - x_1) \cdots (z - x_n) = z^n - s_1 z^{n-1} + s_2 z^{n-2} + \cdots + (-1)^n s_n$, d. h., $s_k := \sum_{i_1 < \ldots < i_k} x_{i_1} \cdots x_{i_k}$ ($\binom{n}{k}$ Summanden).

7.3.2 Satz (Hauptsatz über symmetrische Polynome)**.** *Jedes symmetrische Polynom $f(x_1, \ldots, x_n) \in I[x_1, \ldots, x_n]$ lässt sich mit genau einem Polynom $p(x_1, \ldots, x_n) \in I[x_1, \ldots, x_n]$ in der Form $f(x_1, \ldots, x_n) = p(s_1, \ldots, s_n)$ darstellen.*

Zum Beweis dieses Satzes benötigen wir drei Lemmata:

7.3.3 Lemma. *Ist $f(x_1, \ldots, x_n) \in I[x_1, \ldots, x_n]$ ein symmetrisches Polynom, so gilt* $\mathrm{HG}(f) = a x_1^{i_1} \ldots x_n^{i_n}$ *mit $a \in I \setminus \{0\}$, $i_1 \geq i_2 \geq \ldots \geq i_n$.*

Beweis. Übungsbeispiel. □

7.3.4 Lemma. $\mathrm{HG}(s_1^{i_1} \cdots s_n^{i_n}) = \mathrm{HG}(s_1^{i_1}) \cdots \mathrm{HG}(s_n^{i_n}) = x_1^{i_1} (x_1 x_2)^{i_2} \cdots (x_1 x_2 \cdots x_n)^{i_n}$.

Anders ausgedrückt: $\mathrm{HG}(s_1^{k_1 - k_2} s_2^{k_2 - k_3} \cdots s_{n-1}^{k_{n-1} - k_n} s_n^{k_n}) = x_1^{k_1} \cdots x_n^{k_n}$, $k_1 \geq k_2 \geq \ldots \geq k_n$.

Beweis. Folgt aus der Definition des höchsten Gliedes. □

7.3.5 Lemma. $(i_1, \ldots, i_n) \neq (j_1, \ldots, j_n) \Rightarrow \mathrm{HG}(s_1^{i_1} \cdots s_n^{i_n}) \neq \mathrm{HG}(s_1^{j_1} \cdots s_n^{j_n})$.

Beweis. Sei k der größte Index mit $i_k \neq j_k$. Dann ist $i_k + \cdots + i_n \neq j_k + \cdots + j_n$, und die Behauptung folgt aus Lemma 7.3.4.

Nach diesen Vorbereitungen kommen wir nun zum
Beweis des Hauptsatzes. Sei $f(x_1, \ldots, x_n) \in I[x_1, \ldots, x_n]$. Wir zeigen $f(x_1, \ldots, x_n) = p(s_1, \ldots, s_n)$ durch Induktion nach $h(\mathrm{HG}(f)) =: h(f)$, also nach der Höhe des höchsten Gliedes.

Induktionsanfang: $h(f) = (0, \ldots, 0) \Rightarrow f$ konstant, d. h. $f \in I \Rightarrow p = f$ kann gewählt werden.

Induktionsannahme: Sei $h(f) > (0, \ldots, 0)$ und der Satz bewiesen für alle symmetrischen $g \in I[x_1, \ldots, x_n]$ mit $h(g) < h(f)$.

Induktionsbehauptung: $f(x_1, \ldots, x_n) = p(s_1, \ldots, s_n)$ für ein geeignetes $p \in I[x_1, \ldots, x_n]$. Sei $t(x_1, \ldots, x_n) := f(x_1, \ldots, x_n) - a s_1^{k_1-k_2} s_2^{k_2-k_3} \cdots s_n^{k_n}$, wobei $\mathrm{HG}(f) = a x_1^{k_1} \cdots x_n^{k_n}$ ($a \neq 0$, $k_1 \geq k_2 \geq \ldots \geq k_n$). Dann ist nach Lemma 7.3.4 $h(t) = h(\mathrm{HG}(t)) < h(\mathrm{HG}(f)) = h(f)$. Nach Induktionsannahme gilt $t = q(s_1, \ldots, s_n)$ und damit $f = q(s_1, \ldots, s_n) + a s_1^{k_1-k_2} s_2^{k_2-k_3} \cdots s_n^{k_n} =: p(s_1, \ldots, s_n)$.

Eindeutigkeit: $f(x_1, \ldots, x_n) = p(s_1, \ldots, s_n) = q(s_1, \ldots, s_n) \Rightarrow p(s_1, \ldots, s_n) - q(s_1, \ldots, s_n) =: d(s_1, \ldots, s_n) = 0$. Es gilt: $d(s_1, \ldots, s_n) = \sum_{(i_1, \ldots, i_n) \in \mathbb{N}_0^n} a_{i_1 \ldots i_n} s_1^{i_1} \cdots s_n^{i_n} = 0 = \varphi(x_1, \ldots, x_n)$.

Behauptung: alle $a_{i_1 \ldots i_n} = 0$, d. h., $d(x_1, \ldots, x_n) = 0$. Angenommen, ein Koeffizient wäre von 0 verschieden. Nach Lemma 7.3.5 gilt: $(i_1, \ldots, i_n) \neq (j_1, \ldots, j_n) \Rightarrow \mathrm{HG}(s_1^{i_1} \cdots s_n^{i_n}) \neq \mathrm{HG}(s_1^{j_1} \cdots s_n^{j_n})$. Unter allen $a_{i_1 \ldots i_n} s_1^{i_1} \cdots s_n^{i_n}$ mit $a_{i_1 \ldots i_n} \neq 0$ gibt es daher genau eines mit größtem $\mathrm{HG}(a_{i_1 \ldots i_n} s_1^{i_1} \cdots s_n^{i_n})$. Für dieses wäre nach Lemma 7.3.4 $a_{i_1 \ldots i_n} x_1^{i_1 + \cdots + i_n} \cdots x_n^{i_n}$ das höchste Glied in $\varphi(x_1, \ldots, x_n)$. Widerspruch! □

7.4 Beweis des Fundamentalsatzes

Die folgenden beiden Lemmata werden aus der Analysis als bekannt vorausgesetzt.

7.4.1 Lemma. *Jedes quadratische Polynom hat in $\mathbb{C}$ zwei Nullstellen, und zwar hat $ax^2 + bx + c$ ($a \neq 0$) die Nullstellen*

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

□

7.4.2 Lemma. *Jede Polynomfunktion $z \mapsto a_n z^n + \cdots + a_1 z + a_0$ ist stetig auf ganz $\mathbb{C}$.* □

7.4.3 Lemma. *Sei $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$, $a_n \neq 0$, $n \geq 1$. Dann gibt es ein $r \in \mathbb{R}^+$, sodass für alle $z \in \mathbb{C}$ mit $|z| > r$ gilt: $|a_n z^n| > |a_{n-1} z^{n-1} + \cdots + a_1 z + a_0|$.*

Beweis. Sei $A := \max\{|a_{n-1}|, \ldots, |a_0|\}$, $r := \frac{A}{|a_n|} + 1$. Sei $z \in \mathbb{C}$, $|z| > r$. Dann gilt: $|z| - 1 > r - 1 = \frac{A}{|a_n|} \Rightarrow |a_n| > \frac{A}{|z|-1} \Rightarrow |a_n z^n| = |a_n| \cdot |z|^n > A \cdot \frac{|z|^n}{|z|-1} \geq A \cdot \frac{|z|^n - 1}{|z|-1} = A \cdot (|z|^{n-1} + \cdots + |z| + 1) \geq |a_{n-1}| \cdot |z|^{n-1} + \cdots + |a_1| \cdot |z| + |a_0| \geq |a_{n-1} z^{n-1} + \cdots + a_1 z + a_0|$. □

7.4.4 Folgerung. Sei $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{R}[x]$, $a_n \neq 0$, $n \geq 1$. Dann gibt es ein $r \in \mathbb{R}^+$, sodass für alle $z \in \mathbb{R}$ mit $|z| > r$ gilt: $\operatorname{sign} f(z) = \operatorname{sign}(a_n z^n)$.

7.4.5 Satz. *Sei $f(x) \in \mathbb{R}[x]$, $\operatorname{grad} f(x) = n$ ungerade. Dann gibt es ein $\alpha \in \mathbb{R}$ mit $f(\alpha) = 0$.*

Beweis. Seien $f(x), r$ wie oben. Für $z_1 < -r$ und $z_2 > r$ gilt dann: $\operatorname{sign} f(z_1) = \operatorname{sign}(a_n z_1^n) \neq \operatorname{sign}(a_n z_2^n) = \operatorname{sign} f(z_2)$. Da f stetig ist, gibt es nach dem Zwischenwertsatz ein α mit $z_1 < \alpha < z_2$ und $f(\alpha) = 0$. □

7.4.6 Satz. *Sei $f(x) \in \mathbb{R}[x]$, $\operatorname{grad} f(x) = n \geq 1$, dann gibt es ein $\alpha \in \mathbb{C}$ mit $f(\alpha) = 0$.*

Beweis. Es ist $n = 2^m q$ mit $m \in \mathbb{N}_0$, $q \in \mathbb{N}$, q ungerade. Wir führen den Beweis durch Induktion nach m.

1) $m = 0$: vorheriger Satz.

2) Schluss von $m-1$ auf $m \geq 1$: Sei $f(x) = a_n f_1(x) \cdots f_k(x)$ die Zerlegung von f in normierte irreduzible Polynome aus $\mathbb{R}[x]$. Sei $\operatorname{grad} f_i(x) = n_i = 2^{m_i} q_i$, $m_i \in \mathbb{N}_0$, $q_i \in \mathbb{N}$, q_i ungerade. Es gilt: $n = 2^m q = n_1 + \cdots + n_k$. Es gibt dann ein i mit $m_i \leq m$. (Denn: $m_i > m$, $i = 1, \ldots, k \Rightarrow 2^{m+1} | n_i$, $i = 1, \ldots, k \Rightarrow 2^{m+1} | n$, Widerspruch!)

Fall 1: Es gibt ein i mit $m_i < m$, d. h., $m_i \leq m-1$. Nach Induktionsannahme gibt es ein $\alpha \in \mathbb{C}$ mit $f_i(\alpha) = 0$, woraus $f(\alpha) = 0$ folgt.

Fall 2: Es gibt ein i mit $m_i = m$. Wir setzen zur Vereinfachung $f_i = f$, $n_i = n$, $q_i = q$ und $m_i = m$. Somit haben wir: $f(x) \in \mathbb{R}[x]$ normiert und irreduzibel und $\operatorname{grad} f(x) = n = 2^m q$. Seien $\alpha_1, \ldots, \alpha_n$ die Nullstellen von $f(x)$ in einem Erweiterungskörper von $\mathbb{C}$. In $\mathbb{R}(\alpha_1, \ldots, \alpha_n)[x]$ gilt dann: $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$. Da $\operatorname{char} \mathbb{R} = 0$ und $f(x)$ irreduzibel ist, sind nach Abschnitt 6.4 die α_i paarweise verschieden. Da $\alpha_1, \ldots, \alpha_n$ algebraisch über $\mathbb{R}$ sind, folgt nach dem Gradsatz: $[\mathbb{R}(\alpha_k)(\alpha_j) : \mathbb{R}] < \infty$. Daher sind alle Elemente in $\mathbb{R}(\alpha_k, \alpha_j) = \mathbb{R}(\alpha_k)(\alpha_j)$ algebraisch über $\mathbb{R}$, insbesondere $\alpha_k + \alpha_j$ und $\alpha_k \alpha_j$. Wegen $\operatorname{char} \mathbb{R} = 0$ gilt (siehe Abschnitt 6.4) $\mathbb{R}(\alpha_k + \alpha_j, \alpha_k \alpha_j) = \mathbb{R}(\alpha_k + \alpha_j + c\alpha_k \alpha_j)$ für fast alle $c \in \mathbb{R}$ (d. h. für alle $c \in \mathbb{R}$ bis auf endlich viele). Also gilt auch für fast alle $c \in \mathbb{R}$: $\mathbb{R}(\alpha_k + \alpha_j, \alpha_k \alpha_j) = \mathbb{R}(\alpha_k + \alpha_j + c\alpha_k \alpha_j)$ für alle $k, j = 1, \ldots, n$. Es gibt also ein $c \in \mathbb{R}$ mit $\mathbb{R}(\alpha_k + \alpha_j, \alpha_k \alpha_j) = \mathbb{R}(\alpha_k + \alpha_j + c\alpha_k \alpha_j)$ für alle k, j mit $1 \leq k, j \leq n$. Wir halten nun c fest. Sei $\beta_{jk} := \alpha_k + \alpha_j + c\alpha_j \alpha_k$, $1 \leq k, j \leq n$. Dann gilt für $1 \leq k, j \leq n$: $\beta_{jk} (= \beta_{kj}) \in \mathbb{R}(\alpha_1, \ldots, \alpha_n)$. Sei nun $p(x) := \prod_{1 \leq j < k \leq n} (x - \beta_{jk}) = x^{n(n-1)/2} + \sum_{1 \leq i \leq n(n-1)/2} (-1)^i s_i(\beta_{12}, \ldots, \beta_{n-1\,n}) x^{n(n-1)/2 - i} \in \mathbb{R}(\alpha_1, \ldots, \alpha_n)[x]$ (s_i elementarsymmetrische Polynome). Für $1 \leq i \leq n(n-1)/2$ ist dann $s_i(\beta_{12}, \ldots, \beta_{n-1\,n}) = t_i(\alpha_1, \ldots, \alpha_n)$, mit $t_i(x_1, \ldots, x_n) \in \mathbb{R}[x_1, \ldots, x_n]$, wobei alle $t_i(x_1, \ldots, x_n)$ symmetrische Polynome sind. Aus dem Hauptsatz folgt

$$s_k(\beta_{12}, \ldots, \beta_{n-1\,n}) = t_k(\alpha_1, \ldots, \alpha_n) = p_k(s_1(\alpha_1, \ldots, \alpha_n), \ldots, s_n(\alpha_1, \ldots, \alpha_n)).$$

Daher gilt

$$p(x) = x^{n(n-1)/2} + \sum_{1 \leq k \leq n(n-1)/2} (-1)^k p_k(s_1(\alpha_1, \ldots, \alpha_n), \ldots, s_n(\alpha_1, \ldots, \alpha_n)) x^{n(n-1)/2 - k},$$

wobei $p_k(x_1, \ldots, x_n) \in \mathbb{R}[x_1, \ldots, x_n]$.

Es gilt

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n) = x^n + \sum_{1 \leq i \leq n} (-1)^i s_i(\alpha_1, \ldots, \alpha_n) x^{n-i} \in \mathbb{R}[x],$$

also $s_i(\alpha_1, \ldots, \alpha_n) \in \mathbb{R}$. Daher ist auch $p(x) \in \mathbb{R}[x]$ und $\operatorname{grad} p(x) = \frac{n(n-1)}{2} = \frac{2^m q(2^m q-1)}{2} = 2^{m-1}q'$, wobei q' ungerade. Nach Induktionsannahme hat $p(x)$ eine Nullstelle in $\mathbb{C}$. Wegen $\beta_{jk} \in \mathbb{C}(\alpha_1, \ldots, \alpha_n)$ liegt mindestens ein β_{jk} in $\mathbb{C}$. Sei o. B. d. A. $\beta_{12} = \alpha_1 + \alpha_2 + c\alpha_1\alpha_2 \in \mathbb{C}$. Dann gilt: $\mathbb{C} \supseteq \mathbb{R}(\beta_{12}) = \mathbb{R}(\alpha_1 + \alpha_2, \alpha_1\alpha_2) \Rightarrow \alpha_1 + \alpha_2, \alpha_1\alpha_2 \in \mathbb{C} \Rightarrow (x - \alpha_1)(x - \alpha_2) = x^2 - (\alpha_1 + \alpha_2)x + \alpha_1\alpha_2 \in \mathbb{C}[x]$ mit Nullstellen $\alpha_1, \alpha_2 \Rightarrow \alpha_1, \alpha_2 \in \mathbb{C}$. □

7.4.7 Satz. *Sei $f(x) \in \mathbb{C}[x]$, $\operatorname{grad} f(x) = n \geq 1$, dann gibt es ein $\alpha \in \mathbb{C}$ mit $f(\alpha) = 0$.*

Beweis. Sei α eine Nullstelle von f in einem Erweiterungskörper von $\mathbb{C}$. Dann gilt: $[\mathbb{C}(\alpha) : \mathbb{C}] \leq n \Rightarrow [\mathbb{C}(\alpha) : \mathbb{R}] \leq 2n \Rightarrow \alpha$ algebraisch über $\mathbb{R}$.

Sei $g(x) \in \mathbb{R}[x]$ das Minimalpolynom von α über $\mathbb{R}$. Dann gilt $g(\alpha) = 0$, und es gibt nach dem vorherigen Satz ein $\beta \in \mathbb{C}$ mit $g(\beta) = g(\bar{\beta}) = 0$.

Fall 1: $\beta = \bar{\beta}$, d. h., $\beta \in \mathbb{R}$. Dann ist $g(x) = x - \beta$, da $g(x)$ auch das Minimalpolynom von β über $\mathbb{R}$ ist, woraus $\alpha = \beta \in \mathbb{R}$ folgt.

Fall 2: $\beta \neq \bar{\beta}$: Dann gilt $(x-\beta)(x-\bar{\beta}) = x^2 - (\beta+\bar{\beta})x + \beta\bar{\beta} \in \mathbb{R}[x]$ und $(x-\beta)(x-\bar{\beta})|g(x)$. Daraus folgt $g(x) = x^2 - (\beta + \bar{\beta})x + \beta\bar{\beta}$. Also ist $\alpha \in \{\beta, \bar{\beta}\} \subseteq \mathbb{C}$, d. h., $\alpha \in \mathbb{C}$. □

7.5 Alternativer Beweis des Fundamentalsatzes

Für jedes Polynom $p(x) \in \mathbb{C}[x]$ schreiben wir $|p|$ für die Funktion, die jeder komplexen Zahl a die reelle Zahl $|p(a)|$ zuordnet.
Wir verwenden die folgenden aus der Analysis bekannten Sätze:

- Für jedes Polynom $p(x) \in \mathbb{C}[x]$ ist die Funktion $|p|$ (als Verknüpfung zweier stetiger Funktionen) stetig.
- Für jedes $R \in \mathbb{R}$ ist die Menge $\{a \in \mathbb{C} \mid |a| \leq R\}$ kompakt.
- Jede stetige Funktion auf einer kompakten Menge hat ein Minimum, d.h., wenn $f : C \to \mathbb{R}$ stetig ist, und $C \neq \emptyset$ kompakt, dann gibt es ein $c \in C$ mit $\forall d \in C\ f(c) \leq f(d)$.
- Für alle $a \in \mathbb{C}$ und alle $n \geq 1$ gibt es b mit $b^n = a$.

7.5.1 Satz. *Sei $p(x) \in \mathbb{C}[x]$ nichtkonstantes Polynom, und sei $p(a) \neq 0$. Dann gibt es eine komplexe Zahl b mit $|p(b)| < |p(a)|$.*

7.5.2 Lemma. *Sei $p(x)$ ein Polynom, dann hat $\{\, |p(x)| \mid x \in \mathbb{C} \,\}$, der Wertebereich der Funktion $|p|$, ein kleinstes Element.*

7.5.3 Folgerung. Sei $p(x) \in \mathbb{C}[x]$, dann gibt es ein $a \in \mathbb{C}$ mit $p(a) = 0$.

Beweis. Sei c der kleinste Wert des Wertebereichs von $|p|$. Nach dem gerade bewiesenen Satz ist $c > 0$ unmöglich, also $c = 0$. □

In den folgenden Beweisen verwenden wir die folgenden Abschätzungen.

(a) Sei $p(x) = a_0 + \cdots + a_n x^n$, und sei $C := |a_0| + \cdots + |a_n|$. Dann gilt für alle $z \in \mathbb{C}$:

$$|z| \leq 1 \ \Rightarrow\ |p(z)| \leq C, \qquad |z| \geq 1 \ \Rightarrow\ |p(z)| \leq C|z|^n$$

(b) Sei $p(x) = a_0 + \cdots + a_{n-1}x^{n-1} + x^n$. Dann ist

$$|p(z)| \geq |z|^n - |a_{n-1}z^{n-1} + \cdots + a_0|$$

wobei der Minuend $|a_{n-1}z^{n-1} + \cdots + a_0|$ gemäß (a) abgeschätzt werden kann, also insbesondere für $|z| > 1$:

$$|p(z)| \geq |z|^n - C|z|^{n-1}$$

Beweis des Lemmas. Sei $p(x) = a_0 + \cdots + a_n x^n$ mit $a_n \neq 0$, oBdA $a_n = 1$.
Sei C die Summe der Absolutbeträge der Koeffizienten von p.
Auf der kompakten Menge $\{x \mid |x| \leq 2C\}$ nimmt $|p(x)|$ sicher ein Minimum m^* an. Dieses ist auch ein globales Minimum, denn für $A := |x| \geq 2C$ ist

$$|p(x)| \geq A^n - A^{n-1}C = A^{n-1}(A - C) \geq A^{n-1}\frac{A}{2} > |p(0)| \geq m^*$$

□

Beweis des Satzes. Wir beweisen diesen Satz zunächst nur für $a = 0$ (um die Notation zu vereinfachen). Der allgemeine Satz folgt dann, indem wir statt des Polynoms $p(x)$ das Polynom $q(y) := p(y + a)$ betrachten. ($q(0) = p(a)$.)
Sei also $p(x) \in \mathbb{C}[x]$ nichtkonstantes Polynom mit konstantem Term $c = p(0) \neq 0$. Dann suchen wir ein $b \in \mathbb{C}$, mit $|p(b)| < |c|$.
Um die Notation weiter zu vereinfachen, nehmen wir $c = 1$ an. (Der allgemeine Fall folgt dann, indem wir $p(x)$ durch c dividieren.)
$p(x)$ hat also die Form $1 + Ax^n + \cdots$ mit $A \neq 0$. Sei B eine n-te Wurzel aus $-A$, d.h. $B^n = -A$. Wir betrachten statt $p(x)$ das Polynom $q(y) := p(y/B)$; offenbar hat q dieselbe Wertemenge wie p.
Es gilt $q(y) = 1 + A(y/B)^n + ... = 1 - y^n + r(y)$, wobei $r(y)$ durch y^{n+1} teilbar ist, also $q(y) = 1 - y^n + y^{n+1}R(y)$ mit einem Polynom $R(y)$.
Sei $C > 1$ größer als die Summe der Absolutbeträge der Koeffizienten von R. Für $|y| < 1$ gilt dann $|R(y)| \leq C$.
Gesucht ist nun ein x mit $|p(x)| < 1$, bzw ein y mit $|q(y)| < 1$, wobei $q(y)$ die Form

$$q(y) = 1 - y^n + y^{n+1}R(y)$$

hat.
Sei nun $0 < \varepsilon < 1/(2C)$, also $C < 1/(2\varepsilon)$. Dann ist $C\varepsilon^{n+1} < \frac{1}{2}\varepsilon^n$, also

$$|q(\varepsilon)| \leq |1 - \varepsilon^n| + \varepsilon^{n+1}C < 1 - \varepsilon^n + \frac{1}{2}\varepsilon^n = 1 - \frac{\varepsilon^n}{2} < 1.$$

□

Kapitel 8

Galois-Theorie

8.1 Galois-Verbindungen

8.1.1 Definition. Eine Abbildung

$$\eta : \left\{ \begin{array}{ccc} \mathfrak{P}(A) & \to & \mathfrak{P}(A) \\ X & \mapsto & \eta(X) \end{array} \right.$$

heißt *Hüllenoperator* auf $A :\Leftrightarrow$

(i) $X \subseteq X^* \subseteq A \Rightarrow \eta(X) \subseteq \eta(X^*)$ (monoton),

(ii) $X \subseteq \eta(X)$ (extensiv),

(iii) $\eta(\eta(X)) = \eta(X)$ (idempotent).

8.1.2 Definition. Seien A, B Mengen, und sei $R \subseteq A \times B$ eine Relation. Wir schreiben $xRy :\Leftrightarrow (x, y) \in R$.
Für $X \subseteq A$, $Y \subseteq B$ definieren wir:

$$X^\uparrow := \{b \in B \mid \forall x \in X\, xRb\}, \qquad Y^\downarrow := \{a \in A \mid \forall y \in Y\, aRy\}.$$

Dann gilt offenbar $X \subseteq X^{\uparrow\downarrow}$, $Y \subseteq Y^{\downarrow\uparrow}$. Die Abbildungen $X \mapsto X^\uparrow$ und $Y \mapsto Y^\downarrow$ sind offensichtlich antiton, und die Abbildungen $(\cdot)^{\uparrow\downarrow}$ und $(\cdot)^{\downarrow\uparrow}$ sind monoton und extensiv. Weiters gilt

$$X \subseteq X^{\uparrow\downarrow} \;\Rightarrow\; (X^{\uparrow\downarrow})^\uparrow \subseteq X^\uparrow$$

sowie $X^\uparrow \subseteq (X^\uparrow)^{\downarrow\uparrow}$, daher $X^\uparrow = X^{\uparrow\downarrow\uparrow}$. Daher ist die Abbildung $(\cdot)^{\uparrow\downarrow}$ idempotent und somit ein Hüllenoperator.
Das Tripel (A, B, R) nennen wir **Galois-Verbindung**. Die Elemente von

$$\{Y^\downarrow \mid Y \subseteq B\} = \{X \subseteq A \mid X = X^{\uparrow\downarrow}\} \quad \text{bzw.} \quad \{X^\uparrow \mid X \subseteq B\} = \{Y \subseteq A \mid Y = Y^{\downarrow\uparrow}\}$$

heißen **Galois-abgeschlossene** Mengen.

8.1.A Beispiele

Sei K Körper, sei $A = B = K^n$, sei $R := \{(a, b) \in A \times B \mid a \cdot b = 0\}$ (wobei $\cdot$ das Skalarprodukt ist). Dann ist $X^\uparrow$ der Orthogonalraum von X, und $X^{\uparrow\downarrow}$ ist die lineare Hülle von X.

Sei A die Menge[1] alle Algebren eines vorgegebenen Typs. Sei B die Menge aller möglichen Gesetze (die nur Operations- und Konstantensymbole dieses Typs verwenden). So ein Gesetz können wir als Paar von Termen auffassen.
Sei $R := \{(a,b) |$ das Gesetz b gilt in der Algebra $a\}$. Für eine Menge Y von Gesetzen ist dann $Y^{\downarrow} = \mathrm{Mod}(Y)$, also die Menge aller Algebren, in denen alle Gesetze aus Y gelten. Für eine Menge $X \subseteq A$ von Algebren wird die Menge $X^{\uparrow}$ oft mit $Eq(X)$ bezeichnet; dies ist die Menge aller Gesetze, die in allen Algebren aus X gelten.
Für eine Menge X von Algebren ist $X^{\uparrow\downarrow}$ die von X erzeugte Varietät, das ist die kleinste Varietät, die alle Algebren in X enthält. (Nach dem Satz von Birkhoff ist das der Abschluss von X unter den Operatoren H, S, P; siehe Abschnitt 6.2.)

Klassische Galois-Verbindung: Sei K ein Körper, E ein Erweiterungskörper von K, Kurzschreibweise: $K \leq E$. Weiters sei

$$\mathrm{Gal}(E/K) := \{\varphi \in \mathrm{Aut}(E) \mid \varphi(x) = x,\ \forall x \in K\}.$$

Dabei bezeichnet $\mathrm{Aut}(E)$ die Automorphismengruppe von E, und $\mathrm{Gal}(E/K)$ heißt *Galois-Gruppe* von E über K.

8.1.3 Beispiel. $\mathrm{Gal}(\,\mathbb{Q}(\sqrt{5})/\mathbb{Q}\,)$ enthält neben der identischen Abbildung eine weitere Funktion, nämlich die Abbildung, die jedes $a + b\sqrt{5}$ $(a, b \in \mathbb{Q})$ auf $a - b\sqrt{5}$ abbildet.

8.1.4 Notation. Das Tripel

$$(\,E,\ \mathrm{Gal}(E/K),\ \{(a,\varphi) \in E \times \mathrm{Gal}(E/K)) \mid \varphi(a) = a\}\,)$$

heißt die Galois-Verbindung der Erweiterung $K \leq E$.
Für jede Menge $X \subseteq E$ schreiben wir statt $X^{\uparrow}$ deutlicher $\mathrm{Gal}(E/X)$; für $Y \subseteq \mathrm{Gal}(E/K)$ schreiben wir statt $Y^{\downarrow}$ deutlicher $\mathrm{Fix}_E(Y)$:

$$\mathrm{Gal}(E/X) := \{\,\varphi \in \mathrm{Gal}(E/K) \mid \varphi{\restriction}X = id\,\}$$
$$\mathrm{Fix}_E(Y) := \{\,a \in E \mid \forall \varphi \in Y\ \varphi(a) = a\,\}$$

Man sieht leicht, dass $\mathrm{Gal}(E/X)$ für beliebiges $X \subseteq E$ eine Untergruppe von $\mathrm{Gal}(E/K)$ ist; ebenso ist für $Y \subseteq \mathrm{Gal}(E/K)$ die Menge $\mathrm{Fix}_E(Y)$ immer ein Unterkörper von E, der K enthalten muss.
Daraus folgt, dass $\mathrm{Fix}_E(\mathrm{Gal}(E/X))$ immer den Körper $K(X)$ enthält, und $\mathrm{Gal}(E/\mathrm{Fix}_E(Y))$ immer die von Y erzeugte Untergruppe von $\mathrm{Gal}(E/K)$.

8.2 Separable Erweiterungen

8.2.1 Definition. $f \in K[x] \setminus \{0\}$, f irreduzibel, heißt *separabel* $:\Leftrightarrow$ jede Nullstelle von f im Zerfällungskörper von f ist einfach, oder anders gesagt: In einer geeigneten Körpererweiterung zerfällt f in lauter verschiedene Linearfaktoren.

8.2.2 Anmerkung. f separabel $\Leftrightarrow \mathrm{ggT}(f(x), f'(x)) = 1$, denn:

[1] Mengentheoretisch korrekt ist A eine Klasse. Wenn das nicht erwünscht ist, kann man sich auf jene Algebren in A einschränken, deren Grundmenge Teilmenge einer fest vorgegebenen Menge ist.

„⇐“: Übungsbeispiel.
„⇒“: Im Zerfällungskörper von f sei $f(x) = \prod_{i=1}^{n}(x-\alpha_i)$. Angenommen, $\mathrm{ggT}(f(x), f'(x)) \neq 1 \Rightarrow f(x), f'(x)$ haben gemeinsame Nullstelle, etwa α_1, also $f(x) = (x-\alpha_1)g(x)$, $g(\alpha_1) \neq 0$, $f'(x) = g(x) + (x-\alpha_1)g'(x) \Rightarrow f'(\alpha_1) \neq 0$, Widerspruch!

8.2.3 Lemma. *Sei f irreduzibel über K. Dann gilt:*

$$p(x) := \mathrm{ggT}(f(x), f'(x)) \neq 1 \Leftrightarrow p(x) = f(x) \Leftrightarrow f(x) | f'(x) \Leftrightarrow f'(x) = 0\,.$$

Beweis. Übungsbeispiel. □

8.2.4 Definition. Sei $K \leq E$. Das Element $u \in E$ heißt *separabel* (über K): $\Leftrightarrow$ u ist algebraisch und das Minimalpolynom von u (über K) ist separabel.

$K \leq E$ heißt *separable Erweiterung* $:\Leftrightarrow \forall u \in E : u$ ist separabel über K.

8.2.5 Satz. *a)* $\mathrm{char}\, K = 0 \Rightarrow$ *alle irreduziblen Polynome über K sind separabel.*
b) Für $\mathrm{char}\, K = p > 0$ *gilt: Ein irreduzibles Polynom* $f(x) = \sum_{i=0}^{n} a_i x^i$ *ist separabel* $\Leftrightarrow$ $a_i \neq 0$ *für mindestens ein* $i \not\equiv 0 \bmod p$.

Beweis. Folgt aus dem vorhergehenden Lemma. □

Sei $f(x) \in K[x]$ irreduzibel und nicht separabel, $\mathrm{char}\,(K) = p$. Dann ist $f(x)$ von der Form $\sum_{i=0}^{n} a_i x^{pi}$; wenn wir $f_1(y) := \sum_{i=1}^{n} a_i y^i$ setzen, erhalten wir also $f(x) = f_1(x^p)$. Man sieht leicht, dass f_1 auch irreduzibel ist, denn jede Zerlegung von f_1 induziert eine Zerlegung von f.
Wenn nun f_1 auch nicht separabel ist, können wir die vorige Überlegung auf f_1 anwenden und erhalten $f_2(z)$ mit $f_1(y) = f_2(y^p)$, also $f(x) = f_2(y^{p^2})$. Wenn nötig, setzen wir diesen Prozess fort und erhalten schließlich ein irreduzibles *separables* Polynom $f_k(t)$ mit $f(x) = f_k(x^{p^k})$.
Sei n der Grad von f_k, dann hat f den Grad np^k. Im Zerfällungskörper von $f \cdot f_k$ hat f_k genau n verschiedene Nullstellen $\alpha_1, \ldots, \alpha_n$:

$$f(x) = f_k(x^{p^k}) = \prod_{i=1}^{n} (x^{p^k} - \alpha_i).$$

f hat dann ebenfalls n verschiedene Nullstellen $\beta_1, \ldots, \beta_n$, wobei $\beta_i^{p^k} = \alpha_i$ gilt. Jede dieser Nullstellen tritt mit Vielfachheit p^k auf, denn $x^{p^k} - \alpha_i = x^{p^k} - \beta_i^{p^k} = (x - \beta_i)^{p^k}$.

8.3 Normale Erweiterungen

8.3.1 Definition. Sei $K \leq E$ algebraisch. E heißt *normal* über $K :\Leftrightarrow$ *jedes* irreduzible $f \in K[x]$, welches eine Nullstelle in E hat, zerfällt ganz in E.

8.3.2 Satz. *Sei $K \leq E$, $[E : K] < \infty$. Dann sind folgende Aussagen äquivalent:*

(i) $K \leq E$ normal.

(ii) E ist Zerfällungskörper eines Polynoms $g(x) \in K[x]$.

Beweis. (i) $\Rightarrow$ (ii): E ist Zerfällungskörper (über K) der Menge der Minimalpolynome aller Elemente von E. Wegen $[E : K] < \infty$ reichen schon endlich viele $g_1, \ldots, g_t$ aus, und wir können $g(x) = \prod_{i=1}^{t} g_i(x)$ setzen.
(ii) $\Rightarrow$ (i): Sei umgekehrt E Zerfällungskörper von $g(x) = \prod_{i=1}^{t} g_i(x) \in K[x]$ über K, wobei die g_i irreduzibel über K sind. Sei $f \in K[x]$ ein weiteres *irreduzibles* Polynom, $f(u) = 0$, $u \in E$. Sei F Zerfällungskörper von $f(x)$ über K, F^* Zerfällungskörper von $f(x) \cdot g(x)$ über K mit $F^* = E(v_1, \ldots, v_r)$, wobei $v_1, \ldots, v_r$ die Nullstellen von $f(x)$ sind (F^* ist Zerfällungskörper von $f(x)$ über E). Sei v eine Nullstelle von $f(x)$ in F^*.
Behauptung: $v \in E$.
Es gibt einen Isomorphismus $\sigma : \left\{ \begin{array}{ccc} F^* & \to & F^* \\ a & \mapsto & a, \quad \forall a \in K \\ u & \mapsto & v \end{array} \right.$.
Behauptung: $\sigma(E) = E$.
$E = K(\alpha_1, \ldots, \alpha_n)$, wobei die α_i sämtliche Nullstellen von $g(x) \in K[x]$ sind. $\sigma(g(\alpha_i)) = g(\sigma(\alpha_i)) = 0 \Rightarrow \sigma$ permutiert die Menge $\{\alpha_1, \ldots, \alpha_n\} \Rightarrow \sigma(E) = \sigma(K(\alpha_1, \ldots, \alpha_n)) = K(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)) = E \Rightarrow v \in E$. □

8.3.3 Satz. *Sei $K \leq L$, $\alpha \in L$ algebraisch über K mit Minimalpolynom $m(x) \in K[x]$. Dann sind die folgenden Aussagen äquivalent:*

- *$K(\alpha)$ ist normal über K. (Wir sagen in diesem Fall: „α ist normal über K.“)*
- *$m(x)$ zerfällt in L in Linearfaktoren.*

Beweis. Wenn $K(\alpha)$ normal über K ist, dann zerfällt jedes irreduzible Polynom $p(x) \in K[x]$ über $K(\alpha)$ in Linearfaktoren, also insbesondere auch $m(x)$.
Wenn umgekehrt $m(x)$ in Linearfaktoren zerfällt, dann enthält $K(\alpha)$ den Zerfällungskörper Z von $m(x)$ über K. Z muss aber auch die Nullstelle α enthalten, also $K(\alpha) = Z$. Nach dem vorigen Satz ist Z normal. □

8.3.4 Beispiel. Seien $\alpha, \beta, \gamma \in \mathbb{C}$ die drei Nullstellen des Gleichung $x^3 - 2$, $\alpha := \sqrt[3]{2}$. Dann ist $\mathbb{Q}(\alpha)$ nicht normal über $\mathbb{Q}$, denn in diesem Körper ist $x^3 - 2 = (x - \alpha)(x^2 + \alpha x + \alpha^2)$, wobei der zweite Faktor irreduzibel ist. Die Erweiterung $\mathbb{Q}(\alpha, \beta, \gamma)$ ist der Zerfällungskörper von $x^3 - 2$ über $\mathbb{Q}$, also normal.

8.3.A Die Galois-Gruppe separabler normaler einfacher Erweiterungen

Zur Erinnerung wiederholen wir 6.4.14(e) (siehe auch 6.5.5):

8.3.5 Lemma. *Sei $K \leq L_1$, $K \leq L_2$, $\alpha_\ell \in L_\ell$, und sei $p(x) \in K[x]$ irreduzibles Polynom mit $p(\alpha_\ell) = 0$ für $\ell = 1, 2$.*
Dann gibt es genau einen Isomorphismus $\psi : K(\alpha_1) \to K(\alpha_2)$ mit $\psi(\alpha_1) = \alpha_2$ und $\psi \restriction K = id$.

Beweis. Es ist klar, dass es höchstens ein solches ψ geben kann.
Sei n der Grad von $p(x)$, I das von $p(x)$ erzeugte Ideal. Dann sind die Abbildungen

$$\varphi_\ell : K[x]/I \to K(\alpha_\ell),$$

die durch $\varphi_\ell(f(x) + I) = f(\alpha_\ell)$ definiert sind, Isomorphismen. Die Abbildung $\psi : \varphi_2 \circ \varphi_1^{-1}$ erfüllt offenbar $\psi(\alpha_1) = \alpha_2$ und ist Isomorphismus. □

8.3.6 Satz. *Sei $K \leq L$, $\alpha \in E$ algebraisch vom Grad n über K, $E := K(\alpha)$. Dann hat die Gruppe* $\mathrm{Gal}(E/K)$ *höchstens n Elemente, und es gilt $|\mathrm{Gal}(E/K)| = n$ genau dann, wenn E normal und separabel über K ist.*

Beweis. Sei $m(x)$ das Minimalpolynom von α über K, und seien $\alpha_1, \ldots, \alpha_k$ alle (verschiedenen) Nullstellen von $m(x)$ in E, $\alpha_1 = \alpha$.
Dann gilt:

1. $k \leq n$.
2. Wenn α nicht separabel ist, dann ist $k < n$.
3. Wenn α nicht normal ist, dann ist $k < n$.
4. Wenn α separabel und normal ist, dann ist $k = n$.
5. $\mathrm{Gal}(E/K)$ hat genau k Elemente.

1.–4. sind offensichtlich. (Anmerkung: $E = K(\alpha)$ ist genau dann separabel bzw. normal, wenn α separabel bzw. normal ist.)
Für jedes Element $\varphi \in \mathrm{Gal}(E/K)$ muss $0 = \varphi(0) = \varphi(m(\alpha)) = m(\varphi(\alpha))$ gelten, also $\varphi(\alpha) \in \{\alpha_1, \ldots, \alpha_k\}$.
Jedes Element $\beta \in E = K(\alpha)$ lässt sich eindeutig als

$$\beta = b_0 + \cdots + b_{n-1}\alpha^{n-1}$$

darstellen. Für den Wert von $\varphi(\alpha)$ gibt es also höchstens k Möglichkeiten, und das Verhalten des Automorphismus φ auf $E = K(\alpha)$ ist durch den Wert $\varphi(\alpha)$ schon festgelegt. Daher gilt $|\mathrm{Gal}(E/K)| \leq k$.
Umgekehrt ist nach dem gerade bewiesenen Lemma

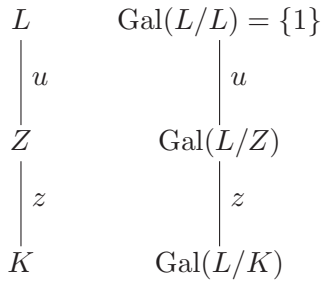
$$\varphi_i : \; b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} \mapsto b_0 + b_1\alpha_i + \cdots + b_{n-1}\alpha_i^{n-1}$$

ein Isomorphismus von $K(\alpha)$ auf $K(\alpha_i)$.
Es gilt $K(\alpha_i) \subseteq E = K(\alpha)$, aber weil die K-Vektorräume $K(\alpha)$ und $K(\alpha_i)$ dieselbe Dimension haben, ist $K(\alpha_i) = K(\alpha)$. Daher ist $\varphi_i \in \mathrm{Gal}(E/K)$, also $|\mathrm{Gal}(E/K)| = k$. □

8.4 Hauptsatz der Galois-Theorie

8.4.1 Lemma. *Sei $K \leq Z \leq L$, L normal und separabel über K, $[L : Z] = u$, $[Z : K] = z$. Dann gilt:*

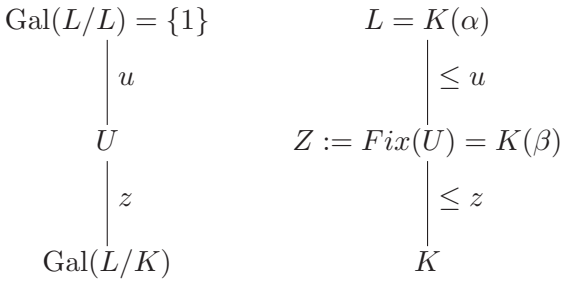
1. $|\mathrm{Gal}(L/K)| = zu$.
2. *L ist normal über Z.*
3. $|\mathrm{Gal}(L/Z)| = u$.
4. $\mathrm{Gal}(L/Z)$ *ist eine Untergruppe von* $\mathrm{Gal}(L/K)$ *mit z Nebenklassen.*



Beweis. 1. Nach dem Gradsatz ist $[L : K] = zu$; weil L normal, separabel und endlich über K ist, muss $\mathrm{Gal}(L/K)$ zu Elemente haben.
2. L ist normal über K, also Zerfällungskörper eines Polynoms $p(x) \in K[x]$ über K. Damit ist L auch Zerfällungskörper dieses Polynoms über Z, also normal über Z.
3. Analog zu 1.
4. Offensichtlich ist $\mathrm{Gal}(L/Z)$ Untergruppe von $\mathrm{Gal}(L/K)$. Nach dem Satz von Lagrange hat $\mathrm{Gal}(L/Z)$ dann $zu/u = z$ Nebenklassen. □

8.4.2 Lemma. *Sei $K \leq L$, L normal und separabel über K, $[L : K] = zu$. Sei $U \leq \mathrm{Gal}(L/K)$ mit u Elementen, und sei $Z := Fix_L(U)$. Dann gibt es ein $\beta \in Fix_L(U)$ mit $\mathrm{Fix}_L(U) = K(\beta)$, weiters gibt es ein $\alpha \in L$ mit $L = K(\alpha) = Z(\alpha)$, und es gilt:*

1. *U hat u Elemente und z Nebenklassen.*
2. *β hat (über K) höchstens z Konjugierte.*
3. $[Z : K] \leq z$.
4. *α hat über Z höchstens Grad u.*
5. $[L : Z] \leq u$.
6. $[L : Z] = u$, $[Z : K] = z$.



Beweis. 1. Die Gruppe $\mathrm{Gal}(L/K)$ hat zu Elemente. Wegen $|U| = u$ folgt $|G/U| = z$.
2. Seien β, β' konjugiert über K (wobei β' im Zerfällungskörper des Minimalpolynoms von β liegt; β' muss also nicht notwendigerweise in $K(\beta)$ liegen, wohl aber in L). Dann gibt es $\sigma \in \mathrm{Gal}(L/K)$ mit $\sigma(\beta) = \beta'$. Jeder Automorphismus τ in der Nebenklasse σU bildet β ebenfalls auf β' ab, denn $\tau = \sigma \circ \upsilon$ für ein $\upsilon \in U$, also $\tau(\beta) = \sigma(\upsilon(\beta)) = \sigma(\beta)$. Daher gibt es höchstens so viele Konjugierte wie Nebenklassen, also hat β höchstens z Konjugierte.
3. β ist zu allen Nullstellen seines (separablen) Minimalpolynoms konjugiert; daher hat dieses Polynom höchstens Grad z.
4. Wir betrachten das Polynom $p(x) := \prod_{\sigma \in U}(x - \sigma(\alpha))$. Dieses Polynom liegt zunächst in $L[x]$; wir behaupten, dass alle Koeffizienten von p aber schon in Z liegen:
Sei $\tau \in U$. Dann ist

$$\tau(p(x)) = \tau \prod_{\sigma \in U}(x - \sigma(\alpha)) = \prod_{\sigma \in U}(x - (\tau \circ \sigma)(\alpha)) = \prod_{\sigma' \in U}(x - \sigma'(\alpha)) = p(x),$$

weil die Abbildung $\sigma \mapsto \tau \circ \sigma$ eine Bijektion von U nach U ist. Also ist $p(x)$ unter allen Automorphismen aus U invariant.

Da α Nullstelle des Polynoms $p(x) \in L[x]$ (vom Grad u) ist, kann der Grad von α höchstens u sein.
5. Folgt aus 4.
6. Folgt aus 3. und 5., weil $[L : K] = zu$.

□

8.4.3 Satz (Hauptsatz)**.** *Sei $K \leq L$, L eine endliche separable normale Erweiterung von K. Dann ist die Abbildung $Z \mapsto \mathrm{Gal}(Z/K)$ eine bijektive (antitone) Abbildung von den Zwischenkörpern Z ($K \leq Z \leq L$) auf die Untergruppen der endlichen Gruppe $\mathrm{Gal}(L/K)$. Die Umkehrabbildung wird durch $U \mapsto Fix_L(U)$ gegeben.*
Wenn $[L : K] = n$ ist, und $U \leq \mathrm{Gal}(L/K)$ eine Untergruppe vom Index z, dann hat der zugehörige Zwischenkörper Grad z über K.
Weiters gilt: Eine Untergruppe $U \leq \mathrm{Gal}(L/K)$ ist genau dann Normalteiler, wenn der zugehörige Zwischenkörper normal über K ist; zu konjugierten Untergruppen gehören konjugierte Zwischenkörper, das heißt: Wenn $U_1 = \sigma^{-1}U_2\sigma$ für ein $\sigma \in \mathrm{Gal}(L/K)$, dann ist $\sigma(Fix(U_1)) = Fix(U_2)$.

Beweis. Sei $K \leq Z \leq L$, mit $[Z : K] = z$, $[L : Z] = u$, $zu = n$. Dann ist (nach dem ersten Lemma) $\mathrm{Gal}(L/Z)$ eine Untergruppe von $\mathrm{Gal}(L/K)$ mit u Elementen und Index z. Sei $\hat{Z} := Fix_L(\mathrm{Gal}(L/Z))$; dann ist (nach dem zweiten Lemma) $\hat{Z}$ ein Zwischenkörper vom Grad z über K.
$\hat{Z}$ ist der Galois-Abschluss von Z, also gilt $Z \subseteq \hat{Z}$. Da aber $\hat{Z}$ dieselbe endliche Dimension über K hat wie Z, muss $\hat{Z} = Z$ gelten.
Ganz analog zeigt man, dass die Abbildung $U \mapsto Fix_Z(U) \mapsto \mathrm{Gal}(L/Fix_Z(U))$ jede Untergruppe U auf sich selbst abbildet.
Die Gleichung zwischen Index einer Untergruppe und Grad der entsprechenden Körpererweiterung folgt ebenfalls leicht aus den bereits bewiesenen Lemmata.
Die Charakterisierung der normalen Zwischenkörper durch Normalteiler überlassen wir dem Leser. □

8.4.4 Anmerkung. Die Endlichkeit der Erweiterung war an einigen Stellen unentbehrlich für den Beweis. Man kann eine analoge Galois-Verbindung zwar auch für Erweiterungen unendlichen Grads definieren, aber man kann dann nicht zeigen, dass alle Untergruppen der Galois-Gruppe auch abgeschlossen sind.

8.4.5 Beispiel. Sei $K := GF(p)$, $L := GF(p^\infty)$. Sei σ die durch $\sigma(a) = a^p$ definierte Abbildung. Dann ist σ ein Automorphismus von L mit $\sigma \restriction K = id$, also $\sigma \in \mathrm{Gal}(L/K)$.

Sei $\Sigma := \langle\sigma\rangle$. Dies ist eine Untergruppe von $\mathrm{Gal}(L/K)$. Ihr Fixkörper ist aber nur K selbst, folglich ist $\mathrm{Gal}(L/Fix(\Sigma)) = \mathrm{Gal}(L/K)$. $\mathrm{Gal}(L/K)$ ist also die kleinste Galois-abgeschlossene Gruppe, die Σ enthält. Daher ist Σ nicht Galois-abgeschlossen, denn man kann zeigen, dass $\Sigma \neq \mathrm{Gal}(L/K)$ ist. (Es gilt sogar, dass $\mathrm{Gal}(L/K)$ überabzählbar ist.)
Die folgende Abbildung τ ist in $\mathrm{Gal}(L/K) \setminus \Sigma$: Wir definieren zunächst rekursiv eine Folge von natürlichen Zahlen:

$$n_1 := 0,\ n_2 := 0 + 1! = 1,\ n_3 := 1 + 2! = 3,\ n_4 := 3 + 3! = 9, \ldots, n_{k+1} := n_k + k!, \ldots$$

Sei nun $\tau_k : GF(p^{k!}) \to GF(p^{k!})$ durch $\tau_k(a) = \sigma^{n_k}(a)$ definiert. Dann ist τ_k ein Automorphismus von $GF(p^{k!})$, und man kann leicht zeigen, dass $\tau_k \restriction GF(p^{(k-1)!}) = \tau_{k-1}$ gilt. Daher gibt es einen Automorphismus τ von $GF(p^\infty)$, der

$$\forall k :\ \tau \restriction GF(p^{k!}) = \tau_k$$

erfüllt. Für jedes k kann man auch sehen, dass τ_k bereits auf der Menge $GF(p^k)$ mit keiner Funktion aus $\{\sigma^{-k}, \ldots, id, \sigma, \ldots, \sigma^k\}$ übereinstimmt, daher ist $\tau \notin \Sigma$.

8.5 Konstruierbarkeit mit Zirkel und Lineal

8.5.1 Definition. Sei A eine nichtleere Menge von Punkten in der Ebene $\mathbb{R} \times \mathbb{R}$. 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 in der Ebene, oder eine Gerade, oder ein Kreis, 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 der Durchschnitt von X_{j_1} und X_{j_2} ist, wobei X_{j_1} ein Kreis oder eine Gerade ist, ebenso X_{j_2}.

3. Wenn X_i eine Gerade g ist, dann geht g durch zwei vorher konstruierte Punkte, d.h., es gibt zwei verschiedene Punkte $p_1 = X_{j_1}$ $p_2 = X_{j_2}$ (mit $j_1, j_2 < i$), 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 $j_1, j_2 < i$, sodass $M = X_{j_1}$ und $r = X_{j_2}$.

5. Wenn X_i eine Zahl z ist, dann ist z die Distanz zwischen zwei früher konstruierten Punkten, d.h., es gibt $j_1, j_2 < i$ (nicht notwendigerweise verschieden), sodass $p_1 := X_{j_1}$ und $p_2 := X_{j_2}$ Punkte mit Abstand z sind.

Üblicherweise enthält die Menge A zumindest den Ursprung und den Punkt $(0, 1)$.
Wir nennen einen Punkt / eine Gerade / eine Zahl „konstruierbar aus A“, wenn der Punkt / die Gerade / die Zahl in einer Konstruktion aus A vorkommen.

Um die Koordinaten (oder deren Distanzen) von konstruierbaren Punkten zu berechnen, muss man offensichtlich endlich oft entweder ein lineares Gleichungssystem (wenn man Geraden mit Geraden schneidet) oder eine quadratische Gleichung lösen (wenn man Kreise mit Kreisen, oder Kreise mit Geraden schneidet). Umgekehrt kann man (zum Beispiel) Höhensatz und Thaleskreis verwenden, um aus einer bereits konstruierten positiven Zahl ihre Quadratwurzel zu konstruieren.
Dies legt folgenden Definition nahe:

8.5.2 Definition. Sei K Körper. Unter eine Quadratwurzelerweiterung von K verstehen wir einen Erweiterungskörper $L \geq K$, für den es eine endliche Folge $K = K_1 \leq K_2 \leq \cdots \leq K_n = L$ gibt, die für $i = 1, \ldots, n-1$ erfüllt: Es gibt $\alpha \in K_{i+1}$, sodass $K_{i+1} = K_i(\alpha)$, und $\alpha^2 \in K_i$, oder äquivalent $[K_{i+1} : K_i] \leq 2$.

8.5.3 Lemma. *Sei L Quadratwurzelerweiterung von K. Dann gibt es eine natürliche Zahl n mit $[L : K] = 2^n$.*

8.5.4 Anmerkung. Nicht jeder Erweiterungskörper von $\mathbb{Q}$, dessen Grad über $\mathbb{Q}$ eine Zweiterpotenz ist, ist eine Quadratwurzelerweiterung von $\mathbb{Q}$.

8.5.5 Satz. *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*[2] *Zahlen bilden eine 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 $A \supseteq \{(0,0),(1,0)\}$ eine Menge von Punkten, und 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.*

8.5.6 Folgerung. Sei A eine Menge von Punkten, die alle rationale Koordinaten haben. Dann gilt:

1. $\sqrt[3]{2}$ ist nicht aus A konstruierbar.

2. Keine transzendente Zahl (wie[3] etwa π)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 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 Dreiceck 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 $\cos(60°) = 4\cos^3(20°) - 3\cos(20°)$, daher ist α Nullstelle des Polynoms $4x^3 - 3x - \frac{1}{2}$. Da dieses Polynom dritten Grades keine rationalen Nullstellen hat, ist es über $\mathbb{Q}$ irreduzibel, somit ist $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Wie in (1) folgt nun, dass α nicht aus A konstruierbar ist. □

[2] 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.

[3] Dass die Ludolphsche Zahl tatsächlich transzendent ist, werden wir in dieser Vorlesung nicht beweisen.

Kapitel 9

Verbände und Boolesche Algebren

9.1 (Halb-)Geordnete Mengen

In 1.6.1 haben wir definiert: Sei M eine Menge und R eine zweistellige Relation auf M mit

1) $\forall x \in M : xRx$ (Reflexivität),

2) $\forall x, y \in M : xRy \wedge yRx \Rightarrow x = y$ (Antisymmetrie),

3) $\forall x, y, z \in M : xRy \wedge yRz \Rightarrow xRz$ (Transitivität),

dann heißt R eine *Halbordnung* auf M. Weiters heißt (M, R) eine *halbgeordnete* Menge. Gilt zusätzlich

4) $\forall x, y \in M : xRy \vee yRx$ (Vergleichbarkeit),

dann heißt (M, R) eine *Kette* oder *linear geordnete* Menge oder *Totalordnung*.

9.1.1 Anmerkung. Statt „Halbordnung“ sagt man oft auch „partielle Ordnung“, abgekürzt po oder p.o., manchmal auch nur „Ordnung“.[1] Diese Ausdrücke werden sowohl für die Relation R selbst wie auch für die gesamte Struktur (M, R) verwendet.
Gelegentlich ist mit „Ordnung“ auch eine *Totalordnung* (=*lineare Ordnung*, *Kette*[2]) gemeint.

Bezeichnungen. Statt R wird meist „$\leq$“ geschrieben. Weiters sei:

$$\begin{aligned} x \geq y &:\Leftrightarrow y \leq x, \\ x < y &:\Leftrightarrow x \leq y,\ x \neq y, \\ x > y &:\Leftrightarrow x \geq y,\ x \neq y. \end{aligned}$$

9.1.2 Anmerkung. Für $A, B \subseteq M$ schreiben wir $A \leq B$ für $\forall x \in A \forall y \in B\ (x \leq y)$. Statt „$a \leq x$ und $b \leq x$“ schreiben wir also $\{a, b\} \leq x$ oder meist weiter abgekürzt „$a, b \leq x$“; analog ist $x \leq a, b$ zu verstehen.
Statt „$a \leq b$ und $b \leq c$“ schreiben wir oft $a \leq b \leq c$.

Eine *strikte Halbordnung* auf einer Menge M ist eine zweistellige Relation S, die

1. areflexiv ($\forall x \in M\, (x, x) \notin R$) und

2. transitiv

[1] englisch: *order oder partial order*
[2] englisch: *: total order, linear order, chain*

ist. Wenn S eine strikte Halbordnung ist, dann ist $S \cup \{(x,x) \mid x \in M\}$ eine Halbordnung; wenn R eine Halbordnung ist, dann ist $R \setminus \{(x,x) \mid x \in M\}$ eine strikte Halbordnung. Jeder Satz über Ordnungen lässt sich also in einen Satz über strikte Ordnungen übersetzen, und umgekehrt.
Gelegentlich ist mit dem Wort „Ordnung“ oder „Halbordnung“ 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 Areflexivität einer Relation zu betonen, verwendet man auch gerne Symbole wie $\subsetneqq$.

9.1.3 Beispiele. 1) $(\mathbb{R}, \leq)$ ist Kette.

2) $(\mathbb{N}_0, |)$ ist halbgeordnete Menge, aber keine Kette.

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

9.1.4 Definition. Sei $(M, \leq)$ halbgeordnete Menge. Dann heißt $k \in M$ *kleinstes* (bzw. *größtes*) Element von $M :\Leftrightarrow \forall x \in M : k \leq x$ (bzw. $k \geq x$).

9.1.5 Beispiele. 1) $(\mathbb{R}, \leq)$ hat kein kleinstes bzw. größtes Element.

2) $(\mathbb{N}_0, |)$ hat 1 als kleinstes und 0 als größtes Element.

3) $(\mathfrak{P}(M), \subseteq)$ hat $\emptyset$ als kleinstes und M als größtes Element.

9.1.6 Anmerkung. Es gibt stets höchstens ein kleinstes bzw. größtes Element, denn: sind k_1, k_2 kleinste Elemente, dann gilt $k_1 \leq k_2 \wedge k_2 \leq k_1$ und damit $k_1 = k_2$. Analog für größte Elemente.

9.1.7 Definition. Sei $(M, \leq)$ halbgeordnete Menge. Dann heißt $m \in M$ *minimales* (bzw. *maximales*) Element von $M :\Leftrightarrow \forall x \in M : x \leq m$ (bzw. $x \geq m$) $\Rightarrow x = m$.

Jedes kleinste Element ist auch minimal, jedes größte auch maximal.

9.1.8 Satz. *a) Sei $(M, \leq)$ halbgeordnete Menge und $N \subseteq M$. Dann ist $(N, \leq)$ ebenfalls eine halbgeordnete Menge. Ist $(M, \leq)$ eine Kette, dann auch $(N, \leq)$. Dabei steht $(N, \leq)$ abkürzend für $(N, \leq \cap (N \times N))$.*

b) Ist $(M, \leq)$ halbgeordnete Menge, dann auch $(M, \geq)$. („Dualitätsprinzip für halbgeordnete Mengen“) □

Duale 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 $(M, \geq)$.

9.1.9 Definition. Sei $(M, \leq)$ halbgeordnete Menge und $N \subseteq M$. Dann heißt $u \in M$ eine *untere Schranke* von $N :\Leftrightarrow \forall x \in N : u \leq x$. Ein größtes Element der Menge aller unteren Schranken heißt ein *Infimum* von N, in Zeichen: $\inf N$ oder $\bigwedge N$. Ein Element $v \in M$ heißt eine *obere Schranke* von $N :\Leftrightarrow \forall x \in N : x \leq v$, und eine kleinste obere Schranke heißt ein *Supremum* von N, in Zeichen: $\sup N$ oder $\bigvee N$.

9.1.10 Beispiele. 1) In $(\mathbb{R}, \leq)$ entsprechen die eben definierten Begriffe den in der Analysis üblichen.

2) In $(\mathbb{N}_0, |)$ gilt für $T \subseteq \mathbb{N}_0$ mit $T \neq \emptyset$: $\inf T = \mathrm{ggT}(T)$ und $\sup T = \mathrm{kgV}(T)$. Weiters ist $\inf \emptyset = 0$ und $\sup \emptyset = 1$.

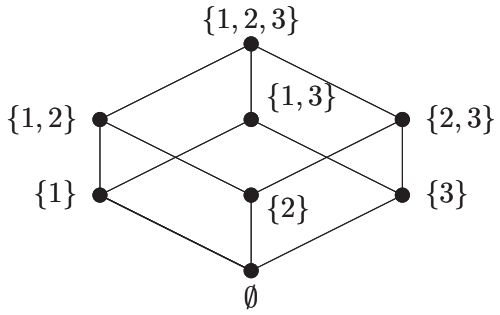
3) In $(\mathfrak{P}(M), \subseteq)$ gilt für $\mathfrak{S} \subseteq \mathfrak{P}(M)$: $\inf \mathfrak{S} = \bigcap \mathfrak{S}$ und $\sup \mathfrak{S} = \bigcup \mathfrak{S}$.

Hassediagramm. Sei $(M, \leq)$ eine endliche halbgeordnete Menge und die Relation „benachbart“ definiert durch:

$$a, b \text{ benachbart } :\Leftrightarrow \begin{cases} 1)\ a < b \text{ oder } b < a, \\ 2)\ \text{es gibt kein } c \text{ mit } a < c < b \text{ oder } b < c < a. \end{cases}$$

Dann ist das Hassediagramm von $(M, \leq)$ gegeben durch den Graphen der Relation „benachbart“. (Knotenmenge M; ist $a < b$, zeichnet man den Knoten a „tiefer“ als den Knoten b und verbindet a und b mit einer Kante, falls sie benachbart sind.)

9.1.11 Beispiel. Das Hassediagramm für $(\mathfrak{P}(\{1,2,3\}), \subseteq)$ sieht so aus:



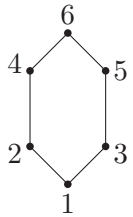
9.2 (Halb-)Ordnungen und Verbände

9.2.1 Definition. Sei $(V, \leq)$ eine halbgeordnete Menge. $(V, \leq)$ heißt *verbandsgeordnet* $:\Leftrightarrow$ $\sup\{a, b\}$ und $\inf\{a, b\}$ existieren für alle $a, b \in V$.

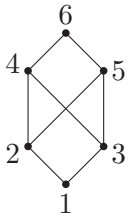
Statt „verbandsgeordnete Menge“ kann man auch *Verband im ordnungstheoretischen Sinn* sagen; die im Abschnitt 1.2 definierten Verbände $(V, \wedge, \vee)$ nennt man dann „Verbände im algebraischen Sinn“.

9.2.2 Beispiel. Auf $M = \{1, 2, 3, 4, 5, 6\}$ seien zwei Halbordnungsrelationen $\leq$ und $\leq'$ definiert.

$(M, \leq)$:



$(M, \leq')$:



$(M, \leq)$ ist verbandsgeordnet (z. B. ist $\inf\{2, 3\} = 1$ und $\sup\{2, 3\} = 6$). Dagegen ist $(M, \leq')$ *nicht* verbandsgeordnet: $\sup\{2, 3\}$ existiert nicht, da die Menge $\{2, 3\}$ die oberen Schranken 4, 5 und 6, also keine kleinste obere Schranke besitzt.

9.2.3 Lemma. *Sei $(V, \wedge, \vee)$ ein Verband, dann gilt:*

a) $\forall a \in V : a \wedge a = a = a \vee a$,

b) $\forall a, b \in V : a \wedge b = a \Leftrightarrow a \vee b = b$.

Beweis. a) Aufgrund der Verschmelzungsgesetze gilt: $a \wedge a = a \wedge (a \vee (a \wedge a)) = a$ und $a \vee a = a \vee (a \wedge (a \vee a)) = a$.

b) $\Rightarrow$: $a \vee b = (a \wedge b) \vee b = b$, $\Leftarrow$: $a \wedge b = a \wedge (a \vee b) = a$, ebenfalls nach den Verschmelzungsgesetzen. □

9.2.4 Satz.

(*a*) *Sei* $(V, \wedge, \vee)$ *ein Verband. Definiert man eine Relation* $\leq$ *auf* V *durch*

$$\forall a, b \in V : \quad a \leq b :\Leftrightarrow a \wedge b = a,$$

dann ist $(V, \leq)$ *eine verbandsgeordnete Menge, wobei* $a \wedge b = \inf\{a, b\}$, $a \vee b = \sup\{a, b\}$.

(*b*) *Sei* $(V, \leq)$ *eine verbandsgeordnete Menge. Definiert man auf* V *zweistellige Operationen* $\wedge, \vee$ *durch*

$$\forall a, b \in V : \qquad a \wedge b := \inf\{a, b\}, \ a \vee b := \sup\{a, b\},$$

dann ist $(V, \wedge, \vee)$ *ein Verband.*

(*c*) *Die in (a) und (b) definierten Zuordnungen sind zueinander invers.*

Beweis. (a) Die Relation $\leq$ ist reflexiv ($a \leq a$ wegen $a \wedge a = a$), antisymmetrisch ($a \leq b \leq a \Rightarrow a \wedge b = a$ und $a \wedge b = b$, also $a = b$) und transitiv ($a \leq b \leq c \Rightarrow a \wedge b = a$, $b \wedge c = b$, daher $a \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge b = a$).

Wir zeigen nun, dass $a \wedge b = \inf\{a, b\}$ gilt: $a \wedge b \leq a, b$ gilt wegen $a \wedge b \wedge a = a \wedge b \wedge b = a \wedge b$; aus $x \leq a, b$ folgt $a \wedge x = b \wedge x = x$, also $(a \wedge b) \wedge x = a \wedge (b \wedge x) = a \wedge x = x$, daher $x \leq a \wedge b$.
Die Beziehung $a \vee b = \sup\{a, b\}$ zeigt man ganz ähnlich.

(b) Wir müssen zeigen, dass die Verbandsgesetze gelten:

$a \wedge b = \inf\{a, b\} = \inf\{b, a\} = b \wedge a$.

Wir überlegen zunächst, dass jede untere Schranke s von $\{a, b, c\}$ auch untere Schranke von $\{a, b \wedge c\}$ ist, und umgekehrt:

$s \leq a, b, c \Rightarrow s \leq a$ und $s \leq b \wedge c = \inf\{b, c\}$;
wenn umgekehrt $s \leq a$ und $s \leq b \wedge c$, dann ist $s \leq a, b, c$.

Daher ist die größte untere Schranke von a, b, c auch gleich der größten unteren Schranke von a und $b \wedge c$:

$$a \wedge (b \wedge c) = \inf\{a, b, c\}.$$

Analog ist auch $(a \wedge b) \wedge c = \inf\{a, b, c\}$, also $(a \wedge b) \wedge c = \inf\{a, b, c\} = a \wedge (b \wedge c)$.

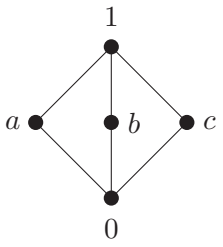
Analog zeigt man die dualen Gesetze.

(c) $(V, \wedge, \vee) \overset{\text{a)}}{\longmapsto} (V, \leq) \overset{\text{b)}}{\longmapsto} (V, \wedge^*, \vee^*)$, wobei $a \wedge^* b = \inf\{a, b\} = a \wedge b$ und $a \vee^* b = \sup\{a, b\} = a \vee b$.

$(V, \leq) \overset{\text{b)}}{\longmapsto} (V, \wedge, \vee) \overset{\text{a)}}{\longmapsto} (V, \leq^*)$, wobei $a \leq^* b \Leftrightarrow a \wedge b = a \Leftrightarrow \inf\{a, b\} = a \Leftrightarrow a \leq b$.
□

Jeder endliche Verband kann somit durch ein Hassediagramm beschrieben werden.

9.2.5 Beispiele. 1)

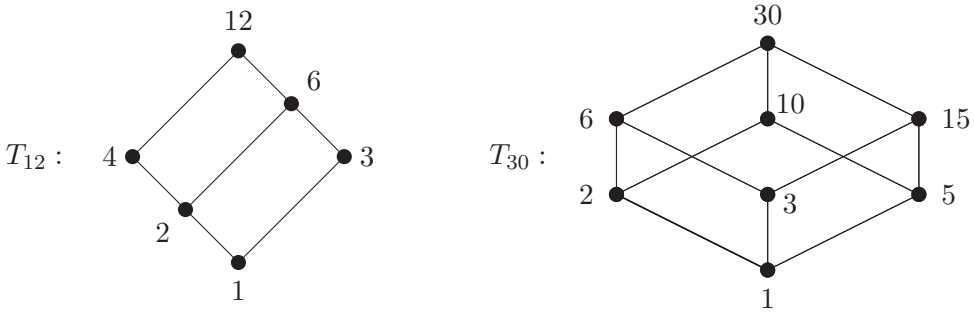


$\wedge$	0	a	b	c	1
0	0	0	0	0	0
a	0	a	0	0	a
b	0	0	b	0	b
c	0	0	0	c	c
1	0	a	b	c	1

$\vee$	0	a	b	c	1
0	0	a	b	c	1
a	a	a	1	1	1
b	b	1	b	1	1
c	c	1	1	c	1
1	1	1	1	1	1

0 ist kleinstes Element und zugleich neutrales Element bei $\vee$. 1 ist größtes Element und zugleich neutrales Element bei $\wedge$.

2) 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



3) Sei A eine Algebra (z.B. eine Gruppe). Mit $\mathrm{Sub}(A)$ bezeichnen wir die Menge der Unteralgebren. $\mathrm{Sub}(A)$ wird durch die Mengeninklusion zu einer verbandsgeordneten Menge: Für $X, Y \in \mathrm{Sub}(A)$ ist nämlich $X \cap Y$ wieder eine Unteralgebra von A und daher die größte untere Schranke von X und Y. Die kleinste obere Schranke ist

$$(*) \qquad X \vee Y := \langle X \cup Y \rangle = \bigcap \{Z \in \mathrm{Sub}(A) \mid X \cup Y \subseteq Z \subseteq A\}.$$

9.2.6 Anmerkung. Die Operationen $\wedge$ und $\vee$ nennt man oft (in Analogie zu den Operationen $\cap$ und $\cup$ in $\mathfrak{P}(X)$) „Schnitt“ und „Vereinigung“[3].

Diese Bezeichnungen können aber gelegentlich missverstanden werden: Wenn wir etwa 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 Vereinigung (also das in $(*)$ definierte Supremum $X \vee Y$) ist aber im Allgemeinen eine echte Obermenge der mengentheoretischen Vereinigung $X \cup Y$.

Dualitätsprinzip für Verbände:

$$(V, \wedge, \vee) \text{ Verband} \Leftrightarrow (V, \vee, \wedge) \text{ Verband},$$
$$(V, \leq) \text{ verbandsgeordnet} \Leftrightarrow (V, \geq) \text{ verbandsgeordnet}.$$

Wenn wir den Verband $(V, \wedge, \vee)$ mit V bezeichnen, nennen wir den Verband $(V, \vee, \wedge)$ den zu V dualen Verband und bezeichnen ihn mit V^d.
Zu jeder Aussage φ über Verbände (im ordnungstheoretischen oder auch im algebraischen Sinn) definieren wir eine Aussage φ^d, die „duale“ Aussage so: Wir ersetzen in φ das Symbol

[3] englisch: *meet, join*

$\wedge$ 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 φ für den Verband V zutrifft (z.B.: „V hat ein größtes Element“), dann trifft die Aussage φ^d auf den Verband V^d zu (z.B.: „V^d hat ein kleinstes Element“). Wenn eine Aussage φ auf alle Verbände zutrifft, dann trifft auch φ^d auf alle Verbände zu.

9.2.7 Satz (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. □

9.2.A Unterverbände

Sei $(V, \wedge, \vee)$ ein Verband. Ein *Unterverband* ist eine Teilmenge von V, die unter $\wedge$ und $\vee$ abgeschlossen ist.

9.2.8 Beispiel. 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.

9.2.9 Anmerkung. 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 $V \times V$; wir schreiben aber meist $\wedge$ und $\vee$ (oder gelegentlich $\wedge_W$ und $\vee_W$) für diese Operationen, statt genauer $\wedge\restriction(V \times V)$ und $\vee\restriction(V \times V)$ 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.

9.2.10 Beispiel. Sei V die Potenzmenge der Menge $\{0, 1, 2\}$, und sei $W_1 := \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$, $W_2 := \{\emptyset, \{0\}, \{1\}, \{0, 1, 2\}\}$.

Dann ist V ein Verband mit Operationen $\cup$ und $\cap$ und der Relation $\subseteq$. Die Halbordnungen $(W_1, \subseteq)$ und $(W_2, \subseteq)$ sind zueinander isomorph; beide sind verbandsgeordnete Mengen. Aber W_1 ist Unterverband von V, W_2 nicht.

9.2.B Kongruenzrelationen

9.2.11 Lemma. *Seien $(V_i, \wedge_i, \vee_i)$ für $i = 1, 2$ Verbände mit den zugehörigen Ordnungen $\leq_i$, und sei $f : V_1 \to V_2$ 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 $f : V \to W$ 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:

9.2.12 Definition. Sei $(L, \leq)$ eine partielle Ordnung. Eine Teilmenge $A \subseteq L$ heißt *konvex*, wenn $\forall a, b \in A \forall x \in L :\ a \leq x \leq b \Rightarrow x \in A$ gilt. Das heißt, mit allen Elementen $a, b \in A$ muss schon das ganze Intervall $[a, b] := \{x \in L \mid a \leq x \leq b\}$ eine Teilmenge von A sein.

9.2.13 Lemma. *Sei θ eine Kongruenzrelation auf einem Verband $(V, \wedge, \vee)$. Dann ist jede Kongruenzklasse eine konvexe Menge, und jede Kongruenzklasse ist Unterverband von V.*

Beweis. Sei $f : (V, \wedge, \vee) \to (W, \wedge, \vee)$ ein Homomorphismus, mit Kern θ. 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 dem vorigen Lemma 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; analog auch unter $\wedge$.

□

9.2.14 Anmerkung. Nicht jede Äquivalenzrelation, deren Klassen konvexe Unterverbände sind, ist eine Kongruenzrelation.

9.2.C Vollständige Verbände

9.2.15 Definition. 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.

9.2.16 Anmerkung. Die reellen Zahlen $\mathbb{R}$ mit der üblichen Ordnung sind im Sinne dieser Definition also nicht vollständig, die erweiterten reellen Zahlen $\mathbb{R} \cup \{-\infty, \infty\}$ schon. Wir[4] nennen eine partielle Ordnung „bedingt vollständig“[5], wenn jede nichtleere nach oben beschränkte Menge ein Supremum und jede nach unten beschränkte nichtleere Menge ein Infimum hat. Eine bedingt vollständige Halbordnung wird durch Adjunktion von zwei neuen Elementen ∞ und $-\infty$ zu einer vollständigen Halbordnung, daher kann man alle Sätze über vollständige Halbordnungen in Sätze über bedingt vollständige Halbordnungen übersetzen. Eine bedingt vollständige Halbordnung ist im Allgemeinen kein Verband. Die Familie aller endlichen Teilmengen von $\mathbb{N}$ ist ein Beispiel eines bedingt vollständigen Verbandes, der nicht vollständig ist.

[4] Achtung! Manche Autoren verwenden den Namen „vollständig“ für die Eigenschaft, die wir hier „bedingt vollständig“ nennen.

[5] englisch: *conditionally complete*

9.2.17 Satz. *Sei $(P, \leq)$ eine Halbordnung, in der jede Teilmenge ein Infimum hat. Dann hat auch jede Teilmenge von P ein Supremum.*

Beweis. Übungsaufgabe. □

9.2.18 Beispiele.

1. Sei A eine Algebra. Die Menge aller Unteralgebren bildet einen vollständigen Verband. Das Infimum einer Familie von Unteralgebren ist einfach der Durchschnitt dieser Unteralgebren.

2. Sei A eine Algebra. Die Menge aller Kongruenzrelationen $\theta \subseteq A \times A$ bildet einen vollständigen Verband. Das Infimum einer Familie von Kongruenzrelationen ist einfach der mengentheoretische Durchschnitt dieser Relationen.

9.3 Boolesche Algebren

Am Ende von Abschnitt 1.2 haben wir definiert:
Eine Algebra $(B, \wedge, \vee, 0, 1, ')$ vom Typ $(2, 2, 0, 0, 1)$ heißt *Boolesche Algebra* $\Leftrightarrow$ die folgenden Gesetze gelten für alle $a, b, c \in B$:

$$\begin{aligned} a \wedge b &= b \wedge a & a \vee b &= b \vee a \\ a \wedge (b \wedge c) &= (a \wedge b) \wedge c & a \vee (b \vee c) &= (a \vee b) \vee c \\ a \wedge (a \vee b) &= a & a \vee (a \wedge b) &= a \\ a \wedge (b \vee c) &= (a \wedge b) \vee (a \wedge c) & a \vee (b \wedge c) &= (a \vee b) \wedge (a \vee c) \\ 1 \wedge a &= a & 0 \vee a &= a \\ a \wedge a' &= 0 & a \vee a' &= 1 \end{aligned}$$

9.3.1 Anmerkung. 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 nächster Abschnitt) zu vermeiden, und um die Verwandtschaft zu Verbänden zu betonen.

Für das Komplement x' werden auch oft andere Symbole verwendet, wie x^c, $-x$, $\neg x$, $\sim x$, $\bar{x}$. Statt $a \wedge b'$ schreibt man manchmal in Analogie zu Mengenalgebren $a \setminus b$.

Dualitätsprinzip:

$(B, \wedge, \vee, 0, 1, ')$ Boolesche Algebra $\Leftrightarrow$ $(B, \vee, \wedge, 1, 0, ')$ Boolesche Algebra.

9.3.2 Lemma. *Sei $(V, \wedge, \vee)$ ein Verband. Dann gilt:*

a) $\forall a, b, c \in V : a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \Leftrightarrow \forall a, b, c \in V : a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$,

b) $\forall a \in V : 0 \vee a = a \Leftrightarrow \forall a \in V : 0 \wedge a = 0$,

c) $\forall a \in V : 1 \wedge a = a \Leftrightarrow \forall a \in V : 1 \vee a = 1$,

Beweis. a) $\Rightarrow$: $(a \vee b) \wedge (a \vee c) = [\underbrace{(a \vee b) \wedge a}_{a}] \vee [(a \vee b) \wedge c] = \underbrace{a \vee (a \wedge c)}_{a} \vee (b \wedge c) = a \vee (b \wedge c)$.

$\Leftarrow$: analog.

b) und c) folgen aus $a \wedge b = a \Leftrightarrow a \vee b = b$. □

9.3.3 Beispiel. $(\mathfrak{P}(M), \cap, \cup, \emptyset, M, ')$ mit $A' = M \setminus A$ ist eine Boolesche Algebra.

9.3.4 Satz (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) Wurde am Ende von Abschnitt 1.2 bewiesen.

b) $a \vee a' = 1$, $a \wedge a' = 0 \overset{\text{a)}}{\Longrightarrow} (a')' = a$.

c) $0 \vee 1 = 1$, $0 \wedge 1 = 0 \overset{\text{a)}}{\Longrightarrow} 0' = 1$, $1' = 0$.

d) $(a \vee b) \vee (a' \wedge b') = (a \vee b \vee a') \wedge (a \vee b \vee b') = 1 \wedge 1 = 1$, $(a \vee b) \wedge (a' \wedge b') = (a \wedge a' \wedge b') \vee (b \wedge a' \wedge b') = 0 \vee 0 = 0 \overset{\text{a)}}{\Longrightarrow} (a \vee b)' = a' \wedge b'$. Analog: $(a \wedge b)' = a' \vee b'$. □

9.3.5 Satz (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) $a \leq b' \Leftrightarrow a \wedge b = 0 \Leftrightarrow b \leq a'$.
Die Gleichung $a \wedge b = 0$ kürzt man (in Analogie zur linearen Algebra) auch mit $a \perp b$ 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). □

9.3.6 Satz (Satz über Homomorphismen). *Seien $(B, \wedge, \vee, 0, 1, ')$ und $(C, \wedge, \vee, 0, 1, ')$ Boolesche Algebren, $\varphi : B \to C$ surjektiv. Dann gilt: φ ist Homomorphismus von $(B, \wedge, \vee, 0, 1, ')$ nach $(C, \wedge, \vee, 0, 1, ') \Leftrightarrow \varphi$ ist Homomorphismus von $(B, \wedge, \vee)$ nach $(C, \wedge, \vee)$. (D. h., es genügt, dass φ mit den Verbandsoperationen verträglich ist.)*

Beweis. $\Rightarrow$: trivial.
$\Leftarrow$: Wegen $0 \vee a = a$ gilt $\varphi(0) \vee \varphi(a) = \varphi(a)$ für alle $a \in B$. Da φ surjektiv ist, gilt $\varphi(0) \vee c = c$ für alle $c \in C$. Also ist $\varphi(0)$ neutral bezüglich $\vee$ in C und daher $\varphi(0) = 0$. Analog zeigt man $\varphi(1) = 1$.
φ ist verträglich mit $'$: $a \vee a' = 1$, $a \wedge a' = 0 \Rightarrow \varphi(a) \vee \varphi(a') = \varphi(1) = 1$, $\varphi(a) \wedge \varphi(a') = \varphi(0) = 0$ $\Rightarrow \varphi(a') = \varphi(a)'$. □

9.4 Boolesche Ringe

9.4.1 Definition. Ein Ring $(R, +, 0, -, \cdot, 1)$ mit Einselement heißt „Boolescher Ring“, wenn $\forall x \in R\ x \cdot x = x$ gilt.

In jedem Booleschen Ring gilt $x + x = 0$ für alle $x \in R$, denn $x + 1 = (x + 1)(x + 1) = xx + x + x + 1 = (x + x) + (x + 1)$.
Daher ist $-x = x$ für alle x; statt $x + y$ kann man also genauso gut $x - y$ schreiben.

9.4.2 Satz.

(*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* $f : R_1 \to R_2$ *ist genau dann Ringhomomorphismus, wenn sie ein Homomorphismus von Booleschen Algebren ist.*

Beweis. Übung. □

9.4.3 Anmerkung. Die Operation $x + y = (x \wedge y') \vee (y \wedge x')$ heißt auch „symmetrische Differenz“; sie wird manchmal $x \,\Delta\, y$ geschrieben.

9.4.4 Satz (Homomorphiesatz für Boolesche Algebren)**.** *Sei* $f : B_1 \to B_2$ *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*

$$x \sim y \Leftrightarrow x + y \in f^{-1}(0)$$

ist.

Beweis. Nach dem allgemeinen Homomorphiesatz gilt $B_2 \cong B_1/kern(f)$, wobei $kern(f)$ die durch

$$(x, y) \in kern(f) \ \Leftrightarrow\ f(x) = f(y)$$

definierte Äquivalenzrelation ist. Nun gilt aber

$$f(x) = f(y) \ \Leftrightarrow\ f(x) - f(y) = 0 \ \Leftrightarrow\ f(x) + f(y) = 0 \ \Leftrightarrow\ f(x + y) = 0,$$

also ist $kern(f) = \{(x, y) \mid x \sim y\}$. □

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; wir wollen diese Ideale nun auch ordnungstheoretisch charakterisieren.

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

- $I \subseteq P$ heißt *Ordnungsideal*[6][7], wenn $\forall i \in I \, \forall p \in P : \; p \leq i \Rightarrow p \in I$ gilt, d.h., wenn I nach unten hin abgeschlossen ist.
- $I \subseteq P$ heißt *gerichtet*[8] (oder genauer: nach oben gerichtet), wenn es für alle $i_1, i_2 \in I$ ein $j \in I$ gibt mit $i_1 \leq j$ und $i_2 \leq j$.

9.4.6 Definition.

- Sei B Boolesche Algebra. $\emptyset \neq I \subseteq B$ heißt Ideal, wenn I ein (nach oben) gerichtetes Ordnungsideal ist. (Äquivalent: Wenn I Ordungsideal ist und unter $\vee$ abgeschlossen ist.)
- *Filter* werden dual definiert: $\emptyset \neq F \subseteq B$ heißt Filter (manchmal auch „duales Ideal“), wenn F unter $\wedge$ abgeschlossen ist und „duales Ordnungsideal“ ist, d.h. $\forall f \in F \, \forall b \in B : f \leq b \Rightarrow b \in F$.

Die leere Menge ist weder Ideal noch Filter. Die ganze Algebra B gilt als „uneigentliches“ Ideal bzw. als uneigentlicher Filter.

9.4.7 Definition. Sei $F \subseteq B$ Filter. Wir schreiben F^* für die Menge $\{b' \mid b \in F\}$.
Sei $I \subseteq B$ Ideal. Wir schreiben I^* für die Menge $\{b' \mid b \in I\}$.

Man zeigt leicht:

9.4.8 Lemma. *Sei B Boolesche Algebra. Dann ist $I \subseteq B$ genau dann Ideal (im gerade definierten Sinn) wenn I Ideal (im ringtheoretischen Sinn) des Booleschen Rings B^{Ring} ist.*
$F \subseteq B$ ist genau dann Filter, wenn F^* Ideal ist.
$I \subseteq B$ ist genau dann Ideal, wenn I^* Filter ist.

9.4.9 Definition. Sei $I \subseteq B$ 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 $F \subseteq B$ Filter. Dann definieren wir die Äquivalenzrelation $\sim_F$ durch $x \sim_F y \Leftrightarrow (x - y)' \in F$.

9.4.10 Lemma. *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*) $\exists f \in F : b \wedge f = c \wedge f$.

[6] englisch: *order ideal oder lower subset*
[7] Ordnungsideale heißen manchmal auch „offene Mengen“. Tatsächlich bildet die Menge aller Ordnungsideale auf P eine Topologie.
[8] englisch: *directed oder upward directed*

(*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): Wenn $b \wedge i' = c \wedge i'$, dann $b \vee i = (b \wedge i) \vee (b \wedge i') \vee i = (b \wedge i') \vee i = (c \wedge i') \vee i = c \vee i$.
(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

$$b \wedge f = c \wedge f \;\Leftrightarrow\; b - c \leq f'.$$

Der Beweis dieser Äquivalenz geht so: 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 $b \wedge f = (b \wedge c \wedge f) \vee (b \wedge c' \wedge f) \leq (b \wedge c \wedge f) \vee (f' \wedge f) = (b \wedge c \wedge f) \leq b \wedge f$, also $b \wedge f = b \wedge c \wedge f$. Analog $c \wedge f = b \wedge c \wedge f$, also $b \wedge f = c \wedge f$. □

9.4.11 Beispiel. 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.

9.4.12 Beispiel. Sei B die Famile aller Borelmengen $X \subseteq [0, 1]$. B ist Boolesche Algebra (mit den üblichen Operationen $\cup, \cap, \ldots$). Sei λ 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 X und Y „bis auf eine Lebesgue-Nullmenge“ übereinstimmen.

9.5 Endliche Boolesche Algebren

9.5.1 Definition. Sei $(V, \wedge, \vee, 0, 1)$ ein Verband mit 0- und 1-Element. Dann heißt $a \in V$ ein *Atom* :$\Leftrightarrow$

1) $0 < a$ und

2) $0 \leq b \leq a \Rightarrow b = 0 \vee b = a$

(d. h., a ist ein oberer Nachbar von 0).

9.5.2 Lemma (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* $a \leq c$.

(A4) $a \leq b \vee c$ *genau dann, wenn* $a \leq b$ *oder* $a \leq c$.

Beweis.

(A1) $a \wedge b \leq a$, daher kann $a \wedge b$ nur die Werte 0 und a annehmen. Daher $a \wedge b \neq 0 \Leftrightarrow a \wedge b = a \Leftrightarrow a \leq b$.

(A2) $a \leq b' \Leftrightarrow a \wedge b = 0$ gilt für beliebige a, b. Wenn aber a Atom ist, gilt mit (A1):

$$a \leq b' \quad \Leftrightarrow \quad a \wedge b = 0 \quad \Leftrightarrow \quad a \not\leq b.$$

(A3) Dies gilt sogar für beliebige $a, b, c \in B$ (und sogar in jedem Verband).

(A4) Wir zeigen statt dessen $a \not\leq b \vee c \;\Leftrightarrow\; a \not\leq b$ und $a \not\leq c$. Wir verwenden das Distributivgesetz $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ sowie Rechenregel (A1):

$$a \not\leq b \vee c \;\Leftrightarrow\; (a \wedge b) \vee (a \wedge c) = 0 \;\Leftrightarrow\; a \wedge b = 0 \text{ und } a \wedge c = 0 \;\Leftrightarrow\; a \not\leq b \text{ und } a \not\leq c.$$

□

9.5.3 Anmerkung. 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 $\cup$.

9.5.4 Lemma. *Sei* $(B, \wedge, \vee, 0, 1, ')$ *eine endliche Boolesche Algebra. Dann gibt es zu jedem Element* $b \in B \setminus \{0\}$ *ein Atom* $a \in B$ *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 $a = b_i$. □

9.5.5 Satz (Satz von Stone für endliche Boolesche Algebren)**.** *Sei* $(B, \wedge, \vee, 0, 1, ')$ *eine Boolesche Algebra und* $M := \{a \in B \mid a \text{ Atom von } B\}$.
Sei $\varphi : B \to \mathfrak{P}(M)$ *gegeben durch* $\varphi(b) := \{a \in M \mid a \leq b\}$.
Dann gilt:

- φ *ist Homomorphismus von Booleschen Algebren.*
- *Wenn* B *endlich ist, dann ist* φ *Isomorphismus der Booleschen Algebren* B *und* $\mathfrak{P}(M)$.

Beweis. Da $\varphi(b) \subseteq M$, ist φ wohldefiniert.

- $\varphi(b') = M \setminus \varphi(b)$:

$$\begin{aligned} a \in \varphi(b') &\Leftrightarrow a \leq b' \\ &\Leftrightarrow a \not\leq b \quad \text{wegen Rechenregel A2} \\ &\Leftrightarrow a \notin \varphi(b) \\ &\Leftrightarrow a \in M \setminus \varphi(b) \end{aligned}$$

- $\varphi(b \vee c) = \varphi(b) \cup \varphi(c)$:

$$\begin{aligned} a \in \varphi(b \vee c) &\Leftrightarrow a \leq b \vee c \\ &\Leftrightarrow a \leq b \text{ oder } a \leq c \quad \text{wegen Rechenregel A4} \\ &\Leftrightarrow a \in \varphi(b) \text{ oder } a \in \varphi(c) \\ &\Leftrightarrow a \in \varphi(b) \cup \varphi(c) \end{aligned}$$

- $\varphi(b \wedge c) = \varphi(b) \cap \varphi(c)$: Analog, mit Hilfe der Rechenregel A3.

- Wenn B endlich ist, dann ist φ surjektiv:

  Sei $U \in \mathfrak{P}(M)$, d. h., $U \subseteq M$. Weil U endlich ist, können wir das Supremum von U bilden: Sei $U = \{a_1, \ldots, a_r\}$ und $b := a_1 \vee \cdots \vee a_r = \sup U$. Dann gilt $\varphi(b) = \varphi(a_1 \vee \cdots \vee a_r) = \varphi(a_1) \cup \cdots \cup \varphi(a_r) \overset{a_i \text{ Atome}}{=} \{a_1\} \cup \cdots \cup \{a_r\} = U$.

- φ ist injektiv (d. h., $b \neq c \Rightarrow \varphi(b) \neq \varphi(c)$). Da φ auch ein Ringhomomorphismus ist, genügt es, $kern(\varphi) = \{0\}$ zu zeigen: Wenn $b \in kern(\varphi)$, dann ist $\varphi(b) = \emptyset$, d.h. es gibt kein Atom $a \leq b$. Nach dem gerade bewiesenen Lemma muss $b = 0$ sein.

□

9.5.6 Anmerkungen. 1) $|M| = |M_1| \Rightarrow (\mathfrak{P}(M), \cap, \cup, \emptyset, M, ') \cong (\mathfrak{P}(M_1), \cap, \cup, \emptyset, M_1, ')$.

2) $|M| = n \in \mathbb{N}_0 \Rightarrow |\mathfrak{P}(M)| = 2^n$.

9.5.7 Folgerung. Ist B endliche Boolesche Algebra, dann gilt $|B| = 2^n$ für ein $n \in \mathbb{N}_0$. Zu jedem $n \in \mathbb{N}_0$ gibt es somit — bis auf Isomorphie — genau eine Boolesche Algebra mit 2^n Elementen, nämlich $\mathfrak{P}(\{0, 1, \ldots, n-1\})$.

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 Übungen), 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.

9.5.8 Definition. Sei M Menge. Eine Menge $\mathfrak{K} \subseteq \mathfrak{P}(M)$ heißt *Mengenkörper*[9] $:\Leftrightarrow$ für alle $A, B \in \mathfrak{K}$ gilt

1) $A \cup B \in \mathfrak{K}$,

2) $A \cap B \in \mathfrak{K}$,

3) $A' \in \mathfrak{K}$,

4) $A \cap B' = A \setminus B \in \mathfrak{K}$,

5) $M \in \mathfrak{K}$.

9.5.9 Beispiel. $\mathfrak{P}(M)$ ist Mengenkörper. Auch $\{M, \emptyset\}$ ist Mengenkörper.

9.5.10 Anmerkung. Die Liste 1)–5) ist redundant. Aus 4)&5) folgen bereits die Bedingungen 1)&2)&3). Ebenso folgen, wenn man $\mathfrak{K} \neq \emptyset$ voraussetzt, aus 3)&4) die übrigen Bedingungen, oder aus 1)&3), oder auch aus 2)&3).

[9] englisch: *field of sets*

9.5.11 Definition. Sei $\mathfrak{K} \subseteq \mathfrak{P}(M)$ ein Mengenkörper. Dann heißt die Boolesche Algebra $(\mathfrak{K}, \cap, \cup, \emptyset, M, ')$ eine *Mengenkörperalgebra.*

(Oft wird in der Notation nicht zwischen der Menge $\mathfrak{K}$ und der Booleschen Algebra $(\mathfrak{K}, \cap, \cup, \emptyset, M, ')$ unterschieden, und beide werden mit „Mengenkörper“ bezeichnet.)

Eine Mengenkörperalgebra ist also eine Unteralgebra von $(\mathfrak{P}(M), \cap, \cup, \emptyset, M, ')$.
Die folgenden Beispiele zeigen, dass eine Mengenkörperalgebra Atome haben kann, aber nicht haben muss.

9.5.12 Beispiele. 1) Sei $(0, 1]$ das halboffene Intervall der reellen Zahlengeraden und $\mathfrak{K} \subseteq \mathfrak{P}((0, 1])$ gegeben durch $\mathfrak{K} := \{\emptyset\} \cup \{\bigcup_{1 \le i \le n}(a_i, b_i] \mid 0 \le a_i < b_i \le 1,\ n \in \mathbb{N}\}$. 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.

Im nächsten Abschnitt werden wir den folgende Darstellungssatz[10] beweisen:

9.5.13 Satz (von Stone)**.** *Jede Boolesche Algebra ist isomorph zu einer Mengenkörperalgebra.*

9.5.14 Anmerkung. $\mathfrak{P}(M) \cong \{0, 1\}^M$ (direkte Potenz). (Jeder Teilmenge wird ihre charakteristische Funktion zugeordnet.) Aus dem Satz von Stone folgt daher: Jede Boolesche Algebra B ist isomorph zu einer Unteralgebra einer Potenz $\{0, 1\}^M$. 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!

9.5.15 Anmerkung. Ein analoger Sachverhalt gilt auch für distributive Verbände. Dazu definieren wir: $\mathfrak{V} \subseteq \mathfrak{P}(M)$ heißt *Mengenverband* $:\Leftrightarrow$ für alle $A, B \in \mathfrak{V}$ gilt $A \cap B, A \cup B \in \mathfrak{V}$. Es gilt dann (ohne Beweis): Jeder distributive Verband ist isomorph zu einem Mengenverband. Daraus folgt wieder: Jedes Gesetz, welches im distributiven Verband $\{0, 1\}$ mit den obigen Operationen $\wedge, \vee$ gilt, muss in allen distributiven Verbänden gelten.

[10] Ein Darstellungssatz ist ein Satz, der aussagt, dass jede abstrakte Struktur mit gewissen Eigenschaften isomorph zu einer „konkreten“ (mehr oder weniger bekannten) Struktur ist. Der Cayleysche Satz für Gruppen besagt, dass jede „abstrakte“ Gruppe zu einer Gruppe von Bijektionen einer Menge isomorph ist; diese Gruppe ist insofern „konkret“, als die Gruppenoperation auf dieser Menge einfach die Verknüpfung von Abbildungen ist.

Der Darstellungssatz von Stone identifiziert jede Boolesche Algebra mit einer Unteralgebra der Potenzmengenalgebra; die Potenzmengenalgebra ist insofern konkret, als die Verbandsoperationen die mengentheoretischen Operationen $\cup$ und $\cap$ sind.

In der linearen Algebra haben Sie einen Darstellungssatz für Vektorräume kennengelernt. Zum Beispiel ist jeder n-dimensionale Vektorraum über dem Körper K zum Vektorraum K^n isomorph, in welchem die Operationen (Addition, Skalarmultiplikation) konkret durch die Körperoperationen in den einzelnen Komponenten gegeben werden.

Eine Beweisskizze des Darstellungssatzes für distributive Verbände finden Sie in den Übungsbeispielen.

9.6 Darstellungssatz von Stone

Wir beginnen mit einer informellen Überlegung:
Sei $\mathfrak{K} \leq (\mathfrak{P}(M), \cap, \cup, \emptyset, M, ')$ ein Mengenkörper. Wie können wir die Menge M aus $\mathfrak{K}$ bestimmen, wenn wir $\mathfrak{K}$ nur bis auf Isomorphie kennen? D.h., wir haben eine Boolesche Algebra B gegeben, und suchen M, sodass B isomorph zu einer Unteralgebra von $\mathfrak{P}(M)$ ist.
Im vorigen Abschnitt haben wir uns mit endlichen Booleschen Algebren B beschäftigt. Die Menge M haben wir als die Menge der Atome von B gefunden. Der Isomorphismus hat jedes Element $b \in B$ mit $\{m \in M \mid m \leq b\}$ identifiziert.
Der selbe Beweis zeigt, dass für jede Boolesche Algebra B mit A als Menge der Atome die Abbildung $b \mapsto \{a \in A \mid a \leq b\}$ ein Homomorphismus von B in $\mathfrak{P}(A)$ 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.
Die Rolle der Atome im vorigen Beweis werden in diesem Abschnitt gewisse Ideale (oder äquivalent: Filter) spielen. Nehmen wir nämlich an, dass wir bereits eine Einbettung $f : B \to \mathfrak{P}(M)$ gefunden haben, mit irgend einer Menge M.
Für jedes $m \in M$ ist nun 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, $I_m = F_m^* = \{b' \mid b \in F_m\}$. 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 es sein, alle echten Ideale $I \subseteq B$ mit $I \cup I^* = B$ zu betrachten, und mit Hilfe dieser Ideale[11] die Menge M zu rekonstruieren.

9.6.1 Anmerkung. 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: $0 \leq x$.)

9.6.2 Definition. Sei B Boolesche Algebra, $F \subseteq B$ ein echter Filter.

- F heißt maximal, wenn es keinen Filter G mit $F \subsetneq G \subsetneq B$ gibt, d.h. wenn F in der durch $\subseteq$ geordneten Menge aller echten Filter ein maximales Element ist.
- F heißt Primfilter, wenn F die folgende Eigenschaft hat:

$$\forall x, y \in B : \; x \vee y \in F \quad \Leftrightarrow \quad x \in F \text{ oder } y \in F.$$

(Anmerkung: Die Implikation $\Leftarrow$ gilt für alle Filter. Die zur obigen Äquivalenz duale Eigenschaft gilt für alle Filter: $\forall x, y \in B : \; x \wedge y \in F \quad \Leftrightarrow \quad x \in F$ und $y \in F$.)

[11] 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 Fernpunkts 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.

- F heißt Ultrafilter, wenn für alle $x \in B$ gilt: $x \in F$ oder $x' \in F$.
  Anmerkung: Aus $x \in F$ *und* $x' \in F$ würde $0 \in F$ folgen, was wir durch die Voraussetzung $F \neq B$ ausgeschlossen haben. Ein echter Filter F ist also genau dann Ultrafilter, wenn für alle $x \in B$ *genau eine* der folgenden Aussagen zutrifft:

$$x \in F, \qquad x' \in F.$$

Die Begriffe „maximales Ideal“, „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.

9.6.3 Beispiele. 1) Sei B Boolesche Algebra, und sei $a \in B$ ein Atom. Dann ist die Menge $\{x \in B \mid a \leq x\}$ ein Primfilter und Ultrafilter. (Filter von der Form $\{x \in B \mid b_0 \leq x\}$ heißen Hauptfilter, Ideale der Form $\{x \in B \mid x \leq c_0\} = \{x \wedge c_0 \mid x \in B\}$ Hauptideale.[12])

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.

9.6.4 Lemma. *Sei B Boolesche Algebra, und sei $F \neq B$ ein echter Filter. Dann sind die folgenden Aussagen äquivalent:*

1. *F ist maximaler Filter.*
2. *$\forall x \in B: \ x \notin F \ \Rightarrow \ x' \in F$.*
3. *F ist Ultrafilter: $\forall x \in B: \ x \notin F \ \Leftrightarrow \ x' \in F$.*
4. *F ist Primfilter: $\forall x, y \in B: \ x \vee y \in F \ \Leftrightarrow \ x \in F$ oder $y \in F$.*
5. *$B \setminus F$ ist ein Ideal.*
6. *$F^* = B \setminus F$.*

Beweis. Wir werden nur die Aussagen (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (2) zeigen.
(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 (ein duales Ordnungsideal). 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 $x \notin F$ folgt wegen der Annahme (2): $x' \in F$. 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

$$x \vee y \notin F \ \Leftrightarrow \ (x \vee y)' \in F \ \Leftrightarrow \ x' \wedge y' \in F \ \Leftrightarrow \ x' \in F \text{ und } y' \in F \ \Leftrightarrow \ x \notin F \text{ und } y \notin F.$$

[12] englisch: *principal filter*, *principal ideal*. (Achtung! „principal“, nicht „principle“)

Aus $x \vee y \notin F \;\Leftrightarrow\; x \notin F$ und $y \notin F$ folgt durch Kontraposition:[13]

$$x \vee y \in F \;\Leftrightarrow\; x \in F \text{ oder } y \in F.$$

(4) $\Rightarrow$ (2): Sei F Primfilter. Wegen $x \vee x' = 1 \in F$ folgt aus der Annahme $x \notin F$ sofort $x' \in F$.

□

Das folgende Lemma ist einfach eine Umformulierung des vorigen Lemmas. Wir schreiben es extra an, um die Analogie zwischen Ultrafiltern und Atomen hervorzuheben.

9.6.5 Lemma (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 $c \in F$.

9.6.6 Folgerung. Sei B Boolesche Algebra, und M die Menge aller Ultrafilter auf B. Wenn wir die Abbildung $\varphi : B \to \mathfrak{P}(M)$ durch

$$\varphi(x) = \{F \in M \mid x \in F\}$$

definieren, dann ist φ ein Homomorphismus von Booleschen Algebren.

Wir rechnen als Beispiel nur die Homomorphiebedingungen für 0, 1 und $\vee$ vor (die für $\wedge$ und $'$ folgen aus U2 und U3):

- $\varphi(0) = \{F \in M \mid 0 \in F\} = \emptyset$, denn kein Ultrafilter (sogar: kein echter Filter) enthält das Nullelement der Booleschen Algebra.
- $\varphi(1) = M$, denn jeder Ultrafilter (überhaupt jeder Filter) enthält das Einselement der Booleschen Algebra.
- $\varphi(b \vee c) = \{F \in M \mid b \vee c \in F\} = \{F \in M \mid b \in F \text{ oder } c \in F\}$ wegen Rechenregel U4. Diese letztere Menge ist gleich $\varphi(b) \cup \varphi(c)$.

9.6.7 Lemma (BPI[14])**.** *Sei B Boolesche Algebra, $b \in B$, $b \neq 0$. Dann gibt es einen Ultrafilter F mit $b \in F$.*

Bevor wir den allgemeinen Beweis führen, illustrieren wir die Beweisidee anhand zweier Speziallfälle:

9.6.8 Beispiele. 1) Sei B endliche Boolesche Algebra, $b \in B$, $b \neq 0$. Wir wissen bereits, dass es ein Atom a mit $a \leq b$ gibt. Der Filter $\{x \in B \mid a \leq x\}$ ist nun ein Ultrafilter, der b enthält.

[13] Die logische Regel der Kontraposition besagt: Wenn $A \Rightarrow B$, dann $\neg B \Rightarrow \neg A$. Daher gilt auch: Wenn $A \Leftrightarrow B$, dann $\neg A \Leftrightarrow \neg B$.

Hingegen ist der Schluss „Wenn $A \Rightarrow B$, dann $B \Rightarrow A$“ nicht allgemein gültig.

In Bezug auf Aussagen gilt ein Analogon der de Morganschen Regeln: die Negation von „A und B“ ist „$\neg A$ oder $\neg B$“.

[14] Dieser Satz wird oft mit BPI abgekürzt: „Boolean prime ideal theorem.“

2) Sei B abzählbare Boolesche Algebra. Sei $B = \{b_1, b_2, \dots\}$. Sei $b \in B$, $b \neq 0$.
Wir definieren eine Folge $(c_n)_{n=0,1,2,\dots}$ so:

- $c_0 := b$.
- Für alle $n \geq 0$: $c_{n+1} := c_n \wedge b_{n+1}$, wenn $c_n \wedge b_{n+1} \neq 0$.
- Für alle $n \geq 0$: $c_{n+1} := c_n \wedge b'_{n+1}$, wenn $c_n \wedge b_{n+1} = 0$.

Aus $c_n \neq 0$ folgt, dass zumindest einer der Ausdrücke $c_n \wedge b_{n+1}$, $c_n \wedge b'_{n+1}$ positiv (d.h., $\neq 0$) sein muss, daraus folgt $c_{n+1} \neq 0$.

Sei nun $F := \{x \mid \exists n : c_n \leq x\}$. Man rechnet leicht nach, dass F ein Filter ist, $0 \notin F$, und $b \in F$. F ist sogar ein Ultrafilter, denn für alle n wissen wir:

$$b_n \in F \text{ oder } b'_n \in F.$$

Für überabzählbare Mengen funktioniert eine ähnliche Strategie, nur müssen wir überabzählbar viele Schritte verwenden. Wir können einen Ultrafilter entweder mit „transfiniter Rekursion“ definieren oder das Lemma von Zorn einsetzen.

9.6.9 Satz (Lemma von Zorn)**.** *Sei $(P, \leq)$ eine nichtleere partielle Ordnung, in der jede Kette eine obere Schranke hat. Dann hat P (mindestens) ein maximales Element.*

9.6.10 Anmerkung. 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). Das Wort „nichtleer“ könnte man also im Lemma von Zorn auch weglassen. Meistens beginnt man in einer Anwendung des Zornschen Lemmas aber mit einem expliziten Beweis, dass die betrachtete Ordnung nicht leer ist, um sich ab dann nur mit nichtleeren Ketten beschäftigen zu müssen.

9.6.11 Anmerkung. In vielen Anwendungen des Zornschen Lemmas ist die betrachtete partielle Ordnung eine durch $\subseteq$ geordnete Menge von Mengen $(\mathfrak{P}, \subseteq)$. Zu jeder Kette $\mathfrak{C} \subseteq \mathfrak{P}$ gibt es dann einen natürlichen Kandidaten für eine obere Schranke, nämlich die Menge $S := \bigcup \mathfrak{C} := \bigcup_{Q \in \mathfrak{P}} Q$. Diese Menge erfüllt automatisch $Q \subseteq S$ für alle $Q \in \mathfrak{C}$; um die Voraussetzung des Zornschen Lemmas zu überprüfen, muss man aber zeigen, dass S auch tatsächlich in $\mathfrak{P}$ liegt.[15]

Das Lemma von Zorn wurde bereits in der linearen Algebra besprochen und verwendet (etwa für den Satz, dass jeder Vektorraum eine Basis hat). In der Mengenlehre zeigt man, dass das Lemma von Zorn aus dem Auswahlaxiom („das Produkt nichtleerer Mengen ist nicht leer“) folgt. Um das Lemma von Zorn besser zu verstehen, zeigen wir hier, wie es aus dem (möglicherweise leichter einzusehenden) Hausdorffschen Kettensatz folgt. (Umgekehrt kann man aus dem Zornschen Lemma auch leicht den Hausdorffschen Kettensatz folgern.)

9.6.12 Satz (Hausdorffscher Kettensatz)**.** *Sei $(Q, \leq)$ eine beliebige partielle Ordnung. Dann gibt es in Q eine maximale Kette („maximal“ bezieht sich auf die Inklusionsrelation $\subseteq$). Das heißt: Es gibt eine Kette $K \subseteq Q$ mit der Eigenschaft, dass es keine echt umfasssende Kette L gibt:*

$$\neg\exists L : L \text{ Kette und } K \subsetneq L \quad \text{bzw.} \quad \forall L \supsetneq K : L \text{ ist keine Kette.}$$

[15] Hier kann die üblicherweise verwendete schlampige Notation Verwirrung stiften. Wenn man von der Ordnung $(\mathfrak{P}, \subseteq)$ spricht, meint man nämlich die Ordnung $(\mathfrak{P}, \leq)$, wobei $\leq$ die Einschränkung der Teilmengenrelation auf P ist, dies wird durch die Notation aber verschleiert. Wenn man nun $S := \bigcup \mathfrak{C}$ setzt, ist $Q \subseteq C$ zwar automatisch erfüllt, aber für $Q \leq C$ muss man erst $C \in \mathfrak{P}$ zeigen.

Ein informeller Beweis des Hausdorffschen Kettensatzes geht so: *Sei K_0 eine beliebige Kette. Wenn K_0 nicht maximal ist, dann gibt es eine Kette K_1 mit $K_0 \subsetneqq K_1$. Wenn K_1 nicht maximal ist, finden wir eine Kette $K_2 \supsetneqq K_1$ etc.*
Die Menge $K_\infty := K_0 \cup K_1 \cup \cdots$ ist nun eine Kette. (Wenn nämlich $x, y \in K_\infty$, dann gibt es ein n mit $x, y \in K_n$, daher sind x und y vergleichbar.)
Wenn K_∞ noch immer nicht maximal ist, gibt es eine Kette $K_{\infty+1}$, $K_\infty \subsetneqq K_{\infty+1}$. Und so weiter, und so weiter.
Um dieses „und so weiter“ korrekt formalisieren zu können (man muss sich insbesondere eine Notation überlegen, mit Hilfe derer man überhaupt erst *formulieren* kann „dieser Prozess terminiert“) verwendet man in der Mengenlehre Wohlordungen und/oder Ordinalzahlen.

Beweis von „Hausdorff $\Rightarrow$ Zorn“. Sei P eine partielle Ordnung, in der alle Ketten obere Schranken haben. Nach dem Hausdorffschen Lemma gibt es eine maximale Kette K. Laut Voraussetzung hat diese Kette eine obere Schranke s.
Wir behaupten, dass s ein maximales Element von P ist. Gäbe es nämlich ein $t \in P$ mit $t > s$, dann wäre die Menge $K \cup \{t\}$ eine Kette. [Warum? Weil für alle $k \in K$ die Beziehung $k \leq s < t$, also $k < t$ gilt. Also sind alle Elemente von K mit t vergleichbar, und untereinander sind sie ohnehin vergleichbar.]
Nun ist $t \in K$ aber unmöglich, weil ja $s < t$ obere Schranke für K ist. Daher ist $K \cup \{t\}$ eine Kette, die eine echte Obermenge von K ist; das ist ein Widerspruch zur Maximalität von K. □

Beweis von BPI. Wir verwenden das Lemma von Zorn, um einen maximalen Filter zu finden, der b enthält.
Sei Q die Menge aller echten Filter.
Sei $Q_0 \subseteq Q$ die Menge aller echten Filter, die b enthalten. Q_0 ist nicht leer, da zum Beispiel der von b erzeugte „Hauptfilter“

$$\{x \in B \mid b \leq x\}$$

in Q_0 liegt. Q_0 wird durch die Relation $\subseteq$ partiell geordnet.
Wir müssen zeigen, dass jede Kette in Q_0 beschränkt ist. (Mit dem Lemma von Zorn erhalten wir dann ein maximales Element von Q_0.)
Wichtig ist, dass alle im Beweis auftretenden Filter echt sind. Wir haben schon angemerkt, dass ein Filter genau dann echt ist, wenn er 0 nicht enthält.
Sei $\mathfrak{K}$ eine Kette in Q_0, also eine Menge von Filtern, die

- paarweise vergleichbar sind: $\forall F, G \in \mathfrak{K} : F \subseteq G$ oder $G \subseteq F$;
- alle echt sind: $\forall F \in \mathfrak{K} : 0 \notin F$;
- alle b enthalten: $\forall F \in \mathfrak{K} : b \in F$.

Sei $H := \bigcup \mathfrak{K} = \bigcup_{F \in \mathfrak{K}} F$. Offensichtlich enthält H das Element b (weil $\mathfrak{K} \neq \emptyset$), und offensichtlich gilt $0 \notin H$. Zu zeigen ist noch, dass H ein Filter ist.
Es ist klar, dass H ein duales Ordnungsideal ist, denn die Vereinigung einer beliebigen Menge von dualen Ordnungsidealen ist duales Ordnungsideal.
Seien nun $x_1, x_2 \in H$. Wir wollen $x_1 \wedge x_2 \in H$ zeigen. Wir finden $F_1, F_2 \in \mathfrak{K}$ mit $x_1 \in F_1$, $x_2 \in F_2$. Ohne Beschränkung der Allgemeinheit dürfen wir $F_1 \subseteq F_2$ annehmen. Somit ist $x_1 \in F_2$ und $x_2 \in F_2$, also auch $x_1 \wedge x_2 \in F_2$, daher $x_1 \wedge x_2 \in H$.
Wir wissen nun, dass H ein echter Filter ist. Nach Definition von H gilt $F \subseteq H$ für alle $F \in \mathfrak{K}$. Daher ist $\mathfrak{K}$ beschränkt.

Wir haben somit bewiesen, dass jede Kette in Q_0 beschränkt ist. Daher hat Q_0 ein maximales Element F.
Wir wollen aber, dass F maximaler Filter ist, d.h. nicht nur maximales Element von Q_0 sondern auch [16] von Q. Wenn aber $G \in Q$ ein Filter mit $G \supseteq F$ ist, dann muss G auch b enthalten; also muss $G \in Q_0$ sein, und weil F **in** Q_0 maximal war, muss $G = F$ gelten. F ist also auch in Q maximal.
Daher ist F maximaler Filter, also Ultrafilter. □

9.6.13 Satz (Satz von Stone)**.** *Sei B eine Boolesche Algebra. Dann gibt es eine Menge M und eine Unteralgebra der Booleschen Algebra $\mathfrak{P}(M)$, die zu B isomorph ist.*

Beweis. Wir setzen $M :=$ Menge aller Ultrafilter auf B. Die oben definierte Abbildung $\varphi : B \to \mathfrak{P}(M)$ ist Homomorphismus von Booleschen Algebren. Sei $C := \varphi(B)$ das Bild von B. Dann ist C Unteralgebra von $\mathfrak{P}(M)$, und $\varphi : B \to C$ surjektiv.
Zu zeigen ist noch, dass φ injektiv ist. Wir verwenden unser Wissen über Ringe: es genügt, $\ker(\varphi) = \{0\}$ zu beweisen.
Sei $b \in \ker(\varphi)$. Das heißt $\varphi(b) = \emptyset$. Es gibt also keinen Ultrafilter F mit $b \in F$. Nach dem Lemma BPI ist das nur möglich, wenn $b = 0$. Also $\ker(\varphi) = \{0\}$, somit ist φ injektiv. □

[16] Sei Q eine Halbordnung, $p \in Q$. Beachten Sie, dass der Ausdruck „p ist maximal mit der Eigenschaft X“ theoretisch 2 Interpretationen zulässt:

- p ist erstens maximales Element von Q, und hat zweitens die Eigenschaft X.
- Unter allen Elementen von Q mit der Eigenschaft X ist p maximal. D.h., p ist maximal in der Menge $Q_0 := \{q \in Q \mid q \text{ hat Eigenschaft } X\}$.

Im Allgemeinen sind diese beiden Eigenschaften nicht äquivalent; wenn aber, wie in unserem Fall, Q_0 ein duales Ordnungsideal in Q ist, dann ist jedes maximale Element von Q_0 auch maximal in Q.