TECHNISCHE
UNIVERSITÄT
WIEN

VIENNA
UNIVERSITY OF
TECHNOLOGY

D I P L O M A R B E I T

Die Catalan'sche Vermutung

ausgeführt am Institut für

Diskrete Mathematik und Geometrie

der Technischen Universität Wien

unter Anleitung von

Univ. Prof. Dipl.-Ing. Dr. techn. Michael Drmota

durch

Thomas Lorenz

Blumengasse 6 / 9

1180 Wien

Datum

Unterschrift

Inhaltsverzeichnis

Kapitel 1

Historischer Überblick

Im Jahr 1844 druckte das Journal für die Reine und Angewandte Mathematik in seiner 27. Ausgabe folgende Zeilen [13]:

> **Note**
> extraite d'une lettre adressée à l'éditeur par Mr. E. Catalan, Repetiere à l'cole polytechnical de Paris.
>
> ---
>
> Je vous prie, Monsieur, de vouloir bien énoncer, dans votre recueil, le théomème suivant, que je croi vrai, bien que je n'aie pas encore réussi à le démontrer complètement: d'autres seront peut-être plus heureux:
>
> Deux nombres entiers consécutifs, autres que 8 et 9, ne peuvent être des puissances exactes; autrement dit: l'équation $x^m - y^n = 1$, dans laquelle les inconnues sont entières et positives, n'admèt qu'une seule solution.

Auf deutsch übersetzt lautet dieser Auszug eines Briefes des, zu der Zeit an der Cole Polytechnical in Paris tätigen, belgischen Mathematikers Eugène Catalan an den Herausgeber des Journals in etwa wie folgt:

> *Ich bitte Sie, Monsieur, in Ihrem Sammelband folgenden Satz zu veröffentlichen, den ich für richtig halte, auch wenn es mir noch nicht gelungen ist, ihn vollständig zu beweisen; Andere haben vielleicht mehr Glück:*
> *Zwei aufeinanderfolgende ganze Zahlen, mit Ausnahme von 8 und 9, können keine echten Potenzen sein; Anders gesagt: Die Gleichung* $x^m - y^n = 1$, *in der die Unbekannten positive ganze Zahlen sind, besitzt nur eine einzige Lösung.*

Catalan ahnte damals wohl noch nicht, dass es knapp 160 Jahre dauern würde, bis es einem "Anderen", nämlich dem rumänischen Mathematiker Preda Mihailescu, gelingen würde diesen Satz zu beweisen, und dass sich seine Behauptung bis zu jenem Zeitpunkt als Catalan'sche Vermutung zu einem der bekanntesten Probleme in der Zahlentheorie entwickeln würde.

Wir werden nun in diesem Kapitel einen möglichst vollständigen Überblick geben über all jene Resultate, die im Laufe der Zeit von den verschiedenen an dem Catalan'schen Problem arbeitenden Mathematikern gefunden wurden, und jeweils neue Erkenntnisse zu diesem Thema brachten. Der letztendliche Beweis der Catalan'schen Vermutung verwendet freilich nur einen Teil der in diesem Kapitel angeführten Ergebnisse, auf diese werden wir uns im weiteren Verlauf der Diplomarbeit konzentrieren.

Für die Details und Beweise zu den anderen, für den von uns dargelegten Beweis der Catalan'schen Vermutung zwar nicht notwendigen, aber zu ihrer Zeit durchaus relevanten, Erkenntnissen verweisen wir zum Einen auf Ribenboims Buch [54], das alle Ergebnisse zu diesem Thema bis zum Jahr 1994 ausführlich behandelt, sowie zum Anderen auf die Zusammenfassung von Mignotte [45], die einen etwas detaillierteren Überblick über die späteren Resultate bietet.

1.1 Spezialfälle mit kleinen Exponenten

Die historisch gesehen ersten Ergebnisse zum Catalan'schen Problem gab es für verschiedene Spezialfälle der Gleichung $x^m - y^n = 1$ mit kleinen Exponenten m und n.

Schon bevor Catalan seine Vermutung formulierte gab es Mathematiker, die sich mit dem Problem von aufeinanderfolgenden Potenzen beschäftigten. Laut [19] stellte bereits Philipe de Vitry im 14. Jahrhundert die Frage, ob alle Potenzen von 2 und 3, mit Ausnahme der Paare 1 und 2, 2 und 3, 3 und 4 sowie 8 und 9, sich um mehr als eine Einheit unterscheiden. Dieses Problem wurde von de Vitrys Zeitgenossen Levi ben Gershon, der auch unter dem Namen Gersonides bekannt ist, gelöst. Ihm gelang es zu zeigen, dass $3^m \pm 1$ immer einen ungeraden Primfaktor besitzt falls $m > 2$, womit kann $3^m \pm 1$ keine Potenz von 2 sein.

Auch Leonard Euler beschäftigte sich mit einem Spezialfall des Catalan'schen Problems, nämlich mit der Gleichung $x^2 - y^3 = 1$. Es gelang ihm 1738 in [22] zu zeigen, dass die einzige Lösung dieser Gleichung in den positiven ganzen Zahlen $x = 3, y = 2$ ist. Wir geben Eulers Beweis dafür in Kapitel 3 wieder.

Catalans Vermutung stellt nun eine Verallgemeinerung dieses Satzes von Euler für beliebige Exponenten dar. Nachdem Catalan seine Vermutung 1844 veröffentlichen lies sah es zunächst so aus, als würde das Problem schon bald gelöst werden. Denn bereits 1850 gelang es dem französischen Mathematiker V.A. Lebesgue[1] in [38] zu zeigen, dass die Gleichung $x^p - y^2 = 1$, wobei p eine Primzahl ist, keine Lösung in den positiven ganzen Zahlen besitzt. Wir geben diesen Beweis in Unterkapitel 3.2 wieder.
Lebesgue merkt in seinem Artikel an, dass die anderen Fälle der Gleichung $x^m - y^n = 1$ mehr Schwierigkeiten zu bereiten scheinen, er aber nicht wisse, welche Fortschritte Catalan mittlerweile selbst auf diesem Gebiet erzielt hatte. Doch auch Catalan konnte keine weiteren Fortschritte erzielen. Die einzige weitere Veröffentlichung von

[1] Nicht zu verwechseln mit dem besser bekannten H.L. Lebesgue, nach dem das Lebesgue-Maß und das Lebesgue-Integral benannt sind.

Catalan zu diesem Thema [14] stammt aus dem Jahr 1885. Darin gibt Catalan einige empirische Beobachtungen, unter anderen zu den Spezialfällen $x^y - y^x = 1$ und $x^p - q^y = 1$, wobei p und q Primzahlen sind, ohne Beweis an und schreibt, dass er die Arbeit an diesem Thema nach einem erfolglosen Jahr aufgegeben hatte.

Lebesgues Resultat sollte für längere Zeit das einzige Ergebnis zu Catalans Vermutung gewesen sein. Erst 1921 gelang es dem Norweger T. Nagell, der sich mit den diophantischen Gleichungen $x^2 + x + 1 = y^n$ und $x^2 + x + 1 = 3y^n$ beschäftigte, zu zeigen, dass die Gleichung $x^3 - y^q = \pm 1$ keine positive ganzzahlige Lösung hat (siehe dazu Unterkapitel 3.4).
Selberg zeigte 1932 in [57], dass die Gleichung $x^4 - y^n = 1$ keine Lösung in den positiven ganzen Zahlen hat, wenn $n > 1$.

Selbergs Ergebnis wurde 1965 von Chao Ko in [33] obsolet gemacht, denn es gelang ihm zu zeigen, dass die Gleichung $x^2 - y^q = 1$ keine positive ganzzahlige Lösung besitzt, falls $q > 5$ ist. Wir geben in Unterkapitel 3.3 einen kürzeren Beweis für diesen Fall wieder, der von Chein [15] 1976 gefunden wurde.

Damit war die Catalan'sche Vermutung für der Fall gerader Exponenten gezeigt, und die Herausforderung bestand nunmehr darin zu zeigen, dass die Gleichung

$$x^p - y^q = 1 \tag{1.1}$$

mit ungeraden Primzahlen[2] p und q, keine Lösung in den ganzen Zahlen besitzt.

In der 2. Hälfte entwickelten sich verschiedene Herangehensweisen an das Catalan'sche Problem:

- Ziel der algebraischen Herangehensweise war es Kriterien zu finden, die jede Lösung der Catalan'schen Gleichung (1.1) erfüllen muss.
- Die analytische Herangehensweise bestand darin obere Schranken für die Anzahl und Größe der Lösungen von (1.1) zu finden, und diese immer weiter zu verbessern.
- In den 90er Jahren des 20. Jahrhunderts entwickelte sich eine neue Herangehensweise indem man versuchte durch sukzessives Ausschließen möglicher Exponentenpaare mittels computerunterstützter Berechnungen untere Schranken für die Exponenten möglicher Lösungen von (1.1) zu finden.

Wir betrachten nun separat welche Resultate mit diesen verschiedenen Herangehensweisen jeweils erzielt werden konnten.

1.2 Die algebraische Herangehensweise

Dem britischen Mathematiker J.W.S. Cassels gelang es als erstem ein algebraisches Kriterium für mögliche Lösungen der Catalan'schen Gleichung zu finden. 1960 konn-

[2]Wegen Nagells Erkenntnis durfte man sogar $p, q > 3$ voraussetzen, jedoch bereitete der Fall p oder q gleich 3 in keinem der weiteren Resultate eine gesonderte Behandlung.

te er in [12] zeigen, dass für jede Lösung (x, y, p, q) von (1.1)

$$p|y \quad \text{und} \quad q|y$$

gelten muss. Dieses Teilbarkeitskriterium von Cassels war eine Grundlage für eine Vielzahl der in der weiteren Folge gefundenen Resultate zur Catalan'schen Vermutung, einschließlich Mihailescus Beweis. Weiters benutzte Cassels als erster die Tatsache, dass mit (x, y, p, q) auch $(-y, -x, q, p)$ eine Lösung von (1.1) sein muss.

Inkeri war der erste, der Cassels Ergebnis nutzte um ein weiteres algebraisches Kriterium zu zeigen. Bereits 1964 zeigte er in [28], dass für eine Lösung (x, y, p, q) der Gleichung (1.1) mit $p \equiv 3 \pmod 4$ entweder q ein Teiler der Klassenzahl des imaginärquadratischen Zahlkörpers $\mathbb{Q}(\sqrt{-p})$ ist, oder die folgende Kongruenz gilt:

$$p^{q-1} \equiv 1 \pmod{q^2}.$$

Erst 1990 gelang es Inkeri auch für den Fall $p \equiv 1 \pmod 4$ ein Kriterium zu finden. In [29] zeigte er, dass für jede Lösung (x, y, p, q) der Gleichung (1.1) gilt

$$q \mid h(\mathbb{Q}(\zeta_p)) \quad \text{oder} \quad p^{q-1} \equiv 1 \pmod{q^2},$$

wobei ζ_p für die p-te Einheitswurzel $\mathrm{e}^{\frac{2\pi i}{p}}$ steht, folglich $\mathbb{Q}(\zeta_p)$ der p-te Kreisteilungskörper ist, und h die Klassenzahl bezeichne.
Dieses Ergebnis ist nun symmetrisch in p und q. Primzahlenpaare (p, q) die die Kongruenzen $p^{q-1} \equiv 1 \pmod{q^2}$ und $q^{p-1} \equiv 1 \pmod{p^2}$ erfüllen nannte man Wieferich Paare, nach dem deutschen Mathematiker Wieferich, der Anfang des 20. Jahrhunderts in [63] das Kriterium $2^{p-1} \equiv 1 \pmod{p^2}$ für den großen Fermat'schen Satz zeigte.[3] Es stellte sich heraus, dass solche Wieferich Paare sehr selten sind.

Der Nachteil von Inkeris Kriterium war jedoch die nahezu unmögliche Berechnung der Klassenzahl $h(\mathbb{Q}(\zeta_p))$ für große p. Die erste Verbesserung erzielte Mignotte, der in [43] in Inkeris Kriterium $\mathbb{Q}(\zeta_p)$ durch den Körper $\mathbb{Q}(\xi)$, wobei $\xi := \zeta_p + \zeta_p^m + \cdots + \zeta_p^{m^{l-1}}$ für bestimmte m und l sei, ersetzen konnte, sodass die Klassenzahl $h(\mathbb{Q}(\xi))$ für viele p leichter zu bestimmen war.
Die nächste Verbesserung gelang Schwarz 1995 in [56]: Er konnte die Klassenzahl $h(\mathbb{Q}(\zeta_p))$ in Inkeris Kriterium durch die relative Klassenzahl $h^-(\mathbb{K}_p)$ ersetzen, wobei $\mathbb{K}_p$ der kleinste imaginäre Unterkörper von $\mathbb{Q}(\zeta_p)$ sei. Der Vorteil der relativen Klassenzahl besteht darin, dass für ihre Berechnung, im Gegensatz zur Klassenzahl, elementare Formeln existieren.

Ein weiteres Bestreben zur Verbesserung der Kriterien war es, die Klassenzahlbedingung von der Wieferichbedingung zu entkoppeln. Einen ersten Teilerfolg in diese Richtung erzielten Mignotte und Roy 1997. Sie konnten in [47] zunächst für den Fall $p \equiv q \equiv 3 \pmod 4$ die Klassenzahlbedingung eliminieren. Im darauffolgenden Jahr gelang es Steiner in [59] dies auch für den Fall $p \equiv 3 \pmod 4$ und $q \equiv 5 \pmod 8$ zeigen.

Schließlich gelang es Mihailescu 1999 in [48] die Klassenzahlbedingung komplett zu eliminieren. Durch Anwendung des Satzes von Stickelberger konnte er in einem

[3] Wieferich zeigte, dass falls die Gleichung $x^p + y^p + z^p = 0$ mit ungerader Primzahl p eine Lösung mit $p \nmid xyz$ besitzt, dann muss die Kongruenz $2^{p-1} \equiv 1 \pmod{p^2}$ erfüllt sein

kurzem und eleganten Beweis das Wieferichkriterium ohne Einschränkungen zeigen: Für jede Lösung (x, y, p, q) von (1.1) muss also

$$p^{q-1} \equiv 1 \,(\mathrm{mod}\, q^2) \quad \text{und} \quad q^{p-1} \equiv 1 \,(\mathrm{mod}\, p^2)$$

gelten. In Unterkapitel 4.2 werden wir uns Mihailescus Beweis dieses Kriteriums widmen.

Ungefähr zur gleichen Zeit als Mihailescu seinen Beweis für das Wieferich Kriterium fand, gelang es den Franzosen Bugeaud und Hanrot auch die Teilbarkeitsbedingung an die Klassenzahl unabhängig von der Wieferichbedingung zu zeigen. In [10] konnten sie beweisen, dass falls eine Lösung (x, y, p, q) von (1.1) existiert mit $q > p$, dann muss

$$q \mid h(\mathbb{Q}(\zeta_p))$$

gelten. Obwohl Mihailescu dieses Ergebnis in seinem Beweis der Catalan'schen Vermutung nicht voraussetzt hat es seine Arbeit stark inspiriert. Wir geben in Unterkapitel 6.3 einen Beweis für dieses Kriterium von Bugeaud und Hanrot.

1.3 Die analytische Herangehensweise

Zunächst betrachtete man die Gleichung (1.1) mit jeweils fixierten Variablen (x, y) oder (p, q) um Aussagen über die Anzahl der möglichen Lösungen in diesen Fällen zu gewinnen.

Für feste p und q folgt aus einer Arbeit von Siegel [58], dass die verallgemeinere Catalan'sche Gleichung $x^p - y^q = k$ nur endlich viele Lösungen besitzt, wie Mahler 1953 in [41] zeigen konnte.
Hyyrö gelang es 1964 in [26] zu zeigen, dass für feste Exponenten p und q die Gleichung (1.1) maximal $\exp(631p^2q^2)$ Lösungen besitzen kann. Er gab auch einen Algorithmus an, mit dem alle Lösungen für diesen Fall, sofern welche existieren, gefunden werden können.
Weiters konnte Hyyrö in derselben Arbeit durch Verwendung von Cassels Teilbarkeitskriterium auch untere Schranken für mögliche Lösungen (x, y) in Abhängigkeit von p und q anzugeben:

$$\begin{aligned} x &\geq \max\left\{p^{q-1}(q-1)^q + 1, q(2p+1)(2q^{p-1}+1)\right\} \\ y &\geq \max\left\{q^{p-1}(p+1)^p - 1, p(q-1)(2p^{q-1}(q-1)^q + 1)\right\}. \end{aligned}$$

Einen Teil dieses Ergebnisses werden wir in Kapitel 4 beweisen. (Satz 4.1.7)

Alan Baker wandte 1968 in [2] die von ihm entwickelte Theorie der Linearformen in Logarithmen algebraischer Zahlen auf die Gleichung $x^p - y^q = k$ an und konnte folgende obere Schranke für die Größe möglicher Lösungen (x, y), bei festgehaltenen $p, q \geq 3$ angeben:

$$\max\{x, y\} < \min\left\{\exp\exp\left((5p)^{10}(q^{10q}|k|)^{q^2}\right), \exp\exp\left((5q)^{10}(p^{10p}|k|)^{p^2}\right)\right\}. \quad (1.2)$$

Für den Fall mit festgehaltenen x und y folgt aus einem Satz von Gel'fond aus [23],

dass es nur endlich viele Lösungen (p, q) geben kann.
Im Jahr 1952 bewies LeVeque in [40], dass für die Gleichung $x^p - y^q = 1$ mit festen $(x, y) \neq (3, 2)$ nur maximal eine Lösung existiert. Ein Jahr später vereinfachte Cassels in [11] LeVeques Beweis und gab einen Algorithmus zur Auffindung der eventuellen Lösung an.

Hyyrö beschäftigte sich noch mit weiteren Fällen:
So gelang es ihm in [27] zu zeigen, dass die Gleichung (1.1) maximal eine Lösung hat, falls x und q oder y und p vorgegeben sind. In der gleichen Arbeit konnte er auch eine obere Schranke für die Anzahl der Lösungen angeben, falls entweder x oder y festgehalten wird.

Ein Durchbruch für den allgemeinen Fall der Catalan'schen Vermutung gelang 1976 schließlich dem Niederländer Robert Tijdeman. Er verwendete Erkenntnisse aus Bakers "sharpening papers" ([3],[4],[5]) über Linearformen in Logarithmen und zeigte, dass es effektiv berechenbare obere Schranken für alle Unbekannten in (1.1) gibt und die Anzahl der Lösungen der Catalan'schen Gleichung somit endlich sein muss. Tijdeman berechnete diese Schranken nicht selbst, aber bereits im darauffolgenden Jahr leitete Langevin in [36] explizite Schranken aus Tijdemans Arbeit ab diese waren von der Größenordnung:

$$\max\{p, q\} \leq 10^{110}, \qquad \max\{x, y\} \leq \exp\exp\exp\exp 700.$$

Die wichtige Erkenntnis aus Tijdemans Arbeit bestand dabei in der Beschränkung der Exponenten p und q, die Abschätzung von $\max\{x, y\}$ folgt direkt aus (1.2).

Das Bestreben der Vertreter der analytischen Herangehensweise lag nun in weiterer Folge darin, die obere Schranke für die Exponenten so weit wie möglich zu verringern. So gelang es Glass, Meronk, Okada und Steiner 1994 in [24] die obere Schranke für p und q auf $3,42 \cdot 10^{28}$ zu senken.
Die Anwendung neuer Erkenntnisse über Linearformen in Logarithmen [6] liefert schließlich kurz vor der Jahrtausendwende folgende, bis heute beste auf diesem Weg bewiesene, obere Schranken für die Exponenten einer möglichen Lösung der Catalan'schen Gleichung (siehe [44]):

$$\min\{p, q\} < 7,15 \cdot 10^{11}, \qquad \max\{p, q\} < 7,78 \cdot 10^{16}. \tag{1.3}$$

1.4 Die computerunterstützte Herangehensweise

Nachdem Tijdeman gezeigt hatte, dass nur endlich viele mögliche Lösungen der Catalan'schen Gleichung existieren, war klar, dass ein Ausprobieren sämtlicher infrage kommender Möglichkeiten theoretisch eine Lösung für das Catalan'sche Problem liefern würde. Jedoch waren die tatsächlich bekannten oberen Schranken für die Variablen astronomisch hoch, sodass an eine praktische Umsetzung dieser Vorgehensweise nicht zu denken war. Doch die algebraischen Kriterien von Inkeri und deren Verbesserungen, durch die man eine Vielzahl der Möglichkeiten a priori ausschließen konnte, und die stetige Weiterentwicklung der Computer nährten die Hoffnungen,

dass man durch Unterstützung von Computerberechnungen vielleicht doch irgendwann das Catalan'sche Problem vollständig lösen könnte. Man begann damit untere Schranken für die Exponenten möglicher Lösungen aufzustellen.

Nachdem Inkeri 1990 sein Kriterium gefunden hatte, machte man sich zunächst auf die Suche nach Wieferich Paaren. Unter Verwendung der oberen Schranken, die sich aus der Anwendung der Theorie der Linearformen in Logarithmen, ergaben fand man heraus, dass nur 3 solcher Paare mit $\min\{p, q\} < 10^5$ zu berücksichtigen waren, nämlich $(83, 4871)$, $(193, 4877)$ und $(2903, 18787)$. Mignotte entwickelte in [42] ein elementares Kriterium, mit dem er die ersten beiden Paare ausschließen konnte. Schließlich gelang es auch das dritte Paar auszuschließen, die Klassenzahlbedingung in Inkeris Kriterium verhinderte jedoch vorläufig noch das Aufstellen einer unteren Schranke für p und q.

Dies gelang Mignotte erst durch seine Verbesserung der Klassenzahlbedingung in [43], er konnte zunächst die Schranke $\min\{p, q\} \geq 97$ angeben.
Das Kriterium von Schwarz erleichterte die Verifizierung der Klassenzahlbedingung bedeutend. Noch im gleichen Jahr, 1995, konnten Mignotte und Roy mit diesem Kriterium in [46] zeigen, dass $\min\{p, q\} \geq 10651$.
Nach mehreren Jahren (Computer-)Rechenzeit konnten Mignotte und Roy die Schranke noch um eine Zehnerpotenz heben. 1997 verkündeten sie in [47] dass $\min\{p, q\} \geq 10^5$.

Der nächste Fortschritt gelang Mignotte durch Anwendung des Kriteriums von Bugeaud und Hanrot, wodurch die Schranke auf $\min\{p, q\} \geq 10^6$ gehoben werden konnte (siehe [44]).
Mihailescus von Klassenzahlen unabhängiges Wieferich Kriterium erleichterte die Berechnungen abermals, sodass Mignotte im März 2000 eine Abschätzung der Exponenten von $\min\{p, q\} \geq 10^7$ bekannt geben konnte.

Schließlich konnte Granville in [25] vermelden, dass Berechnungen von Grantham und Wheeler eine Anhebung der unteren Schranke auf

$$\min\{p, q\} \geq 3 \cdot 10^8$$

ermöglichten. Zusammen mit der oberen Schranke $\max\{p, q\} < 7,78 \cdot 10^{16}$ aus (1.3) war somit gezeigt, dass jede Lösung der Gleichung $x^m - y^n = 1$ Primzahlexponenten haben musste.
Schließlich merkte Granville in seinem Artikel noch an, dass man sich einer Lösung des Catalan'schen Problems durch Computerberechnungen zwar schon annähere, aber eine weitere Verbesserung der oberen Schranken durch neue Erkenntnisse wohl noch vonnöten wäre bevor man die Catalan'sche Vermutung schließlich mit einer finalen Computerberechnung verifizieren könnte.

1.5 Der Beweis der Catalan'schen Vermutung

Im Frühjahr 2002 ging die Meldung um die Welt, dass der, zu der Zeit an der Universität in Paderborn beschäftigte, rumänische Mathematiker Preda Mihailescu die beinahe 160 Jahre alte Catalan'sche Vermutung bewiesen hatte.

Die entscheidende neue Erkenntnis dabei lieferte jedoch nicht eine noch umfangreichere Computerberechnung sondern die Anwendung eines Satzes von Thaine aus [60], der gewissermaßen eine Erweiterung des Satzes von Stickelberger für reelle Zahlkörper darstellt.

Mihailescus Beweis wurde schließlich in [49] veröffentlicht. Er gliedert sich in zwei Teile:

1. Fall $p \mid q-1$ oder $q \mid p-1$

2. Fall $p \nmid q-1$ und $q \nmid p-1$

Die Behandlung dieser beiden Fälle ist sehr unterschiedlich. Um den ersten Fall auszuschließen folgt Mihailescu der Argumentation von Tijdeman, gepaart mit neueren Erkenntnissen aus der Theorie der Linearformen in Logarithmen, und beruft sich schließlich auf die von Mignotte und Roy [47] berechnete Schranke $\min\{p,q\} > 10^5$ um zu zeigen, dass eine Lösung der Catalan'schen Gleichung in diesem Fall dem Wieferich Kriterium widersprechen würde.

Für den Fall $p \nmid q-1$ und $q \nmid p-1$ führt Mihailescu eine Potenzreihenanalyse zur Untersuchung der q-ten Wurzeln bestimmter Elemente von $\mathbb{Q}(\zeta_p)$ durch und wendet den Satz von Thaine an um zu zeigen, dass die Existenz einer Lösung der Catalan'schen Gleichung in diesem Fall zu einem "Überfluss" an q-primären Kreisteilungseinheiten führen würde.
Weiters verwendet Mihailescu in seinem Beweis das Ergebnis von Cassels, die Abschätzungen von Hyyrö und das von ihm gefundene Wieferich Kriterium. Somit entstand der Beweis also durch eine Zusammenführung der drei verschiedenen Herangehensweisen.

Wir widmen uns in Kapitel 5 dem Beweis von Mihailescu und folgen dabei größtenteils den Ausführungen von Bilu [7], der Mihailescus Argumente noch vereinfachen konnte.

Obwohl die Catalan'sche Vermutung damit gezeigt war, war Mihailescu nicht damit zufrieden, dass sich sein Beweis noch auf computerunterstützte Berechnungen berufen musste. Doch bereits im darauffolgenden Jahr gelang es ihm auch für den Fall $p \mid q-1$ oder $q \mid p-1$ einen eigenständigen Beweis zu finden, der weder Computerberechnungen noch die Theorie der Linearformen in Logarithmen verwendet. Stattdessen folgt er der Argumentation von Bugeaud und Hanrot [10] und zeigt durch abermalige Anwendung des Satzes von Stickelberger dass auch in diesem Fall keine Lösung der Catalan'schen Gleichung existiert.
Dieser Beweis wurde schließlich in [51] veröffentlicht. Wir widmen Kapitel 6 diesem Beweis, halten uns dabei aber wieder an die Ausführungen Bilus [8], der auch diesen Beweis Mihailescus überarbeitete.

Somit existieren nun für beide Fälle algebraische Beweise und Catalan's Vermutung wird oft auch schon als Satz von Mihailescu bezeichnet.
Mihailescu gelang es mittlerweile seinen Beweis sogar noch ein Stück selbstständiger zu machen. In [50] zeigte er einen Satz, der die Anwendung des Satzes von Thaine im Beweis der Catalan'schen Vermutung ersetzt.

Kapitel 2

Mathematische Grundlagen

Die Catalan'schen Vermutung wurde mit Mitteln aus dem Gebiet der algebraischen Zahlentheorie, speziell der Theorie der Kreisteilungskörper, bewiesen. Wir wollen deshalb in diesem Kapitel zunächst einen Überblick über diesen Teilbereich der Mathematik geben, und in weiterer Folge die theoretischen Grundlagen für den Beweis der Catalan'schen Vermutung darlegen.

Aus Gründen der Vollständigkeit fangen wir dabei zunächst mit den, wohl hinlänglich bekannten, grundlegenden Teilbarkeitseigenschaften ganzer Zahlen an und wiederholen auch die elementaren Definitionen aus dem Bereich der Algebra. Es sei dabei jedoch darauf hingewiesen, dass bereits die Ergebnisse aus Unterkapitel 2.1 weitestgehend für die nichttriviale Behandlung der Spezialfälle in Kapitel 3 ausreichen.

Weiters geben wir einen Überblick über die Grundlagen der algebraischen Zahlentheorie, über Körpererweiterungen, Dedekind'sche Ringe und algebraischen Zahlkörper. Danach betrachten wir den für uns interessanten Fall von Zahlkörpern, die Kreisteilungskörper, genauer und führen schließlich die für den Beweis der Catalan'schen Vermutung relevanten Ergebnisse aus dieser Theorie an.

Dieses Kapitel orientiert sich einerseits an den von Prof. Drmota an der TU Wien gehaltenen Vorlesungen Zahlentheorie [21] und algebraischer Zahlentheorie [20], andererseits verweisen wir für die Sektionen über elementare Zahlentheorie und Algebra auf die Bücher [39], [64], [9] und [30], für die weiterführenden Sektionen über algebraische Zahlentheorie auf [35], [52] und [55], und für die Sektionen über die Theorie der Kreisteilungskörper ist speziell [62] als Referenz hervorzuheben.

Da es sich bei den in diesem Kapitel angeführten Sätzen um grundlegende und allgemein bekannte Erkenntnisse handelt, führen wir hier keine Beweise an, sondern verweisen jeweils auf entsprechende Stellen in der Literatur.

2.1 Teilbarkeit in den ganzen Zahlen

Ganz einfach gesprochen beschäftigt sich die Zahlentheorie, wie ihr Name es schon sagt, mit den Eigenschaften der ganzen Zahlen. Deshalb wollen wir nun kurz deren

grundlegendsten Teilbarkeitseigenschaften anführen.

Auf den ganzen Zahlen ist die Teilbarkeitsrelation wie folgt definiert.

Definition 1
*Seien a, b ganze Zahlen, dann sagt man a **teilt** b, in Zeichen $a|b$, wenn es eine ganze Zahl q gibt mit $aq = b$.*

Nicht alle Zahlen stehen zueinander in einer Teilbarkeitsrelation, man kann jedoch bezüglich jeder positiven ganzen Zahl eine Kongruenzrelation definieren:

Definition 2
*Seien a, b, m ganze Zahlen, $m \geq 1$, dann sagt man a ist **kongruent** zu b modulo m, in Zeichen $a \equiv b \,(\mathrm{mod}\, m)$, wenn $m \mid a - b$.*

Der Divisionsalgorithmus liefert

Satz 2.1.1 (Division mit Rest)
Für je zwei ganze Zahlen a, b mit $b \neq 0$ gibt es ganze Zahlen q, r mit $0 \leq r < |b|$ sodass $a = qb + r$. (q nennt man den Quotient und r den Rest.)

Beweis. Siehe zum Beispiel [53] Seite 21. □

Es gibt also zu jeder ganzen Zahl a eine modulo m kongruente Zahl r, die dem Betrag nach kleiner ist als m. Man nennt die Menge

$$\overline{a} := \{b \in \mathbb{Z} \mid a \equiv b \,(\mathrm{mod}\, m)\} = a + m\mathbb{Z}$$

die von a erzeugte **Restklasse** modulo m. Auf der Menge der Restklassen kann man durch $\overline{a} + \overline{b} = \overline{a + b}$ und $\overline{a} \cdot \overline{b} = \overline{ab}$ in natürlicher Weise eine Addition und eine Multiplikation definieren, die Wahl der Repräsentanten aus den jeweiligen Restklassen ist dabei nicht relevant. Man bezeichnet die Menge aller Restklassen mit $\mathbb{Z}/m\mathbb{Z}$ oder $\mathbb{Z}_m$ und es gilt $|\mathbb{Z}/m\mathbb{Z}| = m$ und $\langle \mathbb{Z}/m\mathbb{Z}, +, \cdot \rangle$ ist ein kommutativer Ring mit Einselement. (Mehr dazu in Sektion 2.2.)

Ein wichtiger Begriff ist der des größten gemeinsamen Teilers:

Definition 3
*Seien $a_1, \ldots, a_n$ ganze Zahlen, dann heißt eine ganze Zahl d **größter gemeinsamer Teiler** von $a_1, \ldots, a_n$, in Zeichen $ggT(a_1, \ldots, a_n)$, wenn gilt $d|a_i$ für alle $i \in \{1, \ldots, n\}$ und weiters für jedes $t \in \mathbb{Z}$ mit $t|a_i$ für alle $i \in \{1, \ldots, n\}$ folgt, dass $d|t$.*
*Ist $ggT(a, b) = 1$, so nennt man a und b **teilerfremd** oder relativ prim.*

Für $n = 2$ liefert der bekannte Euklidische Algorithmus eine Methode zur Berechnung von $ggT(a, b)$. Für $n > 2$ ist die Berechnung durch folgende Rekursionsformel möglich:

$$ggT(a_1, \ldots, a_n) = ggT\left(ggT(a_1, \ldots, a_{n-1}), a_n\right).$$

Der größte gemeinsame Teiler hat folgende Eigenschaften:

Satz 2.1.2
Für n verschiedene ganze Zahlen $a_1, \ldots, a_n$ gibt es einen größten gemeinsamen Teiler d, der bis auf das Vorzeichen eindeutig bestimmt ist.
Weiters gilt:

(i) *Es gibt ganze Zahlen $x_1, \ldots, x_n$ mit $ggT(a_1, \ldots, a_n) = \sum_{i=1}^{n} x_i a_i$.*

(ii) *Aus $ggT(a_1, \ldots, a_n) = d$ folgt $ggT\left(\frac{a_1}{d}, \ldots, \frac{a_n}{d}\right) = 1$.*

(iii) *Aus $ggT(a, b) = 1$ und $a|bc$ folgt $a|c$.*

Beweis. Siehe [39] Seite 14-15. □

Die für die Darstellung des größten gemeinsamen Teilers als Summe benötigten x_i ergeben sich ebenfalls aus dem Euklidischen Algorithmus.

Ein ganz wesentlicher Begriff in der Zahlentheorie ist jener der Primzahl. Die Primzahlen sind sozusagen die Bausteine aus denen sich die ganzen Zahlen zusammensetzen.

Definition 4
*Eine ganze Zahl $p > 1$ heißt **Primzahl**, wenn sie nur die trivialen Teiler $\pm 1, \pm p$ hat. Die Menge aller Primzahlen bezeichnen wir mit $\mathbb{P}$.*

Bereits Euklid konnte mit einem eleganten Argument zeigen, dass es unendlich viele Primzahlen gibt.
Jede ganze Zahl die dem Betrag nach ≥ 2 ist hat mindestens eine Primzahl als Teiler. Wie oft sie durch eine bestimmte Primzahl teilbar ist besagt die p-adische Bewertung:

Definition 5
*Sei p eine Primzahl und $a \in \mathbb{Z} \setminus \{0\}$, dann bezeichnet $\nu_p(a)$ den **p-adischen Wert** von a oder die Vielfachheit von p in a:*

$$\nu_p(a) = e \text{ falls } p^e | a, \text{ aber } p^{e+1} \nmid a.$$

Nun können wir den Fundamentalsatz der Zahlentheorie formulieren:

Satz 2.1.3 (Fundamentalsatz der Zahlentheorie)
Jede positive ganze Zahl n lässt sich bis auf die Reihenfolge eindeutig als Produkt von Primzahlen darstellen.

$$n = \prod_{p \in \mathbb{P}} p^{\nu_p(n)} \tag{2.1}$$

Beweis. Siehe [39] Seite 18-19. □

Hier muss man festhalten, dass für jedes n in (2.1) immer nur endlich viele $\nu_p(n)$ ungleich 0 sein können.

Die Darstellung in (2.1) nennt man **Primfaktorzerlegung**, sie ist für große Zahlen nur sehr schwer zu finden (viele gängige Verschlüsselungssysteme basieren auf diesem

Problem). Kennt man jedoch die Primfaktorzerlegung verschiedener Zahlen, so kann man auch ihren größten gemeinsamen Teiler leicht bestimmen:

Satz 2.1.4
Seien $a_1, \ldots, a_n$ ganze Zahlen, dann gilt

$$ggT(a_1, \ldots, a_n) = \prod_{p \in \mathbb{P}} p^{min(\nu_p(a_1), \ldots, \nu_p(a_n))}$$

Beweis. Siehe [39] Seite 19. □

2.2 Gruppen und Ringe

Ebenfalls aus Vollständigkeitsgründen beginnen wir mit den Definitionen der einfachsten algebraischen Strukturen:

Definition 6
*Ist auf der Menge G eine Verknüpfung $* : G \times G \to G$, $(x, y) \mapsto x * y$ definiert, die das Assoziativgesetz erfüllt: $(a * b) * c = a * (b * c)$ für alle $a, b, c \in G$, dann nennt man $\langle G, * \rangle$ eine **Halbgruppe**.*
*Man nennt eine Halbgruppe $\langle G, * \rangle$ kommutativ oder **abelsch**, falls das Kommutativgesetz gilt: $a * b = b * a$ für alle $a, b \in G$.*
*Ein Element $e \in G$ heißt **neutrales Element** (in multiplikativen Halbgruppen auch Einselement), falls für alle $a \in G$ gilt: $a * e = e * a = a$. Eine Halbgruppe mit neutralem Element nennt man **Monoid**.*
*Ein Element a eines Monoids $\langle G, * \rangle$ nennt man invertierbar, wenn es ein zu a **inverses Element** $a^{-1} \in G$ gibt mit $a * a^{-1} = a^{-1} * a = e$. Ein Monoid in dem jedes Element invertierbar ist nennt man eine **Gruppe**.*

Das bekannteste Beispiel einer Gruppe ist $\langle \mathbb{Z}, + \rangle$, ihr neutrales Element ist 0. Weitere Beispiele für Gruppen sind etwa die Potenzmenge einer Menge S mit der Vereinigung oder dem Durchschnitt: $\langle \mathbf{P}(S), \cup \rangle$ und $\langle \mathbf{P}(S), \cap \rangle$, wobei einmal die leere Menge und einmal die Gesamtmenge das neutrale Element ist. Diese Gruppen sind sich in ihrer Struktur sehr ähnlich, wir formalisieren diese Ähnlichkeit durch die folgende Definition:

Definition 7
*Seien $\langle G, * \rangle$ und $\langle \widetilde{G}, \widetilde{*} \rangle$ Gruppen, eine Abbildung $\varphi : G \to \widetilde{G}$ heißt (Gruppen-)**Homomorphismus**, falls für alle $a, b \in G$ gilt: $\varphi(a) \,\widetilde{*}\, \varphi(b) = \varphi(a * b)$. $\langle G, * \rangle$ und $\langle \widetilde{G}, \widetilde{*} \rangle$ nennt man **homomorph**.*
*Falls φ bijektiv ist spricht man von einem **Isomorphismus** und schreibt $G \cong \widetilde{G}$. Ist außerdem $G = \widetilde{G}$ so nennt man φ einen **Automorphismus**.*

Im obigen Beispiel ist die Abbildung die jede Menge auf ihr Kompliment abbildet ein Automorphismus der Gruppen $\langle \mathbf{P}(S), \cup \rangle$ und $\langle \mathbf{P}(S), \cap \rangle$.

Definition 8
*Sei $\langle G, * \rangle$ eine Gruppe. Eine nichtleere Teilmenge $U \subseteq G$ nennt man **Untergruppe**, falls $\langle U, * \rangle$ selbst eine Gruppe ist.*

Für jedes Gruppenelement $g \in G$ erhält man durch n-malig wiederholte Verknüpfung von g mit sich selbst dessen n-te **Potenz** eines Elementes wie folgt rekursiv definieren:

$$g^0 := e, \qquad g^1 := g, \qquad g^n := g^{n-1} * g \text{ falls } n > 0, \qquad g^n := (g^{-n})^{-1} \text{ falls } n < 0.$$

Man bezeichnet mit $< g >:= \{g^n \mid n \in \mathbb{Z}\}$ die von g erzeugte zyklische Untergruppe.

Definition 9
*Eine Gruppe $\langle G, * \rangle$ heißt **zyklisch**, falls es ein $g \in G$ gibt, sodass $G =< g >$.*

Wegen $g^x * g^y = g^{x+y} = g^y * g^x$ ist jede zyklische Gruppe insbesondere auch abelsch.

Definition 10
*Die **Ordnung der Gruppe** $\langle G, * \rangle$ ist definiert als die Mächtigkeit $|G|$ der Menge G.*
*Die **Ordnung eines Elements** $g \in G$ ist definiert als die Mächtigkeit der von g erzeugten zyklischen Untergruppe: $ord(g) := | < g > |$.*

Den Zusammenhang zwischen der Ordnung einer Gruppe und der eines Elementes beleuchtet der folgende Satz von Cauchy:

Satz 2.2.1 (Cauchy)
Sei $\langle G, * \rangle$ eine Gruppe und sei die Primzahl p ein Teiler der Ordnung von G, dann enthält G ein Element der Ordnung p.

Beweis. Siehe zum Beispiel [30] Kapitel II Satz 1.2 □

Von besonderer Bedeutung sind Untergruppen deren Ordnung eine Primzahlpotenz ist:

Definition 11
*Sei $\langle G, * \rangle$ eine Gruppe und p eine Primzahl, dann heißt jede Untergruppe von G deren Ordnung eine Potenz von p ist eine **p-Untergruppe** von G.*
*Sei $ord(G) = p^n q$, sodass p und q teilerfremd sind, dann nennt man jede Untergruppe der Ordnung p^n eine **p-Sylow Untergruppe**.*
*Die Menge aller Elemente deren Ordnung eine Potenz von p ist bezeichnet man als die **p-Komponente** von G.*

Die Existenz von p-Sylow Untergruppen folgt aus dem Satz von Sylow:

Satz 2.2.2 (Sylow)
Sei $\langle G, * \rangle$ eine endliche Gruppe der Ordnung $|G| = p^m \cdot q$, wobei q teilerfremd zur Primzahl p ist, dann gibt es zu jedem $1 \leq k \leq m$ mindestens eine Untergruppe von G der Ordnung p^k.

Beweis. Siehe [30] Kapitel II, Satz 1.6 □

Aus dem Satz von Cauchy folgt nun, dass es genau eine p-Sylow Untergruppe gibt, die p-Komponente.

Im allgemeinen Fall einer nicht notwendigerweise endlichen Gruppe G, nennt man eine Untergruppe U als p-Untergruppe, wenn die Ordnung jedes Elements von U

eine Potenz von p ist. Eine Untergruppe S heißt dann p-Sylow Untergruppe, wenn sie maximal in der Menge der p-Untergruppen von G ist. Die Existenz von p-Sylow Untergruppen folgt im allgemeinen Fall aus dem Lemma von Zorn.[1]

Für eine Untergruppe $U \subset G$ und ein Element $g \in G$ nennt man die Menge $g * U := \{g * u \mid u \in U\}$ eine **Linksnebenklasse** von U (analog definiert man Rechtsnebenklassen).
Mit dem **Index** einer Untergruppe U bezeichnet man die Mächtigkeit der Menge der Linksnebenklassen (bzw. der Rechtsnebenklassen), man schreibt $ind(U)$ oder $[G : U]$.

Definition 12
*Eine Untergruppe N einer Gruppe $\langle G, * \rangle$ heißt **Normalteiler**, falls für jedes $x \in G$ gilt: $x * N = N * x$.*

In einer abelschen Gruppe ist jede Untergruppe Normalteiler und die Unterscheidung zwischen Links- und Rechtsnebenklassen nicht notwendig.
Für jeden Normalteiler N kann man mittels $(x * N) * (y * N) = (x * (N * y)) * N = (x * y) * (N * N) = (x * y) * N$ die Verknüpfung auf die Menge der Nebenklassen G/N verallgemeinern und erhält so die **Faktorgruppe** $\langle G/N, * \rangle$.

Die algebraische Struktur der ganzen Zahlen ist jedoch komplexer als die einer Gruppe, man führt daher die Definition eines Ringes ein:

Definition 13
*Man nennt eine Menge R mit zwei Verknüpfungen "$+$" und "$\cdot$", in Zeichen $\langle R, +, \cdot \rangle$, einen **Ring**, wenn gilt:*

(i) $\langle R, + \rangle$ *ist eine kommutative Gruppe,*

(ii) $\langle R, \cdot \rangle$ *eine Halbgruppe*

(iii) es gelten die Distributivgesetze $a(b + c) = ab + ac$ *und* $(a + b)c = ac + bc$.

*R heißt **kommutativer Ring**, falls $\langle R, \cdot \rangle$ kommutativ ist.*
*R heißt **Ring mit 1**, falls $\langle R, \cdot \rangle$ ein Einselement $1 \neq 0$ besitzt.*
*Ein Element a eines Ringes R heißt **Nullteiler**, falls es ein $b \in R \setminus \{0\}$ gibt, sodass $ab = 0$ oder $ba = 0$.*
*Ein kommutativen Ring mit 1 heißt **Integritätsbereich**, falls er keine von 0 verschiedenen Nullteiler besitzt, oder anders gesagt wenn $\langle R \setminus \{0\}, \cdot \rangle$ ein Monoid ist.*
*Ein kommutativen Ring mit 1 heißt **Körper**, falls jedes Element $\neq 0$ ein multiplikatives Inverses besitzt, oder anders gesagt wenn $\langle R \setminus \{0\}, \cdot \rangle$ eine Gruppe ist.*

Wenn es der Kontext erlaubt lassen wir die Verknüpfungen weg und schreiben für den Ring $\langle R, +, \cdot \rangle$ nur R.

Wie bei Gruppen nennt man eine Teilmenge $U \subseteq R$ einen **Unterring** von $\langle R, +, \cdot \rangle$, wenn $\langle U, +, \cdot \rangle$ selbst ein Ring ist. Ebenso erweitert man den Homomorphiebegriff:

[1] Das Lemma von Zorn besagt, dass jede nichtleere halbgeordnete Menge, in der jede Kette (d.h. jede total geordnete Teilmenge) eine obere Schranke hat, mindestens ein maximales Element enthält.

Man nennt eine Abbildung $\varphi : R_1 \to R_2$ einen **Ringhomomorphismus**, falls $\varphi(a+b) = \varphi(a) + \varphi(b)$ und $\varphi(ab) = \varphi(a)\varphi(b)$ für alle $a, b \in R_1$ gilt.

Die ganzen Zahlen $\mathbb{Z}$ sind ein Integritätsbereich. Analog wie in $\mathbb{Z}$ kann man auch allgemeiner für Integritätsbereiche die Teilbarkeitsrelation und den größten gemeinsamen Teiler zweier Elemente definieren.

Definition 14
*Sei $\langle R, +, \cdot \rangle$ ein Integritätsbereich. Man nennt $a \in R \setminus \{0\}$ eine **Einheit**, falls $a|1$. Die Menge aller Einheiten in R bezeichnet man mit $R^\times$, $\langle R^\times, \cdot \rangle$ ist eine Gruppe, die sogenannte Einheitengruppe.*

Der größte gemeinsame Teiler in einem Integritätsbereich ist dann bis auf eine Einheit eindeutig bestimmt. Für die Primzahlen gibt es zwei verallgemeinerte Definitionen:

Definition 15
*Ein Element $a \in R \setminus (R^\times \cup \{0\})$ heißt **irreduzibel**, falls aus $a = bc$ entweder $b \in R^\times$ oder $c \in R^\times$ folgt.*
*$a \in R \setminus (R^\times \cup \{0\})$ heißt **prim** oder ein Primelement, falls aus $a|bc$ entweder $a|b$ oder $a|c$ folgt.*

Aus der Definition folgt, dass jedes Primelement irreduzibel ist. Im allgemeinen Fall ist jedoch nicht jedes irreduzible Element prim!
Die Primzahlen entsprechen ihrer Definition nach den irreduziblen Elementen von $\mathbb{Z}$, wir werden jedoch sehen, dass sie auch tatsächlich prim, im Sinne dieser Definition sind.

Definition 16
Sei $\langle R, +, \cdot \rangle$ ein Ring.
*Ein Unterring $I \subseteq R$ heißt **Ideal**, wenn $aI \subseteq I$ und $Ia \subseteq I$ für alle $a \in R$ gilt.*
*Ein Ideal I heißt **maximal**, falls $I \neq R$ und es kein Ideal J gibt sodass $I \subset J \subset R$.*
*Ein Ideal I heißt **Primideal**, falls aus $ab \in I$ entweder $a \in I$ oder $b \in I$ folgt.*
*In einem kommutativen Ring nennt man ein Ideal I dass von einem Element a erzeugt wird ein **Hauptideal** und schreibt $I = aR = (a)$.*
*Ein kommutativer Ring mit 1 der nur Hauptideale besitzt heißt **Hauptidealring**.*

Neben Hauptidealringen werden auch noch andere Formen von Ringen häufig betrachtet:

Definition 17
Sei $\langle R, +, \cdot \rangle$ ein Integritätsbereich.
*R heißt **faktorieller Ring** oder ZPE-Ring, falls jedes $a \in R \setminus (R^\times \cup \{0\})$ eine Darstellung als Produkt irreduzibler Elemente besitzt, die bis auf die Reihenfolge und Einheiten eindeutig ist.*
*R heißt **noetherscher Ring**, wenn jede aufsteigende Kette von Idealen $I_1 \subseteq I_2 \subseteq \cdots$ abbricht, d.h. es gibt einen Index N sodass für alle $m \geq N$ immer $I_{m+1} = I_m$ gilt.*
*R heißt **euklidischer Ring**, falls es eine Gradfunktion $\delta : R \setminus \{0\} \to \mathbb{Z}^+ \cup \{0\}$ gibt, sodass für alle $a, b \in R$, $b \neq 0$ Elemente $q, r \in R$ existieren, für die $a = bq + r$ gilt und entweder $r = 0$ oder $\delta(r) < \delta(b)$ ist.*

Für faktorielle und für noethersche Ringe gibt es jeweils Kriterien:

Satz 2.2.3
Sei $\langle R, +, \cdot \rangle$ ein Integritätsbereich.

(i) R ist genau dann ein faktorieller Ring, wenn jedes irreduzible Element von R prim ist und wenn weiters für jede unendliche Folge $a_1, a_2, \ldots \in R$ mit $a_{i+1} | a_i$ $(i \geq 1)$ ein Index n existiert, sodass für alle $k \geq n$ gilt $a_k = \varepsilon_k a_n$ für eine Einheit $\varepsilon_k \in R^\times$.

(ii) R ist genau dann noethersch, wenn es in jeder nichtleeren Menge von Idealen in R ein bezüglich der Inklusionsrelation maximales Element gibt.

(iii) R ist genau dann noethersch, wenn jedes Ideal I endlich erzeugt ist, d.h. es gibt $a_1, \ldots, a_n \in I$ sodass $I = (a_1, \ldots, a_n) = \sum_{i=1}^{n} (a_i)$.

Beweis. Siehe zum Beispiel [30] Kapitel III, Sätze 5.9 und 5.10 □

Weiters bestehen folgende Zusammenhänge:

Satz 2.2.4 *(i) Jeder euklidische Ring ist ein Hauptidealring.*

(ii) Jeder Hauptidealring ist faktoriell und noethersch.

Beweis. Siehe zum Beispiel [30] Kapitel III, Sätze 3.4 und 5.11 □

Die Umkehrung dieser beiden Punkte ist jedoch im Allgemeinen nicht gültig.

Die ganzen Zahlen sind nun, wegen der Division mit Rest und beispielsweise dem Absolutbetrag als Gradfunktion, ein euklidischer Ring und damit in weiterer Folge auch ein Hauptidealring sowie faktoriell und noethersch.

Man verallgemeinert die von den ganzen Zahlen bekannte Kongruenzrelation auf Ringe indem man sagt zwei Elemente a, b sind kongruent modulo einem Ideal I, in Zeichen $a \equiv b \,(\mathrm{mod}\, I)$ oder kurz $a \equiv b \,(I)$, falls $a - b \in I$. Auch hier kann man wieder alle kongruenten Elemente zu Äquivalenzklassen $[a]_I = a + I$ zusammenfassen.
Man faktorisiert R nach dem Ideal I bzw. nach der von I induzierten Kongruenzrelation und bezeichnet die Menge der Äquivalenzklassen mit R/I. Auf dieser kann man in natürlicher Weise Addition und Multiplikation definieren: $[a]_I + [b]_I = [a + b]_I$, $[a]_I \cdot [b]_I = [ab]_I$. Auf diese Weise erhält man wieder einen Ring, den sogenannten **Faktorring** $\langle R/I, +, \cdot \rangle$.

Wir fassen in dem folgenden Satz einige Eigenschaften zusammen:

Satz 2.2.5
Sei $\langle R, +, \cdot \rangle$ ein Integritätsbereich.

(i) Ein Ideal I ist genau dann maximal, wenn R/I ein Körper ist.

(ii) Ein Ideal I ist genau dann ein Primideal, wenn R/I ein Integritätsbereich ist.

(iii) Jedes maximale Ideal ist auch ein Primideal.

(iv) Ein Hauptideal (a) ist genau dann ein Primideal, wenn $a = 0$ oder a ein Primelement ist.

(v) In einem Hauptidealring ist jedes Primideal $\neq \{0\}$ maximal.

Beweis. Siehe zum Beispiel [30] Kapitel III, Sätze 3.2 und 5.2 □

Im Hauptidealring $\mathbb{Z}$ ist also ein Ideal $(m) = m\mathbb{Z}$ also genau dann maximal, wenn m eine Primzahl ist. Genau in diesem Fall ist dann $\mathbb{Z}/m\mathbb{Z}$ ein Körper.

Definition 18
Seien I und J Ideale eines kommutativen Ringes R mit 1.
Als Summe von I und J definiert man die Menge $I + J := \{a + b \mid a \in I, b \in J\}$
Das Produkt von I und J ist definiert durch $I \cdot J := \{a_1b_1 + \cdots + a_nb_n \mid a_i \in I, b_j \in J, n \geq 1\}$

Damit kann man auch für Ideale eine Teilbarkeitsrelation definieren:

Definition 19
Ein Ideal J teilt ein Ideal I, falls es ein Ideal K mit $I = J \cdot K$ gibt.

Aufgrund der Idealeigenschaften gilt für beliebige Ideale I und J immer $I \cdot J \subseteq I \cap J$. Die Teilbarkeitsrelation unter Idealen kehrt somit die Enthaltenseinsrelation um, d.h. aus $I|J$ folgt $J \subseteq I$.
Damit ist die folgende Definition des größten gemeinsamen Teilers von Idealen sinnvoll:

Definition 20
*Der **größte gemeinsame Teiler** beliebiger Ideale $I_1, \ldots, I_n$ von R ist wie folgt definiert:*

$$ggT(I_1, \ldots, I_n) = \sum_{k=1}^{n} I_k.$$

*Die Ideale $II_1, \ldots, I_n$ heißen **teilerfremd**, wenn $R = \sum_{k=1}^{n} I_k$ gilt.*

Für paarweise teilerfremde Ideale $I_1, \ldots, I_n$ gilt:

$$I_1 \cdots I_n = I_1 \cap \cdots \cap I_n$$

Satz 2.2.6 (Chinesischer Restsatz)
Seien $I_1, \ldots, I_n$ paarweise teilerfremde Ideale eines kommutativen Ringes R mit 1, dann ist für beliebige $a_1, \ldots, a_n \in R$ das Kongruenzensystem

$$\begin{aligned} x &\equiv a_1 \pmod{I_1} \\ &\vdots \\ x &\equiv a_n \pmod{I_n} \end{aligned}$$

lösbar. Ist y eine Lösung so sind alle Lösungen gegeben durch die $x \in R$ mit $x \equiv y \pmod{I_1 \cdots I_n}$.

Anders formuliert: durch die Abbildung $x \mapsto (x+I_k)_{1\leq k\leq n}$ ist ein surjektiver Ringhomomorphismus von R auf das direkte Produkt der Ringe R/I_k definiert. Sein Kern ist $I = I_1 \cap \ldots \cap I_n$

Beweis. Siehe zum Beispiel [39] Kapitel 13 Satz 3. □

Daraus folgt für paarweise teilerfremde Ideale $I_1, \ldots, I_n$:

$$R/I \cong R/I_1 \times \cdots \times R/I_n$$

2.3 Moduln

Eine weitere in der algebraischen Zahlentheorie wichtige Struktur ist die des Moduls über einem Ring:

Definition 21
*Sei R ein Ring mit Einselement 1_R. Ein linker Modul über R, kurz ein **linker R-Modul**, ist eine abelsche Gruppe $(M,+)$ zusammen mit einer Abbildung $R \times M \to M, \quad (a,x) \mapsto ax$, so dass*

1. $a(x+y) = ax + ay$
2. $(a+b)x = ax + bx$
3. $a(bx) = (ab)x$
4. $1_R x = x$

für alle $a, b \in R$ und $x, y \in M$ gilt.

Analog kann man auch rechte R-Moduln definieren. Ergebnisse über linke R-Moduln lassen sich direkt in solche über rechte R-Moduln übersetzen. Deshalb betrachten wie im Folgenden linke R-Moduln und bezeichnen sie kurz als R-Moduln.

Ist R ein Körper, so entspricht die Definition eines R-Moduls der eines Vektorraumes wie man ihn aus der Linearen Algebra kennt. Jedoch lassen sich Ergebnisse über Vektorräume natürlich nicht direkt auf Moduln übertragen.

Die folgenden von den Gruppen und Ringen bekannten Strukturbegriffe werden in natürlicher Weise auf Moduln erweitert: Für zwei R-Moduln M, M' heißt eine Abbildung $\varphi : M \to M'$ ein **Homomorphismus von R-Moduln**, wenn $\varphi(x+y) = \varphi(x) + \varphi(y)$ und $\varphi(ax) = a\varphi(x)$ für alle $x, y \in M$ und $a \in R$ gilt. Ist φ bijektiv so spricht man von einem R-Modulisomorphismus und schreibt $M \cong M'$.
Eine Teilmenge N eines R-Moduls M heißt **Untermodul** von M, wenn $0 \in N$, $x + y \in N$ und $ax \in N$ für alle $x, y \in N$ und $a \in R$ gilt.
Ist nun N ein Untermodul eines R-Moduls M, so wird auf der Faktorgruppe M/N mittels

$$a(x+N) := ax + N$$

für alle $a \in R, x \in M$ eine R-Modulstruktur eingeführt. Man nennt M/N mit dieser Struktur den **Faktormodul** von M nach N.

Definition 22
Sei M ein R-Modul und $x \in M$. Die Menge

$$\mathrm{ann}_R(x) := \{a \in R \mid ax = 0\}$$

*nennt man den **Annullator** von x in R. Die Menge*

$$Rx := \{ax \mid a \in R\}$$

*heißt der von x **erzeugte Untermodul** von M.*
Analog definiert man für Teilmengen $X \subseteq M$:
$\mathrm{ann}_R(X) := \{a \in R \mid ax = 0, \forall x \in X\}$ *ist der Annullator von X in M und $\sum_{x \in X} Rx$ der von X erzeugten Untermodul von M.*
*M heißt ein **zyklischer R-Modul** falls es ein $m \in M$ gibt sodass $M = Rm$.*
*X heißt ein **Erzeugendensystem** von M (über R) falls $M = \sum_{x \in X} Rx$.*

In einem kommutativen Ring ist der Annullator ein Ideal und zwischen Annullator und erzeugtem Untermodul besteht folgender Zusammenhang:

Satz 2.3.1
Sei M ein R-Modul und $x \in M$, dann gilt

$$R/\mathrm{ann}_R(x) \cong Rx.$$

Für einen zyklischen R-Modul M gilt also $R/\mathrm{ann}_R(M) \cong M$.

Beweis. Siehe zum Beispiel [30] Kapitel VII Satz 2.2. □

Definition 23
*Eine Teilmenge $X \subseteq M$ eines R-Moduls M heißt **linear unabhängig**, wenn für alle $x_1, \ldots, x_n \in X$ und $a_1, \ldots, a_n \in R$ gilt: Aus $a_1x_1 + \cdots + a_nx_n = 0$ folgt $a_1 = \cdots = a_n = 0$.*
*Ein linear unabhängiges Erzeugendensystem (über R) nennt man **Basis** (über R).*
*Ein R-Modul M heißt **frei** (über R), wenn er eine Basis besitzt.*
*Ein R-Modul M heißt **endlich erzeugbar**, wenn er ein endliches Erzeugendensystem besitzt.*

Für die Basen von Moduln über kommutativen Ringen gilt:

Satz 2.3.2
Sei R ein kommutativer Ring mit 1 ungleich dem Nullring, und seien A und B zwei endliche Basen eines R-Moduls M, dann gilt: $|A| = |B|$.

Beweis. Siehe zum Beispiel [30] Kapitel VII Satz 4.3. □

Definition 24
*Wenn, wie unter den obigen Voraussetzungen, je zwei Basen eines freien R-Moduls dieselbe Kardinalität haben, so nennt man diese Kardinalität den **Rang** dieses freien R-Moduls.*

2.4 Körpererweiterungen

Zunächst betrachten wir eine Kennzahl jeden Körpers, seine Charakteristik. Sie ist speziell bei endlichen Körpern von Interesse und wird wie folgt definiert:

Definition 25
*Sei K ein Körper. Die **Charakteristik** von K (man schreibt $char(K)$) ist definiert als die additive Ordnung von "1", falls diese endlich ist. Falls sie jedoch unendlich ist, so definiert man $char(K) = 0$.*
*Der **Primkörper** $P(K)$ ist definiert als der Durchschnitt aller Unterkörper von K.*

Aus der Definition folgt, dass die Charakteristik jedes endlichen Körpers ungleich 0 ist. Da jeder Körper nullteilerfrei ist muss seine Charakteristik, falls sie größer als 0 ist, eine Primzahl sein.

Hat ein Körper K die Charakteristik 0, so ist sein Primkörper isomorph zu $\mathbb{Q}$, gilt $char(K) = p$ so ist der Primkörper $P(K)$ isomorph zu $\mathbb{Z}/p\mathbb{Z}$.

Definition 26
*Seien L, K zwei Körper mit $K \subseteq L$, dann heißt L ein Erweiterungskörper und man spricht von einer **Körpererweiterung** $L|K$. L kann als Vektorraum über K aufgefasst werden. Ist dieser Vektorraum von endlicher Dimension n so heißt die Körpererweiterung $L|K$ endlich und ihr **Erweiterungsgrad** $[L : K] = n$.*

Man kann also jeden Körper K als Erweiterung seines Primkörpers $P(K)$ auffassen. Für endliche Körper erkennt man so sofort, dass die Kardinalität jedes endlichen Körpers eine Potenz seiner Kardinalität sein muss.

Für zwei endliche Körpererweiterungen $L|K$ und $E|L$ ist auch $E|K$ endlich und es gilt:

$$[E : K] = [E : L] \cdot [L : K].$$

Definition 27
Sei $L|K$ eine Körpererweiterung.
*$\alpha \in L$ heißt **algebraisch** über K, falls es ein Polynom $f(x) \in K[x]$ gibt mit $f(\alpha) = 0$. Ist jedes $\alpha \in L$ algebraisch, so nennt man die Körpererweiterung algebraisch.*
*Sei α algebraisch über K, dann heißt das normierte Polynom mit minimalem Grad n, das α als Nullstelle hat, **Minimalpolynom** $m_\alpha(x)$, man sagt α ist algebraisch vom Grad n über K.*
Mit $K(\alpha)$ bezeichnet man den kleinsten Unterkörper von L der K und α enthält.
Gibt es $\alpha_1, \ldots, \alpha_n \in L$ mit $L = K(\alpha_1, \ldots, \alpha_n)$ dann nennt man die Körpererweiterung $L|K$ endlich erzeugt.
*Ist $L = K(\alpha)$ dann nennt man $L|K$ **einfach** und α ein **primitives Element**.*

Jede endliche Körpererweiterung ist endlich erzeugt. Das Minimalpolynom ist eindeutig bestimmt und irreduzibel. Für jedes über K algebraische α ist die Körpererweiterung $K(\alpha)|K$ endlich. Insbesondere ist $[K(\alpha) : K] = n$ gleich dem Grad des Minimalpolynoms und es gilt $K(\alpha) = K[\alpha] = \{a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 \mid a_{n-1}, \ldots, a_0 \in K\}$.

Definition 28
*Ein Körper E heißt **algebraisch abgeschlossen**, falls jedes Polynom $f(x) \in E[x]$ eine Nullstelle $\alpha \in E$ besitzt.*

Jeder Körper K besitzt einen algebraisch abgeschlossenen Erweiterungskörper E der algebraisch über K ist. So einen Körper nennt man **algebraischen Abschluss** $\overline{K}$, er ist bis auf Isomorphie eindeutig bestimmt: Seien E und E' zwei algebraische Abschlüsse von K, dann gibt es einen Isomorphismus $\sigma : E \to E'$ der K elementweise festhält.

Definition 29
*Sei $L|K$ eine Körpererweiterung. L heißt **Zerfällungskörper** einer Familie von Polynomen $(f_i)_{i\in I}$, $f_i(x) \in K[x]$, falls jedes $f_i(x)$ über L in Linearfaktoren zerfällt, und wenn die Körpererweiterung $L|K$ von den Nullstellen der f_i erzeugt wird.*
*$L|K$ heißt **normal**, falls L Zerfällungskörper einer Familie von Polynomen $(f_i)_{i\in I}$, $f_i(x) \in K[x]$ ist.*

Für Zerfällungskörper gilt folgender Existenzsatz:

Satz 2.4.1
Sei K ein Körper. Zu jeder Familie von Polynomen $(f_i)_{i\in I}$, $f_i(x) \in K[x]$ existiert ein Zerfällungskörper, der bis auf Isomorphie (wobei K elementweise festgehalten wird) eindeutig bestimmt ist.

Beweis. Siehe zum Beispiel [30] Kapitel V Satz 4.4. □

Damit lassen sich nun alle endlichen Körper beschreiben:

Korollar 2.4.2
Für jede Primzahl p und jede ganze Zahl $n \geq 1$ gibt es bis auf Isomorphie genau einen Körper mit $q = p^n$ Elementen: den Zerfällungskörper des Polynoms $x^{p^n} - x$ über $\mathbb{Z}/p\mathbb{Z}$, er besteht genau aus den Nullstellen dieses Polynoms.
Man bezeichnet diesen Körper mit $\mathbb{F}_q$ (oder $GF(q)$).

Für normale Körpererweiterungen gilt folgendes Kriterium:

Satz 2.4.3
Eine Körpererweiterung $L|K$ ist genau dann normal, wenn jedes irreduzible Polynom aus $K[x]$, das in L eine Nullstelle besitzt, über L in Linearfaktoren zerfällt.

Beweis. Siehe zum Beispiel [9] Kapitel 3.5 Theorem 4. □

Definition 30
*Ein Polynom $f(x) \in K[x]$ heißt **separabel**, wenn es keine mehrfachen Nullstellen hat (das ist genau dann der Fall, wenn $ggT\big(f(x), f'(x)\big) = 1$ ist).*
Sei $L|K$ eine endliche Erweiterung. $\alpha \in L$ heißt separabel, falls das Minimalpolynom $m_\alpha(x)$ separabel ist.
*Ist jedes $\alpha \in L$ separabel, so nennt man $L|K$ eine **separable Erweiterung**.*

Für die meisten für uns relevanten Körper gilt:

Satz 2.4.4
Ist K eine Körper der Charakteristik 0 oder ein endlicher Körper, so ist jede algebraische Erweiterung von K separabel.

Beweis. Siehe zum Beispiel [64] Satz 6.21. □

Satz 2.4.5
Sei $L|K$ eine algebraische Körpererweiterung vom Grad n. Sie ist genau dann separabel, wenn n paarweise verschiedene K-Isomorphismen von L in einen algebraischen Abschluss $\overline{K}$ existieren.

Beweis. Siehe zum Beispiel [64] Satz 6.22. □

Weiters gilt für separable Erweiterungen:

Satz 2.4.6 (Satz vom primitiven Element)
Jede endliche separable Erweiterung $L|K$ ist einfach, d.h. es gibt ein primitives Element $\vartheta \in L$ mit $K(\vartheta) = L$.

Beweis. Siehe zum Beispiel [9] Kapitel 36 Satz 12. □

Definition 31
*Eine endliche Erweiterung $E|K$ heißt **Galoiserweiterung**, falls sie normal und separabel ist.*

Man erkennt leicht, dass für jede separable Erweiterung $L|K$ ein $E \supseteq L$ existiert, sodass $E|K$ galoissch ist.

Satz 2.4.7
Sei $L|K$ eine separable Erweiterung vom Grad n und G die Gruppe der K-Isomorphismen von L in sich selbst, so sind folgende Aussagen äquivalent:

(i) $L|K$ *ist galoissch*

(ii) K *ist der Fixpunktkörper von* G*, also* $K = \{a \in L \mid \sigma(a) = a \, \forall \sigma \in G\}$

(iii) $|G| = n$.

Beweis. Siehe zum Beispiel [64] Satz 7.1. □

Definition 32
*Die Gruppe G der Automorphismen auf E, die K elementweise festhalten, heißt die **Galoisgruppe** $Gal(E|K)$ der Galoiserweiterung $E|K$.*
*Ist die Galoisgruppe $G = Gal(E|K)$ eine abelsche Gruppe, so nennt man $E|K$ eine **abelsche Erweiterung**.*
*Ist G sogar zyklisch, so nennt man $E|K$ eine **zyklische Erweiterung**.*

Satz 2.4.8 (Hauptsatz der Galoistheorie)
Sei $E|K$ eine Galoiserweiterung und $G = Gal(E|K)$. Ordnet man jeder Untergruppe $U \leq G$ den entsprechenden Fixpunktkörper $L = \{a \in E \mid \sigma(a) = a \, \forall \sigma \in U\}$ zu, so erhält man dadurch eine Bijektion zwischen den Untergruppen von G und den Zwischenkörpern $K \subseteq L \subseteq E$, die die Enthaltenseinsrelation umkehrt. Es gilt

$[E : L] = |U|$ *und* $[L : K] = ind(U) = [G : U]$.
$L|K$ *ist genau dann galoissch, wenn* U *ein Normalteiler von* G *ist. Es gilt dann die Isomorphie* $Gal(L|K) \cong G/U$.

Beweis. Siehe zum Beispiel [9] Kapitel 4.1 Theorem 6. □

Da die Galoisgruppe immer von endlicher Ordnung ist folgt daraus sofort, dass jede separable Erweiterung nur endlich viele Zwischenkörper besitzt.

Definition 33
Sei $L|K$ *eine endliche Erweiterung. Betrachtet man* L *als Vektorraum über* K*, so ist durch jedes* $\alpha \in L$ *eine lineare Abbildung* $a \to \alpha a$ *definiert. Für eine Basis* $\omega_1, \ldots, \omega_n$ *sei* $\alpha\omega_i = \sum_{j=1}^{n} a_{ij}\omega_j$ *,* $a_{ij} \in K$*, dann heißt* $f_\alpha(x) = \det\Big(x \cdot I_n + (a_{ij})\Big)$ *das charakteristische Polynom von* α.
Die Determinante von (a_{ij}) *nennt man die Norm von* α*:*

$$\mathrm{N}_K^L(\alpha) := \det(a_{ij}).$$

Die Spur von (a_{ij}) *nennt man die Spur von* α*:*

$$\mathrm{Sp}_K^L(\alpha) := \sum_{i=1}^{n} a_{ii}.$$

Norm, Spur und charakteristisches Polynom sind natürlich unabhängig von der Wahl der Basis $\omega_1, \ldots, \omega_n$. Weiters ist die Spur additiv und die Norm multiplikativ, also

$$\mathrm{Sp}_K^L(\alpha + \beta) = \mathrm{Sp}_K^L(\alpha) + \mathrm{Sp}_K^L(\beta) \quad \text{und} \quad \mathrm{N}_K^L(\alpha\beta) = \mathrm{N}_K^L(\alpha) \cdot \mathrm{N}_K^L(\beta)$$

und für $K \subseteq L \subseteq E$ gilt:

$$\mathrm{Sp}_K^E(\alpha) = \mathrm{Sp}_K^L(\mathrm{Sp}_L^E(\alpha)) \quad \text{und} \quad \mathrm{N}_K^E(\alpha) = \mathrm{N}_K^L(\mathrm{N}_L^E(\alpha))$$

Wir betrachten nun eine separable Erweiterung $L|K$ vom Grad n. Für ein $\alpha \in L$ nennt man $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ die **Konjugierten** von α, wobei $\sigma_1, \ldots, \sigma_n$ die K-Isomorphismen von L in $\overline{K}$ aus Satz 2.4.5 sind.
Für Norm, Spur und charakteristische Polynome in separablen Erweiterungen gilt

Satz 2.4.9
Sei $L|K$ *eine endliche separable Erweiterung vom Grad* $[L : K] = n$*. Dann ist das charakteristische Polynom von jedem* $\alpha \in L$ *eine Potenz des Minimalpolynoms, also* $f_\alpha(x) = m_\alpha(x)^s$ *für ein* $s \geq 1$*. Weiters besitzt es die Zerlegung*

$$f_\alpha(x) = (x - \sigma_1(\alpha))(x - \sigma_2(\alpha)) \cdots (x - \sigma_n(\alpha))$$

Für Norm und Spur gilt:

$$\mathrm{N}_K^L(\alpha) = \sigma_1(\alpha) \cdots \sigma_n(\alpha) \quad \text{und} \quad \mathrm{Sp}_K^L(\alpha) = \sigma_1(\alpha) + \cdots + \sigma_n(\alpha)$$

Beweis. Siehe zum Beispiel [52] Kapitel I Satz 2.6. □

Definition 34
Sei $L|K$ eine endliche Körpererweiterung vom Grad $[L:K]=n$. Für $\alpha_1,\ldots,\alpha_n \in L$ definiert man die ***Diskriminante*** *wie folgt:*

$$\Delta_K^L(\alpha_1,\ldots,\alpha_n) := \det\big(\mathrm{Sp}_K^L(\alpha_i\alpha_j)\big).$$

Sei α algebraisch vom Grad d über K, dann definiert man

$$\Delta_K(\alpha) := \Delta_K^{K(\alpha)}(1,\alpha,\ldots,\alpha^{d-1}).$$

Für die Diskriminante gilt folgendes Kriterium:

Satz 2.4.10
Sei $L|K$ eine separable Körpererweiterung vom Grad $[L:K]=n$ und $\alpha_1,\ldots,\alpha_n$ eine Basis der Erweiterung, dann gilt

$$\Delta_K^L(\alpha_1,\ldots,\alpha_n) \neq 0.$$

Beweis. Siehe zum Beispiel [52] Kapitel I Satz 2.8. □

Für eine separable Erweiterung $L|K$ kann man die Diskriminante wie folgt berechnen:

$$\Delta_K^L(\alpha_1,\ldots,\alpha_n) = \det(\sigma_j(\alpha_i))$$

wobei $\sigma_j(\alpha_1),\ldots,\sigma_j(\alpha_n)$ die jeweiligen Konjugierten von $\alpha_1,\ldots,\alpha_n$ bezeichnen.

2.5 Dedekind'sche Ringe

Sei $\langle R,+,\cdot\rangle$ nun ein Integritätsbereich. Aus R konstruiert man einen Körper indem man analog zur Konstruktion der rationalen Zahlen aus den ganzen Zahlen vorgeht: Dazu definiert man auf der Menge der Quotienten $\{\frac{a}{b} \mid a,b \in R, b \neq 0\}$ durch $\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$ und $\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}$ eine Addition und eine Multiplikation. Man bezeichnet zwei Quotienten $\frac{a}{b}$ und $\frac{c}{d}$ als äquivalent, falls $ad=bc$ gilt. Auf diese Weise erhält man eine Kongruenzrelation die mit Addition und Multiplikation verträglich ist. Nach dieser faktorisiert man R und erhält so den **Quotientenkörper** von R. Man bettet R in seinen Quotientenkörper ein indem man jedes $a \in R$ mit der Äquivalenzklasse identifiziert, die $\frac{a}{1}$ enthält. Offensichtlich ist nun $\mathbb{Q}$ der Quotientenkörper von $\mathbb{Z}$.

Definition 35
Sei R ein Ring und K ein Körper mit $R \subseteq K$.
Ein Element $\alpha \in K$ heißt ***ganzalgebraisch*** *bezüglich R, falls α Nullstelle eines normierten Polynoms aus $R[x]$ ist.*
Die Menge O der bezüglich R ganzen Elemente nennt man ***ganzalgebraische Hülle*** *von R in K.*
R heißt ***ganzalgebraisch abgeschlossen*** *in K, wenn R gleich seiner ganzalgebraischen Hülle in K ist.*
Ein Integritätsbereich heißt ganzalgebraisch abgeschlossen, wenn er in seinem Quotientenkörper ganzalgebraisch abgeschlossen ist.

Jeder faktorielle Ring ist ganzalgebraisch abgeschlossen. Allgemein gilt für ganzalgebraisch abgeschlossene Ringe:

Satz 2.5.1
Sei R ganzalgebraisch abgeschlossen in seinem Quotientenkörper Q und sei weiters $K|Q$ eine algebraische Körpererweiterung und O die ganzalgebraische Hülle von R in K.

(i) O ist ganzalgebraisch abgeschlossen und bildet einen Ring.

(ii) Für jedes bezüglich R ganzalgebraische $\alpha \in K$ das Minimalpolynom nur Koeffizienten aus R, also $m_\alpha \in R[x]$.

(iii) Für jedes ganzalgebraische $\alpha \in K$ gilt weiters:

$$\mathrm{N}_{K|Q}(\alpha) \in R \quad \text{und} \quad \mathrm{Sp}_{K|Q}(\alpha) \in R.$$

Beweis. Siehe zum Beispiel [30] Kapitel X Satz 1.4, Satz 1.7 und Korollar 1.8. □

Definition 36
Ein Integritätsbereich R heißt Dedekind'scher Ring, falls er die folgenden drei Eigenschaften erfüllt:

(i) R ist noethersch.

(ii) Jedes Primideal $P \neq (0)$ von R ist maximal.

(iii) R ist ganzalgebraisch abgeschlossen.

Man kann Dedekind'sche Ringe als Verallgemeinerung von Hauptidealringen sehen: Jeder Hauptidealring ist ein Dedekind'scher Ring. Umgekehrt gilt:

Satz 2.5.2
Ist ein Dedekind'scher Ring auch faktoriell, so ist er ein Hauptidealring.

Beweis. Siehe zum Beispiel [30] Kapitel X Satz 3.7. □

Im Allgemeinen ist jedoch, wie wir noch an einem Beispiel sehen werden, die Zerlegung in irreduzible Elemente in einem Dedekind'schen Ring nicht eindeutig. Diese wichtige Eigenschaft gilt jedoch für Ideale:

Satz 2.5.3
In einem Dedekind'schen Ring R kann jedes Ideal $I \neq (0), R$ bis auf die Reihenfolge eindeutig als Produkt von Primidealen dargestellt werden:

$$I = \prod_{P \in \mathfrak{P}} P^{\nu_P(I)}$$

wobei $\mathfrak{P}$ die Menge der Primideale $\neq (0)$ von R ist und die P-adische Bewertung $\nu_P(I) \in \mathbb{Z}^+ \cup \{0\}$ nur für endlich viele P ungleich null ist. ($P^0 := R$)

Beweis. Siehe zum Beispiel [30] Kapitel X Satz 3.2. □

Ein wichtiges Ergebnis liefert der folgende Satz:

Satz 2.5.4
Sei R ein Dedekind'scher Ring, Q sein Quotientenkörper, $K|Q$ eine endliche separable Körpererweiterung und O die ganzalgebraische Hülle von R in K. Dann gilt:

(i) O ist ein endlich erzeugbarer R-Modul.

(ii) O ist ein Dedekind'scher Ring.

Beweis. Siehe zum Beispiel [30] Kapitel X Satz 2.3. □

Definition 37
*Sei R ein Integritätsbereich und Q sein Quotientenkörper. Ein R-Modul $I \neq \{0\}$, $I \subseteq Q$ heißt **Bruchideal** oder **gebrochenes Ideal** (von Q), wenn es ein $a \in R$, $a \neq 0$ gibt, sodass $aI \subseteq R$ gilt.*
*Ein Bruchideal der Form $I = aR = (a)$, $a \in Q$ heißt **Hauptbruchideal**.*
*Ein Bruchideal I heißt **invertierbar**, falls es ein Bruchideal I^{-1} gibt, sodass $I \cdot I^{-1} = R$ gilt.*

Offensichtlich ist jedes Ideal ein invertierbares Bruchideal. Im allgemeinen ist nicht jedes Bruchideal invertierbar, in einem Dedekind'schen Ring ist dies jedoch der Fall und es gilt:

Satz 2.5.5
Die Menge der Bruchideale in einem Dedekind'schen Ring bildet eine abelsche Gruppe, das zu einem Bruchideal I Inverse ist dann gegeben durch

$$I^{-1} = \{x \in Q \mid xI \in R.$$

Beweis. Siehe zum Beispiel [52] Kapitel I Satz 3.8. □

Somit folgt auch für Bruchideale die Faktorisierung:

Korollar 2.5.6
Jedes Bruchideal $I \neq (0)$ eines Dedekind'schen Ringes R lässt sich eindeutig in der Form

$$I = \prod_{P \in \mathfrak{P}} P^{\nu_P(I)}$$

darstellen, wobei $\nu_P(I) \in \mathbb{Z}$ nur für endlich viele P ungleich null ist und I genau dann ein (echtes) Ideal ist, wenn $\nu_P(I) \geq 0$ für alle $P \in \mathfrak{P}$ gilt.
Die Menge der Bruchideale eines Dedekind'schen Ringes bildet eine durch die Primideale $P \neq (0)$ erzeugte freie abelsche Gruppe.

2.6 Algebraische Zahlkörper

Die algebraische Zahlentheorie beschäftigt sich im Konkreten mit Erweiterungen der rationalen Zahlen $\mathbb{Q}$ und dem ganzalgebraischen Abschluss der ganzen Zahlen darin:

Definition 38
Sei K ein endlicher Erweiterungskörper von $\mathbb{Q}$, dann heißt K ein algebraischer Zahlkörper.
Den ganzalgebraischen Abschluss von $\mathbb{Z}$ in K nennt man Ganzheitsring oder Ring der ganzen Zahlen und bezeichnet ihn mit O_K.
Den maximalen reellen Unterkörper von K bezeichnet man mit K^+.

Da $\mathbb{C}$ ein algebraischer Abschluss von $\mathbb{Q}$ ist gibt es für jeden algebraischen Zahlkörper K vom Grad n genau $n = s+2t$ Isomorphismen in den Körper der komplexen Zahlen $\mathbb{C}$:

$$\sigma_1, \ldots, \sigma_s, \sigma_{s+1}, \ldots, \sigma_{s+t}, \overline{\sigma_{s+1}}, \ldots, \overline{\sigma_{s+t}}$$

wobei gilt $\sigma_1(K), \ldots, \sigma_s(K) \subseteq \mathbb{R}$ und $\sigma_{s+1}(K), \ldots, \sigma_{s+t}(K) \nsubseteq \mathbb{R}$.
Das Paar $[s, t]$ nennt man **Signatur** von K.

Für algebraische Zahlkörper bedeutet Satz 2.5.4(ii) nun:

Korollar 2.6.1
Der Ganzheitsring O_K jedes algebraischen Zahlkörpers K ist ein Dedekind'scher Ring.

Leider ist jedoch nicht jeder Ganzheitsring auch ein faktorieller Ring:
Betrachtet man beispielsweise $K = \mathbb{Q}(\sqrt{-5})$ so sind die Elemente $2, 3, 1+\sqrt{-5}$ und $1-\sqrt{-5}$ irreduzibel in O_K, es gilt jedoch $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$.

Man muss sich also in O_K mit der eindeutigen Primfaktorzerlegung von Idealen begnügen. Der Einfachheit halber spricht man bei Zahlkörpern manchmal auch von einem Ideal I des Körpers K, gemeint ist dann ein Ideal I von O_K.[2]

Weiters ist jedes von 0 verschiedenes Primideal P eines Ganzheitsringes O_K ist maximal und es gilt:

Satz 2.6.2
Ein von 0 verschiedenes Primideal P eines Ganzheitsringes O_K enthält genau eine Primzahl p.
Außerdem ist O_K/P ein endlicher Körper, der $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ enthält.

Beweis. Siehe zum Beispiel [55] Kapitel 7 Satz A. □

Für ein beliebiges Bruchideal $I = \prod P_i^{r_i}$ gilt dann $|O_K/I| = \prod |O_K/P_i|^{r_i}$. Somit ist auch der Faktorring O_K/I endlich und man definiert:

Definition 39
*Die **Norm** eines Bruchideals I von O_K wird definiert als* $\mathrm{N}(I) := |O_K/I|$.

Nach dem vorigen Satz ist die Norm eines Primideals P somit eine Potenz der in P enthaltenen Primzahl p.
Sei nun $L|K$ eine Erweiterung von Zahlkörpern mit $[L : K] = n$ und $P \lhd O_L$ ein Primideal das die Primzahl p enthält, dann ist $K \cap P = \mathfrak{p}$ ein Primideal von O_K,

[2] Ebenso wird in der Literatur häufig auch von den Einheiten eines Zahlkörpers K gesprochen. Gemeint ist damit jedoch nicht $K^\times = K \setminus \{0\}$ sondern die Einheiten des Ganzheitsringes O_K!

das ebenfalls p enthält. Weiters sind $O_K/\mathfrak{p} \subseteq O_L/P$ übereinanderliegende Körper. Sei $f = [O_L/P : O_K/\mathfrak{p}]$, dann gilt $f \leq n$, und man definiert die relative Norm:

Definition 40
Mit den Definitionen von oben ist die ***relative Norm*** *des Primideals P definiert durch*

$$\mathrm{N}_K^L(P) = \mathfrak{p}^f.$$

Für beliebige Bruchideale $I = \prod_{i=1}^r P_i^{r_i}$ von O_L setzt man die relative Norm multiplikativ fort, also

$$\mathrm{N}_K^L(I) = \prod_{i=1}^r (\mathrm{N}_K^L P_i)^{r_i}.$$

Der folgende Satz stellt die Verbindung zwischen der relativen Norm von Idealen und den anderen Normen her:

Satz 2.6.3 *(i) Sei K ein algebraischer Zahlkörper, für jedes Bruchideal I des Ganzheitsringes O_K gilt:*

$$\mathrm{N}_{\mathbb{Q}}^K(I) = \mathbb{Z} \cdot \mathrm{N}(I)$$

(ii) Sei $L|K$ eine Erweiterung von Zahlkörpern und $x \in L \setminus \{0\}$, dann gilt für das von x erzeugte Hauptideal:

$$\mathrm{N}_K^L(O_L x) = O_K \cdot \mathrm{N}_K^L(x).$$

Beweis. Siehe zum Beispiel [55] Kapitel 13 Satz B und Satz F. □

Auch der Begriff der Diskriminante lässt sich erweitern:

Definition 41
Sei K ein algebraischer Zahlkörper und $(x_1, \ldots, x_n) \in {O_K}^n$ eine $\mathbb{Z}$-Basis des Ganzheitsringes O_K. Die ***Diskriminante*** *von K wird definiert als $\delta_K := \Delta_{\mathbb{Q}}^K(x_1, \ldots, x_n)$. Sei nun $L|K$ eine Erweiterung vom Grad n. Die* ***relative Diskriminante*** *von $L|K$ ist das Ideal $\delta_K^L \lhd O_L$ das erzeugt wird durch die Elemente $\Delta_K^L(x_1, \ldots, x_n)$ für alle möglichen Basen $(x_1, \ldots, x_n) \in {O_L}^n$ von $L|K$.*

Satz 2.5.1(iii) besagt nun, dass die Diskriminante jedes Zahlkörpers ganzzahlig ist.

Ein in der algebraischen Zahlentheorie wichtiges Merkmal eines Zahlkörpers ist seine Klassenzahl ein:

Definition 42
Sei K ein algebraischer Zahlkörper, dann bezeichnen wir mit $I(K)$ die Gruppe der Bruchideale und mit $P(K)$ die Untergruppe der Hauptbruchideale.
Die Faktorgruppe $H(K) := I(K)/P(K)$ heißt ***Idealklassengruppe*** *von K und ihre Mächtigkeit $h(K) := |H(K)|$ bezeichnet man als die* ***Klassenzahl*** *von K.*

Für die Klassenzahl gilt folgender wichtiger Satz:

Satz 2.6.4
Sei K ein algebraischer Zahlkörper, dann gilt

(i) Die Klassenzahl $h(K)$ ist endlich.

(ii) $h(K) = 1$ *genau dann, wenn* O_K *ein faktorieller Ring ist, d.h. wenn in* O_K *eine eindeutige Zerlegung in Primfaktoren existiert.*

Beweis. Siehe zum Beispiel [52] Kapitel 1 Satz 6.3. □

Ein weiteres elementares Ergebnis liefert der folgende Satz von Dirichlet. Er gibt Auskunft über die Struktur der Einheitengruppe des Ganzheitsringes eines Zahlkörpers:

Satz 2.6.5 (Dirichlet'scher Einheitensatz)
Für die Einheitengruppe des Ganzheitsringes O_K *eines algebraischen Zahlkörpers* K *mit der Signatur* $[s, t]$ *gilt die folgende Isomorphie:*

$$O_K{}^\times \cong W \times C_1 \times \cdots \times C_n,$$

wobei W *die Menge der Einheitswurzeln in* K *eine zyklische Gruppe von endlicher Ordnung* w *ist,* $n = s+t-1$ *gilt und jedes* C_i *eine unendliche multiplikative Gruppe ist.*

Beweis. Siehe zum Beispiel [55] Kapitel 10 Theorem 1. □

Es existieren also eine Einheitswurzel $\zeta \in O_K$ und n Einheiten von unendlicher Ordnung $u_1, \ldots, u_n \in O_K{}^\times$ sodass jede Einheit $u \in O_K{}^\times$ geschrieben werden kann in der Form

$$u = \zeta^{e_0} u_1^{e_1} \cdots u_n^{e_n},$$

mit $0 \leq e_0 < w$ und $e_1, \ldots, e_n \in \mathbb{Z}$.

2.7 Verzweigung von Primidealen

Es sei im Folgenden $L|K$ eine separable Erweiterung von Zahlkörpern und O_K bzw. O_L die dazugehörigen Ganzheitsringe. Weiters sei $\mathfrak{p}$ ein Primideal von O_K. Dann ist $I = \mathfrak{p}O_L$ ein Ideal von O_L. Da O_L ein Dedekind'scher Ring ist, besitzt I die eindeutige Zerlegung $I = \prod_{i=1}^{g} P_i^{e_i}$ in Primideale. Ist $P \in \{P_1, \cdots, P_n\}$, so sagt man P liegt über $\mathfrak{p}$, oder auch P teilt $\mathfrak{p}$, und schreibt $P|\mathfrak{p}$. Weiters sieht man leicht, dass $O_K/\mathfrak{p} \subseteq O_L/P$. Man definiert

Definition 43
Seien die Notationen wie oben, dann nennt man e_i *den* ***Verzweigungsindex*** *von* P_i *in* $L|K$ *und bezeichnet diesen mit* $e(P|\mathfrak{p})$.
Die Dimension $f_i := [O_L/P_i : O_K/\mathfrak{p}]$ *heißt* ***Restklassengrad*** *von* P_i *in* $L|K$ *genannt und mit* $f(P_i|\mathfrak{p})$ *bezeichnet.*
g *wird die* ***Zerlegungszahl*** *von* $\mathfrak{p}$ *in* $L|K$ *genannt.*
Ist $e(P_i|\mathfrak{p}) = 1$, *so nennt man* P_i *unverzweigt. Man nennt* $\mathfrak{p}$ ***unverzweigt****, wenn alle* P_i *mit* $P_i|\mathfrak{p}$ *unverzweigt sind. Ist zusätzlich* $g = 1$, *also* $\mathfrak{p}O_L = P$, *dann nennt man* $\mathfrak{p}$ ***träge****.*

Für ein Ideal I von O_K und ein Primideal P von O_L schreibt man $P|I$, falls es ein Primideal $\mathfrak{p}$ von O_K gibt, das I enthält und für das $\mathfrak{p}|P$ gilt. Im Fall $K = \mathbb{Q}$ schreibt man $P|p$ für $P|(p)$, wobei p eine Primzahl ist, beziehungsweise analog $P|n$ für $n \in \mathbb{Z}$.

Verzweigungsindex, Restklassengrad und Zerlegungszahl haben folgende Eigenschaften:

Satz 2.7.1
Seien $K \subseteq F \subseteq L$ separable Erweiterungen von Zahlkörpern und $\mathfrak{p} \lhd O_K, \mathfrak{q} \lhd O_F, P \lhd O_L$ übereinanderliegende Primideale der jeweiligen Ganzheitsringe, d.h. $P|\mathfrak{q}|\mathfrak{p}$, dann gilt

(i)
$$e(P|\mathfrak{p}) = e(P|\mathfrak{q})e(\mathfrak{q}|\mathfrak{p}) \quad \text{und} \quad f(P|\mathfrak{p}) = f(P|\mathfrak{q})f(\mathfrak{q}|\mathfrak{p})$$

(ii) Sei weiters $\mathfrak{p}O_L = \prod_{i=1}^{g} P_i^{e_i}$ dann gilt
$$[L:K] = \sum_{i=1}^{g} e(P_i|\mathfrak{p})f(P_i|\mathfrak{p})$$

(iii) Ist $L|K$ eine Galoiserweiterung mit Galoisgruppe G und $\mathfrak{p}O_L = \prod_{i=1}^{g} P_i^{e_i}$, dann existiert für je zwei über $\mathfrak{p}$ liegende Primideale P_i, P_j ein $\sigma \in G$ sodass $\sigma(P_i) = P_j$.
Weiters gilt dann
$$e_1 = e_2 = \cdots = e_g \quad \text{und } f_1 = f_2 = \cdots = f_g$$
also insbesondere nach Punkt (ii):
$$[L:K] = gef$$

Beweis. Siehe zum Beispiel [35] Kapitel [I,§7] Proposition 21, Proposition 22 und Corollary 2. □

Definition 44
*Sei $L|K$ eine Galoiserweiterung und $\mathfrak{p}$ ein Primideal von O_K mit Zerlegungszahl g, dann sagt man $\mathfrak{p}$ **zerfällt komplett** in $L|K$, falls $g = [L:K]$ (also $e_i = f_i = 1$ für alle $i = 1, \ldots, g$).*

Der nächste Satz von Dedekind stellt eine Verbindung zwischen Verzweigung und der Diskriminante her:

Satz 2.7.2 (Dedekind)
Sei $L|K$ eine Erweiterung von Zahlkörpern und P ein von 0 verschiedenes Primideal des Ganzheitsringes O_K, dann ist P genau dann verzweigt, wenn $P|\delta_K^L$.
Insbesondere existieren also nur endlich viele Primideale die in $L|K$ verzweigt sind.

Beweis. Siehe zum Beispiel [55] Kapitel 13 Theorem 1. □

Betrachtet man den Fall $K = \mathbb{Q}$ so liefert eine Faktorisierung der Diskriminante δ_L alle verzweigten Primzahlen. Mit analytischen Methoden lässt sich eine Abschätzung für die Diskriminante eines Zahlkörpers zeigen:

Satz 2.7.3
Für einen Zahlkörper K vom Grad n gilt:

$$\delta_K \geq \left(\frac{\pi}{4}\right)^n \left(\frac{n^n}{n!}\right)^2 > 1$$

Es gibt also in jedem Zahlkörper zumindest eine verzweigte Primzahl.

Beweis. Siehe zum Beispiel [55] Kapitel 9 Satz G. □

Der folgende Satz liefert eine Möglichkeit zur Berechnung der Zerlegung von Primidealen in gewissen separablen Erweiterungen.

Satz 2.7.4
Sei $L|K$ eine separable Erweiterung von Zahlkörpern, sodass $O_L = O_K[\alpha]$ gilt für ein $\alpha \in L$, und sei weiters $m_\alpha(x) \in O_K[x]$ das Minimalpolynom von α über K. Sei $\mathfrak{p}$ ein Primideal von O_K und $\overline{m_\alpha}$ die Reduktion von m_α modulo $\mathfrak{p}$ und sei

$$\overline{m_\alpha}(x) = \overline{p_1}(x)^{e_1} \cdots \overline{p_g}(x)^{e_g}$$

die Zerlegung von $\overline{m_\alpha}$ in irreduzible, normierte Faktoren über $\overline{O_K} = O_K/\mathfrak{p}$. Dann ist

$$\mathfrak{p}O_L = P_1^{e_1} \cdots P_g^{e_g}$$

die Faktorisierung von $\mathfrak{p}$ in O_L, sodass $e(P_i|\mathfrak{p}) = e_i$ und $f(P_i|\mathfrak{p}) = \deg\overline{p_i}$, und

$$P_i = \mathfrak{p}O_L + p_i(\alpha)O_L,$$

wobei $p_i(x) \in O_K[x]$ ein normiertes Polynom ist dessen Reduktion modulo $\mathfrak{p}$ gleich $\overline{p_i}(x)$ ist.

Beweis. Siehe zum Beispiel [35] Kapitel [I,§7] Proposition 25. □

2.8 Bewertungen und Beträge

Wir verallgemeinern im Folgenden den Begriff der bereits von den ganzen Zahlen bekannten p-adischen Bewertung. Zunächst setzen wir diese jedoch auf $\mathbb{Q}$ fort: jedes $x \in \mathbb{Q}$ lässt sich für eine Primzahl p schreiben als $x = \frac{a}{b}p^r$, mit $ggT(ab, p) = 1$, $a, b, r \in \mathbb{Z}$ und $b \neq 0$. Wir setzen dann

$$\nu_p(x) := r.$$

Definition 45
Sei K ein Körper, eine Funktion $\nu : K \to \mathbb{R} \cup \{\infty\}$ mit den Eigenschaften

(i) $\nu(x) = 0 \Longleftrightarrow x = \infty$,

(ii) $\nu(xy) = \nu(x) + \nu(y)$,

(iii) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$,

*nennt man eine **Bewertung**, oder auch Exponentialbewertung, von K.*

Der Begriff der Bewertung ist eng verknüpft mit jenem des Betrags:

Definition 46
*Sei K ein Körper, eine Funktion $|\cdot| : K \to \mathbb{R}$ nennt man einen **Betrag** von K, oder auch eine Betragsbewertung, wenn sie die folgenden Eigenschaften erfüllt:*

(i) $|x| \geq 0$, *und* $|x| = 0 \iff x = 0$,

(ii) $|xy| = |x| \cdot |y|$,

(iii) $|x + y| \leq |x| + |y|$.

Gilt außerdem die verschärfte Bedingung

(iv) $|x + y| \leq \max\{|x|, |y|\}$,

*so spricht man von einem **nichtarchimedischen** oder ultrametrischen Betrag, anderenfalls von einem **archimedischen** Betrag.*

Wir schließen im Folgenden stets den trivialen Fall aus, für den $|x| = 1$ für alle $x \neq 0$ ist.

Man kann einem nichtarchimedischen Betrag $|\cdot|$ eine Bewertung ν zuordnen, indem man eine reelle Zahl $a > 1$ wählt, und ν wie folgt definiert: $\nu(x) := -\log_a|x|$ für $x \neq 0$ und $\nu(0) = \infty$. Hat man andererseits eine Bewertung ν, so erhält man durch $|x| := a^{-\nu(x)}$, für eine reelle Zahl $a > 1$, einen nichtarchimedischen Betrag.

Definiert man den Abstand von zwei Punkten $x, y \in K$ als den Betrag ihrer Differenz, setzt man also

$$d(x, y) := |x - y|,$$

so ist d eine Metrik und K wird zu einem metrischen, also insbesondere topologischen, Raum.

Definition 47
*Zwei Beträge eines Körpers K heißen **äquivalent**, wenn sie die gleiche Topologie auf K definieren.*
*Die Äquivalenzklassen der nichttrivialen Beträge auf K nennt man die **Stellen** von K*

Satz 2.8.1
Zwei Beträge $|\cdot|_1$ und $|\cdot|_2$ eines Körpers K sind genau dann äquivalent, wenn es eine reelle Zahl $s > 0$ gibt, sodass

$$|x|_1 = {|x|_2}^s$$

für alle $x \in K$ gilt.

Beweis. Siehe zum Beispiel [16] Lemma 4.1.3. □

Auf $\mathbb{Q}$ definiert man für die Primzahl p den **p-adischen** (Absolut-)**Betrag** als

$$|x|_p := p^{-\nu_p(x)},$$

und erhält so einen nichtarchimedischen Betrag. Der gewöhnliche Absolutbetrag ist ein archimedischer Betrag, man bezeichnet ihn manchmal auch mit $|\cdot|_\infty$. Es gilt dann:

Satz 2.8.2
Jeder nichttriviale Betrag von $\mathbb{Q}$ ist äquivalent zu einem Betrag $|\cdot|_p$, mit $p \in \mathbb{P}$, oder $|\cdot|_\infty$.

Beweis. Siehe zum Beispiel [52] Kapitel II Satz 3.7. □

Die Menge $\{|\cdot|_p : p \in \mathbb{P} \cup \infty\}$ ist also ein Repräsentantensystem der Stellen von $\mathbb{Q}$, wir bezeichnen sie mit $M_\mathbb{Q}$.

Wir betrachten nun die Komplettierung eines Körpers bezüglich eines Betrages.

Definition 48
*Ein Körper K heißt **vollständig** bezüglich eines Betrags $|\cdot|$, wenn jede Cauchyfolge $\{a_n\}_{n\in\mathbb{N}}$ (bzgl. $|\cdot|$) in K, gegen ein $a \in K$ konvergiert, also wenn $\lim_{n\to\infty} |a_n - a| = 0$ gilt.*

Aus jedem Körper K mit Betrag $|\cdot|$ erhält man einen bezüglich $|\cdot|$ vollständigen Körper $\widehat{K}$ durch Komplettierung, dabei geht man genau so vor, wie bei der Konstruktion der reellen Zahlen aus den rationalen:
Man bildet den Ring aller Cauchyfolgen (bzgl. $|\cdot|$) in K und faktorisiert diesen nach dem maximalen Ideal der Nullfolgen und erhält so den Körper $\widehat{K}$. Man bettet K in $\widehat{K}$ ein, indem man $a \in K$ mit der Folge $(a, a, a, \ldots)$ identifiziert und erweitert den Betrag $|\cdot|$ auf $\widehat{K}$, indem man dem Element a, das durch die Cauchyfolge $\{a_n\}_{n\in\mathbb{N}}$ repräsentiert wird, den Betrag

$$|a| = \lim_{n\to\infty} |a_n|$$

zuweist. Dieser Limes existiert, da $\{|a_n|\}_{n\in\mathbb{N}}$ eine Cauchyfolge reeller Zahlen ist.
Offensichtlich liefern äquivalente Beträge dieselbe Komplettierung, somit ist die folgende Definition sinnvoll:

Definition 49
*Für einen Zahlkörper K bezeichnet man mit K_ν die oben beschriebene **Komplettierung** von K bezüglich des Betrags $|\cdot|_\nu$.*

Wir bezeichnen im Folgenden einen Betrag $|\cdot|_\nu$ der Einfachheit halber auch schlicht mit ν.

Sei nun $L|K$ eine Körpererweiterung und $|\cdot|_\omega$ ein Betrag von L die Fortsetzung eines Betrages $|\cdot|_\nu$ von K, dann schreiben wir $\omega|\nu$.

Wir betrachten als nächstes, wie sich ein Betrag auf einen Erweiterungskörper fortsetzen lässt. Für vollständige Körper gilt:

Satz 2.8.3
Sei K vollständig bezüglich des Betrags $|\cdot|_\nu$ und $L|K$ eine endliche algebraische Erweiterung vom Grad n, dann hat ν eine eindeutige Fortsetzung ω auf L:

$$|x|_\omega := \sqrt[n]{|\mathrm{N}_K^L(x)|_\nu} \tag{2.2}$$

L ist dann vollständig bezüglich ω.

Beweis. Siehe zum Beispiel [52] Kapitel II Theorem 2.8. □

Hat man nun einen, im Allgemeinen nicht vollständigen, Körper K und einen Betrag ν, so betrachtet man seine Komplettierung K_ν. ν kann, wie wir gesehen haben, auf K_ν und mit (2.2) weiter auf den algebraischen Abschluss $\overline{K_\nu}$ eindeutig fortgesetzt werden. Nun kann man ν auf L definieren, indem man L durch einen K-Isomorphismus in $\overline{K_\nu}$ einbettet. Durch diese Einbettungen können alle Fortsetzungen von ν gewonnen werden. Es gilt:

Satz 2.8.4 (Ostrowski)
Sei K ein Zahlkörper mit der Signatur $[s,t]$ dann gilt:

- *Die archimedischen Beträge von K sind gegeben durch*

  $$|x| = |\sigma(x)|^c,$$

  wobei $c > 0$ und σ eine Einbettung von K in $\mathbb{C}$ ist.

- *Die nichtarchimedischen Beträge von K sind gegeben durch*

  $$|x| = C^{-\nu_P(x)},$$

  wobei P ein Primideal von O_K und die Konstante $C > 1$ ist.

Die Stellen von K stehen also in bijektiver Zuordnung mit den s reellen Einbettungen und den t Paaren nichtreeller Einbettungen von K in $\mathbb{C}$ auf der einen und den Primidealen von O_K auf der anderen Seite.

Beweis. Siehe zum Beispiel [16] Kapitel 4 Lemma 4.1.5, Lemma 4.1.11 und Theorem 4.1.13. □

Mit M_K bezeichnen wir jenes Repräsentantensystem der Stellen des Zahlkörpers K, in dem die Elemente von M_K jene von $M_\mathbb{Q}$ fortsetzen, das entspricht also jenen Beträgen aus dem vorigen Satz mit den Konstanten $c = 1$ beziehungsweise $C = p$, für die im Primideal P enthaltene Primzahl p.

Satz 2.8.5
Sei ν ein Betrag von K, und $L|K$ eine endliche separable Körpererweiterung, dann gilt:

$$[L : K] = \sum_{\omega|\nu} [L_\omega : K_\nu].$$

Weiters gilt für $x \in L$:

$$\prod_{\omega|\nu} |x|_\omega^{[L_\omega:K_\nu]} = |\mathrm{N}_K^L(x)|_\nu.$$

Beweis. Siehe zum Beispiel [34] Kapitel 1 Proposition 4.3 und Theorem 4.5. □

In $\mathbb{Q}$ gilt nun:

$$\prod_{p\in M_{\mathbb{Q}}} |x|_p = |x|_\infty \prod_{p\in\mathbb{P}} p^{-\nu_p(x)} = 1.$$

Wendet man nun Satz 2.8.5 an, so erhält für beliebigen Zahlkörper K und $x \in K$ die **Produktformel**:

$$\begin{aligned} 1 &= \prod_{p\in M_{\mathbb{Q}}} |\mathrm{N}_{\mathbb{Q}}^K(x)|_p \\ &= \prod_{p\in M_{\mathbb{Q}}} \prod_{\nu|p} |x|_\nu^{[K_\nu:\mathbb{Q}_p]} \\ &= \prod_{\nu\in M_K} |x|_\nu^{[K_\nu:\mathbb{Q}_p]} \end{aligned}$$

2.9 Kreisteilungskörper

Die Kreisteilungskörper sind eine wichtige Form algebraischer Zahlkörper und von zentraler Bedeutung für den Beweis der Catalan'schen Vermutung.
Wir fassen nun im Folgenden ihre wichtigsten Eigenschaften zusammen.

Definition 50
Sei $m \in \mathbb{N}$ und $\zeta_m = \mathrm{e}^{\frac{2\pi i}{m}}$ m-te Einheitswurzel, dann heißt $\mathbb{Q}(\zeta_m)$ ***m-ter Kreisteilungskörper****.*

Im folgenden bezeichnen wir mit ζ_m immer die m-te Einheitswurzel $\zeta_m := \mathrm{e}^{\frac{2\pi i}{m}}$.
Wegen

$$x^m - 1 = (x-1)(x-\zeta_m)\cdots(x-\zeta_m^{m-1}) \tag{2.3}$$

ist $\mathbb{Q}(\zeta_m)$ Zerfällungskörper von $x^m - 1$ und somit $\mathbb{Q}(\zeta_m)|\mathbb{Q}$ eine Galoiserweiterung. Dividiert man (2.3) durch $(x-1)$, und setzt dann $x = 1$ so erhält man für m in $\mathbb{Q}(\zeta_m)$ folgende Faktorisierung:

$$m = \prod_{i=1}^{m-1}(1-\zeta_m^i)$$

Definition 51
Die Einheitswurzeln ζ_m^a mit $ggT(a,m) = 1$ und $1 \le a < m$, heißen ***primitive m-te Einheitswurzeln****.*
$\Phi_m(x) := \prod_{ggT(a,m)=1, 1\le a<m}(x-\zeta_m^a)$ heißt das ***m-te Kreisteilungspolynom****, seinen Grad $\varphi(m) := |\{1 \le a < m \mid ggT(a,m) = 1\}|$ nennt man die* ***Euler'sche φ-Funktion****.*

Das m-te Kreisteilungspolynom besitzt folgende Eigenschaften:

Satz 2.9.1
$\Phi_m(x)$ hat nur ganzzahlige Koeffizienten hat und ist irreduzibel in $\mathbb{Z}[X]$. Weiters gilt

$$x^m - 1 = \prod_{d|m} \Phi_d(x).$$

Beweis. Siehe zum Beispiel [31] Kapitel [13,§2] Theorem 1 und Proposition 13.2.2. □

Daraus folgt für die Körpererweiterung $\mathbb{Q}(\zeta_m)|\mathbb{Q}$:

Satz 2.9.2
Die Galoiserweiterung $\mathbb{Q}(\zeta_m)|\mathbb{Q}$ ist vom Grad $\varphi(m)$. Weiters ist ihre Galoisgruppe $G = Gal(\mathbb{Q}(\zeta_m)|\mathbb{Q})$ isomorph zur Einheitengruppe $(\mathbb{Z}/m\mathbb{Z})^\times$ mit dem Isomorphismus

$$(\mathbb{Z}/m\mathbb{Z})^\times \to G, \quad a \mapsto \sigma_a, \quad \sigma_a(\zeta_m) := \zeta_m^a.$$

Beweis. Siehe zum Beispiel [62] Kapitel 2 Theorem 2.5. □

Aufgrund der Kommutativität von $(\mathbb{Z}/m\mathbb{Z})^\times$ ist $\mathbb{Q}(\zeta_m)|\mathbb{Q}$ somit eine abelsche Erweiterung. Für eine Primzahl p ist $(\mathbb{Z}/p\mathbb{Z})^\times$ zyklisch und somit weiters $\mathbb{Q}(\zeta_p)|\mathbb{Q}$ eine zyklische Erweiterung.

Satz 2.9.3
Für $m, n \in \mathbb{N}$ mit $ggT(m,n) = 1$ gilt $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$.

Beweis. Siehe zum Beispiel [62] Kapitel 2 Proposition 2.4. □

Somit sind alle Einheitswurzeln in $\mathbb{Q}(\zeta_m)$ von der Form

$$\pm\zeta_m^a \quad \text{mit } 1 \leq a \leq m.$$

Ein Vorteil der Kreisteilungskörper ist, dass sich ihr Ganzheitsring explizit bestimmen lässt:

Satz 2.9.4
Der Ganzheitsring des Kreisteilungskörpers $\mathbb{Q}(\zeta_m)$ ist $\mathbb{Z}[\zeta_m]$.

Beweis. Siehe zum Beispiel [62] Kapitel 2 Theorem 2.6. □

Auch die Diskriminante von Kreisteilungskörpern lässt sich explizit berechnen:

Satz 2.9.5
Für die Diskriminante des Kreisteilungskörpers $\mathbb{Q}(\zeta_m)$ gilt

$$\delta_{\mathbb{Q}(\zeta_m)} = (-1)^{\frac{\varphi(m)}{2}} \frac{m^{\varphi(m)}}{\prod_{p|m} p^{\frac{\varphi(m)}{p-1}}}.$$

Beweis. Siehe zum Beispiel [62] Kapitel 2 Proposition 2.7. □

Der nächste Satz gibt Aufschluss über die Zerlegung einer Primzahl p in Primideale eines Kreisteilungskörpers.

Satz 2.9.6
Sei p eine Primzahl

1. *p ist genau dann verzweigt in $\mathbb{Q}(\zeta_m)$, wenn $p|m$.*

2. *Falls $p \nmid m$ und $f \in \mathbb{N}$ die kleinste Zahl ist für die $p^f \equiv 1 \pmod{m}$ gilt, dann zerfällt p in $g = \frac{\varphi(m)}{f}$ verschiedene Primideale in $\mathbb{Q}(\zeta_m)$, wobei jedes Primideal Restklassengrad f hat.*
Insbesondere zerfällt p genau dann komplett, wenn $p \equiv 1 \pmod{m}$

Beweis. Siehe zum Beispiel [62] Kapitel 2 Proposition 2.3 und Theorem 2.13. □

Im Körper $\mathbb{Q}(\zeta_p)$ gibt es also genau eine verzweigte Primzahl, nämlich p.

Der folgende Satz von Kronecker und Weber liefert nun eine fundamentale Aussage für abelsche Erweiterungen von $\mathbb{Q}$:

Satz 2.9.7 (Kronecker und Weber)
Sei K ein Zahlkörper und die Erweiterung $K|\mathbb{Q}$ abelsch, dann gibt es ein $m \in \mathbb{N}$ und eine Einheitswurzel ζ_m sodass $K \subseteq \mathbb{Q}(\zeta_m)$.

Beweis. Siehe zum Beispiel [62] Kapitel 14 Theorem 14.1. □

Eine wichtige Rolle für uns spielt auch der maximale reelle Unterkörper eines Kreisteilungskörpers:

$$\mathbb{Q}(\zeta_m)^+ := \mathbb{Q}(\zeta_m + \zeta_m^{-1}).$$

Die Erweiterung $\mathbb{Q}(\zeta_m)|\mathbb{Q}(\zeta_m)^+$ ist vom Grad 2, da $\mathbb{Q}(\zeta_m)^+$ der Fixkörper der komplexen Konjugation ist.

Satz 2.9.8
Der Ganzheitsring von $\mathbb{Q}(\zeta_m)^+$ ist $\mathbb{Z}[\zeta_m + \zeta_m^{-1}]$.

Beweis. Siehe zum Beispiel [62] Kapitel 2 Proposition 2.16. □

Sei H die Idealklassengruppe von $\mathbb{Q}(\zeta_m)$ und H^+ die Idealklassengruppe von $\mathbb{Q}(\zeta_m)^+$, dann lässt sich H^+ auf natürliche Art in H einbetten. Folglich ist die Klassenzahl h^+ von $\mathbb{Q}(\zeta_m)^+$ ein Teiler von $h(\mathbb{Q}(\zeta_m))$ und

Definition 52
*Mit den obigen Notationen nennt man $h^-(\mathbb{Q}(\zeta_m)) = [H : H^+]$ die **relative Klassenzahl**.*

Zwischen den Einheiten in $\mathbb{Q}(\zeta_m)$ und jenen in $\mathbb{Q}(\zeta_m)^+$ besteht folgender Zusammenhang:

Satz 2.9.9
Sei $K := \mathbb{Q}(\zeta_m)$ und bezeichne E die Gruppe der Einheiten in K (genauer: die Einheitengruppe von O_K, also $E := {O_K}^\times$) und E^+ jene in K^+, sowie W die Gruppe der Einheitswurzeln in K, dann gilt

$$[E : WE^+] = \begin{cases} 1 & \text{falls } m \text{ eine Primzahlpotenz ist} \\ 2 & \text{sonst} \end{cases}$$

Beweis. Siehe zum Beispiel [62] Kapitel 4 Theorem 4.12 und Corollary 4.13. □

Im Fall $K = \mathbb{Q}(\zeta_{p^n})$ gibt es also zu jeder Einheit ε von O_K eine Einheit $\varepsilon' \in K^+$ und ein $r \in \mathbb{N}$ sodass gilt:

$$\varepsilon = (\pm\zeta_{p^n})^r \varepsilon'.$$

2.10 Der Sätze von Stickelberger und Thaine

Wir stellen nun noch zwei Sätze aus der Theorie der Kreisteilungskörper vor, deren Anwendung auf das Catalan'sche Problem es Mihailescu ermöglichten die Catalan'sche Vermutung zu beweisen.

Sei nun im Folgenden M eine abelsche Erweiterung von $\mathbb{Q}$. Nach dem Satz von Kronecker und Weber existiert ein $m \in \mathbb{N}$, sodass $M \subseteq \mathbb{Q}(\zeta_m)$. Sei dieses m minimal. Die Galoisgruppe $G := Gal(M|\mathbb{Q})$ ist dann eine Untergruppe von $Gal(\mathbb{Q}(\zeta_m)|\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ und wir bezeichnen mit σ_a jenes Element der Galoisgruppe für das $\sigma_a(\zeta_m) = \zeta_m^a$ gilt, für $1 \leq a < m$ mit $ggT(a, m) = 1$.

Wir betrachten nun den Gruppenring $\mathbb{Z}[G]$ (bzw. $\mathbb{Q}[G]$) und lassen ein Element $\Theta = \sum_{\sigma \in G} c_\sigma \sigma$ auf $\mathbb{Q}(\zeta_m)$ wie folgt operieren:

$$x^\Theta := \prod_{\sigma \in G} \sigma(x)^{c_\sigma}, \quad \text{für } x \in \mathbb{Q}(\zeta_m)$$

In gleicher Weise lässt man Θ auch auf Ideale des Ganzheitsringes wirken und kann so beispielsweise die Gruppe der Ideale, aber auch die Idealklassengruppe als $\mathbb{Z}[G]-$(bzw. $\mathbb{Q}[G]-$)Modul auffassen.
Mit $\{x\}$ bezeichnen wir im Folgenden den gebrochenen Anteil einer rationalen Zahl x, es ist also $x - \{x\} \in \mathbb{Z}$ mit $0 \leq \{x\} < 1$.

Definition 53
*Das **Stickelbergerelement** θ von M ist nun definiert durch:*

$$\theta = \theta(M) := \sum_{1 \leq a < m, ggT(a,m)=1} \left\{\frac{a}{m}\right\} {\sigma_a}^{-1}$$

*Das **Stickelbergerideal** I_S von M ist definiert durch*

$$I_S = I_S(M) := \mathbb{Z}[G] \cap \theta(M)\mathbb{Z}[G]$$

Das Stickelbergerideal enthält also genau die $\mathbb{Z}[G]$-Vielfachen von $\theta(M)$ mit ganzzahligen Koeffizienten.
Für Kreisteilungskörper weiß man, wie das Stickelbergerideal erzeugt ist:

Lemma 2.10.1
Sei nun $M = \mathbb{Q}(\zeta_m)$. Mit I' bezeichnen wir das Ideal von $\mathbb{Z}[G]$, das von den Elementen der Form $c - \sigma_c$, mit $ggT(c, m) = 1$, erzeugt wird. Sei $\beta \in \mathbb{Z}[G]$ und θ das Stickelbergerelement von M, dann gilt

$$\beta\theta \in \mathbb{Z}[G] \Longleftrightarrow \beta \in I'.$$

Es gilt also $I_S(M) = I'\theta$.

Beweis. Siehe zum Beispiel [62] Kapitel 6.2 Lemma 6.9. □

Die wesentliche Eigenschaft des Stickelbergerideals zeigt der Satz von Stickelberger:

Satz 2.10.2 (Stickelberger)
Sei A ein Bruchideal eines abelschen Zahlkörpers M, und sei $\beta \in \mathbb{Z}[G]$ sodass $\beta\theta \in \mathbb{Z}[G]$. Dann ist $A^{\beta\theta}$ ein Hauptbruchideal. Oder mit anderen Worten: Das Stickelbergerideal annulliert die Idealklassengruppe von M.

Beweis. Siehe zum Beispiel [62] Kapitel 6.2 Theorem 6.10. □

Der folgende Satz von Iwasawa stellt nun einen Zusammenhang zwischen dem Stickelbergerideal und der relativen Klassenzahl her:

Satz 2.10.3 (Iwasawa)
Sei $K := \mathbb{Q}(\zeta_p)$ für eine ungerade Primzahl p und G die zugehörige Galoisgruppe, und sei weiters $I_S^- := (1-\iota)I_S(K)$ und $\mathbb{Z}[G]^- := (1-\iota)\mathbb{Z}[G]$, wobei ι die komplexe Konjugation bezeichne, so gilt

$$h^-(K) = [\mathbb{Z}[G]^- : I_S^-].$$

Beweis. Siehe zum Beispiel [62] Kapitel 6.4 Theorem 6.19. □

Da die relative Klassenzahl $h^-(K)$ ein Teiler der Klassenzahl von K ist folgt daraus, dass der Index $[\mathbb{Z}[G]^- : I_S^-]$ endlich ist.

Der Satz von Stickelberger ist für reelle Zahlkörper nicht sehr aussagekräftig. Eine Möglichkeit auch in diesem Fall Annullatoren der Idealklassengruppe zu finden liefert der Satz von Thaine.
Dazu benötigen wir zunächst den Begriff der Kreisteilungseinheiten eines abelschen Zahlkörpers. Diese werden in der Literatur unterschiedlich definiert, Thaine definiert sie wie folgt:

Definition 54
Sei M ein abelscher Zahlkörper, und $m \in \mathbb{Z}$ sodass $M \subseteq \mathbb{Q}(\zeta_m)$. Dann nennt man die Einheiten von M der Form

$$\pm \mathrm{N}^M_{\mathbb{Q}(\zeta_m)} \left(\prod_{a=1}^{m-1} (\zeta_m^a - 1)^{b_a} \right),$$

*mit $b_a \in \mathbb{Z}$ die **Kreisteilungseinheiten** von M.*

Der Satz von Thaine besagt nun Folgendes:

Satz 2.10.4 (Thaine)
Sei M ein reeller abelscher Zahlkörper mit Galoisgruppe $G = Gal(M|\mathbb{Q})$, E die Gruppe der Einheiten von M und C die Gruppe der Kreisteilungseinheiten von M. Sei nun p eine Primzahl, die $[M : \mathbb{Q}]$ nicht teilt und $\Theta \in \mathbb{Z}[G]$ annulliere die p-Sylow-Untergruppe von E/C, dann annulliert 2Θ die p-Sylow-Untergruppe der Idealklassengruppe von M.

Beweis. Siehe zum Beispiel [62] Kapitel 15.2 Theorem 15.2 oder [60] Theorem 3. □

Für unsere Zwecke relevant ist das folgende Korollar:

Korollar 2.10.5
Sei p eine ungerade Primzahl und $M \subseteq \mathbb{Q}(\zeta_p)^+$. Falls $\Theta \in \mathbb{Z}[G]$ dann die p-Sylow-Untergruppe von E/C annulliert, so annulliert Θ auch die p-Sylow-Untergruppe der Idealklassengruppe von M.

Beweis. Siehe zum Beispiel [60] Corollary. □

Kapitel 3

Spezialfälle

In diesem Kapitel beschäftigen wir uns mit den Spezialfällen der Catalan'schen Gleichung $x^m - y^n = 1$ wenn m oder n gerade ist, und geben die jeweiligen Beweise dafür wieder. Dabei werden größtenteils elementare Methoden verwendet.

Die getrennte Behandlung dieser Fälle ist unbedingt notwendig, da alle späteren Resultate, inklusive Mihailescus Beweis der Catalan'schen Vermutung nur mit den Fall ungerader Primzahlexponenten betrachten.

Zum Abschluss dieses Kapitels werfen wir noch einen Blick auf den Fall dass einer der beiden Exponenten gleich 3 ist.

3.1 Die Folge der Quadrate und Kuben

Im Jahr 1738 zeigte Leonhard Euler, dass 8 und 9 die einzigen aufeinanderfolgenden Zahlen in der Folge aller Quadrate und Kuben positiver ganzer Zahlen sind, oder anders - in unserer Notation - ausgedrückt: $x = 3, y = 2$ ist die einzige positive ganzzahlige Lösung der Gleichung $x^2 - y^3 = \pm 1$.

Dazu zeigte er zunächst folgendes Lemma:

Lemma 3.1.1
Seien b und c teilerfremde ganze Zahlen ≥ 1. Wenn $bc(c^2 \pm 3bc + 3b^2)$ das Quadrat einer ganzen Zahl ist, dann ist entweder $b = 1$, $c = 1$ oder $b = 1$, $c = 3$, und der Ausdruck muss gleich $bc(c^2 - 3bc + 3b^2) = 1$ oder 9 sein.

Beweis. Die Diskriminante von $X^2 \pm 3bX + 3b^2$ ist $-3b^2 < 0$, somit ist $c^2 \pm 3bc + 3b^2 > 0$ für alle Werte von b, c.
Angenommen die Behauptung wäre falsch, dann gäbe es ein minimales Quadrat der Form $bc(c^2 \pm 3bc + 3b^2)$ mit $(b, c) \neq (1, 1), (1, 3)$.

Wir zeigen zunächst $3 \nmid c$: Wäre $c = 3d$, dann wäre $3^2 bd(b^2 \pm 3bd + 3d^2)$ ein Quadrat und somit auch $bd(b^2 \pm 3bd + 3d^2)$. Aber

$$0 < bd(b^2 \pm 3bd + 3d^2) = \frac{1}{9} bc(c^2 \pm 3bc + 3b^2) < bc(c^2 \pm 3bc + 3b^2)$$

Wegen der Minimalitätsbedingung muss $(d, b) = (1, 1)$ oder $(1, 3)$ sein, und damit $(b, c) = (1, 3)$ oder $(3, 3)$, was aber wegen der Annahme bzw. $ggT(b, c) = 1$ ausgeschlossen ist.

Es gilt $ggT(b, c^2 \pm 3bc + 3b^2) = 1$; wegen $3 \nmid c$ gilt auch $ggT(c, c^2 \pm 3bc + 3b^2) = 1$. Aufgrund der Eindeutigkeit der Primfaktorzerlegung müssen somit alle drei Faktoren b, c und $c^2 \pm 3bc + 3b^2$ Quadrate sein. Es gibt also ein $e \geq 1$ mit $e^2 = c^2 \pm 3bc + 3b^2$. Wegen $b \neq c$ ist deshalb auch $e \neq c$.

Sei $\frac{m}{n} := \frac{c-e}{b} \neq 0$ mit $n \geq 1$, $ggT(m, n) = 1$, dann gilt $e = c - \frac{m}{n}b$ und weiters

$$c^2 \pm 3bc + 3b^2 = \left(c - \frac{m}{n}b\right)^2 = c^2 - 2bc\frac{m}{n} + b^2\frac{m^2}{n^2}.$$

Umformen und Kürzen durch $b \neq 0$ liefert

$$\frac{b}{c} = \frac{2mn \pm 3n^2}{m^2 - 3n^2} \quad (m^2 \neq 3n^2)$$

Wir zeigen $ggT(2mn \pm 3n^2, m^2 - 3n^2) = 1$ oder 3: Angenommen $2 \mid 2mn \pm 3n^2$ und $2 \mid m^2 - 3n^2$, dann folgt $2|m$ und $2|n$, Widerspruch! Sei also p eine ungerade Primzahl und $r \geq 1$ mit $p^r \mid 2mn \pm 3n^2$ und $p^r \mid m^2 - 3n^2$, dann gilt $p^r \mid m(m \pm 2n)$. Falls $p \mid m \pm 2n$ dann gilt $p \mid 2mn \pm 4n^2$ und, wegen $p \mid 2mn \pm 3n^2$, folgt $p|n$ und damit auch $p|m$,Widerspruch! Es muss also $p^r|m$ gelten; wegen $p \nmid n$ und $p|3n^2$ folgt $p^r|3$, also $p^r = 3$.

Wir behandeln nun diese zwei Fälle getrennt:

1. Fall: $ggT(2mn \pm 3n^2, m^2 - 3n^2) = 1$

Es gilt $3 \nmid m$ und $c = \pm(m^2 - 3n^2)$. Falls $c = -(m^2 - 3n^2)$, dann wäre $c \equiv -m^2 \equiv -1$ (3), was aber nicht möglich ist, da c ein Quadrat ist.
Es ist also $c = m^2 - 3n^2$ und $b = 2mn \pm 3n^2 = n(2m \pm 3n)$. Sei $f^2 := c = m^2 - 3n^2$ mit $f > 0$, dann ist $m > f$, und sei weiters $\frac{u}{v} := \frac{m-f}{n}$ mit $u, v \geq 1$ und $ggT(u, v) = 1$.
Es gilt also $f = m - \frac{u}{v}n$ und weiters $m^2 - 3n^2 = f^2 = \left(\frac{u}{v}n\right)^2$. Elementares Umformen liefert

$$\frac{m}{n} = \frac{u^2 + 3v^2}{2uv} \tag{3.1}$$

Damit folgt

$$\frac{b}{n^2} = \frac{2m}{n} \pm 3 = \frac{u^2 \pm 3uv + 3v^2}{uv}, n^2uv(u^2 \pm 3uv + 3v^2) = bu^2v^2 \tag{3.2}$$

Da b ein Quadrat ist, muss folglich auch $uv(u^2 \pm 3uv + 3v^2)$ ein Quadrat sein. $(v, u) = (1, 1)$ oder $(1, 3)$ sind jedoch unmöglich: $uv(u^2+3uv+3v^2) = 7$ oder 63 ist für diese Werte kein Quadrat. $uv(u^2-3uv+3v^2) = 1$ oder 9, ebenso $u^2v^2 = 1$ oder 9; aus (3.2) folgt somit $b = n^2$. Weiters ergibt sich $\frac{m}{n} = \frac{u^2+3v^2}{2uv} = 2$, und da $f > 0$ und $\frac{m-f}{n} = \frac{u}{v}$ folgt $\frac{f}{n} = \frac{m}{n} - \frac{u}{v} = 1$. Es ist also $n = f = c^2$, und somit $b = c^4$. Wegen $ggT(b, c) = 1$ folgt damit $b = c = 1$, was im Widerspruch zu unserer Annahme steht!

Laut Annahme gilt daher

$$uv(u^2 \pm 3uv + 3v^2) \geq bc(c^2 \pm 3bc + 3b^2) \tag{3.3}$$

Wir zeigen nun $ggT(2uv, u^2+3v^2) \mid 6$: Falls $4|2uv$ und $4 \mid u^2+3v^2$, dann folgt $2|uv$ und es gilt entweder $2|u, 2 \nmid v$ woraus $2 \nmid u^2+3v^2$ folgt, oder $2|v, 2 \nmid u$ woraus wiederum $2 \nmid u^2+3v^2$ folgt, Widerspruch!
Falls p eine ungerade Primzahl ist und $r \geq 1$ mit $p^r|2uv$ und $p^r \mid u^2+3v^2$, dann folgt $p^r|uv$ und es gilt

$$\begin{cases} p^r|u, p \nmid v, & \text{woraus } p^r|3v^2 \text{ und weiters } p^r = 3 \text{ folgt, oder} \\ p^r|v, p \nmid u, & \text{woraus } p^r|u \text{ folgt, Widerspruch!} \end{cases}$$

Es gilt also $ggT(2uv, u^2+3v^2) = 2^r 3^s$, mit $r, s \in \{0, 1\}$. Laut (3.1) gilt $2uvm = n(u^2+3v^2)$, daraus folgt $\frac{2uv}{2^r 3^s} \mid n$ und somit weiters $uv \mid 3n$.

Daraus folgt: $n^2(u^2 \pm 3uv + 3v^2) = uvb$ teilt $3nb = 3n^2(2m \pm 3n)$. Also gilt

$$uv(u^2 \pm 3uv + 3v^2) \mid 3uv(2m \pm 3n) \mid 9n(2n \pm 3m) = 9b$$

Damit gilt wegen (3.6): $bc(c^2 \pm 3bc + 3b^2) \leq 9b$, also $c(c^2 \pm 3bc + 3b^2) \leq 9$. Es gilt aber $\frac{c^3}{4} \leq c(c^2 \pm 3bc + 3b^2)$, da:

$$\frac{3c^2}{4} \pm 3bc + 3b^2 = \frac{3}{4}(c^2 \pm 4bc + 4b^2) = \frac{3}{4}(c \pm 2b)^2 \geq 0$$

Somit muss $c^3 \leq 36$ gelten, also $c \leq 3$, und da c ein Quadrat ist folgt $c = 1$.
Damit erhält man $1 \pm 3b + 3b^2 \leq 9$, also $3b(b \pm 1) \leq 8$, und da b ein Quadrat ist folgt $b = 1$, was einen Widerspruch zur ursprünglichen Annahme darstellt.

2. Fall: $ggT(2mn \pm 3n^2, m^2 - 3n^2) = 3$
Es gilt $3|m$ und damit $3 \nmid n$. Sei $m = 3k$, dann ist $ggT(k, n) = 1$ sowie $ggT(2kn \pm n^2, 3k^2 - n^2) = 1$ und $\frac{b}{c} = \frac{2kn \pm n^2}{3k^2 - n^2}$. Also ist $c = \pm(3k^2 - n^2)$. Es kann aber $3k^2 - n^2$ kein Quadrat sein, sonst wäre $-n^2 \equiv -1$ (3) ein Quadrat. Da c ein Quadrat ist gilt daher $c = n^2 - 3k^2$ und $b = \pm n^2 - 2kn = n(\pm n - 2k)$.

Sei wiederum $f^2 := c = n^2 - 3k^2$ mit $f > 0$, dann ist $n > f$ und es sei weiters $\frac{u}{v} := \frac{n-f}{k}$ mit $u, v \geq 1$ und $ggT(u, v) = 1$. Es gilt $n^2 - 3k^2 = f^2 = \left(n - \frac{u}{v}k\right)^2$, elementares Umformen liefert

$$\frac{n}{k} = \frac{u^2 + 3v^2}{2uv} \tag{3.4}$$

und weiters $\frac{b}{n^2} = \pm 1 - \frac{2k}{n} = \pm 1 - \frac{4uv}{u^2+3v^2}$. Da b, u und v positiv sind ist der Fall mit "-1" nicht möglich und es folgt $\frac{b}{n^2} = \frac{u^2-4uv+3v^2}{u^2+3v^2}$ und weiters

$$n^2(u^2 - 4uv + 3v^2)(u^2 + 3v^2) = b(u^2 + 3v^2)^2 \tag{3.5}$$

Da b ein Quadrat ungleich 0 ist, ist folglich auch

$$(u^2 - 4uv + 3v^2)(u^2 + 3v^2) = (u - v)(u - 3v)(u^2 + 3v^2)$$

ein Quadrat und $(u-v)(u-3v)$ ist positiv mit $u \neq v, u \neq 3v$.
Sei

$$\begin{cases} t & := & \frac{|u-v|}{2} \\ s & := & \frac{|u-3v|}{2} \end{cases} \text{ falls } u,v \text{ beide ungerade, bzw. } \begin{cases} t & := & |u-v| \\ s & := & |u-3v| \end{cases} \text{ sonst.}$$

Es ist also $t > 0$, $s > 0$ und wegen $ggT(u,v) = 1$ auch $ggT(s,t) = 1$.
Im Fall dass u und v beide ungerade sind gilt, da $(u-v)(u-3v) > 0$:

$$\begin{aligned} ts(s^2-3ts+3t^2) &= \frac{|u-v|}{2}\frac{|u-3v|}{2}\frac{1}{4}\Big[(u-3v)^2 - 3|u-v||u-3v| + 3(u-v)^2\Big] \\ &= \frac{1}{16}(u^2-4uv+3v^2)\Big[(u^2-6uv+9v^2) - 3(u^2-4uv+3v^2) \\ &+ 3(u^2-2uv+v^2)\Big] \\ &= \frac{1}{16}(u^2-4uv+3v^2)(u^2+3v^2) \end{aligned}$$

Im Fall dass u oder v gerade ist erhält man auf analoge Weise $ts(s^2-3ts+3t^2) = (u^2-4uv+3v^2)(u^2+3v^2)$. Es ist also in beiden Fällen $ts(s^2-3ts+3t^2)$ ein Quadrat.

Wir zeigen nun, dass $(t,s) = (1,1)$ oder $(1,3)$ nicht möglich ist:
Sonst wäre $ts(s^2-3ts+3t^2) = 1$ oder 9 und im Fall dass u und v beide ungerade sind gilt

$$(u^2-4uv+3v^2)(u^2+3v^2) = 16 \text{ oder } 16 \cdot 9 = 144.$$

Es müsste also $u^2+3v^2 \mid 16$ oder 144 gelten, was aber, wie man leicht überprüfen kann, unmöglich ist für teilerfremde, ungerade u, v.
Falls u oder v gerade ist gilt

$$(u^2-4uv+3v^2)(u^2+3v^2) = 1 \text{ oder } 9,$$

was, wie man ebenfalls leicht überprüfen kann, nicht möglich ist. Somit ist $(t,s) \notin \{(1,1),(1,3)\}$ und laut Annahme gilt

$$(u^2-4uv+3v^2)(u^2+3v^2) \geq ts(s^2-3ts+3t^2) \geq bc(c^2-3bc+3b^2) \quad (3.6)$$

Wie im ersten Fall gilt $ggT(2uv, u^2+3v^2) \mid 6$. Laut (3.4) ist $(u^2+3v^2)k = 2uvn$ woraus $u^2+3v^2 \mid 6n$ folgt, und mit(3.5) gilt

$$(u^2-4uv+3v^2)(u^2+3v^2) = b\left(\frac{u^2+3v^2}{n}\right)^2 \Big| 36b$$

Mit der Ungleichung in (3.6) folgt

$$c(c^2-3bc+3b^2) \leq 36 \quad (3.7)$$

Es gilt jedoch, wie im ersten Fall, $c(c^2-3bc+3b^2) \geq \frac{c^3}{4}$, also folgt $c^3 \leq 4 \cdot 36 = 144$, also $c \leq 5$ und da c ein Quadrat ist gilt $c = 1$ oder 4. Aus (3.7) folgt damit $1-3b+3b^2 \leq 36$ oder $16-12b+3b^2 \leq 9$, und da b ein Quadrat ist kann nur $b = 1$ sein. Für die Werte $b = 1, c = 4$ ergibt aber $bc(c^2-3bc+3b^2) = 28$ kein Quadrat, somit gilt $b = 1, c = 1$ was im Widerspruch zu unserer Annahme steht.

□

Damit lässt sich nun der folgende Satz leicht zeigen:

Satz 3.1.2 (Euler)

(i) Seien x, u teilerfremde ganze Zahlen, $x \neq 0$, $u \geq 1$. Wenn $\left(\frac{x}{u}\right)^3 \pm 1$ das Quadrat einer rationalen Zahl ungleich 0 ist, dann gilt $\frac{x}{u} = 2$.

(ii) Wenn $x, y \geq 1$ ganze Zahlen sind für die $x^3 - y^2 = \pm 1$ gilt, dann ist $x = 2$ und $y = 3$.

Beweis. (*i*) Sei $\left(\frac{x}{u}\right)^3 \pm 1$ das Quadrat einer rationalen Zahl ungleich 0, dann ist $x^3u \pm u^4$ eine positive ganze Zahl und auch ein Quadrat. Sei $z := x \pm u$, also $ggT(z, u) = 1$ und $z \neq \pm u$. Dann gilt

$$0 < x^3u \pm u^4 = u(x \pm u)(x^2 \mp xu + u^2) = uz(z^2 \mp 3uz + 3u^2)$$

also $z \neq 0$. Wegen $z^2 \mp 3uz + 3u^2 \geq 0$ (da die Diskriminante $9u^2 - 12u^2 = -3u^2 < 0$) gilt $z > 0$.
Aus dem Lemma 3.1.1 folgt $(u, z) = (1, 1)$ oder $(1, 3)$ und der Ausdruck muss gleich $uz(z^3 - 3uz + 3u^3)$ sein, was auf $\left(\frac{x}{u}\right)^3 + 1$ führt. Somit ist $z = x + u$ und weiters $x = 2$ und $u = 1$.
(*ii*) ist eine triviale Folgerung aus (*i*). □

3.2 Die Gleichung $X^m - Y^2 = 1$

Bereits 1850, also 6 Jahre nachdem Catalan seine Vermutung formuliert hatte, konnte V.A. Lebesgue in [38] für die Gleichung $X^m - Y^2 = 1$ folgendes zeigen:

Satz 3.2.1 (Lebesgue)
Die Gleichung $X^m - Y^2 = 1$ (mit $m \in \mathbb{Z}$, $m \geq 2$) hat keine positive ganzzahlige Lösung.

Beweis. Der Satz ist trivial für gerades m. Sei m also ungerade und $x, y \geq 1$ ganze Zahlen mit $x^m - y^2 = 1$. Ist y ungerade, dann gilt $x^m \equiv 2 \pmod 4$, was für $m \geq 2$ nicht möglich ist. Also muss y gerade und folglich x ungerade sein.

Sei $i := \sqrt{-1}$, dann gilt $x^m = y^2 + 1 = (y + i)(y - i)$. Sei π prim in den Gauß'schen ganzen Zahlen $\mathbb{Z}[i]$ mit $\pi \mid y + i$ und $\pi \mid y - i$, dann teilt π auch $2i$. Da i eine Einheit ist muss $\pi | 2$ und, da y gerade ist, $\pi | y$ gelten. Wegen $\pi \mid y + i$ gilt damit auch $\pi | i$, was ein Widerspruch zu π prim ist. Daraus folgt der $ggT(y + i, y - i)$ ist eine Einheit von $\mathbb{Z}[i]$.

Der Faktor $y + i$ von x^m ist also, bis auf eine Einheit, eine m-te Potenz: $y + i = (u + iv)^m i^s$, mit $u, v, s \in \mathbb{Z}$, $0 \leq s \leq 3$. Konjugieren liefert: $y - i = (u - iv)^m (-i)^s$. Also $x^m = y^2 + 1 = (u^2 + v^2)^m$, und damit $x = u^2 + v^2$. Da x ungerade ist, muss entweder u oder v gerade sein. Die Subtraktion $(y + i) - (y - i)$ liefert:

$$2i = [(u + iv)^m - (u - iv)^m (-1)^s] i^s.$$

- Falls $s = 2r$ liefert ein Vergleich der Koeffizienten von i:

$$1 = (-1)^r \left[mu^{m-1}v - \binom{m}{3} u^{m-3}v^3 + \cdots \pm v^m \right], \tag{3.8}$$

  und damit $v|1$, also $v = \pm 1$, v ist ungerade, u gerade.

- Falls $s = 2r + 1$ folgt auf gleichem Weg:

$$1 = (-1)^r \left[u^m - \binom{m}{2} u^{m-2}v^2 + \cdots \pm muv^{m-1} \right], \tag{3.9}$$

  und damit $u|1$, also $u = \pm 1$, u ist ungerade, v gerade.

Sei nun $w := u$ (im ersten Fall) oder $w := v$ (im zweiten Fall), dann ist w gerade und in beiden Fällen lassen sich die obigen Gleichungen (3.8) und (3.9) umschreiben zu:

$$1 - \binom{m}{2} w^2 + \binom{m}{4} w^4 - \cdots \pm mw^{m-1} = \pm 1.$$

"-1" auf der rechten Seite ist jedoch unmöglich, da daraus $w^2|2$ folgen würde, was einen Widerspruch zu w gerade darstellt. Mit "$+1$" auf der rechten Seite kann man durch w^2 dividieren und erhält:

$$\binom{m}{2} - \binom{m}{4} w^2 + \cdots \pm mw^{m-3} = 0. \tag{3.10}$$

Nun ist w gerade, also muss $\binom{m}{2}$ auch gerade sein. Sei der 2-adische Wert des ersten Summanden $\nu_2\left(\binom{m}{2}\right) =: t \geq 1$. Es gilt aber

$$\binom{m}{2k} w^{2k-2} = \binom{m}{2} \binom{m-2}{2k-2} \frac{2}{2k(2k-1)} w^{2k-2},$$

und da für $k \geq 2$ immer $2^{2k-2} > k$ gilt folgt daraus $\nu_2(w^{2k-2}) \geq 2k-2 > \nu_2(k)$. Damit gilt für den 2-adischen Wert jedes Summanden in (3.10) mit $k \geq 2$: $\nu_2\left(\binom{m}{2k} w^{2k-2}\right) \geq t + \nu_2\left(\frac{w^{2k-2}}{k}\right) \geq t + 1$. Damit kann die Gleichung (3.10) aber unmöglich erfüllt werden und es ist gezeigt, dass es keine ganzen Zahlen $x, y \geq 1$ mit $x^m - y^2 = 1$ geben kann. □

3.3 Die Gleichung $X^2 - Y^n = 1$

Erst 1965 gelang Chao Ko in [33] der Beweis, dass diese spezielle Gleichung für $n > 1$ nur eine ganzzahlige Lösung, nämlich $3^2 - 2^3 = 1$, hat. Im Jahr 1976 fand Chein einen eleganteren und wesentlich einfacheren Beweis (siehe [15]), den wir im folgenden wiedergeben werden.

Cheins Beweis basiert auf einem Resultat von Nagell aus dem Jahr 1921 für das man wiederum einen Satz von Størmer über diophantische Gleichungen der Form $X^2 - DY^2 = \pm 1$ benötigt, den dieser bereits 1898 bewiesen hatte. Wir werden nun

2 allgemeinere Resultate über Gleichungen der Form $X^2 - DY^2 = C$ anführen, die Størmers Originalresultat als Spezialfall beinhalten. Für die Beweise hierfür verweisen wir jeweils auf Ribenboim's Buch [54].

Das erste Ergebnis stammt von Shepel aus dem Jahr 1935.

Satz 3.3.1
Seien $D > 1$ und $C \neq 0$ quadratfreie ganze Zahlen mit $C|2D$. Sei weiters (x_1, y_1) eine positive ganzzahlige Fundamentallösung (d.h. mit minimalem y_1) der Gleichung

$$X^2 - DY^2 = C \tag{3.11}$$

Dann sind für alle $n \geq 1$ (falls $C > 0$) bzw. für alle ungeraden $n \geq 1$ (falls $C < 0$) die positiven ganzzahligen Lösungen die Zahlen (x_n, y_n), die definiert sind durch

$$|C|^{\frac{n-1}{2}}(x_n + y_n\sqrt{D}) = (x_1 + y_1\sqrt{D})^n$$

Beweis. Siehe [54] Satz P5.10. □

Definition 55
*Eine natürliche Zahl n hat die **Størmer Eigenschaft** bezüglich (C, D) wenn für die Lösung (x_n, y_n) der Gleichung (3.11) gilt: Teilt eine Primzahl p die Zahl y_n, dann teilt sie auch D.*
Die Menge aller Zahlen, die die Størmer Eigenschaft bezüglich (C, D) erfüllen, bezeichnen wir mit $S_{(C,D)}$.

Das zweite Ergebnis ist von Mahler, aus dem Jahr 1935.

Satz 3.3.2

$$S_{(C,D)} \subseteq \{1, 3\} \quad \text{spezieller gilt} \quad S_{(\pm 1,D)} \subseteq \{1\}$$

Beweis. Siehe [54] Sätze A4.1 und A4.2. □

Wir benötigen nun zunächst noch ein allgemeines Lemma:

Lemma 3.3.3
Sei $n > 1$ eine ganze Zahl, seien $x, y \in \mathbb{Z} \setminus \{0\}$ relativ prim, dann gilt:

$$ggT\left(x - y, \frac{x^n - y^n}{x - y}\right) = ggT\left(x - y, n\right).$$

Speziell für eine ungerade Primzahl p folgt dann: $ggT\left(x \pm y, \frac{x^p \pm y^p}{x \pm y}\right) = 1$ oder p.

Beweis. Zunächst gilt

$$\begin{aligned}
\frac{x^n - y^n}{x - y} &= \frac{[(x - y) + y]^n - y^n}{x - y} \\
&= (x - y)^{n-1} + \binom{n}{1} y(x - y)^{n-2} + \cdots + \binom{n}{n-2} y^{n-2}(x - y) + ny^{n-1} \\
&= k(x - y) + ny^{n-1}, \qquad (3.12)
\end{aligned}$$

wobei $k = (x-y)^{n-2} + \binom{n}{1}y(x-y)^{n-3} + \cdots + \binom{n}{n-2}y^{n-2} \in \mathbb{Z}$.
Wegen $ggT(x,y) = 1$ ist auch $ggT(x-y,y) = 1$. Mit der Darstellung von $\frac{x^n-y^n}{x-y}$ aus (3.12) folgt somit

$$ggT\left(x-y, \frac{x^n-y^n}{x-y}\right) = ggT\left(x-y, n\right).$$

Da p ungerade ist gilt $ggT\left(x+y, \frac{x^p+y^p}{x+y}\right) = ggT\left(x-(-y), \frac{x^p-(-y)^p}{x-(-y)}\right)$, woraus die Behauptung folgt. □

Damit können wir nun folgendes Resultat von Nagell beweisen:

Lemma 3.3.4 (Nagell)
Wenn x, y positive ganze Zahlen sind, $q \geq 3$ eine Primzahl mit $x^2 - y^q = 1$, dann gilt

$$2|y \quad \text{und} \quad q|x.$$

Beweis:

- $2|y$: Angenommen y ist ungerade, dann ist x gerade und $ggT(x-1, x+1) = 1$. Da $y^q = (x-1)(x+1)$ muss es daher ganze Zahlen a und b geben, mit

$$\begin{cases} x+1 &= a^q \\ x-1 &= b^q \end{cases}$$

  wobei a und b ungerade sind mit $a > b > 0$. Subtraktion liefert $2 = a^q - b^q = (a-b)\frac{a^q-b^q}{a-b}$ und damit $a-b = 1$ oder 2. Da a und b ungerade sind gilt $a-b = 2$ und somit

$$1 = \frac{a^q-b^q}{a-b} = a^{q-1} + a^{q-2}b + \cdots + ab^{q-2} + b^{q-1}$$

  was unmöglich ist, da $a > b > 0$ und $q \geq 3$. Also ist y gerade.

- $q|x$: Angenommen $q \nmid x$, dann folgt aus

$$x^2 = y^q + 1 = (y+1)\frac{y^q+1}{y+1}$$

  mit Lemma 3.3.3, dass $ggT(y+1, \frac{y^q+1}{y+1}) = 1$. Es gibt also eine ganze Zahl $c > 1$ mit $y+1 = c^2$, und es gilt $x^2 - y^q = x^2 - (c^2-1)[(c^2-1)^{\frac{q-1}{2}}]^2 = 1$. Damit ist $(x, (c^2-1)^{\frac{q-1}{2}})$ eine Lösung der Gleichung $X^2 - (c^2-1)Y^2 = 1$, die die Størmer Eigenschaft bezüglich $(1, c^2-1)$ erfüllt, denn $(c^2-1)^{\frac{q-1}{2}}$ und c^2-1 besitzen dieselben Primteiler. Wegen $c^2 - (c^2-1) = 1$ ist $(c, 1)$ die Fundamentallösung der Gleichung und nach Satz 3.3.2 muss damit $(c^2-1)^{\frac{q-1}{2}} = 1$ gelten, was aber unmöglich ist. Somit gilt auch $q|x$.

□

Für den Beweis von Chein benötigen wir noch ein weiteres Lemma:

Lemma 3.3.5
Sei q eine ungerade Primzahl, $x, y \geq 1$ und $x^2 - y^q = 1$.
Dann gilt entweder

$$\begin{cases} x-1 &= 2a^q \\ x+1 &= 2^{q-1}a'^q \end{cases} \tag{3.13}$$

oder

$$\begin{cases} x+1 &= 2a^q \\ x-1 &= 2^{q-1}a'^q \end{cases} \tag{3.14}$$

mit a ungerade, $ggT(a, a') = 1$, und $y = 2aa'$.

Beweis. Es gilt $y^q = x^2 - 1 = (x+1)(x-1)$. Wenn x gerade ist, dann ist $ggT(x+1, x-1) = 1$ und somit gibt es $c, d \in \mathbb{Z}^+$ mit $x+1 = c^q$, $x-1 = d^q$. Subtraktion liefert $2 = c^q - d^q$, was unmöglich ist. Also muss x ungerade sein und $ggT(x+1, x-1) = 2$, woraus folgt

$$\begin{cases} x-1 &= 2^e c^q \\ x+1 &= 2^f d^q \end{cases}$$

mit c, d ungerade und teilerfremd, $e + f = rq\,(r \geq 1)$ und $\min\{e, f\} = 1$.
Aus $e = 1$ folgt $f = rq - 1 = q - 1 + (r-1)q$, was zur ersten Alternative (3.13) mit $a = c$, $a' = 2^{r-1}d$ führt.
Aus $f = 1$ folgt $e = rq - 1 = q - 1 + (r-1)q$, was zur zweiten Alternative (3.14) mit $a = d$, $a' = 2^{r-1}c$ führt. □

Nun können wir Cheins Beweis für den Satz von Chao Ko ausführen.

Satz 3.3.6 (Chao Ko)
Die Gleichung $X^2 - Y^n = 1$ mit $n > 3$ hat keine positive ganzzahlige Lösung.

Beweis. Für gerades n gibt es offensichtlich keine ganzzahlige Lösung. Aus Satz 3.1.2(ii) wissen wir, dass $x = 3, y = 2$ die einzige Lösung von $X^2 - Y^3 = 1$ ist, somit gibt es auch für den Fall dass n ein Vielfaches von 3 ist keine weitere ganzzahlige Lösung. Es genügt also zu zeigen, dass die Gleichung $X^2 - Y^q = 1$ für jede Primzahl $q > 3$ keine ganzzahlige Lösung hat.

Angenommen es gibt ganze Zahlen x, y mit $x^2 - 1 = y^q$. Aus Lemma 3.3.5 folgt die Existenz ganzer Zahlen $a, b > 0$ mit entweder

$$(I)\begin{cases} x+1 &= 2a^q \\ x-1 &= 2^{q-1}b^q \end{cases} \quad \text{oder} \quad (II)\begin{cases} x+1 &= 2^{q-1}b^q \\ x-1 &= 2a^q \end{cases}$$

wobei a ungerade, $ggT(a, b) = 1$ und $y = 2ab$ ist. Subtraktion und Division durch 2 liefert, je nach Fall

$$a^q - 2^{q-2}b^q = \pm 1$$

Es gilt

$$\left(\frac{x \mp 3}{2}\right)^2 = (a^q \mp 2)^2 = (a^2)^q \mp 2^2(a^q \mp 1) = (a^2)^q \mp (2b)^q.$$

Nach Satz 3.4.3 gilt $q | x$, da aber $q > 3$ gilt $q \nmid \frac{x \mp 3}{2}$, also $q \nmid \frac{(a^2)^q \mp (2b)^q}{a^2 \mp 2b}$, und mit Lemma 3.3.3 folgt

$$ggT\left(a^2 \mp 2b, \frac{(a^2)^q \mp (2b)^q}{a^2 \mp 2b}\right) = 1.$$

Daraus folgt, dass es eine ganze Zahl h geben muss, sodass $a^2 \mp 2b = h^2$ ist, wobei h ein Teiler von $\frac{x \mp 3}{2}$ sein muss. Da a ungerade ist, ist auch h ungerade und somit ist 4 ein Teiler von $a^2 - h^2 = \pm 2b$, also ist b gerade und es gilt

$$(a^2 \mp b)^2 = a^4 \mp 2a^2b + b^2 = a^2(a^2 \mp 2b) + b^2 = (ah)^2 + b^2.$$

Die ganzen Zahlen $ha, b, a^2 \mp b$ sind positiv, relativ prim und bilden eine Lösung der Pythagoräischen Gleichung $X^2 + Y^2 = Z^2$. Somit existieren ganze Zahlen $c, d \geq 1$ mit

$$\begin{cases} ha = c^2 - d^2 \\ b = 2cd \\ a^2 \mp b = c^2 + d^2 \end{cases}$$

Damit folgt $(c \pm d)^2 = c^2 + d^2 \pm 2cd = (a^2 \mp b) \pm b = a^2$.

- Im ersten Fall gilt

  $$b - a = 2cd - (c + d) = (c - 1)(d - 1) + (cd - 1) > 0$$

  also $a < b$. Aber es gilt auch $a^q = 2^{q-2}b^q + 1 > b^q$, also $a > b$, Widerspruch!

- Im zweiten Fall gilt

  $$b - a = 2cd - (c - d) = c(2d - 1) + d > 0$$

  also $a < b$. Aber $a^q = 2^{q-2}b^q - 1 > b^q$, also $a > b$, Widerspruch!

□

Das folgende Ergebnis wurde von Catalan 1885 ohne Beweis angegeben und bereits 1876 von Moret-Blanc bewiesen. Wir können es aus den bisher gezeigten Sätzen nun sehr leicht folgern.

Korollar 3.3.7
Seien $x, y \geq 2$ ganze Zahlen mit $x^y - y^x = 1$, dann muss $x = 3$ und $y = 2$ sein.

Beweis. Es können x und y weder beide gerade, noch beide ungerade sein, da in beiden Fällen $x^y - y^x$ gerade wäre.
Wenn x gerade ist, dann gilt $x = 2u$ und $x^y - (y^u)^2 = 1$ was einen Widerspruch zum Satz von Lebesgue (3.2.1) darstellt.
Wenn y gerade ist, dann gilt $y = 2v$ und $(x^v)^2 - y^x = 1$. Aus dem Satz von Chao Ko (3.3.6) folgt $x = 3$ und aus dem Satz von Euler (3.1.2) $y = 2$. □

3.4 Die Gleichungen $X^m - Y^3 = 1$ und $X^3 - Y^n = 1$, mit $m, n \geq 3$

Nagell konnte 1921 zeigen, dass die Gleichungen $X^m - Y^3 = 1$ ($m \geq 3$) und $X^3 - Y^n = 1$ ($n \geq 2$) keine ganzzahligen Lösungen besitzen. Dafür untersuchte er die Gleichungen

$$X^2 + X + 1 = Y^m \quad \text{und} \quad X^2 + X + 1 = 3Y^m$$

mit $m \geq 2$. Wir wollen hier nur Nagells Resultate anführen, für ausführliche Beweise sei abermals auf die [54] verwiesen.
Das erste Resultat wurde 1942 von Ljunggren für den Fall $m = 3$, der allerdings für die Anwendung des Ergebnisses auf das Catalan Problem nicht benötigt wird, erweitert.

Satz 3.4.1
Die ganzzahligen Lösungen x, y der Gleichung $X^2 + X + 1 = Y^m$ lauten:

(i) Falls m gerade ist: $(0, \pm 1), (-1, \pm 1)$.

(ii) Falls m ungerade ist und $m \neq 3$: $(0, 1), (-1, 1)$.

(iii) Falls $m = 3$: $(0, 1), (-1, 1), (18, 7), (-19, 7)$.

Beweis. Siehe [54] Satz A7.1. □

Satz 3.4.2
Die ganzzahligen Lösungen (x, y) der Gleichung $X^2 + X + 1 = 3Y^m$ lauten:

(i) Falls $m = 2$, so sind alle Lösungen gegeben durch (x_n, y_n), wobei

$$\begin{aligned} x_n &= \pm\frac{\sqrt{3}}{4}\left[(2+\sqrt{3})^{2n+1} - (2-\sqrt{3})^{2n+1}\right] - \frac{1}{2} \\ y_n &= \pm\frac{1}{4}\left[(2+\sqrt{3})^{2n+1} - (2-\sqrt{3})^{2n+1}\right] \end{aligned}$$

für $n \in \mathbb{N}$.

(ii) Falls $m \neq 2$ hat die Gleichung nur die Lösungen $(1, \pm 1), (-2, \pm 1)$ bei geradem m und $(1, 1), (-2, 1)$ bei ungeradem m.

Beweis. Siehe [54] Satz A7.2. □

Mit diesen Ergebnissen konnte Nagell zeigen:

Satz 3.4.3 (Nagell)
Für $m \geq 3$ haben die Gleichungen $X^m - Y^3 = \pm 1$ keine nichttrivialen ganzzahligen Lösungen.

Beweis. Wir dürfen wieder o.B.d.A. annehmen, dass $m = q$ eine Primzahl mit $q > 3$ ist. Seien $x, y \neq 0$ ganze Zahlen mit $x^3 \mp 1 = y^q$, dann ist $(x^2 \pm x + 1)(x \mp 1) = y^q$. Mit Lemma 3.3.3 folgt $ggT\left(\frac{x^3 \mp 1}{x \mp 1}, x \mp 1\right) = 1$ oder 3, und somit ist $x^2 \pm x + 1 = a^q$ oder $3a^q$.
Im Fall $x^2 - x + 1$ ersetzt man x durch $-x$ und erhält $x^2 + x + 1 = a^q$ oder $3a^q$.
Aus den beiden vorangegangenen Sätzen 3.4.1 und 3.4.2 folgt nun, dass $x = \pm 1$ oder -2 sein muss, dann ist aber $x^3 \mp 1$ keine q-te Potenz (für $q > 3$). □

Kapitel 4

Die Kriterien von Cassels und Mihailescu

Nach der Behandlung der Spezialfälle im letzten Kapitel wenden wir uns nun dem allgemeinen Fall der Catalan'schen Vermutung, also der Gleichung $x^p - y^q = 1$ mit ungeraden Primzahlexponenten p und q, zu.
In der zweiten Hälfte des 20. Jahrhunderts wurden mehrere verschiedene algebraische Kriterien für die Lösungen dieser Gleichung gefunden, zwei von ihnen spielen im Beweis von Mihailescu eine tragende Rolle. Es sind dies das von Cassels 1960 gefundene Teilbarkeitskriterium (Satz 4.1.1) und das sogenannte "Wieferich Kriterium" (Satz 4.2.1) von Mihailescu selbst aus dem Jahr 1999.

In diesem Kapitel beweisen wir diese zwei Kriterien und führen weiters als Folgerungen aus dem Ergebnis von Cassels Abschätzungen für die Größe der Lösungen an.

4.1 Das Ergebnis von Cassels

Cassels war der erste, der für den allgemeinen Fall der Catalan'schen Vermutung eine wichtige Aussage zeigen konnte. Die Bedeutung seines Resultats zeigt sich darin, dass die meisten weiterführenden Ergebnisse auf Cassels Aussagen aufbauen.
Konkret gelang es Cassels 1960 folgendes allgemeine Kriterium für Lösungen der Catalan'schen Gleichung zu beweisen:

Satz 4.1.1 (Cassels)
Seien p, q Primzahlen, mit $p > q$, und $x, y > 1$ ganze Zahlen die

$$x^p - y^q = \pm 1$$

erfüllen, dann gilt

$$p|y \quad \text{und} \quad q|x.$$

Hier sei angemerkt, dass die Voraussetzung $p > q$ keinerlei Einschränkung darstellt, da für eine Lösung (x, y, p, q) der Gleichung $x^p - y^q = \pm 1$ mit $p < q$ gilt, dass

$y^q - x^p = \mp 1$ ist und das Kriterium von Cassels somit ebenso gültig ist.[1]

Den Teil "$q|x$" hatte Cassels bereits 1953 in [11] beweisen können. Wir folgen in diesem Unterkapitel seinem Beweis von 1960 aus [12], der das frühere Ergebnis beinhaltet.

Zunächst zeigen wir einige Hilfssätze:

Lemma 4.1.2
Sei p eine Primzahl und $c \neq \mp 1$ eine ganze Zahl, dann gilt

$$ggT\left(\frac{c^p \pm 1}{c \pm 1}, c \pm 1\right) = 1 \text{ oder } p. \tag{4.1}$$

Falls der ggT gleich p ist, dann gilt

$$\frac{c^p \pm 1}{c \pm 1} \equiv p \,(\mathrm{mod}\, p^2). \tag{4.2}$$

Beweis. Die erste Aussage (4.1) folgt direkt aus Lemma 3.3.3.
Wir nehmen nun $p \mid c \pm 1$ an, es gibt also eine ganze Zahl $j > 0$ mit $c \pm 1 = p^j d$ und $ggT(p, d) = 1$. Dann gilt

$$\begin{aligned} \frac{c^p \pm 1}{c \pm 1} &= \frac{(p^j d \mp 1)^p \pm 1}{p^j d} = \frac{p^{j+1} d \mp \frac{p(p-1)}{2}(p^j d)^2 + \cdots}{p^j d} \\ &= p + p^{j+1}\left(\mp d\frac{p-1}{2} + \cdots\right) \equiv p \,(\mathrm{mod}\, p^{j+1}) \end{aligned} \tag{4.3}$$

woraus sofort (4.2) folgt. □

Korollar 4.1.3
Sei $c \pm 1 \neq 0$ und $p^j \mid c \pm 1$, dann gilt

$$\frac{c^p \pm 1}{c \pm 1} \begin{cases} \equiv & p \,(\mathrm{mod}\, p^{j+1}), \\ \neq & p. \end{cases}$$

Beweis. Einfache Folgerung aus Gleichung (4.3). □

Unter den Voraussetzungen von Satz 4.1.1 - $x^p - y^q = \pm 1$ mit $x, y > 1$ und $p > q$ - zeigen wir nun weiters

Lemma 4.1.4

$$q \mid y \pm 1$$

[1] In weiterer Folge betrachten wir meist nur die Gleichung $x^p - y^q = 1$ und lassen Lösungen mit $x, y \in \mathbb{Z} \setminus \{0\}$ zu um die Symmetrie, dass mit (x, y, p, q) auch $(-y, -x, q, p)$ eine Lösung dieser Gleichung ist, zu nützen und $p > q$ voraussetzen zu können.

Beweis. Angenommen $q \nmid y \pm 1$. Es gilt

$$x^p = y^q \pm 1 = (y \pm 1)\left(\frac{y^q \pm 1}{y \pm 1}\right)$$

Nach Lemma 4.1.2 gilt aufgrund unserer Annahme nun $ggT\left(y \pm 1, \frac{y^q \pm 1}{y \pm 1}\right) = 1$. Es gibt also eine ganze Zahl $u > 1$ mit

$$u^p = y \pm 1$$

Nun machen wir eine Fallunterscheidung:

- $x^p - y^q = 1$: Es gilt

  $$x^p = y^q + 1 = (u^p - 1)^q + 1 < u^{pq} \quad \text{also} \quad x \leq u^q - 1.$$

  Aus $p > q$ folgt

  $$x^p \leq (u^q - 1)^p < (u^p - 1)^q \leq y^q, \quad \text{Widerspruch zu } x^p = y^q + 1.$$

- $x^p - y^q = -1$: Analog erhält man $x \geq u^q + 1$, und weiters

  $$x^p \geq (u^q + 1)^p > (u^p + 1)^q \geq y^q, \quad \text{Widerspruch zu } x^p = y^q - 1.$$

□

Korollar 4.1.5
Unter den Voraussetzungen von Satz 4.1.1 gibt es ganze Zahlen u, v sodass

$$y \pm 1 = q^{p-1}u^p, \qquad \frac{y^q \pm 1}{y \pm 1} = qv^p, \tag{4.4}$$

wobei

$$v \equiv 1 \,(\mathrm{mod}\, q^{p-1}), \qquad v \neq 1. \tag{4.5}$$

Und weiters gilt

$$x \neq qu, \qquad x \equiv qu \,(\mathrm{mod}\, q^p). \tag{4.6}$$

Beweis. Die erste Aussage (4.4) folgt direkt aus den Lemmata 4.1.2 und 4.1.4.
Aus 4.1.3 folgt $v^p \neq 1$ und $qv^p \equiv q \,(\mathrm{mod}\, q^p)$ also $v^p \equiv 1 \,(\mathrm{mod}\, q^{p-1})$ und wegen $p > q$ gilt weiters $p \nmid \mathrm{ord}(\mathbb{Z}^\times_{q^{p-1}}) = \varphi(q^{p-1}) = (q-1)q^{p-2}$ woraus die zweite Aussage (4.5) folgt.
Es gilt $x^p = y^q \pm 1 = (y \pm 1)\left(\frac{y^q \pm 1}{y \pm 1}\right) = q^p u^p v^p$, also laut (4.4) $x = quv$, woraus sich mit (4.5) die dritte Aussage (4.6) ergibt. □

Nun können wir den Beweis von Cassels' Satz antreten.

Beweis von Satz 4.1.1. Der Fall $q = 2$ wurde bereits von Nagell, siehe Lemma 3.3.4, bewiesen, wir dürfen also davon ausgehen, dass $p > q \geq 3$ gilt.
Wegen $x^p = (y \pm 1)\left(\frac{y^q \pm 1}{y \pm 1}\right)$ folgt aus (4.4) unmittelbar $q|x$.

Es bleibt also noch $p \mid y$ zu zeigen. Dazu werden wir $p \nmid y$ annehmen und einen Widerspruch herleiten:

Angenommen $p \nmid y$, dann folgt aus Lemma 4.1.2 und $(x \mp 1)\frac{x^p \mp 1}{x \mp 1} = y^q$, dass $x \mp 1$ eine q-te Potenz ist, es gibt also ein ganzzahliges $z > 1$ mit

$$z^q = x \mp 1. \tag{4.7}$$

Die folgende Ungleichungskette

$$z^{pq} \geq \left(\frac{1}{2}x\right)^p \geq \left(\frac{1}{2}\right)^{p+1} y^q \geq \left(\frac{1}{2}\right)^{p+1} \left(\frac{1}{2}q^{p-1}u^p\right)^q \geq u^{pq}$$

liefert die grobe Abschätzung

$$z \geq u \tag{4.8}$$

Als nächstes zeigen wir

$$z^q \geq \frac{1}{2}q^p \tag{4.9}$$

Aus $x = z^q \pm 1$ und Korollar 4.1.5 folgt

$$|z^q \pm 1 - qu| \geq q^p.$$

Nehmen wir nun an (4.9) wäre falsch, es gelte also $z^q < \frac{1}{2}q^p$, dann folgt

$$|qu \mp 1| \geq \frac{1}{2}q^p,$$

was $u > 1$ impliziert und mit (4.8) folgt weiters $z^q \geq u^q \geq qu + 1^{\frac{p}{q}} \geq \frac{1}{2}q^p$, also gilt (4.9).

Laut Voraussetzung gilt $q \geq 3$ und $p \geq 5$, man kann sich leicht davon überzeugen, dass $1 - 2q^{-p} \geq 1 - 2 \cdot 3^{-p} > 3^{-\frac{1}{p}} \geq q^{-\frac{1}{p}}$. Daraus ergibt sich mit (4.7) und (4.9) die Abschätzung

$$\min(x^p, y^q) \geq (z^q - 1)^p \geq z^{pq}(1 - z^{-q})^p \geq z^{pq}(1 - 2q^{-p})^p > q^{-1}z^{pq}.$$

Es gilt $1 = |x^{\frac{p}{q}q} - y^q| = |x^{\frac{p}{q}} - y| \cdot |x^{\frac{p}{q}(q-1)} + \cdots + y^{q-1}|$ und mit der vorigen Abschätzung folgt

$$|x^{\frac{p}{q}} - y| = \frac{1}{|x^{\frac{p}{q}(q-1)} + \cdots + y^{q-1}|} \leq \frac{1}{q \cdot \min(x^{\frac{p}{q}(q-1)}, y^{q-1})} = \frac{1}{q \cdot \min(x^p, y^q)^{\frac{q-1}{q}}} < z^{-p(q-1)}. \tag{4.10}$$

Mit (4.7) und dem binomischen Lehrsatz folgt

$$x^{\frac{p}{q}} = (z^q \pm 1)^{\frac{p}{q}} = \sum_{r=0}^{\infty} \tau_r \tag{4.11}$$

wobei

$$\tau_r = (\pm 1)^r \frac{\frac{p}{q}(\frac{p}{q} - 1) \cdots (\frac{p}{q} - r + 1)}{r!} z^{p-rq} \tag{4.12}$$

Im Folgenden sei

$$R := \left\lfloor \frac{p}{q} \right\rfloor + 1 \quad \text{und weiters} \quad \rho := \left\lfloor \frac{R}{q-1} \right\rfloor .$$

Wir betrachten nun folgenden Ausdruck

$$z^{Rq-p} q^{R+\rho} \tau_r = z^{q(R-r)} q^{\rho} (\pm 1)^r \frac{p(p-q)\cdots(p-(r-1)q)}{r!} \tag{4.13}$$

Wie man leicht sehen kann gilt für alle Primzahlen $l \neq q$ dass $\nu_l(r!) \leq \nu_l(p(p-q)\cdots(p-(r-1)q))$ und für $r \leq R$ gilt $\nu_q(r!) = \sum_{k=1}^{\infty} \left\lfloor \frac{r}{q^k} \right\rfloor \leq \sum_{k=1}^{\infty} \frac{R}{q^k} = \frac{R}{q-1}$, also $\nu_q(r!) \leq \rho$. Damit ist gezeigt, dass (4.13) für $r \leq R$ ganzzahlig ist, und es folgt sofort, dass

$$I := z^{Rq-p} q^{R+\rho} \left((y - x^{\frac{p}{q}}) + \sum_{r>R} \tau_r \right)$$

ebenfalls eine ganze Zahl ist. Wir schreiben

$$I = I_1 + I_2 + I_3 \quad \text{wobei} \begin{cases} I_1 &= z^{Rq-p} q^{R+\rho} (y - x^{\frac{p}{q}}), \\ I_2 &= z^{Rq-p} q^{R+\rho} \tau_{R+1}, \\ I_3 &= z^{Rq-p} q^{R+\rho} \sum_{r>R+1} \tau_r. \end{cases} \tag{4.14}$$

Wir wollen zeigen, dass die Eigenschaft, dass I eine ganze Zahl ist, zu einem Widerspruch führt, da $I \neq 0$ aber gleichzeitig $|I| < 1$ gelten muss. Dazu benötigen wir aber zuerst noch ein paar Abschätzungen.

Zunächst folgt aus (4.9) für $r > R$:

$$\left| \frac{\tau_{r+1}}{\tau_r} \right| = \left| \frac{\frac{p}{q} - r}{r+1} z^{-q} \right| < z^{-q} \leq 2q^{-p} \leq 2p^{-q} \tag{4.15}$$

Als nächstes ergibt sich aus den beiden Ungleichungsketten

$$\left| \frac{p}{q} \left(\frac{p}{q} - 1 \right) \cdots \left(\frac{p}{q} - R \right) \right| \leq R(R-1)\cdots 2 \left| \left(\frac{p}{q} - R + 1 \right) \right| \left| \left(\frac{p}{q} - R \right) \right| \leq \frac{1}{4} R! \quad \text{und}$$

$$\left| \frac{p}{q} \left(\frac{p}{q} - 1 \right) \cdots \left(\frac{p}{q} - R \right) \right| \geq (R-1)(R-2)\cdots 1 \left| \left(\frac{p}{q} - R + 1 \right) \right| \left| \left(\frac{p}{q} - R \right) \right| \geq (R-1)! \frac{1}{q^2}$$

mit (4.12) die Abschätzung

$$\frac{1}{q^2(R+1)^2} \leq |z^{(R+1)q-p} \tau_{R+1}| \leq \frac{1}{4}. \tag{4.16}$$

Mit (4.15) folgt

$$\left| \frac{I_3}{I_2} \right| \leq \sum_{s=1}^{\infty} (2q^{-p})^s = \frac{2q^{-p}}{1-2q^{-p}} \leq \frac{2 \cdot 3^{-5}}{1 - 2 \cdot 3^{-5}} < \frac{1}{10}. \tag{4.17}$$

Mit

$$R+1-p=\left\lfloor\frac{p}{q}\right\rfloor+2-p\leq\left\lfloor\frac{5}{3}\right\rfloor+2-5=-2 \tag{4.18}$$

und (4.9) folgt aus (4.10) und der linken Seite von (4.16)

$$\left|\frac{I_1}{I_2}\right|\leq q^2(R+1)^2z^{(R+1-q)q}\leq q^2p^2(z^q)^{-2}\leq q^2p^2(\frac{1}{2}q^p)^{-2},$$

und damit

$$\left|\frac{I_1}{I_2}\right|\leq(2pq^{1-p})^2\leq(2\cdot5\cdot3^{1-5})^2\leq\frac{1}{10}. \tag{4.19}$$

Mit (4.14), (4.17) und (4.19) sieht man nun, dass $I\neq0$ sein muss, und da I ganzzahlig ist folgt somit

$$|I|\geq1. \tag{4.20}$$

Andererseits folgt aus der rechten Seite von (4.16) mit (4.9)

$$|I_2|\leq\frac{1}{4}z^{-q}q^{R+\rho}\leq\frac{1}{2}q^{R+\rho-p},$$

und damit folgt aus (4.14), (4.17) und (4.19) nun

$$|I|\leq\left(1+\frac{1}{10}+\frac{1}{10}\right)\frac{1}{2}q^{R+\rho-p}<q^{R+\rho-p}. \tag{4.21}$$

Laut (4.18) gilt $\rho=\left\lfloor\frac{R}{q-1}\right\rfloor\geq4$ und damit weiter

$$\left\lfloor\frac{p}{q}\right\rfloor+1=R\geq4(q-1),$$

und somit

$$p>q\left\lfloor\frac{p}{q}\right\rfloor\geq q(4q+5).$$

Daraus folgt nun

$$\begin{aligned}R+\rho&\leq R\left(1+\frac{1}{q-1}\right)\leq\left(\frac{p}{q}+2\right)\left(\frac{q}{q-1}\right)=\frac{p}{q-1}+\frac{2q}{q-1}\\&=\frac{p}{q-1}+\frac{2q(4q-5)}{(q-1)(4q-5)}<p\left(\frac{1}{1-q}+\frac{2}{(q-1)(4q-5)}\right)<p,\end{aligned}$$

also $R+\rho-p<0$ und mit (4.21) somit

$$|I|<1$$

was offensichtlich einen Widerspruch zu (4.20) darstellt.
Somit ist die ursprüngliche Annahme $p\nmid y$ falsifiziert, also gilt

$$p\mid y$$

□

Wir fassen die für den weiteren Verlauf wichtigen Ergebnisse noch einmal gesammelt zusammen:

Korollar 4.1.6
Seien x, y ganze Zahlen ungleich 0 und p, q ungerade Primzahlen, sodass $x^p - y^q = 1$, dann gilt

$$p|y \quad \text{und} \quad q|x,$$

und weiters gibt es von 0 verschiedene ganze Zahlen a, b und positiveganzeZahlen, u, v, sodass:

$$x - 1 = p^{q-1}a^q, \quad \frac{x^p - 1}{x - 1} = pu^q, \quad y = pau,$$
$$y + 1 = q^{p-1}b^p, \quad \frac{y^q + 1}{y + 1} = qv^p, \quad x = qbv,$$

mit $p \nmid u$ und $ggT(a, u) = 1$, sowie $q \nmid v$ und $ggT(b, v) = 1$.

Neben diesen Ergebnissen ergibt sich aus Cassels Satz noch eine weitere für uns relevante Konsequenz, die Möglichkeit untere Schranken für die Größe von x und y anzugeben.

So sieht man unmittelbar, dass nach Korollar 4.1.6 gelten muss:

$$|x| \geq p^{q-1} - 1$$

und

$$|y| \geq q^{p-1} - 1.$$

Für den Beweis der Catalan'schen Vermutung werden allerdings noch stärkere Abschätzungen benötigt. Hyyrö konnte unter der Verwendung des Ergebnisses von Cassels folgendes Resultat zeigen:

Satz 4.1.7 (Hyyrö)
Seien x, y ganze Zahlen ungleich 0 und p, q zwei verschiedene ungerade Primzahlen, mit $x^p - y^q = 1$, dann gilt

$$|x| \geq p^{q-1}(q-1)^q + 1.$$

Beweis. Wir verwenden Korollar 4.1.6 und nützen die folgende Gegebenheit: die Zahlen x, y, a, b sind entweder alle positiv, was wir als den "positiven Fall" bezeichnen, oder alle negativ, der "negative Fall".
Wegen $q|x$ gilt

$$p^{q-1}a^q = x - 1 \equiv -1 \,(\mathrm{mod}\, q).$$

Da $p^{q-1} \equiv 1 \,(\mathrm{mod}\, q)$ folgt daraus $a^q \equiv -1 \,(\mathrm{mod}\, q)$, also $a \equiv -1 \,(\mathrm{mod}\, q)$. Analog folgt $b \equiv 1 \,(\mathrm{mod}\, p)$.
Im positiven Fall gilt somit $a \geq q - 1$ und weiters $x \geq p^{q-1}(q+1)^q + 1$.
Im negativen Fall ist entweder $a \leq -q - 1$, woraus

$$|x| \geq p^{q-1}(q+1)^q - 1 \geq p^{q-1}(q-1)^q + 1$$

folgt, oder $a = -1$.

Es bleibt zu zeigen, dass dieser letzte Fall nicht auftreten kann. Wir nehmen also an, dass $a = -1$ wäre. Dann folgt $1 - x = 1 + |x| = p^{q-1}$. Da wir im negativen Fall sind haben wir $b \leq 1 - p$ und weiters

$$|y| = (|x|^p + 1)^{\frac{1}{q}} \leq (1 + |x|)^{\frac{p}{q}} < p^p < 2^{p-1}(p-1)^p < q^{p-1}|b|^p = |1 + y| < |y|,$$

Widerspruch! □

Damit können wir aus dem Satz von Cassels noch eine weitere Abschätzung folgern die wir an einem späteren Punkt benötigen:

Korollar 4.1.8
Für ganze Zahlen x, y ungleich 0 und verschiedene ungerade Primzahlen p, q, die $x^p - y^q = 1$ erfüllen, gilt

$$|x| \geq q^{p-1}.$$

Beweis. Falls $p \mid q-1$ dann folgt $p < q$ und es gilt $p^{q-1} \geq q^{p-1}$ Somit folgt die Aussage aus Satz 4.1.7.

Es gelte nun $p \nmid q-1$ und es sei v jene positive ganze Zahl aus Korollar 4.1.6 für die $\frac{y^q+1}{y+1} = qv^p$ gilt, dann haben wir

$$\begin{aligned} q(v^p-1) &= \frac{y^q+1}{y+1} - q \\ &= y^{q-1} - y^{q-2} + y^{q-3} - \cdots - y + 1 - q \\ &= y^{q-1} - 1 - y^{q-2} - 1 + y^{q-3} - 1 - \cdots - y - 1 + 1 - 1 \\ &= ((-y)^{q-1} - 1) + ((-y)^{q-2} - 1) + ((-y)^{q-3} - 1) + \cdots + (-y - 1). \end{aligned}$$

Da $y+1$ jedes $(-y)^i - 1$ teilt folgt also $y+1 \mid q(v^p-1)$. Sei nun b jene ganze Zahl aus Korollar 4.1.6 für die $y+1 = q^{p-1}b^p$ gilt, dann folgt weiters $q^{p-1}b^p \mid q(v^p-1)$. Es gilt also $q^{p-2} \mid v^p - 1$, oder anders $v^p \equiv 1 \pmod{q^{p-2}}$.

Die Ordnung der Gruppe $(\mathbb{Z}/q^{p-2}\mathbb{Z})^\times$ ist $\varphi(q^{p-2}) = q^{p-3}(q-1)$. Da nun p laut unserer Annahme diese Ordnung nicht teilt, gilt auch $v \equiv 1 \pmod{q^{p-2}}$, oder wieder anders geschrieben $q^{p-2} \mid v - 1$. Da der Fall $v = 1$ ausgeschlossen ist folgt damit $v \geq q^{p-2}$.

Laut Korollar 4.1.6 gilt außerdem $x = qvb$ und somit folgt $|x| \geq qv \geq q^{p-1}$. □

4.2 Mihailescus Wieferich Kriterium

Nachdem bereits Inkeri gezeigt hatte, dass für nichttriviale Lösungen (x, y, p, q) der Catalan'schen Gleichung $x^p - y^q = 1$ die Primzahlen p, q ein Wieferich Paar bilden, sofern nicht $p \mid h(\mathbb{Q}(\zeta_q))$ oder $q \mid h(\mathbb{Q}(\zeta_p))$, und Mignotte und Schwarz die Kriterien für die Teilbarkeit der Klassenzahlen jeweils noch weiterentwickeln konnte, gelang es Mihailescu 1999 (siehe [48]) schließlich alle Voraussetzungen an die Klassenzahlen aus diesen Kriterien zu beseitigen und die Wieferich Bedingung uneingeschränkt zu zeigen.

Mit anderen Worten, Mihailescu bewies folgenden Satz:

Satz 4.2.1 (Mihailescus Wieferich Kriterium)
Sei (x, y, p, q) eine nichttriviale Lösung der Catalan'schen Gleichung $x^p - y^q = 1$ mit ungeraden Primzahlen p, q, dann gilt

$$p^{q-1} \equiv 1 \pmod{q^2} \quad \text{und} \quad q^{p-1} \equiv 1 \pmod{p^2}.$$

Um diesen Satz zu beweisen betrachten wir den p-ten Kreisteilungskörper $\mathbb{Q}(\zeta_p)$. Um die Notation etwas abzukürzen sei im Folgenden stets $\zeta := \zeta_p$ und $G := Gal(\mathbb{Q}(\zeta)|\mathbb{Q})$. Mit σ_c bezeichnen wir dann jenes Element von G, für das $\zeta^{\sigma_c} = \zeta^c$ ist.

Wir rufen in Erinnerung, dass p in K die Faktorisierung $p = \prod_{i=1}^{p-1}(1-\zeta^i)$ besitzt und da alle $\frac{1-\zeta^i}{1-\zeta}$ Einheiten sind und für die Ideale gilt somit $(p) = (1-\zeta)^{p-1}$. Weiters ist p die einzige verzweigte Primzahl, alle anderen, insbesondere q, lassen sich eindeutig als Produkt verschiedener Primideale darstellen.

Der wesentliche Punkt in Mihailescus Beweis ist die Anwendung des Satzes von Stickelberger. Sei $\theta := \sum_{a=1}^{p-1} \left\{\frac{a}{p}\right\} {\sigma_a}^{-1}$ das Stickelbergerelement, dann wissen wir dass das Stickelbergerideal I_S erzeugt wird von den Elementen der Form $(n-\sigma_n)\theta$ (Lemma 2.10.1). Also von

$$\Theta_n := \sum_{a=1}^{p-1}(n-\sigma_n)\left\{\frac{a}{p}\right\}{\sigma_a}^{-1} = \sum_{a=1}^{p-1}\left(n\left\{\frac{a}{p}\right\} - \left\{\frac{na}{p}\right\}\right){\sigma_a}^{-1} = \sum_{a=1}^{p-1}\left\lfloor\frac{na}{p}\right\rfloor{\sigma_a}^{-1}, \tag{4.22}$$

und speziell gilt $\Theta_2 = \sum_{a=\frac{p+1}{2}}^{p-1} {\sigma_a}^{-1}$.

Bevor wir den Beweis beginnen benötigen wir noch zwei allgemeine Lemmata.

Lemma 4.2.2
Sei L ein Zahlkörper und Q ein Primideal von O_L, dessen Norm eine Potenz der Primzahl q ist, und seien weiters $\alpha, \beta \in O_L$ mit $\alpha^q \equiv \beta^q \pmod{Q}$, dann gilt auch $\alpha^q \equiv \beta^q \pmod{Q^2}$.

Beweis. Sei also $\mathrm{N}(Q) = q^r$, dann folgt $z^{q^r} \equiv z \pmod{Q}$ für alle $z \in O_L$. Erhebt man nun die Kongruenz $\alpha^q \equiv \beta^q \pmod{Q}$ zur q^{r-1}-ten Potenz, so erhält man $\alpha \equiv \alpha^{q^r} \equiv \beta^{q^r} \equiv \beta \pmod{Q}$.
Sei nun $\gamma = \alpha - \beta$, dann ist $\gamma \in Q$ und wir haben

$$\alpha^q - \beta^q = (\beta-\gamma)^q - \beta^q = \sum_{j=1}^{q}\binom{q}{j}\gamma^j\beta^{q-j} \equiv 0 \pmod{(q\gamma, \gamma^q)}.$$

Da aber $q\gamma \in Q^2$ und $\gamma^q \in Q^2$ gilt $Q^2 \mid (q\gamma, \gamma^q)$ und es folgt $\alpha^q \equiv \beta^q \pmod{Q^2}$. □

Lemma 4.2.3
Sei L ein Zahlkörper und α eine ganzalgebraische Zahl, deren Konjugierte alle Absolutbetrag 1 haben, dann ist α eine Einheitswurzel.

Beweis. Nach Satz 2.4.9 besitzt das charakteristische Polynom von α die Zerlegung $f_\alpha(x) = \prod_{i=1}^{n}(x - \sigma_i(\alpha))$, wobei n der Grad der Erweiterung $L|\mathbb{Q}$ ist. Da alle $\sigma_i(\alpha)$ Absolutbetrag 1 haben sind die Koeffizienten der charakteristischen Polynome, und damit auch der Minimalpolynome, aller Potenzen von α durch einen Wert, der allein von n abhängt, beschränkt. Da diese Koeffizienten rationale Zahlen sind, gibt es also nur endlich viele irreduzible Polynome, die als Minimalpolynom für eine Potenz von α in Frage kommen. Folglich hat α nur endlich viele verschiedene Potenzen und ist daher eine Einheitswurzel. □

Mihailescu zeigt nun folgende Aussage, aus der das Wieferich Kriterium dann einfach folgt:

Satz 4.2.4
Sei (x, y, p, q) eine nichttriviale Lösung der Catalan'schen Gleichung $x^p - y^q = 1$ mit ungeraden Primzahlen p, q, dann gilt

$$q^2|x \quad \text{und} \quad p^2|y.$$

Wir formulieren den ersten Beweisschritt in einem eigenem Lemma, da wir die Aussage in den Kapiteln 5 und 6 in anderen Beweisen wiederverwenden werden.

Lemma 4.2.5
Unter den obigen Voraussetzungen ist $\beta_i := \frac{x-\zeta^i}{1-\zeta^i}$ eine ganzalgebraische Zahl, für $i = 1, \ldots, p-1$.
Die Hauptideale (β_i) sind jeweils q-te Potenz eines Ideals von O_K.

Beweis. Aus dem Ergebnis von Cassels (Korollar 4.1.6) folgt $x \equiv 1 \,(\mathrm{mod}\, p)$ und damit $x - \zeta^i \equiv 1 - \zeta^i \equiv 0 \,(\mathrm{mod}\, (1-\zeta^i))$. Somit ist jedes $\beta_i := \frac{x-\zeta^i}{1-\zeta^i}$ ganzalgebraisch.

Es gilt $(1-\zeta^i)\beta_i - (1-\zeta^j)\beta_j = \zeta^j - \zeta^i$, und da als Ideale betrachtet $(1-\zeta^i) = (1-\zeta^j) = (\zeta^j - \zeta^i) = (1-\zeta)$ gilt, folgt daraus $ggT(\beta_i, \beta_j) = 1$ für $i \neq j$.
Nach Cassels (Korollar 4.1.6) gilt weiters $\prod_{i=1}^{p-1} \beta_i = \frac{(x^p-1)}{p(x-1)} = u^q$ und wegen der Teilerfremdheit der Ideale (β_i) folgt, dass es für jedes β_i ein Ideal U_i von O_K gibt, sodass $(\beta_i) = {U_i}^q$. □

Beweis von Satz 4.2.4. Wir wenden den Satz von Stickelberger an und erhalten für ein beliebiges $\Theta \in I_S$ ein $\alpha \in O_K$, sodass $(\beta_1)^\Theta = (\alpha)^q$, wobei $(\alpha) = {U_1}^\Theta$ ist, mit den Notationen von Lemma 4.2.5. Wir können weiters schreiben:

$$\left(\frac{1-\zeta^{-1}x}{1-\zeta^{-1}}\right)^\Theta = \left(\frac{x-\zeta}{1-\zeta}\right)^\Theta = \varepsilon\alpha^q, \tag{4.23}$$

wobei ε eine Einheit von O_K ist. Es ist $\frac{\overline{\varepsilon}}{\varepsilon} \in O_K$ und alle Konjugierten von $\frac{\overline{\varepsilon}}{\varepsilon}$ haben Absolutbetrag 1. Nach Lemma 4.2.3 ist $\frac{\overline{\varepsilon}}{\varepsilon}$ somit eine Einheitswurzel.

Sei nun $\lambda := (1-\zeta^{-1})^\Theta$, dann ist $\frac{\lambda}{\overline{\lambda}}$ eine Einheitswurzel, da jeder Faktor von $\frac{\lambda}{\overline{\lambda}}$ von der Form $\frac{1-\zeta^i}{1-\overline{\zeta}^i}$ ist und damit laut Lemma 4.2.3 eine Einheitswurzel. Die Einheitswurzeln in K sind genau die $2p$-ten Einheitswurzeln, und wegen $ggT(2p, q) = 1$ ist jede eine q-te Potenz. Somit existiert also in O_K eine $2p$-te Einheitswurzel δ sodass $\overline{\lambda}\overline{\varepsilon} = \lambda\varepsilon\delta^q$ ist.

Wir multiplizieren nun die Gleichung (4.23) mit λ und ziehen von jeder Seite ihr komplex Konjugiertes ab und erhalten:

$$(1-\zeta^{-1}x)^\Theta - (1-\zeta x)^\Theta = \lambda\varepsilon\alpha^q - \overline{\lambda\varepsilon\alpha^q} = \lambda\varepsilon(\alpha^q - (\overline{\alpha}\delta)^q). \tag{4.24}$$

Aus $q|x$ folgt, dass die linke Seite von (4.24) $1 - 1 \equiv 0 \,(\mathrm{mod}\, q)$ ist.

Sei Q ein Primideal von O_K, das q teilt. Da (λ) eine Potenz von $(1-\zeta)$, und somit teilerfremd zu Q, und ε eine Einheit ist folgt aus (4.24), dass $Q \mid (\alpha^q - (\overline{\alpha}\delta)^q)$ und mit Lemma 4.2.2 auch $Q^2 \mid (\alpha^q - (\overline{\alpha}\delta)^q)$.

Sei Θ nun wie folgt dargestellt $\Theta = \sum_{i=1}^{p-1} a_i\sigma_i$ mit $a_i \in \mathbb{Z}$ (man beachte die Umordnung im Vergleich zu (4.22)), dann gilt

$$(1 - x\zeta)^{\Theta} = \prod_{i=1}^{p-1}(1 - x\zeta^i)^{a_i} \equiv 1 - x\sum_{i=1}^{p-1} a_i\zeta^i \,(\mathrm{mod}\, x^2)$$

Wir wissen, dass $Q|x$, und wenn wir die obige Kongruenz in (4.24) einsetzen erhalten wir

$$x\sum_{i=1}^{p-1}(a_i - a_{p-i})\zeta^i \equiv 0 \,(\mathrm{mod}\, Q^2).$$

Es gilt also entweder $Q^2|x$ oder $\sum_{i=1}^{p-1}(a_i - a_{p-i})\zeta^i \equiv 0 \,(\mathrm{mod}\, Q)$. Angenommen es gilt Zweiteres für alle Primidealteiler Q von q, dann müsste q für jedes i $(1 \leq i \leq p-1)$ gelten $q \mid a_i - a_{p-i}$. Ist jedoch $\Theta = \Theta_2$ aus (4.22), dann gilt $a_1 = 1, a_{p-1} = 0$ und q müsste ihre Differenz teilen: $q|1$, Widerspruch!

Es gilt also $Q^2|x$ für zumindest einen Primidealteiler Q von q. Sei Q' ein weiterer Primidealteiler von q, dann existiert ein $\sigma \in G$ mit $\sigma(Q) = Q'$ und somit folgt $\sigma(Q^2) = Q'^2 \mid x$, und somit gilt $q^2|x$.

Die Aussage $p^2|y$ kann analog, durch einen symmetrischen Beweis gezeigt werden. □

Damit können wir nun Mihailescus Wieferich Kriterium einfach beweisen:

Beweis von Satz 4.2.1. Laut Korollar 4.1.6 gilt $x - 1 = p^{q-1}a^q$ und mit $q^2|x$ folgt $p^{q-1}a^q \equiv -1 \,(\mathrm{mod}\, q^2)$. Wegen $p^{q-1} \equiv 1 \,(\mathrm{mod}\, q)$ folgt $a^q \equiv -1 \,(\mathrm{mod}\, q)$ und mit Lemma 4.2.2 auch $a^q \equiv -1 \,(\mathrm{mod}\, q^2)$. Insgesamt ergibt sich damit $p^{q-1} \equiv -p^{q-1}a^q \equiv 1 \,(\mathrm{mod}\, q^2)$.

Die Aussage $q^{p-1} \equiv 1 \,(\mathrm{mod}\, p^2)$ folgt, wie oben, analog. □

Kapitel 5

Mihailescus Beweis der Catalan'schen Vermutung

Wir beschäftigen uns in diesem Kapitel mit Mihailescus Beweis für die Catalan'sche Vermutung aus dem Jahr 2002 [49] und konzentrieren uns dabei auf den Fall $p \nmid q-1$ und $q \nmid p-1$. Auf den Fall $p \mid q-1$ oder $q \mid p-1$ gehen wir hier zunächst nur kurz ein, da wir in Kapitel 6 einen neueren Beweis für diesen Fall wiedergeben, der nicht auf Erkenntnissen aus der Theorie der Linearformen von Logarithmen und dem Ergebnis von Tijdeman [61] beruht und auch keine computerunterstützten Berechnungen mehr benötigt.

Mihailescus Beweis wurde von Yuri F. Bilu in [7] überarbeitet und vereinfacht. Unabhängig von Bilu überarbeitete auch Rene Schopf Mihailescus Beweis, seine Version wird in [18] und [17] wiedergegeben. Wir halten uns im Folgenden größtenteils an Bilus Version, in Unterkapitel 5.5 folgen wir Schools Argumentation.

5.1 Der Fall $p \mid q-1$ oder $q \mid p-1$

Um den Fall $q \mid p-1$, und damit aus Symmetriegründen auch $p \mid q-1$, auszuschließen folgt Mihailescu Tijdemans Argumentation und wendet ein neueres Ergebnis über Linearformen von Logarithmen aus [37] an um zu zeigen dass

Satz 5.1.1
Für Lösungen der Catalan'schen Gleichung $x^p - y^q = 1$ gilt

$$\text{Falls} \quad q > 10^5, \quad \text{dann folgt} \quad p < q^2 \tag{5.1}$$

Beweis. Siehe [49], Appendix B. □

Nun beruft sich Mihailescu auf computergestützte Berechnungen, wie jene von Mignotte und Roy in [47], die zeigen, dass

$$\min\{p, q\} \geq 10^5. \tag{5.2}$$

Würde nun für eine Lösung der Catalan'schen Gleichung $q \mid p-1$, also $p \equiv 1 \pmod{q}$ gelten, dann folgt aus Mihailescus Wieferich Kriterium (Satz 4.2.1), wonach $p^{q-1} \equiv$

$1 \pmod{q^2}$, dass

$$p \equiv 1 \pmod{q^2},$$

was im Widerspruch zu (5.1) steht, da $p \geq 3$ ist. Somit muss $q \mid p-1$, und wegen der Symmetrie auch $p \mid q-1$, gelten.

Für weitere Details verweisen wir auf [49] Appendix B oder [7] Kapitel 4. Eine sehr ausführliche Zusammenfassung dieses analytischen Teils von Mihailescus Beweis und Tijdemans Arbeit findet sich in [65].

5.2 Notationen und Vorarbeiten

In diesem Unterkapitel halten wir zunächst einige Notationen für dieses Kapitel fest und sammeln danach in einigen Hilfssätzen generelle Informationen und Erkenntnisse, die wir im weiteren Verlauf des Beweises verwenden werden.

Wir bezeichnen in diesem Kapitel mit $K := \mathbb{Q}(\zeta)$ den p-ten Kreisteilungskörper, wobei p eine ungerade Primzahl sei und wir mit ζ die primitive p-te Einheitswurzel $\zeta := \mathrm{e}^{\frac{2\pi i}{p}}$ bezeichnen. Die Galoisgruppe von K bezeichnen wir mit $G := Gal(\mathbb{Q}(\zeta)|\mathbb{Q})$. Es ist dann $G = \{\sigma_a \mid 1 \leq a \leq p-1\}$, wobei σ_a jenes Element von G sei, für das $\zeta^{\sigma_a} = \zeta^a$ gilt. Für uns von Interesse sind speziell $\sigma_1 = 1$, die Identität, und $\sigma_{p-1} =: \iota$ die komplexe Konjugation.

In diesem Kapitel sei q stets eine von p verschiedene ungerade Primzahl, die $q \nmid p-1$ erfüllt.

Man kann die Elemente des Gruppenrings $\mathbb{Z}[G]$ auf Elemente beziehungsweise Ideale von K wirken lassen und damit beispielsweise $K^\times$ aber auch die Gruppe der Ideale und alle Unter- und Faktorgruppen dieser Gruppen als $\mathbb{Z}[G]$-Moduln auffassen. Wir betrachten daher zunächst den Gruppenring $\mathbb{Z}[G]$ beziehungsweise allgemeine Gruppenringe genauer und definieren:

Definition 56
*Sei R ein kommutativer Ring und H eine endliche abelsche Gruppe, dann heißt $\omega(\Theta)$ das **Gewicht** von Θ, wobei die Gewichtsfunktion ω wie folgt definiert ist:*

$$\omega : R[H] \to R, \Theta \mapsto \omega(\Theta) := \sum_{\sigma \in H} m_\sigma.$$

Die Gewichtsfunktion ist additiv und multiplikativ und definiert somit einen Ringhomomorphismus von $R[H]$ nach R. Der Kern der Gewichtsfunktion ist somit ein Ideal:

Definition 57
*Den Kern der Gewichtsfunktion nennt man **Augmentationsideal**.*

Das Augmentationsideal enthält also alle Elemente vom Gewicht 0. Es wird über R von den Elementen der Form $\sigma - \tau$, mit $\sigma, \tau \in H$, erzeugt.

Wir betrachten nun den speziellen Gruppenring $\mathbb{Z}[G]$. Jeder $\mathbb{Z}[G]$-Modul, der von q annulliert wird, ist auch ein $\mathbb{F}_q[G]$-Modul. Wir halten für diese Moduln folgende Definitionen fest:

Definition 58
*Ein Element Θ aus $\mathbb{Z}[G]$ oder $\mathbb{F}_q[G]$ nennt man **gerade**, wenn es durch $1+\iota$ teilbar ist.*
*$\Theta = \sum_{\sigma\in G} n_\sigma \sigma \in \mathbb{Z}[G]$ heißt **nichtnegativ**, wenn $n_\sigma \geq 0$ für alle $\sigma \in G$, und weiters heißt Θ **positiv**, wenn es nichtnegativ und ungleich 0 ist.*

Den Grund warum wir in weiten Teilen des Beweises mit $\mathbb{F}_q[G]$ anstelle von $\mathbb{Z}[G]$ arbeiten liefert folgender Satz, den wir allgemein formulieren:

Satz 5.2.1
Sei H eine endliche zyklische Gruppe der Ordnung n und L ein Körper dessen Charakteristik n nicht teilt. Dann lässt sich der Gruppenring $L[H]$ darstellen als direktes Produkt endlich vieler Körper.

Beweis. Sei ρ das erzeugende Element der zyklischen Gruppe H, dann gilt $\rho^n = 1$. Die Elemente von $L[H]$ sind also alle von der Form $\sum_{i=0}^{n-1} m_\rho \rho^i$. Somit liefert die Zuordnung $\rho \mapsto X$ einen Isomorphismus $L[H]\widetilde{\to}L[X]/(X^n-1)$.
Das Polynom X^n-1 ist separabel im algebraischen Abschluss $\overline{L}$, da seine Ableitung gleich nX^{n-1} ist und somit ungleich 0, da n die Charakteristik von L nicht teilt. Sei $X^n-1 = \prod_i g_i(X)$ die Zerlegung von X^n-1 in irreduzible Polynome über $L[X]$. Da X^n-1 separabel ist sind alle $g_i(X)$ verschieden und somit teilerfremd. Der chinesische Restsatz besagt nun, dass $L[X]/(X^n-1) \cong \prod_i L[X]/(g_i(X))$ und da jedes $g_i(X)$ irreduzibel ist, ist $L[X]/(g_i(X))$ ein Körper. Genauer gesagt sind die $L[X]/(g_i(X))$ endliche Körpererweiterungen von L. □

Die Galoisgruppe G ist eine zyklische Gruppe der Ordnung $p-1$, aufgrund der Voraussetzung $q \nmid p-1$ lässt sich der Gruppenring $\mathbb{F}_q[G]$ also als direktes Produkt endlich vieler Körper darstellen. Diese sind endliche Körpererweiterungen von $\mathbb{F}_q$ und somit selbst endliche Körper.

Diese Darstellung ist für uns von Vorteil, da ein direktes Produkt von Körpern einige nützliche Eigenschaften besitzt, die wir in den nächsten beiden Lemmata zusammenfassen:

Lemma 5.2.2
Sei $R := \prod_{\alpha\in A} K_\alpha$ ein direktes Produkt von Körpern K_α, dann hat R die folgenden Eigenschaften:

(i) Für $B \subseteq A$ ist die Menge $I(B) := \{(x_\alpha)_{\alpha\in A} \mid x_\alpha = 0, \forall \alpha \in B\}$ ein Ideal von R, und alle Ideale von R sind von dieser Gestalt.
Speziell ist jeder Faktorring von R selbst ein direktes Produkt von Körpern.

(ii) Für je zwei Ideale $I, I' \trianglelefteq R$ gilt $II' = I \cap I'$. Weiters existieren für jedes $b \in II'$ ein $a \in I$ und ein $a' \in I'$ sodass $aa' = b$ gilt.
Speziell ist $I^2 = I$ und für jedes $a \in I$ existieren $a_1, a_2 \in I$ mit $a_1 a_2 = a$.

(iii) Für jedes Ideal $I \trianglelefteq R$ gibt es ein eindeutig bestimmtes Ideal $I^\perp \trianglelefteq R$ sodass

$$II^\perp = (0) \quad \text{und} \quad I + I^\perp = R.$$

(iv) Für je zwei Ideale $I, I' \trianglelefteq R$ gilt

$$(II')^\perp = I^\perp + I'^\perp \quad \text{und} \quad (I + I')^\perp = I^\perp I'^\perp.$$

Weiters gilt $II' = (0)$ genau dann wenn $I' \subseteq I^\perp$.

Beweis.

(i): Die Mengen $I(B)$ erfüllen die Eigenschaft $yI(B) \subseteq I(B)$ für alle $y \in R$ und sind somit Ideale. Wir müssen noch zeigen, dass alle Ideale von dieser Gestalt sind. Mit $\mathbf{1}_\beta$ bezeichnen wir jenes Element $(x_\alpha)_{\alpha\in A}$ für das $x_\beta = 1$ und $x_\alpha = 0$ für $\alpha \neq \beta$.
Sei nun I ein beliebiges Ideal von R, dann definieren wir eine Teilindexmenge $C := \{\beta \in A \mid \exists (x_\alpha)_{\alpha\in A} \in I \text{ mit } x_\beta \neq 0\}$. Für ein $\gamma \in C$ sei nun $y = (y_\alpha)_{\alpha\in A}$ ein Element von I mit $y_\gamma \neq 0$. Aufgrund der Idealeigenschaft folgt dann, dass $\mathbf{1}_\gamma Ry \subseteq I$, und da K_γ ein Körper ist das Produkt $\mathbf{1}_\gamma Ry = \mathbf{1}_\gamma R$. Dies gilt für alle $\gamma \in C$ und somit folgt $\bigcup_{\gamma\in C} \mathbf{1}_\gamma R = I(A \setminus C) \subseteq I$ und da $x_\beta = 0$ für $\beta \in A \setminus C$ für alle Elemente von I gilt, folgt $I(A \setminus C) = I$.

(ii): Punkt (ii) folgt direkt aus (i).

(iii): Sei I das Ideal $I(B)$, dann definieren wir $I^\perp := I(A \setminus B)$, dann gilt $II^\perp = (0)$ und $I + I^\perp = R$. Sei nun $\tilde{I}$ ein Ideal, dass ebenfalls diese Bedingungen erfüllt, dann folgt aus $I\tilde{I} = (0)$ dass $\tilde{I} \subseteq I^\perp$ und aus $I + \tilde{I} = R$ folgt $I^\perp \subseteq \tilde{I}$ und somit $\tilde{I} = I^\perp$.

(iv): Punkt (iv) folgt direkt aus (iii).

□

Moduln über direkten Produkten von Körpern haben folgende Eigenschaften:

Lemma 5.2.3
Sei wieder $R := \prod_{\alpha\in A} K_\alpha$ ein direktes Produkt von Körpern.

(i) Sei M ein zyklischer R-Modul und M' ein Untermodul, dann gilt

$$\mathrm{ann}_R(M') + \mathrm{ann}_R(M/M') = R \quad \text{und} \quad \mathrm{ann}_R(M')\mathrm{ann}_R(M/M') = \mathrm{ann}_R(M).$$

(ii) Sei M ein R-Modul, dann existiert ein $a \in M$ mit $\mathrm{ann}_R(a) = \mathrm{ann}_R(M)$. Oder anders ausgedrückt, M hat einen Untermodul, der isomorph zu $R/\mathrm{ann}_R(M)$ ist.
Für endliche R gilt dann $|M| \geq |R/\mathrm{ann}_R(M)|$, mit "=" genau dann, wenn M zyklisch ist.

Beweis.

(i): Nach 5.2.2(i) existieren Teilmengen $B, B' \subseteq A$ mit $I(B) = \mathrm{ann}_R(M)$ und $I(B') = \mathrm{ann}_R(M')$, und es gilt $B' \subseteq B$. Da M zyklisch ist gilt $M \cong R/I(B) \cong I(A \setminus B)$. Das Bild von M' unter diesem Isomorphismus ist $I(A \setminus B')$. Somit ist $\mathrm{ann}_R(M/M') = I(B \setminus B')$ und es folgt $\mathrm{ann}_R(M') + \mathrm{ann}_R(M/M') = I(B') + I(B \setminus B') = R$ und $\mathrm{ann}_R(M')\mathrm{ann}_R(M/M') = I(B')I(B \setminus B') = I(B) = \mathrm{ann}_R(M)$.

(ii): Wir schreiben kurz $I(\beta)$ für $I(\{\beta\})$ und definieren das Element $\mathbf{1}_\beta$ wie im Beweis von Lemma 5.2.2. Wir halten fest, dass es für jedes $x \in R \setminus I(\beta)$ ein $y \in R$ gibt mit $yx = \mathbf{1}_\beta$.
Sei wieder $B \subseteq A$ sodass $\mathrm{ann}_R(M) = I(B)$. Wir zeigen zunächst, dass für jedes $\beta \in B$ ein $b_\beta \in M$ existiert, mit $\mathrm{ann}_R(b_\beta) \subseteq I(\beta)$. Angenommen für jedes $b \in M$ existiere ein $x \in R \setminus I(\beta)$ mit $xb = 0$, dann folgt aber mit dem y von vorhin, dass $yxb = \mathbf{1}_\beta b = 0$ für alle $b \in M$, was ein Widerspruch ist, da $\mathbf{1}_\beta \notin \mathrm{ann}_R(M) = I(B)$.
Wir definieren nun $a := \sum_{\beta \in B} \mathbf{1}_\beta b_\beta$ mit diesen b_β. Sei nun $x = (x_\alpha)_{\alpha \in A}$, dann gilt für jedes $\beta \in B$ dass $0 = \mathbf{1}_\beta xa = 1_\beta x b_\beta$. Also $1_\beta x \in I(\beta)$ wegen der Wahl der b_β und somit $x_\beta = 0$ für alle $\beta \in B$, also $x \in I(B)$.

□

Definition 59
Sei I ein Ideal eines kommutativen Ringes R mit Einselement, man nennt I ein ***radikales Ideal****, falls R/I keine nilpotenten*[1] *Elemente ungleich 0 enthält.*

Für den Gruppenring $\mathbb{Z}[G]$ ergibt sich nun sofort folgende Konsequenz:

Lemma 5.2.4
Ein Ideal des Gruppenrings $\mathbb{Z}[G]$ das eine Primzahl enthält, die die Ordnung von G nicht teilt, ist ein radikales Ideal.

Beweis. Sei I ein Ideal von $\mathbb{Z}[G]$ das die Primzahl q enthält, die die Ordnung von G nicht teilt. Dann gilt $\mathbb{Z}[G]/I = \mathbb{F}_q[G]/I'$, wobei I' das Bild von I in $\mathbb{F}_q[G]$ ist. Aus Lemma 5.2.1 folgt, dass $\mathbb{F}_q[G]$ ein direktes Produkt von Körpern ist, und laut Lemma 5.2.2 (i) ist damit auch $\mathbb{F}_q[G]/I'$ ein direktes Produkt von Körpern. Somit enthält $\mathbb{Z}[G]/I$ keine nilpotenten Elemente ungleich 0. □

Nun zeigen wir noch, wie man von dem Annullator über $\mathbb{Z}[G]$ auf jenen über $\mathbb{F}_q[G]$ schließen kann:

Lemma 5.2.5
Sei R ein kommutativer Ring mit 1 und M ein endlich erzeugter R-Modul. Für ein Ideal I, für das $I + \mathrm{ann}_R(M)$ ein radikales Ideal von R ist, gilt dann dass der Annullator $\mathrm{ann}_{R/I}(M/IM)$ das Bild von $\mathrm{ann}_R(M)$ in R/I ist.

Beweis. Wir müssen zeigen, dass für alle $\alpha \in R$ gilt

$$\alpha M \subseteq IM \iff \alpha \in I + \mathrm{ann}_R(M).$$

Für $\alpha \in I + \mathrm{ann}_R(M)$ gilt trivialerweise $\alpha M \subseteq IM$, es bleibt also noch die Richtung "$\Rightarrow$" zu zeigen. Sei dazu ϕ ein R-Modulendomorphismus von M mit $\phi(M) \subseteq IM$, dann erfüllt ϕ laut [1] Proposition 2.4 eine Gleichung der Form $\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0$, mit $a_1, \ldots, a_n \in I$. Aufgrund der Voraussetzung $\alpha M \subseteq IM$ können wir nun ϕ gleich der Multiplikation mit α setzen und erhalten so $\alpha^n + a_1\alpha^{n-1} + \cdots + a_n \in \mathrm{ann}_R(M)$, also $\alpha^n \in I + \mathrm{ann}_R(M)$. Da dieses Ideal radikal ist folgt daraus, dass $\alpha \in I + \mathrm{ann}_R(M)$. □

[1] Ein Element r eines Ringes nennt man nilpotent, falls es eine natürliche Zahl n gibt, sodass $r^n = 0$ ist.

5.3 Wichtige Annullatoren

In diesem Unterkapitel definieren und untersuchen wir einige $\mathbb{F}_q[G]$-Moduln und ihre Annullatoren, die eine wichtige Rolle in Mihailescus Beweis spielen. Danach geben wir einen kurzen Überblick über den weiteren Verlauf des Beweises.

Zunächst definieren wir:

Definition 60
Das ***Normelement*** $\mathcal{N}$ *von* $\mathbb{F}_q[G]$ *(bzw.* $\mathbb{Z}[G]$*) ist wie folgt definiert:*

$$\mathcal{N} := \sum_{\sigma \in G} \sigma \in \mathbb{F}_q[G] \text{ (bzw.} \mathbb{Z}[G]).$$

Der Name erklärt sich dadurch, dass das Normelement von $\mathbb{Z}[G]$ gilt $\alpha^{\widetilde{\mathcal{N}}} = \mathrm{N}_{\mathbb{Q}}^{K}(\alpha)$.

Nun berechnen wir die Ideale $(\mathcal{N})^{\perp}$ und $(1+\iota)^{\perp}$ aus Lemma 5.2.2:

Lemma 5.3.1
Das Ideal $(\mathcal{N})^{\perp}$ *ist das Augmentationsideal von* $\mathbb{F}_q[G]$*, weiters gilt* $(1+\iota)^{\perp} = (1-\iota)$.

Beweis. Sei I das Augmentationsideal von $\mathbb{F}_q[G]$. Da G eine zyklische Gruppe ist, ist das Produkt eines Elementes $\Theta \in \mathbb{F}_q[G]$ mit $\mathcal{N}$ nur von dessen Gewicht abhängig: $\Theta\mathcal{N} = \omega(\Theta)\mathcal{N}$. Somit gilt $I(\mathcal{N}) = (0)$.
I wird erzeugt von den Elementen $\sigma_i - \sigma_j$, mit $i \neq j$ und $\sigma_i, \sigma_j \in G$. Somit ist $\mathcal{N} - \sum_{j \neq i}(\sigma_i - \sigma_j) = (p-1)\sigma_i \in I + (\mathcal{N})$, für jedes $\sigma_i \in G$, und wegen $q \nmid p-1$ folgt $I + (\mathcal{N}) = \mathbb{F}_q[G]$ und somit $I = (\mathcal{N})^{\perp}$ nach Lemma 5.2.2 (iii).

Die zweite Aussage folgt sofort aus $(1+\iota)(1-\iota) = (0)$ und $(1+\iota)+(1-\iota) = (2) = F_q[G]$. □

Wir müssen noch festlegen, wie die Elemente aus $\mathbb{F}_q[G]$ auf jene aus $K^{\times}$ wirken:

Definition 61
Für $\gamma \in K^{\times}$ *und* $\Theta \in \mathbb{F}_q[G]$ *sei* $\gamma^{\Theta} := \gamma^{\widetilde{\Theta}}$*, wobei* $\widetilde{\Theta}$ *eine Fortsetzung von* Θ *in* $\mathbb{Z}[G]$ *ist.*

Somit ist γ^{Θ} also nur bis auf Multiplikation mit q-ten Potenzen eindeutig bestimmt! Dies wird im Folgenden jedoch nicht zu Problemen führen, da in jedem Ausdruck ein γ^{Θ} enthält stets auch eine q-te Potenz eines (unbestimmten) Elements von $K^{\times}$ enthalten sein wird, beziehungsweise wir nur Annullatoren in $\mathbb{F}_q[G]$ von entsprechenden Faktormoduln betrachten.

Im Folgenden bezeichnen wir mit E die Gruppe der Einheiten von O_K. Wir betrachten nun die Faktorgruppe E/E^q und berechnen ihren Annullator:

Satz 5.3.2
Die Faktorgruppe E/E^q *ist ein zyklischer* $\mathbb{F}_q[G]$*-Modul, und es gilt:*

$$\mathrm{ann}_{\mathbb{F}_q[G]}(E/E^q) = (\mathcal{N}, 1-\iota). \tag{5.3}$$

Beweis. Wir zeigen zunächst (5.3). Sei W die Gruppe der Einheitswurzeln in K, dann schreiben wir $\overline{E} := E/W$. Da alle Einheitswurzeln in K q-te Potenzen sind ist $\overline{E}/\overline{E}^q$ isomorph zu E/E^q.

Wir definieren $\widetilde{\mathcal{N}}' := \sum_{i=1}^{\frac{p-1}{2}} \sigma_i \in \mathbb{Z}[G]$, das entspricht dem Normelement von $\mathbb{Z}[G^+]$, und bezeichnen mit $\mathcal{N}'$ das Bild von $\widetilde{\mathcal{N}}'$ in $\mathbb{F}_q[G]$, sodass dann gilt $\mathcal{N} = \mathcal{N}'(1+\iota)$.

Wir bestimmen zunächst den Annullator des $\mathbb{Z}[G]$-Moduls $\overline{E}$:
Aus Lemma 4.2.3 folgt dass für jedes $\varepsilon \in E$ das Element $\frac{\varepsilon}{\bar{\varepsilon}}$ eine Einheitswurzel ist. Weiters können wir jedes $\varepsilon \in E$ schreiben als Produkt $\varepsilon = \zeta^k \varepsilon'$ mit $1 \leq k < p$ und einer reellen Einheit $\varepsilon' \in E^+$. Wegen $\varepsilon'^{\widetilde{\mathcal{N}}'} = \mathrm{N}_{\mathbb{Q}}^{K^+}(\varepsilon') = \pm 1$ ist dann $\varepsilon^{\widetilde{\mathcal{N}}'} \in W$. Somit ist $\mathrm{ann}_{\mathbb{Z}[G]}(\overline{E}) = (\widetilde{\mathcal{N}}', 1-\iota)$.

Aus Lemma 5.2.4 folgt nun, dass das Ideal $q + (\widetilde{\mathcal{N}}', 1-\iota)$ ein radikales Ideal von $\mathbb{Z}[G]$ ist. Wendet man Lemma 5.2.5 an, so erhält man $\mathrm{ann}_{\mathbb{F}_q[G]}(\overline{E}/\overline{E}^q) = (\mathcal{N}', 1-\iota)$. Wegen

$$\mathcal{N}' = \frac{1}{2}\left(\mathcal{N} + (1-\iota)\mathcal{N}'\right) \in (\mathcal{N}, 1-\iota)$$

gilt $(\mathcal{N}', 1-\iota) = (\mathcal{N}, 1-\iota)$, woraus (5.3) folgt.

Das Element $1-\iota$ hat Gewicht 0 und ist daher im Augmentationsideal $(\mathcal{N})^\perp$ enthalten. Somit gilt $\mathcal{N} \cap (1-\iota) = \mathcal{N}(1-\iota) = (0)$ und es folgt

$$|(\mathcal{N}, 1-\iota)| = |(\mathcal{N})| \cdot |(1-\iota)| = q \cdot q^{\frac{p-1}{2}} = q^{\frac{p+1}{2}}.$$

Daraus erhalten wir $|\mathbb{F}_q[G]/(\mathcal{N}, 1-\iota)| = q^{\frac{p-3}{2}}$. Aus dem Dirichlet'schen Einheitensatz (Satz 2.6.5) folgt nun $\left|\overline{E}/\overline{E}^q\right| = q^{\frac{p-3}{2}}$.
Zusammen gilt also $\left|\overline{E}/\overline{E}^q\right| = \left|\mathbb{F}_q[G]/\mathrm{ann}_{\mathbb{F}_q[G]}(\overline{E}/\overline{E}^q)\right|$ und aus Lemma 5.2.3 (ii) folgt, dass der $\mathbb{F}_q[G]$-Modul $\overline{E}/\overline{E}^q$, und somit auch der isomorphe Modul E/E^q, zyklisch ist. □

Weiters betrachten wir die Gruppe der Kreisteilungseinheiten von K. Diese ist eine Untergruppe von E, wir bezeichnen sie im Folgenden mit C.
Eine spezielle Rolle spielen die q-primären Kreisteilungseinheiten.

Definition 62
*Ein Element $\alpha \in O_K$ heißt **q-primär**, falls es ein $\gamma \in O_K$ gibt mit $\alpha \equiv \gamma^q \pmod{q^2}$.*

Die Gruppe der q-primären Kreisteilungseinheiten von K bezeichnen wir im Folgenden mit C_q.

Für den Beweis betrachten wir die drei $\mathbb{F}_q[G]$-Moduln E/CE^q, C/C_q und $C_q/(C_q \cap E^q)$ und ihre Annullatoren und zeigen zunächst folgenden Satz:

Satz 5.3.3
Die drei $\mathbb{F}_q[G]$-Moduln

$$E/CE^q, \qquad C/C_q, \qquad C_q/(C_q \cap E^q)$$

sind zyklisch. Ihre Annullatoren

$$I_1 := \mathrm{ann}_{\mathbb{F}[G]}(E/CE^q), \qquad I_2 := \mathrm{ann}_{\mathbb{F}[G]}(C/C_q), \qquad I_3 := \mathrm{ann}_{\mathbb{F}[G]}(C_q/(C_q \cap E^q))$$

sind paarweise teilerfremd und es gilt

$$I_1 I_2 I_3 = (\mathcal{N}, 1-\iota). \tag{5.4}$$

Beweis. Es gilt

$$E/E^q \supseteq CE^q/E^q \supseteq C_q E^q/E^q. \tag{5.5}$$

Da Untermoduln von zyklischen Moduln wieder zyklisch sind, und da laut Satz 5.3.2 E/E^q zyklisch ist, sind auch diese drei Moduln zyklisch. Da selbiges auch für Faktormoduln von zyklischen Moduln gilt, sind E/CE^q, $C/C_q \cong CE^q/C_q E^q$ und $C_q/(C_q \cap E^q) \cong C_q E^q/E^q$ ebenfalls zyklisch.

Aus dem ersten Teil von Lemma 5.2.3 (i) folgt die Teilerfremdheit der drei Annullatoren. Wendet man die zweite Aussage von 5.2.3 (i) an so folgt aus (5.3):

$$\begin{aligned}
(\mathcal{N}, 1-\iota) &= \operatorname{ann}(E/E^q) \\
&= \operatorname{ann}\left((E/E^q)/(CE^q/E^q)\right)\operatorname{ann}(CE^q/E^q) \\
&= \operatorname{ann}(E/CE^q)\operatorname{ann}\left((CE^q/E^q)/(C_qE^q/E^q)\right)\operatorname{ann}(C_qE^q/E^q) \\
&= \operatorname{ann}(E/CE^q)\operatorname{ann}(CE^q/C_qE^q)\operatorname{ann}(C_q/(C_q\cap E^q)) \\
&= \operatorname{ann}(E/CE^q)\operatorname{ann}(C/C_q)\operatorname{ann}(C_q/(C_q\cap E^q)) \\
&= I_1 I_2 I_3.
\end{aligned}$$

(Wobei ann hier immer für $\operatorname{ann}_{\mathbb{F}[G]}$ steht.) □

Wir werfen nun einen kurzen Blick auf unsere weitere Vorgehensweise. Dazu gehen wir, wie im Folgenden immer, davon aus, dass (x, y, p, q) eine Lösung der Catalan'schen Gleichung $x^p - y^q = 1$ ist.

- Zunächst zeigen wir in Unterkapitel 5.4, dass für bestimmte gerade Θ mit $\omega(\Theta) = 0$, nämlich für jene aus $I_1 I_3$, das Element $(x-\zeta)^\Theta \in K^\times$ eine q-te Potenz ist.
- Danach zeigen wir in Unterkapitel 5.5, unter der Annahme $p, q \geq 7$, dass, falls $(x-\zeta)^\Theta$ für ein gerades Θ mit Gewicht 0 eine q-te Potenz ist, dann muss $\Theta = 0$ gelten.
- Schließlich führen wir diese beiden Aussagen in Unterkapitel 5.6 mit Hilfe von Satz 5.3.3 auf einen Widerspruch, womit gezeigt ist, dass die Catalan'sche Gleichung $x^p - y^q = 1$ unter den gegebenen Voraussetzungen keine Lösung besitzt.

5.4 Eine Anwendung des Satzes von Thaine

In diesem Unterkapitel gehen wir davon aus, dass (x, y, p, q) eine Lösung der Catalan'schen Gleichung $x^p - y^q = 1$ sei.

Unser Ziel ist es zu zeigen, dass das Element $(x-\zeta)^\Theta$ für bestimmte $\Theta \in \mathbb{F}_q[G]$ eine q-te Potenz ist. Genauer gesagt werden wir am Ende dieses Unterkapitels folgenden Satz beweisen:

Satz 5.4.1
Für jedes gerade $\Theta \in I_1 I_3$ mit Gewicht 0 ist $(x-\zeta)^\Theta$ eine q-te Potenz in $K^\times$, also

$$(x-\zeta)^\Theta \in (K^\times)^q.$$

Ein wesentliches Argument unseres Beweises liefert der Satz von Thaine (Satz 2.10.4). Da dieser jedoch nur eine Aussage über reelle abelsche Zahlkörper liefert müssen wir ihn zunächst etwas umformulieren.

Wir bezeichnen im Folgenden mit H die Idealklassengruppe von K und mit H^+ die Idealklassengruppe von $K^+ = \mathbb{Q}(\zeta + \overline{\zeta})$, dem maximalen reellen Teilkörper von K.

Satz 5.4.2
Sei Θ ein gerades Element von $\mathbb{Z}[G]$ das die q-Sylow Untergruppe von E/C annulliert. Dann annulliert Θ auch die q-Sylow Untergruppe von H^+.

Beweis. Wir bezeichnen mit G^+ die Galoisgruppe von K^+, mit E^+ die Einheitengruppe und mit C^+ die Gruppe der Kreisteilungseinheiten von K^+. Nun wissen wir, dass E^+ in E enthalten ist, und dass $C^+ = C \cap E^+$ gilt. Es folgt daher $E^+/C^+ \subseteq E/C$ und somit annulliert Θ auch die q-Sylow Untergruppe von E^+/C^+.

Da Θ gerade ist gilt $\Theta = (1+\iota)\Theta'$ für ein $\Theta' \in \mathbb{Z}[G]$. Da $G^+ = (1+\iota)G$ ist, folgt dass $\Theta \in \mathbb{Z}[G^+]$. Somit können wir Korollar 2.10.5 anwenden, und es folgt dass Θ auch die q-Sylow Untergruppe von H^+ annulliert. □

Da wir jedoch nicht in $\mathbb{Z}[G]$ sondern in $\mathbb{F}_q[G]$ arbeiten und auch eine Aussage über H, anstelle von H^+, benötigen, müssen wir diese Aussage noch weiter modifizieren um sie für den Beweis von Satz 5.4.1 verwenden zu können. Konkret werden wir folgendes Korollar verwenden:

Korollar 5.4.3
Jedes gerade $\Theta \in I_1$ besitzt eine Fortsetzung $\widetilde{\Theta} \in \mathbb{Z}[G]$, die die q-Sylow Untergruppe von H annulliert.

Beweis. Wir schreiben $\Theta = (1+\iota)\Theta'$ mit $\Theta' \in I_1$. Sei nun q^m die Ordnung der q-Sylow Untergruppe von E/C, dann existieren laut Lemma 5.2.2(ii) Elemente $\Theta_1, \ldots, \Theta_m \in I_1 = \mathrm{ann}_{\mathbb{F}_q[G]}(E/CE^q)$ sodass $\Theta = (1+\iota)^2\Theta_1 \cdots \Theta_m$.

Seien nun $\widetilde{\Theta}_1, \ldots, \widetilde{\Theta}_m$ jeweils Fortsetzungen von $\Theta_1, \ldots, \Theta_m$, dann definieren wir $\widetilde{\Theta}' := (1+\iota)\widetilde{\Theta}_1 \cdots \widetilde{\Theta}_m$ und $\widetilde{\Theta} := (1+\iota)\widetilde{\Theta}'$. Da jedes Θ_i laut Definition E/CE^q annulliert gilt also $E^{\widetilde{\Theta}_i} \subseteq CE^q$, und weiters $E^{\widetilde{\Theta}'} \subseteq CE^{q^m}$.

Laut der Definition von m bedeutet das also, dass $\widetilde{\Theta}'$ die q-Sylow Untergruppe von E/C annulliert. Aus Satz 5.4.2 folgt nun, dass $\widetilde{\Theta}'$ auch die q-Sylow Untergruppe von H^+ annulliert. Und wegen $H^{1+\iota} \subseteq H^+$ annulliert $\widetilde{\Theta} = (1+\iota)\widetilde{\Theta}'$ die q-Sylow Untergruppe von H. □

Wir verwenden nun dieses Korollar und zeigen zunächst folgendes Lemma:

Lemma 5.4.4
Für jedes gerade $\Theta \in I_1$ mit Gewicht 0 gilt

$$(x-\zeta)^\Theta \in E(K^\times)^q.$$

Beweis. Sei $\lambda := \frac{x-\zeta}{1-\zeta}$. Aus Lemma 4.2.5 folgt, dass das Hauptideal (λ) die q-te Potenz eines Ideals $A \trianglelefteq O_K$ ist, also $(\lambda) = A^q$. Die Idealklasse, in der A enthalten ist, hat also die Ordnung q und gehört damit zur q-Komponente der Idealklassengruppe H. Da die Idealklassengruppe eines Zahlkörpers immer endlich ist, ist die q-Komponente von H gleich ihrer q-Sylow Untergruppe.

Da wir uns in Definition 61 nicht auf eine bestimmte Fortsetzung von Θ festgelegt haben, die das Element λ^Θ bestimmt, dürfen wir nun jene Fortsetzung $\widetilde{\Theta}$ aus Korollar 5.4.3 wählen, die die q-Sylow Untergruppe von H annulliert.

Wie wir vorhin gesehen haben, ist A in der q-Sylow Untergruppe von H enthalten, somit ist $A^{\widetilde{\Theta}}$ ein Hauptideal. Also ist das Hauptideal (λ^Θ) die q-te Potenz eines weiteren Hauptideals, und es folgt $\lambda^\Theta \in E(K^\times)^q$.

Nun gehört Θ aber laut Voraussetzung dem Augmentationsideal von $\mathbb{F}_q[G]$ an. Dieses wird bekanntlich von den Elementen der Form $\sigma - \tau$, mit $\sigma, \tau \in G$, erzeugt. Nun ist $(1-\zeta)^{\sigma-\tau}$ eine Kreisteilungseinheit und somit ist auch $(1-\zeta)^\Theta$ eine Kreisteilungseinheit, und es folgt

$$(x-\zeta)^\Theta = \lambda^\Theta (1-\zeta)^\Theta \in E(K^\times)^q.$$

□

Als nächstes verwenden wir Mihailescus Wieferich Kriterium aus Kapitel 4 um die Aussage von Lemma 5.4.4 noch zu erweitern:

Lemma 5.4.5
Für jedes gerade $\Theta \in I_1$ mit Gewicht 0 gilt

$$(x-\zeta)^\Theta \in C_q(K^\times)^q.$$

Beweis. Laut Lemma 5.2.2(ii) können wir $\Theta = \Theta_1\Theta_2$ schreiben, wobei $\Theta_1 \in I_1$ gerade und von Gewicht 0 sei, und $\Theta_2 \in I_1$ beliebig. Aus Lemma 5.4.4 wissen wir, dass $(x-\zeta)^\Theta \in E(K^\times)^q$ und wegen $\Theta_2 \in I_1 = \mathrm{ann}_{\mathbb{F}_q[G]}(E/CE^q)$ folgt

$$(x-\zeta)^\Theta = (x-\zeta)^{\Theta_1\Theta_2} \in E^{\Theta_2}(K^\times)^q \subseteq C(K^\times)^q.$$

Wir können also $(x-\zeta)^\Theta = \eta\alpha^q$ schreiben, mit $\eta \in C$ und $\alpha \in K^\times$. Mihailescus Wieferich Kriterium (Satz 4.2.1) besagt nun, dass $q^2 | x$. Also gilt $\eta\alpha^q \equiv (-\zeta)^\Theta \pmod{q^2}$. Da nun ζ eine p-te Einheitswurzel ist ζ, und somit auch $-\zeta$, auch eine q-te Potenz in $K^\times$. Also ist η eine q-primäre Kreisteilungseinheit, womit die Behauptung des Lemmas gezeigt ist. □

Damit können wir nun den Satz 5.4.1 mit einem analogen Argument wie im Beweis des letzten Lemmas beweisen:

Beweis von Satz 5.4.1. Sei nun $\Theta \in I_1 I_3$ gerade und von Gewicht 0. Laut Lemma 5.2.2(ii) können wir wieder $\Theta = \Theta_1\Theta_2$ schreiben, wobei $\Theta_1 \in I_1$ gerade und von Gewicht 0 sei, und $\Theta_2 \in I_3$. Mit Lemma 5.4.5 und $I_3 = \mathrm{ann}_{\mathbb{F}_q[G]}(C_q/(C_q \cap E^q))$ folgt nun

$$(x-\zeta)^\Theta = (x-\zeta)^{\Theta_1\Theta_2} \in C_q^{\Theta_2}(K^\times)^q \subseteq (K^\times)^q.$$

□

5.5 Eine Anwendung der Runge Methode

In diesem Unterkapitel gehen wir von einer Lösung (x, y, p, q) der Catalan'schen Gleichung $x^p - y^q = 1$ aus, die $p, q \geq 7$ erfüllt.

Es ist für uns praktischer in $\mathbb{Z}[G]$ zu arbeiten. Das Ziel dieses Unterkapitels ist es den folgenden Satz zu zeigen:

Satz 5.5.1
Sei Θ ein gerades positives Element von $\mathbb{Z}[G]$ dessen Gewicht durch q teilbar ist, und für dessen Gewicht weiters gilt $\omega(\Theta) \leq q\frac{p-1}{2}$. Falls $(x-\zeta)^\Theta \in (K^\times)^q$, dann gilt $\Theta \in q\mathbb{Z}[G]$.

Da wir für Mihailescus Beweis aber eine Aussage über $\mathbb{F}_q[G]$ benötigen, zeigen wir im Anschluss ein entsprechendes Korollar.

Sei nun im Folgenden $\Theta := \sum_{\sigma\in G} n_\sigma \sigma \in \mathbb{Z}[G]$ ein Element, das die obigen Voraussetzungen erfüllt, wir müssen zeigen, dass die Koeffizienten n_σ durch q teilbar sind. Nach den Voraussetzungen des Satzes existiert ein $\alpha \in K^\times$ sodass

$$\alpha^q = (x-\zeta)^\Theta.$$

Weiters existiert eine ganze Zahl m mit $\omega(\Theta) = mq$. Da Θ gerade und positiv ist gilt $m \neq 0$ und somit laut Voraussetzung $1 \leq m \leq \frac{p-1}{2}$. Da Θ gerade ist muss weiters auch $\omega(\Theta)$ gerade sein, also $m \in 2\mathbb{Z}$. Es gilt also

$$\left(1-\frac{\zeta}{x}\right)^\Theta = \left(\frac{1}{x}\right)^\Theta (x-\zeta)^\Theta = \left(\frac{1}{x}\right)^{\omega(\Theta)} (x-\zeta)^\Theta = \left(\frac{\alpha}{x^m}\right)^q. \tag{5.6}$$

Wir werden im Beweis von Satz 5.5.1 das Element α genauer analysieren. Dazu verwenden wir Potenzreihen um die q-te Wurzel von $\left(1-\frac{\zeta}{x}\right)^\Theta$ in $K^\times$ zu berechnen.

Die Methode von Runge besteht nun darin zu zeigen, dass eine gewisse Teilsumme einer Reihe so nah an deren Grenzwert ist, dass sie übereinstimmen. In unserem Fall werden wir zeigen, dass die Differenz zwischen einer Teilsumme unserer Potenzreihe und der q-ten Wurzel α eine ganzalgebraische Zahl mit Norm kleiner 1 ist, und somit gleich 0 sein muss.

Die Potenzreihe die wir dazu verwenden lautet

$$F(T) := (1-\zeta T)^{\frac{\Theta}{q}} = \prod_{\sigma\in G} (1-\zeta^\sigma T)^{\frac{n_\sigma}{q}},$$

wobei $(1-\zeta^\sigma T)^{\frac{n_\sigma}{q}}$ definiert sei als

$$(1-\zeta^\sigma T)^{\frac{n_\sigma}{q}} := \sum_{k\geq 0} \binom{\frac{n_\sigma}{q}}{k} (-\zeta^\sigma T)^k.$$

Da Θ durch $1+\iota$ teilbar ist, hat $F(T)$ Koeffizienten in $\mathbb{Q}(\zeta+\zeta^{-1}) = K^+ \subseteq \mathbb{R}$, wir können also $F(T) = \sum_{k\geq 0} \alpha_k T^k$ schreiben mit $\alpha_k \in K^+$. Als Reihe in $\mathbb{R}$ gesehen hat diese Potenzreihe Konvergenzradius 1.
Wie man aus Gleichung (5.6) sieht, verwenden wir die Potenzreihe $F(T)$ für $T = \frac{1}{x}$.

Wir untersuchen nun die Potenzreihe $F(T)$ genauer und halten zunächst folgende allgemeine Eigenschaft formaler Potenzreihen fest:

Lemma 5.5.2
Sei R ein Integritätsbereich und Q sein Quotientenkörper. Seien weiters $\sum_{k\geq 0}\frac{a_k}{k!}T^k$, $\sum_{k\geq 0}\frac{b_k}{k!}T^k \in Q[[T]]$ zwei formale Potenzreihen für die $a, b \in R$ und ein Ideal $I \trianglelefteq R$ existieren, sodass

$$a_k, b_k \in R, \qquad a_k \equiv a^k \,(\mathrm{mod}\, I), \qquad b_k \equiv b^k \,(\mathrm{mod}\, I) \qquad \forall k = 0, 1, \ldots$$

gilt, dann folgt

$$\left(\sum_{k\geq 0}\frac{a_k}{k!}T^k\right)\left(\sum_{k\geq 0}\frac{b_k}{k!}T^k\right) = \sum_{k\geq 0}\frac{c_k}{k!}T^k$$

mit $c_k \in R$ und $c_k \equiv (a+b)^k \,(\mathrm{mod}\, I)$.

Beweis. Durch Bildung des Cauchyprodukts erhält man $c_k = \sum_{i=0}^{k}\binom{k}{i}a_i b_{k-i} \equiv \sum_{i=0}^{k}\binom{k}{i}a^i b^{k-i} = (a+b)^k \,(\mathrm{mod}\, I)$. □

Nun können wir eine Aussage über die Koeffizienten der Potenzreihe $F(T)$ treffen:

Lemma 5.5.3
Die Potenzreihe $F(T)$ hat die Form

$$F(T) = \sum_{k\geq 0}\frac{a_k}{k!q^k}T^k$$

mit $a_k \in \mathbb{Z}[\zeta]$ und $a_k \equiv (-\sum_{\sigma\in G} n_\sigma \zeta^\sigma)^k \,(\mathrm{mod}\, q)$.
Weiters gilt

$$q^{k+\nu_q(k!)}\frac{a_k}{k!q^k} \in \mathbb{Z}[\zeta]$$

.

Beweis. Wir wenden Lemma 5.5.2 mit $R = \mathbb{Z}[\zeta]$ an auf die Potenzreihen

$$\begin{aligned}
(1-\zeta^\sigma qT)^{\frac{n_\sigma}{q}} &= \sum_{k\geq 0}\binom{\frac{n_\sigma}{q}}{k}(-\zeta^\sigma qT)^k \\
&= \sum_{k\geq 0}\left(\frac{1}{q}\right)^k \frac{n_\sigma(n_\sigma-q)(n_\sigma-2q)\cdots(n_\sigma-(k-1)q)}{k!}(-\zeta^\sigma qT)^k \\
&= \sum_{k\geq 0}\frac{n_\sigma(n_\sigma-q)(n_\sigma-2q)\cdots(n_\sigma-(k-1)q)}{k!}(-\zeta^\sigma T)^k
\end{aligned}$$

für $\sigma \in G$. Die Koeffizienten dieser Potenzreihen haben also die Form $\frac{a_k}{k!}$ mit

$$a_k = n_\sigma(n_\sigma-q)(n_\sigma-2q)\cdots(n_\sigma-(k-1)q)(-\zeta^\sigma)^k \in \mathbb{Z}[\zeta].$$

Man erkennt sofort, dass $a_k \equiv (-n_\sigma\zeta^\sigma)^k \,(\mathrm{mod}\, q)$. Laut Lemma 5.5.2 gilt daher $F(qT) = \sum_{k\geq 0}\frac{c_k}{k!}T^k$ mit $c_k \in \mathbb{Z}[\zeta]$ und $c_k \equiv (-\sum_{\sigma\in G} n_\sigma\zeta^\sigma)^k \,(\mathrm{mod}\, q)$.
Weiters sind für jede Primzahl p ungleich q, wegen $ggT(p,q) = 1$, mindestens $\left\lfloor\frac{k}{p}\right\rfloor$

der Faktoren $(n_\sigma - jq)$ mit $0 \leq j \leq k-1$ kongruent 0 modulo p. Analoges gilt für die Potenzen p^i, also gilt:

$$\nu_p(a_k) = \nu_p(n_\sigma(n_\sigma - q)(n_\sigma - 2q)\cdots(n_\sigma - (k-1)q)) \geq \left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{k}{p^2} \right\rfloor + \cdots = \nu_p(k!),$$

woraus die letzte Aussage folgt. □

Mit $F_l(T)$ bezeichnen wir die l-te Teilsumme von $F(T)$, also $F_l(T) = \sum_{k=0}^{l} \alpha_k T^k$. Wir betrachten $F(T)$ nun als Potenzreihe über $\mathbb{R}$ und geben eine Abschätzung für die Differenz der Werte $F(t)$ und $F_l(t)$:

Lemma 5.5.4
Für jedes $t \in \mathbb{R}$ mit $|t| < 1$ gilt

$$|F(t) - F_l(t)| \leq \binom{m+l}{m+1} \frac{|t|^{l+1}}{(1-|t|)^{m+l}}.$$

Beweis. Wir vergleichen zunächst die Koeffizienten von $\sum_{k\geq 0} \binom{\frac{n_\sigma}{q}}{k}(-\zeta^\sigma T)^k$ mit jenen von $(1-T)^{-\frac{n_\sigma}{q}} = \sum_{k\geq 0} \binom{\frac{n_\sigma}{q}}{k}(-T)^k$ und betrachten dazu folgende Ungleichung, die für alle positiven rationalen Zahlen a und ganzzahlige k gilt:

$$\begin{aligned} \left|\binom{a}{k}\right| &= \left|\frac{a(a-1)(a-2)\cdots(a-(k-1))}{k!}\right| \\ &\leq (-1)^k \frac{-a(-a-1)(-a-2)\cdots(-a-(k-1))}{k!} \\ &= (-1)^k \binom{-a}{k}. \end{aligned}$$

Da Θ ein positives Element ist gilt $n_\sigma \geq 0$ für alle $\sigma \in G$ und wir können folgern

$$\left|\binom{\frac{n_\sigma}{q}}{k}(-\zeta^\sigma)^k\right| = \left|\binom{\frac{n_\sigma}{q}}{k}\right| \leq (-1)^k \binom{\frac{n_\sigma}{q}}{k}.$$

Es sind also die Absolutbeträge der Koeffizienten von $\sum_{k\geq 0} \binom{\frac{n_\sigma}{q}}{k}(-\zeta^\sigma T)^k$ kleiner oder gleich jene von $\sum_{k\geq 0} \binom{\frac{n_\sigma}{q}}{k}(-T)^k$.

Somit sind auch die Absolutbeträge der Koeffizienten von $F(T)$ kleiner oder gleich jene von $\prod_{\sigma\in G}(1-T)^{-\frac{n_\sigma}{q}} = (1-T)^{-\frac{1}{q}\sum_{\sigma\in G} n_\sigma} = (1-T)^{-m}$, da ja $\omega(\Theta) = mq$. Für $t \in \mathbb{R}$ mit $|t| < 1$ gilt also die Ungleichung

$$|F(t) - F_l(t)| \leq |(1-t)^{-m} - S_l(t)|,$$

wobei $S_l(t)$ die l-te Teilsumme der Taylorreihenentwicklung von $(1-t)^{-m}$ sei.

Die Berechnung des Restgliedes der Taylorreihe ergibt

$$(1-t)^{-m} - S_l(t) = \left.\frac{d^{l+1}(1-z)^{-m}}{dz^{l+1}}\right|_{z=\xi} \frac{t^{l+1}}{(l+1)!}$$

für ein $\xi \in \mathbb{R}$ mit $|\xi| < |t|$.
Somit folgt

$$\begin{aligned}(1-t)^{-m} - S_l(t) &= \frac{t^{l+1}}{(l+1)!}\frac{(m+l)!}{(m-1)!}(1-|\xi|)^{-m-l} \\ &= t^{l+1}\binom{m+l}{l+1}\frac{1}{(1-|\xi|)^{m+l}} \\ &\leq \frac{|t|^{l+1}}{(1-|t|)^{m+l}}\binom{m+l}{m+1}.\end{aligned}$$

□

Bevor wir zum Beweis von Satz 5.5.1 kommen benötigen wir noch eine wichtige Aussage über die Wirkung der Galoisgruppe G auf die Werte der Potenzreihe $F(T)$.

Zunächst halten wir die folgenden Notationen fest. Sei $\sigma \in G$, dann bezeichne $F^\sigma(t)$ den Wert der Potenzreihe, die man durch die Wirkung von σ auf die Koeffizienten von $F(t)$ erhält, also $F^\sigma(t) = (1-\zeta t)^{\frac{\sigma\Theta}{q}}$. Mit $\sigma(F(t))$ bezeichnen wir das Bild des Wertes von $F(t)$ unter σ, also $\sigma(F(t)) = \left((1-\zeta T)^{\frac{\Theta}{q}}\right)^\sigma$.

Die Gleichung

$$\sigma(F(t)) = F^\sigma(t) \tag{5.7}$$

muss nicht notwendigerweise gelten. Es ist sogar im Allgemeinen ihre linke Seite nicht wohldefiniert, da $F(t) = (1-\zeta t)^{\frac{\Theta}{q}}$ nicht notwendigerweise in K liegen muss.

Wir benötigen also eine zusätzliche Voraussetzung um die Gültigkeit der Gleichung (5.7) zu sichern:

Lemma 5.5.5
Sei $t \in \mathbb{Q}$ mit $|t| < 1$ sodass $F(t) = (1-\zeta t)^{\frac{\Theta}{q}} \in K$, dann gilt $\sigma(F(t)) = F^\sigma(t)$ für alle $\sigma \in G$.

Beweis. Wie wir bereits festgestellt haben hat die Potenzreihe $F(T) = (1-\zeta T)^{\frac{\Theta}{q}}$ reelle Koeffizienten, da Θ gerade ist. Es gilt also

$$\alpha := (1-\zeta t)^{\frac{\Theta}{q}} \in \mathbb{R}.$$

Somit ist α im maximalen reellen Unterkörper $K^+ = \mathbb{Q}(\zeta + \zeta^{-1})$ enthalten, woraus $\alpha^\sigma = \sigma(F(t)) \in \mathbb{R}$ für alle $\sigma \in G$ folgt.

Andererseits ist auch $\sigma\Theta$ gerade, und somit ist auch $F^\sigma(t) = (1-\zeta t)^{\frac{\sigma\Theta}{q}} \in \mathbb{R}$.

Es gilt nun $(\alpha^\sigma)^q = (\alpha^q)^\sigma = \left((1-\zeta t)^\Theta\right)^\sigma = (1-\zeta t)^{\sigma\Theta}$. Somit ist also $\sigma(F(t)) = \alpha^\sigma$ gleich der reellen q-ten Wurzel von $(1-\zeta t)^{\sigma\Theta}$, also gleich $F^\sigma(t)$. □

Nun können wir uns dem Beweis von Satz 5.5.1 zuwenden:

Beweis von Satz 5.5.1. Laut unseren Voraussetzungen ist $\alpha \in K^\times$ eine q-te Wurzel von $(x-\zeta)^\Theta$, und da K neben 1 keine weiteren q-ten Einheitswurzeln enthält ist α die einzige q-te Wurzel von $(x-\zeta)^\Theta$ in K.

Wegen $1+\iota \mid \Theta$ wissen wir dass $\left(1-\frac{\zeta}{x}\right)^{\Theta} \in K^{+} \subseteq \mathbb{R}$ und wegen $|x|>1$ gilt $1-\left|\frac{\zeta^{\sigma}}{x}\right|>0$ für alle $\sigma \in G$. Somit haben wir $\left(1-\frac{\zeta}{x}\right)^{\Theta}>0$.

Da auch m gerade ist folgt, dass $(x-\zeta)^{\Theta}=x^{\omega(\Theta)}\left(1-\frac{\zeta}{x}\right)^{\Theta}=x^{mq}\left(1-\frac{\zeta}{x}\right)^{\Theta}$ eine positive reelle Zahl ist. Somit ist α gleich der reellen q-ten Wurzel von $x^{mq}\left(1-\frac{\zeta}{x}\right)^{\Theta}$, es gilt also

$$\alpha = x^m\left(1-\frac{\zeta}{x}\right)^{\frac{\Theta}{q}} = x^m F\left(\frac{1}{x}\right) \in K^{\times}. \tag{5.8}$$

Somit ist auch $F\left(\frac{1}{x}\right) \in K$ und laut Lemma 5.5.5 gilt daher $\sigma\left(F\left(\frac{1}{x}\right)\right)=F^{\sigma}\left(\frac{1}{x}\right)$ für alle $\sigma \in G$.
Nun definieren wir

$$\gamma := q^{m+\nu_q(m!)}x^m F_m\left(\frac{1}{x}\right).$$

Aus Lemma 5.5.3 folgt, dass $\gamma \in \mathbb{Z}[\zeta]=O_K$.

Der wichtigste Schritt in unserem Beweis ist es nun zu zeigen, dass $\gamma = q^{m+\nu_q(m!)}\alpha$. Dazu nutzen wir aus, dass sowohl γ als auch α, und somit auch die Differenz $q^{m+\nu_q(m!)}\alpha-\gamma$, ganzalgebraisch sind. Da die Norm jedes Elements aus O_K ganzzahlig ist, genügt es zu zeigen, dass

$$|\sigma(q^{m+\nu_q(m!)}\alpha-\gamma)|<1 \tag{5.9}$$

für alle $\sigma \in G$ gilt, da daraus folgt, dass zunächst die Norm und damit die Differenz selbst gleich 0 ist.

Um (5.9) zu zeigen benutzen wir zunächst die obige Erkenntnis $\sigma\left(F\left(\frac{1}{x}\right)\right)=F^{\sigma}\left(\frac{1}{x}\right)$ und sehen:

$$\begin{aligned}
|\sigma(q^{m+\nu_q(m!)}\alpha-\gamma)| &= |q^{m+\nu_q(m!)}\sigma(\alpha)-\sigma(\gamma)| \\
&= q^{m+\nu_q(m!)}\left|x^m\sigma\left(F\left(\frac{1}{x}\right)\right)-x^m\sigma\left(F_m\left(\frac{1}{x}\right)\right)\right| \\
&= q^{m+\nu_q(m!)}\left|x^m F^{\sigma}\left(\frac{1}{x}\right)-x^m F_m^{\sigma}\left(\frac{1}{x}\right)\right| \qquad (5.10)
\end{aligned}$$

Aus Lemma 5.5.4 folgt

$$\begin{aligned}
\left|x^m F^{\sigma}\left(\frac{1}{x}\right)-x^m F_m^{\sigma}\left(\frac{1}{x}\right)\right| &\leq \binom{2m}{m+1}\frac{|x|^m\frac{1}{(|x|)^{m+1}}}{\left(1-\frac{1}{|x|}\right)^{2m}} \\
&= \binom{2m}{m+1}\frac{1}{|x|}\frac{1}{(1-|x|)^{2m}} \qquad (5.11)
\end{aligned}$$

Gemeinsam mit den beiden Ungleichungen

$$m+\nu_q(m!)=m+\left\lfloor\frac{m}{q}\right\rfloor+\left\lfloor\frac{m}{q^2}\right\rfloor+\cdots \leq m\left(1+\frac{1}{q}+\frac{1}{q^2}+\cdots\right)=\frac{mq}{q-1}=m+\frac{m}{q-1}$$

und

$$\binom{2m}{m+1}<(1+1)^{2m}=4^m=q^{m\frac{\log 4}{\log q}}$$

folgt durch Zusammensetzen von (5.10) und (5.11)

$$\begin{aligned} |\sigma(q^{m+\nu_q(m!)}\alpha-\gamma)| &\leq q^{m+\nu_q(m!)}\binom{2m}{m+1}\frac{1}{|x|}\frac{1}{(1-|x|)^{2m}} \\ &\leq q^{m+\frac{m}{q-1}}q^{m\frac{\log 4}{\log q}}\frac{1}{|x|}\frac{1}{(1-|x|)^{2m}}. \end{aligned} \tag{5.12}$$

Wir schätzen nun zunächst den Ausdruck $\frac{1}{(1-|x|)^{2m}}$ ab, wobei wir $p > 2m$, wegen $1 \leq m \leq \frac{p-1}{2}$, und $|x| \geq q^{p-1}$, was wir in Korollar 4.1.8 gezeigt haben, verwenden:

$$\begin{aligned} \frac{1}{(1-|x|)^{2m}} &\leq \frac{1}{(1-|x|)^{p-1}} \leq \frac{1}{(1-q^{p-1})^{p-1}} \\ &< \frac{1}{(1-q^{p-1})^{p-1}}\frac{(q^{p-1})^p}{q^{p-1}-1} = \left(\frac{q^{p-1}}{q^{p-1}-1}\right)^p \\ &= \left(1-\frac{1}{q^{p-1}}\right)^{-p}. \end{aligned} \tag{5.13}$$

Wir verwenden abermals $m \leq \frac{p-1}{2}$ und $|x| \geq q^{p-1}$ und erhalten durch Einsetzen von (5.13) in (5.12)

$$|\sigma(q^{m+\nu_q(m!)}\alpha-\gamma)| \leq q^{\frac{p-1}{2}\left(-1+\frac{1}{q-1}+\frac{\log 4}{\log q}\right)}\left(1-\frac{1}{q^{p-1}}\right)^{-p}.$$

Wir wollen nun zeigen, dass der Ausdruck auf der rechten Seite kleiner als 1 ist. Dazu nehmen wir den q-Logarithmus und zeigen dass dieser negativ ist.

Zunächst erhalten wir als q-Logarithmus folgenden Ausdruck

$$\frac{p-1}{2}\left(-1+\frac{1}{q-1}+\frac{\log 4}{\log q}\right)-p\frac{\log\left(1-\frac{1}{q^{p-1}}\right)}{\log q}.$$

Nun verwenden wir unsere Voraussetzung $q \geq 7$ und erhalten:

$$\frac{p-1}{2}\left(-1+\frac{1}{q-1}+\frac{\log 4}{\log q}\right) \leq \frac{p-1}{2}\left(-1+\frac{1}{6}+\frac{\log 4}{\log 7}\right)$$

sowie

$$\begin{aligned} -\log\left(1-\frac{1}{q^{p-1}}\right) &= \log\left(\frac{q^{p-1}-1}{q^{p-1}}\right)^{-1} = \log\left(\frac{q^{p-1}}{q^{p-1}-1}\right) \\ &\leq \log\left(\frac{7^2}{7^2-1}\right) = \log\left(\frac{49}{48}\right) < \frac{1}{48}. \end{aligned}$$

Zusammen folgt aus diesen Ungleichungen:

$$\begin{aligned} &\frac{p-1}{2}\left(-1+\frac{1}{q-1}+\frac{\log 4}{\log q}\right)-p\frac{\log\left(1-\frac{1}{q^{p-1}}\right)}{\log q} \\ &\leq \frac{p-1}{2}\left(-1+\frac{1}{6}+\frac{\log 4}{\log 7}\right)+\frac{p}{48\log 7} < 0 \end{aligned}$$

für alle $p \geq 7$.

Wir haben somit $|\sigma(q^{m+\nu_q(m!)}\alpha - \gamma)| < 1$ für alle $\sigma \in G$ gezeigt, und es folgt

$$q^{m+\nu_q(m!)}\alpha = \gamma = q^{m+\nu_q(m!)}x^m F_m\left(\frac{1}{x}\right) = \sum_{k=0}^{m} q^{m+\nu_q(m!)}\frac{a_k}{k!q^k}x^{m-k}. \tag{5.14}$$

Wir wissen, dass $q^{m+\nu_q(m!)}\alpha \in O_K$, und nach Lemma 5.5.3 sind auch die Koeffizienten auf der rechten Seite von (5.14) ganzalgebraisch. Wegen $m \geq 1$ ist $q^{m+\nu_q(m!)}\alpha$ trivialerweise durch q teilbar. Weiters sind für $k < m$ die Koeffizienten $q^{m+\nu_q(m!)}\frac{a_k}{k!q^k}$ ebenfalls durch q teilbar. Somit muss auch der m-te Koeffizient der rechten Seite von (5.14), nämlich $q^{m+\nu_q(m!)}\frac{a_m}{m!q^m}$, durch q teilbar sein.

Wegen $\nu_q\left(q^{m+\nu_q(m!)}\frac{a_m}{m!q^m}\right) = \nu_q(a_m)$ folgt daher $q|a_m$, also $a_m \equiv 0 \,(\mathrm{mod}\, q)$.

Andererseits wissen wir aber aus Lemma 5.5.3, dass

$$a_m \equiv \left(-\sum_{\sigma\in G} n_\sigma \zeta^\sigma\right)^m \,(\mathrm{mod}\, q).$$

Nun wissen wir aber aus Lemma 5.2.4, dass (q) ein radikales Ideal von $\mathbb{Z}[G]$ ist, und somit $\mathbb{Z}[G]/(q)$ kein nilpotentes Element enthält. Es muss also $\sum_{\sigma\in G} n_\sigma\zeta^\sigma \equiv 0 \,(\mathrm{mod}\, q)$ gelten, und da die ζ^σ linear unabhängig über $\mathbb{Q}$ sind, folgt $q|n_\sigma$ für alle $\sigma \in G$, also $\Theta \in q\mathbb{Z}[G]$. □

Nun müssen wir Satz 5.5.1 noch Umformulieren um daraus eine Aussage über $\mathbb{F}_q[G]$ zu gewinnen. Dazu zeigen wir zunächst folgendes Lemma:

Lemma 5.5.6
Sei $\Theta \in \mathbb{F}_q[G]$, dann besitzt entweder Θ oder $-\Theta$ eine nichtnegative Fortsetzung $\widetilde{\Theta} \in \mathbb{Z}[G]$ mit $\omega(\widetilde{\Theta}) \leq q^{\frac{p-1}{2}}$.
Falls Θ im Augmentationsideal von $\mathbb{F}_q[G]$ liegt, so gilt weiters $q|\omega(\widetilde{\Theta})$.
Falls Θ gerade ist, so ist es auch $\widetilde{\Theta}$.

Beweis. Sei $\widetilde{\Theta}_1$ die kleinste nichtnegative Fortsetzung von Θ, also $\widetilde{\Theta}_1 := \sum_{\sigma\in G}\widetilde{n}_\sigma\sigma$ mit $\widetilde{n}_\sigma \in \{0, 1, \ldots, q-1\}$. Weiters definieren wir $\widetilde{\Theta}_2 := q\sum_{\sigma\in G}\sigma - \widetilde{\Theta}_1$, somit ist $\widetilde{\Theta}_2$ eine nichtnegative Fortsetzung von $-\Theta$.

Sowohl $\widetilde{\Theta}_1$ als auch $\widetilde{\Theta}_2$ sind gerade, falls Θ gerade ist, und die beiden Gewichte $\omega(\widetilde{\Theta}_1)$ und $\omega(\widetilde{\Theta}_2)$ sind durch q teilbar, falls Θ im Augmentationsideal liegt.

Schließlich ist wegen $\omega(\widetilde{\Theta}_1) + \omega(\widetilde{\Theta}_2) = q(p-1)$ sichergestellt, dass eines der beiden Gewichte $\omega(\widetilde{\Theta}_1)$ und $\omega(\widetilde{\Theta}_2)$ kleiner oder gleich $q^{\frac{p-1}{2}}$ ist. □

Nun müssen wir den Satz 5.5.1 noch in folgendes, für Mihailescus Beweis relevantes, Korollar umformulieren:

Korollar 5.5.7
Sei (x, y, p, q) eine Lösung der Catalan'schen Gleichung $x^p - y^q = 1$ mit $p, q \geq 7$, und sei $\Theta \in \mathbb{F}_q[G]$ ein gerades Element des Augmentationsideals sodass $(x-\zeta)^\Theta \in (K^\times)^q$ gilt, dann folgt $\Theta = 0$.

Beweis. Sei $\Theta \neq 0$ ein Element von $\mathbb{F}_q[G]$, dass die geforderte Bedingung erfüllt. Da $(x-\zeta)^{\Theta}$ eine q-te Potenz in $K^{\times}$ ist, ist auch $(x-\zeta)^{-\Theta}$ eine q-te Potenz.
Nun folgt aus Lemma 5.5.6 dass entweder Θ oder $-\Theta$ eine gerade und positive Fortsetzung $\widetilde{\Theta}$ in $\mathbb{Z}[G]$ hat, deren Gewicht $\omega(\widetilde{\Theta})$ durch q teilbar und kleiner oder gleich $\frac{q(p-1)}{2}$ ist.
Es sind also alle Voraussetzungen von Satz 5.5.1 erfüllt, und die Behauptung folgt aus der Anwendung dieses Satzes. □

5.6 Abschluss des Beweises

In diesem Unterkapitel schließen wir den Beweis der Catalan'schen Vermutung ab, indem wir aus den bisher in diesem Kapitel gezeigten Aussagen einen Widerspruch ableiten.

Zunächst benötigen wir jedoch noch den folgenden Satz, der für von der Catalan'schen Vermutung unabhängige, verschiedene ungerade Primzahlen p und q gilt:

Satz 5.6.1
Falls $p > q$, so gilt $C \neq C_q$.

Beweis. Um die Aussage $C \neq C_q$ zu zeigen werden wir die Annahme, alle Kreisteilungseinheiten seien q-primär, auf einen Widerspruch führen.

Laut unserer Annahme ist nun speziell auch $1+\zeta^q = \frac{1-\zeta^{2q}}{1-\zeta^q} \in C_q$. Es existiert also ein $\gamma \in \mathbb{Z}[\zeta]$ mit $1+\zeta^q \equiv \gamma^q \,(\mathrm{mod}\, q^2)$. Damit gilt weiters $(1+\zeta)^q \equiv 1+\zeta^q \equiv \gamma^q \,(\mathrm{mod}\, q)$, also $(1+\zeta)^q - \gamma^q \equiv ((1+\zeta)-\gamma)^q \equiv 0 \,(\mathrm{mod}\, q)$.
Da jedoch (q) ein radikales Ideal ist folgt daraus $(1+\zeta)-\gamma \equiv 0 \,(\mathrm{mod}\, q)$, also $1+\zeta \equiv \gamma \,(\mathrm{mod}\, q)$ woraus $(1+\zeta)^q \equiv \gamma^q \,(\mathrm{mod}\, q^2)$ folgt. Somit haben wir

$$(1+\zeta)^q \equiv 1+\zeta^q \,(\mathrm{mod}\, q^2) \tag{5.15}$$

gezeigt. Wir betrachten nun das folgende Polynom

$$f(T) := \frac{1}{q}\left((1+T)^q - 1 - T^q\right).$$

Aus dem binomischen Lehrsatz erkennt man, dass es sich hierbei um ein normiertes Polynom mit ganzzahligen Koeffizienten vom Grad $q-1$ handelt. Wir können nun die Gleichung (5.15) umschreiben in $f(\zeta) \equiv 0 \,(\mathrm{mod}\, q)$.

Wir haben somit $f(\zeta^\sigma) \equiv 0 \,(\mathrm{mod}\, q)$ für alle $\sigma \in G$. Sei nun $\mathfrak{q}$ ein Primideal von O_K, das q enthält, dann erhalten wir $p-1$ Kongruenzen

$$f(\zeta^\sigma) \equiv 0 \,(\mathrm{mod}\, \mathfrak{q}). \tag{5.16}$$

Nun wissen wir aber, dass für zwei verschiedene $\sigma, \tau \in G$ gilt $\zeta^\sigma - \zeta^\tau \in (p) = (1-\zeta)$, und da jedes Primideal von O_K jeweils nur eine Primzahl enthält folgt daher $\zeta^\sigma - \zeta^\tau \not\equiv 0 \,(\mathrm{mod}\, \mathfrak{q})$, also $\zeta^\sigma \not\equiv \zeta^\tau \,(\mathrm{mod}\, \mathfrak{q})$.
Es muss daher der Grad des Polynoms $f(T)$ größer oder gleich der Anzahl der Kongruenzen aus (5.16) sein, also $q-1 \geq p-1$, was aber im Widerspruch zu unserer Voraussetzung $p > q$ steht. □

Nun haben wir alle Voraussetzungen geschaffen um den folgenden Satz von Mihailescu zu zeigen, der Gewissheit über die Richtigkeit von Catalans Vermutung brachte.

Satz 5.6.2 (Mihailescu)
Die Gleichung

$$x^p - y^q = 1$$

besitzt keine Lösung mit $x, y \in \mathbb{Z} \setminus \{0\}$ *und ungeraden Primzahlen* p, q.

Beweis. Wie wir bereits am Anfang dieses Kapitels gezeigt haben, dürfen wir davon ausgehen, dass $p \nmid q - 1$ und $q \nmid p - 1$, einen Beweis dafür geben wir in Kapitel 6. Wir dürfen also die Erkenntnisse aus den Unterkapiteln 5.2 und 5.3 anwenden.

Sei nun (x, y, p, q) eine Lösung, dann dürfen wir weiters $p > q$ voraussetzen, da wir im Fall $q > p$ mit $(-y, -x, q, p)$ anstelle von (x, y, p, q) weiterarbeiten können. Wegen Korollar 6.3.2 dürfen wir weiters auch von $q \geq 7$ ausgehen[2]. Es sind also alle Voraussetzungen der Sätze 5.4.1 und 5.6.1 sowie von Korollar 5.5.7 erfüllt.

Aus Satz 5.4.1 und Korollar 5.5.7 folgt, dass alle geraden Elemente aus $I_1 I_3$ mit Gewicht 0 gleich 0 sind, also

$$(1 + \iota)(\mathcal{N})^{\perp} I_1 I_3 = (0),$$

wobei $(\mathcal{N})^{\perp}$ laut Lemma 5.3.1 das Augmentationsideal von $\mathbb{F}_q[G]$ ist. Daraus folgt nun mit Lemma 5.2.2(iii) und (iv) sowie abermals Lemma 5.3.1 und Satz 5.3.3

$$I_1 I_3 \subseteq \left((1 + \iota)(\mathcal{N})^{\perp}\right)^{\perp} = (1 + \iota)^{\perp} + (\mathcal{N}) = (1 - \iota) + (\mathcal{N}) = I_1 I_2 I_3. \tag{5.17}$$

Andererseits sind laut Satz 5.3.3 I_2 und $I_1 I_3$ teilerfremd, also folgt aus (5.17) weiter

$$1 \in I_2 + I_1 I_3 \subseteq I_2 + I_1 I_2 I_3 = I_2,$$

also $I_2 = (1) = \mathbb{F}_q[G]$. Da jedoch laut Definition $I_2 = \operatorname{ann}_{\mathbb{F}_q[G]}(C/C_q)$ ist, folgt daher $C/C_q = \{0\}$. Also $C = C_q$, was im Widerspruch steht zu Satz 5.6.1. □

[2] Mihailescu verweist an dieser Stelle auf (5.2).

Kapitel 6

Ein algebraischer Beweis für den Fall $p \mid q-1$ oder $q \mid p-1$

In seinem Beweis der Catalan'schen Vermutung aus 2002 verwendete Mihailescu noch analytische Methoden aus der Theorie der Linearformen von Logarithmen, verwies auf das Ergebnis von Tijdeman sowie auf computerunterstützte Berechnungen um diesen Fall zu behandeln. Mihailescu setzte seine Arbeit an der Catalan'schen Vermutung jedoch fort, mit dem Ziel auch für diesen Fall einen unabhängigen Beweis zu finden.

Bereits 1999 hatten Bugeaud und Hanrot in [10] ein Kriterium bewiesen, wonach für eine Lösung (x, y, p, q) der Catalan'schen Gleichung mit $q > p$, der Exponent q die relative Klassenzahl $h^-(\mathbb{Q}(\zeta_p))$ teilen muss.

Obwohl Mihailescu in seinem Beweis dieses Kriterium nicht verwendete, war es für ihn eine Anregung. Er modifizierte die Argumente von Bugeaud und Hanrot und schaffte es so in [51] einen eigenständigen Beweis für diesen Fall des Catalan'schen Problems zu finden, der weder Tijdemans Resultat noch Linearformen von Logarithmen benutzt und auch keine Computerberechnungen mehr benötigt, sondern rein auf der Theorie der Kreisteilungskörper beruht und abermals den Satz von Stickelberger verwendet.

In diesem Kapitel geben wir nun diesen Beweis für den Fall $p \mid q-1$ oder $q \mid p-1$ wieder. Dabei halten wir uns an die Version von Yuri Bilu, der in [8] auch diesen Beweis von Mihailescu überarbeitete und noch vereinfachen konnte. Bilus Version des Beweises beinhaltet weiters einen Beweis für das Kriterium von Bugeaud und Hanrot.

6.1 Notationen und Vorarbeiten

In diesem Unterkapitel halten wir wieder zunächst die generellen Notationen für dieses Kapitel fest und sammeln einige Fakten, die wir im weiteren Verlauf des Kapitels benötigen.

In diesem Kapitel seien p, q jeweils zwei verschiedene ungerade Primzahlen.

Wir betrachten wiederum den p-ten Kreisteilungskörper $K := \mathbb{Q}(\zeta)$, wobei ζ die primitive p-te Einheitswurzel $\zeta := \mathrm{e}^{\frac{2\pi i}{p}}$ sei, und $G := Gal(K|\mathbb{Q})$ die Galoisgruppe von K. Wir verwenden wieder die Notation σ_a für jenes Element von G, für das $\sigma_a(\zeta) = \zeta^a$ gilt, und bezeichnen mit $\iota := \sigma_{p-1}$ die komplexe Konjugation.

Nun betrachten wir den Gruppenring $\mathbb{Z}[G]$. Sei im Folgenden $\Theta := \sum_{\sigma\in G} m_\sigma \sigma \in \mathbb{Z}[G]$, dann definieren wir die Größenfunktion auf $\mathbb{Z}[G]$ wie folgt:

Definition 63
*Es heißt $\|\Theta\|$ die **Größe** von Θ, sie ist folgt definiert:*

$$\|\Theta\| := \sum_{\sigma\in G} |m_\sigma|$$

Für die Größenfunktion gelten die folgenden Ungleichungen:

$$\|\Theta_1\Theta_2\| \le \|\Theta_1\| \cdot \|\Theta_2\| \quad \text{und} \quad \|\Theta_1 + \Theta_2\| \le \|\Theta_1\| + \|\Theta_2\|.$$

Für nichtnegative Θ, also falls $m_\sigma \ge 0$ für alle $\sigma \in G$, gilt dann $\|\Theta\| = \omega(\Theta)$, wobei ω die Gewichtsfunktion ist.

Wir definieren weiters:

$$\Theta^+ := \sum_{\sigma\in G} \max\{m_\sigma, 0\} \quad \text{und} \quad \Theta^- := \sum_{\sigma\in G} \min\{m_\sigma, 0\}$$

Dann sind Θ^+ und Θ^- nichtnegativ, $\Theta = \Theta^+ - \Theta^-$ und $\|\Theta\| = \|\Theta^+\| + \|\Theta^-\|$.

Definition 64
*Sei I ein Ideal von $\mathbb{Z}[G]$, dann definieren wir den **augmentierten Teil** von I als*

$$I^{\mathrm{aug}} := \{\Theta \in I : \omega(\Theta) = 0\},$$

*den **Minus-Teil** von I als*

$$I^- := (1-\iota)I,$$

*und für $r > 0$ die **r-Kugel** von I als*

$$I(r) := \{\Theta \in I : \|\Theta\| \le r\}.$$

Wir definieren als nächstes die logarithmische Höhe eines algebraischen Elements, und betrachten deren für uns wichtige Eigenschaften:

Definition 65
*Sei α algebraisch über $\mathbb{Q}$ und K ein beliebiger Zahlkörper, der α enthält, dann definieren wir die **logarithmische Höhe** $\mathrm{h}(\alpha)$ wie folgt:*

$$\mathrm{h}(\alpha) := \frac{1}{[K:\mathbb{Q}]} \sum_{\nu\in M_K} [K_\nu : \mathbb{Q}_\nu] \log \max\{|\alpha|_\nu, 1\}.$$

Es zeigt sich, dass die Definition unabhängig von der Wahl des Zahlkörpers K ist, es ist also $\mathrm{h} : \overline{\mathbb{Q}} \to \mathbb{R}_{\geq 0}$ eine wohldefinierte Funktion. Man erkennt sofort folgende Eigenschaften:

$$\begin{aligned} \mathrm{h}(\alpha_1 + \cdots + \alpha_n) &\leq \mathrm{h}(\alpha_1) + \cdots + \mathrm{h}(\alpha_n) + \log n && (6.1) \\ \mathrm{h}(\alpha_1 \cdots \alpha_n) &\leq \mathrm{h}(\alpha_1) + \cdots + \mathrm{h}(\alpha_n) && (6.2) \\ \mathrm{h}(\alpha^m) &= |m|\mathrm{h}(\alpha) && (6.3) \end{aligned}$$

für beliebige $\alpha, \alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$ und $m \in \mathbb{Z}$. Für $\alpha \in \mathbb{Z}$ erkennt man $\mathrm{h}(\alpha) = \log|\alpha|$ und falls α eine Einheitswurzel ist gilt $\mathrm{h}(\alpha) = 0$.

Sei K ein Zahlkörper, dann folgt mit der bekannten Produktformel $\prod_{\nu \in M_K} |\alpha|_\nu^{[K_\nu:\mathbb{Q}_\nu]} = 1$ für jedes $\alpha \in K^\times$ die folgende Ungleichung:

$$\begin{aligned} \mathrm{e}^{-[K:\mathbb{Q}]\,\mathrm{h}(\alpha)} &= \prod_{\nu \in M_K} \max\{|\alpha|_\nu, 1\}^{-[K_\nu:\mathbb{Q}_\nu]} = \prod_{\nu \in M_K} \min\{|\alpha|_\nu, 1\}^{[K_\nu:\mathbb{Q}_\nu]} \\ &\leq \prod_{\nu \in V} |\alpha|_\nu^{[K_\nu:\mathbb{Q}_\nu]} \end{aligned}$$

für jede Teilmenge $V \subseteq M_K$. Also gilt für $K \subseteq \mathbb{C}$ insbesondere

$$|\alpha|^f \geq \mathrm{e}^{-[K:\mathbb{Q}]\,\mathrm{h}(\alpha)}, \tag{6.4}$$

wobei $f = 1$ für $K \subseteq \mathbb{R}$ und $f = 2$ sonst.

Aus der Produktformel folgt weiters folgende nützliche Identität:

$$\mathrm{h}\left(\frac{\alpha}{\beta}\right) = \frac{1}{[K:\mathbb{Q}]} \sum_{\nu \in M_K} [K_\nu : \mathbb{Q}_\nu] \log \max\{|\alpha|_\nu, |\beta|_\nu\} \tag{6.5}$$

für beliebige $\alpha \in K$ und $\beta \in K^\times$.

6.2 Das Mihailescu Ideal

Wie wir bereits in Kapitel 5 gesehen haben, ist eine der grundlegenden Eigenschaften einer Lösung (x, y, p, q) der Catalan'schen Gleichung die, dass $(x-\zeta)^\Theta$ eine q-te Potenz ist für bestimmte $\Theta \in \mathbb{Z}[G]$.
Bilu führt nun allgemein für die Elemente von $\mathbb{Z}[G]$, die diese Eigenschaft erfüllen, die folgende Definition ein:

Definition 66
*Das **Mihailescu Ideal** I_M besteht aus allen $\Theta \in \mathbb{Z}[G]$, sodass $(x-\zeta)^\Theta$ eine q-te Potenz ist. In Zeichen:*

$$I_M := \{\Theta \in \mathbb{Z}[G] \mid (x-\zeta)^\Theta \in (K^\times)^q\}$$

Es sei hier angemerkt, dass Bilu das Mihailescu Ideal für beliebige feste Primzahlen $p, q > 2$ und festes $x \in \mathbb{Z}$ definiert. Für die folgenden Ergebnisse in diesem Unterkapitel ist es also nicht notwendig, von einer Lösung der Catalan'schen Gleichung auszugehen.

Unser Ziel ist es in diesem Unterkapitel zu zeigen, dass für hinreichend großes $|x|$ der augmentierte Teil I_M^{aug} nur wenige Elemente kleiner Größe enthält.

Zunächst betrachten wir die algebraische Zahl $(x-\zeta)^\Theta$ und zeigen als erstes eine Abschätzung für ihre Höhe:

Lemma 6.2.1
Für beliebige $x \in \mathbb{Z}$ und $\Theta \in \mathbb{Z}[G]$ gilt

$$\mathrm{h}\left((x-\zeta)^\Theta\right) \leq \frac{\|\Theta\| + |\omega(\Theta)|}{2} \log(|x|+1).$$

Beweis. Wir schreiben $\Theta = \Theta^+ - \Theta^-$. Wir setzen $\alpha = (x-\zeta)^{\Theta^+}$ und $\beta = (x-\zeta)^{\Theta^-}$ in (6.5) ein und erhalten

$$\mathrm{h}\left((x-\zeta)^\Theta\right) = \frac{1}{[K:\mathbb{Q}]} \sum_{\nu \in M_K} [K_\nu : \mathbb{Q}_\nu] \log X_\nu,$$

wobei

$$X_\nu = \max\left\{ \left|(x-\zeta)^{\Theta^+}\right|_\nu, \left|(x-\zeta)^{\Theta^-}\right|_\nu \right\}.$$

Offensichtlich gilt

$$X_\nu \leq (|x|+1)^{\max\{\|\Theta^+\|, \|\Theta^-\|\}}$$

falls ν archimedisch ist und $X_\nu \leq 1$ falls ν nichtarchimedisch ist. Daraus folgt

$$\mathrm{h}\left((x-\zeta)^\Theta\right) \leq \left(\max\{\|\Theta^+\|, \|\Theta^-\|\}\right) \log(|x|+1).$$

Wegen

$$\max\{\|\Theta^+\|, \|\Theta^-\|\} = \frac{\|\Theta\| + |\omega(\Theta)|}{2}$$

folgt die Aussage des Lemmas. □

Als nächstes stellen wir fest, dass $(x-\zeta)^\Theta$ "nahe" an 1 ist, falls $\omega(\Theta) = 0$ ist. Im folgenden steht log für den Hauptzweig des komplexen Logarithmus, für den gilt:

$$-\pi < \mathrm{Im} \log z \leq \pi.$$

Lemma 6.2.2
Falls $|x| > 1$ und $\omega(\Theta) = 0$ ist, dann gilt $|\log(x-\zeta)^\Theta| \leq \frac{\|\Theta\|}{|x|-1}$.

Beweis. Für jede komplexe Zahl z mit $|z| < 1$ wissen wir

$$|\log(1+z)| \leq \frac{|z|}{1-|z|}.$$

Speziell gilt also

$$\left|\log\left(1 - \frac{\zeta^a}{x}\right)\right| \leq \frac{1}{|x|-1}.$$

Wegen $\omega(\Theta) = 0$ gilt $(x-\zeta)^\Theta = \left(1-\frac{\zeta}{x}\right)^\Theta$ und somit folgt die Aussage des Lemmas. □

Nun zeigen wir noch, dass $(x-\zeta)^\Theta$ unter gewissen Voraussetzungen ungleich 1 ist:

Lemma 6.2.3
Sei x eine ganze Zahl mit $|x| > 2$, und zusätzlich $x \neq 2$ falls $p = 3$, dann gilt $(x-\zeta)^\Theta \neq 1$ für alle $\Theta \in \mathbb{Z}[G] \setminus \{0\}$.

Beweis. Sei $\mathfrak{p}$ das Primideal von O_K, das über p liegt, dann wissen wir, dass $\mathfrak{p}^{p-1} = (p)$ und $\mathfrak{p} = (\zeta^\sigma - \zeta^\tau)$ für je zwei verschiedene $\sigma, \tau \in G$ gilt. Speziell gilt für verschiedene σ und τ:

$$(x-\zeta^\sigma, x-\zeta^\tau) \mid \mathfrak{p}. \tag{6.6}$$

Angenommen $(x-\zeta)$ habe keinen anderen Primidealteiler als $\mathfrak{p}$, also $(x-\zeta) = \mathfrak{p}^k$, aus (6.6) folgt dann $k \leq 1$. Wir betrachten nun die relative Norm $\mathrm{N}_{\mathbb{Q}}^K(x-\zeta) = \mathrm{N}_{\mathbb{Q}}^K(\mathfrak{p}^k) = (p^k)$. Wir wissen, dass für die Norm des Elements $x-\zeta$ gilt $\mathrm{N}_{\mathbb{Q}}^K(x-\zeta) = \Phi_p(x)$, wobei

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + 1$$

das p-te Kreisteilungspolynom ist. Es folgt also $\Phi_p(x) = p^k \in \{\pm 1, \pm p\}$.

Andererseits gilt offensichtlich

$$|\Phi_p(x)| \geq 2^{p-2} > p$$

für $p \geq 5$ und $|x| \geq 2$, beziehungsweise $|\Phi_3(x)| > 3$ für $|x| \geq 3$ oder $x = 2$, ein Widerspruch zu $\Phi_p(x) \in \{\pm 1, \pm p\}$!

Somit gibt es also einen von $\mathfrak{p}$ verschiedenen Primidealteiler $\mathfrak{q}$ von $(x-\zeta)$. Sei $l := \nu_{\mathfrak{q}}(x-\zeta)$, dann folgt aus (6.6):

$$\nu_{\mathfrak{q}^\sigma}(x-\zeta^\tau) = \begin{cases} l & \text{falls } \sigma = \tau \\ 0 & \text{falls } \sigma \neq \tau \end{cases}$$

Für ein beliebiges $\Theta = \sum_{\sigma \in G} m_\sigma \sigma \in \mathbb{Z}[G]$ erhalten wir also

$$\nu_{\mathfrak{q}^\sigma}\left((x-\zeta)^\Theta\right) = l m_\sigma \quad \forall \sigma \in G$$

Ist nun $(x-\zeta)^\Theta = 1$, dann folgt wegen $l \neq 0$ dass $m_\sigma = 0$ ist für alle $\sigma \in G$, also $\Theta = 0$. □

Wir betrachten nun die q-te Wurzel von $(x-\zeta)^\Theta$. Nach der Definition des Mihailescu Ideals existiert für jedes $\Theta \in I_M$ ein $\alpha \in K^\times$ sodass $\alpha^q = (x-\zeta)^\Theta$. Dieses α ist eindeutig, da K keine q-ten Einheitswurzeln (außer 1) enthält, wir schreiben daher $\alpha = \alpha(\Theta)$. Aus der Eindeutigkeit folgt weiters, dass $\alpha(\Theta_1 + \Theta_2) = \alpha(\Theta_1) \cdot \alpha(\Theta_2)$, für $\Theta_1, \Theta_2 \in I_M$. Die Abbildung $\alpha : I_M \to K^\times$ ist also ein Gruppenhomomorphismus.

Wir halten folgende Beobachtung fest:

Lemma 6.2.4
Sei $|x| \geq 2$ und $x \neq 2$ falls $p = 3$ ist, dann gilt für jedes $\Theta \in I_M \setminus \{0\}$, dass $\alpha(\Theta) \neq 1$, und weiters

$$\mathrm{h}(\alpha(\Theta)) \leq \frac{\|\Theta\| + \omega(\Theta)}{2q} \log(|x|+1).$$

Beweis. Die erste Aussage folgt direkt aus Lemma 6.2.3. Es gilt $q\mathrm{h}(\alpha(\Theta)) = \mathrm{h}\left((x-\zeta)^{\Theta}\right)$ laut (6.3) und mit Lemma 6.2.1 folgt die zweite Aussage. □

Es ist jedoch entscheidend, dass für $\Theta \in I_M^{\mathrm{aug}}$ die komplexe Zahl $\alpha(\Theta)$ nahe einer q-ten Einheitswurzel in $\mathbb{C}$ liegt. Genauer gilt folgendes Lemma:

Lemma 6.2.5
Sei $|x| \geq 2$ und weiters

$$r < \frac{\pi}{2}(|x|-1). \tag{6.7}$$

Dann existiert für jedes $\Theta \in I_M^{\mathrm{aug}}(2r)$ eine eindeutig bestimmte q-te Einheitswurzel $\xi = \xi(\Theta)$ sodass

$$\left|\log\left(\alpha(\Theta)\xi(\Theta)^{-1}\right)\right| \leq \frac{\|\Theta\|}{q(|x|-1)}.$$

Weiters gilt $\xi(-\Theta) = \xi(\Theta)^{-1}$ und für $\Theta_1, \Theta_2 \in I_M^{\mathrm{aug}}(r)$ gilt $\xi(\Theta_1+\Theta_2) = \xi(\Theta_1)\xi(\Theta_2)$. Die Abbildung $\xi : I_M^{\mathrm{aug}}(r) \to {\mu_q}^1$ ist also ein "lokaler Homomorphismus".

Beweis. Die Existenz von $\xi(\Theta)$ folgt aus Lemma 6.2.2. Für $\Theta \in I_M^{\mathrm{aug}}(2r)$ gilt

$$\|\Theta\| \leq 2r < \pi(|x|-1),$$

und es folgt

$$\left|\log\left(\alpha(\Theta)\xi(\Theta)^{-1}\right)\right| \leq \frac{\|\Theta\|}{q(|x|-1)} < \frac{\pi}{q}. \tag{6.8}$$

Für je zwei verschiedene $\xi_1, \xi_2 \in \mu_q$ gilt jedoch $\left|\log \xi_1\xi_2^{-1}\right| \geq \frac{2\pi}{q}$, woraus die Eindeutigkeit von $\xi(\Theta)$ folgt. Die lokale Homomorphiebedingung folgt wiederum aus der Eindeutigkeit. □

Nun zeigt Mihailescu die folgende Aussage über den augmentierten Teil von I_M:

Satz 6.2.6 (Mihailescu)
Sei ε eine reelle Zahl mit $0 < \varepsilon \leq 1$ und sei weiters

$$|x| \geq \max\left\{\left(\frac{36\cdot 2^{p-1}}{(p-1)^2}\right)^{\frac{1}{\varepsilon}}, \frac{4}{\pi}\frac{q}{p-1}+1\right\}. \tag{6.9}$$

Setzt man $r := (2-\varepsilon)\frac{q}{p-1}$, dann gilt

$$|I_M^{\mathrm{aug}}(r)| \leq q.$$

Wir dürfen annehmen dass $q > p$, anderenfalls wäre $r < 2$ und die Aussage des Satzes trivialerweise erfüllt. Da p, q ungerade Primzahlen sind gilt also $q \geq 5$. Weiters folgt aus der Voraussetzung

$$|x| \geq \frac{4}{\pi}\frac{q}{p-1}+1,$$

dass

$$r < 2\frac{q}{p-1} \leq \frac{\pi}{2}(|x|-1).$$

[1] Mit μ_q bezeichnen wir die Gruppe der q-ten Einheitswurzeln.

Es ist also die Bedingung (6.7) aus Lemma 6.2.5 erfüllt und somit gibt es zu jedem $\Theta \in I_M^{\text{aug}}(2r)$ eine eindeutig bestimmte q-te Einheitswurzel $\xi(\Theta)$.

Um den Beweis etwas zu vereinfachen formulieren wir folgendes Lemma:

Lemma 6.2.7
Unter den Voraussetzungen des Satzes 6.2.6 sei $\Theta \in I_M^{\text{aug}}(2r)$ mit $\xi(\Theta) = 1$, dann gilt $\Theta = 0$.

Beweis. Wir betrachten ein festes $\Theta \in I_M^{\text{aug}}(2r) \setminus \{0\}$ mit $\xi(\Theta) = 1$ und setzen $\alpha := \alpha(\Theta)$. Da Θ aus dem augmentierten Teil von I_M ist gilt natürlich $\omega(\Theta) = 0$.

Zunächst folgern wir 2 Ungleichungen: Aus der Abschätzung aus Lemma 6.2.4 erhält man mit (6.1)

$$\mathrm{h}(\alpha - 1) \leq \frac{\|\Theta\|}{2q} \log(|x| + 1) + \log 2, \tag{6.10}$$

und aus der Gleichung (6.8) folgt

$$|\log \alpha| \leq \frac{\|\Theta\|}{q(|x| - 1)} < \frac{\pi}{q} \leq \frac{\pi}{5}, \tag{6.11}$$

wegen $q \geq 5$.

Wir betrachten nun die komplexe Funktion $\mathrm{e}^z - 1$ für $|z| \leq s$. Aus der Dreiecksungleichung folgt

$$|\mathrm{e}^z - 1| = \left| z + \frac{z^2}{2!} + \frac{z^3}{3!} + \cdots \right| \leq s + \frac{s^2}{2!} + \frac{s^3}{3!} + \cdots = \mathrm{e}^s - 1.$$

Das Lemma von Schwarz[2] impliziert

$$|\mathrm{e}^z - 1| \leq \frac{\mathrm{e}^s - 1}{s} |z|.$$

Nimmt man nun $s = \frac{\pi}{5}$ so erkennt man leicht, dass $|\mathrm{e}^z - 1| \leq 1.4|z|$ gilt. Damit folgt aus (6.11):

$$|\alpha - 1| \leq 1.4 |\log \alpha| \leq 1.4 \frac{\|\Theta\|}{q(|x| - 1)}. \tag{6.12}$$

Die Ungleichung aus (6.4) für die, laut Lemma 6.2.4 von 0 verschiedene, algebraische Zahl $\alpha - 1$ lautet nun $|\alpha - 1|^2 \geq \mathrm{e}^{-(p-1)\mathrm{h}(\alpha-1)}$. Wir setzen in diese Ungleichung nun die zuvor erhaltenen Abschätzungen für $|\alpha - 1|$ aus (6.12) und für $\mathrm{h}(\alpha - 1)$ aus (6.10) ein und erhalten

$$2 \left(\log(|x| - 1) - \log \frac{1.4\|\Theta\|}{q} \right) \leq (p - 1) \left(\frac{\|\Theta\|}{2q} \log(|x| + 1) + \log 2 \right),$$

was wir umschreiben können zu

$$\left(2 - \frac{p-1}{2q} \|\Theta\| \right) \log |x| \leq \begin{array}{l} 2 \log \frac{1.4\|\Theta\|}{q} + 2 \log \frac{|x|}{|x|-1} \\ + \frac{p-1}{2q} \|\Theta\| \log \frac{|x|+1}{|x|} + (p-1) \log 2. \end{array} \tag{6.13}$$

[2] Das Lemma von Schwarz besagt, dass für eine holomorphe Funktion f auf der komplexen Einheitskreisscheibe die $f(z) \leq 1$ für alle z und $f(0) = 0$ erfüllt, gilt dass $|f(z)| \leq |z|$ für alle z. In unserem Fall betrachten wir die Funktion $f\left(\frac{z}{s}\right) = \frac{\mathrm{e}^z - 1}{\mathrm{e}^s - 1}$.

Laut Voraussetzung gilt

$$\frac{p-1}{2q}\|\Theta\| \leq \frac{p-1}{2q}2r = 2-\varepsilon < 2.$$

Nun ersetzen wir $\frac{p-1}{2q}\|\Theta\|$ durch $2-\varepsilon$ in der linken Seite von (6.13) und durch 2 in der rechten Seite und erhalten

$$\varepsilon \log|x| \leq 2\log\frac{5.6}{p-1} + 2\log\frac{|x|+1}{|x|-1} + (p-1)\log 2.$$

Wegen der Voraussetzung (6.9) gilt $|x| \geq 36$ und damit folgt

$$\varepsilon \log|x| \leq 2\log\frac{5.6}{p-1} + 2\log\frac{37}{35} + (p-1)\log 2 < \log 36\frac{2^{p-1}}{(p-1)^2},$$

was einen Widerspruch zu (6.9) darstellt! Es muss also $\Theta = 0$ gelten. □

Nun ist der Beweis von Satz 6.2.6 einfach:

Beweis von Satz 6.2.6. Seien $\Theta_1, \Theta_2 \in I_M^{\text{aug}}(r)$ mit $\xi(\Theta_1) = \xi(\Theta_2)$. Dann folgt aus der lokalen Homomorphiebedingung aus Lemma 6.2.5 dass $\xi(\Theta_1 - \Theta_2) = 1$ ist und aus dem eben gezeigten Lemma 6.2.7 folgt nun $\Theta_1 - \Theta_2 = 0$.
Somit ist die Abbildung $\xi : I_M^{\text{aug}}(r) \to \mu_q$ also injektiv, woraus die Aussage des Satzes folgt. □

Satz 6.2.6 impliziert, dass $|I_M^{\text{aug}}(2)| \leq q$ falls $p \leq (1-\frac{\varepsilon}{2})q + 1$ und wenn (6.9) erfüllt ist. Bugeaud und Hanrot verwendeten anstelle von (6.9) eine etwas stärkere Voraussetzung und konnten damit auch eine entsprechend stärkere Aussage zeigen.

Satz 6.2.8 (Bugeaud und Hanrot)
Sei $p \leq (2-\varepsilon)q + 1$, wobei $0 < \varepsilon \leq 1$, und sei weiters

$$|x| \geq \max\left\{\left(\frac{36\cdot 2^{p-1}}{(p-1)^2}\right)^{\frac{1}{\varepsilon}}, 8\left(0.8q(p')^{\frac{1}{p-1}}\right)^q\right\}, \tag{6.14}$$

wobei $p' = 1$ falls $x \equiv 1 \pmod p$ und $p' = p$ sonst. Dann gilt

$$|I_M^{\text{aug}}(2)| = \{0\}.$$

Beweis. Sei $\Theta \in I_M^{\text{aug}}$ mit $\|\Theta\| = 2$ und $\alpha := \alpha(\Theta)$. Aus Lemma 6.2.7 folgt, dass $\xi(\sigma\Theta) \neq 1$ ist für alle $\sigma \in G$. Ebenfalls gilt $|\arg(\alpha^\sigma)| \geq \frac{\pi}{q}$ für alle $\sigma \in G$, woraus $|\alpha^\sigma - 1| > \sin\left(\frac{\pi}{q}\right)$ für alle $\sigma \in G$ folgt. Anders ausgedrückt gilt

$$|\alpha - 1|_\nu > \sin\left(\frac{\pi}{q}\right) > \frac{2.5}{q}$$

für alle archimedischen Beträge ν.

Sei nun $\Theta := \sigma_1 - \sigma_2$, wobei σ_1, σ_2 verschiedene Elemente von G sind, und $\zeta_i := \zeta^{\sigma_i}$. Angenommen $|\alpha - 1|_\nu < 1$ für ein nichtarchimedisches ν, dann gilt $|\alpha^q - 1|_\nu \leq |\alpha - 1|_\nu < 1$. Es gilt jedoch

$$\alpha^q - 1 = (x - \zeta)^\Theta - 1 = \frac{\zeta_2 - \zeta_1}{x - \zeta_2}.$$

Wir wissen $\zeta_2 - \zeta_1$ teilt $x - \zeta_2$ genau dann, wenn $x \equiv 1 \,(\mathrm{mod}\, p)$. Wir schließen weiters dass $|\alpha - 1|_\nu \geq 1$ für alle nichtarchimedischen ν falls $x \equiv 1 \,(\mathrm{mod}\, p)$, und

$$|\alpha - 1|_\nu \geq |\zeta_2 - \zeta_1|_\nu = |p|_\nu^{\frac{1}{p-1}}$$

für alle nichtarchimedischen ν falls $x \not\equiv 1 \,(\mathrm{mod}\, p)$.

Wir haben gezeigt, dass

$$\left|(\alpha - 1)^{-1}\right|_\nu < 0.4q$$

falls ν archimedisch ist, und

$$\left|(\alpha - 1)^{-1}\right|_\nu \leq |p'|_\nu^{-\frac{1}{p-1}}$$

falls ν nichtarchimedisch ist. Es folgt

$$\mathrm{h}(\alpha - 1) = \mathrm{h}\left((\alpha - 1)^{-1}\right) < \log 0.4q + \frac{\log p'}{p-1} = \log 0.4q(p')^{\frac{1}{p-1}}$$

und

$$\mathrm{h}(\alpha) \leq \mathrm{h}(\alpha - 1) + \log 2 < \log 0.8q(p')^{\frac{1}{p-1}}$$

Durch elementares Umformen und Anwenden der Regeln (6.1) - (6.3) erhalten wir

$$\begin{aligned} \log|x| &= \mathrm{h}(x) = \mathrm{h}\left(\frac{\zeta_2 - \zeta_1}{\alpha^q - 1} + \zeta_2\right) \leq q\mathrm{h}(\alpha) + 3\log 2 \\ &< \log 8\left(0.8q(p')^{\frac{1}{p-1}}\right)^q, \end{aligned}$$

was einen Widerspruch zu (6.14) darstellt! □

Wir streichen in einem Korollar noch den Spezialfall $\varepsilon = 1$ und $x \equiv 1 \,(\mathrm{mod}\, p)$ heraus:

Korollar 6.2.9
Sei $p < q$, sei $x \equiv 1 \,(\mathrm{mod}\, p)$ und sei weiters $|x| \geq 8(0.8q)^q$. Dann gilt

$$I_M^{\mathrm{aug}} = \{0\}.$$

Beweis. Wie man leicht sieht, gilt $0.8q > 2$ und $16 > \frac{36}{(p-1)^2}$. Zusammen ergibt sich

$$8(0.8q)^q > 16 \cdot 2^{q-1} > \frac{36 \cdot 2^{p-1}}{(p-1)^2}$$

für $q > p$. Die Aussage des Korollars folgt nun direkt aus Satz 6.2.8. □

6.3 Das Kriterium von Bugeaud und Hanrot

Im Gegensatz zur logarithmischen Höhe h steht im Folgenden h für die Klassenzahl!

Wir rufen uns zunächst ein paar Definitionen in Erinnerung: Mit K bezeichnen wir weiterhin den p-ten Kreisteilungskörper $\mathbb{Q}(\zeta)$, wobei ζ für die p-te Einheitswurzel $\mathrm{e}^{\frac{2\pi i}{p}}$ steht. Mit K^+ bezeichnen wir den maximalen reellen Unterkörper von K, also $K^+ = K \cap \mathbb{R}$. Seien H und H^+ die Idealklassengruppen von K beziehungsweise K^+, dann lässt sich H^+ in H einbetten und man definiert die relative Klassenzahl h^- von K als den Index $[H : H^+]$. Für $h^-(K)$ schreibt man oft auch $h^-(p)$.

Nun können wir das folgende Kriterium von Bugeaud und Hanrot zeigen.

Satz 6.3.1 (Kriterium von Bugeaud und Hanrot)
Sei (x, y, p, q) eine Lösung der Catalan'schen Gleichung $x^p - y^q = 1$, mit ungeraden Primzahlen $q > p$, dann gilt

$$q \mid h^-(p).$$

Beweis. Wir nehmen an, dass $q \nmid h^-(p)$ und werden dies auf einen Widerspruch führen.

Dazu sei $\lambda := \frac{x-\zeta}{1-\zeta}$, Lemma 4.2.5 besagt dann, dass $(\lambda) = A^q$ ist für ein Ideal A von K. Die Idealklasse von A gehört also zur q-Komponente von H. Da q laut unserer Annahme die relative Klassenzahl $h^-(K)$ nicht teilt ist die q-Komponente von H in H^+ enthalten. Es gibt also eine Einheit $\alpha \in K^\times$ und ein Ideal B von K^+ sodass $A = \alpha B$. Da B^q ein Hauptideal ist, gibt es ein $\beta \in K^+$ mit $(\beta) = B$. Es gilt dann $\lambda = \varepsilon \alpha^q \beta$, wobei ε eine Einheit von K ist.

Wir wissen, dass jede Einheit von K eine reelle Einheit mal einer Einheitswurzel ist. Da die Einheitswurzeln in K auch q-te Potenzen in K sind, gibt es daher $\alpha' \in K$ und $\beta' \in K^+$ mit $\lambda = \alpha'^q \beta'$.

Wir betrachten nun $(x-\zeta)^{1-\iota}$, wobei $\iota = \sigma^{p-1} \in G$ die komplexe Konjugation bezeichnet, und rufen uns in Erinnerung, dass $\frac{1-\zeta}{1-\overline{\zeta}}$ eine Einheitswurzel, und somit eine q-te Potenz in K ist. Es gilt

$$(x-\zeta)^{1-\iota} = \frac{x-\zeta}{x-\overline{\zeta}} = \frac{1-\zeta}{1-\overline{\zeta}} \cdot \frac{\lambda}{\overline{\lambda}} = \frac{1-\zeta}{1-\overline{\zeta}} \left(\frac{\alpha'}{\overline{\alpha'}}\right)^q \in \left(K^\times\right)^q.$$

In anderen Worten, $1-\iota$ ist ein Element des Mihailescu Ideals I_M von K.

Nach dem Satz von Cassels (Korollar 4.1.6) gilt jedoch $x \equiv 1 \pmod p$ und mit der Abschätzung von Hyyrö (Satz 4.1.7) gilt weiters

$$|x| \geq p^{q-1}(q-1)^q + 1 > 8(0.8q)^q.$$

Es sind also alle Voraussetzungen von Korollar 6.2.9 erfüllt und wir können schließen, dass I_M kein Element mit Gewicht 0 und Größe 2 enthält.

Es gilt jedoch offensichtlich $\|1-\iota\| = 2$ und $\omega(1-\iota) = 0$, Widerspruch! □

Zur Berechnung der relativen Klassenzahl $h^-(p)$ gibt es verschiedene Formeln (siehe beispielsweise [62] Theorem 4.17). Bereits Kummer berechnete $h^-(p)$ für $p < 100$. In einschlägiger Literatur findet man Tabellen für die relative Klassenzahl von Kreisteilungskörpern, siehe beispielsweise Washingtons Buch [62].

Mithilfe solcher Tabellen ist es nicht schwer nachzuprüfen, dass für $p \leq 41$ die relative Klassenzahl $h^-(p)$ keine Primteiler besitzt, die größer als p sind, somit gilt:

Korollar 6.3.2
Sei (x, y, p, q) eine Lösung der Catalan'schen Gleichung $x^p - y^q = 1$, dann gilt

$$p, q \geq 43.$$

Für unsere Zwecke ist es sogar ausreichend, zu wissen, dass $q \nmid h^-(p)$ für $p \leq 7$ und $q > p$, was man anhand der Tabelle sofort erkennt, da $h^-(p) = 1$ für $p \leq 19$.

6.4 Der Minus-Teil des Stickelbergerideals

Wir untersuchen in diesem Unterkapitel den Minus-Teil des Stickelbergerideals I_S von $\mathbb{Z}[G]$. Unser Ziel ist es eine untere Schranke für die Anzahl der in dem Minus-Teil enthaltenen Elemente von beschränkter Größe anzugeben.

Wir rufen uns in Erinnerung (Lemma 2.10.1), dass das Stickelbergerideal I_S erzeugt wird von den Elementen

$$\Theta_k := (k - \sigma_k)\theta \quad ggT(k, p) = 1$$

wobei

$$\theta := \sum_{a=1}^{p-1} \frac{a}{p} \, {\sigma_a}^{-1}$$

das Stickelbergerelement ist.

Der Minus-Teil des Stickelbergerideals ist definiert als $I_S^- := (1 - \iota)I_S$. Wir zeigen folgenden Satz:

Satz 6.4.1
Es gibt eine $\mathbb{Z}$-Basis $\theta_1, \ldots, \theta_{\frac{p-1}{2}}$ von $(1 - \iota)I_S$, die

$$\|\theta_k\| \leq p - 1$$

für $K = 1, \ldots, \frac{p-1}{2}$ erfüllt.

Beweis. Zuerst bestimmen wir den $\mathbb{Z}$-Rang von $I_S^- = (1 - \iota)I_S$. Offensichtlich ist der $\mathbb{Z}$-Rang von $\mathbb{Z}[G]$ gleich $p - 1$. Für $\sigma_k \in G$ gilt $\iota\sigma_k = \sigma_{p-k}$ und wir haben $(1 - \iota)\sigma_k = \sigma_k - \sigma_{p-k}$ und $(1 - \iota)\sigma_{p-k} = \sigma_{p-k} - \sigma_k$. Somit ist

$$\left\{ \sigma_k - \sigma_{p-k} \mid k = 1, \ldots, \frac{p-1}{2} \right\}$$

eine $\mathbb{Z}$-Basis von $\mathbb{Z}[G]^-$ und der $\mathbb{Z}$-Rang von $\mathbb{Z}[G]^-$ ist daher $\frac{p-1}{2}$. Aus dem Satz von Iwasawa (Satz 2.10.3) folgt, dass der Index $[\mathbb{Z}[G]^- : I_S^-]$ endlich ist, und daher ist der $\mathbb{Z}$-Rang von I_S^- ebenfalls $\frac{p-1}{2}$.

I_S wird von allen Θ_k mit $ggT(k,p)=1$ erzeugt. Laut (4.22) ist $\Theta_k = \sum_{a=1}^{p-1} \left\lfloor \frac{ka}{p} \right\rfloor {\sigma_a}^{-1}$ Wegen

$$\begin{aligned}\Theta_k + p\theta &= \sum_{a=1}^{p-1} \left\lfloor \frac{ka}{p} \right\rfloor {\sigma_a}^{-1} + p\sum_{a=1}^{p-1} \frac{a}{p} {\sigma_a}^{-1} = \sum_{a=1}^{p-1} \left(\left\lfloor \frac{ka}{p} \right\rfloor + a \right) {\sigma_a}^{-1} \\ &= \sum_{a=1}^{p-1} \left\lfloor \frac{ka}{p} + a \right\rfloor {\sigma_a}^{-1} = \sum_{a=1}^{p-1} \left\lfloor \frac{(k+p)a}{p} \right\rfloor {\sigma_a}^{-1} \\ &= \Theta_{k+p}\end{aligned}$$

ist $\{\Theta_1, \ldots, \Theta_{p-1}, p\theta\}$ ein $\mathbb{Z}$-Erzeugendensystem von I_S. Wegen

$$\begin{aligned}\Theta_k(1-\iota) + \Theta_{p-k}(1-\iota) &= (k-\sigma_k)\theta(1-\iota) + (p-k-\sigma_{p-k})\theta(1-\iota) \\ &= \theta(p(1-\iota) - \sigma_k + \sigma_{p-k} - \sigma_{p-k} + \sigma_k) \\ &= p\theta(1-\iota)\end{aligned}$$

wird das Ideal I_S^- über $\mathbb{Z}$ erzeugt von

$$\{\Theta_k(1-\iota) \mid k = 1, \ldots, \frac{p+1}{2}\}.$$

Da $\Theta_1 = 0$ wird I_S^- bereits erzeugt von $\theta_1, \ldots, \theta_{\frac{p-1}{2}}$, wobei

$$\theta_k := (\Theta_{k+1} - \Theta_k)(1-\iota).$$

Da der $\mathbb{Z}$-Rang von I_S^- gleich $\frac{p-1}{2}$ ist, ist $\{\theta_1, \ldots, \theta_{\frac{p-1}{2}}\}$ eine $\mathbb{Z}$-Basis von I_S^-.
Nun müssen wir noch die Größe der θ_k bestimmen. Zunächst berechnen wir

$$\omega(\theta) = \sum_{a=1}^{p-1} \frac{a}{p} = \frac{1}{p} \sum a = 1^{p-1} a = \frac{1}{p} \frac{p(p-1)}{2} = \frac{p-1}{2}.$$

Da die Gewichtsfunktion multiplikativ ist gilt

$$\omega(\Theta_k) = \omega(k-\sigma_k)\omega(\theta) = (k-1)\frac{p-1}{2}.$$

Nun wissen wir, dass $\Theta_k = \sum_{a=1}^{p-1} \left\lfloor \frac{ka}{p} \right\rfloor {\sigma_a}^{-1}$. Es sind somit alle Koeffizienten in $\Theta_{k+1} - \Theta_k$ größer oder gleich 0. Folglich gilt

$$\|\Theta_{k+1} - \Theta_k\| = \omega(\Theta_{k+1} - \Theta_k) = \frac{p-1}{2}.$$

Und damit gilt für die Größe der θ_k:

$$\|\theta_k\| = \|(\Theta_{k+1} - \Theta_k)(1-\iota)\| \leq \|\Theta_{k+1} - \Theta_k\| \cdot \|1-\iota\| = p-1.$$

□

Wir definieren

Definition 67
Sei n eine positive ganze Zahl und r eine positive reelle Zahl, dann bezeichnen wir mit $S(n,r)$ die Anzahl der Punkte $(x_1,\ldots,x_n) \in \mathbb{Z}^n$ für die $|x_1|+\cdots+|x_n| \leq r$ gilt. In Zeichen:

$$S(n,r) := \left|\{(x_1,\ldots,x_n) \in \mathbb{Z}^n : |x_1|+\cdots+|x_n| \leq r\}\right|.$$

Als direkte Konsequenz aus Satz 6.4.1 ergibt sich nun die folgende Abschätzung für die Anzahl der Elemente in I_S^-:

Korollar 6.4.2
Sei r eine positive ganze Zahl, dann enthält das Ideal I_s^- mindestens $S\left(\frac{p-1}{2}, \frac{r}{p-1}\right)$ Elemente deren Größe r nicht übersteigt. In Zeichen:

$$\left|\{\Theta \in I_S^- : \|\Theta\| \leq r\}\right| \geq S\left(\frac{p-1}{2}, \frac{r}{p-1}\right).$$

Wir benötigen nun noch eine qualitative Aussage für die Anzahl $S(n,r)$. Für den ganzzahligen Fall $r = k \in \mathbb{Z}$ findet sich folgendes Lemma in [32]:

Lemma 6.4.3
Für positive ganzzahlige n, k gilt

$$S(n,k) = \sum_{j=0}^{n} 2^j \binom{n}{j}\binom{k}{j}.$$

Beweis. Als erstes sehen wir, dass aus der Definition von $S(n,k)$ folgende Rekursionsgleichung folgt:

$$S(n,k) = S(n-1,k) + 2\sum_{j=1}^{k-1} S(n-1,j), \quad S(0,r) := 0. \tag{6.15}$$

Wobei hier der erste Term auf der rechten Seite alle Punkte $(x_1,\ldots,x_n)$ mit $x_n = 0$ und $\sum_{I=1}^{n-1}|x_i| \leq k$ zählt, und im zweiten Term $2S(n-1,j)$ jene mit $x_n = \pm(k-j)$ sodass $\sum_{I=1}^{n-1}|x_i| \leq j$ gelten muss.

Wir definieren eine doppelte erzeugende Funktion als die (formale) Potenzreihe

$$P(z,u) := \sum_{n,k\geq 0} S(n,k) z^k u^n.$$

Nach der Rekursionsgleichung (6.15) gilt

$$P(z,u) - \sum_{k\geq 0} S(0,k) z^k = uP(z,u) + 2zu \sum_{k,n\geq 0} z^k u^n \sum_{j=1}^{k} S(n,j)$$

also

$$P(z,u) - \frac{1}{1-z} = uP(z,u) + \frac{2zu}{1-z} P(z,u).$$

Durch Umformen erhalten wir daraus:

$$P(z,u) = \frac{1}{1-z-u-zu}. \tag{6.16}$$

Laut Definition gilt $S(n,k) = [z^k u^n]P(z,u)$, wobei $[z^k u^n]P(z,u)$ für den Koeffizienten von $z^k u^n$ in $P(z,u)$ steht. Wir berechnen nun aus (6.16) zuerst den Koeffizienten von z^k in $P(z,u)$:

$$[z^k]P(z,u) = [z^k]\frac{1}{1-u} \cdot \frac{1}{1-\frac{z(u+1)}{u-1}} = \frac{(1+u)^k}{(1-u)^{k+1}}.$$

Wir können nun weiter umformen:

$$\begin{aligned}\frac{(1+u)^k}{(1-u)^{k+1}} &= \frac{1}{1-u}\left(1+\frac{2u}{1-u}\right)^k = \sum_{j\geq 0}\binom{k}{j}2^j\frac{u^j}{(1-u)^{j+1}} \\ &= \sum_{j\geq 0}\binom{k}{j}2^j\sum_{n\geq 0}\binom{n+j}{n}u^{n+j} = \sum_{j\geq 0}\binom{k}{j}2^j\sum_{n\geq j}\binom{n}{j}u^n\end{aligned}$$

Aus $S(n,r) = [z^k u^n]P(z,u)$ folgt nun schließlich

$$S(n,k) = [u^n]\frac{(1+u)^k}{(1-u)^{k+1}} = \sum_{j\geq 0}2^j\binom{n}{j}\binom{k}{j}.$$

□

6.5 Abschluss des Beweises

In diesem Unterkapitel führen wir die bisher in diesem Kapitel gezeigten Ergebnisse zusammen um damit die Catalan'sche Vermutung für den Fall $p \mid q-1$ oder $q \mid p-1$ zu zeigen.

Dazu zeigen wir zuerst folgendes Lemma, das eine Verbindung zwischen dem Stickelberger- und dem Mihailescuideal herstellt:

Lemma 6.5.1
Sei (x,y,p,q) eine Lösung der Catalan'schen Gleichung $x^p - y^q = 1$ mit ungeraden Primzahlen p,q, dann gilt:

$$I_S^- \subset I_M.$$

Beweis. Wir müssen zeigen, dass für jedes $\Theta \in (1-\iota)I_S$ das Element $(x-\zeta)^\Theta$ eine q-te Potenz in K ist.
Sei Θ nun ein beliebiges Element von I_S^-, dann gilt $\Theta = (1-\iota)\Theta'$ für ein $\Theta' \in I_S$. Sei $\lambda := \frac{x-\zeta}{1-\zeta}$, dann folgt aus Lemma 4.2.5, dass es ein Ideal A von O_K gibt, sodass $(\lambda) = A^q$.

Aus dem Satz von Stickelberger folgt, dass $A^{\Theta'}$ ein Hauptideal ist. Es gibt also ein $\alpha \in O_K$, sodass $\left(\lambda^{\Theta'}\right) = (\alpha)^q$, beziehungsweise $\lambda^{\Theta'} = \eta\alpha^q$ für eine Einheit η von O_K. Wir erhalten

$$(x-\zeta)^\Theta = \left(\frac{1-\zeta}{1-\overline{\zeta}}\right)^{\Theta'}\frac{\eta}{\overline{\eta}}\left(\frac{\alpha}{\overline{\alpha}}\right)^q.$$

Wie wir bereits früher gesehen haben sind sowohl $\frac{\eta}{\overline{\eta}}$ als auch $\frac{1-\zeta}{1-\overline{\zeta}}$ Einheitswurzeln, und da alle Einheitswurzeln in K q-te Potenzen sind, ist somit auch $(x-\zeta)^{\Theta}$ eine q-te Potenz. □

Da $\omega(1-\iota)=0$ ist und die Gewichtsfunktion multiplikativ ist, ist das Ideal $(1-\iota)I_S$ sogar im augmentierten Teil von I_M enthalten, also $I_S^- \subseteq I_M^{\mathrm{aug}}$.

Aus Korollar 6.4.2 folgt für jedes reelle $r>0$ die untere Schranke

$$|I_M^{\mathrm{aug}}| \geq S\left(\frac{p-1}{2}, \frac{r}{p-1}\right). \tag{6.17}$$

Wir haben jedoch in Satz 6.2.6 eine obere Schranke für $|I_M^{\mathrm{aug}}|$ gezeigt. Unser Ziel ist es nun zu zeigen, dass diese beiden Schranken widersprüchlich sind.

Um die untere Schranke aus (6.17) dazu verwenden zu können brauchen wir noch folgende einfache Abschätzung für $S(n,r)$:

Lemma 6.5.2
Seien n und r ganze Zahlen mit $n \geq 5$ und $r \geq 4$, dann gilt:

$$S(n,r) > 4n^2(r+1).$$

Beweis. Da r ganzzahlig ist gilt laut Lemma 6.4.3:

$$S(n,r) = \sum_{j=0}^{n} 2^j \binom{n}{j}\binom{r}{j}$$

Wegen $n \geq 5$ und $r \geq 4$ können wir abschätzen:

$$\begin{aligned} 4\binom{n}{2}\binom{r}{2} &= n(n-1)r(r-1) \\ &\leq \cdot\frac{4}{5}\cdot n^2 \cdot \frac{4}{5}\cdot(r+1)\cdot 3 \\ &= \frac{48}{25}n^2(r+1), \end{aligned}$$

und

$$\begin{aligned} 8\binom{n}{3}\binom{r}{3} &= \frac{2}{9}n(n-1)(n-2)r(r-1)(r-2) \\ &\leq \frac{2}{9}\cdot\frac{4}{5}\cdot n^2\cdot 3\cdot\frac{4}{5}\cdot(r+1)\cdot 3\cdot 2 \\ &= \frac{64}{25}n^2(r+1). \end{aligned}$$

Daraus folgt nun

$$S(n,r) \geq 4\binom{n}{2}\binom{r}{2} + 8\binom{n}{3}\binom{r}{3} \geq \frac{112}{25}n^2(r+1) > 4n^2(r+1).$$

□

Damit können wir jetzt die bisherigen Ergebnisse anwenden und folgende wichtige Aussage beweisen:

Satz 6.5.3
Sei (x, y, p, q) eine Lösung der Catalan'schen Gleichung $x^p - y^q = 1$ mit ungeraden Primzahlen p, q, dann gilt:

$$q < 4(p-1)^2.$$

Beweis. Wir setzen

$$r := \left\lfloor \frac{q}{(p-1)^2} \right\rfloor \quad \text{und} \quad n := \frac{p-1}{2}.$$

Angenommen es wäre $q \geq 4(p-1)^2$, dann gilt $r \geq 4$. Es gilt auch $n \geq 5$, da $p \geq 11$ nach Korollar 6.3.2, die Voraussetzungen aus Lemma 6.5.2 sind also erfüllt.
Die Abschätzung von Hyyrö aus Satz 4.1.7 liefert

$$|x| \geq p^{q-1}(q-1)^q + 1 \geq \max\left\{ \left(\frac{36 \cdot 2^{p-1}}{(p-1)^2} \right), \frac{4}{\pi} \frac{q}{p-1} + 1 \right\}.$$

Nun wenden wir Satz 6.2.6 mit $\varepsilon = 1$, die Gleichung (6.17) und Lemma 6.5.2 an und erhalten die Ungleichungskette

$$q \geq |I_M^{\text{aug}}((p-1)r)| \geq S(n, r) > 4n^2(r+1) > 4\left(\frac{p-1}{2}\right)^2 \frac{q}{(p-1)^2} = q,$$

Widerspruch! □

Nun können wir durch Anwendung von Mihailescus Wieferich Kriterium die Catalan'sche Vermutung für den Fall $p \mid q-1$ oder $q \mid p-1$ zeigen:

Satz 6.5.4
Die Gleichung $x^p - y^q = 1$ besitzt keine Lösung mit ganzzahligen x, y und ungeraden Primzahlen p, q für die $p \mid q-1$ oder $q \mid p-1$ gilt.

Beweis. Angenommen es gibt eine Lösung (x, y, p, q) mit $p \mid q-1$, dann ist $q \equiv 1 \pmod{p}$. Mihailescus Wieferich Kriterium (Satz 4.2.1) besagt dass $q^{p-1} \equiv 1 \pmod{p^2}$, zusammen folgt also

$$q \equiv 1 \pmod{p^2}.$$

Anders ausgedrückt ist $q = kp^2 + 1$ für ein $k \in \mathbb{Z}$. Da q und p beide ungerade sind kann q nicht gleich $p^2 + 1$ oder $3p^2 + 1$ sein. Und da laut Korollar 6.3.2 $p \neq 3$ ist folgt $3 \mid 2p^2 + 1$ (da $p^2 \equiv 1 \pmod{3}$) und somit $q \neq 2p^2 + 1$.

Es gilt also $q \geq 4p^2 + 1$, was ein Widerspruch zu Satz 6.5.3 ist!

Der Fall $q \mid p-1$ folgt sofort, da dann $(-y, -x, q, p)$ ebenfalls eine Lösung ist. □

Literaturverzeichnis

[1] Atiyah, M. ; I.G., M. : *Introduction to Commutative Algebra*. Addison-Wesley, 1969

[2] Baker, A. : Bounds for the solutions of the hyperelliptic equation. In: *Proceedings of the Cambridge Philosophical Society* 65 (1969), S. 439–444

[3] Baker, A. : A sharpening of the bounds for linear forms in logarithms. In: *Acta arithmetica* 21 (1972), S. 117–129

[4] Baker, A. : A sharpening of the bounds for linear forms in logarithms.II. In: *Acta arithmetica* 24 (1973), S. 33–36

[5] Baker, A. : A sharpening of the bounds for linear forms in logarithms.III. In: *Acta arithmetica* 27 (1975), S. 247–252

[6] Bennett, C. ; Blass, J. ; Glass, A. ; Meronk, D. ; Steiner, R. : A small contribution to Catalan's equation. In: *Journal de Théorie des Nombres de Bordeaux* 9 (1997), Nr. 1, S. 97–136

[7] Bilu, Y. : Catalan's conjecture (after Mihailescu). In: *Astérisque* Bd. 294, 2004, S. 1–26

[8] Bilu, Y. : Catalan without logarithmic forms (after Bugeaud, Hanrot and Mihailescu). In: *Journal de Théorie des Nombres de Bordeaux* 17 (2005), Nr. 1, S. 69–85

[9] Bosch, S. : *Algebra*. 5.,überarbeitete Auflage. Springer, 2004

[10] Bugeaud, Y. ; Hanrot, G. : Un nouveau critère pour l'équation de Catalan. In: *Mathematika* 47 (2000), S. 63–73

[11] Cassels, J. W. S.: On the equation $a^x + b^y = 1$. In: *American journal of mathematics* 75 (1953), S. 159–162

[12] Cassels, J. W. S.: On the equation $a^x + b^y = 1$. II. In: *Proceedings of the Cambridge Philosophical Society* 56 (1960), S. 97–103

[13] Catalan, E. : Note extraite d'une lettre adressée à l'editeur. In: *Journal für die reine und angewandte Mathematik* 27 (1844), S. 192

[14] Catalan, E. : Quelques théorèmes empiriques. In: *Mémoires de la Société Royale des Sciences de Liège* 12 (1885), S. 42–43

[15] Chein, E. Z.: A note on the equation $x^2 = y^q + 1$. In: *Proceedings of the American Mathematical Society* 56 (1976), S. 83–84

[16] Cohen, H. : *Graduate Text in Mathematics*. Bd. 239: *Number theory, Volume I: Tools and Diophantine Equations*. Springer, 1996

[17] Cohen, H. : Démonstration de la conjecture de Catalan. In: *Théorie algorithmique des nombres et équations diophantiennes*. Palaiseau : Ed. de l'Ecole Polytechnical, 2005, S. 1–83

[18] Daems, J. : *A cyclotomic proof of Catalan's conjecture*, Universitet Leiden, Diplomarbeit, 2003

[19] Dickson, L. : *History of the theory of numbers*. Bd. II. Chelsea Publishing Company, 1952

[20] Drmota, M. : *Algebraische Zahlentheorie*. Skriptum an der TU Wien

[21] Drmota, M. : *Zahlentheorie für TM*. Skriptum an der TU Wien

[22] Euler, L. : Therorematum quorundam arithmeticorum demonstrationes. In: *Commentarii Academiae Scientiarum Imperialis Petropolitanae* 10 (1738), S. 125–146

[23] Gel'fond, A. : On the approximation of transcendental numbers by algebraic numbers. In: *Doklady Akademii Nauk SSSR* 2 (1935), S. 177–182

[24] Glass, A. ; Meronk, D. ; Okada, T. ; Steiner, R. : A small contribution to Catalan's equation. In: *Journal of Number Theory* 47 (1994), Nr. 2, S. 131–137

[25] Granville, A. : The latest on Catalan's Conjecture. In: *MAA Focus. The newsmagazine of the Mathematical Association of America* 25 (May/June 2001), Nr. 4, S. 4–5

[26] Hyyrö, S. : Über das Catalansche Problem. In: *Annales Universitatis Turkuensis. Series A.I.* N°.79 (1964), S. 8 Seiten

[27] Hyyrö, S. : Über die Gleichung $ax^n - bx^n = 1$ und das Catalansche Problem. In: *Annales Academiae Scientiarum Fennicae. Series A I.* N°.355 (1964), S. 50 Seiten

[28] Inkeri, K. : On Catalan's Problem. In: *Acta arithmetica* 9 (1964), S. 285–290

[29] Inkeri, K. : On Catalan's Conjecture. In: *Journal of number theory* 34 (1990), Nr. 2, S. 142–152

[30] Jantzen, J. C. ; Schwermer, J. : *Algebra*. Springer, 2006

[31] K., I. ; Rosen, M. : *Graduate Text in Mathematics*. Bd. 84: *A classical introduction to modern number theory*. Springer, 1982

[32] Kirschenhofer, P. ; Pethö, A. ; Tichy, R. F.: On analytical and Diophantine properties of a family of counting polynomials. In: *Acta scientiarum mathematicarum* 65 (1999), S. 47–59

[33] Ko, C. : On the diophantine equation $x^2 = y^n + 1$. In: *Scientia Sinica* 14 (1965), S. 457–460

[34] Lang, S. : *Fundamentals of diophantine geometry.* Springer, 1983

[35] Lang, S. : *Graduate Text in Mathematics.* Bd. 110: *Algebraic Number Theory.* Springer, 1986

[36] Langevin, M. : Quelques applications de nouveaux résultats de Van der Poorten. In: *Séminaire Delange-Pisot-Poitou. Théorie des nombres,* 17 (1975/76), Nr. 2, S. 11 Seiten

[37] Laurent, M. ; Mignotte, M. ; Nesterenko, Y. : Formes linéaires en deux logarithmes et déterminants d'interpolation. In: *Journal of Number Theory* 55 (1995), Nr. 2, S. 285–321

[38] Lebesgue, V. : Sur l'impossibilité en numbres entieres de l'équation $x^m = y^2 + 1$. In: *Nouvelles annales de mathématiques* 9 (1850), S. 178–181

[39] Leutbecher, A. : *Zahlentheorie : eine Einführung in die Algebra.* Springer, 1996

[40] LeVeque, W. : On the equation $a^x - b^y = 1$. In: *American Journal of Mathematics* 74 (1952), S. 325–331

[41] Mahler, K. : On the greatest prime factor of $ax^m + by^n$. In: *Nieuw Archief voor Wiskunde, III. Serie* 1 (1964), S. 113–122

[42] Mignotte, M. : Un critère élémentaire pour l'équation de Catalan. In: *La Société Royale du Canada. L'Académie des Sciences. Comptes Rendus Mathématiques* 15 (1993), Nr. 5, S. 199–200

[43] Mignotte, M. : A criterion on Catalan's equation. In: *Journal of Number Theory* 52 (1995), Nr. 2, S. 280–283

[44] Mignotte, M. : Catalan's equation just before 2000. In: *Number theory. Proceedings of the symposium in memory of Kustaa Inkeri held in Turku, May 31-June 4, 1999.* Walter de Gruyter & Co., 2001, S. 247–254

[45] Mignotte, M. : Die Catalansche Gleichung. In: *Mathematische Semesterberichte* 50 (2003), Nr. 2, S. 167–179

[46] Mignotte, M. ; Roy, Y. : Catalan's equation has no new solution with either exponent less than 10651. In: *Experimental Mathematics* 4 (1995), Nr. 4, S. 259–268

[47] Mignotte, M. ; Roy, Y. : Minorations pour l'équation de Catalan. In: *Comptes Rendus de l'Académie des Sciences. Série I. Mathématique* 324 (1997), Nr. 4, S. 377–380

[48] Mihailescu, P. : A class number free criterion for Catalan's Conjecture. In: *Journal of number theory* 99 (2002), Nr. 2, S. 225–231

[49] Mihailescu, P. : Primary Cyclotomic Units and a Proof of Catalan's Conjecture. In: *Journal für die reine und angewandte Mathematik* 572 (2004), S. 167–195

[50] Mihailescu, P. : Reflection, Bernoulli numbers and the proof of Catalan's conjecture. In: *European Congress of Mathematics. Proceedings of the 4th Congress (4ECM) held in Stockholm, June 27-July 2, 2004*. European Mathematical Society, 2005, S. 325–340

[51] Mihailescu, P. : On the class groups of cyclotomic extensions in the presence of a solution to Catalan's Equation. In: *Journal of number theory* 118 (2006), Nr. 1, S. 123–144

[52] Neukirch, J. : *Algebraische Zahlentheorie*. Unveränd. Nachdr. der 1. Aufl. Springer, 2002

[53] Remmert, R. ; Ullrich, P. : *Elementare Zahlentheorie*. Birkhäuser, 1987

[54] Ribenboim, P. : *Catalan's Conjecture (are 8 and 9 the only consecutive primes?)*. Academic Press, 1994

[55] Ribenboim, P. : *Classical Theory of Algebraic Numbers*. Springer, 2001 (Universitext)

[56] Schwarz, W. : A note on Catalan's equation. In: *Acta Arithmetica* 72 (1995), Nr. 3, S. 277–279

[57] Selberg, S. : The diophantine equation $x^4 = 1 + y^n$, with $n > 1$, $|x| > 1$ is impossible in integers. In: *Norsk matematisk tidsskrift* 14 (1932), S. 79–80

[58] Siegel, C. : Über einige Anwendungen diophantischer Approximationen. In: *Sitzungsberichte der Deutschen Akademie der Wissenschaften zu Berlin, Mathematisch-Naturwissenschaftliche Klasse* (1929), S. 1–77

[59] Steiner, R. : Class Number Bounds on Catalan's Equation. In: *Mathematics of Computation* 67 (1998), Nr. 223, S. 1317–1322

[60] Thaine, F. : On the ideal class groups of real abelian number fields. In: *Annals of Mathematics. Second Series* 128 (1988), Nr. 1, S. 1–18

[61] Tijdeman, R. : On the equation of Catalan. In: *Acta Arith.* 29 (1976), S. 197–209

[62] Washington, L. C.: *Graduate Text in Mathematics*. Bd. 83: *Introduction to Cyclotomic Fields*. 2nd Edition. Springer, 1997

[63] Wieferich, A. : Zum letzten Fermat'schen Theorem. In: *Journal für die reine und angewandte Mathematik* 136 (1909), S. 293–302

[64] Wolfart, J. : *Einführung in Zahlentheorie und Algebra.* Vieweg, 1996

[65] Ziegler, V. : *Diophantische Gleichungen: Das Problem von Catalan und Thue-Gleichungen*, TU Graz, Diplomarbeit, 2003