Fermats großer Satz

Bachelorarbeit (korrigierte Fassung) von

Daniel Zachow

Betreuerin: Prof. Dr. Annette Huber-Klawitter

24. Juli 2020

Albert-Ludwigs-Universität Freiburg
Fakultät für Mathematik und Physik

Inhaltsverzeichnis

Die folgenden Notationen werden in der Arbeit verwendet:

Notation	Erklärung
n	positive ganze Zahl; Exponent der Fermat-Gleichung
$\mathbb{N}_0$	natürliche Zahlen einschließlich 0
$\mathbb{N}$	natürliche Zahlen beginnend ab 1
$\mathbb{Z}$	Ring der ganzen Zahlen
$\mathbb{Q}$	Körper der rationalen Zahlen
$\mathbb{C}$	Körper der komplexen Zahlen
i	imaginäre Einheit $\mathrm{i} = \sqrt{-1}$
$a \mid b$	a teilt b
$a \nmid b$	a teilt b nicht
$\mathrm{ggT}(a, b)$	größter gemeinsamer Teiler von a und b
$a \sim b$	a und b sind assoziiert
$\mathcal{O}_L$	Ring der ganzen Zahlen eines Zahlkörpers L
$\mathcal{O}$	ein Dedekind-Ring
Cl_L	die Idealklassengruppe eines Quotientenkörpers L
h_L	die Ordnung der Idealklassengruppe Cl_L (Klassenzahl)
$\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$	Ideale
$\langle a \rangle$	von a erzeugtes Hauptideal
$a \equiv b \pmod{m}$	a kongruent b modulo m
$a \equiv b \pmod{\mathfrak{a}}$	Kongruenzrelation modulo ein Ideal
$\alpha, \beta, \ldots$	griech. Buchstaben stehen für (ganz-)algebraische Zahlen
ω	eine primitive dritte Einheitswurzel in $\mathbb{C}$
ζ_n	eine primitive n-te Einheitswurzel in $\mathbb{C}$

1. Einleitung

Mit Fermats großem Satz hat die Mathematik eine Aussage, die in mindestens drei diametral verschiedenen Aspekten bemerkenswert ist (dazu zählt nicht, dass es für das Theorem im Deutschen gleich mehrere, wenn auch ähnliche, Bezeichnungen gibt: Mehr oder minder gebräuchlich sind "großer Satz von Fermat", "großer fermat'scher Satz", "fermats letzter Satz" und der Titel der Arbeit mit und ohne Apostroph sowie Schreibweisen, in denen die Adjektive "groß" und "fermat'sch" großgeschrieben werden). Und zwar ist es für ein bedeutendes mathematisches Problem selten, dass es gemeinhin verständlich ist (1). Dennoch dauerte es mehr als 350 Jahre bis 1994, ehe ein Beweis gefunden wurde, obwohl sich viele Mathematiker und Laien daran versuchten (2), und das obwohl nach [Roq98], S. 17, keine direkte Anwendung innerhalb oder außerhalb der Mathematik bekannt ist (3). Letztlich ist Fermats großer Satz auch aus dem Grund bedeutsam, weil mit seiner Beschäftigung bedeutende Entwicklungen in der Algebra und Zahlentheorie einhergingen, etwa der Begriff des *Ideals*.

Fermats großer Satz besagt, dass es keine ganzen Zahlen x, y, z ungleich Null und keine natürliche Zahl $n > 2$ gibt mit $x^n + y^n = z^n$. Für $n = 2$ ist die Gleichung bekanntermaßen ein Sonderfall des Satzes von Pythagoras, deren positive ganzzahlige Lösungen *pythagoräische Tripel* heißen. Ein Ziel der Arbeit ist es, die allgemeinste Form pythagoräischer Tripel zu bestimmen. Dem übergeordnet sollen Beweise von Fermats großem Satz für ausgewählte Exponenten nachvollzogen und ausgearbeitet werden, und zwar für $n = 3$, $n = 4$ sowie wenn n eine sogenannte *reguläre* Primzahl ist.

Methodik

Die Arbeit ist (mit Einleitung) in vier Kapitel mit Anhang gegliedert. Im zweiten Kapitel erfolgt ein kurzer Abriss der Beweisgeschichte. Ein klassischer Ansatz ist es, für eine Primzahl $p > 2$ die linke Seite $x^p + y^p$ als $(x + y)(x + \zeta_p y) \dots (x + \zeta_p^{p-1} y)$ zu faktorisieren, was zum Erweiterungsring $\mathbb{Z}[\zeta_p]$ der ganzen Zahlen führt. Dabei ist ζ_p eine primitive p-te Einheitswurzel in den komplexen Zahlen. In dem Zusammenhang gehen wir insbesondere auf das damit verknüpfte Problem ein, dass $\mathbb{Z}[\zeta_p]$ im Allgemeinen kein ZPE-Ring ist.

Kapitel 3 ist als Vorarbeit für das anschließende Hauptkapitel konzipiert. Hier untersuchen wir die Eigenschaften von $\mathbb{Z}[\zeta_p]$ als *Ganzheitsring* des *zyklotomischen Körpers* $\mathbb{Q}(\zeta_p)$. Dafür bedarf es zunächst einer Erklärung der beiden Begriffe: Letzteres ist ein *algebraischer Zahlkörper*, also eine endliche Erweiterung $L/\mathbb{Q}$ des Körpers der rationalen Zahlen. Den Namen entsprechend enthält L *algebraische* und sein Ganzheitsring $\mathcal{O}_L$ *ganz-algebraische* Zahlen als Verallgemeinerung des Konzepts der rationalen und der (rationalen) ganzen Zahl. Gleichzeitig ist L der Quotientenkörper von $\mathcal{O}_L$. Das Maß dafür, inwieweit ein Ganzheitsring im Wesentlichen eindeutige Primelementzerlegung

besitzt, ist die Ordnung der *Idealklassengruppe*, die *Klassenzahl*. Unabhängig von ihrem Wert ist jeder Ganzheitsring ein *Dedekind-Ring*, in welchem zumindest die Zerlegung eines *Ideals* in Prim*ideale* eindeutig ist. Um das Kapitel nicht mit (Hilfs-)Konzepten aus der algebraischen Zahlentheorie zu überladen, verschieben wir den theoretischen Hintergrund in Anhang B.

Im vierten Kapitel analysieren wir zuerst die Gestalt pythagoräischer Tripel mit dem Ziel, alle ganzzahligen Lösungen von $x^2+y^2=z^2$ zu erhalten. Danach suchen wir einen geometrischen Zugang zu pythagoräischen Tripeln. Im deutlich umfassenderen zweiten Teil des Kapitels arbeiten wir Beweise von Fermats großem Satz für $n=4$, $n=3$ und n gleich eine reguläre Primzahl p aus. Die Reihenfolge entspricht der zunehmenden Komplexität. So sind $n=4$ und $n=3$ die ersten Fälle, für die ein Beweis gefunden wurde. Der dritte Fall stellt einen Meilenstein in der Beweisgeschichte dar, da nicht nur einzelne, sondern womöglich unendlich viele Primzahlen regulär sind. Im Rahmen der Arbeit kann Fermats großer Satz für reguläre Primzahlen allerdings nur unter der Voraussetzung betrachtet werden, dass p keines der x, y, z teilt. Man spricht hierbei von "Fall 1" im Gegensatz zu "Fall 2", bei dem p genau eine der drei Zahlen teilt. Vorab wird als "Zwischenspiel" des Kapitels die Idee verfolgt, wie sich Fermats großer Satz verhält, wenn als Definitionsmenge nicht ganze Zahlen, sondern ein anderer Zahlbereich oder ein Polynomring über einem Körper dient. Den Abschluss bildet ein vergleichendes Fazit der Beweise.

In Anhang A schließlich werden grundlegende idealarithmetische Aussagen wiederholt und in Anhang B ist, wie bereits angesprochen, das theoretische Fundament für die Kapitel 3 und 4.6 untergebracht.

Für den Blick in die Beweishistorie von Fermats großem Satz (Kapitel 2) wurden verschiedene Literaturquellen herangezogen: Einer Gesamtschau dienten *Geschichte der Mathematik kompakt* von F. M. Brückler, der Vortrag *Zum Fermat-Problem* von P. Roquette und die Website *MacTutor History of Mathematics Archives* von E. F. O'Connor und J. J. Robertson. Für das Problem der Eindeutigkeit der Primelementzerlegung erwies sich u.a. *4000 Jahre Algebra* des Autorenkollektivs um H.-W. Alten als fruchtbar. Für die Entwicklungen Mitte der 1980er bis Mitte der 90er Jahre wurde ergänzend auf *An Overview of the Proof of Fermat's Last Theorem* von G. Stevens zurückgegriffen.

Quellen für Kapitel 3 und Anhang B sind im Wesentlichen *Quadratische Zahlkörper* von F. Lemmermeyer, die gleichnamigen Lehrbücher *Einführung in die algebraische Zahlentheorie* von A. Schmidt bzw. J. Neukirch sowie *Elementare und algebraische Zahlentheorie* von St. Müller-Stach und J. Piontkowski.

Im vierten Kapitel war für die Fälle $n=2$, $n=4$ und $n=3$ der zahlentheoretische Klassiker *An Introduction to the Theory of Numbers* von G. H. Hardy and E. M. Wright grundlegend. Für $n=4$ und den geometrischen Zugang zu pythagoräischen Tripeln wurde ferner *Elementare Zahlentheorie* von N. Oswald und J. Steuding genutzt. Bei der Betrachtung von Fermats großem Satz für Polynome diente der Artikel *Remarks on the History of Fermat's Last Theorem 1844 to 1984* von M. Rosen als Grundlage. Der Abschnitt über einen Beweis für n gleich reguläre Primzahl basiert schließlich auf dem 1. Kapitel aus *Introduction to Cyclotomic Fields* von L. C. Washington; ergänzende Anmerkungen entstammen u.a. *Einführung in die Zahlentheorie* von P. Bundschuh.

2. Zur Beweisgeschichte des Satzes

Der Namensgeber des Satzes, Pierre de Fermat (1601/8–1665, die genauen Daten sind nach [Roq98], S. 4, unsicher), schlug einen juristischen Berufsweg ein. Mathematik betrieb er, wie die meisten Mathematiker seiner Zeit, nebenher, wobei er seine Erkenntnisse und Hypothesen weder veröffentlichte noch in privaten Abhandlungen festhielt. Sein Einfluss auf die Mathematik resultiert stattdessen zeitlebens aus Briefwechseln mit vielen bedeutenden Gelehrten sowie später aus seinem Nachlass. Neben Briefen gehörten dazu Bücher, die Fermat mit Randnotizen versehen hatte (ebd. und [Brü17], S. 146). So geht die heute als Fermats großer Satz (bzw. bis zu ihrem Beweis auch als Fermat'sche Vermutung) bekannte Aussage auf seine folgende Anmerkung in einer Kopie der *Arithmetika* zurück, an der Diophant den Fall $n = 2$ diskutierte ([Roq98], S. 4); eine Übersetzung aus dem Lateinischen lautet:

> *"Es ist aber nicht möglich, einen Kubus in zwei Kuben, oder ein Biquadrat in zwei Biquadrate und allgemein eine Potenz, höher als die zweite, in zwei Potenzen mit demselben Exponenten zu zerlegen. Ich habe hierfür einen wahrhaft wunderbaren Beweis, doch ist dieser Rand zu schmal, um ihn zu fassen."* ([Kra02], S. 217)

In moderner Formulierung behauptet er hier, dass es für $n > 2$ keine Zerlegung

$$x^n + y^n = z^n \tag{2.1}$$

mit $x, y, z \in \mathbb{N}$ gibt. In Fermats großem Satz werden ganzzahlige x, y und z ungleich Null betrachtet (vgl. Satz 4.1). Aus erhaltenen Briefen ist überliefert, dass sich Fermat selbst mit den Fällen $n = 3$ und $n = 4$ auseinandersetzte. Für letzteren fand er einen Beweis (genauer gesagt, konnte er die Behauptung für $n = 4$ plausibel darlegen; [Roq98], S. 4). Dass Fermat seine Vermutung tatsächlich allgemein beweisen konnte, kann als äußerst unwahrscheinlich eingeschätzt werden.

Grundsätzlich ist es ausreichend, das Theorem für $n = 4$ und ungerade Primzahlen zu beweisen. Der Grund liegt darin, dass jede natürliche Zahl $n > 2$ zumindest aus 4 oder einer Primzahl $p \geq 3$ zusammengesetzt ist. Ist nun Fermats großer Satz für $n = 4$ und $n = p$ wahr (d. h., es gibt keine x, y, z mit $x^n + y^n = z^n$), dann existieren insbesondere keine Potenzen x^d, y^d und z^d, $d \in \mathbb{N}$, mit

$$\left(x^d\right)^n + \left(y^d\right)^n = \left(z^d\right)^n.$$

Den groben Verlauf der Beweishistorie umreißt die modifizierte und mit Hilfe von [OR96] ergänzte Übersicht aus [Roq98], S. 6, auf der nächsten Seite. Diese möchten wir im Folgenden durch einige Anmerkungen zum Problem der Primelementzerlegung und anschließend zum letztendlichen Beweis von Fermats großem Satz durch A. Wiles abrunden.

Fermat (1601/08–1665) um 1630 Problemstellung; Beweis für $n = 4$ und später andeutungsweise für $n = 3$.

Euler (1707–1783) $n = 3$: insgesamt vollständiger Beweis mittels komplexer Zahlen, jedoch verteilt auf zwei getrennte Arbeiten.

Gauß (1777–1850) $n = 3$: vollständiger Beweis.

Germain (1776–1831) um 1820 Beweis von Fall 1 für (später nach ihr benannte) Sophie-Germain-Primzahlen p, bei denen $2p + 1$ ebenfalls prim ist.

Dirichlet (1805–1859) $n = 5$: 1825 unvollständiger Beweis, den Dirichlet selbst und unabhängig von ihm Legendre vervollständigen konnten.

Dirichlet (1805–1859) $n = 14$: 1832 vollständiger Beweis.

Lamé (1795–1870) $n = 7$: 1839 vollständiger Beweis.

Lamé (1795–1870) n beliebig: im März 1847 falscher Beweis mittels Faktorisierung von $x^n + y^n = z^n$, der eindeutige Primelementzerlegung voraussetzt. Daraufhin briefliche Schilderung Kummers, dass die getroffene Voraussetzung ungültig ist (ein Nachweis gelang ihm bereits 1844)

Kummer (1810–1893) n gleich reguläre Primzahl: Beweis im September 1847.

Wiles (*1953) n beliebig: 1994 vollständiger Beweis durch Beweis der Taniyama-Shimura(-Weil)-Vermutung für eine bestimmte Klasse elliptischer Kurven.

Bei Betrachtung der Übersicht fällt auf, dass Fermats großer Satz bis in die 1840er Jahre nur für $n = 3$, 4, 5 und 7 durch Beweise von Fermat, L. Euler bzw. C. F. Gauß, L. Dirichlet/A. Legendre und G. Lamé vollständig bekannt war (was für $n \leq 100$ immerhin zwei Drittel der Fälle abdeckt). Den ersten großen Erfolg lieferte 1847 dann E. Kummer, indem er zeigte, dass Fermats großer Satz für reguläre Primzahlen – Primzahlen, welche nicht die Klassenzahl des zyklotomischen Körpers $\mathbb{Q}(\zeta_p)$ teilen (der Begriff wird in Abschnitt 3.1 geklärt) – gültig ist. Drei Jahre zuvor veröffentlichte Kummer seine Resultate zur Theorie der *idealen Zahlen* ([Ros97], Einleitung), die ihm eine teilweise "Rettung" des Ansatzes von Lamé ermöglichte (s. Übersicht). Der Beweis war mit umfassender Vorarbeit verbunden. So definierte Kummer z.B. die Idealklassengruppe (Definition A.25), zeigte, dass sie endlich ist (Bemerkung A.26), und musste fundierte Untersuchungen zu den Einheiten in $\mathbb{Q}(\zeta_p)$ anstellen ([Ros97], Einleitung). Darüber hinaus gelang es ihm, die Regularität von p durch die Teilbarkeitsrelation von p und bestimmten Bernoulli-Zahlen auszudrücken (vgl. Abschnitt 4.6)*.

Unter den Primzahlen bis 100 sind nur 37, 59 und 67 nicht regulär ([Was97], Kap. 1, Remarks). Streicht man z.B. für $n \leq 1000$ nach dem Sieb des Eratosthenes die Zahl 4, alle regulären Primzahlen sowie jeweils deren Vielfache, so gewinnt man aufgrund der wenigen Lücken einen visuellen Eindruck der Bedeutung von Kummers "monumentalem Theorem".

Mehr als ein Jahrhundert nach Kummers Beweis erfolgte dann ein entscheidender Impuls zur Lösung des Fermat-Problems. Wir versuchen die Grundideen zu skizzieren: Mitte der 1980er Jahre regte als erstes G. Frey an, dass eine Verbindung zwischen Fer-

*Sein 1850 im Crelles Journal publizierter Beweis kann online unter http://www.digizeitschriften.de/main/dms/img/?PPN=GDZPPN002146738 eingesehen werden.

mats großem Satz und der in den 1950er Jahren aufgestellten Modularitätsvermutung von Y. Taniyama und G. Shimura (mit späteren Beiträgen von A. Weil) bestehen könnte ([Brü17], S. 151). In dieser wird vermutet, dass jede *elliptische Kurve* mit einer *Modulform* – zwei Objekte aus "entgegengesetzten Enden der Mathematik" – verknüpft ist ([Sin97], S. 217). Vage ausgedrückt bilden Modulformen eine Klasse auf der oberen Halbebene der komplexen Zahlenebene definierter, holomorpher Funktionen ([AN20], Definition 3.1), während eine über den rationalen Zahlen definierte elliptische Kurve nach [Kra02], S. 219, durch die kubische Gleichung $y^2 = x^3 + ax^2 + bx + c$ mit ganzzahligen Koeffizienten festgelegt ist. Frey ging nun von einer hypothetischen Lösung a, b, c der Fermat-Gleichung $a^p + b^p + c^p = 0$ aus ([Sin97], S. 228). Daraus konstruierte er die "bemerkenswerte" ([Ste97], §1) elliptische Kurve

$$E_{a^p,b^p,c^p} : y^2 = x(x - a^p)(x + b^p)$$

(ebd.). Insbesondere vermutete er, dass diese nicht modular sei im Widerspruch zur Modularitätsvermutung. Stellt sich diese nun als wahr heraus, so darf die *Frey-Kurve* nicht existieren. Daraus folgt wiederum, dass die Fermat-Gleichung keine Lösung besitzt, also Fermats großer Satz wahr ist ([Sin97], S. 230). 1985/6 formulierte J-P. Serre dann die sogenannte *Epsilon-Vermutung*, aus der die Nichtmodularität folgt. Ihr Beweis gelang K. Ribet im selben Jahr ([Ste97], S. 1). Der Beweis der Modularitätsvermutung für eine bestimmte Klasse elliptischer Kurven (alias *semistabile* elliptische Kurven, zu denen die Frey-Kurven gehören), welche bereits Fermats großen Satz nach sich zieht, wurde schließlich 1994 von A. Wiles in Kooperation mit R. Taylor gefunden (ebd., S. 1f). Detailliertere Ausführungen können u.a. ebd. sowie in [Rib99] nachgelesen werden. Wiles' 96-seitiger Beweis ist 1995 unter dem Titel *Modular elliptic curves and Fermat's Last Theorem* in *Annals of Mathematics*, 141 (3), veröffentlicht.

Das Problem der Primelementzerlegung und Kummers ideale Zahlen

Wie in der Einleitung angedeutet, bestand der klassische Beweisansatz für Fermats großen Satz vor dem Zugang über elliptische Kurven/Modulformen in der Annahme einer ganzzahligen Lösung x, y, z und der anschließenden Faktorisierung von $x^n + y^n$ in ganz-algebraische Zahlen ([Ros97], §1 unter Gleichung (1)). Dadurch wird das additive Problem in ein multiplikatives überführt. Beispielsweise ist

$$x^3 + y^3 = (x + y)(x + \zeta_3 y)(x + \zeta_3^2 y).$$

Für eine ungerade Primzahl p ist entsprechend

$$x^p + y^p = (x + y)(x + \zeta_p y) \dots (x + \zeta_p^{p-1} y) \tag{2.2}$$

([Roq98], S. 7f). Dies führt zum Erweiterungsring $\mathbb{Z}[\zeta_p]$ der ganzen Zahlen, adjungiert eine primitive komplexe p-te Einheitswurzel ζ_p. Die Identität (2.2) leiten wir in Abschnitt 4.4 her und den Ring $\mathbb{Z}[\zeta_p]$ untersuchen wir eingehender in Kapitel 3.

Im Hinblick auf die Fermat-Gleichung (2.1) mündet die Zerlegung aus (2.2) in der Frage, ob das p-fache Produkt eine p-te Potenz z^p sein kann (ebd., S. 8). Ab dieser Stelle krankte der Beweisversuch von Lamé (s. Übersicht) an der – wie zuerst Kummer

für $\mathbb{Z}[\zeta_{23}]$ darlegen konnte – unzulässigen Annahme, dass in $\mathbb{Z}[\zeta_p]$ die Primelementzerlegung eindeutig sei ([JJ98], Kap. 11.9).

Wir veranschaulichen das Problem anhand des einfachen Rings

$$\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$$

und skizzieren abschließend daran Kummers Rettungsansatz. Dabei orientieren wir uns an [ADNE+14], S. 422ff. Als erstes untersuchte Gauß eingehend (die hinterher nach ihm benannten) komplexen Zahlen der Form $a + b\mathrm{i}$ mit ganzzahligen a, b. Im Zuge dessen konnte er zeigen, dass eindeutige Primfaktorisierung vorliegt. Während einige ganze Zahlen wie 3 prim bleiben, ist z. B. $5 = (1+2\mathrm{i})(1-2\mathrm{i})$ aus Primelementen zusammengesetzt. Seine geäußerte Vermutung, dass auch die Arithmetik von Zahlen der Form $a + b\zeta_3$ im Wesentlichen zu der in $\mathbb{Z}$ analog sei, wurde von G. Eisenstein bestätigt (deshalb werden diese auch *Eisenstein-Zahlen* genannt). Die Gauß'schen und die Eisenstein-Zahlen diskutieren wir in Abschnitt 3.2 in Vorarbeit für den Beweis von Fermats großem Satz für $n = 3$.

Demgegenüber besitzt im Ring $\mathbb{Z}[\sqrt{-3}]$ die Zahl 4 mit

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$$

zwei Zerlegungen in irreduzible Faktoren, die sich um mehr als Einheiten und Reihenfolge unterscheiden (vgl. Definition A.8). Um das einzusehen, betrachten wir die multiplikative, auf $\mathbb{Z}[\sqrt{-3}]$ definierte Norm $N(a + b\sqrt{-3}) = a^2 + 3b^2$. Hiernach ist

$$N(2) = 4 \quad \text{und} \quad N(1 \pm \sqrt{-3}) = 4.$$

Aus der Multiplikativität folgert man leicht, dass die Einheiten Norm 1 haben müssen und damit 1 und -1 die Einheiten von $\mathbb{Z}[\sqrt{-3}]$ sind. Wäre nun 2 bzw. $1 \pm \sqrt{-3}$ aus Nichteinheiten z, w zusammengesetzt, dann wäre

$$4 = N(2) = N(zw) = N(z)N(w) = 2 \cdot 2.$$

Gleiches gilt für $N(1 \pm \sqrt{-3})$, jedoch ist $a^2 + 3b^2 = 2$ nicht ganzzahlig lösbar. Da weiter $2 \neq \pm 1 \cdot (1 \pm \sqrt{-3})$ gilt, sind 2 und $1 \pm \sqrt{-3}$ nicht assoziiert und die Zerlegungen damit im Wesentlichen unterschiedlich.

Geleitet von der Vorstellung, dass Primzahlen teilweise aus *idealen Primfaktoren* zusammengesetzt sind, gelang es Kummer, die Eindeutigkeit der Primelementzerlegung mit Hilfe seiner Theorie der *idealen Zahlen* (die R. Dedekind später zum Begriff des Ideals weiterentwickelte) wiederherzustellen. Im Beispiel lassen sich die Faktoren 2 und $1 \pm \sqrt{-3}$ aus den Primelementen p und q zu

$$2 = pq, \quad 1 + \sqrt{-3} = p^2, \quad 1 - \sqrt{-3} = q^2$$

zusammengesetzt denken ([Neu07], Beispiel von Kap. 1.3). Daraus resultiert schließlich die eindeutige Zerlegung

$$4 = (pq)^2 = p^2 q^2$$

der Zahl 4 in irreduzible Faktoren.

3. Der Ring $\mathbb{Z}[\zeta_p]$

Der historische Abriss hat gezeigt, dass der klassische Beweisansatz für Fermats großen Satz zu $\mathbb{Z}[\zeta_p]$ führt. Mit Blick auf die Beweisvorhaben setzen wir uns deshalb nun mit den Eigenschaften des Rings $\mathbb{Z}[\zeta_p]$ auseinander, insbesondere mit der Frage nach der Eindeutigkeit der Primzerlegung. Der theoretische Hintergrund für dieses Kapitel steht in Anhang B.

3.1. Zahlkörper und ihre Ganzheitsringe

Wir beginnen mit den Definitionen des algebraischen Zahlkörpers und seines Ganzheitsrings. Gemeinhin heißt ein Element eines Erweiterungskörpers $L \supseteq K$ *algebraisch über* K, wenn es Nullstelle eines Polynoms $P \neq 0$ mit Koeffizienten aus K ist. Ist jedes Element aus L algebraisch über K, so wird L/K *algebraisch* genannt. Das ist insbesondere der Fall, wenn der Grad $[L : K]$ endlich ist.

Definition 3.1. ([Neu07], Beginn Kap. 1.2)
Ein *Zahlkörper* (auch *algebraischer Zahlkörper*) L ist eine endliche Körpererweiterung der rationalen Zahlen. Seine Elemente heißen *algebraische Zahlen.*

Definition 3.2. ([Lem17], Einleitung Kap. 2.2)
Sei L ein Zahlkörper. Eine Zahl $\alpha \in L$ heißt *ganz-algebraisch* oder *algebraisch ganz*, wenn sie Nullstelle eines normierten Polynoms mit ganzzahligen Koeffizienten ist. Ihre Gesamtheit $\mathcal{O}_L$ nennt man den *Ring der ganzen Zahlen* oder *Ganzheitsring* von L.

Bemerkung 3.3. Ein Zahlkörper L ist der Quotientenkörper seines Ganzheitsrings ([MSP11], Satz 16.10). Sie stellen gewissermaßen Analoga von $\mathbb{Z}$ und $\mathbb{Q}$ dar. Weiter sind Ganzheitsringe Integritätsringe ([Lem17], Beginn Kap. 3) und (ganz-)algebraische Zahlen sind komplexe Zahlen, d. h. $\mathbb{Q} \subseteq L \subsetneq \mathbb{C}$ ([Sch07], Einleitung Kap. 6.1).

Beispiel 3.4. Die trivialen Beispiele für solche Paare sind $\mathbb{Q}$ und $\mathbb{Z}$ selbst, da jedes $a \in \mathbb{Z}$ Nullstelle von $x - a \in \mathbb{Z}[T]$ ist. Gegen Ende von Kapitel 2 hatten wir $\mathbb{Z}[\sqrt{-3}]$ als einen Ring angeführt, in dem 4 auf unterschiedliche Weise primfaktorisiert werden kann. Zahlkörper der Form $\mathbb{Q}(\sqrt{d})$, für die $d \in \mathbb{Z}$ quadratfrei und ungleich 0 oder 1 ist, heißen *quadratische Zahlkörper* ([Sch07], Definition 6.1.1). Wie wir in Bemerkung 3.8 kurz ansprechen werden, gilt allerdings $\mathbb{Z}[\sqrt{-3}] \subsetneq \mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$.

Wie die Notation vermuten lässt, steht $\mathbb{Z}[\zeta_p]$ in Verbindung mit $\mathbb{Q}(\zeta_p)$:

Definition 3.5. Für eine natürliche Zahl $n > 2$ und eine primitive komplexe n-te Einheitswurzel ζ_n heißt $\mathbb{Q}(\zeta_n)$ der n-te *Kreisteilungskörper* oder n-te *zyklotomische Körper* ([IR90], Beginn Kap. 13.2).

Da das Minimalpolynom von ζ_n über $\mathbb{Q}$ den Grad $\varphi(n)$ hat, bilden

$$1, \zeta_n, \ldots, \zeta_n^{\varphi(n)-1}$$

eine Basis des $\mathbb{Q}$-Vektorraums $\mathbb{Q}(\zeta_n)$. Dadurch erhalten wir eine grobe Vorstellung zyklotomischer Körper. Für eine Primzahl $p \geq 3$ widmen wir uns nun in den nächsten beiden Abschnitten dem Ganzheitsring von $\mathbb{Q}(\zeta_p)$.

3.2. Der Ring $\mathbb{Z}[\zeta_3]$

Als Einstieg betrachten wir zunächst den besonders einfachen Ganzheitsring $\mathbb{Z}[\mathrm{i}]$ des zyklotomischen Körpers $\mathbb{Q}(\mathrm{i})$ ([Lem17], Satz 2.2).

Der Gauß'sche Zahlring $\mathbb{Z}[\mathrm{i}]$

Der *Ring der Gauß'schen Zahlen* oder *Gauß'sche Zahlring*

$$\mathbb{Z}[\mathrm{i}] = \{a + b\mathrm{i} \mid a, b \in \mathbb{Z}\}$$

entsteht aus $\mathbb{Z}$ durch Adjunktion der imaginären Einheit $\mathrm{i} = \sqrt{-1}$, welche neben $-\mathrm{i}$ die einzige primitive vierte Einheitswurzel ist. Seine Einheiten sind ± 1 und $\pm\mathrm{i}$. Der Ring ist nach Gauß benannt, der, wie in Kapitel 2 erwähnt, als erstes die arithmetischen Eigenschaften von Zahlen der Form $a + b\mathrm{i}$ eingehend untersuchte ([IR90], nach Beweis von Proposition 1.4.1). Die Gauß'schen Zahlen bilden die Ecken eines quadratischen Gitters auf der komplexen Ebene, dessen Knoten ganzzahlige Koordinaten haben (Abb. 3.1).

Der Gauß'sche Zahlring weist den folgenden, zu $\mathbb{Z}$ identischen Wesenszug auf:

Satz 3.6. *Der Gauß'sche Zahlring mit der Norm* $N\colon \mathbb{Z}[\mathrm{i}]\setminus\{0\} \to \mathbb{N}_0$*, definiert durch* $N(a + b\mathrm{i}) = a^2 + b^2$*, ist euklidisch.*

Bemerkung 3.7. Als euklidischer Ring ist $\mathbb{Z}[\mathrm{i}]$ nach Satz A.13 mithin faktoriell, besitzt also (bis auf Einheiten und Reihenfolge) eindeutige Primelementzerlegung. Die Norm einer Gauß'schen Zahl entspricht dem Betragsquadrat einer komplexen Zahl.

Wir orientieren uns am Beweis von Satz 3.25 in [Wol11]:

Beweis von Satz 3.6. Seien $\alpha, \delta \in \mathbb{Z}[\mathrm{i}]$, $\delta \neq 0$, beliebig gegeben. Wir betrachten den Punkt $\pi \coloneqq \alpha/\delta$ in der komplexen Ebene und den ihm am nächsten liegenden Punkt $\pi' \in \mathbb{Z}[\mathrm{i}]$ mit ganzzahligen Koordinaten (Abb. 3.1). Nun wählen wir geschickterweise $\chi \coloneqq \pi - \pi'$ und $\varrho \coloneqq \delta\chi$. Dann ist $\varrho = \delta\chi = \delta\pi - \delta\pi' = \alpha - \delta\pi' \in \mathbb{Z}[\mathrm{i}]$ und obendrein $\alpha = \pi'\delta + \varrho$ wie gewünscht.

Der Abstand von π zu π' ist $|\chi| = |\pi - \pi'| \leq \sqrt{2}/2 < 1$. Somit gilt als zweites

$$N(\varrho) = N(\delta x) \overset{\text{Bem.}}{\underset{3.7}{=}} |\delta\chi|^2 = |\delta|^2|\chi|^2 < |\delta|^2 = N(\delta). \qquad \square$$

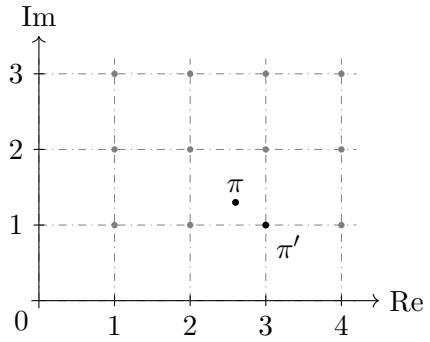

Abb. 3.1.: Die Gauß'schen Zahlen als Gitterpunkte (Quelle: eigen)

Der Ring der Eisenstein-Zahlen $\mathbb{Z}[\omega]$

Der Ganzheitsring von $\mathbb{Q}(\zeta_3)$ ist $\mathbb{Z}[\zeta_3]$ ([Lem17], Satz 2.2 und Einleitung Kap. 4.2). In dem Zusammenhang wird für ζ_3 auch ρ (z. B. ebd. und [HW75]) oder ω (z. B. [IR90]) geschrieben. Wir wählen Letzteres. Als primitive dritte Einheitswurzel ist ω eine der beiden Lösungen des zweiten Faktors von $T^3-1=(T-1)(T^2+T+1)$. Diese errechnen sich mit der p-q-Formel zu

$$\omega = -\frac{1}{2} \pm \sqrt{\frac{1}{4}-1} = -\frac{1}{2} \pm \frac{\sqrt{-3}}{2}.$$

Geometrisch betrachtet ist ω eine der beiden von 1 verschiedenen Ecken eines in den Einheitskreis auf der komplexen Ebene eingeschriebenen gleichseitigen Dreiecks. Dem Gauß'schen Zahlring entsprechend hat $\mathbb{Z}[\omega]$ die Form

$$\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$$

([IR90], vor Proposition 1.4.2). Seine Elemente, die auch *Eisenstein-Zahlen* genannt werden (vgl. Kapitel 2), bilden die Ecken einer Parkettierung der komplexen Ebene mit regelmäßigen Dreiecken (Abb. 3.2). In Abb. 3.2 sind auch die sechs Einheiten

$$\pm 1,\ \pm\omega,\ \pm\omega^2 \tag{3.1}$$

von $\mathbb{Z}[\omega]$ eingezeichnet. Daraus folgt, dass jede Eisenstein-Zahl $\eta \neq 0$ sechs Assoziierte hat ([Lem17], Beginn Kap. 4.2).

Dass $\mathbb{Z}[\omega]$ und $\mathbb{Z}[\mathrm{i}]$ tatsächlich Ringe sind, lässt sich mit etwas Schreibaufwand leicht nachrechnen. Wir verweisen hier z. B. auf [IR90], vor Proposition 1.4.2.

Bemerkung 3.8. In Beispiel 3.4 haben wir die quadratischen Zahlkörper $\mathbb{Q}(\sqrt{d})$ erklärt. Ihre Elemente haben die Form $a + b\sqrt{d}$ mit $a, b \in \mathbb{Q}$. Hierbei bilden $\mathbb{Q}(\mathrm{i}) = \mathbb{Q}(\sqrt{-1})$ und $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$ die beiden Ausnahmen, bei denen ein zyklotomischer gleichzeitig ein quadratischer Zahlkörper ist ([Lem17], Kap. 4.2, zweiter Absatz). Daher haben, anders als man es anfänglich vermuten könnte, die Zahlen aus $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$ die gleiche Form wie Eisenstein-Zahlen. D.h., $\mathbb{Z}[\sqrt{-3}] \subsetneq \mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$. In [Lem17], Satz 2.2, sind die Ganzheitsringe quadratischer Zahlkörper angegeben.

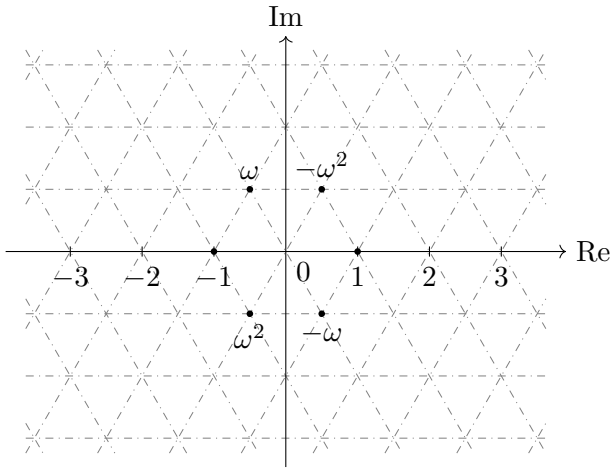

Abb. 3.2.: Die Eisenstein-Zahlen als Gitterpunkte (nach [Lem17], Kap. 4.2)

Wir beweisen nun die Aussage, dass die Primelementzerlegung in $\mathbb{Z}[\omega]$ eindeutig ist:

Satz 3.9. *Der Ganzheitsring $\mathbb{Z}[\omega]$ ist euklidisch und damit insbesondere faktoriell.*

Beweis. Nach [HW75], Beginn Kap. 12.9, ist die Norm auf $\mathbb{Z}[\omega]$ gegeben durch $N(a + b\omega) = (a + b\omega)(a + b\omega^2)$. Wir vereinfachen den Funktionsterm von N mit Hilfe der Identitäten

$$\omega^3 = 1 \quad \text{und} \quad \omega + 1 = -\omega^2, \tag{3.2}$$

die daraus resultieren, dass ω Nullstelle von $T^3 - 1$ und $T^2 + T + 1$ ist:

$$N(a + b\omega) = (a + b\omega)(a + b\omega^2) = a^2 + ab(\omega^2 + \omega) + b^2\omega^3 \overset{(3.2)}{=} a^2 - ab + b^2.$$

Die folgende Rechnung zeigt nun, dass die Norm auf $\mathbb{Z}[\omega]$ (genauso wie die Norm auf $\mathbb{Z}[\mathrm{i}]$) dem Betragsquadrat einer komplexen Zahl entspricht:

$$|a+b\omega|^2 = \left|a - \frac{b}{2} \pm \frac{\sqrt{3}b}{2}\mathrm{i}\right|^2 = \left(a - \frac{b}{2}\right)^2 + \left(\frac{\sqrt{3}b}{2}\right)^2 = a^2 - ab + \underbrace{\frac{b^2}{4} + \frac{3b^2}{4}}_{=b^2} = N(a+b\omega).$$

Ab hier läuft der Beweis analog zum Beweis von Satz 3.6, da der Abstand eines Punktes $\pi = \eta/\vartheta$ mit $\eta, \vartheta \in \mathbb{Z}[\omega]$, $\vartheta \neq 0$, zum nächsten Gitterpunkt laut Abb. 3.2 kleiner gleich dem Umkreisradius $1/\sqrt{3} < 1$ eines der gleichseitigen Dreiecke ist. □

3.3. Der Ring $\mathbb{Z}[\zeta_p]$ für eine ungerade Primzahl p

Nach Ende von Abschnitt 3.1 kennen wir die Form des p-ten Kreisteilungskörpers für eine ungerade Primzahl p als

$$\mathbb{Q}(\zeta_p) = \{a_0 + a_1\zeta_p + \ldots + a_{p-2}\zeta_p^{p-2} \mid a_j \in \mathbb{Q}\}.$$

Dass $\mathbb{Z}[\zeta_p]$ tatsächlich der Ganzheitsring von $\mathbb{Q}(\zeta_p)$ ist (eine Aussage, die nicht trivial zu beweisen ist), wird z. B. als Proposition 1.2 in [Was97] gezeigt. Allerdings wissen wir damit noch wenig über Gestalt und Eigenschaften von $\mathbb{Z}[\zeta_p]$. Wir beginnen mit der Gestalt und brauchen dafür zuerst den Begriff des R-Moduls:

Definition 3.10. ([Bos18], Beginn Kap. 2.9)
Ein *R-Modul* $(M, +, \cdot)$ ist eine Menge M mit zwei Verknüpfungen $+\colon M \times M \to M$ und $\cdot\colon R \times M \to M$, so dass wie bei Vektorräumen $(M, +)$ eine abelsche Gruppe ist und bzgl. der Multiplikation "$\cdot$" für alle $r, s \in R$ und $x, y \in M$ gilt:

$$\begin{aligned} r \cdot (x + y) &= r \cdot x + r \cdot y, \\ (r + s) \cdot x &= r \cdot x + s \cdot x, \\ r \cdot (s \cdot x) &= (rs) \cdot x, \\ 1 \cdot x &= x. \end{aligned}$$

Als abelsche Gruppe weist $\mathbb{Z}[\zeta_p]$ die Struktur eines $\mathbb{Z}$-Moduls auf ([MSP11], nach Definition 6.1). Nun benötigen wir noch den Begriff der Ganzheitsbasis:

Definition 3.11. ([Sch07], Definition 6.1.9)
Eine Menge $\{r_1, \ldots, r_m\}$ von Elementen eines Rings R heißt *Ganzheitsbasis* von R, wenn sich jedes Ringelement $r \in R$ eindeutig als $\mathbb{Z}$-Linearkombination

$$r = a_1 r_1 + \ldots + a_m r_m,$$

$a_1, \ldots, a_m \in \mathbb{Z}$, darstellen lässt.

Lemma 3.12. *Die Zahlen* $1, \zeta_p, \ldots, \zeta_p^{p-2}$ *bilden eine Ganzheitsbasis von* $\mathbb{Z}[\zeta_p]$.

Beweis. Ein Beweis findet sich z. B. in [Neu07] als Beweis von Satz 10.2. □

Vereinfacht gesagt haben somit $\mathbb{Z}[\zeta_p]$ und $\mathbb{Q}(\zeta_p)$ eine gleiche "Basis" mit dem Unterschied, dass $\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$ einmal eine Ganzheitsbasis/Basis eines $\mathbb{Z}$-Moduls und im anderen Fall eine $\mathbb{Q}$-Vektorraumbasis ist.

Über die allgemeine Länge einer Basis von $\mathbb{Z}[\zeta_p]$ gibt die folgende Aussage Auskunft:

Satz 3.13. *Sei L ein Zahlkörper mit Ganzheitsring $\mathcal{O}_L$. Ist $[L : \mathbb{Q}] = n$, dann hat $\mathcal{O}_L$ eine Ganzheitsbasis der Länge n.*

Beweis. Wir verweisen auf Satz 6.1.10 aus [Sch07], der durch den letzten Absatz des Kapitels 6.1 ergänzt wird. □

Bemerkung 3.14. Da $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \varphi(p) = p - 1$ ist, hat $\mathbb{Z}[\zeta_p]$ eine Ganzheitsbasis der Länge $p - 1$.

Wir kommen nun zur Frage nach der Eindeutigkeit der Primzerlegung in $\mathbb{Z}[\zeta_p]$. Aus Bemerkung A.26 wissen wir, dass die Idealklassengruppe eines Zahlkörpers L endlich ist. Weiter ist $\mathcal{O}_L$ genau dann faktoriell, wenn $h_L = 1$ ist (Satz A.27):

Satz 3.15. *([IR90], Kap. 13.3, Notes)*
Sei p eine ungerade Primzahl. Der prime zyklotomische Körper $\mathbb{Q}(\zeta_p)$ hat Klassenzahl eins für $p = 3, 5, 7, 11, 13, 17$ und 19.

Bemerkung 3.16. Nach Satz A.19 ist der Ganzheitsring $\mathcal{O}_L$ eines Zahlkörpers L ein Dedekind-Ring (s. Definition A.17). Also besitzt $\mathbb{Z}[\zeta_p]$ genau dann eindeutige Primelementzerlegung, wenn p eine der in Satz 3.15 genannten Primzahlen ist, während für *jede* ungerade Primzahl p ein von $\langle 0\rangle$ und $\mathbb{Z}[\zeta_p]$ verschiedenes Ideal von $\mathbb{Z}[\zeta_p]$ eindeutig in Primideale zerlegbar ist (Satz A.18).

Wir haben uns in diesem Abschnitt sinnvollerweise auf Inhalte beschränkt, die eine Vorstellung von $\mathbb{Z}[\zeta_p]$ erlauben und die für den Beweis für n gleich reguläre Primzahl notwendig sind (so wie wir es in Abschnitt 3.2 für $n = 3$ getan haben). Für die ausgewählten Beweise werden jeweils noch weitere, allerdings spezifischere, Aussagen benötigt, die wir dann als Hilfssätze dem jeweiligen Beweis voranstellen.

Zum Abschluss geben wir als Beispiel die Zerlegung eines Hauptideals von $\mathbb{Z}[\zeta_{23}]$ in Primideale an. Und zwar zerfällt $\langle 2\rangle$ nach [Was97], Kap. 2, Remark, in Ideale $\mathfrak{p}$ und $\overline{\mathfrak{p}}$, die von zwei ganz-algebraischen Zahlen erzeugt werden:

$$\langle 2\rangle = \langle 2, 1 + \sqrt{-23}\rangle\langle 2, 1 - \sqrt{-23}\rangle.$$

4. Die Gleichung $x^n + y^n = z^n$

In diesem Hauptkapitel der Arbeit werden wir Fermats großen Satz für ausgewählte Exponenten n beweisen:

Satz 4.1. *(Fermats großer Satz)*
Die Gleichung

$$x^n + y^n = z^n, \qquad xyz \neq 0, \tag{4.1}$$

besitzt für eine natürliche Zahl $n > 2$ keine ganzzahlige Lösung.

Die Voraussetzung "$xyz \neq 0$" ist gleichbedeutend mit "$x \neq 0$, $y \neq 0$ und $z \neq 0$". Dadurch werden die "trivialen" Lösungen ausgeschlossen: Ist nämlich $xy = 0$, so lösen $z, 0, z$ und $0, z, z$ Gleichung (4.1) für ungerade n bzw. $\pm z, 0, \pm z$ und $0, \pm z, \pm z$ für gerade n. Ist $z = 0$, so ist $x, -x, 0$ die einzige Lösung für ungerade n und $0, 0, 0$ die einzige für gerade n (vgl. auch [Bun08], Kap. 4.2.1).

Zunächst diskutieren wir in den ersten beiden Abschnitten den neben $n = 1$ einzigen und einzig interessanten Fall $n = 2$, für den Gleichung (4.1) nichttrivial lösbar ist. Hauptziel ist die Bestimmung der allgemeinsten Form pythagoräischer Tripel (Satz 4.5), mittels der sich systematisch alle ganzzahligen Lösungen von $x^2+y^2 = z^2$ erzeugen lassen. In Unterkapitel 4.2 betrachten wir den Fall $n = 2$ geometrisch. In Unterkapitel 4.3 beweisen wir dann Fermats großen Satz für den einfachsten Fall $n = 4$ mit Hilfe von Satz 4.5.

Bis hierhin argumentieren wir innerhalb der ganzen Zahlen. In Abschnitt 4.4 verfolgen wir nun als "Zwischenspiel" die Idee, wie sich Satz 4.1 über den Zahlbereichen $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ einerseits (Teil 1) und andererseits über einem Polynomring über einem Körper verhält (Teil 2). An Letzterem ist interessant, dass der untersuchte Beweis den in Kapitel 2 beschriebenen klassischen Ansatz über die Faktorisierung von $x^p + y^p$ verfolgt. Außerdem erweist sich der Beweis als deutlich einfacher als der von Satz 4.1 für $n = 3$ (Abschnitt 4.5) oder n gleich reguläre Primzahl (Abschnitt 4.6). Im Fall $n = 3$ argumentieren wir im Ganzheitsring $\mathbb{Z}[\zeta_3]$, der in Abschnitt 3.2 beschrieben ist. Während für uns bedeutsame Wesenszüge von $\mathbb{Z}[\zeta_p]$ in Abschnitt 3.3 dargelegt sind, kann der theoretische Hintergrund für die Abschnitte 3.2 und 3.3 wiederum in Anhang B nachgeschlagen werden.

Bei allen betrachteten Sonderfällen von Fermats großem Satz (einschließlich dem "Zwischenspiel") nehmen wir zunächst die Existenz einer Lösung x, y, z an und führen dann (außer im letzten Fall) die Annahme durch die Methode des *unendlichen Abstiegs* zum Widerspruch. Diese von Fermat nachentdeckte Vorgehensweise ist eine Form des Unmöglichkeitsbeweises. Hierbei wird ausgenutzt, dass es in einer Teilmenge von $\mathbb{N}$ keine unendliche, monoton fallende Folge gibt. Ausgangspunkt bildet die Annahme, dass ein gegebenes Problem eine (Teil-)Lösung in den natürlichen Zahlen hat. Gelingt

es nun, zu zeigen, dass zu einer jeden Lösung eine kleinere existiert, so läge eine solche Folgen vor – Widerspruch. Ein klassisches Beispiel ist der Widerspruchsbeweis der Irrationalität von $\sqrt{2}$ von Euklid (vgl. [Woh11], Einleitung Kap. 6.1).

4.1. Der Fall $n = 2$ arithmetisch

Mit einer Gleichung der Gestalt $x^2 + y^2 = z^2$ wird (spätestens bei Benennung der Variablen als a, b und c) gemeinhin der Satz des Pythagoras assoziiert:

In einem rechtwinkligen Dreieck sind die Quadrate der beiden Katheten x und y gleich dem Quadrat der Hypotenuse z; in Formeln (und im Bild)

$$x^2 + y^2 = z^2. \tag{4.2}$$

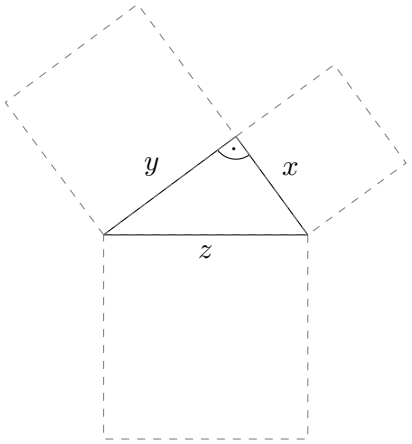

Abb. 4.1.: Rechtwinkliges Dreieck mit Seitenquadraten (Quelle: eigen)

Das Standardbeispiel ist $3^2 + 4^2 = 5^2$. Bekanntlich genügen der Gleichung (4.2) nicht nur natürliche Zahlen. Beschränkt man sich auf ganzzahlige Lösungen, dann löst aufgrund der Quadrate ein Tripel (x, y, z) natürlicher Zahlen (4.2) genau dann, wenn $(\pm x, \pm y, \pm z)$ es tut. Daher können wir uns im Folgenden bedenkenlos auf $x, y, z \in \mathbb{N}$ beschränken:

Definition 4.2. Lösungen x, y, z der Gleichung $x^2 + y^2 = z^2$ in natürlichen Zahlen heißen *pythagoräische Tripel*. Gilt weiter $\mathrm{ggT}(x, y, z) = 1$, so heißt (x, y, z) *primitives* pythagoräisches Tripel ([OS15], Aufgabe 7.4).

Die Lösungen der diophantischen Gleichung $x^2 + y^2 = z^2$

Wie der Name erwarten lässt, wurden im antiken Griechenland pythagoräische Tripel berechnet. Tatsächlich kann deren Suche mindestens bis in das altbabylonische Reich (ca. 1900–1600 v. Chr.) zurückverfolgt werden ([ADNE+14], S. 43).

Grundsätzlich genügen für eine Lösung x, y, z wegen

$$(mx)^2 + (my)^2 = m^2(x^2 + y^2) = (mz)^2$$

auch die Vielfachen mx, my, mz der Gleichung (4.2). Ist (x, y, z) primitiv, so sind x, y, z (wie gerade definiert wurde) teilerfremd. Wie wir gleich in Lemma 4.3 a) sehen werden, ist das gleichbedeutend damit, dass x, y, z *paarweise* teilerfremd sind. Folglich sind primitive pythagoräische Tripel die Grundbausteine aller ganzzahligen Lösungen von (4.2), da sie nicht weiter reduziert werden können.

Lemma 4.3 benennt zwei Eigenschaften einer (hypothetischen) Lösung der Fermat-Gleichung und ist ein Hilfssatz für den Beweis einer Formel zur Erzeugung primitiver pythagoräischer Tripel (vgl. [Bun08], letzter Absatz Kap. 4.2.1):

Lemma 4.3. *Seien x, y, z, $xyz \neq 0$, ganzzahlig und $n \geq 2$ eine natürliche Zahl mit $x^n + y^n = z^n$. Dann gilt:*

a) *x, y, z sind genau dann teilerfremd, wenn sie paarweise teilerfremd sind.*

b) *Sei $n = 2$. Sind x, y, z teilerfremd, so ist z ungerade und x und y haben unterschiedliche Parität.*

Bemerkung 4.4. Ist $\mathrm{ggT}(x, y, z) > 1$, dann folgt aus Lemma 4.3 a), indem man die Identität $x^n + y^n = z^n$ durch die n-te Potenz von $\mathrm{ggT}(x, y, z)$ teilt, die Existenz paarweise teilerfremder X, Y, Z mit $X^n + Y^n = Z^n$ (s. Beweis).

Beweis von Lemma 4.3.

a) Die Rückrichtung ist klar und gilt allgemein. Wir zeigen die Rechtsimplikation durch Kontraposition. Sei dafür zunächst $\mathrm{ggT}(x, y) = d > 1$. Dann gilt

$$z^n = x^n + y^n = (Xd)^n + (Yd)^n = (X^n + Y^n)d^n$$

und damit auch $d \mid z$. Ähnlich gilt für $\mathrm{ggT}(x, z) = d$

$$x^n + y^n = (Xd)^n + y^n = (Zd)^n \iff y^n = d^n(Z^n - X^n),$$

also auch $d \mid y$. Der letzte Fall "$\mathrm{ggT}(y, z) = d$" ist dem zweiten analog.

b) Die Parität von z folgt aus der von x und y. Diese bestimmen wir wie in [Bun08] (ebd.) per Ausschluss:

Ungerade $x = 2M + 1$ und $y = 2N + 1$ wären $\equiv \pm 1 \pmod 4$, d.h. $x, y \in [\pm 1]$. Aus $x^2 = 4(M^2 + M) + 1$ und $y^2 = 4(N^2 + N) + 1$ folgt dann $x^2 + y^2 \in [2]$. Allerdings ist $z^2 \notin [2]$, da eine gerade Quadratzahl $\equiv 0 \pmod 4$ und eine ungerade $\equiv 1 \pmod 4$ ist.

Da nach a) andererseits $\mathrm{ggT}(x, y) = 1$ gilt, können x und y auch nicht beide gerade sein. Also haben x, y und damit x^2, y^2 unterschiedliche Parität, weshalb z^2 bzw. z ungerade ist. □

Sei künftig ohne Einschränkung x gerade. Pythagoras selbst wird eine Formel zugeschrieben, mit der unendlich viele, jedoch weder alle noch ausschließlich *primitive* pythagoräische Tripel generiert werden können ([Bun08], Beginn Kap. 4.2.1). Mittels Lemma 4.3 können wir nun einen Satz beweisen, der eine Konstruktionsvorschrift umfasst, die auf Euklids *Elemente*, Buch X, zurückgeht (ebd., Beginn Kap. 4.2.2):

Satz 4.5. *Die Zahlen x, y und z bilden genau dann ein primitives pythagoräisches Tripel, wenn*

$$x = 2ab, \quad y = a^2 - b^2 \quad \textit{und} \quad z = a^2 + b^2 \tag{4.3}$$

ist für teilerfremde ganzzahlige $a > b > 0$ unterschiedlicher Parität ([OS15], Satz 7.4).

Bemerkung 4.6. Mit der Rückrichtung des Theorems lassen sich systematisch alle primitiven pythagoräischen Tripel generieren, z.B. indem man für $a = 2, 3, 4, \ldots$ jeweils alle $0 < b < a$ mit $\mathrm{ggT}(a, b) = 1$ und $a + b \equiv 1 \pmod 2$ bestimmt. Auf S. 19 sind sämtliche primitiven pythagoräischen Tripel (x, y, z) bis $z = 1285$ aufgelistet. Darauf aufbauend sind – wie wir dargelegt haben – genau alle $(\pm mx, \pm my, \pm mz)$ mit $m \in \mathbb{N}$ die nichttrivialen ganzzahligen Lösungen von Gleichung (4.2).

Beweis von Satz 4.5. Wir beginnen mit der Rückrichtung. Die Zahlen $x = 2ab$, $y = a^2 - b^2$ und $z = a^2 + b^2$ eingesetzt in (4.2) ergeben wie gewünscht

$$x^2 + y^2 = 4a^2b^2 + a^4 - 2a^2b^2 + b^4 = (a^2 + b^2)^2 = z^2. \tag{4.4}$$

Um zu zeigen, dass (x, y, z) primitiv ist, nehmen wir wegen $2 \nmid y$ bzw. $2 \nmid z$ zunächst einen gemeinsamen Primteiler $p > 2$ von x, y, z an. Mit $\mathrm{ggT}(a, b) = 1$ und dem Lemma von Euklid folgt dann einerseits aus $p \mid x = 2ab$ *entweder* $p \mid a$ *oder* $p \mid b$. Andererseits folgt aus $p \mid y = a^2 - b^2$ jedoch, dass p entweder a *und* b oder *keins von beiden* teilt, Widerspruch. Also ist (x, y, z) ein primitives pythagoräisches Tripel.

Die Rechtsimplikation orientiert sich an den Beweisen von [HW75], Theorem 225, und [OS15], Satz 7.4: Wir wählen nun umgekehrt ein primitives pythagoräisches Tripel (x, y, z) und zeigen (1) $x = 2ab$, $y = a^2 - b^2$, $z = a^2 + b^2$ für (2) teilerfremde ganze Zahlen $a > b > 0$ unterschiedlicher Parität.

(1) Wir betrachten

$$\frac{z + y}{2} \quad \text{und} \quad \frac{z - y}{2}. \tag{4.5}$$

Da nach Lemma 4.3 b) y und z ungerade sind, sind die beiden Ausdrücke ganzzahlig. Obendrein sind sie teilerfremd: Angenommen,

$$d \mid \frac{z + y}{2} \text{ und } d \mid \frac{z - y}{2} \implies d \mid \frac{z + y \pm (z - y)}{2},$$

also $d \mid y$ und $d \mid z$. Aus der Voraussetzung $\mathrm{ggT}(x, y, z) = 1$ folgt nach Lemma 4.3 a) jedoch $\mathrm{ggT}(y, z) = 1$, Widerspruch. Also sind die Ausdrücke teilerfremd.

Gemäß dritter binomischer Formel ist

$$\left(\frac{x}{2}\right)^2 = \frac{z^2 - y^2}{4} = \left(\frac{z + y}{2}\right)\left(\frac{z - y}{2}\right). \tag{4.6}$$

Wegen des Quadrats sind die Exponenten der Primfaktorzerlegung von $(x/2)^2$

gerade. Da beide Faktoren auf der rechten Seite teilerfremd sind, müssen auch ihre Primfaktoren gerade Exponenten haben. D. h., beide Faktoren sind Quadrate

$$\frac{z+y}{2} = a^2, \quad \frac{z-y}{2} = b^2. \tag{4.7}$$

Ohne Einschränkung gilt $a, b > 0$. Die linke Gleichung als $y = 2a^2 - z$ eingesetzt in die rechte ergibt $z = a^2 + b^2$ und daraus folgt wiederum $y = a^2 - b^2$, indem man z in eine der beiden Gleichungen einsetzt. Die Zahl x schließlich ergibt sich nun aus der Faktorisierung (4.6) zu $x^2 = z^2 - y^2 = 4a^2b^2$. Daher ist $x = 2ab$ wie gewünscht.

(2) Aus der Teilerfremdheit von a^2 und b^2 folgt unmittelbar $\mathrm{ggT}(a, b) = 1$.

Da z nach Lemma 4.3 b) ungerade ist, gilt zudem $z = a^2 + b^2 \equiv a + b \equiv 1 \pmod 2$. D. h., genau einer der Summanden a, b muss ungerade sein, weil ihre Summe $a + b$ bei Division durch 2 den Rest 1 lässt, also ungerade ist.

Schließlich ist wegen $y = a^2 - b^2 > 0$ (da a und b als positiv vorausgesetzt werden können) $a > b > 0$. □

4.2. Der Fall $n = 2$ geometrisch

Der folgende Abschnitt orientiert sich an [OS15], nach Aufgabe 7.6. Die in Satz 4.5 geschilderte Beziehung ergibt sich auch über einen geometrischen Zugang. Sei dazu (x, y, z) ein primitives pythagoräisches Tripel. Formen wir die Identität $x^2 + y^2 = z^2$ um zu

$$\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1, \tag{4.8}$$

so genügen $x/z, y/z \in \mathbb{Q}$ der Koordinatengleichung $X^2 + Y^2 = 1$ des Einheitskreises. D. h., es gibt eine Abbildung $f\colon (x, y, z) \mapsto (x/z, y/z)$ aus der Menge der primitiven pythagoräischen Tripel zu den Punkten des Einheitskreises mit positiven rationalen Koordinaten. Diese ist injektiv, denn aus $(x/z, y/z) = (x'/z', y'/z')$ folgt $x = dx'$, $y = dy'$, $z = dz'$ oder $x' = dx$, $y' = dy$, $z' = dz$, $d \in \mathbb{N}$. Wegen $\mathrm{ggT}(x, y, z) = \mathrm{ggT}(x', y', z') = 1$ ist $d = 1$ und damit $x = x'$, $y = y'$, $z = z'$.

Sei nun g_t eine Gerade durch den Nordpol $(0, 1)$ des Einheitskreises mit Steigung t und sei $(p, q) \in \mathbb{Q}^2$, $p \neq 0$, ihr zweiter Schnittpunkt (Abb. 4.2). Aus $1 = t \cdot 0 + c$ folgt

$$q = tp + 1. \tag{4.9}$$

Wir bestimmen p und q in Abhängigkeit von t, indem wir zuerst p und $q = tp + 1$ in $X^2 + Y^2 = 1$ und dann das Ergebnis in die Geradengleichung (4.9) einsetzen:

$$\begin{aligned} 1 = p^2 + (tp+1)^2 = p^2 + t^2p^2 + 2tp + 1 \quad &\overset{-1}{\Longleftrightarrow} \quad 0 = p(p + t^2p + 2t) \\ &\overset{:p\neq 0}{\Longleftrightarrow} \quad 0 = p(1 + t^2) + 2t. \end{aligned}$$

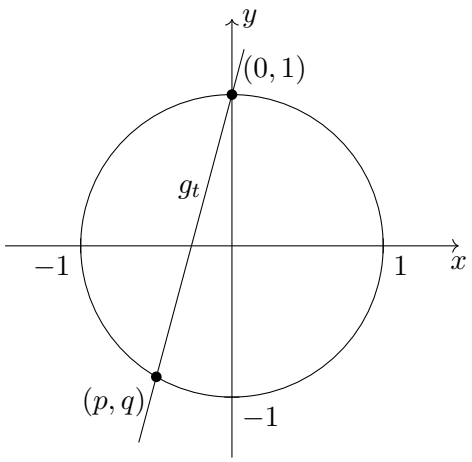

Abb. 4.2.: Sekante durch den Einheitskreis (Quelle: eigen)

Dann ist $p = -\frac{2t}{1+t^2}$ und somit

$$q \overset{(4.9)}{=} -t \cdot \frac{2t}{1+t^2} + 1 = -\frac{2t^2}{1+t^2} + \frac{1+t^2}{1+t^2} = \frac{1-t^2}{1+t^2}.$$

Da p und q rational sind, ist t es auch. Wir setzen deshalb $t = -\frac{b}{a}$ für teilerfremde $a, b \in \mathbb{Z}$, $a \neq 0$. Damit ist

$$(p,q) = \left(\frac{-2t}{1+t^2}, \frac{1-t^2}{1+t^2}\right) = \left(\frac{2\,{}^b\!/_a}{1+({}^b\!/_a)^2}, \frac{1-({}^b\!/_a)^2}{1+({}^b\!/_a)^2}\right) \overset{\cdot {}^{a^2}\!/_{a^2}}{=} \left(\frac{2ab}{a^2+b^2}, \frac{a^2-b^2}{a^2+b^2}\right).$$

Abhängig davon, in welchem Quadranten oder ob (p, q) auf der x-Achse liegt, ist $2ab$ bzw. $a^2 - b^2$ positiv, negativ oder Null. Zu Beginn des Abschnitts hatten wir primitive pythagoräische Tripel auf Punkte des offenen Kreisbogens im 1. Quadranten des Einheitskreises abgebildet. Liegt (p, q) auf diesem Kreisbogen, so ist $a > b > 0$ und damit sind $\mathcal{X} \coloneqq 2ab$, $\mathcal{Y} \coloneqq a^2 - b^2$ und $\mathcal{Z} \coloneqq a^2 + b^2$ jeweils > 0.

Ohne Einschränkung sind $p = {}^{\mathcal{X}}\!/_{\mathcal{Z}}$, $q = {}^{\mathcal{Y}}\!/_{\mathcal{Z}}$ vollständig gekürzt. Da der Zähler $2ab$ gerade ist, muss der Nenner $a^2 + b^2$ ungerade sein. Nach Beweis von Satz 4.5 haben dann a und b unterschiedliche Parität. Somit ist $(\mathcal{X}, \mathcal{Y}, \mathcal{Z})$ nach Satz 4.5 ein primitives pythagoräisches Tripel. Also gibt es auch eine Abbildung $f^{-1}\colon ({}^{\mathcal{X}}\!/_{\mathcal{Z}}, {}^{\mathcal{Y}}\!/_{\mathcal{X}}) \mapsto (\mathcal{X}, \mathcal{Y}, \mathcal{Z})$ aus der Menge der Punkte des Einheitskreises mit positiven rationalen Koordinaten zur Menge der primitiven pythagoräischen Tripel. Da f^{-1} ebenfalls injektiv ist, ist f somit bijektiv ([SV12], S. 40f).

Bemerkung 4.7. Um den gesamten Einheitskreis einzubeziehen, müssen wir anfangs $(\pm x, \pm y, \pm z)$ abbilden, wobei wie bisher (x, y, z) ein primitives pythagoräisches Tripel ist. Im Übrigen wird die Primitivität benötigt, damit f bijektiv ist. Andernfalls würden z. B. $(3, 4, 5)$ und $(6, 8, 10)$ auf denselben Punkt $({}^3\!/_5, {}^4\!/_5)$ abgebildet.

(3, 4, 5)	(68, 285, 293)	(231, 520, 569)	(348, 805, 877)
(5, 12, 13)	(207, 224, 305)	(48, 575, 577)	(369, 800, 881)
(8, 15, 17)	(136, 273, 305)	(368, 465, 593)	(451, 780, 901)
(7, 24, 25)	(25, 312, 313)	(240, 551, 601)	(60, 899, 901)
(20, 21, 29)	(75, 308, 317)	(35, 612, 613)	(616, 663, 905)
(12, 35, 37)	(204, 253, 325)	(105, 608, 617)	(464, 777, 905)
(9, 40, 41)	(36, 323, 325)	(336, 527, 625)	(43, 924, 925)
(28, 45, 53)	(175, 288, 337)	(429, 460, 629)	(533, 756, 925)
(11, 60, 61)	(180, 299, 349)	(100, 621, 629)	(129, 920, 929)
(33, 56, 65)	(225, 272, 353)	(200, 609, 641)	(215, 912, 937)
(16, 63, 65)	(27, 364, 365)	(315, 572, 653)	(580, 741, 941)
(48, 55, 73)	(76, 357, 365)	(300, 589, 661)	(301, 900, 949)
(13, 84, 85)	(252, 275, 373)	(385, 552, 673)	(420, 851, 949)
(36, 77, 85)	(135, 352, 377)	(52, 675, 677)	(615, 728, 953)
(39, 80, 89)	(152, 345, 377)	(37, 684, 685)	(387, 884, 965)
(65, 72, 97)	(189, 340, 389)	(156, 667, 685)	(124, 957, 965)
(20, 99, 101)	(228, 325, 397)	(111, 680, 689)	(248, 945, 977)
(60, 91, 109)	(40, 399, 401)	(400, 561, 689)	(473, 864, 985)
(15, 112, 113)	(120, 391, 409)	(185, 672, 697)	(696, 697, 985)
(44, 117, 125)	(29, 420, 421)	(455, 528, 697)	(372, 925, 997)
(88, 105, 137)	(87, 416, 425)	(260, 651, 701)	(559, 840, 1009)
(17, 144, 145)	(297, 304, 425)	(259, 660, 709)	(45, 1012, 1013)
(24, 143, 145)	(145, 408, 433)	(333, 644, 725)	(660, 779, 1021)
(51, 140, 149)	(203, 396, 445)	(364, 627, 725)	(496, 897, 1025)
(85, 132, 157)	(84, 437, 445)	(108, 725, 733)	(315, 988, 1037)
(119, 120, 169)	(280, 351, 449)	(407, 624, 745)	(645, 812, 1037)
(52, 165, 173)	(168, 425, 457)	(216, 713, 745)	(620, 861, 1061)
(19, 180, 181)	(261, 380, 461)	(468, 595, 757)	(731, 780, 1069)
(57, 176, 185)	(31, 480, 481)	(39, 760, 761)	(495, 952, 1073)
(104, 153, 185)	(319, 360, 481)	(481, 600, 769)	(585, 928, 1097)
(95, 168, 193)	(93, 476, 485)	(195, 748, 773)	(47, 1104, 1105)
(28, 195, 197)	(44, 483, 485)	(273, 736, 785)	(744, 817, 1105)
(133, 156, 205)	(155, 468, 493)	(56, 783, 785)	(141, 1100, 1109)
(84, 187, 205)	(132, 475, 493)	(432, 665, 793)	(235, 1092, 1117)
(21, 220, 221)	(217, 456, 505)	(168, 775, 793)	(329, 1080, 1129)
(140, 171, 221)	(336, 377, 505)	(555, 572, 797)	(423, 1064, 1145)
(60, 221, 229)	(220, 459, 509)	(280, 759, 809)	(765, 868, 1157)
(105, 208, 233)	(279, 440, 521)	(429, 700, 821)	(517, 1044, 1165)
(120, 209, 241)	(308, 435, 533)	(540, 629, 829)	(611, 1020, 1189)
(32, 255, 257)	(92, 525, 533)	(41, 840, 841)	(49, 1200, 1201)
(23, 264, 265)	(341, 420, 541)	(123, 836, 845)	(147, 1196, 1205)
(96, 247, 265)	(33, 544, 545)	(116, 837, 845)	(245, 1188, 1213)
(69, 260, 269)	(184, 513, 545)	(205, 828, 853)	(705, 992, 1217)
(115, 252, 277)	(165, 532, 557)	(232, 825, 857)	(441, 1160, 1241)
(160, 231, 281)	(396, 403, 565)	(287, 816, 865)	(539, 1140, 1261)
(161, 240, 289)	(276, 493, 565)	(504, 703, 865)	(637, 1116, 1285)

Tab. 4.1.: Die ersten primitiven pythagoräischen Tripel (Quelle: eigen)

4.3. Der Fall $n = 4$

Es mag seltsam anmuten, dass Gleichung (4.1) für $n = 2$, nicht aber für $n = 4$ von Null verschiedene ganzzahlige Lösungen haben soll. Fermats großer Satz sagt also aus, dass bei pythagoräischen Tripeln (x, y, z) nicht alle drei Zahlen gleichzeitig Quadratzahlen sind. Tatsächlich ist in Tabelle 4.1 (S. 19) jeweils höchstens eines der x, y, z Quadratzahl, z. B. $x = 6^2$, $y = 77$, $z = 85$.

Satz 4.8. *(Fermats großer Satz für $n = 4$)*
Die Gleichung

$$x^4 + y^4 = z^4, \qquad xyz \neq 0, \tag{4.10}$$

besitzt keine ganzzahlige Lösung.

Zur besseren Nachvollziehbarkeit erläutern wir zuerst die

Beweisidee. Der Beweis orientiert sich an den ähnlichen Beweisen von Theorem 226 in [HW75] und Satz 7.5 in [OS15]: Wir betrachten die leicht abgewandelte Gleichung $x^4 + y^4 = w^2$, $xyw \neq 0$. Hat diese keine ganzzahlige Lösung, so gilt das wegen $z = w^2$ auch für (4.10). Ausgehend von ganzzahligen x, y, w mit $x^4 + y^4 = w^2$, wobei w als minimal vorausgesetzt wird, erkennen wir nach Satz 4.5 in $x^2 = 2ab$, $y^2 = a^2 - b^2$ und $w = a^2 + b^2$ ein primitives pythagoräisches Tripel. Durch geschickte Ausnutzung von Zahlbeziehungen versuchen wir dann y sowie die Teiler f, d von a und b erneut als primitives pythagoräisches Tripel festzustellen. Infolgedessen finden sich ganze Zahlen $\mathcal{X}, \mathcal{Y}$ mit $\mathcal{X}\mathcal{Y}d \neq 0$, $\mathcal{X}^4 + \mathcal{Y}^4 = d^2$ und $d < w$ im Widerspruch zur Minimalität von w (vgl. Methode des (in diesem Fall nicht) unendlichen Abstiegs am Ende der Einleitung zu Kapitel 4).

Beweis von Satz 4.8. Wir betrachten die modifizierte Fermat-Gleichung

$$x^4 + y^4 = w^2, \tag{4.11}$$

$xyw \neq 0$, und nehmen an, sie sei ganzzahlig lösbar. Unter allen Lösungen x, y, w wählen wir diejenige mit kleinstem w. Daraus folgt $\mathrm{ggT}(x, y) = 1$. Andernfalls könnten wir in (4.11) den größten gemeinsamen Teiler t von x, y als t^4 ausklammern, d. h. $t^2 \mid w$, womit w nicht minimal wäre. Also sind x, y, w und damit auch x^2, y^2, w teilerfremd.

Nach Satz 4.5 bilden x^2, y^2, w somit ein primitives pythagoräisches Tripel,

$$x^2 = 2ab, \quad y^2 = a^2 - b^2, \quad w = a^2 + b^2, \tag{4.12}$$

wobei $a > b > 0$ teilerfremd und unterschiedlicher Parität sind[†]. Genauer muss a ungerade und b gerade sein. Andernfalls wäre

$$y^2 = a^2 - b^2 = (2M)^2 - (2N + 1)^2 = 4M^2 - 4(N^2 + N) - 1 \equiv -1 \pmod 4$$

[†]In Abschnitt 4.1 hatten wir bei primitiven pythagoräischen Tripeln (X, Y, Z) ohne Einschränkung X als die gerade und Y als die ungerade der beiden Zahlen festgelegt.

im Widerspruch zu $y^2 = 4(m^2+m)+1 \equiv 1 \pmod 4$. Also können wir $b = 2c$ setzen.

Wir betrachten nun die Identität

$$\left(\frac{x}{2}\right)^2 = \frac{x^2}{4} \overset{(4.12)}{=} \frac{ab}{2} = ac. \tag{4.13}$$

Da aus $\mathrm{ggT}(a,b) = 1$ genauso $\mathrm{ggT}(a,c) = 1$ folgt, sind die Faktoren a, c aufgrund ihrer eindeutigen Primfaktorzerlegung jeweils Quadrate

$$a = d^2, \qquad c = f^2 \tag{4.14}$$

mit $d > 0$, $f > 0$ (einen ähnlichen Schritt sind wir beim Beweis von Satz 4.5 gegangen). Dabei ist, weil a, c teilerfremd sind und a ungerade ist, auch

$$\mathrm{ggT}(d,f) = 1 \quad \text{und} \quad d \text{ ungerade.} \tag{4.15}$$

Wegen (4.14) ist nun $y^2 = a^2 - b^2 = (d^2)^2 - (2c)^2 = (d^2)^2 - (2f^2)^2$, d.h.

$$(2f^2)^2 + y^2 = (d^2)^2.$$

Dabei sind $d^2, 2f^2, y$ teilerfremd, denn aus (4.15) folgt $\mathrm{ggT}(d^2, 2f^2) = 1$ und damit insbesondere $\mathrm{ggT}(d^2, 2f^2, y) = 1$. Also bilden $2f^2, y, d^2$ ein primitives pythagoräisches Tripel, d.h., nach Satz 4.5 ist

$$f^2 = kl \text{ (genauer } 2f^2 = 2kl), \qquad d^2 = k^2 + l^2,$$

für teilerfremde $k > l > 0$ (sogar unterschiedlicher Parität). Hierbei folgt unmittelbar aus $\mathrm{ggT}(k,l) = 1$ (vgl. Lemma 4.3 a)), dass die Faktoren k, l wieder Quadrate $k = \mathcal{X}^2$ und $l = \mathcal{Y}^2$ sein müssen mit $\mathcal{X} > 0$, $\mathcal{Y} > 0$. Eingesetzt in $d^2 = k^2 + l^2$ ergeben sie die Identität

$$\mathcal{X}^4 + \mathcal{Y}^4 = d^2$$

und somit $\mathcal{X}, \mathcal{Y}, d$ als scheinbare Lösung von Gleichung (4.11). Jedoch steht

$$d \le d^2 = a \le a^2 < a^2 + b^2 = w$$

im Widerspruch zur eingangs vorausgesetzten Minimalität von w. Folglich war die Annahme einer ganzzahligen Lösung von $x^4 + y^4 = w^2$ mit $xyw \neq 0$ falsch und damit ist auch $x^4 + y^4 = z^4$ mit $xyz \neq 0$ nicht ganzzahlig lösbar. □

4.4. Zwischenspiel: Fermats großer Satz für Polynome

In diesem Zwischenkapitel spinnen wir den Gedanken, inwieweit Fermats großer Satz damit verträglich ist, wenn wir den Bereich $\mathbb{Z}$ durch $\mathbb{Q}$, $\mathbb{R}$ oder $\mathbb{C}$ (jeweils ausschließlich der Null; Teil 1) oder sogar durch einen Polynomring ersetzen (Teil 2). Der Beweis für Polynome beinhaltet dabei die Grundideen früherer Beweisversuche, namentlich vor dem Zugang über elliptische Kurven/Modulformen, die wir im zweiten Kapitel angeschnitten haben ([Ros97], Beginn §2).

Teil 1: Fermats großer Satz für andere Zahlbereiche

Wir beginnen damit, die Fermat-Gleichung $x^n + y^n = z^n$, $n \geq 2$, $xyz \neq 0$, über dem Körper $\mathbb{Q}$ zu betrachten. Sei hierfür eine Lösung $x = x_1/x_2$, $y = y_1/y_2$, $z = z_1/z_2$ mit ganzzahligen $x_1, x_2, y_1, y_2, z_1, z_2 \neq 0$ angenommen, d. h.

$$\left(\frac{x_1}{x_2}\right)^n + \left(\frac{y_1}{y_2}\right)^n = \left(\frac{z_1}{z_2}\right)^n. \tag{4.16}$$

Ohne Einschränkung sind x, y, z vollständig gekürzt. Für $n = 2$ ist jede ganzzahlige Lösung auch eine rationale (reelle/komplexe). Umgekehrt ist die Frage, ob es rationale Lösungen gibt, die nicht ganzzahlig sind. In (4.4) hatten wir gezeigt, dass $x = 2ab$, $y = a^2 - b^2$, $z = a^2 + b^2$ die Gleichung $x^2 + y^2 = z^2$ lösen, ohne dabei die Voraussetzung zu beachten, dass $a > b > 0$ teilerfremde natürliche Zahlen unterschiedlicher Parität sind. Somit können wir z.B. $a = p_1/p_2$ und $b = q_1/q_2$ rational wählen mit $p_1, p_2, q_1, q_2 \neq 0$, $\mathrm{ggT}(p_1, p_2) = 1$ und $\mathrm{ggT}(q_1, q_2) = 1$, und dadurch rationale Lösungen generieren.

Beispiel 4.9. Für $a = 1/2$, $b = 1/3$ ist $x = 1/3$, $y = 5/36$, $z = 13/36$ und damit

$$\left(\frac{1}{3}\right)^2 + \left(\frac{5}{36}\right)^2 = \frac{144}{1296} + \frac{25}{1296} = \frac{169}{1296} = \left(\frac{13}{36}\right)^2.$$

Bleibt noch der Fall $n > 2$. Multiplizieren wir hierfür die Gleichung (4.16) mit dem Produkt aus den Nennern (inkl. Exponent),

$$(x_1 y_2 z_2)^n + (x_2 y_1 z_2)^n = (x_2 y_2 z_1)^n,$$

so erhalten wir eine äquivalente Gleichung, deren Basen ganzzahlig-wertig sind und die damit nach Satz 4.1 unlösbar ist. Also bleibt Fermats großer Satz auch über $\mathbb{Q}$ wahr.

Über $\mathbb{R}$ und $\mathbb{C}$ ist dagegen klar, dass $x^n + y^n = z^n$ für jede Wahl von zwei der drei Zahlen x, y, z (bei $\mathbb{R}$ mit der Einschränkung, dass Radikanden nichtnegativ sein müssen) lösbar ist, weil $\mathbb{C}$ algebraisch abgeschlossen ist.

Teil 2: Fermats großer Satz für Polynome

Die Idee, Fermats großen Satz für Polynome zu betrachten, entstammt [Ros97], §1. Sei hierfür $K[T]$ ein Polynomring über einem Körper K der Charakteristik $q \geq 0$. Wir bemerken zunächst, dass Fermats großer Satz falsch wird, wenn wir statt ganzzahligen Lösungen polynomiale Lösungen x, y, z, $xyz \neq 0$, suchen, da die Fermat-Gleichung z.B. für $K = \mathbb{C}$ auch durch drei Konstanten lösbar ist (z.B. $1, 2, \sqrt[3]{9}$ für $n = 3$). Also schließen wir rein konstante Lösungen aus. Außerdem setzen wir x, y, z als teilerfremd voraus, da für jede konstante Lösung x, y, z auch Px, Py, Pz, $P \in K[T]$, der Fermat-Gleichung genügen. Schließlich ist auch der Fall $n = q^m$ trivial, da aufgrund der Homomorphie-Eigenschaft des Frobenius-Endomorphismus $x^{q^m} + y^{q^m} = (x + y)^{q^m}$ für beliebige x, y gilt.

Wir formulieren nun Fermats großen Satz für Polynome für eine ungerade Primzahl p:

Satz 4.10. *(FGS für Polynome für n gleich ungerade Primzahl p)*
Die Gleichung $x^p + y^p = z^p$, $xyz \neq 0$, hat für eine Primzahl $p > 2$ und teilerfremde $x, y, z \in K[T]$, wobei K ein Körper der Charakteristik $q \neq p$ ist, nur Konstanten als Lösung.

Beispiel 4.11. Für $n = 2$ löst $x = 2ab$, $y = a^2 - b^2$, $z = a^2 + b^2$ die Gleichung (4.1) unter den Voraussetzungen von Satz 4.10, wenn a, b von Null verschiedene Polynome und nicht beide konstant sind. So erhalten wir z.B. für $a = T$ und $b = 1$ die Polynome $x = 2T$, $y = T^2 - 1$, $z = T^2 + 1$ mit

$$(2T)^2 + (T^2 - 1)^2 = 4T^2 + T^4 - 2T^2 + 1 = T^4 + 2T^2 + 1 = (T^2 + 1)^2.$$

Wie in Kapitel 2 angekündigt, zeigen wir vor dem Beweis noch das folgende

Lemma 4.12. *Sei p eine ungerade Primzahl, $K[T]$ ein Polynomring über einem Körper K der Charakteristik $q \neq p$ und $x, y \in K[T] \setminus \{0\}$. Dann gilt*

$$x^p + y^p = \prod_{i=0}^{p-1} (x + \zeta_p^i y), \tag{4.17}$$

wobei ζ_p eine primitive p-te Einheitswurzel in $K^\times$ ist.

Beweis. Die Beweisidee stammt aus [Sch07], Einleitung Kap. 7.3. Bekanntermaßen ist $T^p - 1 = \prod_{i=0}^{p-1}(T - \zeta_p^i)$. Für $T = -x/y$ erhalten wir

$$\left(\frac{x}{-y}\right)^p - 1 = \prod_{i=0}^{p-1} \left(\frac{x}{-y} - \zeta_p^i\right).$$

Multiplikation mit $(-y)^p = -y^p$ liefert dann, indem wir jeden der p Faktoren rechts mit $-y$ multiplizieren, die Identität (4.17). □

Die Beweisgrundlage für Satz 4.10 bildet [Ros97], §1:

Beweis von Satz 4.10. Angenommen, es gäbe eine Lösung x, y, z, deren höchster Grad $d > 0$ ist. Bemerkung 4.4 gilt uneingeschränkt für Polynome, so dass wir x, y, z als *paarweise* teilerfremd voraussetzen können. Ähnlich wie im Fall $n = 4$ gehen wir nach der Methode des unendlichen Abstiegs vor, indem wir eine weitere Lösung x', y', z' finden, deren höchster Grad $d > d' > 0$ ist.

Weiter können wir K als algebraisch abgeschlossen voraussetzen, da die Koeffizienten von x, y, z insbesondere Elemente aus dem Abschluss sind. Wir faktorisieren $x^p + y^p$ gemäß Lemma 4.12, so dass wir die folgende Identität erhalten:

$$\prod_{i=0}^{p-1} \left(x + \zeta_p^i y\right) = z^p \tag{4.18}$$

Wir setzen $\zeta = \zeta_p$ und zeigen nun, dass die Faktoren $(x + \zeta^i y)$, $i = 0, \ldots, p-1$, paarweise teilerfremd sind. Angenommen, $t \mid (x + \zeta^i y)$ und $t \mid (x + \zeta^j y)$ für ein nicht-

konstantes Polynom $t \in K[T]$ und $i \neq j$. Dann teilt t auch die Differenzen

$$(x + \zeta^j y) - (x + \zeta^i y) = \zeta^j y - \zeta^i y = (\zeta^{j-i} - 1)\zeta^i y$$

und

$$\zeta^j(x + \zeta^i y) - \zeta^i(x + \zeta^j y) = \zeta^j x \cancel{+ \zeta^{i+j} y} - \zeta^i x \cancel{- \zeta^{i+j} y} = (\zeta^{j-i} - 1)\zeta^i x.$$

Da das Polynom $(\zeta^{j-i} - 1)\zeta^i$ konstant ist, folgt $t \mid x$ und $t \mid y$ im Widerspruch zur vorausgesetzten Teilerfremdheit von x und y.

Nun zerlegen wir z^p in p-te Potenzen irreduzibler Polynome (da K abgeschlossen ist, also in p-te Potenzen von Linearfaktoren). Die Faktorisierung ist, weil $K[T]$ ein ZPE-Ring ist, bis auf Einheiten und Reihenfolge der Faktoren eindeutig.

Da die Faktoren $(x + \zeta^i y)$, $i = 0, \ldots, p-1$, paarweise teilerfremd sind, wird jedes $(x+\zeta^i y)$ von der p-ten Potenz mindestens eines Linearfaktors geteilt, der hingegen alle $(x + \zeta^j y)$, $j \neq i$, nicht teilt. D.h., die Faktoren sind ein Produkt aus einer Konstanten λ und der p-ten Potenz eines Polynoms. Mehr noch ist auch λ eine p-te Potenz: Wegen $\lambda \in K$ ist $T^p - \lambda \in K[T]$, das wegen der Abgeschlossenheit eine Nullstelle in K hat, und zwar $\mu = \sqrt[p]{\lambda}$, so dass $\lambda = \mu^p$ ist.

Wir betrachten nun die ersten drei Faktoren aus Identität (4.18), die nunmehr p-te Potenzen von Polynomen sind:

$$x + y = u^p, \quad x + \zeta y = v^p, \quad x + \zeta^2 y = w^p. \tag{4.19}$$

Wir eliminieren x und y aus den drei Gleichungen, indem wir zunächst die erste in die zweite einsetzen:

$$x = u^p - y \implies x + \zeta y = u^p - y + \zeta y = u^p + (\zeta - 1)y = v^p \iff (\zeta - 1)y = v^p - u^p.$$

Einsetzen von x, y in die dritte Gleichung aus (4.19) ergibt dann

$$\begin{aligned}
\cancel{(\zeta - 1)} w^p &= (\zeta - 1)(u^p - y) + (\zeta - 1)\zeta^2 y \\
&= (\zeta - 1)u^p - (v^p - u^p) + \zeta^2(v^p - u^p) \\
&= \zeta u^p \cancel{- u^p} - v^p \cancel{+ u^p} + \zeta^2 v^p - \zeta^2 u^p \\
&= (\zeta^2 - 1)v^p - (\zeta - 1)\zeta u^p \\
&= (\zeta + 1)\cancel{(\zeta - 1)} v^p - \cancel{(\zeta - 1)}\zeta u^p,
\end{aligned}$$

also

$$w^p + \zeta u^p = (\zeta + 1)v^p. \tag{4.20}$$

Als Konstanten sind ζ und $(\zeta + 1)$, wie wir vorhin gesehen haben, p-te Potenzen. Deshalb können wir $x' = w$, $y' = \sqrt[p]{\zeta}\, u$ und $z' = \sqrt[p]{\zeta + 1}\, v$ setzen, so dass x', y', z' eine weitere Lösung der Fermat-Gleichung (4.1) ist. Hier geht auch die Voraussetzung $p > 2$ ein, denn für $p = 2$ wäre $\zeta_p = -1$ und folglich $z' = \sqrt{-1 + 1}\, v = 0$. Nach (4.19) ist $\operatorname{grad} x'^p = p \cdot \operatorname{grad} x' \leq p \cdot \max\{\operatorname{grad} x, \operatorname{grad} y\}$; Gleiches gilt auch für y'^p und z'^p. Da $\max\{\operatorname{grad} x, \operatorname{grad} y\} \leq d$ ist, haben x', y', z' somit den höchsten Grad $d' \leq d/p < d$. Wiederholen wir das gesamte Vorgehen für x', y', z' usw., so ist der höchste Grad einer weiteren Lösung – weil die Grade von Polynomen endlich sind – irgendwann gleich 0 im Widerspruch zur Voraussetzung $\max\{\operatorname{grad} x, \operatorname{grad} y, \operatorname{grad} z\} \geq 1$. □

4.5. Der Fall $n = 3$

In den Fällen $n = 2$ und $n = 4$ sowie bei Fermats großem Satz für Polynome haben wir u.a. genutzt, dass ganze Zahlen bzw. Polynome mit Koeffizienten aus einem Körper im Wesentlichen eindeutig in Irreduziblen zerlegbar sind. Den Beweis für $n = 3$ führen wir über dem Erweiterungsring $\mathbb{Z}[\omega]$ der Eisenstein-Zahlen, der in Abschnitt 3.2 entsprechend ausgearbeitet ist. Da – wie in Satz 3.9 gezeigt – $\mathbb{Z}[\omega]$ faktoriell ist, können wir weiter mit Eindeutigkeit der Primelementzerlegung argumentieren.

Satz 4.13. *(Fermats großer Satz für $n = 3$)*
Die Gleichung

$$x^3 + y^3 = z^3, \qquad xyz \neq 0, \tag{4.21}$$

besitzt keine ganzzahlige Lösung.

Bevor wir den Satz beweisen, geben wir ein Beispiel, das ihn "beinahe" widerlegt. Die Beweisführung folgt dann der von Theorem 227 aus [HW75] unter Zuhilfenahme des Beweises von Satz 3J aus [Rib79]. Anders als in [HW75] stellen wir ein dort integriertes Lemma voran, um uns auf das Wesentliche zu konzentrieren. Das Lemma baut wiederum auf einem Hilfssatz (also gewissermaßen einem "Lemma-Lemma") auf. Den Beweis von Satz 4.21 selbst strukturieren wir aufgrund dessen Länge in vier Zwischenbehauptungen.

Beispiel 4.14. Für $x = 6$, $y = 8$ und $z = 9$ gelingt es, zwei aus Einheitswürfeln aufgebaute Kuben der Kantenlänge x bzw. y zu einem dritten zusammenzusetzen, dem bloß ein Einheitswürfel fehlt: $6^3 + 8^3 = 9^3 - 1$ ([Sin97], S. 54).

Wie im Vorkapitel 3.2 verwenden wir nachfolgend lateinische Buchstaben für ganze und griechische Buchstaben für Eisenstein-Zahlen, um die Ausführungen übersichtlicher zu gestalten. Außerdem erinnern wir an die Identität (A), leiten (B) aus $\omega^2 + \omega + 1 = 0$ her, und definieren in (C) die Zahl λ:

$$\omega^3 = 1, \tag{A}$$
$$\omega + 1 = -\omega^2, \tag{B}$$
$$\lambda \coloneqq 1 - \omega. \tag{C}$$

Lemma 4.15. *Jede Eisenstein-Zahl η ist kongruent 0 oder kongruent ± 1 mod λ.*

Bemerkung 4.16. Für eine ganze Zahl a haben wir für den Modul 3 die analoge Aussage a kongruent 0 oder kongruent ± 1 mod 3.

Beweis von Lemma 4.15. Zum einen gilt für eine Eisenstein-Zahl

$$a + b\omega \;=\; a + (b - b) + b\omega \;=\; a + b - b(1 - \omega) \overset{(C)}{\equiv} a + b \pmod{\lambda}. \tag{4.22}$$

Zum anderen ist

$$3 = 1 + 1 + 1 \overset{(A+B)}{=} 1 + \omega^3 - \omega^2 - \omega = (1 - \omega^2) - \omega(1 - \omega^2) \overset{(C)}{=} \lambda(1 - \omega^2), \quad (4.23)$$

also $\lambda \mid 3$. Sei nun $c \in \{0, \pm 1\}$. Nach Bemerkung 4.16 ist $a + b \equiv c \pmod 3$, also $a + b = 3d + c$. Aus $\lambda \mid 3$ folgt weiter $3d + c = \lambda\delta + c$. Es gilt also $a + b \equiv c \pmod \lambda$. Mit (4.22) folgt dann $a + b\omega \equiv a + b \equiv c \pmod \lambda$. □

Lemma 4.17. *Ist eine Eisenstein-Zahl $\eta = a + b\omega$ nicht durch λ teilbar, dann ist $\eta^3 \equiv \pm 1 \pmod{\lambda^4}$.*

Beweis. Zunächst folgt aus $\lambda \nmid \eta$ nach dem "Lemma-Lemma" $\eta \equiv \pm 1 \pmod \lambda$. Aus Gründen der Übersicht setzen wir $\alpha := \pm\eta$, also $\alpha \equiv 1 \pmod \lambda$ bzw. $\alpha = \beta\lambda + 1$. Das Polynom $T^3 - 1 = (T - 1)(T - \omega)(T - \omega^2)$ betrachtend setzen wir $T = \alpha$, d.h.

$$\begin{aligned} \alpha^3 - 1 &= (\alpha - 1)(\alpha - \omega)(\alpha - \omega^2) \\ &= \beta\lambda(\beta\lambda + 1 - \omega)(\beta\lambda + 1 - \omega^2) \\ &\overset{(C)}{=} \beta\lambda(\beta\lambda + \lambda)\big(\beta\lambda + (1 + \omega)(1 - \omega)\big) \\ &\overset{(C)}{=} \beta\lambda^3(\beta + 1)\big(\beta + (1 + \omega)\big) \\ &\overset{(B)}{=} \lambda^3\beta(\beta + 1)(\beta - \omega^2) \end{aligned} \quad (4.24)$$

Betrachten wir nun $1 - \omega^2 = (1 - \omega)(1 + \omega) \overset{(C)}{=} \lambda(1 + \omega) \overset{(B)}{=} -\lambda\omega^2$, so ist $1 - \omega^2 \equiv 0 \pmod \lambda$, was äquivalent ist zu $\beta - \omega^2 \equiv \beta - 1 \pmod \lambda$ bzw.

$$\beta(\beta + 1)(\beta - \omega^2) \equiv \beta(\beta + 1)(\beta - 1) \pmod \lambda.$$

Nach Lemma 4.15 ist β, $\beta + 1$ oder $\beta - 1$ durch λ teilbar, d.h. $\beta(\beta + 1)(\beta - \omega^2) \equiv 0 \pmod \lambda$. Also ist

$$\lambda^3\beta(\beta + 1)(\beta - \omega^2) \equiv 0 \pmod{\lambda^4}.$$

Da hier nach (4.24) die linke Seite gleich $\alpha^3 - 1$ und außerdem $\alpha = \pm\eta$ ist, folgt $\pm\eta^3 - 1 = \alpha^3 - 1 \equiv 0 \pmod{\lambda^4}$ und daraus schließlich $\pm\eta^3 \equiv 1 \pmod{\lambda^4}$ bzw. $\eta^3 \equiv \pm 1 \pmod{\lambda^4}$. □

Nach dieser Vorarbeit kommen wir nun zum Beweis von Satz 4.13:

Beweis von Satz 4.13. Wir werden zeigen, dass die Gleichung

$$\xi^3 + \upsilon^3 + \zeta^3 = 0, \qquad \xi\upsilon\zeta \neq 0, \quad (4.25)$$

keine Lösung im Erweiterungsring $\mathbb{Z}[\omega]$ hat. Daraus folgt sodann insbesondere, dass $\xi^3 + \upsilon^3 = -\zeta^3$, $\xi\upsilon(-\zeta) \neq 0$, und damit (4.21) keine ganzzahlige Lösung hat.

Sei also angenommen, (4.25) besitzt eine Lösung ξ, υ, ζ in den Eisenstein-Zahlen. Nach Bemerkung 4.4 können wir ξ, υ, ζ als paarweise teilerfremd voraussetzen. Wir kommen nun zur ersten Zwischenbehauptung:

Lemma 4.18. *Gilt $\xi^3 + \upsilon^3 + \zeta^3 = 0$, dann ist genau eines der ξ, υ, ζ durch λ teilbar.*

Beweis. Wegen $\mathrm{ggT}(\xi, \upsilon) = \mathrm{ggT}(\xi, \zeta) = \mathrm{ggT}(\upsilon, \zeta) = 1$ teilt λ höchstens eine der drei Zahlen. Angenommen, $\lambda \nmid \xi$, $\lambda \nmid \upsilon$ und $\lambda \nmid \zeta$. So ist auch jeweils ihre dritte Potenz nicht durch λ teilbar. Nach Lemma 4.17 gilt dann

$$0 = \xi^3 + \upsilon^3 + \zeta^3 \equiv \pm 1 \pm 1 \pm 1 \pmod{\lambda^4},$$

also $\lambda^4 \mid \pm 1 \pm 1 \pm 1$. Die acht Kombinationen fallen zusammen zu $\lambda^4 \mid \pm 1$ und $\lambda^4 \mid \pm 3$. Die erste Möglichkeit scheidet aus, weil die Nichteinheit λ^4 keine Einheit teilt. Für die zweite Möglichkeit erinnern wir an die Identität $3 = \lambda(1 - \omega^2)$ aus (4.23) und formen sie weiter um zu

$$3 = \lambda(1 - \omega^2) = \lambda(1 - \omega)(1 + \omega) \overset{(C)}{=} \lambda^2(1 + \omega),$$

d.h., $\lambda^2 \mid 3$ einerseits. Andererseits gilt auch

$$\lambda^2 = (1 - \omega)^2 = 1 - 2\omega + \omega^2 \overset{(B)}{=} 1 - 2\omega - (\omega + 1) = -3\omega$$

oder $3 \mid \lambda^2$. Also sind ± 3 und λ^2 assoziiert. D.h., würde nun $\lambda^4 \mid \pm 3$ gelten, dann gilt auch $\lambda^4 \mid \lambda^2$, Widerspruch. Somit teilt λ genau eines der ξ, υ, ζ. □

Aufgrund der Form von Gleichung (4.25) können wir nun ohne Einschränkung $\lambda \mid \zeta$ voraussetzen (andernfalls deklarieren wir ξ bzw. υ um in ζ und umgekehrt). D.h., $\zeta = \lambda^m \gamma$ für ein γ mit $\lambda \nmid \gamma$ und $m \geq 1$. Damit erhalten wir

$$\xi^3 + \upsilon^3 + \lambda^{3m}\gamma^3 = 0$$

mit

$$m \geq 1, \quad \mathrm{ggT}(\xi, \upsilon) = 1, \quad \lambda \nmid \xi, \quad \lambda \nmid \upsilon, \quad \lambda \nmid \gamma. \tag{4.26}$$

Es erweist sich nun als beweistechnisch günstig, sogar zu zeigen, dass es unter den Voraussetzungen (4.26) keine Eisenstein-Zahlen ξ, υ, γ und keine Einheit ε gibt mit

$$\xi^3 + \upsilon^3 + \varepsilon\lambda^{3m}\gamma^3 = 0. \tag{4.27}$$

Lemma 4.19. *Genügen ξ, υ, γ den Voraussetzungen (4.26) und der Identität (4.27) für eine Einheit ε, so ist $m \geq 2$.*

Beweis. Subtrahieren wir Gleichung (4.27) mit $\varepsilon\lambda^{3m}\gamma^3$, dann gilt nach Lemma 4.17

$$-\varepsilon\lambda^{3m}\gamma^3 = \xi^3 + \upsilon^3 \equiv \pm 1 \pm 1 \pmod{\lambda^4},$$

also $-\varepsilon\lambda^{3m}\gamma^3 \equiv \pm 2 \pmod{\lambda^4}$ oder $-\varepsilon\lambda^{3m}\gamma^3 \equiv 0 \pmod{\lambda^4}$. Die erste Möglichkeit ist äquivalent zu $\pm 2\lambda \equiv -\varepsilon\lambda^{3m+1}\gamma^3 \pmod{\lambda^4}$. Wegen $\lambda^4 \mid \lambda^{3m+1}$ folgt daraus $\pm 2\lambda \equiv 0 \pmod{\lambda^4}$, also $\lambda^4 \mid \pm 2\lambda$ bzw. $\lambda^3 \mid \pm 2$ und damit auch $\lambda^2 \mid \pm 2$. Da jedoch (wie wir im Beweis von Lemma 4.18 gezeigt haben) λ^2 und ± 3 assoziiert sind, folgt weiter $\pm 3 \mid \pm 2$, Widerspruch.

Damit bleibt die zweite Möglichkeit. Tatsächlich folgt aus $-\varepsilon\lambda^{3m}\gamma^3 \equiv 0 \pmod{\lambda^4}$ wegen $\lambda \nmid \gamma$ und $\lambda \nmid \varepsilon$, dass der Exponent $m \geq 2$ sein muss. Andernfalls wäre λ^{3m} nicht durch λ^4 teilbar. □

In der Gleichung (4.27) faktorisieren wir nun $\xi^3 + \upsilon^3$ gemäß Lemma 4.15, indem wir $n = 3$, $x = \xi$ und $y = \upsilon$ setzen. Wir erhalten

$$(\xi + \upsilon)(\xi + \omega\upsilon)(\xi + \omega^2\upsilon) = \xi^3 + \upsilon^3 = -\varepsilon\lambda^{3m}\gamma^3. \tag{4.28}$$

Lemma 4.20. *Genügen ξ, υ, γ den Voraussetzungen (4.26) und der Identität (4.28) für eine Einheit ε, dann sind zwei der drei Faktoren $(\xi + \upsilon)$, $(\xi + \omega\upsilon)$ und $(\xi + \omega^2\upsilon)$ durch λ und der dritte durch λ^{3m-2} teilbar.*

Von Lemma 4.20 an beginnen wir mit dem "unendlichen Abstieg" in Bezug auf m. Und zwar zeigen wir, dass wenn Gleichung (4.27) unter den Bedingungen (4.26) für ein $m \geq 2$ erfüllt werden kann, so ist sie auch für $m - 1$ anstelle von m und dann auch $m - 2$ usw. erfüllbar, bis wir irgendwann bei $m = 1$ angelangt sind. Dann erhalten wir einen Widerspruch zu Lemma 4.19.

Beweis von Lemma 4.20. Für die Faktoren $(\xi + \upsilon)$, $(\xi + \omega\upsilon)$ und $(\xi + \omega^2\upsilon)$ gilt:

(1) Wegen $m \geq 2$ ist $3m > 3$. Deshalb muss in (4.28) wegen λ^{3m} mindestens einer der Faktoren durch λ^2 teilbar sein; wir nennen ihn η und die anderen H_1, H_2.

(2) Wir betrachten die drei Differenzen aus jeweils zwei Faktoren,

   (a) $(\xi + \upsilon) - (\xi + \omega\upsilon) = \upsilon(1 - \omega) \overset{(C)}{=} \upsilon\lambda$,

   (b) $(\xi + \upsilon) - (\xi + \omega^2\upsilon) = \upsilon(1 - \omega^2) \overset{(A)}{=} \upsilon(\omega^3 - \omega^2) = -\upsilon\omega^2(-\omega + 1) \overset{(C)}{=} -\omega^2\upsilon\lambda$,

   (c) $(\xi + \omega\upsilon) - (\xi + \omega^2\upsilon) = \omega\upsilon(1 - \omega) \overset{(C)}{=} \omega\upsilon\lambda$.

   D.h., sie sind durch λ, wegen $\lambda \nmid \upsilon$ und $\lambda \nmid \omega$ aber nicht durch λ^2 teilbar. Aus $\lambda \mid \pm\eta \pm H_1$ (bzw. $\lambda \mid \pm\eta \pm H_2$) und $\lambda \mid \pm\eta$ folgt $\lambda \mid \pm H_1$ (bzw. $\lambda \mid \pm H_2$). Also teilt λ alle drei Faktoren.

Aus (1) und (2) folgt schließlich $\lambda^{3m-2} \mid \eta$, $\lambda \mid H_1$, $\lambda \mid H_2$. □

Ohne Einschränkung setzen wir $\lambda^2 \mid (\xi + \upsilon)$ voraus (andernfalls ersetzen wir nachfolgend υ durch $\omega\upsilon$ oder $\omega^2\upsilon$). Somit ist

$$\xi + \upsilon = \kappa_1\lambda^{3m-2}, \qquad \xi + \omega\upsilon = \kappa_2\lambda, \qquad \xi + \omega^2\upsilon = \kappa_3\lambda \tag{4.29}$$

für drei Eisenstein-Zahlen $\kappa_1, \kappa_2, \kappa_3$ mit $\lambda \nmid \kappa_1$, $\lambda \nmid \kappa_2$, $\lambda \nmid \kappa_3$.

Lemma 4.21. *Die Zahlen $\kappa_1, \kappa_2, \kappa_3$ sind Assoziierte von Kuben,*

$$\kappa_1 = \epsilon_1\theta^3, \qquad \kappa_2 = \epsilon_2\phi^3, \qquad \kappa_3 = \epsilon_3\psi^3. \tag{4.30}$$

Beweis. Teilt ein δ z.B. κ_2 und κ_3, so teilt δ auch

$$\lambda(\kappa_2 - \kappa_3) = \xi + \omega\upsilon - (\xi + \omega^2\upsilon) = \omega\upsilon(1 - \omega) \overset{(C)}{=} \omega\upsilon\lambda$$

und

$$\lambda(\omega\kappa_3 - \omega^2\kappa_2) = \omega(\xi + \omega^2\upsilon) - \omega^2(\xi + \omega\upsilon) \overset{(A)}{=} \omega\xi + \upsilon - \omega^2\xi - \upsilon \overset{(C)}{=} \omega\xi\lambda,$$

also $\delta \mid \omega\upsilon$ und $\delta \mid \omega\xi$. Da ω eine Einheit und $\mathrm{ggT}(\upsilon, \xi) = 1$ ist, ist δ ebenfalls eine Einheit, also $\mathrm{ggT}(\kappa_2, \kappa_3) = 1$. Die Teilerfremdheit von κ_1, κ_2 und κ_1, κ_3 folgt analog.

Die Identitäten (4.29) eingesetzt in die Faktorisierung aus (4.28) liefert

$$-\varepsilon\lambda^{3m}\gamma^3 = (\kappa_1\lambda^{3m-2})(\kappa_2\lambda)(\kappa_3\lambda) \iff -\varepsilon\gamma^3 = \kappa_1\kappa_2\kappa_3.$$

Aus der paarweisen Teilerfremdheit von $\kappa_1, \kappa_2, \kappa_3$ folgt nun, da $\mathbb{Z}[\omega]$ ein ZPE-Ring ist, dass $\kappa_1, \kappa_2, \kappa_3$ Assoziierte von Kuben sein müssen. □

Setzen wir (4.30) in (4.29) ein, so erhalten wir

$$\xi + \upsilon = \epsilon_1\lambda^{3m-2}\theta^3, \qquad \xi + \omega\upsilon = \epsilon_2\lambda\phi^3, \qquad \xi + \omega^2\upsilon = \epsilon_3\lambda\psi^3 \tag{4.31}$$

für paarweise teilerfremde θ, ϕ, ψ mit $\lambda \nmid \theta$, $\lambda \nmid \phi$, $\lambda \nmid \psi$.

Wir konstruieren nun folgende Nullsumme, welche die rechten Seiten aus (4.31) als Summanden hat; dabei verwenden wir die Identitäten $0 = \omega^2 + \omega + 1$ und $\omega^4 = \omega$:

$$\begin{aligned}
0 &= 0 \cdot (\xi + \upsilon) \\
&= (1 + \omega + \omega^2)(\xi + \upsilon) \\
&= \xi + \upsilon + \omega\xi + \omega\upsilon + \omega^2\xi + \omega^2\upsilon \\
&= \xi + \upsilon + \omega\xi + \omega^2\upsilon + \omega^2\xi + \omega^4\upsilon \\
&= \xi + \upsilon + \omega(\xi + \omega\upsilon) + \omega^2(\xi + \omega^2\upsilon) \\
&\overset{(4.31)}{=} \epsilon_1\lambda^{3m-2}\theta^3 + \epsilon_2\omega\lambda\phi^3 + \epsilon_3\omega^2\lambda\psi^3.
\end{aligned}$$

Teilen durch $\epsilon_2\omega\lambda \neq 0$ ergibt dann

$$\phi^3 + \epsilon_4\psi^3 + \epsilon_5\lambda^{3m-3}\theta^3 = 0 \tag{4.32}$$

für Einheiten $\epsilon_4 = (\epsilon_3\omega)/\epsilon_2$ und $\epsilon_5 = \epsilon_1/(\epsilon_2\omega)$. Stellen wir Gleichung (4.32) um zu $\phi^3 + \epsilon_4\psi^3 = -\epsilon_5\lambda^{3m-3}\theta^3$, so folgt wegen $m \geq 2$ und damit $3m - 3 \geq 3$ nun

$$\phi^3 + \epsilon_4\psi^3 \equiv 0 \pmod{\lambda^2}$$

(sogar mod λ^3). Wegen $\lambda \nmid \phi$ und $\lambda \nmid \psi$ gilt nach Lemma 4.17 hierbei $\phi^3 \equiv \pm 1 \pmod{\lambda^4}$ und $\psi^3 \equiv \pm 1 \pmod{\lambda^4}$, also $\phi^3 = \delta\lambda^4 \pm 1 = (\delta\lambda^2)\lambda^2 \pm 1$ für ein δ (Gleiches gilt für ψ^3). D.h., $\phi^3 \equiv \pm 1 \pmod{\lambda^2}$ und $\psi^3 \equiv \pm 1 \pmod{\lambda^2}$. Damit erhalten wir die Kongruenz

$$\phi^3 + \epsilon_4\psi^3 \equiv \pm 1 \pm \epsilon_4 \equiv 0 \pmod{\lambda^2}.$$

Als Einheit ist $\epsilon_4 = \pm 1, \pm\omega$ oder $\pm\omega^2$. Wir gehen zuerst die acht Fälle $\pm 1 \pm \omega$, $\pm 1 \pm \omega^2$ mit Hilfe der Identitäten (B), (C) durch: $1 - \omega = \lambda$, $-1 + \omega = -\lambda$, $1 + \omega = -\omega^2$, $-1 - \omega = \omega^2$, $1 + \omega^2 = -\omega$, $-1 - \omega^2 = \omega$, $1 - \omega^2 = (1 + \omega)(1 - \omega) = -\omega^2\lambda$ und $-1 + \omega^2 = \omega^2\lambda$. D. h., $\pm 1 \pm \epsilon_4$ ist assoziiert mit 1 oder λ. Da λ^2 aber weder 1 noch λ teilt, bleibt letztlich $\epsilon_4 = \pm 1$. Aus (4.32) wird dann

$$\phi^3 \pm \psi^3 + \epsilon_5\lambda^{3m-3}\theta^3 = 0.$$

Für den Fall $\epsilon_4 = -1$ können wir in (4.30) ohne Einschränkung ψ durch $-\psi$ ersetzen. Insgesamt haben nun festgestellt, dass eines der beiden Tripel $(\theta, \phi, \pm\psi)$ die Gleichung

$$\xi^3 + \upsilon^3 + \varepsilon\lambda^{3m}\gamma^3 = 0$$

für $m - 1$ anstelle von m löst. Für die neue Lösung können wir nun unser Vorgehen wiederholen und so fort, bis wir den Widerspruch $m = 1$ zu Lemma 4.19 erhalten. Somit hat Gleichung (4.25) keine Lösung in den Eisenstein-Zahlen und damit hat besonders Gleichung (4.21) keine ganzzahlige Lösung. □

4.6. Der Fall n gleich reguläre Primzahl

Im letzten Kapitel beweisen wir Fermats großen Satz nicht für ein einzelnes n, sondern für möglicherweise unendlich viele, nämlich für reguläre Primzahlen. Wie in Kapitel 2 erwähnt, wurde dieser Fall zuerst von Kummer bewiesen. Eine Primzahl p heißt *regulär*, wenn sie keinen Zähler der Bernoulli-Zahlen $B_2, B_4, \ldots, B_{p-3}$ mit geradem Index teilt, andernfalls heißt sie *irregulär* ([Was97], Kap. 1, Remarks). Die Bernoulli-Zahlen sind über die in der offenen Kreisfläche $|z| < 2\pi$ konvergente Taylor-Reihe

$$\frac{z}{e^z - 1} = \sum_{k=0}^{\infty} B_k \frac{z^k}{k!}$$

der komplexwertigen Funktion $\frac{z}{e^z-1}$ definiert. Ihre ersten Glieder sind $B_0 = 1$, $B_1 = \pm 1/2$, $B_2 = 1/6$, $B_4 = -1/30$, $B_6 = 1/42$, $B_8 = -1/30$, $B_{10} = 5/66$, $B_{12} = -691/2730$ und $B_k = 0$ für ungerade $k \geq 3$ ([Bun08], Kap. 4.2.8).

Unter den Primzahlen bis 100 sind nur 37, 59 und 67 irregulär und unter den 168 Primzahlen bis 1000 sind 104 regulär (Folgen A007703 und A000928 in der OEIS), was einem Anteil von 61,9 % entspricht. Bis heute ist offen, ob es unendlich viele reguläre Primzahlen gibt ([Sha19], S. 18). Weitergehende kalkulatorische Befunde deuten darauf hin. So sind unter den Primzahlen bis 125 000 ca. 61 % regulär ([Was97], Kap. 1, Remarks). Dagegen wurde 1915 von K. L. Jensen bewiesen, dass unendliche viele irreguläre Primzahlen existieren ([Bun08], Kap. 4.2.8).

Kummer konnte zeigen, dass die Eigenschaft einer Primzahl p, regulär zu sein, gleichbedeutend dazu ist, dass p nicht die Klassenzahl von $\mathbb{Q}(\zeta_p)$ teilt. Für gewöhnlich ist die Bestimmung der Klassenzahl eines Zahlkörpers äußerst aufwändig ([Lem17], Beginn Kap. 7). Kummer gelang es, diese von einigen primen Kreisteilungskörpern zu berechnen, z. B. $h_{\mathbb{Q}(\zeta_{23})} = 3$ und $h_{\mathbb{Q}(\zeta_{37})} = 37$ ([MSP11], nach D.21).

Angelehnt an [Was97], Theorem 1.1, formulieren wir nun Fall 1 von Fermats großem Satz für reguläre Primzahlen:

Satz 4.22. *(FGS für n gleich reguläre Primzahl p, Fall 1)*
Die Gleichung

$$x^p + y^p = z^p, \qquad p \nmid xyz, \tag{4.33}$$

besitzt für ungerade Primzahlen p, welche die Klassenzahl des p-ten Kreisteilungskörpers

$\mathbb{Q}(\zeta_p)$ *nicht teilen, keine ganzzahlige Lösung.*

Bemerkung 4.23. Da 0 durch jede ganze Zahl ungleich 0 teilbar ist, impliziert $p \nmid xyz$ die notwendige Voraussetzung $xyz \neq 0$. In der Einleitung wurde angesprochen, dass Fermats großer Satz in zwei Fälle aufgeteilt werden kann ([OR96]):

Fall 1: Keines der x, y, z ist durch n teilbar.

Fall 2: Genau eines der x, y, z ist durch n teilbar.

Der zweite Fall von Theorem 4.22 ist deutlich schwieriger zu beweisen. Wir gehen im Anschluss an den Beweis des ersten Falls kurz darauf ein.

Für Fall 1 orientieren wir uns am Beweis von Theorem 1.1 in [Was97]. Die nötigen Vorarbeiten finden sich Kapitel 3. Der theoretische Hintergrund kann in Anhang B nachgeschlagen werden. Anders als in [Was97] stellen wir einige dort in den Beweis integrierte Hilfssätze voran, um uns auf die Kernargumentation zu konzentrieren.

Sei dazu p eine reguläre Primzahl und $\zeta = \zeta_p$ eine primitive p-te Einheitswurzel in $\mathbb{Z}[\zeta]$. Außerdem schreiben wir (rationale) ganze Zahlen in lateinischen und Zahlen aus $\mathbb{Z}[\zeta_p]$ in griechischen Buchstaben:

Lemma 4.24. *Seien r, s teilerfremd zu p. Dann ist $(\zeta^r - 1)/(\zeta^s - 1)$ eine Einheit in $\mathbb{Z}[\zeta]$.*

Bemerkung 4.25. Die Einheiten aus Lemma 4.24 werden *zyklotomische Einheiten* genannt ([Was97], Lemma 1.3).

Beweis von Lemma 4.24. Wir drücken r durch s und ein t mit $r = st \pmod p$ aus (Potenzen einer n-ten Einheitswurzel sind gleich, wenn sich ihre Exponenten um ein ganzzahliges Vielfaches von n unterscheiden). Aus $\mathrm{ggT}(p, rs) = 1$ folgt $\zeta^s \neq 1$, da ζ primitiv ist. Daher gilt mit der geometrischen Summenformel

$$\frac{1-\zeta^r}{1-\zeta^s} = \frac{1-\zeta^{st}}{1-\zeta^s} = 1 + \zeta^s + \ldots + \zeta^{s(t-1)} \in \mathbb{Z}[\zeta].$$

Wegen $\zeta^r \neq 1$ gilt analog $(\zeta^s - 1)/(\zeta^r - 1) \in \mathbb{Z}[\zeta]$. D.h., $(\zeta^r - 1)/(\zeta^s - 1)$ besitzt ein Inverses in $\mathbb{Z}[\zeta]$, ist also eine Einheit. □

Lemma 4.26. *a) Es gilt $\langle p \rangle = \langle 1 - \zeta \rangle^{p-1}$.*

b) Das Hauptideal $\langle 1 - \zeta \rangle$ aus a) ist ein Primideal in $\mathbb{Z}[\zeta]$.

Beweis. a) Das Polynom $T^{p-1} + T^{p-2} + \ldots + T + 1$ hat die Nullstellen $\zeta, \ldots, \zeta^{p-1}$. Für $T = 1$ ist die Summe gleich p, d.h. $p = \prod_{i=1}^{p-1}(1 - \zeta^i)$. Nach Lemma 4.24 gibt es für jedes i ein $\varepsilon \in \mathbb{Z}[\zeta]$ mit

$$1 - \zeta^i = \frac{1-\zeta^i}{1-\zeta}(1-\zeta) = \varepsilon(1-\zeta). \tag{4.34}$$

Da $(1-\zeta)$ und $\varepsilon(1-\zeta)$ assoziiert sind, folgt mit Lemma A.6 a) die Gleichheit $\langle 1-\zeta \rangle = \langle 1 - \zeta^i \rangle$ von Idealen. Aus $p = (1-\zeta)\ldots(1-\zeta^{p-1})$ folgt mit Lemma A.1 dann weiter

$\langle p \rangle = \langle 1 - \zeta \rangle \dots \langle 1 - \zeta^{p-1} \rangle = \langle 1 - \zeta \rangle^{p-1}$.

b) Wir betrachten aus Teil a) die Darstellung

$$\langle p \rangle = \langle 1 - \zeta \rangle^{p-1}. \tag{4.35}$$

Da p eine (ganzzahlige) Primzahl ist, ist $\langle p \rangle = \langle 1 - \zeta \rangle^{p-1}$ nach Lemma A.6 c) ein Primideal in $\mathbb{Z}$. Als dieses zerfällt es nach Satz A.28 eindeutig in ein Produkt aus Primidealen $\mathfrak{p}_1^{(p-1)e_1} \cdot \ldots \cdot \mathfrak{p}_m^{(p-1)e_m}$. Wir erinnern nun an die fundamentale Gleichung aus Satz A.29:

$$(p-1)e_1 f_1 + \ldots + (p-1)e_m f_m = [\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1. \tag{4.36}$$

Aus (4.35), $f_i \neq 0$ für $i = 1, \ldots, m$, und der Gültigkeit von (4.36) folgt in Bezug auf die Primidealzerlegung $e_i = 1$ und $\mathfrak{p}_i = \langle 1 - \zeta \rangle$ für ein i und $e_j = 0$ für alle $j \neq i$. Somit ist $\langle 1 - \zeta \rangle$ ein Primideal. □

Lemma 4.27. *Sei ε eine Einheit in $\mathbb{Z}[\zeta]$. Dann gibt es eine Einheit $u \in \mathbb{Q}(\zeta + \zeta^{-1})$ und eine ganze Zahl r mit $\varepsilon = \zeta^r u$.*

Bemerkung 4.28. ζ^{-1} ist das komplex Konjugierte zu ζ. Als Punkte des Einheitskreises liegen ζ und ζ^{-1} achsensymmetrisch zur reellen Achse in der komplexen Ebene. Daher ist $\zeta + \zeta^{-1} \in \mathbb{R}$, $\mathbb{Q}(\zeta + \zeta^{-1}) \subset \mathbb{R}$ und somit u reell. Aus $\zeta + \zeta^{-1} \in \mathbb{Q}(\zeta)$ folgt zudem $\mathbb{Q}(\zeta + \zeta^{-1}) \subset \mathbb{Q}(\zeta)$. Der Körper $\mathbb{Q}(\zeta + \zeta^{-1})$ wird *maximal reeller Unterkörper* von $\mathbb{Q}(\zeta)$ genannt ([Was97], Remark zu Proposition 1.5).

Beweis. Lemma 4.27 wird als Proposition 1.5 in [Was97] bewiesen. □

Lemma 4.29. *Sei $\alpha \in \mathbb{Z}[\zeta]$. Dann ist α^p kongruent einer ganzen Zahl a mod p.*

Beweis. Nach Lemma 3.12 ist $\alpha = a_0 + a_1\zeta + \ldots + a_{p-2}\zeta^{p-2}$ für ganze Zahlen $a_0, \ldots, a_{p-2}$. Bezeichnet σ_{p-2} die Summe aus den letzten $(p-2)$ Summanden, so ist

$$\alpha^p = (a_0 + \sigma_{p-2})^p = \sum_{j=0}^{p} \binom{p}{j} a_0^{p-j} \sigma_{p-2}^j.$$

Schreibt man die Summe aus, dann sind alle Summanden außer dem ersten und dem letzten,

$$\frac{p!}{0! \cdot p!} a_0^p \sigma_{p-2}^0 = a_0^p, \qquad \frac{p!}{p! \cdot 0!} a_0^0 \sigma_{p-2}^p = \sigma_{p-2}^p,$$

durch p teilbar. Somit folgt in iterativer analoger Weise

$$\begin{aligned} \alpha^p &\equiv a_0^p + \sigma_{p-2}^p \\ &\equiv a_0^p + (a_1^p \zeta)^p + \sigma_{p-3}^p \\ &\equiv \ldots \\ &\equiv a_0^p + (a_1^p \zeta)^p + \ldots + (a_{p-3}\zeta^{p-3})^p + \sigma_1^p \pmod{p}, \end{aligned}$$

wobei $\sigma_1^p = (a_{p-2}\zeta^{p-2})^p$ ist. Da jede p-te Potenz einer p-ten Einheitswurzel gleich 1 ist, erhalten wir schließlich

$$\alpha^p \equiv a_0^p + a_1^p + \ldots + a_{p-2}^p \pmod{p}$$

mit $a \coloneqq a_0^p + a_1^p + \ldots + a_{p-2}^p \in \mathbb{Z}$. □

Lemma 4.30. *Sei $\alpha = a_0 + a_1\zeta + \ldots + a_{p-1}\zeta^{p-1}$ mit $a_i \in \mathbb{Z}$, wobei mindestens ein $a_i = 0$ ist. Ist α durch eine Zahl $d \in \mathbb{Z}$ teilbar, dann teilt d jedes a_j.*

Beweis. Lemma 3.14 zufolge hat $\mathbb{Z}[\zeta]$ eine Ganzheitsbasis der Länge $p-1$. Da $1 + \zeta + \ldots + \zeta^{p-1} = 0$ eine $\mathbb{Z}$-Linearkombination der Null ist, sind die p Summanden linear abhängig. Dagegen ist jede $(p-1)$-elementige Teilmenge von $\{1, \zeta, \ldots, \zeta^{p-1}\}$ eine Basis des $\mathbb{Z}$-Moduls $\mathbb{Z}[\zeta]$, da sie ein Erzeugendensystem und linear unabhängig ist. Da mindestens ein $a_i = 0$ ist, sind die anderen a_j die Koeffizienten der eindeutigen Darstellung von α durch $1, \zeta, \ldots, \zeta^{i-1}, \zeta^{i+1}, \ldots, \zeta^{p-1}$.

Sei nun j der Index mit $a_j = 0$. Nach Voraussetzung ist $\alpha = d\beta$ für ein $\beta \in \mathbb{Z}[\zeta]$. Wir schreiben β in unserer Ganzheitsbasis, also

$$\beta = b_0 + b_1\zeta + \ldots + b_{j-1}\zeta^{j-1} + b_{j+1}\zeta^{j+1} + \ldots + b_{p-1}\zeta^{p-1}.$$

Dann gilt

$$d\beta = db_0 + db_1\zeta + \ldots + db_{j-1}\zeta^{j-1} + db_{j+1}\zeta^{j+1} + \ldots + db_{p-1}\zeta^{p-1}.$$

Da $\zeta^0, \ldots, \zeta_{j-1}, \zeta_{j+1}, \ldots, \zeta^{p-1}$ linear unabhängig sind über $\mathbb{Z}$, folgt $db_i = a_i$ für $i \neq j$. Für $i = j$ ist ohnehin $0 = a_j = db_j = 0$. D.h., $d \mid a_i$ für alle i. □

Wir können nun Fermats großen Satz für n gleich reguläre Primzahl p beweisen.

Beweis von Satz 4.22. Wir beginnen wieder mit der Annahme, dass ganze Zahlen x, y und z existieren, welche die Gleichung (4.33) lösen. Nach Lemma 4.3 können x, y, z als paarweise teilerfremd vorausgesetzt werden. Wir behandeln zuerst die Fälle $p = 3$ und $p = 5$:

Aus $3 \nmid x$ bzw. $x = 3k \pm 1$ folgt $x^3 = 27k^3 \pm 27k^2 + 9k \pm 1$ (binomischer Lehrsatz), also $x^3 \equiv \pm 1 \pmod 9$. Gleiches gilt für y und z. Somit ist $x^3 + y^3 \equiv -2$, 0 oder 2 (mod 9). Wegen $z^3 \equiv \pm 1 \pmod 9$ folgt damit $x^3 + y^3 \neq z^3$, Widerspruch.

Analog ist $5 \nmid x$ gleichbedeutend zu $x = 5k + r$ mit $r \pm 1$ oder $r \pm 2$. Daraus folgt $x^5 = 25 \cdot (\ldots) + r^5$, also $x^5 \equiv r^5 \pmod{25}$. Gleiches gilt wieder für y und z. Somit ist $x^5 + y^5 \equiv s \pmod{25}$ mit $s \in \{0, \pm 2, \pm 6, \pm 8, \pm 14\}$. Da jedoch $z^5 \equiv r^5 \pmod{25}$ und $r^5 \in \{\pm 1, \pm 7\}$ ist, folgt damit der Widerspruch $x^5 + y^5 \neq z^5$.

Für $p = 7$ scheitert das Vorgehen, da $1^7 + 30^7 \equiv 31^7 \pmod{49}$ ist. Genauso lassen sich nach [Was97] (Beweis von Theorem 1.1) auch Kongruenzen für höhere 7er-Potenzen als 49 finden.

D.h., wir können nachfolgend $p > 5$ voraussetzen. Außerdem gilt ohne Einschränkung $p \nmid x - y$: Nehmen wir dafür an, $p \mid x - y$, also $x - y \equiv 0 \pmod p$ bzw. $x \equiv y \pmod p$. Da x, y, z eine Lösung von $x^p + y^p = z^p$ ist, erhalten wir nach Umordnung $x, -z, -y$ als Lösung von $x^p + (-z)^p = (-y)^p$. Daraus folgt $x \equiv -z \pmod p$. Aus $x^p + y^p = z^p$ folgt

$x^p + y^p \equiv z^p \pmod p$. Nach Fermats *kleinem* Satz ist $x^p \equiv x \pmod p$, $y^p \equiv y \pmod p$ (und damit $x^p + y^p \equiv x + y \pmod p$) und $z^p \equiv z \pmod p$. Daraus folgt $z \equiv x + y \equiv -2z \pmod p$, also $3z \equiv 0 \pmod p$ bzw. $p \mid 3z$ im Widerspruch zu $p > 3$ und $p \nmid z$. Wir werden die Voraussetzung gegen Ende des Beweises benötigen.

Wir betrachten nun die Identität $x^p + y^p = z^p$ in faktorisierter Form (vgl. Lemma 4.12):

$$\prod_{i=0}^{p-1}(x + \zeta^i y) = z^p. \tag{4.37}$$

Dann ersetzen wir die Terme auf beiden Seiten durch die von ihnen erzeugten Ideale, wodurch die Gleichheit erhalten bleibt. Nach Lemma A.1 gilt dabei $\langle\prod_{i=0}^{p-1} x + \zeta^i y\rangle = \prod_{i=0}^{p-1}\langle x + \zeta^i y\rangle$ und $\langle z^p\rangle = \langle z\rangle^p$. D.h., wir haben

$$\prod_{i=0}^{p-1}\langle x + \zeta^i y\rangle = \langle z\rangle^p. \tag{4.38}$$

Lemma 4.31. *Die Ideale $\langle x + \zeta^i y\rangle$, $i = 0, \ldots, p-1$, sind paarweise teilerfremd.*

Beweis. Angenommen, ein Primideal $\mathfrak{p}$ von $\mathbb{Z}[\zeta]$ teilt $\langle x+\zeta^i y\rangle$ und $\langle x+\zeta^j y\rangle$ für $i \neq j$. D.h., $x + \zeta^i y \in \mathfrak{p}$ und $x + \zeta^j y \in \mathfrak{p}$. Da $\mathfrak{p}$ ein Ideal ist, ist auch

$$(x + \zeta^i y) - (x + \zeta^j y) = \zeta^i(1 - \zeta^{j-i})y \overset{(4.34)}{=} \varepsilon(1 - \zeta)y \in \mathfrak{p}$$

und

$$\zeta^j(x + \zeta^i y) - \zeta^i(x + \zeta^j y) = \zeta^j(1 - \zeta^{j-i})x \overset{(4.34)}{=} \varepsilon'(1 - \zeta)x \in \mathfrak{p}$$

für Einheiten $\varepsilon, \varepsilon' \in \mathbb{Z}[\zeta]$. Mit Lemma A.6 a) und b) gilt dann zum einen

$$\mathfrak{p} \mid \langle\varepsilon(1 - \zeta)y\rangle = \langle 1 - \zeta\rangle \cdot \langle y\rangle.$$

Daraus folgt, weil $\mathfrak{p}$ prim ist, $\mathfrak{p} \mid \langle 1 - \zeta\rangle$ oder $\mathfrak{p} \mid \langle y\rangle$. Nach Lemma 4.26 ist $\langle 1 - \zeta\rangle$ ein Primideal, das als solches in einem Dedekind-Ring per definitionem maximal ist (Definition A.17). D.h., aus $\mathfrak{p} \mid \langle 1 - \zeta\rangle$ folgt $\mathfrak{p} = \langle 1 - \zeta\rangle$, womit sogar $\mathfrak{p} = \langle 1 - \zeta\rangle$ oder $\mathfrak{p} \mid \langle y\rangle$ gilt.

Analog gilt zum anderen

$$\mathfrak{p} \mid \langle\varepsilon'(1 - \zeta)x\rangle = \langle 1 - \zeta\rangle \cdot \langle x\rangle,$$

also $\mathfrak{p} = \langle 1 - \zeta\rangle$ oder $\mathfrak{p} \mid \langle x\rangle$.

Angenommen, $\mathfrak{p} \neq \langle 1 - \zeta\rangle$. Dann gilt $\mathfrak{p} \mid \langle x\rangle$ und $\mathfrak{p} \mid \langle y\rangle$, also $x, y \in \mathfrak{p}$. Da x und y ganzzahlig sind mit $\mathrm{ggT}(x, y) = 1$, gibt es nach der Relation von Bézout ganze Zahlen s, t mit $1 = sx + ty$. Daraus folgt, weil $x, y \in \mathfrak{p}$, $s, t \in \mathbb{Z}[\zeta]$ und $\mathfrak{p}$ ein Ideal von $\mathbb{Z}[\zeta]$ ist, $1 = sx + ty \in \mathfrak{p}$, also $\mathfrak{p} = \langle 1\rangle = \mathbb{Z}[\zeta]$ im Widerspruch zu $\mathfrak{p} \subsetneq \mathbb{Z}[\zeta]$ (vgl. Definition A.4). Deshalb muss $\mathfrak{p} = \langle 1 - \zeta\rangle$ sein.

Wir betrachten nun die dritte Differenz $(x + y) - (x + \zeta^i y) = (1 - \zeta^i)y = \varepsilon''(1 - \zeta)y$, wobei ε'' eine Einheit ist. Aus $\varepsilon'' y \in \mathbb{Z}[\zeta]$ und $1 - \zeta \in \mathfrak{p}$ folgt der Definition eines Ideals nach $\varepsilon''(1 - \zeta)y \in \mathfrak{p}$. D.h., einerseits gilt $x + y \equiv x + \zeta^i y \pmod{\mathfrak{p}}$ (vgl. Definition A.7). Nach unserer Wahl von $\mathfrak{p}$ ist andererseits $x + \zeta^i y \in \mathfrak{p}$ und damit $(x + \zeta^i y) - 0 \in \mathfrak{p}$, d. h.,

es gilt $x + \zeta^i y \equiv 0 \pmod{\mathfrak{p}}$. Insgesamt erhalten wir also

$$x + y \equiv 0 \pmod{\mathfrak{p}}$$

und damit $x + y \in \mathfrak{p}$. Da außerdem $x + y \in \mathbb{Z}$ ist, folgt $x + y \in (\mathfrak{p} \cap \mathbb{Z})$.

Aus dem vorletzten Absatz wissen wir, dass $\mathfrak{p} = \langle 1 - \zeta \rangle$ ist. Nach Lemma 4.26 gilt $\langle 1 - \zeta \rangle^{p-1} = \langle (1 - \zeta)^{p-1} \rangle = \langle p \rangle$, d.h., $\langle (1 - \zeta)^{p-1} \rangle \mid \langle p \rangle$. Daraus folgt $(1 - \zeta)^{p-1} \mid p$ und damit $(1 - \zeta) \mid p$ bzw. $\delta(1 - \zeta) = p$ für ein $\delta \in \mathbb{Z}[\zeta]$. Nach Idealdefinition gilt nun $\delta(1 - \zeta) \in \langle 1 - \zeta \rangle$ und damit $p \in \langle 1 - \zeta \rangle$. Kurzgefasst ist also $p \in \mathfrak{p}$. Gleichzeitig ist $p \in \mathbb{Z}$. Da p irreduzibel in $\mathbb{Z}$ und $1 \notin \mathfrak{p}$ ist, gibt es keinen Teiler von p, der sowohl aus $\mathfrak{p}$ als auch aus $\mathbb{Z}$ ist. Also ist $x + y \in (\mathfrak{p} \cap \mathbb{Z}) = \langle p \rangle$, d.h. $p \mid x + y$. Damit gilt

$$x + y \equiv 0 \pmod{p}.$$

Nach Fermats kleinem Satz gilt nun jedoch

$$z \equiv z^p = x^p + y^p \equiv x + y \equiv 0 \pmod{p},$$

also $p \mid z$ im Widerspruch zur Voraussetzung $p \nmid xyz$ von Satz 4.22. □

Damit kommen wir zur Idealgleichung (4.38) zurück und setzen den Beweis von Satz 4.22 fort. Da $\mathbb{Z}[\zeta]$ ein Dedekind-Ring ist, zerfallen die paarweise teiler*fremden* Ideale $\langle x + \zeta^i y \rangle$, $i = 0, \ldots, p-1$, eindeutig in paarweise *verschiedene* Primideale, deren Produkt gleich $\langle z \rangle^p$ ist. Deshalb müssen ihre Exponenten durch p teilbar sein, d.h., jeder Faktor ist p-te Potenz eines Ideals:

$$\langle x + \zeta^i y \rangle = \mathfrak{a}_i^p.$$

Hierbei ist $\mathfrak{a}_i^p$ ein Hauptideal, da es von $x + \zeta^i y$ erzeugt wird.

An dieser Stelle brauchen wir die Voraussetzung, dass die Klassenzahl von $\mathbb{Q}(\zeta)$ nicht durch p teilbar ist:

Lemma 4.32. *Ist* $\mathfrak{a}^m$ *ein Hauptideal und* $\mathrm{ggT}(m, h_{\mathbb{Q}(\zeta)}) = 1$*, so ist* $\mathfrak{a}$ *bereits ein Hauptideal.*

Beweis. Vorlage ist der Beweis von Korollar 6.6.14 in [Sch07]. Wir zeigen die Aussage für einen beliebigen Zahlkörper L. Nach der Relation von Bézout gibt es ganze Zahlen s, t mit $1 = sm + th_L$, d.h. $\mathfrak{a}^1 = (\mathfrak{a}^m)^s (\mathfrak{a}^{h_L})^t$. Hier ist $\mathfrak{a}^m$ und damit $(\mathfrak{a}^m)^s$ nach Voraussetzung ein Hauptideal. Weiter ist in einer endlichen Gruppe Cl_L der Ordnung h_L die h_L-te Potenz eines Gruppenelements (in dem Fall einer Idealklasse $[\mathfrak{a}]$) das neutrale Element $[\mathfrak{a}]^{h_L}$. Da per definitionem $[\mathfrak{a}]^{h_L} = [\mathfrak{a}^{h_L}]$ ist, liegt $\mathfrak{a}^{h_L}$ und somit auch $(\mathfrak{a}^{h_L})^t$ in der Idealklasse der Hauptideale. Daher ist auch $\mathfrak{a}^1 = \mathfrak{a}$ als Produkt von Hauptidealen ein Hauptideal. □

Sagen wir nun $\langle x + \zeta^i y \rangle = \langle \alpha_i \rangle^p = \langle \alpha_i^p \rangle$. Für eine Einheit ϵ ist dann

$$x + \zeta^i y = \epsilon \alpha_i^p,$$

wobei $\epsilon = \zeta^r u$ ist nach Lemma 4.27 für eine ganze Zahl r und eine reelle Einheit u.

Im Folgenden genügt es, $i = 1$ zu betrachten, so dass wir auch den Index $\alpha_1 = \alpha$ weglassen. Einerseits gilt nach Lemma 4.29 nun

$$x + \zeta y = \epsilon\alpha^p = \zeta^r u\alpha^p \equiv \zeta^r ua \pmod{p}.$$

Da für reelle Zahlen die komplexe Konjugation die Identität ist, gilt zum anderen

$$x + \zeta^{-1}y = x + \overline{\zeta}y = \overline{x + \zeta y} = \overline{\epsilon\alpha^p} = \overline{\zeta}^r \overline{u\alpha}^p \equiv \zeta^{-r} u\overline{a} \pmod{\overline{p}}$$

mit $\overline{a} = a$ und $\overline{p} = p$. D.h., es gilt

$$x + \zeta y \equiv \zeta^r ua \pmod{p} \quad \text{und} \quad x + \zeta^{-1}y \equiv \zeta^{-r} ua \pmod{p}$$

bzw.

$$x + \zeta y \equiv \zeta^r ua \pmod{p} \quad \text{und} \quad \zeta^{2r}(x + \zeta^{-1}y) \equiv \zeta^r ua \pmod{p}.$$

Daraus folgt

$$x + \zeta y \equiv \zeta^{2r}(x + \zeta^{-1}y) \pmod{p}$$

und damit

$$x + \zeta y - \zeta^{2r}x - \zeta^{2r-1}y \equiv 0 \pmod{p}. \tag{4.39}$$

Mit Hilfe dieser Kongruenz können wir den Beweis von Satz 4.22 abschließen, indem wir bemerken, dass zwei der 1, ζ, ζ^{2r}, ζ^{2r-1} gleich sind. Sei dazu angenommen, sie wären paarweise verschieden. Dann ist $p \geq 5$, denn für $p = 3$ bleibt nur $\zeta^{2r} = \zeta^2$ oder $\zeta^{2r-1} = \zeta^2$ und damit wäre $\zeta^{2r-1} = \zeta$ bzw. $\zeta^{2r} = 1$, Widerspruch. Da wir die Fälle $p = 3$ und $p = 5$ bereits am Anfang erledigt haben, können wir sogar $p > 5$ ansetzen. Dann ist $\{1, \zeta, \zeta^{2r-1}, \zeta^{2r}\} \subsetneq \{1, \zeta, \ldots, \zeta^{p-1}\}$. Damit ist bezüglich der Summe aus (4.39) die Voraussetzung für Lemma 4.30 gegeben: Hiernach gilt, da p die Summe teilt, $p \mid x$ und $p \mid y$ im Widerspruch zur Voraussetzung $p \nmid xyz$. Also sind mindestens zwei der 1, ζ, ζ^{2r}, ζ^{2r-1} gleich.

Wegen $1 \neq \zeta$ und $\zeta^{2r} \neq \zeta^{2r-1}$ unterscheiden wir hinsichtlich (4.39) nun die drei Fälle $1 = \zeta^{2r}$, $1 = \zeta^{2r-1}$ bzw. $\zeta = \zeta^{2r}$, und $\zeta = \zeta^{2r-1}$:

(1) $1 = \zeta^{2r}$. Hierbei vereinfacht sich (4.39) zu $\zeta y - \zeta^{-1}y \equiv 0 \pmod{p}$. Daraus folgt $p \mid y$ nach Lemma 4.30, Widerspruch.

(2) $1 = \zeta^{2r-1}$. Aus (4.39) wird dann $(x - y) - (x - y)\zeta \equiv 0 \pmod{p}$ und damit $p \mid x - y$ nach Lemma 4.30. Das steht im Widerspruch zur Voraussetzung, die wir am Anfang des Beweises getroffen haben.

(3) $\zeta = \zeta^{2r-1}$. Damit wird (4.39) zu $x - \zeta^2 x \equiv 0 \pmod{p}$, also $p \mid x$ nach Lemma 4.30, Widerspruch.

Damit ist Satz 4.22 bewiesen: Ausgehend von der Annahme, dass es ganze Zahlen x, y, z gibt mit $p \nmid xyz$ und $x^p + y^p = z^p$, haben wir die faktorisierte Form dieser Identität als Gleichheit von Idealen, $\prod_{i=0}^{p-1}\langle x + \zeta^i y\rangle = \langle z\rangle^p$, betrachtet. Mit Hilfe (erstens) der eindeutigen Primidealzerlegung und (zweitens) der Voraussetzung $p \nmid h_{\mathbb{Q}(\zeta)}$, die uns zur Kongruenz (4.39) geführt haben, konnten wir schließlich zeigen, dass keine solche Gleichheit existiert. Da $\prod_{i=0}^{p-1}\langle x + \zeta^i y\rangle = \langle z\rangle^p$ äquivalent ist zu $\prod_{i=0}^{p-1}(x + \zeta^i y) \sim$

z^p, existiert auch insbesondere die eingangs angenommene Lösung x, y, z der Fermat-Gleichung nicht, q.e.d. □

Der Fall 2 und Fazit

Wie in Bemerkung 4.23 angekündigt, gehen wir am Ende des Unterkapitels kurz auf den zweiten Fall ein. Anschließend vergleichen wir als Fazit die Beweise für $n = 3$, n gleich reguläre Primzahl (Fall 1) und von Fermats großem Satz für Polynome.

Satz 4.33. *(Fermats großer Satz für n gleich Primzahl p, Fall 2)*
Die Gleichung

$$x^p + y^p = z^p, \qquad xyz \neq 0,$$

hat für eine Primzahl $p > 2$, die genau eines der x, y, z teilt, keine ganzzahlige Lösung.

In [Was97], Kap. 9, und [Rib79], Kap. V.3, findet sich jeweils ein Beweis des Theorems, in dem dessen Aussage durch bestimmte Voraussetzungen an die Klassenzahl von $\mathbb{Q}(\zeta)$ eingeschränkt wird. Wie wir im Beweis von Satz 4.3 festgestellt haben, folgt $p \mid x$, $p \mid y$ und $p \mid z$, wenn p zwei der drei Zahlen teilt. Da eine Lösung x, y, z als paarweise teilerfremd vorausgesetzt werden kann (Bemerkung 4.4), genügt im Fall 2 die Voraussetzung, dass p genau eines der x, y, z teilt.

Betrachten wir den Anfang des Beweises von Satz 4.22 (also des Falls 1), so fällt auf, dass wir bereits dort für $p = 3$ und $p = 5$ die Voraussetzung $p \nmid xyz$ verwendet haben. Dabei zeigte sich auch eindrucksvoll, in welcher Kürze sich der erste Fall von Fermats großem Satz für $n = 3$ mit elementaren Mitteln beweisen lässt – im Gegensatz zum mehrseitigen Beweis in Abschnitt 4.5, der beide Fälle mit einschließt. Insbesondere fußte dann der Beweis des Lemmas 4.31, also dass $\langle x + \zeta^i y\rangle$, $i = 0, \ldots, p-1$, paarweise teilerfremd sind, auf der Voraussetzung $p \nmid xyz$.

Für den abschließenden Vergleich der Beweise für $n = 3$, n gleich reguläre Primzahl (Fall 1) und von Fermats großem Satz für Polynome wollen wir diese kurz mit (3), (p) und (P) bezeichnen. Wie bei einer solchen Aussage üblich, haben wir die Beweise durch Widerspruch geführt; genauer haben wir bei (3) und (P) die Methode des unendlichen Abstiegs angewendet. In allen drei Fällen wird das ursprünglich additive Problem mittels Faktorisierung in ein multiplikatives der Form (4.18) bzw. (4.28) bzw. (4.38) umgewandelt. Anschließend wurde gezeigt, dass die Faktoren paarweise teilerfremd sind (bei (3) mit der Einschränkung, dass $\xi + \upsilon$, $\xi + \omega\upsilon$, $\xi + \omega^2\upsilon$ durch λ teilbar sind). Aus der Eindeutigkeit der Primzerlegung folgt dann als gleichartiger Zwischenschritt, dass die (um λ reduzierten) Faktoren gleich einer p-ten (dritten) Potenz sind.

Bei (3) und (p) gibt es noch eine weitere auffällige Analogie. Und zwar spielt bei (3) das Primelement[‡] $\lambda = 1 - \zeta_3$ mit $\lambda^2 \sim 3$ eine zentrale Rolle. Das Gegenstück bei (p) ist das Primideal $\langle 1 - \zeta_p\rangle$, wobei $\langle 1 - \zeta_p\rangle^{p-1} = \langle p\rangle$ ist. Zusammengefasst weisen die drei Beweise also grundlegende gemeinsame Argumentationsstrukturen auf. Deutliche

[‡]Nach Beweis von Satz 3.9 ist $N(1 - \omega) = 1^2 - 1 \cdot (-1) + (-1)^2 = 3$ und die Norm auf $\mathbb{Z}[\omega]$ multiplikativ. Sei nun $\lambda = \eta_1\eta_2$ eine Zerlegung. Aus $3 = N(\lambda) = N(\eta_1)N(\eta_2)$ folgt, da 3 eine Primzahl ist, $N(\eta_1) = 1$ oder $N(\eta_2) = 1$. Also ist η_1 oder η_2 eine Einheit und damit λ irreduzibel bzw. prim.

Unterschiede ergeben sich aus den unterschiedlichen Voraussetzungen – bei (P) liegt ein Polynomring über einem abgeschlossenen Körper vor, während bei (p) im Allgemeinen nur die Zerlegung in Primideale eindeutig ist und zusätzlich $p \nmid xyz$ gilt.

Anhang

A. Idealarithmetik in Integritätsringen

In Integritätsringen lassen sich Teilbarkeitsbeziehungen weitgehend unverändert idealtheoretisch interpretieren. Dabei orientieren wir uns in diesem kurzen Abschnitt an den Ausführungen in [KM17], Kap. 16.1-2. Sei hierfür R ein Integritätsring, $a, b, c, p, u \in R$ und $\mathfrak{a}, \mathfrak{b}, \mathfrak{m}, \mathfrak{p}$ Ideale von R. Für Beispiele wählen wir jeweils $R = \mathbb{Z}$.

Korollar A.1. *Das Produkt $\langle a\rangle\langle b\rangle = \langle ab\rangle$ zweier Hauptideale ist wieder ein Hauptideal.*

Beweis. Das Korollar wird in [KM17] als Lemma 15.9 bewiesen. □

Definition A.2. ([KM17], Kap. 16.2, Bemerkung)
Man sagt, ein Ideal $\mathfrak{a}$ *teilt* ein Ideal $\mathfrak{b}$, symbolisch $\mathfrak{a} \mid \mathfrak{b}$, wenn $\mathfrak{a} \supseteq \mathfrak{b}$.

Sind $\mathfrak{a}$ und $\mathfrak{b}$ Hauptideale, dann liegt somit insbesondere der Erzeuger von $\mathfrak{b}$ in $\mathfrak{a}$ und ist ein Vielfaches des Erzeugers von $\mathfrak{a}$.

Beispiel A.3. Beispielsweise gilt $\langle 2\rangle\langle 6\rangle = \langle 12\rangle$ und $\langle 2\rangle \mid \langle 6\rangle$.

Definition A.4. ([Fis17], Kap. 2.2.13, Definition 1)
Ein Ideal $\mathfrak{p} \neq R$ heißt *Primideal*, wenn für beliebige Ideale $\mathfrak{a}, \mathfrak{b}$ aus $\mathfrak{p} \mid \mathfrak{ab}$ stets $\mathfrak{p} \mid \mathfrak{a}$ oder $\mathfrak{p} \mid \mathfrak{b}$ folgt.

Beispiel A.5. In $\mathbb{Z}$ ist die Menge der geraden Zahlen $\langle 2\rangle$ ein Primideal. Da in $\mathbb{Z}$ jedes Ideal als Hauptideal darstellbar ist, folgt aus $\mathfrak{p} \mid \langle a\rangle\langle b\rangle = \langle ab\rangle$, dass a oder b gerade ist und somit ist $\langle a\rangle$ oder $\langle b\rangle$ teilbar durch $\langle 2\rangle$ (genauer bleiben nur die Möglichkeiten $a = \pm 2$, $b = \pm 1$ und $a = \pm 1$, $b = \pm 2$). Dagegen ist $\langle 6\rangle$ kein Primideal, denn aus $\langle 6\rangle \mid \langle 2\rangle\langle 3\rangle$ folgt weder $2 \in \langle 6\rangle$ noch $3 \in \langle 6\rangle$.

Mit dem folgenden "Sammel"lemma werden wir sehen, dass genau jedes von einer Primzahl erzeugte Hauptideal ein Primideal von $\mathbb{Z}$ ist:

Lemma A.6. *Es gilt:*

a) $a \sim b \iff \langle a\rangle = \langle b\rangle$*;*

b) $p \neq 0$ *ist genau dann prim, wenn* $\langle p\rangle$ *ein Primideal ist;*

c) $u \in R^\times \iff \langle u\rangle = R$ *für eine Einheit* u*;*

d) $a \mid b \iff \langle a\rangle \mid \langle b\rangle$.

Beweis. Das Sammellemma ist ein Teil von Lemma 16.5 in [KM17]. □

Abschließend erinnern wir an die Kongruenzrelation modulo einem Ideal:

Definition A.7. ([Sch07], Definition 6.2.11)
Elemente a, b heißen *kongruent modulo* $\mathfrak{a}$, in Formeln $a \equiv b \pmod{\mathfrak{a}}$, wenn $a - b \in \mathfrak{a}$ ist.

B. Eindeutigkeit der Primzerlegung

Wir wollen an die Definition eines faktoriellen und später eines Dedekind-Rings erinnern, da deren Kenntnis für die Arbeit wesentlich ist. Beide sind Integritätsringe, so dass im Folgenden mit R und S, sofern nicht anders angegeben, stets ein Integritätsring gemeint ist. In Ersterem ist die *Zerlegung* in *Primelemente* bis auf Reihenfolge *eindeutig* (ZPE) und in Letzterem die *Zerlegung* in *Primideale* (ZPI). Am Ende steht die Aussage, unter welchem Umstand ein Ganzheitsring (wie $\mathbb{Z}[\zeta_p]$) faktoriell ist.

Definition A.8. ([KM17], Definition 17.1.1)
Ein Integritätsring heißt *faktoriell* oder *ZPE-Ring*, wenn in ihm jede Nichteinheit $a \neq 0$ eine bis auf Reihenfolge und Assoziiertheit eindeutige Zerlegung

$$a = q_1 q_2 \dots q_r$$

in irreduzible Elemente besitzt. D. h., für eine weitere Darstellung $a = q_1' q_2' \dots q_s'$ gilt $r = s$ und nach eventueller Umnummerierung der q_j' ist $q_i \sim q_i'$ für $i = 1, \dots, r$.

Kurz und präzise gesagt ist in einem faktoriellen Ring die Zerlegung in Primelemente bis auf Einheiten und Reihenfolge eindeutig.

Beispiel A.9. Bekanntlich sind ± 1 die einzigen Einheiten im Ring $\mathbb{Z}$, in dem die Primfaktorzerlegung bis auf Reihenfolge und Vorzeichen eindeutig bestimmt ist. Ein weiteres wichtiges Beispiel in der Algebra sind Polynomringe $R[T]$ über einem faktoriellen Ring R. Ein Beispiel für eine irreduzibles Polynom im Ring $\mathbb{Q}[T]$ ist das neunte Kreisteilungspolynom $\Phi(T) = T^6 + T^3 + 1$, wie sich mit Hilfe des Eisensteinkriteriums unter Verwendung der Substitution $T = T' + 1$ zeigen lässt.

Definition A.10. ([Fis17], Kap. 2.2.7, Definition)
Ein euklidischer Ring R ist ein Integritätsring mit einer Abbildung $N\colon R \backslash \{0\} \to \mathbb{N}_0$, so dass gilt: Für alle $a, d \in R$, $d \neq 0$, existieren $q, r \in R$ mit $a = qd + r$, wobei $r = 0$ oder $N(r) < N(d)$ ist.

Bemerkung A.11. Vereinfacht gesprochen kann man in einem euklidischen Ring mit Rest teilen. Die bei Zahlringen *Norm* genannte Abbildung N verkörpert die Eigenschaft, dass ein Rest r stets "kleiner" wird als der Divisor d.

Beispiel A.12. $\mathbb{Z}$ hat als Norm den Betrag, der auch für 0 definiert ist. Weiter ist $R[T]$ mit der Abbildung $\operatorname{grad}\colon R[T] \backslash \{0\} \to \mathbb{N}_0$, die jedem Polynom $P \neq 0$ seinen Grad zuordnet, euklidisch, wenn R ein Körper ist ([Fis17], Kap. 2.2.7, Korollar). Ein Beispiel für einen ZPE-Ring, der nicht euklidisch ist, ist $\mathbb{Z}[T]$.

Satz A.13. *Jeder euklidische Ring ist faktoriell.*

Beweis. Hierfür wird typischerweise gezeigt, dass ein euklidischer Ring ein Hauptidealring und dieser wiederum faktoriell ist, vgl. z.B. [KM17], Satz 18.4 und Satz 18.1. □

Der Satz erweist sich vielfach als nützlich, um nachzuweisen, dass ein Ring faktoriell ist. Für die nun folgende Definition eines Dedekind-Rings wiederholen wir den Begriff des ganzen Elements, des noetherschen Rings und des maximalen Ideals:

Definition A.14. ([Neu07], Definition 2.1; [MSP11], Definition 16.4)
Man sagt, R ist *ganz-abgeschlossen*, wenn R ganz-abgeschlossen in seinem Quotientenkörper ist.

Definition A.15. ([KM17], Lemma 19.10 (3))
Ein Integritätsring heißt *noethersch*, wenn in ihm jedes Ideal endlich erzeugt ist.

Somit sind Hauptidealringe wie die in A.12 aufgeführten Beispiele noethersch.

Definition A.16. ([KM17], Einleitung Kap. 15.8)
Ein Ideal $\mathfrak{m} \subsetneq R$ heißt *maximal*, wenn es kein weiteres Ideal $\mathfrak{a} \subsetneq R$ von gibt, das $\mathfrak{m}$ enthält. D.h., für jedes solche Ideal $\mathfrak{a} \supseteq \mathfrak{m}$ folgt direkt $\mathfrak{a} = \mathfrak{m}$.

Definition A.17. ([MSP11], Definition 18.5)
Ein *Dedekind-Ring* $\mathcal{O}$ ist ein ganz-abgeschlossener, noetherscher Integritätsring, in dem jedes Primideal $\mathfrak{p} \neq 0$ ein maximales Ideal ist.

Wir kommen nun zu zwei zentralen Aussagen des Abschnitts. Gemeinhin wollen wir nachfolgend mit $\mathcal{O}$ einen Dedekind-Ring mit Quotientenkörper L bezeichnen.

Satz A.18. *In einem Dedekindring $\mathcal{O}$ besitzt jedes von $\langle 0 \rangle$ und $\mathcal{O}$ verschiedene Ideal $\mathfrak{a}$ eine bis auf Reihenfolge eindeutige Zerlegung*

$$\mathfrak{a} = \mathfrak{p}_1^{m_1} \dots \mathfrak{p}_r^{m_r}$$

in Primideale $\mathfrak{p}_i$ von $\mathcal{O}$.

Beweis. Dieser bedeutende Satz wird z.B. als Theorem 3.3 in [Neu07] bewiesen. □

Satz A.19. *Der Ganzheitsring eines Zahlkörpers ist ein Dedekind-Ring.*

Beweis. Ein Beweis findet sich u.a. in [MSP11] im Anschluss an Satz 18.6. □

Somit ist $\mathbb{Z}[\zeta_p]$ ein Dedekind-Ring. Am Ende von Abschnitt 3.3 hatten wir als Beispiel angegeben, dass das Hauptideal $\langle 2 \rangle$ von $\mathbb{Z}[\zeta_{23}]$ eindeutig als $\langle 2, 1+\sqrt{-23} \rangle \langle 2, 1-\sqrt{-23} \rangle$ in Primideale faktorisiert. Um entscheiden zu können, ob ein Dedekind-Ring faktoriell ist, arbeiten wir nun auf den Begriff der Klassenzahl hin.

Definition A.20. ([MSP11], Definition 18.7; [Sch07], Definition 6.4.1)
Eine Teilmenge $\mathfrak{g} \subset L$ heißt *gebrochenes Ideal* von L, wenn ein $\alpha \in \mathcal{O}$, $\alpha \neq 0$, existiert,

so dass

$$\alpha\mathfrak{g} = \{\alpha\gamma \mid \gamma \in \mathfrak{g}\}$$

ein Ideal von $\mathcal{O}$ ist.

Bemerkung A.21. Zur besseren Abgrenzung nennt man (gewöhnliche) Ideale auch *ganze* Ideale. Die gebrochenen Ideale eines Zahlkörpers sind quasi das Gegenstück der multiplikativen (rationalen) Inversen ganzer Zahlen: Ähnlich wie die ganzen Zahlen außer ± 1 keine solchen Inversen besitzen, gilt für Ideale $\mathfrak{a}, \mathfrak{b}$, $\mathfrak{a} \subsetneq \mathcal{O}$, von $\mathcal{O}$ stets $\mathfrak{ab} \subseteq \mathfrak{a} \neq \mathcal{O}$ (der Ring $\mathcal{O}$ selbst ist das Einselement in $\mathcal{O}$; [Neu07], vor Definition 3.7).

Satz A.22. *Die Menge der von $\langle 0\rangle$ verschiedenen, gebrochenen Ideale bildet eine multiplikative abelsche Gruppe J_L von L. Hierbei ist $\mathcal{O}$ das neutrale Element und das inverse Element zu $\mathfrak{g}$ ist*

$$\mathfrak{g}^{-1} = \{\alpha \in L \mid \alpha\mathfrak{g} \subseteq \mathcal{O}\}.$$

Beweis. Diese Aussage wird z.B. in [Neu07] als Satz 3.8 dargelegt. □

Beispiel A.23. In $\mathbb{Q}$ ist die Menge $\mathfrak{g} = \{a/m \mid a \in \mathbb{Z}\}$ für ein festes $m \in \mathbb{N}$ ein gebrochenes Ideal, denn mit demselben $m \in \mathbb{Z}$ ist $m\mathfrak{g} = \mathbb{Z}$ ein Ideal von $\mathbb{Z}$. Weiter ist $\mathfrak{g}^{-1}$ die Menge aller ganzzahligen Vielfachen der Kehrbrüche m/a.

Lemma A.24. *Die Menge der gebrochenen Hauptideale $\{\langle\alpha\rangle = \alpha\mathcal{O} \mid \alpha \in L\setminus\{0\}\}$ bildet eine Untergruppe P_L von J_L.*

Beweis. Auch dieser Hilfssatz wird gegen Ende von [Neu07], Kap. 1.3, bewiesen. □

Definition A.25. ([MSP11], Definition 18.17)
Die Quotientengruppe

$$Cl_L = J_L/P_L$$

heißt die *Idealklassengruppe* von L. Ihre Ordnung h_L heißt die *Klassenzahl* von L.

Bemerkung A.26. Die Klassenzahl eines Zahlkörpers L ist ein Maß dafür, wie weit sein Ganzheitsring $\mathcal{O}_L$ davon entfernt ist, eindeutig in Primelemente zu faktorisieren. Bei Zahlkörpern ist sie stets endlich ([MSP11], Satz 18.19).

Wann genau der Ganzheitsring faktoriell ist, sagt nun folgender Satz aus:

Satz A.27. *Für einen Zahlkörper L sind die folgenden Aussagen äquivalent:*

a) $h_L = 1$.

b) $\mathcal{O}_L$ *ist ein faktorieller Ring.*

c) $\mathcal{O}_L$ *ist ein Hauptidealring.*

Für einen Beweis verweisen wir z.B. auf den Beweis von Korollar 18.18 in [MSP11]. In Satz 3.15 haben wir bereits aufgelistet, dass $h_{\mathbb{Q}(\zeta_p)} = 1$ ist genau dann, wenn $p \leq 19$ ist.

Als Letztes wollen wir die "fundamentale Gleichung" aus der algebraischen Zahlentheorie erinnern. Die beiden nächsten Aussagen können samt Beweise in [Neu07] vor und als Satz 8.2 nachgelesen werden:

Satz A.28. *Ein Primideal $\langle p \rangle$ von $\mathcal{O}_L$ (Ganzheitsring eines Zahlkörpers L) zerfällt in $\mathcal{O}_L$ eindeutig in ein Produkt*

$$\langle p \rangle = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$$

von Primidealen $\mathfrak{p}_i$.

Bemerkung A.29. Der Exponent e_i, *Verzweigungsindex* genannt, der sogenannte *Trägheitsgrad* f_i von $\mathfrak{p}_i$ über $\langle q \rangle$, welcher durch

$$f_i \coloneqq [\mathcal{O}_L/\mathfrak{p}_i : \mathbb{Z}/\langle q \rangle]$$

definiert ist, und der Grad der Körpererweiterung $L/\mathbb{Q}$ stehen dabei in der folgenden Beziehung:

$$\sum_{i=1}^{r} e_i f_i = [L : \mathbb{Q}]. \qquad \text{(fundamentale Gleichung)}$$

Literaturverzeichnis

[ADNE+14] Alten, H.-W.; Djafari Naini, A.; Eick, B.; Folkerts, M.; Schlosser, H.; Schlote, K.-H.; Wesemüller-Kock, H.; Wussing, H.: *4000 Jahre Algebra*. Springer Spektrum, 2014

[AN20] Alfes-Neumann, C.: *Modulformen*. Springer Spektrum, 2020

[Bos18] Bosch, S.: *Algebra*. Birkhäuser Basel, 2018

[Brü17] Brückler, F. M.: *Geschichte der Mathematik kompakt*. Springer Spektrum, 2017

[Bun08] Bundschuh, P.: *Einführung in die Zahlentheorie*. Springer-Verlag Berlin Heidelberg, 2008

[Fis17] Fischer, G.: *Lehrbuch der Algebra*. Springer Spektrum, 2017

[HW75] Hardy, G. H.; Wright, E. M.: *An Introduction to the Theory of Numbers*. Oxford University Press, 1975

[IR90] Ireland, K.; Rosen, M.: *A Classical Introduction to Modern Number Theory*. Springer-Verag New York, 1990

[JJ98] Jones, G. A.; Jones, J. M.: *Elementary Number Theory*. Springer-Verlag London, 1998

[KM17] Karpfinger, Ch.; Meyberg, K.: *Algebra*. Springer Spektrum, 2017

[Kra02] Kramer, J.: *Der große Satz von Fermat – die Lösung eines 300 Jahre alten Problems*. In: Aigner M.; Behrends, E. (Hrsg.): *Alles Mathematik*. Vieweg+Teubner Verlag, 2002

[Lem17] Lemmermeyer, F.: *Quadratische Zahlkörper*. Springer Spektrum, 2017

[MSP11] Müller-Stach, St.; Piontkowski, J.: *Elementare und algebraische Zahlentheorie*. Vieweg+Teubner Verlag, 2011

[Neu07] Neukirch, J.: *Algebraische Zahlentheorie*. Springer-Verlag Berlin Heidelberg New York, 2007

[OR96] O'Connor, J. J.; Robertson, E. F.: *Fermat's last theorem*. In: MacTutor History of Mathematics Archives. URL: https://mathshistory.st-andrews.ac.uk/HistTopics/Fermat's_last_theorem/ (Abruf am 18.06.2020), 1996

[OS15] Oswald, N.; Steuding, J.: *Elementare Zahlentheorie.* Springer Spektrum, 2015

[Rib79] Ribenboim, P.: *13 Lectures on Fermat's Last Theorem.* Springer-Verlag New York, 1979

[Rib99] Ribenboim, P.: *Fermat's Last Theorem for Amateurs.* Springer-Verlag New York, 1999

[Roq98] Roquette, P.: *Zum Fermat-Problem.* URL: https://www.mathi.uni-heidelberg.de/~roquette/fermat.pdf (Abruf am 12.05.2020), 1998

[Ros97] Rosen, M.: *Remarks on the History of Fermat's Last Theorem 1844 to 1984.* In: Cornell, G.; Silverman, J.; Stevens, G. (Hrsg.): *Modular Forms and Fermat's Last Theorem.* Springer-Verlag New York, 1997

[Sch07] Schmidt, A.: *Einführung in die algebraische Zahlentheorie.* Springer-Verlag Berlin Heidelberg, 2007

[Sha19] Sharifi, R.: *Iwasawa Theory: A Climb up the Tower.* In: *Notices of the American Mathematical Society* (66) (2019)

[Sin97] Singh, S.: *Fermats letzter Satz.* Carl Hanser Verlag München Wien, 1997

[Ste97] Stevens, G.: *An Overview of the Proof of Fermat's Last Theorem.* In: Cornell, G.; Silverman, J.; Stevens, G. (Hrsg.): *Modular Forms and Fermat's Last Theorem.* Springer-Verlag New York, 1997

[SV12] Scherfner, M.; Volland, T.: *Mathematik für das erste Semester.* Springer Spektrum, 2012

[Was97] Washington, L. C.: *Introduction to Cyclotomic Fields.* Springer-Verlag New York, 1997

[Woh11] Wohlgemuth, M.: *Mathematisch für Anfänger.* Springer Spektrum, 2011

[Wol11] Wolfart, J.: *Einführung in die Zahlentheorie und Algebra.* Vieweg+Teubner, 2011

Folgende weitere Quellen wurden für die Bearbeitung ergänzend herangezogen:

Brünner, A. (2003): *Leonhard Eulers Beweis, daß weder die Summe noch die Differenz zweier Kubikzahlen wieder eine Kubikzahl sein kann*. URL: https://www.arndt-bruenner.de/mathe/Allgemein/eulericubi.htm (Abruf am 13.07.2020)

Huber-Klawitter, A.: *Algebraische Zahlentheorie – Sommersemester 2014*. Bearbeitungsstand: 27.07.2014. URL: https://home.mathematik.uni-freiburg.de/arithgeom/lehre/ss14/algzt.html (Abruf am 12.05.2020)

Jannsen, U. (o. J.): *Algebraische Zahlentheorie I – Wintersemester 2007/08*. URL: http://www.mathematik.uni-regensburg.de/Jannsen/home/UebungWS0708/AlgZahlN.pdf (Abruf am 29.05.2020)

Magidin, A. (2011): *How to show that* $1-\zeta$ *is prime in the order* $\{1,\zeta,\ldots,\zeta^{l-2}\}$*?*. In: Mathematics Stack Exchange. URL: https://math.stackexchange.com/questions/20438/how-to-show-that-1-zeta-is-prime-in-the-order-1-zeta-ldots-zetal (Abruf am 25.06.2020)

Martin_Infinite (2015): *Teilerfremdheit*. In: Matroids Matheplanet. URL: https://www.matheplanet.com/matheplanet/nuke/html/viewtopic.php?topic=208377 (Abruf am 16.06.2020)

O'Connor, J. J.; Robertson, E. F. (1996): *Marie-Sophie Germain*. In: MacTutor History of Mathematics Archive. URL: https://mathshistory.st-andrews.ac.uk/Biographies/Germain/ (Abruf am 04.07.2020)

Silverman, J. H. (2012): *A Friendly Introduction to Number Theory*. URL: http://www.math.brown.edu/~jhs/frintdir/frintch2ch3.pdf (Abruf am 19.06.2020), Pearson Education, Inc.

Soergel, W.: *Algebra und Zahlentheorie mit grundlegenden Abschnitten aus der Linearen Algebra*. Bearbeitungsstand: 10.02.2020. URL: http://home.mathematik.uni-freiburg.de/soergel/Skripten/XXALMG.pdf (Abruf am 29.04.2020)

Spannagel, Ch. (2012): *Der große Satz von Fermat Teil 1*. In: YouTube. URL: https://www.youtube.com/watch?v=dy-Queapz-I (Abruf am 26.04.2020)

Spannagel, Ch. (2012): *Der große Satz von Fermat Teil2*. In: YouTube. URL: https://www.youtube.com/watch?v=3rS5dlZaymM (Abruf am 26.04.2020)

Wendt, M. (o. J.): *Skript zur Vorlesung Algebraische Zahlentheorie – WS 2011/12*. URL: http://home.mathematik.uni-freiburg.de/arithgeom/lehre/ws11/azt/wendt-azt11.pdf (Abruf am 04.07.2020)

Wikipedia: *Algebraische Zahl*. In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 01.04.2020, 11:43, UTC. URL: https://de.wikipedia.org/w/index.php?title=Algebraische_Zahl&oldid=198349550 Abruf am 23.05.2020)

Wikipedia: *Algebraischer Zahlkörper*. In: Wikipedia – Die freie Enzyklopädie. Bearbei-

tungsstand: 21.01.2020, 19:04 UTC. URL: https://de.wikipedia.org/w/index.php?title=Algebraischer_Zahlk%C3%B6rper&oldid=196046266 (Abruf am 23.05.2020)

Wikipedia: *Bernoulli-Zahl*. In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 02.07.2019, 20:33 UTC. URL: https://de.wikipedia.org/w/index.php?title=Bernoulli-Zahl&oldid=190075844 (Abruf am 13.06.2020)

Wikipedia: *Dedekindring*. In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 18.05.2019, 12:25 UTC. URL: https://de.wikipedia.org/w/index.php?title=Dedekindring&oldid=188698405 (Abruf am 03.06.2020)

Wikipedia: *Einheitswurzel*. In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 09.12.2018, 11:42 UTC. URL: https://de.wikipedia.org/w/index.php?title=Einheitswurzel&oldid=183543794 (Abruf am 16.05.2020)

Wikipedia: *Eisenstein-Zahl*. In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 01.02.2020, 22:14 UTC. URL: https://de.wikipedia.org/w/index.php?title=Eisenstein-Zahl&oldid=196411093 (Abruf am 26.05.2020)

Wikipedia: *Elliptische Kurve*. In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 14.05.2020, 21:27, 13:51 UTC. URL: https://de.wikipedia.org/w/index.php?title=Elliptische_Kurve&oldid=199961060 (Abruf am 02.07.2020)

Wikipedia: *Ernst Eduard Kummer*. In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 29.12.2019, 10:12 UTC. URL: https://de.wikipedia.org/w/index.php?title=Ernst_Eduard_Kummer&oldid=195308245 (Abruf am 11.06.2020)

Wikipedia: *Freie abelsche Gruppe*. In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 30.07.2019, 15:25, UTC. URL: https://de.wikipedia.org/w/index.php?title=Freie_abelsche_Gruppe&oldid=190888683 (Abruf am 14.06.2020)

Wikipedia: *Ganzheitsring*. In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 18.12.2019, 13:51 UTC. URL: https://de.wikipedia.org/w/index.php?title=Ganzheitsring&direction=prev&oldid=201418323 (Abruf am 15.05.2020)

Wikipedia: *Gaußsche Zahl*. In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 26.12.2019, 16:23 UTC. URL: https://de.wikipedia.org/w/index.php?title=Gau%C3%9Fsche_Zahl&oldid=195234063 (Abruf am 21.05.2020)

Wikipedia: *Großer Fermatscher Satz*. In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 20.11.2020, 12:20 UTC. URL: https://de.wikipedia.org/w/index.php?title=Gro%C3%9Fer_Fermatscher_Satz&oldid=196003351 (Abruf am 22.04.2020)

Wikipedia: *Hauptideal*. In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 31.08.2019, 12:26 UTC. URL: https://de.wikipedia.org/w/index.php?title=Hauptideal&oldid=191845152 (Abruf am 04.06.2020)

Wikipedia: *Ideal (Ringtheorie)*. In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 01.05.2020, 21:48 UTC. URL: https://de.wikipedia.org/w/index.php?title=Ideal_(Ringtheorie)&oldid=199511340 (Abruf am 04.06.2020)

Wikipedia: *Idealklassengruppe*. In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 26.04.2018, 14:36 UTC. URL: https://de.wikipedia.org/w/index.php?title=Idealklassengruppe&oldid=176889081 (Abruf am 16.05.2020)

Wikipedia: *Klassenzahl*. In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 25.09.2019, 17:37 UTC. URL: https://de.wikipedia.org/w/index.php?title=Klassenzahl&oldid=192586318 (Abruf am 16.05.2020)

Wikipedia: *Kongruenz (Zahlentheorie)*. In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 02.02.2020, 11:58 UTC. URL: https://de.wikipedia.org/w/index.php?title=Kongruenz_(Zahlentheorie)&oldid=196424651 (Abruf am 30.04.2020)

Wikipedia: *Kreisteilungskörper*. In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 29.06.2016, 14:18 UTC. URL: https://de.wikipedia.org/w/index.php?title=Kreisteilungsk%C3%B6rper&oldid=155728802 (Abruf am 06.06.2020)

Wikipedia: *Modul (Mathematik)*. In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 30.06.2020, 16:57 UTC. URL: https://de.wikipedia.org/w/index.php?title=Modul_(Mathematik)&oldid=201447761 (Abruf am 02.07.2020)

Wikipedia: *Modularitätssatz*. In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 11.05.2020, 20:31 UTC. URL: https://de.wikipedia.org/w/index.php?title=Modularit%C3%A4tssatz&oldid=199857318 (Abruf am 02.07.2020)

Wikipedia: *Modulform*. In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 19.02.2020, 21:00 UTC. URL: https://de.wikipedia.org/w/index.php?title=Modulform&oldid=196973419 (Abruf am 02.07.2020)

Wikipedia: *Pythagoreisches Tripel*. In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 22.04.2020, 10:43 UTC. URL: https://de.wikipedia.org/w/index.php?title=Pythagoreisches_Tripel&oldid=199157800 (Abruf am 22.04.2020)

Wikipedia: *Quadratischer Zahlkörper*. In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 28.11.2019, 13:46 UTC. URL: https://de.wikipedia.org/w/index.php?title=Quadratischer_Zahlk%C3%B6rper&oldid=194458783 (Abruf am 06.06.2020)

Wikipedia: *Reguläre Primzahl*. In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 04.04.2019, 10:36 UTC. URL: https://de.wikipedia.org/w/index.php?title=Regul%C3%A4re_Primzahl&oldid=187224674 (Abruf am 07.06.2020)

Wikipedia: *Unendlicher Abstieg*. In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 04.02.2020, 13:55 UTC. URL: https://de.wikipedia.org/w/index.php?title=Unendlicher_Abstieg&oldid=196490736 (Abruf am 03.05.2020)

Wikipedia: *Verzweigung (Algebra)*. In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 06.10.2019, 05:59 UTC. URL: https://de.wikipedia.org/w/index.php?title=Verzweigung_(Algebra)&oldid=192889849 (Abruf am 08.06.2020)