Quadratische Zahlkörper
Schnupperkurs

Franz Lemmermeyer
hb3@ix.urz.uni-heidelberg.de

30. Juli 1999

Vorwort

Dieser 'Schnupperkurs'[1] soll anhand der Theorie der quadratischen Zahlkörper in die algebraische Zahlentheorie einführen; der Beschränkung auf quadratische Zahlkörper liegt die Einsicht zugrunde, daß man hier noch (fast) alle Beispiele von Hand rechnen kann.

Als Voraussetzungen sind Kenntnisse der linearen Algebra (Vektorräume, lineare Abbildungen, Matrizenrechnung), sowie eine Vertrautheit mit Begriffen der elementaren Zahlentheorie (eindeutige Primfaktorzerlegung, Kongruenzrechung, quadratische Reste) zu nennen.

Von den Anwendungen der Theorie quadratischer Zahlkörper erwähnen wir die folgenden: man kann damit diophantische Gleichungen wie $y^2 = x^3 - 2$ oder $x^3 + y^3 = z^3$ lösen, den Lucas–Lehmer–Test beweisen (damit kann man relativ schnell feststellen, ob eine Zahl der Form $2^p - 1$ prim ist), und Algorithmen zur Faktorisierung großer Zahlen entwickeln: der erste Faktorisierungsalgorithmus, der auf der Theorie quadratischer Zahlkörper aufbaute, war Shanks 'square form factorization'; diese Methode ist für 'kleine' Zahlen N (zwischen 10 und 20 Stellen) wohl immer noch die schnellste und für programmierbare Taschenrechner ideal, weil sie nur mit Zahlen $< \sqrt{N}$ rechnet; der schnellste bekannte Faktorisierungsalgorithmus überhaupt ist das 'number field sieve', das auf der Arithmetik beliebiger Zahlkörper aufbaut.

Einige Lehrbücher

[Ar] M. Artin, *Algebra*, Birkhäuser Verlag, xiii, 705 p. DM 88.00 (1993).

[Ba] P. Bachmann, *Zahlentheorie III. Die Lehre von der Kreisteilung*, reprint 1968

[C1] H. Cohn, *A classical invitation to algebraic numbers and class fields*, 2nd ed. Universitext, Springer-Verlag xiii, 328 p. (1988).

[C2] H. Cohn, *Advanced number theory*, Dover Publications, Inc. XI, 276 p. (1980); reprint of *A second course in number theory*, John Wiley and Sons, Inc. XIII, 276 p. (1962).

[1] Zweistündige Vorlesung an der Universität des Saarlands, Wintersemester 1997/98.

[Fr] G. Frey, *Elementare Zahlentheorie*, Vieweg & Sohn, 119 S. (1984)

[Gu] K.-B. Gundlach, *Einführung in die Zahlentheorie*, B.I. Mannheim, 311 S. (1972).

[HW] G.H. Hardy, E.M. Wright, *An introduction to the theory of numbers*, 5th ed. Clarendon Press. XVI, 426 p. (1979).

[Ho] L. Holzer, *Zahlentheorie*, Teil I. Teubner (1958) 202 S; Teil II. Teubner (1959) 126 S; Teil III. Teubner (1965) 146 S.

[IR] K. Ireland, K. Rosen, *A classical introduction to modern number theory*, 2nd ed. Graduate Texts in Mathematics, 84. Springer-Verlag xiv, 389 p. (1990).

[Ko] A.I. Kostrikin, *Introduction to algebra*, Universitext, Springer-Verlag. XIII, 575 p. (1982). Zbl 482.00001

[Le] A. Leutbecher, *Zahlentheorie. Eine Einführung in die Algebra*, Springer, xii, 354 p. (1996).

[Lb] H. Lüneburg, *Vorlesungen über Zahlentheorie*, Birkhäuser Verlag 1978

[M1] R. Mollin, *Fundamental Number Theory with Applications*, CRC Press 1998.

[M2] R. Mollin, *Quadratics*, CRC Press, xx, 387 p. (1996).

[SO] W. Scharlau, H. Opolka, *Von Fermat bis Minkowski. Eine Vorlesung über Zahlentheorie und ihre Entwicklung*, Springer-Verlag. XI, 224 S., 13 Abb. (1980).

[So] J. Sommer, *Vorlesungen über Zahlentheorie*, (1907)

[ST] I. Stewart, D. Tall, *Algebraic number theory*, 2nd ed. Chapman and Hall 1987; XIX, 262 p.

[Za] D. Zagier, *Zetafunktionen und quadratische Körper*, Springer-Verlag. IX, 144 S. (1981).

Die beiden angegebenen Algebrabücher von M. Artin (Sohn von E. Artin) und A. Kostrikin zählen meiner Meinung nach zu den besten Einführungen, die es auf diesem Gebiet gibt. Für den Kurs interessant sind jeweils die Ausführungen über Hauptidealringe, euklidische Ringe, und ZPE-Ringe – vielleicht bleibt der eine oder andere aber an etwas anderem hängen.

Von den Zahlentheoriebüchern gehen die meisten gleich in die vollen – am ehesten brauchbar scheint noch Stewarts und Talls Buch zu sein. Die andern Bücher enthalten jeweils ein oder mehrere Kapitel über quadratische Zahlkörper. Ein Muß ist aber das Buch von Scharlau und Opolka.

Einige URLs

`http://www.rzuser.uni-heidelberg.de/~hb3/` ist meine homepage.

`http://www.maths.ex.ac.uk/~rjc/rjc.html` ist Robin Chapmans homepage und enthält ein kleines Skript über algebraische Zahlen (Notes on Algebraic Numbers).

`http://www.math.uga.edu/~ntheory/web.html` ist die homepage des Number Theory Web, verwaltet von Keith Matthews.

`http://turing.wins.uva.nl/~psh/` ist Peter Stevenhagens homepage und enthält das Skript Getaltheorie 1 (auf englisch).

`http://hasse.mathematik.tu-muenchen.de/nfdb/Welcome_e` ist die homepage des 'Number Field Database', verwaltet von Gerhard Niklasch.

`http://www.algebra.tu-bs.de/mathiak/skripte/` ist die homepage von Karl Mathiak und enthält Skripte zur Algebra und Zahlentheorie; das Skript 'Zahlentheorie I' enthält Stoff über quadratische Zahlkörper.

Inhaltsverzeichnis

Kapitel 1

Motivation und Vorstellung der Akteure

Quadratische Zahlkörper gehören naturgemäß zur algebraischen Zahlentheorie, also der Theorie der algebraischen Zahlen. Diese treten bei der Untersuchung mancher Probleme der elementaren Zahlentheorie ganz natürlich auf, wie die folgenden Beispiele zeigen.

1.1 Identitäten

Ein beliebtes Problem bei Schülerolympiaden ist das folgende: sind die natürlichen Zahlen m und n Summen zweier Quadrate, dann auch ihr Produkt mn. Der Beweis besteht einfach aus dem Nachrechnen der Identität

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

Hier stellt man sich natürlich die Frage, wo das herkommt. Die Idee ist folgende: $a^2 + b^2$ ist das Quadrat des Abstands der komplexen Zahl $a + bi$ vom Ursprung, also $a^2 + b^2 = (a + bi)(a - bi) = \mu\overline{\mu}$, wo $\mu = a + bi$ und $\overline{\mu}$ das Konjugiert-Komplexe von μ ist. Setzt man $\nu = c + di$, so wird

$$(a^2 + b^2)(c^2 + d^2) = \mu\overline{\mu}\nu\overline{\nu} = \mu\nu\,\overline{\mu\nu}.$$

Hieraus folgt die Identität sofort wegen $\mu\nu = (a + bi)(c + di) = ac - bd + (ad + bc)i$.

Übung. Sind a und b in der Form $x^2 - my^2$ darstellbar, dann auch ihr Produkt.

Man sieht also, daß die Einführung von Zahlen der Form $x + y\sqrt{m}$ mit rationalen Zahlen x, y das Auffinden von Identitäten wie den obigen erleichtert.

1.2 * Fibonacci-Zahlen

Die Fibonacci-Zahlen[1] F_n sind für $n \geq 1$ definiert durch die Rekursion $F_1 = F_2 = 1$ und $F_{n+1} = F_n + F_{n-1}$, $n \geq 2$. Hier eine kleine Tabelle:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
F_n	1	1	2	3	5	8	13	21	34	55	89	144	233	377	610

Sind a und b ganze Zahlen, so schreibt man $a \equiv b \bmod n$ falls $a-b$ durch n teilbar ist. Wir wollen die durch $a_n \equiv F_n \bmod n$ und $-\frac{n}{2} < a_n \leq \frac{n}{2}$ definierte Folge untersuchen. Wir rechnen:

n	1	2	3	4	5	6	7	8	9	10	11	13	17	19
a_n	0	1	-1	-1	0	2	-1	-3	-2	5	1	-1	-1	1

Wir beobachten, daß für alle Primzahlen $p \neq 5$ entweder $F_p \equiv 1 \bmod p$ oder $F_p \equiv -1 \bmod p$ gilt. Führt man die Rechnung weiter fort, so findet man $F_p \equiv 1 \bmod p$ für $p = 11, 19, 29, 31$, und $F_p \equiv -1 \bmod p$ für $p = 3, 7, 13, 17, 23, 37$. Man kommt so zu folgender Vermutung:

$$\begin{aligned} p \equiv \pm 1 \bmod 5 &\implies F_p \equiv +1 \bmod p \\ p \equiv \pm 2 \bmod 5 &\implies F_p \equiv -1 \bmod p \end{aligned}$$

Wie kann man das beweisen? Eine Möglichkeit ist via der Binetschen[2] Formel

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad \text{mit } \alpha = \frac{1+\sqrt{5}}{2},\ \beta = \frac{1-\sqrt{5}}{2}.$$

Im Nachhinein beweist man diese Formel leicht mit Induktion; herleiten kann man sie elegantissime mit etwas linearer Algebra:

[1] Nach Leonardo Fibonacci (1170–1250); dieser veröffentlichte 1202 das 'Liber abaci', das einen wesentlichen Beitrag zur Einführung der Dezimalsystems in Europa leistete und in dem auch die Fibonacci-Zahlen erstmals definiert werden.

[2] Jacques Binet (1786–1856), französischer Mathematiker

Übung. Man überzeuge sich zuerst von der Gültigkeit der Gleichung

$$\begin{pmatrix} F_n & F_{n+1} \\ F_{n+1} & F_{n+2} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{n+1}.$$

Dann diagonalisiere man $T = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ (d.h. man finde eine invertierbare Matrix $S \in M_2(\mathbb{C})$ mit $S^{-1}TS = \left(\begin{smallmatrix} \alpha & 0 \\ 0 & \beta \end{smallmatrix}\right) =: D$) und beachte, daß $T^n = (SDS^{-1})^n = SD^nS^{-1}$ gilt. Da man Diagonalmatrizen einfach potenzieren kann, erhält man nun eine Formel für die F_n.

Nun wissen wir, daß in $\mathbb{Z}$ die Formel $(a+b)^p \equiv a^p + b^p \bmod p$ gilt; wenn wir mal so tun, als sei dies auch für Zahlen der Form $c + d\sqrt{5}$ richtig, so finden wir

$$\alpha^p \equiv \frac{1^p + \sqrt{5}^p}{2^p} = \frac{1 + 5^{(p-1)/2}\sqrt{5}}{2} \bmod p, \tag{1.1}$$

und analog

$$\beta^p \equiv \frac{1 - 5^{(p-1)/2}\sqrt{5}}{2} \bmod p.$$

Also ergibt sich $F_p = \frac{\alpha^p - \beta^p}{\alpha - \beta} \equiv 5^{(p-1)/2} \bmod p$; nach dem Eulerschen Kriterium ist $5^{(p-1)/2} \equiv (\frac{5}{p}) \bmod p$, und das quadratische Reziprozitätsgesetz sagt $(\frac{5}{p}) = (\frac{p}{5})$. Daraus ergibt sich sofort die Behauptung. Es scheint also, als würde so etwas wie der 'kleine Fermatsche Satz' auch für Zahlen der Form $a + b\sqrt{5}$ gelten – jedenfalls lieferte seine Anwendung ein richtiges Ergebnis. Daß bei unserem Beweis etwas nicht ganz sauber war, erkennt man daran, daß die zu beweisende Kongruenz in $\mathbb{Z}$ lebt, die Kongruenz (1.1) dagegen nicht.

Übung. Man beweise die obige Vermutung mit elementaren Mitteln durch Entwickeln von α^p via der binomischen Formel. Man zeige auch, daß für prime $p \equiv \pm 1 \bmod 5$ immer $p \mid F_{p-1}$, für prime $p \equiv \pm 2 \bmod 5$ dagegen $p \mid F_{p+1}$ gilt; Letzteres stammt von Lagrange.[3]

1.3 Die elliptische Kurve $y^2 = x^3 - 2$

Bereits Fermat[4] hat behauptet, daß $x = 3$, $y = \pm 5$ die einzigen ganzzahlige Lösungen der diophantischen Gleichung $y^2 = x^3 - 2$ sind; die Idee, zur Løßung

[3] Joseph Louis Lagrange (1736–1813), italienisch-französischer Mathematiker, der in der Zahlentheorie vor allem für seinen Beweis des Vierquadratesatzes bekannt ist.

[4] Pièrre Fermat (1601–1665), wurde durch das Studium der von Bachet herausgegebenen Bücher Diophants zur Untersuchung zahlentheoretischer Probleme angeregt; in eines

dieser Gleichung die algebraischen Zahlen $\mathbb{Z}[\sqrt{-2}\,]$ zu verwenden, stammt von Euler.[5]

Zuerst beachte man, daß x (und damit auch y) ungerade sein muß: andernfalls wäre nämlich x^3-2 genau durch 2 teilbar und könnte kein Quadrat sein. Euler schreibt jetzt die Gleichung in der Form $y^2+2=x^3$ und faktorisiert die linke Seite im Ring $R=\mathbb{Z}[\sqrt{-2}\,]$: $(y+\sqrt{-2}\,)(y+\sqrt{-2}\,)=x^3$. Ein gemeinsamer Teiler der beiden Faktoren auf der linken Seite würde auch deren Differenz $2\sqrt{-2}=-(\sqrt{-2}\,)^3$ teilen. Aber $\sqrt{-2}$ kann kein Teiler von $y\pm\sqrt{-2}$ sein, da sonst $\sqrt{-2}\mid y$ und folglich $2\mid y$ sein müßte. Also sind $y+\sqrt{-2}$ und $y+\sqrt{-2}$ teilerfremd, und ihr Produkt ist eine dritte Potenz. Also, sagt sich Euler, müssen beide Faktoren (bis auf eine Einheit ±1) selbst dritte Potenzen sein (hier ist die Lücke: es ist nicht klar, ob im Ring R eine eindeutige Primfaktorzerlegung existiert). Daher folgt $y+\sqrt{-2}=\pm(r+s\sqrt{-2}\,)^3$, und dies führt auf die beiden Gleichungen $\pm y=r^3-6rs^2$ und $\pm1=s(3r^2-2s^2)$. Aus der letzten folgt $s=\pm1$, damit $r=\pm1$, und schließlich $y=\pm5$, also Fermat's Behauptung.

Diophantische Gleichungen der Form $E: y^2=x^3+ax+b$ mit $a,b\in\mathbb{Z}$ heißen, falls x^3+ax+b keine doppelte Nullstelle in $\mathbb{C}$ besitzt, *elliptische Kurven*. Die wesentliche Eigenschaft elliptischer Kurven ist folgende: betrachtet man alle rationalen Punkte auf einer elliptischen Kurve E (also alle Paare $(x,y)\in\mathbb{Q}\times\mathbb{Q}$, die der Gleichung E genügen), so kann man auf dieser Menge (wenn man noch ein 'künstliches' neutrales Element einführt) eine Addition so erklären, daß diese Menge zu einer abelschen Gruppe wird. Die Untersuchung dieser abelschen Gruppen ist erstaunlich interessant und ergiebig – einer der besten Algorithmen zum Auffinden 'kleiner' Faktoren (bis 40 Dezimalstellen) einer Zahl beruht auf Rechnungen in solchen Gruppen.

---

dieser Bücher trug er die berüchtigte Vermutung ein, daß die Gleichung $x^n+y^n=z^n$ für kein $n\geq3$ Lösungen in den natürlichen Zahlen hat, und behauptete sogar, dafür einen wunderbaren Beweis zu besitzen, den der Rand des Buches leider nicht fassen könne. Da er diese Behauptung nie öffentlich erhoben hat (sie wurde von seinem Sohn Samuel posthum publiziert) und Fermat nicht gerade an Bescheidenheit gelitten hat, nimmt man an, daß er kurz danach eine Lücke in seinem 'Beweis' gefunden hat. Die Fermatsche Vermutung wurde 1993 von A. Wiles bewiesen (mit einer Lücke, die 1995 von ihm und R. Taylor geschlossen wurde).

[5]Leonhard Euler (1707–1783) war wohl der produktivste Mathematiker aller Zeiten, was den Umfang seiner Publikationen angeht (fast die Hälfte seiner Arbeiten entstand nach seiner Erblindung!). Er wurde von Goldbach zum Studium der Fermatschen Werke animiert und war bis zum Auftritt von Lagrange auf der mathematischen Bühne der einzige Zahlentheoretiker seiner Zeit.

Es sei an dieser Stelle auch daran erinnert, daß der Beweis der Fermatschen Vermutung (unter anderem) durch Wiles auf der Theorie elliptischer Kurven beruht.

Wiles hat sein Resultat in drei Vorlesungen auf einer bereits heute legendären Tagung in Cambridge vorgestellt; der Rest der Welt wurde durch emails auf dem laufenden gehalten:

The following came from Karl today re Andrew's talk which may be of interest:

Hi. Andrew gave his first talk today. He did not announce a proof of Taniyama-Weil, but he is moving in that direction and he has two more lectures. He is still being very secretive about the final result.

My best guess is that he is going to prove that if E is an elliptic curve over Q and the Galois representation on the points of order 3 on E satisfies certain hypotheses, then E is modular. From what he has said it seems he will not prove the full conjecture. What I don't know now is whether this will apply to Frey's curves, and therefore say something about Fermat. I'll keep you posted.

Hier die Nachricht von Karl Rubin vom nächsten Tag:

No more real news in today's lecture. Andrew stated a general theorem about lifting Galois representations along the lines I suggested yesterday. It does not apply to all elliptic curves. But the punch line will come tomorrow.

I don't really know why he is doing it this way. It's clear he knows what he is going to say tomorrow. He is having people check pieces of it. But this is a truly massive piece of work that he has been working on for many years, and he seems confident of it. I'll let you know what happens tomorrow.

sowie eine von Ken Ribet:

from K.A.Ribet@newton.cam.ac.uk Tue Jun 22 08:23:55 1993

He's holding his fire until tomorrow. He gave a talk concentrating on the Kolyvagin-esque aspects of his argument. He finished with a theorem with a fair number of hypotheses, the conclusion of which was that all deformations (with certain properties) of a given modular mod p representation are themselves modular. He promised to talk about applications to elliptic curves tomorrow.

Und dann der Clou:

Wed, 23 Jun 93 10:50 BST
Andrew Wiles just announced, at the end of his 3rd lecture here, that he has proved Fermat's Last Theorem. He did this by proving that every semistable elliptic curve over Q (i.e. square-free conductor) is modular. The curves that Frey writes down, arising from counterexamples to Fermat, are semistable and by work of Ribet they cannot be modular, so this does it.

It's an amazing piece of work.

Karl

23 Jun 93 10:48 BST
Wiles announced that semistable elliptic curves over Q are modular. He sketched a beautiful argument using Hilbert irreducibility and various modular curves which reduces this statement to something which he announced yesterday. So in some sense his lecture yesterday represented the "hard work"; today's was more of a reward for our attention.

-ken

1.4 Quadratische Zahlkörper

Sei $m \in \mathbb{Z} \setminus \{0, 1\}$ eine ganze quadratfreie Zahl; dann heißt die Menge $k = \mathbb{Q}(\sqrt{m}\,) = \{a + b\sqrt{m} : a, b \in \mathbb{Q}\}$ ein *quadratischer Zahlkörper*. Man nennt k reell- bzw. imaginärquadratisch, je nachdem $m > 0$ oder $m < 0$ gilt. Daß k tatsächlich ein Körper ist, rechnet man leicht nach. Das Element $\alpha = a + b\sqrt{m} \in k$ ist Nullstelle des quadratischen Polynoms $P_\alpha(x) = x^2 - 2ax + a^2 - mb^2 \in \mathbb{Q}[x]$; dessen zweite Nullstelle $\alpha' = a - b\sqrt{m}$ nennt man die *Konjugierte* von α. Weiter heißt

$$\begin{array}{lcccll} \mathrm{N}\alpha & = & \alpha\alpha' & = a^2 - mb^2 & \text{die } \textit{Norm} \text{ von } \alpha, \\ \mathrm{Tr}\,\alpha & = & \alpha + \alpha' & = 2a & \text{die } \textit{Spur} \text{ von } \alpha, \text{ und} \\ \mathrm{disc}\,(\alpha) & = & (\alpha - \alpha')^2 & = 4mb^2 & \text{die } \textit{Diskriminante} \text{ von } \alpha. \end{array}$$

Proposition 1.1. *Für alle $\alpha, \beta \in k$ gilt $N(\alpha\beta) = N\alpha\, N\beta$ und $\mathrm{Tr}\,(\alpha + \beta) = \mathrm{Tr}\,\alpha + \mathrm{Tr}\,\beta$. Weiter ist $N\alpha = 0$ genau dann, wenn $\alpha = 0$ ist, und $\mathrm{disc}\,(\alpha) = 0$ genau dann, wenn $\alpha \in \mathbb{Q}$ ist.*

Beweis. Übung. □

Die Abbildung $\sigma : k \longrightarrow k : \alpha \longmapsto \sigma(\alpha) := \alpha'$ heißt auch der *nichttriviale Automorphismus* von $k/\mathbb{Q}$.

Übung. $\sigma : k \longrightarrow k$ ist ein Ringhomomorphismus, d.h. es gilt $\sigma(\alpha+\beta) = \sigma(\alpha)+\sigma(\beta)$ und $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$ für alle $\alpha, \beta \in k$. Zeige weiter, daß ein $\alpha \in k$ genau dann in $\mathbb{Q}$ liegt, wenn $\alpha = \sigma(\alpha)$ ist. Schließlich ist α genau dann ganz (Definition sh. unten), wenn auch $\sigma(\alpha)$ ganz ist. Wegen $\sigma \circ \sigma = \mathrm{id}$ (die identische Abbildung) ist $\{\mathrm{id}, \sigma\}$ eine Gruppe der Ordnung 2, die man die *Galoisgruppe*[6] von $k/\mathbb{Q}$ nennt und mit $\mathrm{Gal}\,(k/\mathbb{Q})$ bezeichnet.

Sind $k \subseteq K$ Körper, so kann man K als k-Vektorraum auffassen: die Vektoren sind die Elemente aus K (diese bilden bekanntlich eine additive Gruppe), die Skalare sind die Elemente von k, und die Skalarmultiplikation ist die gewöhnliche Multiplikation in K. Die Dimension von K als k-Vektorraum nennt man auch seinen *Grad* über k und schreibt $(K : k) := \dim_k K$. Selbstverständlich hat $\mathbb{Q}(\sqrt{m}\,)$ Grad 2 über $\mathbb{Q}$: eine Basis ist $\{1, \sqrt{m}\}$, denn jedes Element läßt sich eindeutig als $\mathbb{Q}$-Linearkombination dieser Elemente schreiben.

Unsere erste Aufgabe ist es, die "ganzen" Elemente in diesen quadratischen Zahlkörpern zu identifizieren. Die Lösung ist nicht ganz offensichtlich (es ist nämlich nicht immer $R = \mathbb{Z}[\sqrt{m}\,]$, wie man vielleicht naiv vermuten würde); man nennt vielmehr $\alpha \in k$ *ganz*, wenn $P_\alpha(x) \in \mathbb{Z}[x]$ ist, d.h. wenn das Polynom $P_\alpha(x)$ ganze Koeffizienten hat. Die Menge der ganzen Elemente von k nennt man $\mathcal{O}_k$. Nun gilt

Satz 1.2. *Es ist* $\mathcal{O}_k = \{a + b\sqrt{m} \;:\; a, b \in \mathbb{Z}\}$, *falls* $m \equiv 2, 3 \bmod 4$, *und* $\mathcal{O}_k = \{\frac{1}{2}(a + b\sqrt{m}\,) : a, b \in \mathbb{Z}, a \equiv b \bmod 2\}$, *falls* $m \equiv 1 \bmod 4$.

Beweis. Sei $\alpha = r + s\sqrt{m}$ ganz mit $r, s \in \mathbb{Q}$; damit sind $\mathrm{Tr}\,\alpha = 2r$ und $N\alpha = r^2 - ms^2$ ganz. Setzt man $2r \in \mathbb{Z}$ in die zweite Gleichung ein, so findet man, daß $4ms^2$ ganz ist. Da m quadratfrei ist, muß dann sogar $4s^2$, also schließlich $2s$ ganz sein (das geht so: sei $4s^2 = x^2/y^2$ mit teilerfremden $x, y \in \mathbb{Z}$; da $4ms^2$ ganz ist, folgt $y^2 \mid mx^2$; wegen $\mathrm{ggT}\,(x, y) = 1$ muß dann $y^2 \mid m$ sein, und die Quadratfreiheit von m zeigt $y = \pm 1$). Wir dürfen daher $2r = a$ und $2s = b$ schreiben mit $a, b \in \mathbb{Z}$. Jetzt nutzen wir noch einmal aus, daß $N\alpha = r^2 - ms^2$ ganz ist und finden, daß $a^2 - mb^2 \equiv 0 \bmod 4$ sein muß.
A) Ist $m \equiv 2 \bmod 4$, so folgt $2 \mid a$, $4 \mid a^2$ und $2 \mid b$, also $r, s \in \mathbb{Z}$: jede ganze Zahl hat die Form $r + s\sqrt{m}$ mit ganzen Zahlen $r, s \in \mathbb{Z}$.
B) Ist $m \equiv 3 \bmod 4$, so folgt $0 \equiv a^2 - mb^2 \equiv a^2 + b^2 \bmod 4$; dies geht nur, wenn a und b gerade sind, und wie eben folgt, daß r und s ganz sein müssen.

[6] Nach Évariste Galois (1811–1832), einem französischen Mathematiker, der nach einem Duell im Alter von 20 Jahren starb.

C) Ist schließlich $m \equiv 1 \bmod 4$, so erhalten wir $0 \equiv a^2 - mb^2 \equiv a^2 - b^2 \bmod 4$, was genau dann richtig ist, wenn $a \equiv b \bmod 2$ gilt. Also haben alle ganzen Zahlen hier die Form $\frac{1}{2}(a + b\sqrt{m})$, wo a und b entweder beide gerade oder beide ungerade sind. Daß diese Zahlen auch wirklich ganz sind, rechnet man einfach nach. □

Der Körper $k = \mathbb{Q}(\sqrt{m})$ besteht aus allen $\mathbb{Q}$-Linearkombinationen von 1 und $\sqrt{m}$. Gilt etwas ähnliches für $\mathcal{O}_k$? Man kann sich fragen, ob es ein $\omega \in \mathcal{O}_k$ gibt, sodaß $\mathcal{O}_k$ aus allen $\mathbb{Z}$-Linearkombinationen von 1 und ω besteht (in diesem Fall schreiben wir $\mathcal{O}_k = \mathbb{Z} \oplus \omega\mathbb{Z}$ und nennen $\{1, \omega\}$ eine *Ganzheitsbasis*). Dies ist in der Tat so:

Korollar 1.3. *Es gilt* $\mathcal{O}_k = \mathbb{Z} \oplus \omega\mathbb{Z}$ *mit*

$$\omega = \begin{cases} \sqrt{m}, & \text{falls } m \equiv 2, 3 \bmod 4; \\ \frac{1+\sqrt{m}}{2}, & \text{falls } m \equiv 1 \bmod 4. \end{cases}$$

Insbesondere ist $\mathcal{O}_k$ *ein Ring.*

Beweis. Nur im zweiten Fall ist wirklich etwas zu zeigen. Sei also $\alpha = \frac{1}{2}(a + b\sqrt{m})$ mit $a \equiv b \bmod 2$; setzt man $c = \frac{a-b}{2}$ und $d = b$, so ist $\alpha = c + d\omega$ mit $c, d \in \mathbb{Z}$. Die Umkehrung ist genauso trivial.

Daß$\mathcal{O}_k$ ein Ring ist, sieht man jetzt dadurch ein, daß man zeigt, daß Summe, Differenz und Produkt zweier Zahlen der Form $a + b\omega$ mit $a, b \in \mathbb{Z}$ wieder diese Form haben (wir hätten dies bereits im Anschluß an Satz 1.2 machen können, hätten dann aber wesentlich mehr rechnen müssen). Dazu ist im wesentlichen nur zu zeigen, daß das Produkt zweier Zahlen wieder diese Form hat, und das läuft auf den Nachweis hinaus, daß $\omega^2 = r + s\omega$ mit $r, s \in \mathbb{Z}$ gilt. Tatsächlich ist $\omega^2 = m = m + 0\omega$ für $m \equiv 2, 3 \bmod 4$, und $\omega^2 = \frac{1+m+2\sqrt{m}}{4} = \frac{m-1}{4} + \omega$ für $m \equiv 1 \bmod 4$. □

Übung. Ist $\{1, \omega\}$ eine Ganzheitsbasis von $\mathcal{O}_k$, dann auch $\{1, \omega - a\}$ für jedes $a \in \mathbb{Z}$.

Die Größe $d = \operatorname{disc} k := \left|\begin{smallmatrix} 1 & \omega \\ 1 & \omega' \end{smallmatrix}\right|^2 = (\omega - \omega')^2$ heißt die *Diskriminante* von k. Man findet $\operatorname{disc} k = 4m$, falls $m \equiv 2, 3 \bmod 4$, und $\operatorname{disc} k = m$, falls $m \equiv 1 \bmod 4$ ist. Die Diskriminante ist ein nützlicher Begriff, da sie Fallunterscheidungen zu vermeiden hilft. Beispielsweise ist $\{1, \frac{d+\sqrt{d}}{2}\}$ für jeden quadratischen Zahlkörper mit Diskriminante d eine Ganzheitsbasis.

Unser nächstes Ergebnis rechtfertigt im Nachhinein unsere Definition ganzer Zahlen in quadratischen Zahlkörpern:

Proposition 1.4. *Es gilt* $\mathcal{O}_k \cap \mathbb{Q} = \mathbb{Z}$.

Beweis. Wegen $\mathbb{Z} \subseteq \mathcal{O}_k \cap \mathbb{Q}$ ist nur die andere Inklusion zu zeigen. Sei also $\alpha \in \mathcal{O}_k$; dann gilt $\alpha = \frac{1}{2}(a + b\sqrt{m}\,)$ mit $a \equiv b \bmod 2$. Wenn $\alpha \in \mathbb{Q}$ sein soll, muß $b = 0$ sein; also ist a gerade, folglich $\alpha = \frac{a}{2} \in \mathbb{Z}$. □

Bemerkung. Man kann zeigen, daß $\mathcal{O}_k$ der maximale Teilring von k mit der Eigenschaft $\mathcal{O}_k \cap \mathbb{Q} = \mathbb{Z}$ ist; man nennt $\mathcal{O}_k$ deshalb oft die *Maximalordnung* von k. Ein Ring $\mathcal{O} \subset k$ heißt *Ordnung*, wenn $\mathbb{Z} \subsetneq \mathcal{O} \subseteq \mathcal{O}_k$ gilt. Mit Proposition 1.4 folgt daraus sofort, daß jede Ordnung $\mathcal{O}$ die Eigenschaft $\mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$ besitzt.

Bemerkung. Allgemein sind *algebraische Zahlen* per definitionem Nullstellen von Polynomen mit rationalen Koeffizienten; eine algebraische Zahl α heißt *ganz*, wenn α Nullstelle eines Polynoms $\in \mathbb{Z}[x]$ mit Leitkoeffizient 1 ist. Die algebraischen Zahlen bilden einen Körper, die ganzen algebraischen Zahlen einen Ring. Beispiele für nichtquadratische Zahlkörper sind der rein kubische Zahlkörper $\mathbb{Q}(\sqrt[3]{2}\,) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \;:\; a, b, c \in \mathbb{Q}\}$ oder der Kreisteilungskörper $\mathbb{Q}(\zeta_p)$, wo ζ_p eine Nullstelle von $\frac{x^p-1}{x-1} = 1 + x + \ldots + x^{p-1}$ und $p \geq 5$ prim ist.

Übung. Seien $k \subseteq K$ Körper; verifiziere, daß K ein k-Vektorraum ist. Sei $\alpha \in K$; zeige, daß $\mu_\alpha : \beta \longmapsto \alpha\beta$ (die Multiplikation mit α) eine k-lineare Abbildung des Vektorraums K in sich ist. Sei $n = \dim_k K$ endlich. Wähle eine k-Basis von K; dann läßt sich μ_α durch eine Matrix $M_\alpha \in M_n(k)$ beschreiben. Zeige, daß $N\alpha := \det M_\alpha$ und $\operatorname{Tr}\alpha := \operatorname{Tr} M_\alpha$ nicht von der Wahl der Basis abhängen, und daß für alle $\alpha, \beta \in K$ gilt: $N(\alpha\beta) = N(\alpha)N(\beta)$, $\operatorname{Tr}(\alpha + \beta) = \operatorname{Tr}(\alpha) + \operatorname{Tr}(\beta)$. Schließlich überzeuge man sich davon, daß N und Tr für quadratische Zahlkörper mit der bereits definierten Norm, bzw. Spur übereinstimmen.

Übung. Bestimme alle $m < 0$, für die der Ganzheitsring $\mathcal{O}_k$ von $k = \mathbb{Q}(\sqrt{m}\,)$ ein Element der Norm 2 oder 3 enthält.

Übung. Eine abelsche Gruppe M heißt G-Modul, wenn die Gruppe G auf ihr operiert, d.h. wenn es eine Abbildung $G \times M \longrightarrow M : (g, m) \longmapsto gm$ gibt mit den Eigenschaften 1. $g(m + m') = gm + gm'$; 2. $(gg')m = g(g'm)$; 3. $1m = m$ für alle $g, g' \in G$ und alle $m, m' \in M$. Zeige, daß die Galoisgruppe $G = \operatorname{Gal}(k/\mathbb{Q})$ auf den abelschen Gruppen k, $k^\times$ und $\mathcal{O}_k$ via $(\sigma, \alpha) \longmapsto \sigma(\alpha)$ operiert.

Übung. Eine Ganzheitsbasis der Form $\{\omega, \sigma(\omega)\}$ (das soll bedeuten: $\mathcal{O}_k = \omega\mathbb{Z} \oplus \sigma(\omega)\mathbb{Z}$) heißt *normale Ganzheitsbasis*. Zeige, daß $\mathcal{O}_k$ genau dann eine solche besitzt, wenn $m \equiv 1 \bmod 4$ gilt, d.h. wenn $\operatorname{disc} k$ ungerade ist.

An dieser Stelle sei die Lektüre des Artikels von Boas Erez über normale Ganzheitsbasen empfohlen:
B. Erez, *Representations of groups in algebraic number theory. An introduction* (Italienisch), Proc. Colloq. Locarno/Italy 1988–1989, Note Mat. Fis. 3, vol. 4, 41–65 (1990). Eine Übertragung ins Deutsche findet man auf
`http://www.rzuser.uni-heidelberg.de/~hb3/trans.html`

Zusammenfassung.

Wir haben die folgenden Begriffe eingeführt, die für den Rest der Vorlesung von grundlegender Bedeutung sind:

- quadratische Zahlkörper
- Norm, Spur und Diskriminante
- Galoisgruppe quadratischer Erweiterungen (von $\mathbb{Q}$)
- Ganzheitsring (Maximalordnung)
- Ganzheitsbasis

Kapitel 2

Teilbarkeit in Integritätsbereichen

Ein Ring R heißt *Integritätsbereich*, wenn er nullteilerfrei ist, d.h. wenn aus $ab = 0$ immer folgt, daß $a = 0$ oder $b = 0$ ist. Enthält R ein neutrales Element berzüglich der Multiplikation, so heißt er *Ring mit* 1. Im folgenden soll Ring immer kommutativer Integritätsbereich mit 1 bedeuten – andere Ringe kommen bei uns nicht vor. Unser Ziel ist die Definition von Einheiten, primen und irreduziblen Elementen (also eine Wiederholung von Stoff aus einer Algebra-Einführung), und die Untersuchung der Frage, in welchen quadratischen Zahlringen der Satz von der eindeutigen Primfaktorzerlegung gilt.

2.1 Einheiten, prime und irreduzible Elemente

Wir verallgemeinern den Begriff der Teilbarkeit ganzer Zahlen: Sind $a, b \in R$ gegeben, so sagt man, b teile a, wenn ein $c \in R$ existiert mit $a = bc$, und man schreibt $b \mid a$.

Übung. Seien $\alpha, \beta \in \mathcal{O}_k$. Dann gilt $\alpha \mid N\alpha$; ist weiter $\alpha \mid \beta$, so folgt $N\alpha \mid N\beta$ (sogar in $\mathbb{Z}$).

Allgemeiner schreibt man $a \equiv b \bmod mR$, wenn $m \mid (a - b)$ in R gilt. Für diese Kongruenzen gelten die bekannten Rechenregeln, deren Beweis wir einmal mehr als Übungsaufgabe stellen:

Übung. Sei R ein Ring; für alle $a, b, c, d, m, n \in R$ gilt dann
a) $a \equiv b \bmod m$, $c \equiv d \bmod m \Longrightarrow a + c \equiv b + d \bmod m$.
b) $a \equiv b \bmod m$, $c \equiv d \bmod m \Longrightarrow ac \equiv bd \bmod m$.
c) $n \mid m$ und $a \equiv b \bmod m \Longrightarrow a \equiv b \bmod n$.

Damit kann man zeigen:

Proposition 2.1. *Seien $a, b, m \in \mathbb{Z}$ und $a \equiv b \bmod m\mathcal{O}_k$; dann ist auch $a \equiv b \bmod m\mathbb{Z}$.*

Beweis. Es ist $a \equiv b \bmod m$ in $\mathcal{O}_k$ äquivalent zu $a - b = m\gamma$ für ein $\gamma \in \mathcal{O}_k$. Wegen $\gamma = \frac{a-b}{m}$ ist aber $\gamma \in \mathcal{O}_k \cap \mathbb{Q}$, und Proposition 1.4 zeigt $\gamma \in \mathbb{Z}$, also $a \equiv b \bmod m\mathbb{Z}$ in $\mathbb{Z}$. □

Übung. Zeige, daß aus $a \mid b$ in $\mathbb{Z}$ immer auch $a \mid b$ im Ring $\mathcal{O}_k$ ganzer Zahlen eines quadratischen Zahlkörpers k folgt.

Hilfreich beim Rechnen mit quadratischen Irrationalitäten ist auch folgendes Resultat:

Proposition 2.2. *Sei $\{1, \omega\}$ eine Ganzheitsbasis eines quadratischen Zahlkörpers. Für ein $m \in \mathbb{Z}$ ist dann $m \mid (a + b\omega)$ in $\mathcal{O}_k$ genau dann, wenn $m \mid a$ und $m \mid b$ in $\mathbb{Z}$ gelten.*

Beweis. Übung. □

Teiler der 1 heißen *Einheiten* des Rings; die Menge $R^\times$ aller Einheiten von R ist eine Gruppe bezüglich der Ringmultiplikation und wird die *Einheitengruppe* von R genannt.

Übung. Zeige, daß die Einheiten eines Rings eine Gruppe bilden.

Ist $R = K$ ein Körper, so gilt $R^\times = K^\times = K \setminus \{0\}$. Weitere Beispiele von Einheitengruppen sind

R	$\mathbb{Z}$	$\mathbb{Z}[x]$	$\mathbb{Q}[x]$	$\mathbb{Z}[\sqrt{-2}\,]$	$\mathbb{Z}[i]$	$\mathbb{Z}[\sqrt{2}\,]$
$R^\times$	$\{-1, +1\}$	$\{-1, +1\}$	$\mathbb{Q}^\times$	$\{-1, +1\}$	$\{\pm 1, \pm i\}$	$\pm(1 + \sqrt{2}\,)^n$

Für quadratische Zahlkörper k ist das Erkennen von Einheiten relativ leicht:

Proposition 2.3. *Ein Element $\varepsilon \in \mathcal{O}_k$ ist genau dann eine Einheit, wenn $N\varepsilon = \pm 1$ ist.*

Beweis. Sei $\varepsilon \in \mathcal{O}_k$ eine Einheit; dann ist $\varepsilon\eta = 1$ für ein $\eta \in \mathcal{O}_k$, und Normenbildung liefert $N\varepsilon N\eta = N(1) = 1$. Da $N\varepsilon$ und $N\eta$ ganze Zahlen sind, deren Produkt 1 ist, muß entweder $N\varepsilon = N\eta = 1$ oder $N\varepsilon = N\eta = -1$ sein.

Ist umgekehrt $N\varepsilon = 1$, so zeigt $\varepsilon\varepsilon' = 1$, daß ε eine Einheit ist. □

Insbesondere zeigt dieses Ergebnis, daß die Norm ein Homomorphismus $E_k \longrightarrow E_{\mathbb{Z}} = \{\pm 1\}$ ist.

Übung. Sei $\mathcal{O}_k$ Ring ganzer Zahlen in einem quadratischen Zahlkörper, und sei $E_k = \mathcal{O}_k^\times$ seine Einheitengruppe. Zeige, daß E_k ein $\mathrm{Gal}\,(k/\mathbb{Q})$-Modul ist.

Übung. Zeige, daß im Körper $\mathbb{Q}[i]$ der Gaußschen Zahlen $N\alpha = 1$ gilt für $\alpha = \frac{1+2i}{1-2i}$, und daß α keine Einheit in $\mathbb{Z}[i]$ ist.

Die Einheitengruppen von imaginärquadratischen Zahlkörpern sind jetzt ganz einfach zu bestimmen:

Satz 2.4. *Sei $m < 0$ quadratfrei, $k = \mathbb{Q}(\sqrt{m}\,)$, und $R = \mathcal{O}_k$ der Ring ganzer Zahlen in k. Dann gilt*

$$R^\times = \begin{cases} \langle i \rangle, & \text{falls } m = -1; \\ \langle -\rho \rangle, & \text{falls } m = -3; \\ \langle -1 \rangle, & \text{sonst.} \end{cases}$$

Hier bezeichnet $i = \sqrt{-1}$ eine vierte und $\rho = \frac{1}{2}(-1 + \sqrt{-3}\,)$ eine dritte Einheitswurzel.

Beweis. Sei zuerst $m \equiv 1, 2 \bmod 4$ und $\varepsilon = a + b\sqrt{-m}$ eine Einheit. Dann folgt $1 = N\varepsilon = a^2 + mb^2$ (der Fall $N\varepsilon = -1$ kann wegen $m > 0$ nicht eintreten). Für $m > 1$ kann dies nur für $a = \pm 1$, $b = 0$ erfüllt sein, also für $\varepsilon = \pm 1$ (und ± 1 sind natürlich Einheiten). Im Falle $m = 1$ dagegen gibt es vier Möglichkeiten: erstens $a = \pm 1$, $b = 0$, und zweitens $a = 0$, $b = \pm 1$. Alle diese Einheiten sind Potenzen von $i = \sqrt{-1}$.

Ist $-m \equiv 1 \bmod 4$, so setzen wir $\varepsilon = \frac{1}{2}(a + b\sqrt{-m}\,)$ und finden $4 = a^2 + mb^2$ als notwendige und hinreichende Bedingung dafür, daß ε Einheit ist. Für $m > 3$ gibt es wieder nur die trivialen Lösungen, die $\varepsilon = \pm 1$ entsprechen; im Falle $m = 3$ dagegen erhalten wir die Einheiten

$$\pm 1, \quad \pm\frac{-1 + \sqrt{-3}}{2}, \quad \pm\frac{1 + \sqrt{-3}}{2}.$$

Setzen wir $\rho = \frac{-1+\sqrt{-3}}{2}$ (dies ist eine dritte Einheitswurzel wegen $\rho^3 = 1$), so wird E_k von $-\rho$ (einer sechsten Einheitswurzel) erzeugt. □

Für reell-quadratische Zahlkörper läuft die Bestimmung der Einheitengruppe auf die Lösung der *Pellschen Gleichung*[1] $t^2 - mu^2 = \pm 4$ hinaus; daß diese für Nichtquadrate $m \geq 2$ immer lösbar ist, werden wir etwas später beweisen. An dieser Stelle begnügen wir uns mit der Bemerkung, daß $\varepsilon = 1+\sqrt{2}$ wirklich eine Einheit unendlicher Ordnung ist: aus $(1 + \sqrt{2})^n = \pm 1$ folgt nämlich $1 = |\pm 1| = |1 + \sqrt{2}|^n > 1$ für alle $n \geq 1$, und entsprechend $1 = |\pm 1| = |1 + \sqrt{2}|^n < 1$ für alle $n \leq -1$. Insbesondere ist $\mathbb{Z}[\sqrt{2}]$ ein Ring mit unendlich vielen Einheiten.

Elemente $a, b \in R$ heißen *assoziiert*, wenn es eine Einheit $e \in R^\times$ gibt mit $a = be$; man schreibt $a \sim b$ und rechnet leicht nach, daß dies eine Äquivalenzrelation auf R definiert.

Ein Element $a \in R \setminus R^\times$ heißt *unzerlegbar* oder *irreduzibel*, wenn a nur triviale Teiler hat, also Einheiten und Assoziierte, oder genauer: wenn aus $a = bc$ immer folgt, daß b oder c eine Einheit ist. Dagegen heißt $p \in R \setminus R^\times$ *prim*, wenn aus $p \mid ab$ immer folgt, daß $p \mid a$ oder $p \mid b$ gilt. Man beachte, daß Einheiten per definitionem weder prim noch irreduzibel sind.

Proposition 2.5. *Primelemente sind irreduzibel.*

Beweis. Sei a prim. Wäre a zerlegbar, so gäbe es $b, c \in R \setminus R^\times$ mit $a = bc$. Jetzt ist $a \mid bc$; wäre $a \mid b$, also $b = ad$ für ein $d \in R$, so folgte $a = acd$, also $1 = cd$, und c ist eine Einheit im Widerspruch zur Voraussetzung. □

Vom Ring $R = \mathbb{Z}$ wissen wir, daß irreduzible Elemente auch immer prim sind. Im allgemeinen ist das aber nicht der Fall. Betrachten wir z.B. den Ring $R = \mathbb{Z}[\sqrt{-5}]$. Hierin ist 2 irreduzibel. Dies beweist man am einfachsten so: Wäre 2 reduzibel, also $2 = \alpha\beta$ mit $\alpha, \beta \in R$, so müßte $4 = N(2) = N\alpha N\beta$ sein. Die kleinsten Normen in R sind $N(\pm 1) = 1$, $N(\pm 2) = 4$, und $N(\pm\sqrt{-5}) = 5$. Die Gleichung $4 = N\alpha N\beta$ kann also nur dann erfüllt sein, wenn $\alpha = \pm 2$ und $\beta = \pm 1$ ist oder umgekehrt.

[1] John Pell (1611–1685), englischer Mathematiker. Es wird oft gesagt, daß der Name 'Pellsche' Gleichung auf einen Fehler Eulers zurückgehe, der ihr diesen Namen verliehen hat, obwohl Pell nichts damit zu tun gehabt habe. Allerdings hat man die Gleichung in jüngster Zeit in einem Buch (Teutsche Algebra) des Schweizer Mathematikers Johann Rahn (1622–1676) entdeckt, an dem Pell während seines Aufenthalts in Zürich mitgearbeitet hat.

Andererseits ist 2 nicht prim in R: das Produkt $6 = (1+\sqrt{-5})(1-\sqrt{-5})$ ist nämlich durch 2 teilbar, während 2 keinen der beiden Faktoren teilt (denn $(1+\sqrt{-5})/2$ ist kein Element von $R = \mathbb{Z}[\sqrt{-5}]$).

Bemerkung. Nimmt man $\omega = \frac{1}{2}(1+\sqrt{-5})$ zu R hinzu, rechnet also im Ring $S = \mathbb{Z}[\omega]$, so funktioniert dieser Schluß nicht mehr. Tatsächlich ist S ein ZPE-Ring (sh. unten), hat aber wegen $S = \{2^{-n}(a+b\sqrt{-5}) : a, b \in \mathbb{Z}, n \in \mathbb{N}\}$ die unangenehme Eigenschaft, daß $S \cap \mathbb{Q} = \mathbb{Z}[\frac{1}{2}]$ ist (mit anderen Worten: S ist keine Ordnung).

Übung. Ebenso wie das Beispiel $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$ behandle man $2 \cdot 3 = -\sqrt{-6} \cdot \sqrt{-6}$ in $\mathbb{Z}[\sqrt{-6}]$ und $2 \cdot 3 = \sqrt{6} \cdot \sqrt{6}$ in $\mathbb{Z}[\sqrt{6}]$.

Übung. Man zeige, daß Elemente $\pi \in \mathcal{O}_k$ irreduzibel sind, falls $N\pi$ eine rationale Primzahl ist. (Tatsächlich sind solche Elemente sogar prim, aber ein direkter Beweis ist weitaus weniger offensichtlich.)

Übung. Sei $k = \mathbb{Q}(\sqrt{m})$; welche der rationalen Primzahlen $p \in \{2, 3, 5\}$ sind in $\mathcal{O}_k$ mit $m \in \{-5, -3, -2, -1, 2, 3, 5\}$ irreduzibel, welche nicht?

2.2 ZPE-Ringe

ZPE-Ringe sind solche, in denen der Satz von der eindeutigen Zerlegbarkeit in Primelemente gilt. Genauer fordern wir

Z–1 Jede Nichteinheit $\neq 0$ ist Produkt endlich vieler irreduzibler Elemente;

Z–2 irreduzible Elemente sind prim;

Z–3 Sei $a \in R \setminus \{0\}$ und $a = ep_1 \cdots p_s = e'q_1 \cdots q_t$, wo $e, e' \in R^\times$ Einheiten und die p_j und q_j irreduzible Elemente in R sind. Dann ist $s = t$, und man kann die q_j so umordnen, daß $p_i \sim q_i$ für $i = 1, \ldots, s$ gilt.

Man betrachte den Ring A, der entsteht, wenn man zu $\mathbb{Z}$ alle 2^n-ten Wurzeln der 2 adjungiert, also $A = \mathbb{Z}[\sqrt{2}, \sqrt[4]{2}, \sqrt[8]{2}, \ldots]$. In diesem Ring besitzt 2 keine Zerlegung in irreduzible Elemente: es ist ja $2 = \sqrt{2}\sqrt{2} = \sqrt[4]{2}\,\sqrt[4]{2}\,\sqrt[4]{2}\,\sqrt[4]{2} = \ldots$ usw. Die erste Forderung ist also durchaus sinnvoll. Was Z–2 und Z–3 angeht, so gilt:

Proposition 2.6. *Ist R ein Ring mit Z–1, so sind Z–2 und Z–3 äquivalent.*

Beweis. Z–2 $\Longrightarrow$ Z–3: Da die p_i irreduzibel sind, sind sie nach Voraussetzung prim; insbesondere teilt p_1 eines der q_j, sagen wir q_1. Da q_1 irreduzibel ist, muß $p_1 \sim q_1$ sein. Da R Integritätsbereich ist, kann man p_1 kürzen und erhält $e_1 p_2 \cdots p_s = e_1' q_2 \cdots q_t$. Induktion liefert die Behauptung.

Z–3 $\Longrightarrow$ Z–2: Sei a irreduzibel und $a \mid xy$, wo $x, y \in R$. Dann gibt es ein $b \in R$ mit $ab = xy$. Wegen Z–3 ist die Zerlegung in irreduzible Elemente bis auf Reihenfolge und Einheiten eindeutig; also muß eine Assoziierte des irreduziblen a in der Faktorisierung von x oder y vorkommen, und es folgt $a \mid x$ oder $a \mid y$. Also ist a prim. □

Da $1+\sqrt{-5}$ in $R = \mathbb{Z}[\sqrt{-5}\,]$ zwar irreduzibel, aber nicht prim ist, kann R kein ZPE-Ring sein. Diese Tatsache beweist auch, daß die eindeutige Primfaktorzerlegung in $\mathbb{Z}$, die vielen Neulingen in der elementaren Zahlentheorie selbstverständlich vorkommt, wirklich bewiesen werden muß. Die Hauptleistung der Griechen, die sich erstmals an einem solchen Beweis versucht haben, besteht daher wohl nicht im Beweis selbst, sondern in der Einsicht, daß es eines solchen überhaupt bedarf! Man schaue sich in dieser Hinsicht auch das vorzügliche Büchlein *Von Zahlen und Figuren*, [Springer Verlag, 173 S. (1933), 164 S. (1968)] von Rademacher und Töplitz an.

In beliebigen Ringen heißt $d \in R$ ein *größter gemeinsamer Teiler* von $a, b \in R$ (wir schreiben $d \sim \mathrm{ggT}\,(a, b)$), wenn gilt:

G–1 $d \mid a$ und $d \mid b$;

G–2 gilt $c \mid a$ und $c \mid b$ für ein $c \in R$, dann ist $c \mid d$.

In ZPE-Ringen kann man größte gemeinsame Teiler zumindest theoretisch leicht hinschreiben: sind nämlich $a = u \prod p^{\alpha_p}$ und $b = v \prod p^{\beta_p}$ die Primfaktorzerlegungen von a und b (mit Einheiten $u, v \in R^\times$), dann rechnet man sofort nach, daß $d = \prod p^{\min(\alpha_p, \beta_p)}$ ein größter gemeinsamer Teiler von a und b ist. Der Nachteil dieser Methode, den ggT zweier Zahlen zu berechnen, wird schon für $R = \mathbb{Z}$ sichtbar: man muß dazu die beiden Zahlen faktorisieren, und das ist ein *schwieriges* Problem.

Zwei Elemente a, b eines ZPE-Rings R nennt man *teilerfremd*, wenn ihr größter gemeinsamer Teiler eine Einheit ist. Man beachte, daß wir hier die ZPE-Eigenschaft voraussetzen! Der Grund dafür wird erst später klar werden: nur unter dieser Zusatzvoraussetzung ist nämlich das von d erzeugte Hauptideal (d) gleich dem Ideal (a, b).

Proposition 2.7. *Ist R ein ZPE-Ring, sind $a, b \in R$ teilerfremd, und gilt $ab = ex^n$ ($n \geq 2$) für ein $e \in R^\times$ und ein $x \in R$, dann gibt es Einheiten $e_1, e_2 \in R^\times$ und $c, d \in R$ mit $a = e_1 c^n$ und $b = e_2 d^n$.*

Beweis. Durch Induktion über die Anzahl der Primfaktoren von a. Ist a eine Einheit, so folgt die Behauptung mit $c = 1$, $d = x$ $e_1 = a$ und $e_2 = ea^{-1}$.

Sei die Behauptung bewiesen für alle $a \in R$ mit höchstens t verschiedenen Primfaktoren. Sei dann p ein Primelement mit $p \mid a$; genauer nehmen wir an, es sei $p^h \parallel a$. Wegen $p^h \parallel x^n$ (hier benutzen wir die Teilerfremdheit von a und b) muß $h = nk$ für ein $k \in \mathbb{N}$ gelten und $p^k \parallel x$ sein. Damit ist $a = p^h a_1$, $x = p^k x_1$ und $a_1 b = e x_1^n$. Nach Induktionsvoraussetzung ist $a_1 = e_1 c^n$ und $b = e_2 d^n$, und jetzt folgt die Behauptung wegen $a = e_1 (cp^k)^n$. □

Korollar 2.8. *Ist R ein ZPE-Ring, ist $\mathrm{ggT}\,(a, b) = p$ für $a, b, p \in R$ mit p prim, und gilt $ab = ex^n$ ($n \geq 2$) für ein $e \in R^\times$ und ein $x \in R$, dann gibt es Einheiten $e_1, e_2 \in R^\times$ und $c, d \in R$ mit $a = e_1 p c^n$ und $b = e_2 p^{n-1} d^n$ (gegebenenfalls muß man dazu a und b vertauschen).*

Beweis. Übung. Man versuche, auf $a = pa_1$ und $b = p^{n-1} b_1$ zu kommen und wende dann Proposition 2.7 auf a_1 und b_1 an. □

Übung Man bestimme alle ganzen Punkte auf der elliptischen Kurve $4y^2 = x^3 + 1$ (d.h. alle Paare $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, die dieser Gleichung genügen).

2.3 Hauptidealringe

Hauptidealringe werden bei uns vorläufig keine große Rolle spielen; sie kommen eigentlich bloß als Hilfsobjekt in der Inklusionskette

$$\text{Euklidische Ringe} \subset \text{Hauptidealringe} \subset \text{ZPE-Ringe}$$

vor, mit der wir uns ZPE-Ringe verschaffen werden. Beide Inklusionen werden übrigens echt sein; jedoch kann man zeigen, daß für Ganzheitsringe quadratischer (sogar beliebiger) Zahlkörper die zweite Inklusion eine Gleichheit ist.

Zuerst jedoch müssen wir klären, was ein Hauptidealring ist. Sei dazu R ein Ring; ein Teilring I heißt *Ideal*, wenn $I \cdot R \subseteq I$ gilt, d.h. wenn I bezüglich Multiplikation mit Ringelementen abgeschlossen ist. Man beachte, daß für

die Aussage "I ist Teilring" nur die schwächere Bedingung $I \cdot I \subset I$ erfüllt zu sein braucht. Dennoch gilt z.B. in $R = \mathbb{Z}$, daß *jeder* Teilring auch Ideal ist; daß dies nicht immer so ist, zeigt folgendes Beispiel: die Menge

$$T = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in \mathbb{Z} \right\}$$

ist Teilring von $R = M_2(\mathbb{Z})$, dem Ring aller 2×2-Matrizen mit Einträgen aus $\mathbb{Z}$ (eigentlich kein Ring in unserem Sinne, da er weder kommutativ, noch nullteilerfrei ist). Allerdings ist T kein Ideal: denn dazu müßte das Produkt der Einheitsmatrix (diese liegt sicher in T) mit einer unteren Dreiecksmatrix wie $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ (diese liegt sicher in R) wieder in T liegen.

Übung. Sei k ein quadratischer Zahlkörper. Zeige, daß $\mathbb{Z}$ ein Unterring von $\mathcal{O}_k$, aber kein Ideal in $\mathcal{O}_k$ ist.

Ideale gibt es wie Sand am Meer: sind $a_1, \ldots, a_n \in R$ gegeben, so ist die Menge aller R-Linearkombinationen

$$I = (a_1, \ldots, a_n) := \{a_1 r_1 + \ldots + a_n r_n : r_j \in R\}$$

dieser Elemente ein Ideal, das man das von $a_1, \ldots, a_n$ erzeugte Ideal nennt. Daß I Teilring ist, ist klar; nachzuweisen bleibt die Idealeigenschaft $IR \subseteq I$. Das ist aber ebenfalls klar: mit $a = a_1 r_1 + \ldots + a_n r_n \in I$ liegt nämlich sicher auch $ar = a_1(r_1 r) + \ldots + a_n(r_n r)$ in I. Ist $a_1, a_2, \ldots$ eine Folge von Ringelementen, so definiert man $I = (a_1, a_2, \ldots)$ als die Menge aller *endlichen* R-Linearkombinationen der a_i.

Bemerkung. Sand am Meer ist etwas übertrieben, da nicht gesagt ist, daß all diese Ideale auch wirklich verschieden sind. Ist beispielsweise $R = K$ ein Körper, dann gibt es nur zwei Ideale: das Nullideal (0) und das Einsideal $(1) = R$.

Ideale, die von einem Element a erzeugt werden, heißen *Hauptideale*. Diese haben die Gestalt $I = (a) = \{ar : r \in R\}$ und werden manchmal auch $I = aR$ geschrieben; sie bestehen offenbar aus allen Vielfachen von a.

Ein Ring, in dem *jedes* Ideal ein Hauptideal ist, heißt *Hauptidealring*. Bekanntlich ist $\mathbb{Z}$ ein solcher: das Ideal $(a_1, \ldots, a_n)$ wird nämlich von $d = \mathrm{ggT}\,(a_1, \ldots, a_n)$ erzeugt. Ein bekanntes Beispiel für einen ZPE-Ring, der kein Hauptidealring ist, ist der Polynomring $\mathbb{C}[x, y]$ in zwei Variablen: hier ist (x, y) kein Hauptideal, wie man leicht nachprüft.

Bemerkung. Daß $\mathbb{C}[x,y]$ ein ZPE-Ring ist, folgt dagegen aus einem bekannten Satz der Algebra: ist R ein ZPE-Ring, dann auch der Polynomring $R[y]$. Da $R = \mathbb{C}[x]$ ein ZPE-Ring ist (R ist sogar euklidisch), ergibt sich die Behauptung damit sofort.

Übung. Ist $(2,x)$ in $\mathbb{Z}[x]$ ein Hauptideal? In $\mathbb{Q}[X]$?

Auch aus der Zerlegung $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ können wir uns ein Ideal in $R = \mathbb{Z}[\sqrt{-5}]$ basteln, das kein Hauptideal ist: sei nämlich $I = (2, 1+\sqrt{-5})$. Wäre $I = (\alpha)$ für ein $\alpha \in R$, so folgte $\alpha \mid 2$ und $\alpha \mid (1+\sqrt{-5})$; da aber 2 und $(1+\sqrt{-5})$ in R beide irreduzibel sind, muß α eine Einheit sein, also $I = (1) = R$. Dann läßt sich aber 1 als R-Linearkombination $1 = 2\alpha + (1+\sqrt{-5})\beta$ mit $\alpha, \beta \in R$ darstellen; Multiplikation mit $1-\sqrt{-5}$ liefert $1-\sqrt{-5} = 2\alpha(1-\sqrt{-5}) + 6\beta$, und jetzt ist die rechte Seite durch 2 teilbar, die linke aber nicht.

Übung. Finde ein Ideal in $\mathbb{Z}[\sqrt{-6}]$, welches kein Hauptideal ist.

Satz 2.9. *Hauptidealringe sind ZPE-Ringe.*

Beweis. Angenommen, Z–1 wäre nicht erfüllt. Dann gibt es ein $a_1 \in R$, das sich nicht als Produkt irreduzibler Elemente schreiben läßt (insbesondere ist a_1 also nicht irreduzibel). Es ist also $a_1 = a_2 b_2$ (mit Nichteinheiten $a_2, b_2 \in R \setminus R^\times$), wobei a_2 (ohne Einschränkung) wieder kein Produkt irreduzibler Elemente ist. Dies gibt $a_2 = a_3 b_3$ usw., und wir erhalten eine Folge von Zahlen $a_1, a_2, a_3 \ldots \in R$ mit $a_2 \mid a_1$, $a_3 \mid a_2$, ..., wobei a_i und a_{i+1} nicht assoziiert sind.

Sei nun $I = (a_1, a_2, \ldots)$ das von den a_i erzeugte Ideal. Nach Voraussetzung gibt es ein $a \in R$ mit $I = (a)$, und folglich existieren $m \in \mathbb{N}$ und $r_i \in R$ mit $a = r_1 a_1 + \ldots + r_m a_m$ (selbstverständlich werden i.A. einige der r_i verschwinden). Wegen $a_m \mid a_{m-1} \mid \cdots \mid a_1$ ist $a_m \mid a$. Wegen $a_{m+1} \in (a)$ gibt es ein $r \in R$ mit $a_m = ar$, d.h. es ist $a \mid a_{m+1}$. Nach Konstruktion der a_i ist aber $a_{m+1} \mid a_m$, folglich sind a_m und a_{m+1} assoziiert im Widerspruch zur Konstruktion der a_i.

Jetzt zeigen wir, daß irreduzible Elemente prim sind. Sei dazu $a \in R$ irreduzibel, und seien $x, y \in R$ gegeben mit $a \mid xy$ und $a \nmid x$: wir müssen dann $a \mid y$ beweisen. Nun ist $(a,x) = (d)$ für ein $d \in R$; also ist $d \mid a$ und $d \mid x$. Wäre $d \sim a$, so folgte $a \mid x$ im Widerspruch zur Voraussetzung. Da a irreduzibel ist, muß d eine Einheit sein. Also ist $d^{-1} \in R$ und damit $1 = d^{-1}d \in (d) = (a,x)$, d.h. es existieren $m, n \in R$ mit $1 = ma + nx$.

Multiplikation mit y gibt $y = may + nxy$, und wegen $a \mid xy$ folgt $a \mid y$. Das war zu zeigen. □

Eine wichtige Eigenschaft von Hauptidealringen ist die Tatsache, daß sie 'bezoutsch'[2] sind: ein Ring heißt *bezoutsch*, wenn zu $a, b \in R$ immer ein $d \sim \mathrm{ggT}\,(a, b)$ existiert und darüberhinaus $d = ar + bs$ eine R-Linearkombination von a und b ist. Hauptidealringe sind immer bezoutsch: zu $a, b \in R$ bilde man nämlich das Ideal (a, b); da R Hauptidealring ist, gilt $(a, b) = (d)$ für ein $d \in R$. Wir behaupten, daß $d \sim \mathrm{ggT}\,(a, b)$ gilt. Zum einen gibt es aber wegen $a \in (d)$ ein Element $t \in R$ mit $a = dt$; dies zeigt $d \mid a$, und analog folgt $d \mid b$, d.h. d ist wirklich ein gemeinsamer Teiler von a und b. Zum andern existieren wegen $d \in (a, b)$ Elemente $r, s \in R$ mit $d = ar + bs$; ist nun e irgendein gemeinsamer Teiler von a und b, so teilt e auch $ar + bs = d$, d.h. d ist in der Tat ein größter gemeinsamer Teiler. Die Bezout-Eigenschaft haben wir dabei schon mitbewiesen.

Übung. Sei R ein Ring, der $\mathbb{Z}$ enthält (z.B. $R = \mathcal{O}_k$). Sind $a, b \in \mathbb{Z}$ teilerfremd in $\mathbb{Z}$, dann auch in R. (Hinweis: Bezout).

2.4 Euklidische Ringe

Um in einem Ring R die ZPE-Eigenschaft nachzuweisen, werden wir uns zu anfang ausschließlich des euklidischen Algorithmus bedienen. Eine Funktion $f : R \longrightarrow \mathbb{N}_0$ heißt *euklidische Funktion*, wenn gilt:

E–1 $f(a) = 0$ genau dann, wenn $a = 0$;

E–2 zu $a \in R$ und $b \in R \setminus \{0\}$ gibt es ein $c \in R$ mit $f(a - bc) < f(b)$.

Existiert eine euklidische Funktion für R, so heißt R *euklidisch*.

Offenbar ist die Betragsfunktion $|\cdot|$ eine euklidische Funktion auf $\mathbb{Z}$ (**Übung!**. Ist K ein Körper, so ist $f(a) = 2^{\deg a}$ eine euklidische Funktion auf $R = K[x]$ (und $g(a) = 3^{\deg a}$ eine andere). Hierbei bezeichnet $\deg a$ den Grad eines Polynoms $a \in K[x]$ (beachte, daß das Nullpolynom per definitionem Grad $-\infty$ besitzt und folglich $2^{\deg 0} = 2^{-\infty} = 0$ ist wie gewünscht).

Satz 2.10. *Euklidische Ringe sind Hauptidealringe.*

[2] Étienne Bezout (1730–1783), französischer Mathematiker und Lehrbuchautor; was er mit dieser Eigenschaft zu tun hat, ist nicht klar.

Beweis. Sei f eine euklidische Funktion auf R und $A \subseteq R$ ein Ideal in R. Unter den Elementen in $A \setminus \{0\}$ gibt es eines (sagen wir a), für welches f minimal wird (denn f nimmt nur natürliche Zahlen als Werte an). Wir behaupten, daß $A = (a)$ ist. Wegen $a \in A$ ist sicher $(a) \subseteq A$, sodaß nur die andere Inklusion zu zeigen ist. Sei daher $b \in A$ beliebig; wegen E–2 existiert ein $q \in R$ mit $f(b - aq) < f(a)$; da f auf $A \setminus \{0\}$ minimal gewählt wurde, muß $f(b-aq) = 0$ sein, nach E–2 also $b = aq$. Also ist $b \in (a)$, und, da $b \in A$ beliebig war, auch $A \subseteq (a)$. □

Insbesondere haben euklidische Ringe R die Bezout-Eigenschaft, d.h. $d \sim \mathrm{ggT}\,(a,b)$ läßt sich als $d = ar + bs$ mit $r, s \in R$ schreiben. Was das Leben in euklidischen Ringen so angenehm macht, ist die Tatsache, daß man bei gegebenem $a, b \in R$ sowohl $d \sim \mathrm{ggT}\,(a,b)$, als auch die Bezout-Elemente r und s mit dem euklidischen Algorithmus *berechnen* kann.

Dazu seien $a, b \in R \setminus \{0\}$; wenden wir den Euklidischen Algorithmus an, so finden wir $q_0, r_1 \in R$ mit $a - bq_0 = r_1$ und $f(r_1) < f(b)$. Ebenso existieren $q_1, r_2 \in R$ mit $b - r_1 q_1 = r_2$ und $f(r_2) < f(r_1)$ (falls nicht schon $r_1 = 0$ ist; in diesem Fall ist $a = bq$ und $d = b = 0a + 1b$, also alles trivial). So fahren wir fort und finden eine Kette

$$\begin{array}{rcll} a - bq_0 & = & r_1 & f(r_1) < f(b), \\ b - r_1 q_1 & = & r_2 & f(r_2) < f(r_1), \\ r_1 - r_2 q_2 & = & r_3 & f(r_3) < f(r_2), \\ & \vdots & & \vdots \\ r_{n-2} - r_{n-1} q_{n-1} & = & r_n & f(r_n) < f(r_{n-1}) \\ r_{n-1} - r_n q_n & = & r_{n+1} & f(r_{n+1}) < f(r_n). \end{array}$$

Nun können die natürlichen Zahlen $f(r_j)$ nicht beliebig klein werden; folglich gibt es ein $n \in \mathbb{N}$ mit $r_{n+1} = 0$. Wir behaupten, daß dann $r_n \sim \mathrm{ggT}\,(a,b)$ gilt. Aus der letzten Zeile folgt $r_n \mid r_{n-1}$, dann ergibt die vorletzte $r_n \mid r_{n-2}$, und so hangelt man sich durch bis $r_n \mid r_1$, $r_n \mid b$ und $r_n \mid a$. Also ist r_n ein gemeinsamer Teiler von a und b. Ist umgekehrt d irgendein gemeinsamer Teiler von a und b, so liefert die erste Zeile $d \mid r_1$, die zweite $d \mid r_2$, usw., und schließlich $d \mid r_n$, mit anderen Worten: r_n ist ein größter gemeinsamer Teiler.

Die Bezout-Elemente $r, s \in R$ erhält man so: wir starten mit $r_n = r_{n-2} - r_{n-1} q_{n-1}$ und ersetzen das r_j mit dem größten vorkommenden Index durch die Linearkombination der vorhergehenden Zeile, also hier r_{n-1} durch $r_{n-1} = r_{n-3} - r_{n-2} q_{n-2}$. Damit haben wir r_n als Linearkombination von r_{n-2} und

r_{n-3}. Jetzt ersetzen wir r_{n-2} durch $r_{n-2} = r_{n-4} - r_{n-3}q_{n-3}$ usw., bis wir schließlich r_n als R-Linearkombination von a und b dargestellt haben.

Zur Berechnung dieser Bezout-Elemente per Computer gibt es eine (bezüglich Code und Rechenzeit) sparsame Implementierung, die unter dem Namen *Berlekamp-Algorithmus* bekannt ist. Das ganze funktioniert wie folgt: gegeben seien $a, b \in R$, wo R euklidisch bezüglich f ist; (Initialisierung) setze $a = r_{-2}$, $b = r_{-1}$, sowie $p_{-2} = 0$, $p_{-1} = 1$ und $q_{-1} = 0$. Dann berechne man induktiv A_k, r_k, p_k, q_k für $k \geq 0$ via

$$\begin{aligned} r_{k-2} &= a_k r_{k-1} + r_k, \\ p_k &= a_k p_{k-1} + p_{k-2}, \\ q_k &= a_k q_{k-1} + q_{k-2}. \end{aligned}$$

Sei n der kleinste Index mit $r_n = 0$; dann ist $p_n r_{n-1} = a$, $q_n r_{n-1} = b$ (Kontrolle), $bp_{n-1} - aq_{n-1} = (-1)^n r_{n-1}$ und $r_{n-1} \sim \mathrm{ggT}\,(a, b)$. Als **Übung** verifiziere man, daß der Algorithmus wirklich funktioniert.

Übung. Man berechne die Bezout-Elemente zu $\mathrm{ggT}\,(21, 15)$ in $\mathbb{Z}$.

Übung. Man berechne den größten gemeinsamen Teiler der Polynome $x^n + x^2 - 2$ $(n \geq 3)$ und $x^2 - 1$ in $\mathbb{Z}[x]$ (das Ergebnis wird von n abhängen). Wie kann man im Nachhinein leicht kontrollieren, daß $x - 1$ immer ein gemeinsamer Teiler ist? Was läßt sich über die Bezout-Elemente sagen?

Übung. Seien $\alpha, \beta \in \mathcal{O}_k$ und $(N\alpha, N\beta) = 1$ in $\mathbb{Z}$. Dann ist $\mathrm{ggT}\,(\alpha, \beta) \sim 1$ in $\mathcal{O}_k$, selbst dann, wenn $\mathcal{O}_k$ kein ZPE-Ring ist.

Übung. Die Bezout-Elemente verdanken ihre Bedeutung der Tatsache, daß man sie zum Invertieren von Restklassen verwenden kann: seien z.B. a und m teilerfremd; man zeige, wie man die Restklasse $a \bmod m$ in $(\mathbb{Z}/m\mathbb{Z})^\times$ invertieren kann (invertieren bedeutet, ein $b \in \mathbb{Z}$ zu finden mit $ab \equiv 1 \bmod m$). Man berechne $\frac{1}{2} \bmod 21$ und $\frac{1}{5} \bmod 33$.

Übung. Zeige, daß $\mathrm{ggT}\,(2, x) = 1$ im ZPE-Ring $\mathbb{Z}[x]$ gilt, und daß hierzu keine Bezout-Elemente existieren.

Übung. Die Bezeichnung offenes Problem ist hier eher angebracht; wer keine vollständige Lösung hinbekommt, sollte also nicht verzweifeln (und wer eine findet, sollte den Fehler suchen). Es geht um die elliptische Kurve $y^2 = x^3 + k^2$

für ein festes $k \in \mathbb{Z}$. Man versuche, mit dem in Kapitel 1 vorgestellten Verfahren etwas über die ganzzahligen Lösungen dieser Gleichung herauszubekommen.

Im Verlaufe der Rechnungen wird es vorteilhaft sein, an k (und vielleicht auch an x, y) Bedingungen zu stellen; eine typische Bedingung ist z.B. die Annahme, k sei eine ungerade Primzahl.

2.5 Die Fermatgleichung $x^4 + y^4 = z^4$

Einer der wenigen Beweise von Fermat, die überlebt haben, ist der von

Satz 2.11. *Die diophantische Gleichung $x^4 + y^4 = z^2$ hat nur die trivialen Lösungen (das sind solche mit $xy = 0$).*

Insbesondere hatt also $x^4 + y^4 = z^4$ keine nicht-trivialen Lösungen. Der Beweis beruht auf der Idee des unendlichen Abstiegs (descente infinie; infinite descent): ausgehend von einer Lösung $(x, y, z) \in \mathbb{N}^3$ konstuiert man eine neue Lösung $(e, f, g) \in \mathbb{N}^3$, die "kleiner" ist; da natürliche Zahlen nicht beliebig verkleinert werden können, folgt so ein Widerspruch.

Bevor wir beginnen, erinnern wir an ein Resultat, das bereits den Griechen bekannt war: dazu nennen wir ein Tripel $(x, y, z) \in \mathbb{N}^3$ ein primitives pythagoräisches Tripel, wenn $x^2 + y^2 = z^2$ gilt und x, y und z paarweise teilerfremd sind. Man sieht sofort, daß z nicht gerade sein kann: denn dann müssen x und y wegen der Teilerfremdheit ungerade sein, folglich ist $x^2 + y^2 \equiv 1 + 1 = 2 \bmod 4$, und eine Zahl $\equiv 2 \bmod 4$ kann kein Quadrat sein. Also ist z ungerade, folglich x oder y gerade; wir wollen im folgenden immer annehmen, daß x die gerade Zahl ist (ansonsten vertauschen wir x und y).

Proposition 2.12. *Ist (x, y, z) ein primitives pythagoräisches Tripel, so gibt es $a, b, c \in \mathbb{N}$ mit $x = 2ab$, $y = a^2 - b^2$ und $z = a^2 + b^2$.*

Beweis. Es ist $x^2 = (z - y)(z + y)$; ein gemeinsamer Teiler d von $z - y$ und $z + y$ teilt deren Summe $2z$ und deren Differenz $2y$. Da nach Voraussetzung $(y, z) = 1$ ist, ist d ein Teiler von 2. Andererseits sind y und z ungerade, d.h. 2 ist in der Tat ein gemeinsamer Teiler von $z - y$ und $z + y$. Nach Korollar 2.8 ist daher $z + y = \pm a^2$ und $z - y = \pm b^2$; da $z \pm y$ positiv ist, gilt jeweils das positive Vorzeichen, und wir erhalten nach Addition, bzw. Subtraktion der beiden Gleichungen $z + y = a^2$ und $z - y = b^2$ und anschließender Division durch 2 die gewünschten Beziehungen $y = a^2 - b^2$

und $z = a^2 + b^2$. Multiplikation der beiden Gleichungen schließlich gibt nach Ziehen der Quadratwurzel $x = 2ab$. □

Jetzt wollen wir die Fermatsche Behauptung beweisen und nehmen dazu an, es gebe eine Lösung $(x, y, z) \in \mathbb{N}^3$ von $x^4 + y^4 = z^2$ mit $xy \neq 0$. Ist p ein gemeinsamer Teiler von x und z, so folgt $p \mid y$, damit $p^4 \mid z^2$ und $p^2 \mid z$; damit kann man p^4 kürzen, und mit diesem Verfahren läßt sich schließlich jeder gemeinsame Teiler von x und z (ebenso von x und y oder von y und z) eliminieren. Wir dürfen also annehmen, daß x, y, z paarweise teilerfremd sind.

Nach Proposition 2.12 existieren $a, b \in \mathbb{N}$ mit $x^2 = 2ab$, $y^2 = a^2 - b^2$ und $z = a^2 + b^2$. Da x gerade ist, muß y ungerade sein. Also ist entweder a gerade und b ungerade oder umgekehrt; im ersten Fall wäre $1 \equiv y^2 = a^2 - b^2 \equiv 0 - 1 \equiv -1 \bmod 4$: Widerspruch. Also ist a ungerade und b gerade, und wegen $b^2 + y^2 = a^2$ folgt nun durch nochmaliges Anwenden von Proposition 2.12 die Existenz von $c, d \in \mathbb{N}$ mit $b = 2cd$, $y = c^2 - d^2$ und $a = c^2 + d^2$. Damit folgt dann $x^2 = 4cd(c^2 + d^2)$, also $(x/2)^2 = cd(c^2 + d^2)$. Nun sind c, d und $c + d$ paarweise teilerfremd (ein gemeinsamer Faktor würde auch a und b, also x und y, teilen), und ihr Produkt ist ein Quadrat; nach zweimaliger Anwendung von Proposition 2.7 (zuerst auf das Paar cd und $x^2 + d^2$, dann auf das Paar c und d) folgt, daß diese Faktoren bis auf eine Einheit ± 1 selbst Quadrate sin müssen; indem wir c und d positiv wählen, können wir $c = e^2$, $d = f^2$ und $c^2 + d^2 = g^2$ für $e, f, g \in \mathbb{N}$ erreichen.

Damit ist jetzt aber $e^4 + f^4 = g^2$, d.h. wir haben eine Lösung der Gleichung vom Ausgangstyp gefunden, und zwar eine neue wegen

$$z = a^2 + b^2 = (c^2 + d^2)^2 + 4c^2d^2 > g^4 \geq g;$$

mit anderen Worten: zu jeder Lösung $(x, y, z) \in \mathbb{N}^3$ mit $xy \neq 0$ gibt es eine Lösung $(e, f, g) \in \mathbb{N}^3$ mit $0 < g < z$ (wäre $g = 0$, so folgte $e = f = 0$ und damit $b = 0$, also $x = 0$: Widerspruch). Also kann es keine Lösung $(x, y, z) \in \mathbb{N}^3$ mit $xy \neq 0$ geben, da wir nach endlich vielen Schritten auf eine Lösung mit $0 < g < 1$ kommen würden. Damit ist Fermat's Behauptung bewiesen.

Auf den ersten Blick ist der Beweis durchaus beeindruckend; andererseits steckt nichts dahinter als eine wiederholte Anwendung von Proposition 2.7!

2.6 * Die diophantische Gleichung $y^2 = x^3 + 1$

Während die ganzzahligen Punkte auf $4w^2 = x^3 + 1$ (also solche auf $y^2 = x^3 + 1$ mit geradem y) leicht bestimmen lassen, führt der allgemeine Fall auf schwierige Probleme. Wir beginnen damit, unsere Gleichung in der Form $x^3 = y^2 - 1 = (y-1)(y+1)$ zu schreiben; ein gemeinsamer Teiler von $y+1$ und $y-1$ teilt deren Differenz 2, d.h. es gibt zwei Möglichkeiten:

1. y ist gerade: dann ist $\mathrm{ggT}\,(y+1, y-1) = 1$, und nach Proposition 2.7 gibt es Zahlen $a, b \in \mathbb{Z}$ mit $y+1 = \pm a^3$ und $y-1 = \pm b^3$. Indem wir $-1 = (-1)^3$ in die dritte Potenz hineinziehen, dürfen wir die Vorzeichen weglassen und haben $y+1 = a^3$ und $y-1 = b^3$. Differenzbildung liefert $2 = a^3 - b^3 = (a-b)(a^2+ab+b^2)$; also ist $a-b$ ein Teiler von 2.

   Ist $a - b = \pm 1$, so ergibt sich $\pm 2 = a^2 + ab + b^2 = (b \pm 1)^2 + b(b \pm 1) + b^2 = 3b^2 \pm 3b + 1$. Löst man die beiden dazugehörigen quadratischen Gleichungen, so ergibt sich ein Widerspruch (die Lösungen sind nicht ganz).

   Ist dagegen $a - b = \pm 2$, so folgt entsprechend $\pm 1 = a^2 + ab + b^2 = (b \pm 2)^2 + b(b \pm 2) + b^2 = 3b^2 \pm 6b + 4$, und jetzt kommt man auf die einzige Lösung $b = -1$, $a = 1$, $y = 0$ und $x = -1$.

2. y ist ungerade: dann ist $\mathrm{ggT}\,(y+1, y-1) = 2$, und nach Proposition 2.7 gibt es Zahlen $a, b \in \mathbb{Z}$ mit $y+1 = 2a^3$ und $y-1 = 4b^3$, wobei wir die Vorzeichen wieder als dritte Potenzen entsorgt haben (die Möglichkeit $y+1 = 4a^3$ und $y-1 = 2b^3$ kann durch Ersetzen von y durch $-y$ auf die erste zurückgeführt werden). Wie oben folgt jetzt durch Bilden der Differenz und Teilen durch 2 die Gleichung $1 = a^3 - 2b^3$.

   Unglücklicherweise ist es sehr schwer zu zeigen, daß diese Gleichung nur die Lösungen $(a, b) = (1, 0), (-1, -1)$ besitzt. Diese führen auf die Lösungen $(y, x) = (\pm 1, 0), (\pm 3, 2)$ der Ausgangsgleichung (man beachte, daß sich für y wirklich beide Vorzeichen ergeben, da wir im Beweis an einer Stelle y durch $-y$ ersetzt haben).

Welche Möglichkeiten gibt es, den Beweis zu beenden? Einmal kann man $a^3 - 2b^3 = 1$ direkt angreifen, indem man $1 = (a - b\sqrt[3]{2})(a^2 + \sqrt[3]{2}\,ab + \sqrt[3]{4}\,b^2)$ schreibt und bemerkt, daß damit $a - b\sqrt[3]{2}$ eine Einheit im Ring $\mathbb{Z}[\sqrt[3]{2}\,]$ ist. Man kann zeigen, daß $R^\times = \langle -1, 1 - \sqrt[3]{2}\,\rangle$ ist, und die Behauptung läuft dann darauf hinaus zu beweisen, daß $\pm(1 - \sqrt[3]{2}\,)^n = a - b\sqrt[3]{2}$ notwendig

$|n| \leq 1$ impliziert (im allgemeinen wird diese Potenz nämlich die Gestalt $r + s\sqrt[3]{2} + t\sqrt[3]{4}$ für ein $t \neq 0$ haben).

Die andere Möglichkeit ist, die Gleichung $y^2 = x^3+1$ in der Form $y^2 = (x+1)(x+\rho)(x+\rho^2)$ zu schreiben, wo $\rho = \frac{1}{2}(-1+\sqrt{-3}\,)$ eine dritte Einheitswurzel ist, und dann in $\mathbb{Z}[\rho]$ zu rechnen.

Beidesmal muß man aber in einen algebraischen Zahlkörper $\neq \mathbb{Q}$ gehen, um die Gleichung zu lösen.

Zusammenfassung

Wir haben folgende Begriffe definiert:

- Einheiten, Assoziierte
- prime und irreduzible Elemente
- Teilbarkeit und Kongruenzen

Wichtigste Ergebnisse sind:

- Primelemente sind irreduzibel; die Umkehrung gilt in ZPE-Ringen
- ZPE-Ringe $\supset$ Hauptidealringe $\supset$ euklidische Ringe

Darüberhinaus gilt: In ZPE-Ringen existiert ein ggT, in Hauptidealringen existieren sogar Bezout-Elemente, und in euklidischen Ringen existiert ein Verfahren, mit denen man diese berechnen kann.

Kapitel 3

Arithmetik in einigen quadratischen Zahlkörpern

3.1 Die Gaußschen Zahlen

$\mathbb{Z}[i]$ ist normeuklidisch

Betrachten wir $R = \mathbb{Z}[i]$; wir wollen zeigen, daß die Norm eine euklidische Funktion auf R ist. Dazu müssen wir zu jedem $\alpha \in R$ und jedem $\beta \in R \setminus \{0\}$ ein $\gamma \in R$ finden mit

$$N(\alpha - \beta\gamma) < N(\beta). \tag{3.1}$$

Da es hier um unendlich viele Paare (α, β) geht, sieht dies ziemlich schwierig aus. Hier kommt uns die Multiplikativität der Norm zugute: dividieren durch $N(\beta)$ in (3.1) zeigt nämlich, daß es genügt, zu jedem $\xi = \alpha/\beta \in k$ ein $\gamma \in R$ zu finden mit

$$N(\xi - \gamma) < 1. \tag{3.2}$$

Damit haben wir immer noch unendlich viele ξ zu betrachten, aber jetzt kommt ein wesentlicher Punkt: können wir in (3.2) für ein ξ ein geeignetes $\gamma \in R$ finden, dann auch automatisch für jedes $\zeta \in k$, das sich von ξ nur um eine ganze Zahl aus R unterscheidet: ist nämlich $\zeta = \xi - \eta$ für ein $\eta \in R$, so folgt aus (3.1) sofort $N(\zeta - (\gamma - \eta)) < 1$.

Es genügt daher, nur solche $\xi \in k$ zu betrachten, die die Form $\xi = x + yi$ mit $|x|, |y| \leq \frac{1}{2}$ haben. Wir behaupten, daß für alle solchen ξ ein einziger Wert

von γ genügt, nämlich $\gamma = 0$. In der Tat ist $N(\xi - \gamma) = N(\xi) = x^2 + y^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1$. Also ist $\mathbb{Z}[i]$ euklidisch bezüglich der Norm (normeuklidisch) und damit insbesondere ein ZPE-Ring.

Übung. Bestimme $\mathrm{ggT}\,(1+i, 1-i)$, $\mathrm{ggT}\,(1+2i, 1-2i)$ und $\mathrm{ggT}\,(1+12i, 7+4i)$ mit dem euklidischen Algorithmus in $\mathbb{Z}[i]$. Kontrolliere das Ergebnis durch Primfaktorzerlegung. Man bestimme auch die dazugehörigen Bezout-Elemente.

Historisch war $\mathbb{Z}[i]$, von $\mathbb{Z}$ selbst einmal abgesehen, der erste Ring algebraischer Zahlen, von dem man die ZPE-Eigenschaften nachweisen konnte. Dies hat Gauß[1] 1828 in seiner Abhandlung über biquadratische Reste getan, und zwar auf demselben Weg wie wir hier.[2]

Primelemente und Assoziierte

Nachdem wir nun gesehen haben, daß $\mathbb{Z}[i]$ als euklidischer Ring sicher auch ZPE-Ring ist, somit jedes Element auf im wesentlichen eindeutige Art und Weise ein Produkt von Primelementen ist, ist es an der Zeit, diese Primelemente genau zu bestimmen. Wir beginnen mit einer allgemein gültigen Beobachtung:

Proposition 3.1. *Sei $\mathcal{O}_k$ der Ganzheitsring in einem quadratischen Zahlkörper k. Dann gibt es zu jedem Primelement $\pi \in \mathcal{O}_k$ genau eine rationale Primzahl $p \in \mathbb{Z}$ mit $\pi \mid p\mathcal{O}_k$. Insbesondere ist $N\pi = \pm p$ oder $N\pi = \pm p^2$.*

Beweis. Wegen $\pi \mid N\pi$ teilt π einen der Primteiler p von $N\pi \in \mathbb{Z}$; wäre auch $\pi \mid q$ für ein primes $q \neq p$, so müßte π den $\mathrm{ggT}\,(p, q) = 1$ teilen und wäre

[1] Carl Friedrich Gauß (1777–1855) war wohl der bedeutendste Mathematiker aller Zeiten; noch als Jugendlicher löste er ein 2000 Jahre altes Problem, indem er zeigte, daß sich das regelmäßige 17-Eck mit Zirkel und Lineal konstruieren läßt - für den Beweis entwickelte er die Kreisteilung, heute Teil der algebraischen Zahlentheorie. Wenig später fand er den ersten vollständigen Beweis des quadratischen Reziprozitätsgesetzes und lieferte im Lauf der Jahre insgesamt acht Beweise desselben. Ebenfalls auf sein Konto geht die Entdeckung der elliptischen Funktionen (das sind doppeltperiodische analytische Funktionen $\mathbb{C} \longrightarrow \mathbb{C}$, die beim Berechnen des Ellipsenumfangs auftreten – daher der Name), die er allerdings – wie vieles andere – nie publiziert hat.

[2] Der erste Ring $\neq \mathbb{Z}$ überhaupt, von dem man zeigte, daß er "euklidisch" ist, war der Polynomring $\mathbb{Q}[X]$; die Existenz eines Euklidischen Algorithmus in diesem Ring wurde vom holländischen Mathematiker Simon Stevin (* 1548 Brügge, † 1620 Den Haag) bewiesen. Stevin hat elf Mathematikbücher geschrieben und den Dezimalzahlen zu ihrem Siegeszug in Europa verholfen.

Einheit. Die zweite Behauptung folgt leicht aus $\pi \mid p$ durch Normbildung: wir finden nämlich $N\pi \mid p^2$ in $\mathbb{Z}$, und da $N\pi \neq \pm 1$ ist (sonst wäre π Einheit), kommen nur die beiden Möglichkeiten $N\pi = \pm p$ und $N\pi = \pm p^2$ in Frage. □

Wir haben also folgende Möglichkeiten:
1) p ist auch in $\mathcal{O}_k$ prim: dann ist $Np = p^2$;
2) p ist in $\mathcal{O}_k$ nicht prim, aber irreduzibel;
3) p ist in $\mathcal{O}_k$ reduzibel.

Im ersten Fall nennt man p eine *träge* Primzahl; der zweite kann nur dann eintreten, wenn $\mathcal{O}_k$ kein ZPE-Ring ist (und im Falle $\mathcal{O}_k = \mathbb{Z}[\sqrt{-5}]$ haben wir bereits gesehen, daß $2\mathcal{O}_k$ nicht prim, aber irreduzibel ist). Untersuchen wir also den dritten Fall: hier ist $p = \alpha\beta$ für Nichteinheiten $\alpha, \beta \in R$. Aus $N\alpha N\beta = p^2$ ergibt sich dann zwangsläufig $N\alpha = N\beta = \pm p$; schließlich ergibt $\pm p = N\alpha = \alpha\alpha'$, daß $\beta = \pm\alpha'$ sein muß. Schreiben wir daher π statt α, so finden wir $\pm = \pi\pi'$, wobei π und π' Primzahlen der Norm $\pm p$ sind. Die einzige noch offene Frage ist, ob π und π' wirklich verschiedene Primelemente sind, oder ob vielleicht $\pi \sim \pi'$ gilt.

Solche Fragen werden wir später allgemein angehen; hier begnügen wir uns mit dem Studium der Primelemente von $\mathbb{Z}[i]$. Wir behaupten:

Proposition 3.2. *Sei $p \in \mathbb{N}$ eine rationale Primzahl; dann gibt es folgende Möglichkeiten:*

1. *$p = 2$: dann ist p reduzibel in $\mathbb{Z}[i]$: es gilt $2 = i(1-i)^2$, und $\pi = 1 - i$ ist bis auf Assoziierte das einzige Primelement, das 2 teilt;*

2. *$p \equiv 3 \bmod 4$: dann ist p träge, d.h. p ist ein Primelement der Norm p^2 in $\mathbb{Z}[i]$;*

3. *$p \equiv 1 \bmod 4$: dann gilt $p = \pi\pi'$ für prime Elemente $\pi = a + bi$ und $\pi' = a - bi$ in $\mathbb{Z}[i]$. Dabei sind π und π' nicht assoziiert.*

Beweis. Die erste Behauptung kann man einfach nachrechnen. Zum Beweis der zweiten nehmen wir an, $p \equiv 3 \bmod 4$ sei nicht prim; da $\mathbb{Z}[i]$ ein ZPE-Ring ist, ist p reduzibel, folglich $\pm p = N\pi$ für ein Primelement $\pi = a + bi$. Offenbar muß das positive Vorzeichen gelten, aber nun ist $p = a^2 + b^2$ niemals $\equiv 3 \bmod 4$, da Quadrate immer $\equiv 0, 1 \bmod 4$ sind: Widerspruch.

Sei schließlich $p \equiv 1 \bmod 4$. Nach dem Eulerschen Kriterium ist -1 quadratischer Rest modulo p, d.h. es gibt ein $x \in \mathbb{N}$ mit $x^2 \equiv -1 \bmod p$ (dies folgt auch einfach aus der Existenz einer Primitivwurzel g modulo p: denn

wegen $g^{(p-1)/2} \equiv -1 \bmod p$ ist $x \equiv g^{(p-1)/4} \bmod p$ eine Lösung der Kongruenz $x^2 \equiv -1 \bmod p$). Dies bedeutet, daß $x^2+1 = (x+i)(x-i)$ durch p teilbar ist. Da keiner der beiden Faktoren durch p teilbar ist, kann p nicht prim sein, und da $\mathbb{Z}[i]$ ein ZPE-Ring ist, muß p reduzibel sein, also $p = \pi\pi'$ für ein $\pi = a + bi$. Wäre $\pi \sim \pi'$, so müßte $\pi'/\pi = \pi'^2/p = (a^2 - b^2 + 2abi)/p$ ganz sein, also $p \mid a^2 - b^2$ und $p \mid ab$. Die zweite Bedingung liefert $p \mid a$ oder $p \mid b$, die erste dann $p \mid a$ und $p \mid b$, also $p \mid \pi$: Widerspruch aus Normgründen. □

Als Korollar halten wir fest:

Korollar 3.3. *(Fermat, Euler) Jede Primzahl der Form* $4n + 1$ *(*$n \in \mathbb{N}$*) ist Summe zweier Quadrate.*

Übung. Diese Folgerung aus der Tatsache, daß $\mathbb{Z}[i]$ euklidisch ist, läßt sich natürlich verallgemeinern. Wie würde man beweisen, daß jede positive rationale Primzahl $p \equiv 1, 3 \bmod 8$ sich in der Form $p = c^2 + 2d^2$ schreiben läßt?

Übung. Zeige, daß sowohl $\{0, \pm 1, \pm i\}$, als auch $\{0, 1, 2, 3, 4\}$ ein vollständiges Restsystem modulo $1 + 2i$ in $\mathbb{Z}[i]$ ist.

Übung. Zeige, daß die Assoziierten von $a+bi \in \mathbb{Z}[i]$ durch $\pm(a+bi)$, $\pm(-b+ai)$ gegeben sind.

Übung. Zeige, daß die folgenden Aussagen für ein $\alpha \in \mathbb{Z}[i]$ äquivalent sind:

1. $(1 + i) \nmid \alpha$;
2. $N\alpha$ ist ungerade;
3. $N\alpha \equiv 1 \bmod 4$;
4. α besitzt eine Assoziierte der Form $a + bi$ mit $a - 1 \equiv b \equiv 0 \bmod 2$;
5. α besitzt eine Assoziierte kongruent $1 \bmod (2 + 2i)$.

Übung. Bestimme alle ganzzahligen Lösungen von $y^2 = x^3 - 1$.

3.2 Die Eisensteinschen Zahlen

Den Ring $\mathbb{Z}[\rho]$ nennt man auch den Ring der Eisensteinschen Zahlen; Eisenstein[3] hat diesen Ring bei seinem Beweis des kubischen Reziprozitätsgesetzes benutzt.

$\mathbb{Z}[\rho]$ ist normeuklidisch

Wie in Gleichung (3.2) haben wir zu zeigen, daß es zu jedem $\xi = x+y\sqrt{-3} \in k = \mathbb{Q}(\sqrt{-3}\,)$ ein $\gamma = \frac{1}{2}(a+b\sqrt{-3}\,) \in \mathcal{O}_k$ gibt (hier ist also $a \equiv b \bmod 2$) mit $N(\xi-\gamma) < 1$. Nun ist $\xi - \gamma = \frac{1}{2}((2x-a)+(2y-b)\sqrt{-3}\,)$; wir können $b \in \mathbb{Z}$ so wählen, daß $|2y-b| \le \frac{1}{2}$ wird. Jetzt müssen wir $a \in \mathbb{Z}$ so bestimmen, daß $|2x-a|$ klein wird und $a \equiv b \bmod 2$ gilt. Indem wir a nur aus den ganzen Zahlen $\equiv b \bmod 2$ wählen, ist letzteres immer machbar; offenbar können wir dabei $|2x-a| \le 1$ erreichen (die nächste ganze Zahl mit vorgegebener Parität hat höchstens Abstand 1 von $2x$). Damit ist dann $N(\xi-\gamma) \le \frac{1}{4}(1+\frac{3}{4}) = \frac{7}{16} < 1$.

Es ist nicht schwer zu zeigen, daß man die Konstante $\frac{7}{16}$ auf $\frac{1}{3}$ verbessern kann; für uns ist das aber ohne Belang.

Primelemente und Assoziierte

Da es in $R = \mathbb{Z}[\rho]$ sechs Einheiten gibt, nämlich ± 1, $\pm\rho$, $\pm\rho^2$, hat jedes von 0 verschiedene Element auch sechs Assoziierte. Ist $\alpha = a+b\rho$, so findet man

$$\begin{array}{rclrcl} \alpha & = & a+b\rho & -\alpha & = & -a-b\rho \\ \alpha\rho & = & -b+(a-b)\rho & -\alpha\rho & = & b+(b-a)\rho \\ \alpha\rho^2 & = & b-a-a\rho & -\alpha\rho^2 & = & a-b+a\rho \end{array}$$

Weiter ist $\sqrt{-3} = \rho - \rho^2$ ein Primelement mit $3 = -(\sqrt{-3}\,)^2$, während für das assoziierte Element $\lambda = 1-\rho$ die Beziehung $(1-\rho)^2 = -3\rho$ gilt.

Wann ist ein Element $\alpha = a+b\rho$ durch λ teilbar? Wegen $\alpha = a+b\rho = a+b-b(1-\rho) \equiv a+b \bmod \lambda$ ist dies genau dann der Fall, wenn $a+b \not\equiv 0 \bmod 3$ ist. In diesem Fall ist aber eine der drei Zahlen a, b oder $a-b$ durch drei

[3] Ferdinand Gotthold Max Eisenstein, 1823–1859; wie Galois, Abel und Riemann ist er sehr jung gestorben. Bekannt ist er vor allem für sein Irreduzibilitätskriterium (das eigentlich auf Schönemann zurückgeht) und durch die Eisensteinreihen in der Theorie der modularen Formen.

teilbar, und die obige Liste zeigt, daß es dann eine Assoziierte von α gibt, deren Koeffizient von ρ durch 3 teilbar ist.

Proposition 3.4. *Ist $\alpha \in \mathbb{Z}[\rho]$ nicht durch $\sqrt{-3}$ teilbar, dann gibt es ein $t \in \{0,1,2\}$ derart, daß $\rho^t\alpha = a + b\rho$ mit $b \equiv 0 \bmod 3$ gilt. Insbesondere besitzt $a = N\alpha$ die Darstellung $4a = L^2 + 27M^2$.*

Die letzte Behauptung folgt sofort durch Bilden der Norm, wenn man $a = L$ und $b = 3M$ setzt.

Andererseits ist in obigem Argument mindestens eine der drei Zahlen a, b und $a - b$ gerade; derselbe Gedanke liefert dann

Proposition 3.5. *Zu jedem $\alpha \in \mathbb{Z}[\rho]$ gibt es ein $t \in \{0,1,2\}$ derart, daß $\rho^t\alpha = a + b\rho$ mit $b \equiv 0 \bmod 2$ gilt. Mit anderen Worten: α besitzt eine Assoziierte der Form $c + d\sqrt{-3}$ mit $c, d \in \mathbb{Z}$.*

Schreibt man $b = 2y$, so folgt $\alpha = a + y(-1 + \sqrt{-3}\,) = x + y\sqrt{-3}$ mit $x = a - y \in \mathbb{Z}$; jedes Element in $\mathbb{Z}[\rho]$ besitzt also eine Assoziierte, die sich in der Form $x + y\sqrt{-3}$ schreiben läßt.

Die Bestimmung der Primelemente in $\mathbb{Z}[\rho]$ verläuft wie in $\mathbb{Z}[i]$ auch, sodaß wir uns mit dem Anschreiben des Resultats begnügen und die Arbeit den Hörern als Übungsaufgabe überlassen; es sei allerdings noch bemerkt, wie man zeigen kann, daß die Kongruenz $x^2 \equiv -3 \bmod p$ für prime $p \equiv 1 \bmod 3$ lösbar ist. Dazu setze man $r = g^{(p-1)/3}$, wo g eine Primitivwurzel modulo p ist. Offenbar gilt $r^3 \equiv 1 \bmod 3$, d.h. r ist eine (primitive) dritte Einheitswurzel in $\mathbb{Z}/3\mathbb{Z}$. Wäre r eine solche in $\mathbb{C}$, so wüßten wir, wie wir daraus eine Quadratwurzel aus 3 konstruieren können: wegen $\rho = \frac{1}{2}(-1 + \sqrt{-3}\,)$ ist z.B. $2\rho + 1$ eine solche. Setzen wir daher $x = 2r + 1$, so bekommen wir $x^2 = 1 + 4r + 4r^2 = -3 + 4(1 + r + r^2)$. Es genügt daher zu zeigen, daß $S = 1 + r + r^2 \equiv 0 \bmod p$ gilt. Nun ist aber $rS = r + r^2 + r^3 \equiv r + r^2 + 1 = S \bmod p$, folglich $p \mid (r-1)S$. Da aber $r \not\equiv 1 \bmod p$ ist, muß S durch p teilbar sein.

Proposition 3.6. *Der Ring $\mathbb{Z}[\rho]$ ist euklidisch und damit ZPE-Ring. Die Primelemente sind bis auf Assoziierte die folgenden:*

1. *$\lambda = 1 - \rho = \sqrt{-3}\rho^2$ ist der Primteiler der 3;*
2. *die Primzahlen $q \equiv 2 \bmod 3$;*
3. *die Elemente π und π' mit $\pi\pi' = p$, wo p eine Primzahl $\equiv 1 \bmod 3$ ist.*

Als weitere Übung zerlege man 7, 13 und 19 in ihre Primfaktoren.

Die Fermatgleichung $x^3 + y^3 + z^3 = 0$

Bereits Euler hat einen Beweis für die Fermatsche Behauptung gegeben, die diophantische Gleichung

$$x^3 + y^3 + z^3 = 0 \tag{3.3}$$

habe nur die trivialen Lösungen ($xyz = 0$), der Eigenschaften von Zahlen der Form $c^2 + 3d^2$ benutzt (ob Eulers Beweis eine Lücke enthält oder nicht, ist umstritten – auf jeden Fall enthalten seine Arbeiten einen vollständigen Beweis). Der erste Beweis mittels der Arithmetik von $\mathbb{Z}[\rho]$ stammt von Gauß, der schärfer gezeigt hat, daß (3.3) selbst in $\mathbb{Z}[\rho]$ nur die triviale Lösung hat. Im folgenden geben wir eine strenge Version des Eulerschen Beweises mit den Methoden von Gauß. Die Idee des Beweises geht auf Fermat zurück, der sie 'descente infinie' (unendlicher Abstieg, im Englischen infinite descent) genannt hat: man nimmt an, eine Gleichung habe eine Lösung $(x, y, z, \dots)$ in ganzen Zahlen und zeigt dann, daß es zu jeder Lösung eine 'kleinere' Lösung $(u, v, w, \dots)$ gibt (kleiner in dem Sinne, daß z.B. $|u| < |x|$ oder ähnliches gilt). Da natürliche Zahlen aber nicht beliebig klein werden können, folgt daraus ein Widerspruch.

Satz 3.7. *Die diophantische Gleichung $x^3 + y^3 + z^3 = 0$ besitzt in $\mathbb{Z}$ nur triviale Lösungen, also solche mit $xyz = 0$.*

Beweis. Um die Beweisidee klarer hervortreten zu lassen, verschieben wir die technischen Angelegenheiten auf den Schluß unseres Beweises.

Sei $[x, y, z]$ eine Lösung von (3.3) mit $xyz \neq 0$; ist $d = \mathrm{ggT}(x, y)$, so folgt $d^3 \mid z^3$, also $d \mid z$, und $x' = x/d$, $y' = y/d$, $z' = z/d$ liefern eine Lösung $[x', y', z']$ mit $\mathrm{ggT}(x', y') = \mathrm{ggT}(y', z') = \mathrm{ggT}(z', x') = 1$. Wir dürfen also ohne Beschränkung der Allgemeinheit von vornherein annehmen, daß $\mathrm{ggT}(x, y) = \mathrm{ggT}(y, z) = \mathrm{ggT}(z, x) = 1$ ist.

Betrachten wir (3.3) nun modulo 9. Wäre keine der drei Zahlen durch 3 teilbar, so folgte $x^3 \equiv \pm 1 \bmod 9$, $y^3 \equiv \pm 1 \bmod 9$, und $z^3 \equiv \pm 1 \bmod 9$, also $\pm 1 \pm 1 \pm 1 \equiv 0 \bmod 9$: Widerspruch. Folglich ist eine (und wegen der Teilerfremdheit genau eine) der drei Zahlen durch 3 teilbar, sagen wir z. Wir definieren $n \geq 1$ durch $3^n \parallel z$. Wegen[(1)] $\mathrm{ggT}(x + y, x^2 - xy + y^2) = 3$ folgt dann mit Proposition 2.7 aus $(x + y)(x^2 - xy + x^2) = z^3$, daß

$$x + y = 3^{3n-1}a^3 \tag{3.4}$$

$$x^2 - xy + y^2 = 3b^3 \tag{3.5}$$

mit $3 \nmid ab$ gilt. Im Ring $R = \mathbb{Z}[\rho]$ zerfällt $x^2 - xy + y^2$ in zwei Faktoren:

$$x^2 - xy + y^2 = (x + y\rho)(x + y\rho^2).$$

Schreiben wir $x + y\rho = \alpha$, so ist $x + y\rho^2 = \alpha'$. Wegen[(2)] $\mathrm{ggT}\,(x + y\rho, x + y\rho^2) \sim \sqrt{-3}$ folgt aus der Teilerfremdheit von $\alpha/\sqrt{-3}$ und $\alpha'/\sqrt{-3}$, daß $\alpha = x + y\rho = \rho^{-t}\sqrt{-3}\,\gamma^3$ für ein geeignetes $t \in \{0, \pm 1\}$ und $\gamma \in \mathbb{Z}[\rho]$ gilt. Dabei dürfen wir annehmen, daß $\gamma = (g + h\sqrt{-3}\,)^3$ mit $g, h \in \mathbb{Z}$ sind (denn dies können wir durch geeignete Multiplikation von γ mit Potenzen von ρ sicher erreichen; diese Potenzen von ρ stören wegen der dritten Potenz von γ nicht). Weiter kann man leicht[(3)] $t = 1$ zeigen; damit ist

$$\alpha = x + y\rho = \rho^{-1}\sqrt{-3}\,(g + h\sqrt{-3}\,)^3, \tag{3.6}$$

wegen $\rho\alpha = -y + (x - y)\rho = -\frac{x+y}{2} + \frac{x-y}{2}\sqrt{-3}$ daher $x + y = -2(9g^2h - 9h^3)$, und somit zusammen mit (3.4) $3^{3n-1}a^3 = -18h(g - h)(g + h)$, oder

$$(3^{n-1}a)^3 = -2h(g - h)(g + h). \tag{3.7}$$

Wegen[(4)] $\mathrm{ggT}\,(2h, g+h) = \mathrm{ggT}\,(g+h, g-h) = \mathrm{ggT}\,(2h, g-h) = 1$ liefert eine letzte Anwendung von Proposition (2.7) die Existenz von $A, B, C \in \mathbb{Z}$ mit $-2h = A^3$, $g + h = B^3$ und $g - h = -C^3$, $ABC = 3^{n-1}a$ und $A^3 + B^3 + C^3 = -2h + g + h - (g - h) = 0$. Also ist (3.3) auch lösbar mit ganzen Zahlen A, B, C derart, daß ABC genau durch 3^{n-1} teilbar ist (in der Ausgangslösung war xyz genau durch 3^n teilbar). Indem man so fortfährt, erhält man irgendwann eine Lösung $[a, b, c]$ mit $3 \nmid abc$: eine solche kann es aber, wie wir eingangs gesehen haben, nicht geben.

Dieser Widerspruch beendet den Beweis. Nachzuweisen sind allerdings noch die Teilerfremdheitsaussagen (1), (2) und (4), sowie die Behauptung (3) über die Einheit ρ^t.

Beginnen wir mit (2). Ein gemeinsamer Teiler von α und α' teilt auch die Differenz $\alpha - \alpha' = y(\rho - \rho^2)$, sowie $\alpha\alpha' = 3b^3$ und damit erst recht z^3. Wegen $(y, z) = 1$ kann also nur das Primelement $\sqrt{-3} = \rho - \rho^2$ gemeinsamer Teiler von α und α' sein. Dieses ist auch in der Tat ein solcher: wären nämlich α und α' teilerfremd, so müßte mit ihrem Produkt auch eine unter ihnen durch 3 teilbar sein: das geht aber nur für $3 \mid x$, $3 \mid y$, und dies widerspricht der angenommenen Teilerfremdheit. Insbesondere ist das Produkt $(x^2 - xy + y^2) = (x + y\rho)(x + y\rho^2)$ genau durch 3 teilbar; dies ist der zweite Teil von (1). Der erste folgt leicht: ist p ein Primteiler von $x + y$, also $x \equiv -y \bmod p$,

so folgt $x^2 - xy + y^2 \equiv 3y^2 \bmod p$. Aber $p \mid y$ widerspricht (wegen $x \equiv -y \bmod p$) der Teilerfremdheit von x und y, folglich kommen nur Potenzen von 3 als gemeinsame Teiler in Frage. Wegen $3 \parallel (x^2 - xy + y^2)$ und der Tatsache, daß $(x^2 - xy + y^2)(x + y) = -z^3$ eine dritte Potenz ist, muß also $3 = \mathrm{ggT}\,(x + y, x^2 - xy + y^2)$ sein wie behauptet.

Als nächstes zeigen wir (3). Sei dazu p ein gemeinsamer Primteiler von $g + h$ und $g - h$; wäre $p = 2$, also g und h entweder beide gerade oder beide ungerade, so folgte $2 \mid (g + h\sqrt{-3}\,)$, somit $2 \mid \alpha$ und endlich $2 \mid x$, $2 \mid y$: Widerspruch. Ist $p \geq 3$, so teilt p mit $g + h$ und $g - h$ auch deren Summe $2g$ und Differenz $2h$, d.h. es ist $p \mid g$ und $p \mid h$, somit wie oben $p \mid x$ und $p \mid y$ im Widerspruch zur Voraussetzung.

Schließlich kümmern wir uns um (4). Wegen $1 \sim (g + h\sqrt{-3}, \sqrt{-3}\,)$ folgt $(g + h\sqrt{-3}\,)^3 \equiv g^3 \equiv \pm 1 \bmod 3\sqrt{-3}$, andererseits zeigt $\alpha \equiv x(1 - \rho) \bmod 9$, daß $\pm(1 - \rho) \equiv \pm\rho^{-t}\sqrt{-3} \bmod 3$ gilt. Setzt man $\sqrt{-3} = \rho - \rho^2$ ein, so sieht man, daß $t = 1$ sein muß. □

Mit derselben Methode kann man zeigen, daß die Gleichung $x^3 + y^3 = 3z^3$ nur nichttriviale Lösungen besitzt; entsprechend sind die einzigen Lösungen von $x^3 + y^3 = 2z^3$ mit $xyz \neq 0$ gegeben durch (x, x, x); beide Sätze stammen von Legendre[4], der weiter behauptet hat, $x^3 + y^3 = az^3$ habe für $a = 3, 4, 5, 6, 8, \ldots$ nur nichttriviale Lösungen. Pépin dagegen hat darauf verwiesen, daß $17^3 + 37^3 = 6 \cdot 21^3$ ist. Nagell hat schließlich gezeigt, daß die Gleichung $x^3 + y^3 = az^3$ für $a > 2$ entweder keine oder unendlich viele primitive Lösungen besitzt. (Eine Lösung $(x, y, z) \in \mathbb{Z}^3$ heißt primitiv, wenn x, y, z paarweise teilerfremd sind. Ist $(x, y, z) \in \mathbb{Z}^3$ irgendeine Lösung, so kann man sich dazu leicht unendlich viele nicht-primitive Lösungen (kx, ky, kz) mit $k \in \mathbb{Z}$ basteln.

Ein weiteres Ergebnis kann man dem Büchlein "Lectures on Elliptic Curves", Cambridge Univ. Press 1991, von J.W.S. Cassels entnehmen: dort wird skizziert, daß die Gleichung $x^3 + y^3 = q_1 q_2 z^3$, wo $q_1 \equiv 2 \bmod 9$ und $q_2 \equiv 5 \bmod 9$ prim sind, nur trivial lösbar ist. Das legt die Frage nach, was solche Gleichungen in einem Buch über elliptische Kurven zu suchen haben. Tatsächlich ist die Fermatkurve $x^3 + y^3 = z^3$ eine elliptische Kurve: dividiert man durch z und setzt $r = x/z$, $s = y/z$, so folgt $r^3 + s^3 = 1$; mit $r = u + v$ und $s = u - v$ erhält man weiter $2u^3 + 6uv^2 = 1$, also $2 + 6(v/u)^2 = 1/u^3$.

[4] Adrien-Marie Legendre, 1752 – 1833; er hat das quadratische Reziprozitätsgesetz in seiner heutigen Form ausgesprochen, und ist außerdem für seine Arbeiten auf dem Gebiet der elliptischen Funktionen bekannt.

Multipliziert man dies mit 6^3 und setzt $Y = 36v/u$, $X = 6/u$, so ergibt sich die elliptische Kurve $Y^2 = X^3 - 432$.

Übung. Man zeige, daß $x^3+y^3 = dz^3$ für jedes rationale $d \neq 0$ eine elliptische Kurve ist.

3.3 * Elemente mit Primnorm sind prim

Daß ein $\pi \in \mathcal{O}_k$, für das $p = N\pi$ eine rationale Primzahl ist, immer irreduzibel ist, haben wir schon gesehen. Tatsächlich sind solche π aber sogar prim:

Proposition 3.8. *Ist k ein quadratischer Zahlkörper mit Ganzheitsring $\mathcal{O}_k$, so ist jedes $\pi \in \mathcal{O}_k$ mit primer Norm auch prim.*

Ist $\mathcal{O}_k$ ein ZPE-Ring, ist dies leicht einzusehen: Elemente mit primer Norm sind irreduzibel, und in ZPE-Ringen sind irreduzible Elemente prim. Um dies allgemein zu beweisen, seien $\alpha, \beta \in \mathcal{O}_k$ gegeben mit $\pi \mid \alpha\beta$; zu zeigen ist, daß dies $\pi \mid \alpha$ oder $\pi \mid \beta$ impliziert. In der Sprache von Kongruenzen müssen wir also aus $\alpha\beta \equiv 0 \bmod \pi$ schließen, daß $\alpha \equiv 0 \bmod \pi$ oder $\beta \equiv 0 \bmod \pi$ gilt; mit anderen Worten: zu zeigen ist, daß der Restklassenring $\mathcal{O}_k/\pi\mathcal{O}_k$ nullteilerfrei ist. Tatsächlich werden wir sogar zeigen, daß $\mathcal{O}_k/\pi\mathcal{O}_k \simeq \mathbb{F}_{|p|} = \mathbb{Z}/p\mathbb{Z}$ isomorph zum Körper mit $|p|$ Elementen ist.

Sei dazu $\{1, \omega\}$ eine Ganzheitsbasis von $\mathcal{O}_k$, also $\mathcal{O}_k = \mathbb{Z} \oplus \mathbb{Z}\omega$; damit ist $\pi = a + b\omega$ für $a, b \in \mathbb{Z}$. Wir behaupten, daß b nicht durch π (und erst recht nicht durch $p = \pi\pi'$) teilbar ist. Aus $\pi \mid b$ folgt nämlich wegen $a = \pi - b\omega$ sofort $\pi \mid a$, und durch Normbildung $p \mid a^2$ und $p \mid b^2$; da p prim in $\mathbb{Z}$ ist, gilt $p \mid a$ und $p \mid b$; dann wäre aber $\pi = a + b\omega$ durch $p = \pi\pi'$ teilbar und folglich π' eine Einheit: Widerspruch.

Damit existiert ein $c \in \mathbb{Z}$ mit $bc \equiv 1 \bmod p$ (insbesondere ist $bc \equiv 1 \bmod \pi\mathcal{O}_k$). Wir finden $b\omega \equiv -a \bmod \pi$, nach Multiplikation mit c somit $\omega \equiv -ac \bmod \pi\mathcal{O}_k$. Ist nun irgendein $\gamma = r + s\omega \in \mathcal{O}_k$ gegeben, so folgt $\gamma \equiv r + sbc \bmod \pi\mathcal{O}_k$, d.h. modulo π ist jedes Element einer ganzen Zahl aus $\mathbb{Z}$ kongruent. Indem wir diese Zahl modulo p (und p ist ein Vielfaches von π) reduzieren, folgt weiter, daß γ modulo π einer der Zahlen $0, 1, 2, \ldots, p-1$ kongruent ist.

Jetzt ist die Nullteilerfreiheit aber ganz leicht zu zeigen: ist $\alpha\beta \equiv 0 \bmod \pi$ und sind $A, B \in \{0, 1, \ldots, p-1\}$ Zahlen mit $\alpha \equiv A \bmod \pi\mathcal{O}_k$ und $\beta \equiv B \bmod \pi\mathcal{O}_k$, so folgt $\pi \mid AB$; Normbildung liefert $p \mid A^2B^2$, folglich $p \mid A$ oder

$p \mid B$. Also ist $A = 0$ oder $B = 0$, und damit schließlich $\alpha \equiv A = 0 \bmod \pi$ oder $\beta \equiv B = 0 \bmod \pi$.

3.4 Die Pellsche Gleichung

Im Gegensatz zu imaginärquadratischen Zahlkörpern scheinen die Ganzheitsringe reellquadratischer Körper $\mathbb{Q}(\sqrt{m})$ nichttriviale Einheiten (also solche nicht endlicher Ordnung) zu besitzen; die folgende Tabelle gibt solche Einheiten für kleine Werte von m:

m	2	3	5	6	7
ε	$1+\sqrt{2}$	$2+\sqrt{3}$	$\frac{1}{2}(1+\sqrt{5})$	$5+2\sqrt{6}$	$8+3\sqrt{7}$

Dies legt die Vermutung nahe, daß dies für alle $m > 0$ richtig ist; da Einheiten ganze Elemente mit Norm ± 1 sind, läuft dies auf die Aussage hinaus, daß die *Pellsche Gleichung* $x^2 - my^2 = 1$ für alle quadratfreien $m > 0$ lösbar ist. Tatsächlich gilt etwas mehr:

Satz 3.9. *Sei $m > 0$ kein Quadrat. Dann ist die Gleichung $x^2 - my^2 = 1$ in ganzen Zahlen x, y nichttrivial lösbar.*

Der Beweis des Satzes ist etwas verwickelt; im wesentlichen beruht er auf dem Dirichletschen Schubfachprinzip, das sich folgendermaßen aussprechen läßt:

> Legt man $N+1$ Perlen in N Schubfächer, dann enthält ein Schubfach mindestens zwei Perlen.

Übung. Man zeige mit dem Schubfachprinzip: zu jeder reellen Zahl gibt es unendlich viele Paare $(p, q) \in \mathbb{Z} \times \mathbb{Z}$ mit $|x - \frac{p}{q}| < \frac{1}{q^2}$. (Hinweis: betrachte die Reste modulo 1 der Zahlen $0, x, 2x, \ldots, nx$; diese $n+1$ Reste liegen in den n Intervallen $[0, \frac{1}{n}), [\frac{1}{n}, \frac{2}{n}), \ldots, [\frac{n-1}{n}, 1)$).

Wir beginnen mit dem

Hilfssatz 3.10. *Seien ξ_1 und ξ_2 zwei von 0 verschiedene reelle Zahlen derart, daß ξ_1/ξ_2 irrational ist. Dann gibt es zu jedem $N \in \mathbb{N}$ Zahlen $A, B \in \mathbb{Z}$, die nicht beide gleich 0 sind und die folgenden Ungleichungen genügen:*

$$|A\xi_1 + B\xi_2| \le \tfrac{1}{N}(|\xi_1| + |\xi_2|), \quad |A| \le N,\ |B| \le N. \tag{3.8}$$

Beweis. Wir nehmen an, daß ξ_1 und ξ_2 beide positiv sind (andernfalls müssen die Vorzeichen von a und b im folgenden Beweis entsprechend geändert werden). Wir betrachten die Funktion

$$f : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{R} : (a, b) \longmapsto a\xi_1 + b\xi_2 \tag{3.9}$$

und behaupten, daß f injektiv ist. In der Tat folgt aus $f(a, b) = f(a', b')$ sofort $(a - a')\xi_1 + (b - b')\xi_2 = 0$, und dies steht im Widerspruch dazu, daß ξ_1/ξ_2 irrational ist.

Es gibt $(N+1)^2$ Paare ganzer Zahlen in $[0, N] \times [0, N]$, und deren Funktionswerte liegen im Intervall $[0, N(|\xi_1| + |\xi_2|)]$. Teilen wir dieses Intervall in N^2 gleichlange Stücke der Länge $\frac{1}{N}(|\xi_1| + |\xi_2|)$, so muß es wegen $(N + 1)^2 > N^2$ und dem Dirichletschen Schubfachprinzip zwei Paare $(a, b) \neq (a', b')$ geben mit $|f(a, b) - f(a', b')| \leq \frac{1}{N}(|\xi_1| + |\xi_2|)$. Setzen wir jetzt $A = a - a'$ und $B = b - b'$, so haben diese die gewünschten Eigenschaften. □

Korollar 3.11. *Sei $m \in \mathbb{N}$ kein Quadrat. Dann gibt es ein $c \in \mathbb{Z}$ derart, daß die Gleichung $A^2 - mB^2 = c$ unendlich viele Lösungen $(A, B) \in \mathbb{Z} \times \mathbb{Z}$ besitzt.*

Beweis. Nach obigem Hilfssatz gibt es Zahlen $A, B \in \mathbb{Z}$, die nicht beide 0 sind und den Ungleichungen

$$|A - B\sqrt{m}\,| \leq \tfrac{1}{N}(1 + \sqrt{m}\,), \ |A| \leq N, \ |B| \leq N \tag{3.10}$$

genügen. Die Dreiecksungleichung liefert

$$|A + B\sqrt{m}\,| \leq |A| + |B\sqrt{m}\,| \leq N(1 + \sqrt{m}\,), \tag{3.11}$$

und Multiplikation von (3.10) und (3.11) gibt

$$|A^2 - mB^2| \leq (1 + \sqrt{m}\,)^2. \tag{3.12}$$

Jetzt lassen wir $N \to \infty$ gehen. Dann müssen unendlich viele verschiedene Paare (A, B) auftreten, da aus der Endlichkeit folgen würde, daß die Menge $\{|A - B\sqrt{m}\,| : A, B \in \mathbb{Z}\}$ ein Minimum besäße, was wegen (3.10) aber nicht sein kann.

Da aber $|A^2 - mB^2|$ durch (3.10) nach oben beschränkt ist, muß es ein $c \in \mathbb{Z}$ mit $|c| \leq (1 + \sqrt{m}\,)^2$ geben, für das $A^2 - mB^2 = c$ unendlich viele Lösungen besitzt. □

Jetzt können wir Satz 3.9 beweisen: nach obigem Korollar gibt es für ein geeignetes $m \in \mathbb{Z}$ unendlich viele Paare (A, B) mit $A^2 - mB^2 = c$ (und offenbar dürfen wir dabei $A > 0$ annehmen). Darunter wählen wir $(c+1)^2$ Lösungen aus und betrachten deren Restklassen modulo c. Nach dem Dirichletschen Schubfachprinzip gibt es also Paare $(A_1, B_1) \neq (A_2, B_2)$ mit $A_1 \equiv A_2 \bmod c$ und $B_1 \equiv B_2 \bmod c$. Mit $\eta_j = A_j + B_j\sqrt{m}$ ist dann $N\eta_1 = N\eta_2 = m$ und $\eta_1 \equiv \eta_2 \bmod c$. Aus $N(\eta_1/\eta_2) = 1$ folgt, daß η_1/η_2 eine Einheit ist, *wenn* wir zeigen können, daß diese Zahl ganz ist. Nun gilt aber $\eta_1/\eta_2 = 1 + (\eta_1 - \eta_2)/\eta_2 = 1 + (\eta_1 - \eta_2)\eta_2'/m$. Da aber die Differenz $\eta_1 - \eta_2$ nach Konstruktion durch m teilbar ist, ist η_1/η_2 in der Tat ganz und damit eine Einheit. Zu zeigen ist jetzt noch, daß $\eta_1/\eta_2 \neq \pm 1$ ist. Aber $\eta_1/\eta_2 \neq 1$ folgt aus $\eta_1 \neq \eta_2$, und $\eta_1/\eta_2 \neq -1$ folgt aus der Tatsache, daß A_1 und A_2 beide positiv sind. Damit ist 3.9 bewiesen.

Wir wissen jetzt, daß es in jedem reellquadratischen Zahlkörper nichttriviale Einheiten gibt. Tatsächlich kann man die Einheitengruppe als abstrakte Gruppe ganz genau bestimmen: für reellquadratische k gilt $\mathcal{O}_k^\times \simeq (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}$. Dies ist der Inhalt von

Satz 3.12. *Ist k ein reellquadratischer Zahlkörper, so gibt es eine Einheit $\varepsilon \in \mathcal{O}_k^\times$ derart, daß jede Einheit $\eta \in \mathcal{O}_k^\times$ sich eindeutig in der Form $\eta = \pm\varepsilon^t$ für ein $t \in \mathbb{Z}$ schreiben läßt.*

Man sieht sofort, daß mit ε auch $\pm\varepsilon^{\pm 1}$ (und nur diese vier) die Eigenschaft in Satz 3.12 haben; von diesen vier Einheiten sind genau zwei positiv, und von diesen beiden ist genau eine > 1. Diese Einheit $\varepsilon > 1$ nennt man auch die *Fundamentaleinheit* von k.

Beweis. Wir identifizieren nun die Zahlen $a + b\sqrt{m}$ mit denjenigen reellen Zahlen, die der positiven Quadratwurzel von m entsprechen. Die einzigen Einheiten $\eta \in \mathcal{O}_k^\times$ mit $|\eta| = 1$ sind dann $\eta = \pm 1$ (dies folgt aus der Irrationalität von m).

Wir behaupten, daß es unter allen Einheiten mit $|\eta| > 1$ eine mit minimalem Betrag gibt. Andernfalls gibt es eine (sogar unendlich viele) Einheit mit $1 < |\eta| < \frac{5}{4}$. Wegen $|\eta\eta'| = 1$ folgt daraus $\frac{4}{5} < |\eta'| < 1$. Schreibt man $\eta = a + b\sqrt{m}$ (mit möglicherweise halbzahligen a, b), so folgt $2|a| = |\eta + \eta'| \leq |\eta| + |\eta'| < \frac{9}{4}$, also $|a| \leq 1$. Da $a = 0$ unmöglich ist, muß $a = \pm 1$ sein. Aus $1 < |\eta| < \frac{5}{4}$ folgt dann sofort $b = 0$, also $\eta = 1$ im Widerspruch zur Annahme.

Sei nun ε eine Einheit mit minimalem Betrag > 1. Wir behaupten, daß ε dann die Eigenschaften aus Satz 3.12 besitzt. Wäre dies nämlich nicht so,

gäbe es eine Einheit η mit $\varepsilon^n < |\eta| < \varepsilon^{n+1}$ für geeignetes $n \in \mathbb{N}$. Dann ist aber $\eta\varepsilon^{-n}$ eine Einheit, deren Betrag echt zwischen 1 und ε liegt: dies widerspricht der Wahl von ε.

Die Eindeutigkeit ist klar: aus $\pm\varepsilon^t = \pm\varepsilon^u$ folgt $|\varepsilon^{t-u}| = 1$, was wegen der Irrationalität von ε sofort $t = u$ impliziert; damit folgt dann wiederum die Übereinstimmung des Vorzeichens. □

Bemerkung. Der hier angeführte Existenzbeweis taugt nicht zur Berechnung der Fundamentaleinheit (außer für ganz kleine m); beispielsweise ist $\varepsilon = 48842 + 5967\sqrt{67}$ die Fundamentaleinheit von $\mathbb{Q}(\sqrt{67})$. Es gibt glücklicherweise ein recht gutes Verfahren zur Berechnung von Fundamentaleinheiten quadratischer Körper, das auf der Kettenbruchentwicklung von $\sqrt{m}$ beruht. Ein ähnlich schnelles Verfahren für Zahlkörper höheren Grades ist unbekannt.

3.5 * Welche Zahlen sind Normen?

Die einzige uns bisher bekannte Methode, die Unlösbarkeit der Gleichung $x^2 - my^2 = c$ bei gegebenen $m \in \mathbb{N}$ und $c \in \mathbb{Z}$ zu beweisen, ist diejenige, die Gleichung als Kongruenz modulo n aufzufassen, wobei n ein Teiler von m oder c ist; beispielsweise ist $x^2 - 10y^2 = \pm 2$ in $\mathbb{Z}$ nicht lösbar, weil es die Kongruenz $x^2 \equiv \pm 2 \bmod 5$ nicht ist. Diese Methode versagt aber bei der Gleichung $x^2 - 79y^2 = \pm 3$, und der Grund ist einfach: $x^2 - 79y^2 = -3$ hat die rationale Lösung $x = \frac{2}{5}$, $y = \frac{1}{5}$; insbesondere ist sie lösbar modulo jedem zu 5 teilerfremden $n \in \mathbb{Z}$. Entsprechend zeigt $x = \frac{13}{7}$ und $y = \frac{2}{7}$, daß sie modulo jedem zu 7 teilerfremden $n \in \mathbb{Z}$ lösbar ist. Insgesamt sehen wir, daß $x^2 - 79y^2 \equiv -3 \bmod m$ für alle $m \in \mathbb{Z}$ lösbar ist.

Um zu zeigen, daß $x^2 - 79y^2 = -3$ wirklich keine ganzzahlige Lösung besitzt, müssen wir uns daher etwas anderes einfallen lassen. Sei dazu allgemein $k = \mathbb{Q}(\sqrt{m})$ ein reellquadratischer Zahlkörper, und sei $\varepsilon = t + u\sqrt{m} > 1$ die Fundamentaleinheit (beachte, daß t und u halbzahlig sein dürfen). Sei weiter $\alpha \in \mathcal{O}_k$ eine Lösung der Gleichung $|N\alpha| = c$. Nun macht man sich geometrisch leicht klar, daß es ein $n \in \mathbb{Z}$ gibt, sodaß folgende Ungleichung erfüllt ist:

$$1 \le |\varepsilon^n \alpha| < |\varepsilon|.$$

Setzen wir $\beta = \varepsilon^n\alpha$ und schreiben $\beta = a + b\sqrt{m}$ (wieder dürfen a und b

halbzahlig sein), dann folgt

$$|\beta'| = \frac{|\beta\beta'|}{|\beta|} = \frac{c}{|\beta|},$$

und daher die Abschätzungen

$$\frac{c}{|\varepsilon|} < |\beta'| \leq c.$$

Die Dreiecksungleichung liefert jetzt

$$\begin{aligned} |2a| = |\beta + \beta'| \leq |\beta| + |\beta'| < |\varepsilon| + c, \\ |2b|\sqrt{m} = |\beta - \beta'| \leq |\beta| + |\beta'| < |\varepsilon| + c. \end{aligned} \tag{3.13}$$

Hieraus folgen sofort Schranken für a und b, und jetzt kann man das Problem in endlich vielen Schritten lösen, indem man einfach durchprobiert. Bevor man dies bei unserem Beispiel mit $m = 79$ durchführt, sollte man sich aber Gedanken darüber machen, ob sich diese Schranken nicht verbessern lassen: es ist nämlich hier $\varepsilon = 80 + 9\sqrt{79} \approx 160$, sodaß man relativ viele Paare (a, b) zu betrachten hat!

In der Tat lassen sich die Schranken wesentlich verschärfen. Setzen wir nämlich wie oben $\beta = \varepsilon^n \alpha$ und wählen $n \in \mathbb{Z}$ so, daß

$$\frac{\sqrt{c}}{\sqrt{\varepsilon}} \leq |\beta| < \sqrt{c|\varepsilon|}$$

gilt, so erhalten wir wie oben die Abschätzungen

$$|\beta| < \sqrt{c|\varepsilon|} \quad \text{und} \quad |\beta'| \leq \sqrt{c|\varepsilon|},$$

was dann bereits auf $|2a| < 2\sqrt{c|\varepsilon|}$ führt, die deutlich besser ist als $|2a| < |\varepsilon| + c$.

Tatsächlich kann man aber noch einmal in etwa einen Faktor 2 gewinnen, wenn man folgenden Hilfssatz verwendet:

Hilfssatz 3.13. *Genügen $x, y \in R$ den Ungleichungen $0 < x \leq r$, $0 < y \leq r$ und $0 < xy \leq s$, dann ist $x + y \leq r + \frac{s}{r}$.*

Beweis. Es ist $0 < (r - x)(r - y) = r^2 - r(x + y) + xy \leq r^2 + s - r(x + y)$, und die Behauptung folgt. □

Wir haben eine solche Situation vorliegen mit $r = \sqrt{c|\varepsilon|}$ und $s = c$; also folgt $|\beta + \beta'| \le c\big(\sqrt{|\varepsilon|} + \frac{1}{\sqrt{|\varepsilon|}}\big)$; da man $\frac{1}{\sqrt{|\varepsilon|}}$ z.B. durch 1 nach oben abschätzen kann, ist diese Schranke für große ε tatsächlich um etwa einen Faktor 2 besser. Wir fassen zusammen:

Satz 3.14. *Sei k ein quadratischer Zahlkörper mit Einheit $\varepsilon > 1$; dann existiert zu jedem $\alpha \in \mathcal{O}_k$ mit Norm $|N\alpha| = c$ eine Assoziierte $\beta = a + b\sqrt{m}$ (mit höchstens halbzahligen a, b), sodaß die folgenden Schranken gelten:*

$$\begin{aligned} |a| &\le \frac{1}{2}\sqrt{c}\big(\sqrt{|\varepsilon|} + \tfrac{1}{\sqrt{|\varepsilon|}}\big) \\ |b| &\le \frac{1}{2\sqrt{m}}\sqrt{c}\big(\sqrt{|\varepsilon|} + \tfrac{1}{\sqrt{|\varepsilon|}}\big) \end{aligned} \tag{3.14}$$

Für $m = 79$, $\varepsilon = 80 + 9\sqrt{79}$ und $c = 3$ folgt damit $|b| \le 1.24...$, d.h. es ist nur $b = 1$ zu betrachten (auf $b = -1$ können wir aus Symmetriegründen verzichten, der Fall $b = 0$ ist offensichtlich unmöglich). Aber die Gleichung $a^2 - 79 \cdot 1^2 = \pm 3$ ist nicht lösbar, da 79 ± 3 keine Quadratzahl ist. Also gibt es in $\mathbb{Z}[\sqrt{79}\,]$ kein Element der Ordnung ± 3, d.h. 3 ist irreduzibel, wegen $3 \mid (2 - \sqrt{79}\,)(2 + \sqrt{79}\,)$ aber nicht prim.

3.6 Der Lucas-Lehmer-Test

Seit Euklid wissen wir, daß es keine größte Primzahl geben kann; trotzdem gibt es eine größte *bekannte* Primzahl, und solange keine einfache Primzahlformel gefunden wird, wird dies auch so bleiben. Die größte bekannte Primzahl ist in der Regel eine Zahl der Form $2^p - 1$ mit p prim; Zahlen dieser Form heißen Mersenne-Zahlen.[5] Es ist leicht zu zeigen, daß $2^p - 1$ nur dann prim sein kann, wenn p selbst prim ist: dies folgt leicht aus der

[5] Marin Mersenne (1588–1648), Priester. Er stand mit vielen Mathematikern brieflich in Verbindung und war fuer die Verbreitung neuer Resultate "zuständig". Bekannt ist er für seine Vermutung, daß $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$, und 257 die einzigen Primzahlen ≤ 257 sind, für die $2^p - 1$ prim ist. Tatsächlich führen $p = 67$ und $p = 257$ auf zusammengesetzte Zahlen, während $p = 61, 89, 107$ Primzahlen liefern, aber nicht auf seiner Liste stehen. Daß $2^{67} - 1$ nicht prim ist, hat man schon früh mit dem LL-Test erkannt; die tatsächliche Faktorisierung gelang Coleman, der dafür, wie er selbst sagte, die "Sonntage von drei Jahren" verbraten hat. Heute liefert ein gutes Faktorisierungsprogramm das Ergebnis $2^{67} - 1 = 193707721 \cdot 761838257287$ in Sekundenschnelle. Dagegen kostet die Faktorisierung von $2^{257} - 1 = 535006138814359 \cdot 1155685395246619182673033 \cdot$

Tatsache, daß $2^a - 1$ immer ein Teiler von $2^{ab} - 1$ ist wegen $x^{ab} - 1 = (x^a - 1)(x^{ab-a} + x^{ab-2a} + \ldots + x^a + 1)$, was sich durch Ausmultiplizieren leicht verifizieren läßt.

Der Grund, warum Rekordprimzahlen in der Regel Mersennesche Zahlen sind, liegt in folgendem sehr einfachen Test (benannt nach Lucas[6] und Lehmer[7]), mit dem man die Primalität solcher Zahlen beweisen kann: $M_p = 2^p - 1$ (mit $p \geq 3$) ist prim genau dann wenn $S_{p-1} \equiv 0 \bmod M_p$ ist, wo die Folge S_n rekursiv definiert ist durch $S_1 = 4$ und $S_{n+1} = S_n^2 - 2$.

Beispiel: sei $p = 5$; dann ist $M_5 = 31$, und wir finden

$$\begin{aligned} S_1 &= 4 \\ S_2 &= 14 \\ S_3 &= 194 \equiv 8 \bmod 31 \\ S_4 &\equiv 62 \equiv 0 \bmod 31, \end{aligned}$$

und damit ist M_5 prim.

Daß dieser Test funktioniert, liegt erstens daran, daß $M_p + 1$ eine einfache Primfaktorzerlegung besitzt (es ist eine 2-Potenz), und zweitens an der Arithmetik des quadratischen Zahlkörpers $\mathbb{Q}(\sqrt{3})$. Auf den ersten Blick hat dieser Körper nichts mit dem Lucas-Lehmer-Test zu tun; schaut man aber ein zweites mal hin, bemerkt man folgendes:

Lemma 3.15. *Sei $\omega = 2 + \sqrt{3}$ (dies ist die Grundeinheit von $\mathbb{Z}[\sqrt{3}]$) und $\overline{\omega} = 2 - \sqrt{3}$ dessen Konjugierte. Dann gilt $S_{n+1} = \omega^{2^n} + \overline{\omega}^{2^n}$ für alle $n \geq 0$.*

Beweis. Vollständige Induktion. □

Damit ist die Verbindung zur Arithmetik von $\mathbb{Z}[\sqrt{3}]$ hergestellt; dieser wollen wir uns jetzt näher widmen.

37455059850181093658177663009631318139 3 auch heute noch einiges an Rechenzeit. Eine Tabelle mit allen bekannten Faktoren von Mersenne-Zahlen $2^n - 1$ findet man auf `ftp://ftp.ox.ac.uk/pub/math/cunningham/2-`. Das kleinste n, für das $2^n - 1$ nicht vollständig faktorisiert ist, ist $n = 571$; nach Abdivision der beiden Faktoren 5711 und 27409 bleibt eine zusammengesetzte Zahl mit 164 Dezimalstellen [Mitte 1998 ist $n = 601$ der "kleinste Verbrecher"]. Für mehr über Mersenne-Zahlen schaue man sich `http://www.scruznet.com/~luke/mersenne.htm` an.

[6] François Edouard Anatole Lucas, 1842–1891; französischer Mathematiker. Er zeigte mit seinem Test, daß $2^{127} - 1$ prim ist.

[7] D. Lehmer, amerikanischer Mathematiker.

Die Arithmetik in $\mathbb{Z}[\sqrt{3}\,]$

Wir beginnen damit zu zeigen, daß $R = \mathbb{Z}[\sqrt{3}\,]$ normeuklidisch ist. Sei dazu $\xi = x + y\sqrt{3} \in k = \mathbb{Q}(\sqrt{3}\,)$ und $\alpha = a + b\sqrt{3} \in R$ (also $a, b \in \mathbb{Z}$) so gewählt, daß $|x-a|, |y-b| \leq \frac{1}{2}$ gilt. Dann wird $|N(\xi - \alpha)| = |(x-a)^2 - 3(y-b)^2| \leq \frac{3}{4}$ wegen $(x-a)^2 - 3(y-b)^2 \leq (x-a)^2 \leq \frac{1}{4}$ und $(x-a)^2 - 3(y-b)^2 \geq -3(y-b)^2 \geq -\frac{3}{4}$. Insbesondere ist R normeuklidisch.

Proposition 3.16. *Sei q eine rationale Primzahl, die auch in R prim ist. Dann ist R/qR ein endlicher Körper mit q^2 Elementen.*

Beweis. Daß der Restklassenring modulo qR höchstens q^2 Elemente besitzt, ist klar, da jedes ganze $a + b\sqrt{3}$ zu einem Element von $\{r + s\sqrt{3} : 0 \leq r, s \leq q-1\}$ kongruent modulo qR ist. Weiter sieht man sofort, daß keine zwei Elemente dieser Menge kongruent modulo q sind, d.h. der Restklassenring hat wirklich q^2 Elemente. Schließlich ist R/qR nullteilerfrei: aus $\alpha\beta \equiv 0 \bmod qR$ folgt ja, weil q prim ist, immer $\alpha \equiv 0 \bmod qR$ oder $\beta \equiv 0 \bmod qR$.

Es genügt daher zu zeigen, daß nullteilerfreie endliche Ringe automatisch Körper sind. Das einzige, was nachzuweisen ist, ist die Existenz eines Inversen Elements. Sei also A ein endlicher Integritätsbereich und $a \neq 0$. Wegen der Endlichkeit von A müssen in der Folge $a, a^2, \ldots, a^m$ irgendwann zwei Elemente gleich sein, d.h. es gibt $i < j$ mit $a^i = a^j$. Wegen der Nullteilerfreiheit darf man kürzen, d.h. es ist $a^{j-i} = 1$. Damit ist aber a^{j-i-1} ein Inverses von a. □

Ist p eine ungerade Primzahl und $p \nmid m$, so folgt aus $m^{p-1} \equiv 1 \bmod p$ und der Tatsache, daß die Gleichung $x^2 - 1$ in einem Körper (wie z.B. $\mathbb{Z}/p\mathbb{Z}$) genau zwei Nullstellen hat, daß $m^{(p-1)/2} \equiv \pm 1 \bmod p$. Wir definieren daher ein Symbol $(\frac{m}{p}) = \pm 1$ dadurch, daß wir $m^{(p-1)/2} \equiv (\frac{m}{p}) \bmod p$ verlangen.

Hilfssatz 3.17. *Es ist $(\frac{-3}{p}) = +1$, falls $p \equiv 1 \bmod 3$, und $(\frac{-3}{p}) = -1$, falls $p \equiv -1 \bmod 3$.*

Beweis. Sei $p \equiv 1 \bmod 3$; dann ist $x^2 \equiv -3 \bmod p$ lösbar, wie wir gezeigt haben. Erhebt man dies in die $\frac{p-1}{2}$-te Potenz, so folgt $(-3)^{(p-1)2} \equiv x^{p-1} \equiv 1 \bmod p$, also $(\frac{-3}{p}) = 1$.

Ist aber $p \equiv 2 \bmod 3$, so muß $(\frac{-3}{p}) = -1$ gelten: denn wäre $(\frac{-3}{p}) = 1$, also $(-3)^{(p-1)/2} \equiv 1 \bmod p$, so muß -3 eine gerade Potenz einer Primitivwurzel g modulo p sein; mit anderen Worten: dann ist -3 quadratischer Rest modulo

p. Aber dann folgt aus dem Beweis von Proposition 3.6, daß $p = x^2 + 3y^2$ für ganze $x, y \in \mathbb{Z}$ gilt. Dies aber impliziert sofort $p \equiv x^2 \equiv 1 \bmod 3$. □

Korollar 3.18. *Es ist* $(\frac{3}{p}) = +1$, *falls* $p \equiv \pm 1 \bmod 12$, *und* $(\frac{3}{p}) = -1$, *falls* $p \equiv \pm 5 \bmod 12$.

Beweis. Dies folgt sofort aus $(\frac{-1}{p}) = (-1)^{(p-1)/2}$. □

Selbstverständlich folgt dies alles sofort aus dem quadratischen Reziprozitätsgesetz. Die Primelemente von $\mathbb{Z}[\sqrt{3}\,]$ bestimmt man nun wie in den Fällen $\mathbb{Z}[i]$ und $\mathbb{Z}[\rho]$:

Proposition 3.19. *Die folgenden Zahlen sind die Primelemente von* $\mathbb{Z}[\sqrt{3}\,]$*:*

1. $1 + \sqrt{3}$ *ist der Primteiler der* 2 *wegen* $2\varepsilon = (1 + \sqrt{3}\,)^2$ *mit* $\varepsilon = 2 + \sqrt{3}$*;*
2. $\sqrt{3}$ *ist der Primteiler der* 3 *wegen* $\sqrt{3}^2 = 3$*;*
3. *die Primzahlen* $q \equiv \pm 5 \bmod 12$ *sind träge;*
4. *die Primzahlen* $p \equiv \pm 1 \bmod 12$ *zerfallen in zwei verschiedene Primelemente* π *und* π'*; insbesondere läßt sich jedes prime* $p \equiv \pm 1 \bmod 12$ *in der Form* $\pm p = x^2 - 3y^2$ *darstellen.*

Proposition 3.20. *Sei* $p \nmid 4m$ *prim und* $k = \mathbb{Q}(\sqrt{m})$*; dann gilt für alle* $\alpha \in \mathcal{O}_k$

$$\alpha^p \equiv \begin{cases} \alpha \\ \overline{\alpha} \end{cases} \bmod p, \text{ falls } \left(\frac{m}{p}\right) = \begin{cases} +1 \\ -1 \end{cases} \text{ ist.}$$

Beweis. Schreiben wir $\alpha = \frac{1}{2}(a + b\sqrt{m}\,)$ mit $a, b \in \mathbb{Z}$, so folgt aus der Tatsache, daß die Binomialkoeffizienten $\binom{p}{t}$ für $1 \le t \le p-1$ alle durch p teilbar sind, sofort $(2\alpha)^p \equiv a^p + b^p\sqrt{m}^p \equiv a + (\frac{m}{p})b\sqrt{m}$, denn es ist $a^p \equiv a \bmod p$ und $\sqrt{m}^p = m^{(p-1)/2}\sqrt{m}$. Die Behauptung folgt jetzt aus $2^p \equiv 2 \bmod p$. □

Der Test von Lucas-Lehmer

Sei nun $q = M_p = 2^p - 1$ prim; wir wollen zeigen, daß der Lucas-Lehmer-Test M_p als Primzahl erkennt, d.h. daß S_{p-1} durch M_p teilbar ist. Dazu beachten wir, daß M_p wegen $p \ge 3$ ungerade sicher $\equiv 7 \bmod 8$ und außerdem $\equiv 1 \bmod 3$ ist; zusammen ergibt dies $M_p \equiv 7 \bmod 24$. Wir behaupten, daß M_p in $\mathbb{Z}[\sqrt{3}\,]$ irreduzibel ist. Wäre nämlich $M_p = \pi\pi'$ mit $\pi = a + b\sqrt{3}$, so müßte

$a^2-3b^2 = N\pi = \pm M_p$ gelten; wegen $M_p \equiv 1 \bmod 3$ und $a^2-3b^2 \equiv 0,1 \bmod 3$ kann nur das positive Vorzeichen richtig sein, aber dann ist $a^2-3b^2 \equiv a^2+b^2 \equiv 0,1 \bmod 4$ im Widerspruch dazu, daß $M_p \equiv 7 \bmod 8$ ist.

Da $R = \mathbb{Z}[\sqrt{3}\,]$ ein ZPE-Ring ist, ist M_p nicht nur irreduzibel, sondern prim in R. Ist $q \geq 5$ irgendein Primelement in R, so folgt $(a + b\sqrt{3}\,)^q \equiv a+(\frac{3}{q})b\sqrt{3} \bmod qR$, also $(a+b\sqrt{3}\,)^q \equiv a-b\sqrt{3} \bmod qR$ für $q \equiv 7 \bmod 24$. Für $a = 2$, $b = 1$ liefert dies $\omega^q \equiv \overline{\omega} \bmod qR$ und somit $\omega^{q+1} \equiv \omega\overline{\omega} = 1 \bmod qR$. Da R/qR ein Körper ist, gibt es genau zwei Quadratwurzeln der 1, nämlich 1 und -1; insbesondere ist $\omega^{(q+1)/2} \equiv \pm 1$. Wir behaupten, daß das negative Vorzeichen gilt.

Dazu beachten wir, daß $2\omega = 4 + 2\sqrt{3} = (1 + \sqrt{3}\,)^2$ ein Quadrat ist; es folgt $2^{(q+1)/2}\omega^{(q+1)/2} = (1 + \sqrt{3}\,)^{q+1}$. Die Binomialentwicklung zeigt jetzt $(1+\sqrt{3}\,)^q \equiv 1+\sqrt{3}^q = 1+3^{(q-1)/2}\sqrt{3} \bmod q$. Nach Hilfssatz 3.17 ist $3^{(q-1)/2} = -(-3)^{(q-1)/2} \equiv -1 \bmod q$, folglich $(1 + \sqrt{3}\,)^{q+1} \equiv (1 + \sqrt{3}\,)(1 - \sqrt{3}\,) = -2 \bmod qR$. Wegen $2^{(q+1)/2} = 2 \cdot 2^{(q-1)/2} \equiv 2 \bmod q$ ist also schließlich

$$\omega^{(q+1)/2} = 2^{-(q+1)/2}(1 + \sqrt{3}\,)^{q+1} \equiv -1 \bmod qR$$

wie behauptet. Mit $\omega\overline{\omega} = 1$ folgt also

$$S_{p-1} = \omega^{(q+1)/4} + \overline{\omega}^{(q+1)/4} = \omega^{(q+1)/4}\big(1 + \omega^{-(q+1)/2}\big) \equiv 0 \bmod qR.$$

Ist umgekehrt $S_{p-1} \equiv 0 \bmod q$, so muß, wie wir eben gesehen haben, $\omega^{(q+1)/2} \equiv -1 \bmod qR$ sein. Da $\frac{q+1}{2} = 2^{p-1}$ eine 2-Potenz ist, muß $\frac{q+1}{2}$ der kleinste Exponent $n > 0$ sein, für den $\omega^n \equiv -1 \bmod qR$ wird. Andererseits gilt für jeden Teiler $\ell \mid q$ dieselbe Kongruenz $\omega^{(q+1)/2} \equiv -1 \bmod e \ll R$, und wieder ist der Exponent $\frac{q+1}{2}$ minimal. Andererseits ist entweder $\omega^{\ell+1} \equiv 1 \bmod \ell R$ oder $\omega^{\ell-1} \equiv 1 \bmod \ell R$ nach Proposition 3.20, d.h. es ist $\ell - 1 \geq 2\frac{q+1}{2} = q + 1$ oder $\ell + 1 \geq 2q + 1$. Der erste Fall ist unmöglich, der zweite zeigt $\ell \geq q$, d.h. jeder Teiler von q ist $\geq q$; mit anderen Worten: q ist prim.

3.7 * Euklidische Quadratische Zahlkörper

Unter den quadratischen Zahlkörpern gibt es nicht sehr viele, von denen man weiß, daß sie euklidisch sind; im Falle imaginärquadratischer Körper kann man sie jedoch alle bestimmen: es sind $\mathbb{Q}(\sqrt{m}\,)$ für $m = -1$, -2, -3, -7, -11 (Beweis als Übung).

Man kann zeigen, daß die restlichen imaginärquadratischen Zahlkörpern nicht nur nicht normeuklidisch sind, sondern überhaupt keine euklidische

Funktion besitzen. Trotzdem sind die Ringe ganzer Zahlen in den Körpern mit $m = -19, -43, -67, -163$ noch ZPE-Ringe. Wir werden dies später umsonst bekommen, daher verzichten wir hier auf einen (möglichen, aber mühsamen) Beweis.

Im reellquadratischen Fall liegen die Dinge nicht so einfach: die Klassifikation aller normeuklidischen (hier: euklidisch bezüglich des Betrags der Norm) quadratischen Zahlkörper war im wesentlichen Anfang der 50er Jahre abgeschlossen. Hier ist das Ergebnis:

Satz 3.21. *Die Ringe ganzer Zahlen in* $\mathbb{Q}(\sqrt{m})$*,* $m > 0$*, sind normeuklidisch genau für* $m = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$.

Im Gegensatz zum imaginärquadratischen Fall ist es aber durchaus möglich, daß es noch andere Ringe gibt, die euklidisch sind. Tatsächlich erwartet man (und kann es unter der Annahme der Richtigkeit der verallgemeinerten Riemannschen Vermutung sogar beweisen), daß jeder reellquadratische ZPE-Ring euklidisch ist. Der einzige, der in obiger Liste nicht auftaucht und für den man dies wirklich zeigen kann, ist $\mathbb{Q}(\sqrt{69})$.

Daß die in Satz 3.21 angegebenen Ringe auch wirklich normeuklidisch sind, ist nur für kleine Werte von $\operatorname{disc} k$ leicht nachzuweisen; läßt man den Computer als Hilfsmittel zu, kann man in wenigen Minuten nachrechnen, daß die angegebenen Ringe normeuklidisch sind. Der Beweis, daß es alle andern nicht sind, ist allerdings auch heute noch ziemlich verwickelt.

Ein direkter Nachweis der ZPE-Eigenschaft quadratischer Zahlringe wird durch ein auf Dedekind[8] und Hasse[9] zurückgehendes Kriterium ermöglicht:

Satz 3.22. *Sei* k *ein quadratischer Zahlkörper; dann ist* $\mathcal{O}_k$ *genau dann ein ZPE-Ring, wenn es für alle* $\alpha, \beta \in \mathcal{O}_k \setminus \{0\}$ *mit* $\beta \nmid \alpha$ *Elemente* $\gamma, \delta \in \mathcal{O}_k$ *gibt mit* $0 < |N(\alpha\gamma - \beta\delta)| < |N\beta|$.

Mit diesem Kriterium kann man (wenn auch mit Müh und Not) folgendes beweisen:

[8] Richard Dedekind (1831–1916) war der erste Algebraiker; Begriffe wie Ring, Körper und insbesondere Ideal gehen auf ihn zurück.

[9] Helmut Hasse (1898–1979) ist einer der ganz großen Zahlentheoretiker dieses Jahrhunderts. Das Lokal-Global-Prinzip, explizite Reziprozitätsgesetze, oder die Riemannsche Vermutung für elliptische Kurven waren Ergebnisse, die unser Bild der Mathematik nachhaltig geprägt haben, sich aber ohne tiefere Kenntnisse der algebraischen Zahlentheorie nur unzureichend erklären lassen.

Satz 3.23. *Sei k quadratischer Zahlkörper mit Diskriminante d; setze $M_k = \sqrt{d/5}$, falls $d > 0$, und $M_k = \sqrt{-d/3}$, falls $d < 0$. Dann ist $\mathcal{O}_k$ ein ZPE-Ring genau dann, wenn für alle Primzahlen $p < M_k$ und $(d/p) \neq -1$ Elemente $\pi \in \mathcal{O}_k$ existieren mit $|N\pi| = p$.*

Übung. Zeige damit, daß $\mathcal{O}_k$ für $d = -19, -43, -67, -163$ ZPE-Ring ist.

Es ist ein nicht ganz einfach zu beweisender Satz (von Heegner, Stark und Baker), daß es jenseits von -163 keinen imaginärquadratischen Körper mehr gibt, dessen Maximalordnung ein ZPE-Ring ist.

Zusammenfassung

In diesem Kapitel standen Anwendungen im Vordergrund. Merken sollte man sich,

- daß $\mathbb{Z}[i]$ und $\mathbb{Z}[\rho]$ normeuklidische Ringe sind, und daß der Zerfall von Primzahlen p in diesen Ringen mit den Darstellungen von p in der Form $x^2 + y^2$, bzw. $x^2 + 3y^2$ oder $L^2 + 27M^2$ zusammenhängt.
- daß die Pellsche Gleichung $x^2 - my^2 = 1$ für jede quadratfreie natürliche Zahl nichttrivial lösbar ist, und daß die Einheitengruppe reellquadratischer Zahlkörper $\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ ist.

Kapitel 4

Idealarithmetik in quadratischen Zahlkörpern

4.1 Motivation

In Kapitel 2 haben wir gesehen, daß die Zerlegung $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ ein Beispiel für nichteindeutige Faktorisierung in irreduzible Elemente im Ring $R = \mathbb{Z}[\sqrt{-5}]$ ist. Das Problem ist, daß 2 und $1+\sqrt{-5}$, obwohl sie beide irreduzibel sind und, da sie nicht assoziiert sind, teilerfremd sind, einen gemeinsamen "Faktor" zu besitzen scheinen: so ist z.B. $(1+\sqrt{-5})^2 = -4+2\sqrt{-5}$) durch 2 teilbar.

Wäre R ein Hauptidealring, so könnte man diesen gemeinsamen Faktor sofort hinschreiben: wäre $(2, 1+\sqrt{-5}) = (\alpha)$, so wäre $\alpha \sim \text{ggT}\,(2, 1+\sqrt{-5})$. Nun ist aber R kein Hauptidealring, und $(2, 1+\sqrt{-5})$ ist kein Hauptideal. Dedekinds Idee war es, das Ideal $(2, 1+\sqrt{-5})$ als den "richtigen" gemeinsamen Teiler von 2 und $(1+\sqrt{-5})$ zu betrachten. Bevor wir aber sagen können, wann ein Ideal eine Zahl (bzw. das von dieser Zahl erzeugte Ideal) teilt, müssen wir erst das Produkt von Idealen definieren.

Das ist ganz einfach: Sind A, B Ideale in einem Ring R, so ist $AB = \{\alpha_1\beta_1 + \ldots + \alpha_m\beta_m : \alpha_j \in A, \beta_j \in B\}$, also die Menge der endlichen Summen von Produkten $\alpha_j\beta_j$, wieder ein Ideal in R. Man rechnet leicht nach, daß damit $(\alpha_1, \ldots, \alpha_m)(\beta_1, \ldots, \beta_n) = (\alpha_1\beta_1, \alpha_1\beta_2, \ldots, \alpha_m\beta_n)$ gilt; insbesondere ist $(\alpha)(\beta) = (\alpha\beta)$, d.h. Hauptideale multiplizieren sich wie gewünscht. Ohne Probleme rechnet man die folgenden Eigenschaften nach:

Proposition 4.1. *Sind A, B, C Ideale in einem Ring R, so gilt $AB = BA$,*

$(AB)C = A(BC)$ *und* $AR = A(1) = A$.

In quadratischen Zahlkörpern kann man zu einem Ideal $\mathfrak{a}$ darüberhinaus noch das zu $\mathfrak{a}$ konjugierte Ideal $\mathfrak{a}^\sigma = \mathfrak{a}'$ definieren, das aus allen α' besteht, für die $\alpha \in \mathfrak{a}$ ist. Wieder rechnet man problemlos nach, daß Konjugation mit Multiplikation vertauschbar ist, d.h. daß $(\mathfrak{ab})^\sigma = \mathfrak{a}^\sigma \mathfrak{b}^\sigma$ gilt.

Das Rechnen mit Idealen ist etwas gewöhnungsbedürftig, aber nicht schwer: betrachten wir z.B. die Ideale $\mathfrak{a} = (2, 1+\sqrt{-5})$, $\mathfrak{b} = (3, 1+\sqrt{-5})$ und $\mathfrak{c} = (3, 1-\sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$. Dann ist

$$\begin{aligned} \mathfrak{a}^2 &= (2\cdot 2, 2(1+\sqrt{-5}), 2(1+\sqrt{-5}), -4+2\sqrt{-5}) \\ &= (4, 2(1+\sqrt{-5}), -4+2\sqrt{-5}) \\ &= (2)(2, 1+\sqrt{-5}, -2+\sqrt{-5}); \end{aligned}$$

im letzten Ideal ist aber $\sqrt{-5} = 2 + (-2+\sqrt{-5})$ und damit auch $1 = (1+\sqrt{-5}) - \sqrt{5}$ enthalten, d.h. es ist $\mathfrak{a}^2 = (2)(1) = (2)$.

Ähnlich ist

$$\begin{aligned} \mathfrak{bc} &= (9, 3(1+\sqrt{-5}), 3(1-\sqrt{-5}), 6) \\ &= (3)(3, 1+\sqrt{-5}, 1-\sqrt{-5}, 2) \\ &= (3)(1) = (3). \end{aligned}$$

Etwas weniger offensichtlich ist

$$\begin{aligned} \mathfrak{b}^2 &= (9, 3(1+\sqrt{-5}), (1+\sqrt{-5})^2) \\ &= (2+\sqrt{-5})(2-\sqrt{-5}, 1-\sqrt{-5}, -2) \\ &= (2+\sqrt{-5}). \end{aligned}$$

Übung. Man verifiziere $\mathfrak{ab} = (1+\sqrt{-5})$, $\mathfrak{ac} = (1-\sqrt{-5})$, und $\mathfrak{c}^2 = (2-\sqrt{-5})$.

Betrachten wir noch einmal die Ausgangsgleichung: $2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. Nimmt man auf beiden Seiten das von diesen Zahlen erzeugte Ideal, so folgt $(2)(3) = (2\cdot 3) = (1+\sqrt{-5})(1-\sqrt{-5})$ (daß hier auf der rechten Seite das Produkt zweier Ideale steht und nicht das zweier Zahlen, ist nur im Zusammenhang mit der linken Seite zu erkennen). Setzen wir $(2) = \mathfrak{a}^2$ und $(3) = \mathfrak{bc}$ ein, so folgt die Idealgleichung $(6) = \mathfrak{a}^2\mathfrak{bc}$; gruppiert man die Faktoren in der Form $\mathfrak{a}^2 \cdot (\mathfrak{bc})$, so erhält man die Zerlegung $(6) = (2)(3)$ in

zwei Hauptideale; dagegen liefert $(\mathfrak{ab})(\mathfrak{ac}) = (1+\sqrt{-5})(1-\sqrt{-5})$ die zweite Zerlegung in Hauptideale.

Wir sehen: die wesentlich verschiedenen Faktorisierungen auf Zahlniveau entsprechen den verschiedenen Gruppierungen von Idealfaktoren, und die Zerlegung des Ideals in die "Primideale" $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ scheint eindeutig zu sein. Daß dies kein spezielles Phänomen in $\mathbb{Z}[\sqrt{-5}]$ ist, wollen wir im nächsten Abschnitt zeigen.

Übung. Erkläre $2 \cdot 3 = -\sqrt{-6}^2$ durch Faktorisierung in Ideale.

Übung. Sei $K = \mathbb{Q}(\sqrt{-23})$; zeige $(2) = \mathfrak{a}\mathfrak{a}'$ für $\mathfrak{a} = (2, \frac{1+\sqrt{-23}}{2})$ und $\mathfrak{a}^3 = (\frac{3-\sqrt{-23}}{2})$. Warum kann $\mathfrak{a}^2$ kein Hauptideal sein?

4.2 Eindeutige Primidealzerlegung

Die Idealnorm

Wir beginnen mit der Beobachtung, daß jedes Ideal in $\mathcal{O}_K$ von höchstens zwei Elementen erzeugt wird. (Im allgemeinen ist das nicht richtig: man betrachte z.B. das Ideal (X_1, X_2, X_3) im Polynomring $\mathbb{Z}[X_1, X_2, X_3, X_4]$.)

Proposition 4.2. *Sei $\mathfrak{a} \subset \mathcal{O}_K$ ein $\mathbb{Z}$-Modul in $\mathcal{O}_K$, also eine additive Untergruppe von $\mathcal{O}_K$. Dann gibt es $m, n \in \mathbb{N}_0$ und $a \in \mathbb{Z}$ mit $\mathfrak{a} = n\mathbb{Z} \oplus (a + m\omega)\mathbb{Z}$ (d.h. jeder solche $\mathbb{Z}$-Modul besitzt eine $\mathbb{Z}$-Basis).*

Ist $\mathfrak{a} \neq (0)$ sogar Ideal, dann gilt $m \mid n$, $m \mid a$ (also $a = mb$ für ein $b \in \mathbb{Z}$) und $n \mid m \cdot N(b+\omega)$. Insbesondere wird jedes Ideal in $\mathcal{O}_K$ von höchstens zwei Elementen erzeugt.

Beweis. Wir betrachten die Untergruppe $H = \{s : r + s\omega \in \mathfrak{a}\}$ von $\mathbb{Z}$. Jedes solche H hat die Form $H = m\mathbb{Z}$ für ein $m \geq 0$, und nach Konstruktion gibt es ein $a \in \mathbb{Z}$ mit $a + m\omega \in \mathfrak{a}$. Weiter ist auch $\mathfrak{a} \cap \mathbb{Z}$ eine Untergruppe von $\mathbb{Z}$, also $\mathfrak{a} \cap \mathbb{Z} = n\mathbb{Z}$ für ein $n \geq 0$. Wir behaupten nun, daß $\mathfrak{a} = n\mathbb{Z} \oplus (a + m\omega)\mathbb{Z}$ ist. Die Inklusion $\supseteq$ ist klar; sei also $r + s\omega \in \mathfrak{a}$. Wegen $s \in H$ ist dann $s = um$ für ein $u \in \mathbb{Z}$, und dann ist $r - ua = r + s\omega - u(a + m\omega) \in \mathfrak{a} \cap \mathbb{Z}$, also $r - ua = vn$. Nun folgt aber $r + s\omega = r - ua + u(a + m\omega) = vn + u(a + m\omega) \in n\mathbb{Z} \oplus (a + m\omega)\mathbb{Z}$.

Ab jetzt nehmen wir an, $\mathfrak{a}$ sei ein Ideal. Mit $c \in \mathfrak{a} \cap \mathbb{Z}$ ist dann auch $c\omega \in \mathfrak{a}$, nach Definition von H als den 'Koeffizienten von ω' von Elementen in $\mathfrak{a}$ also $c \in H$. Dies zeigt $n\mathbb{Z} = \mathfrak{a} \cap \mathbb{Z} \subseteq H = m\mathbb{Z}$, also $m \mid n$ (sind die Vielfachen von

n in den Vielfachen von m enthalten, muß m ein Teiler von n sein; diesem "Teilen bedeutet Enthalten" werden wir noch des öfteren begegnen).

Um $m \mid a$ zu zeigen, stellen wir fest, daß $\omega^2 = x + y\omega$ für $x, y \in \mathbb{Z}$ gilt: $\{1, \omega\}$ ist ja Ganzheitsbasis. Da $\mathfrak{a}$ Ideal ist, ist mit $a + m\omega$ auch $(a + m\omega)\omega = mx + (a + my)\omega \in A$, nach Definition von H also $amy \in H$ und somit $a + my$ ein Vielfaches von m: dies impliziert sofort $m \mid a$, also $a = mb$ für ein $b \in \mathbb{Z}$.

Um die letzte Teilbarkeitsbeziehung nachzuweisen, setzen wir $\alpha = a + m\omega = m(b + \omega)$. Mit $\alpha \in \mathfrak{a}$ ist natürlich erst recht $\alpha(b + \omega')$ im Ideal $\mathfrak{a}$ enthalten. Wegen $\frac{1}{m} N\alpha = m(b + \omega)(b + \omega') \in \mathfrak{a} \cap \mathbb{Z}$ ist $\frac{1}{m} N\alpha$ also Vielfaches von n. □

Unser nächstes Ziel ist die Aussage, daß die "Norm" $\mathfrak{a}\mathfrak{a}'$ eines Ideals $\mathfrak{a}$ von einem Element in $\mathbb{Z}$ erzeugt wird. Für Hauptideale ist dies wegen $(\alpha)(\alpha)' = (\alpha)(\alpha') = (\alpha\alpha') = (N\alpha)$ klar.

Proposition 4.3. *Sei $\mathfrak{a} \neq (0)$ ein Ideal in $\mathcal{O}_K$; dann gibt es ein $a \in \mathbb{N}$ mit $\mathfrak{a}\mathfrak{a}' = (a)$.*

Bemerkung. Auch hier ist die Bezeichnung (a) etwas ungenau, da hieraus nicht hervorgeht, ob man das Ideal (a) in $\mathbb{Z}$ oder das von a in $\mathcal{O}_K$ erzeugte Ideal meint; dies ist wieder aus dem Zusammenhang zu erschließen. Oben ist selbstverständlich das Ideal $(a) = a\mathcal{O}_K$ gemeint, da auf der linken Seite ebenfalls ein Ideal in $\mathcal{O}_K$ steht.

Zum Beweis von Proposition 4.3 verwenden wir den folgenden Hilfssatz von Hurwitz:

Hilfssatz 4.4. *Seien $\alpha, \beta \in \mathcal{O}_K$ und $m \in \mathbb{N}$. Sind $N\alpha$, $N\beta$ und $\operatorname{Tr} \alpha\beta'$ durch m teilbar, dann gilt $m \mid \alpha\beta'$ und $m \mid \alpha'\beta$.*

Beweis. Sei $\gamma = \alpha\beta'/m$; dann ist $\gamma' = \alpha'\beta/m$, und wir wissen, daß $\gamma + \gamma' = (\operatorname{Tr} \alpha\beta')/m$ und $\gamma\gamma' = \frac{N\alpha}{m}\frac{N\beta}{m}$ ganze Zahlen sind. Da mit Norm und Spur einer Zahl auch die Zahl selbst ganzalgebraisch ist, folgt $\gamma \in \mathcal{O}_K$ und damit die Behauptung. □

Beweis von 4.3. Wir schreiben $\mathfrak{a} = (\alpha, \beta)$ für $\alpha, \beta \in \mathcal{O}_K$ (dies geht wegen Proposition 4.2). Dann ist $\mathfrak{a}' = (\alpha', \beta')$ und somit $\mathfrak{a}\mathfrak{a}' = (N\alpha, \alpha\beta', \alpha'\beta, N\beta)$. Setzen wir $a = \operatorname{ggT}(N\alpha, N\beta, \operatorname{Tr} \alpha\beta')$ (in $\mathbb{Z}$), so zeigt der Hilfssatz von Hurwitz, daß $\frac{\alpha\beta'}{a}$ und $\frac{\alpha'\beta}{a}$ ganz sind; wir erhalten also $\mathfrak{a}\mathfrak{a}' = (a)(\frac{N\alpha}{a}, \frac{N\beta}{a}, \frac{\alpha\beta'}{a}, \frac{\alpha'\beta}{a})$,

wobei das letzte Ideal wegen Hurwitz in $\mathcal{O}_K$ liegt. Um $\mathfrak{a}\mathfrak{a}' = (a)$ zu beweisen, genügt also der Nachweis von $1 \in (\frac{N\alpha}{a}, \frac{N\beta}{a}, \frac{\alpha\beta'}{a}, \frac{\alpha'\beta}{a})$. Aber 1 ist als $\mathbb{Z}$-Linearkombination von $\frac{N\alpha}{a}$, $\frac{N\beta}{a}$ und $\frac{\operatorname{Tr}\alpha\beta'}{a}$ erst recht $\mathcal{O}_K$-Linearkombination von $\frac{N\alpha}{a}$, $\frac{N\beta}{a}$ und $\frac{\alpha\beta'}{a} + \frac{\alpha'\beta}{a}$: die Behauptung folgt. □

Die natürliche Zahl m in Proposition 4.3 nennt man die Norm des Ideals $\mathfrak{a}$; es ist also $\mathfrak{a}\mathfrak{a}' = (N\mathfrak{a})$. Wegen $(N\mathfrak{a}\mathfrak{b}) = (\mathfrak{a}\mathfrak{b})(\mathfrak{a}\mathfrak{b})' = (\mathfrak{a}\mathfrak{a}')(\mathfrak{b}\mathfrak{b}') = (N\mathfrak{a})(N\mathfrak{b})$ ist die Idealnorm multiplikativ. Weitere wichtige Eigenschaften:

- $N\mathfrak{a} = 1 \iff \mathfrak{a} = (1)$: denn ist $N\mathfrak{a} = 1$, so folgt $(1) = \mathfrak{a}\mathfrak{a}' \subseteq \mathfrak{a} \subseteq \mathcal{O}_K = (1)$, und die Umkehrung ist klar.

- $N\mathfrak{a} = 0 \iff \mathfrak{a} = (0)$: denn aus $\mathfrak{a}\mathfrak{a}' = (0)$ folgt $N\alpha = \alpha\alpha' = 0$ für alle $\alpha \in \mathfrak{a}$.

- ist $\mathfrak{a} = n\mathbb{Z} + m(b+\omega)\mathbb{Z}$ wie in Prop. 4.2, so ist $N\mathfrak{a} = mn$. Beweis: sei $\alpha = m(b+\omega)$; dann ist $\mathfrak{a} = (n, \alpha)$, $\mathfrak{a}' = (n, \alpha')$ und $\mathfrak{a}\mathfrak{a}' = (n^2, mn(b+\omega'), mn(b+\omega), m^2N(b+\omega)) = (mn)(\frac{n}{m}, b+\omega, b+\omega', \frac{1}{n}N(b+\omega))$. Wegen Proposition 4.2 ist das letzte Ideal $\subseteq \mathcal{O}_K$, also $(N\mathfrak{a}) = \mathfrak{a}\mathfrak{a}' \subseteq (mn)\mathcal{O}_K = (mn)$ und daher $mn \mid N\mathfrak{a}$.

  Für die andere Richtung $N\mathfrak{a} \mid mn$ geht man so vor: Sei $A = N\mathfrak{a}$, also $\mathfrak{a}\mathfrak{a}' = (A)$. Wegen $\alpha \in \mathfrak{a}$ und $n \in \mathfrak{a}'$ ist $n\alpha \in \mathfrak{a}\mathfrak{a}' = (A)$, also $A \mid n\alpha = na + nm\omega$; da $\{1, \omega\}$ eine Ganzheitsbasis von $\mathcal{O}_K$ ist, impliziert dies $A \mid na$ und $A \mid nm$.

Die Kürzungsregel

Jetzt wenden wir uns dem Satz der eindeutigen Primidealzerlegung zu. Die Beweisidee ist dieselbe wie im Zahlfall; während wir aber dort aus $\alpha\beta = \alpha\gamma$ mit $\alpha \neq 0$ sofort schließen können, daß $\beta = \gamma$ gilt (wir brauchen ja nur mit dem Inversen von α zu multiplizieren), können wir dies im Idealfall noch nicht, weil wir (noch) kein "inverses Ideal" $\mathfrak{a}^{-1}$ zur Verfügung haben. Daß diese "Kürzungsregel" dennoch richtig ist, ist der Inhalt von

Proposition 4.5. *Sind $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ Ideale $\neq (0)$ in $\mathcal{O}_K$ und gilt $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c}$, so folgt $\mathfrak{b} = \mathfrak{c}$.*

Beweis. Die Idee ist, die Kürzungsregel für Ideale auf diejenige für Zahlen zurückzuführen; der Weg dorthin läuft natürlich über Hauptideale.

Sei daher zuerst $\mathfrak{a} = (\alpha)$ ein Hauptideal; dann ist $\alpha\mathfrak{b} = \mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c} = \alpha\mathfrak{c}$. Für jedes $\beta \in \mathfrak{b}$ ist also $\alpha\beta \in \alpha\mathfrak{c}$, folglich existert ein $\gamma \in \mathfrak{c}$ mit $\alpha\beta = \alpha\gamma$. Dies zeigt $\beta = \gamma \in \mathfrak{c}$, somit $\mathfrak{b} \subseteq \mathfrak{c}$. Aus Symmetriegründen muß dann $\mathfrak{b} = \mathfrak{c}$ sein.

Ist $\mathfrak{a}$ ein beliebiges Ideal, so impliziert $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c}$ sofort, daß $(\mathfrak{a}\mathfrak{a}')\mathfrak{b} = (\mathfrak{a}\mathfrak{a}')\mathfrak{c}$ ist; da $\mathfrak{a}\mathfrak{a}' = (N\mathfrak{a})$ ein Hauptideal ist, folgt die Behauptung aus dem ersten Teil des Beweises. □

Damit bilden die Ideale in $\mathcal{O}_K$ eine Halbgruppe mit Kürzungsregel; solche Objekte kann man formal zu einer Gruppe machen, indem man die Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$ imitiert. Man kann einem Element $\mathfrak{a}\mathfrak{b}^{-1}$ dieser Gruppe aber auch eine Menge zuordnen, indem man $\mathfrak{a}\mathfrak{b}^{-1} = \frac{1}{b}\mathfrak{a}\mathfrak{b}'$ setzt, wo b die Norm von $\mathfrak{b}$ ist, und allgemein $\frac{1}{m}\mathfrak{a} = \{\frac{\alpha}{m} : \alpha \in \mathfrak{a}\}$ definiert. Solche Mengen nennt man auch 'gebrochene Ideale'.

Teilbarkeit von Idealen

Nachdem wir Produkte von Idealen definiert haben, können wir uns Teilbarkeitsfragen widmen. Selbstverständlich sagen wir, ein Ideal $\mathfrak{b}$ sei durch ein Ideal $\mathfrak{a}$ teilbar, wenn es ein Ideal $\mathfrak{c}$ gibt mit $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$. Wegen $\mathfrak{c} \subseteq \mathcal{O}_K$ folgt aus $\mathfrak{a} \mid \mathfrak{b}$ also, daß $\mathfrak{b} = \mathfrak{a}\mathfrak{c} \subseteq \mathfrak{a}(1) = \mathfrak{a}$ ist, d.h. Teilen impliziert Enthalten. Tatsächlich gilt auch die Umkehrung:

Proposition 4.6. *Sind $\mathfrak{a}, \mathfrak{b}$ Ideale $\neq (0)$ mit $\mathfrak{a} \supseteq \mathfrak{b}$, so ist $\mathfrak{a} \mid \mathfrak{b}$.*

Beweis. Aus $\mathfrak{a} \supseteq \mathfrak{b}$ folgt $\mathfrak{b}\mathfrak{a}' \subseteq \mathfrak{a}\mathfrak{a}' = (a)$ mit $a = N\mathfrak{a}$. Dann ist $\mathfrak{c} = \frac{1}{a}\mathfrak{b}\mathfrak{a}'$ ein Ideal wegen $\frac{1}{a}\mathfrak{a}'\mathfrak{b} \subseteq \mathcal{O}_K$ (die Idealeigenschaften sind einfach nachzuweisen). Aus $\mathfrak{a}\mathfrak{c} = \frac{1}{a}\mathfrak{b}\mathfrak{a}\mathfrak{a}' = \mathfrak{b}$ folgt jetzt die Behauptung. □

Aus der kommutativen Algebra sind die Begriffe irreduzible, maximale und prime Ideale bekannt: Ein Ideal $\mathfrak{a} \neq (1)$ heißt

- irreduzibel, wenn $\mathfrak{a} \neq \mathfrak{b}\mathfrak{c}$ für Ideale $\mathfrak{b}, \mathfrak{c} \neq (1)$ gilt;
- maximal, wenn aus $\mathfrak{a} \subseteq \mathfrak{b} \subseteq (1)$ immer $\mathfrak{b} = \mathfrak{a}$ oder $\mathfrak{b} = (1)$ folgt;
- prim, wenn aus $\mathfrak{a} \mid \mathfrak{b}\mathfrak{c}$ immer $\mathfrak{a} \mid \mathfrak{b}$ oder $\mathfrak{a} \mid \mathfrak{c}$ folgt.

In Ganzheitsringen algebraischer Zahlkörper ist man in der angenehmen Situation, daß alle drei Begriffe zusammenfallen; irreduzible und maximale Ideale sind per definitionem dasselbe:

- Irreduzible Ideale sind maximal: wäre nämlich $\mathfrak{a}$ nicht maximal, gäbe es ein Ideal $\mathfrak{b}$ mit $\mathfrak{a} \subsetneq \mathfrak{b} \subsetneq (1)$; also folgte $\mathfrak{b} \mid \mathfrak{a}$ mit $\mathfrak{b} \neq (1), \mathfrak{a}$.
- Maximale Ideale sind irreduzibel: denn aus $\mathfrak{a} = \mathfrak{bc}$ folgt $\mathfrak{a} \subsetneq \mathfrak{b} \subsetneq (1)$.

Ebenfalls aus der Definition folgt, daß maximale Ideale notwendig prim sind:

- Irreduzible (und damit maximale) Ideale sind prim: hier müssen wir eine Kleinigkeit tun. Sei $\mathfrak{a}$ irreduzibel, $\mathfrak{a} \mid \mathfrak{bc}$ und $\mathfrak{a} \nmid \mathfrak{b}$; zu zeigen ist $\mathfrak{a} \mid \mathfrak{c}$. Dazu stellen wir fest, daß das Ideal $\mathfrak{a}+\mathfrak{b} = \{\alpha+\beta : \alpha \in \mathfrak{a}, \beta \in \mathfrak{b}\}$ (man rechne nach, daß dies wirklich ein Ideal ist; sobald wir die Eindeutigkeit der Primidealzerlegung bewiesen haben werden, wird sich herausstellen, daß $\mathfrak{a}+\mathfrak{b}$ nichts anderes als der ggT von $\mathfrak{a}$ und $\mathfrak{b}$ ist) das Ideal $\mathfrak{a}$ enthält, also teilt; aber es ist $\mathfrak{a}+\mathfrak{b} \neq \mathfrak{a}$, da sonst $\mathfrak{a} = \mathfrak{a}+\mathfrak{b} \supseteq \mathfrak{b}$ und damit $\mathfrak{a} \mid \mathfrak{b}$ folgen würde im Widerspruch zur Voraussetzung. Da $\mathfrak{a}$ irreduzibel ist, muß $\mathfrak{a}+\mathfrak{b} = (1)$ sein, d.h. es gibt $\alpha \in \mathfrak{a}$ und $\beta \in \mathfrak{b}$ mit $1 = \alpha+\beta$. Ist $\gamma \in \mathfrak{c}$, so folgt $\gamma = \alpha\gamma + \beta\gamma$; nun ist $\alpha\gamma \in \mathfrak{a}$ und $\beta\gamma \in \mathfrak{bc} \subseteq \mathfrak{a}$, also $\gamma \in \mathfrak{a}$. Damit haben wir $\mathfrak{c} \subseteq \mathfrak{a}$ gezeigt, also $\mathfrak{a} \mid \mathfrak{c}$.

Dagegen benutzt der Beweis, daß Primideale in Ganzheitsringen quadratischer Zahlkörper maximal sind, die nicht allgemein gültige Proposition 4.6:

- Primideale sind irreduzibel (also maximal): denn aus $\mathfrak{a} = \mathfrak{bc}$ und $\mathfrak{a} \nmid \mathfrak{b}$ folgt $\mathfrak{a} \mid \mathfrak{c}$, wegen $\mathfrak{c} \mid \mathfrak{a}$ somit (to divide is to contain) $\mathfrak{a} = \mathfrak{c}$ und damit $\mathfrak{b} = (1)$.

Man könnte meinen, daß man aus $\mathfrak{a} \mid \mathfrak{c}$ und $\mathfrak{c} \mid \mathfrak{a}$ auch ohne 4.6 auf die Gleichheit $\mathfrak{a} = \mathfrak{c}$ kommt: denn man hat ja $\mathfrak{a} = \mathfrak{cd}$ und $\mathfrak{c} = \mathfrak{ae}$, also $\mathfrak{a} = \mathfrak{dea}$. Hieraus kann man aber (ohne Kürzungsregel) nicht auf $\mathfrak{de} = (1)$ schließen!

Jetzt können wir:

Satz 4.7. *Jedes von* (0) *verschiedene Ideal* $\mathfrak{a}$ *im Ganzheitsring* $\mathcal{O}_K$ *eines quadratischen Zahlkörpers* K *läßt sich bis auf die Reihenfolge eindeutig als Produkt von Primidealen schreiben.*

Beweis. Wir beginnen mit dem Nachweis der Existenz einer Zerlegung in irreduzible Ideale. Ist $\mathfrak{a}$ bereits irreduzibel, sind wir fertig. Andernfalls ist $\mathfrak{a} = \mathfrak{bc}$; sind $\mathfrak{b}$ und $\mathfrak{c}$ irreduzibel, sind wir fertig, andernfalls zerlegen wir weiter. Wegen $N\mathfrak{a} = N\mathfrak{b}N\mathfrak{c}$ und $1 < N\mathfrak{b}, N\mathfrak{c} < N\mathfrak{a}$ etc. muß dieses Verfahren aber irgendwann einmal abbrechen, da die Norm als natürliche Zahl nicht beliebig klein werden kann.

Seien jetzt $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$ zwei Zerlegungen von $\mathfrak{a}$ in Produkte von Primidealen. Da $\mathfrak{p}_1$ prim ist, teilt es ein $\mathfrak{q}_j$ auf der rechten Seite, z.B. $\mathfrak{p}_1 \mid \mathfrak{q}_1$; da $\mathfrak{q}_1$ irreduzibel ist, muß $\mathfrak{p}_1 = \mathfrak{q}_1$ sein, und die Kürzungsregel liefert $\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s$. Die Behauptung folgt jetzt mit Induktion. □

Bemerkung. Die Voraussetzung, daß sich alles im Ganzheitsring abspielt, ist wichtig: im Ring $R = \mathbb{Z}[\sqrt{-3}\,]$ beispielsweise gibt es keine eindeutige Zerlegung in Primideale: es ist nämlich $(2)(2) = (1+\sqrt{-3}\,)(1-\sqrt{-3}\,)$, und das Ideal (2) ist irreduzibel. Weiter kann nicht $(2) = (1+\sqrt{-3}\,)$ sein, da sonst $\frac{1+\sqrt{-3}}{2} \in R$ sein müßte.

Das Rechnen modulo Idealen I ist einfach: man schreibt $a \equiv b \bmod I$ für $a - b \in I$. Man beachte, daß dies die gewöhnliche Kongruenzrechnung verallgemeinert: ist $I = mR$ Hauptideal, so ist $a - b \in mR$ äquivalent mit $m \mid (a-b)$. Die Menge der Restklassen eines Rings modulo I bildet einen Ring, der mit R/I bezeichnet wird.

Übung. Sei $\mathfrak{a} \neq (0)$ ein Ideal in einem Zahlring $\mathcal{O}_K$; zeige, daß $N\mathfrak{a} = \#\mathcal{O}_K/\mathfrak{a}$ gilt. (Hinweis: man schreibe $\mathfrak{a} = n\mathbb{Z} \oplus m(b+\omega)\mathbb{Z}$ und rechne nach, daß $\{r + s\omega : 0 \le r < n, 0 \le s < m\}$ ein vollständiges Restsystem ist.

Übung. Sei R ein Ring; man zeige: ein Ideal $I \neq R$ ist maximal genau dann, wenn R/I ein Körper ist, und prim genau dann, wenn R/I nullteilerfrei (also ein Integritätsbereich) ist. Man beachte, daß hieraus sofort folgt, daß maximale Ideale prim sind.

Übung. Sei R ein Ring, in dem die eindeutige Zerlegun in Primideale gilt (solche Ringe heißen *Dedekind-Ringe*). Zeige: sind $\mathfrak{A}$ und $\mathfrak{B}$ teilerfremde Ideale mit $\mathfrak{AB} = \mathfrak{e}^n$, so gilt $\mathfrak{A} = \mathfrak{a}^n$ und $\mathfrak{B} = \mathfrak{b}^n$.

Übung. Seien $\mathfrak{a}$ und $\mathfrak{b}$ Ideale in $\mathcal{O}_K$. Zeige $\mathfrak{a} \cap \mathfrak{b} \supseteq \mathfrak{ab}$, und beweise, daß sogar Gleichheit gilt, falls $\mathfrak{a}$ und $\mathfrak{b}$ teilerfremd sind.

Beschreibung der Primideale

Ist $\mathfrak{p}$ ein Primideal, so gibt es genau eine Primzahl p mit $\mathfrak{p} \mid (p)$: es ist nämlich $\mathfrak{p} \mid \mathfrak{pp}' = (N\mathfrak{p})$; wenn man $N\mathfrak{p}$ in $\mathbb{Z}$ in Primfaktoren zerlegt und beachtet, daß $\mathfrak{p}$ prim ist, so folgt die Existenz von p. Daß $\mathfrak{p}$ keine zwei verschiedenen Primzahlen teilen kann, versteht sich inzwischen von selbst. Man sagt in diesem Fall, $\mathfrak{p}$ liege über p. Da das Ideal (p) Norm p^2 hat, hat jedes Primideal über p die Norm p oder p^2.

Die Bestimmung aller Primideale in $\mathcal{O}_K$ ist nicht mehr schwer: den Fall $p = 2$ erledigt die folgende

Übung. Sei $K = \mathbb{Q}(\sqrt{m})$ ein quadratischer Zahlkörper, m quadratfrei;

- ist $m \equiv 2 \bmod 4$, so ist $(2) = (2, \sqrt{m})^2$;
- ist $m \equiv 3 \bmod 4$, so ist $(2) = (2, 1 + \sqrt{m})^2$;
- ist $m \equiv 1 \bmod 8$, so ist $(2) = \mathfrak{a}\mathfrak{a}'$ mit $\mathfrak{a} = (2, \frac{1+\sqrt{m}}{2})$ und $\mathfrak{a} \neq \mathfrak{a}'$;
- ist $m \equiv 5 \bmod 8$, so ist (2) prim.

Die ersten drei Behauptungen rechnet man einfach nach, im letzten muß man zeigen, daß ein Primideal mit Norm 2 für $m \equiv 1 \bmod 4$ notwendig die Form $(2, a+\frac{1+\sqrt{m}}{2})$ hat; hieraus folgt dann $m \equiv (2a+1)^2 \bmod 8$, also $m \equiv 1 \bmod 8$.

Satz 4.8. *Sei p eine ungerade Primzahl, $K = \mathbb{Q}(\sqrt{m})$ ein quadratischer Zahlkörper, und d seine Diskriminante. Dann gilt:*

- *ist $p \mid d$, so ist $(p) = (p, \sqrt{m})^2$: p ist verzweigt;*
- *ist $(d/p) = +1$, so ist $(p) = \mathfrak{p}\mathfrak{p}'$ mit $\mathfrak{p} \neq \mathfrak{p}'$: p ist zerlegt;*
- *ist $(d/p) = -1$, so ist $(p) = \mathfrak{p}$ prim: p ist träge.*

Beweis. Sei zuerst $p \mid d$; da p ungerade ist, ist auch $p \mid m$. Jetzt folgt $(p, \sqrt{m})^2 = (p^2, p\sqrt{m}, m) = (p)(p, \sqrt{m}, \frac{m}{p}) = (p)$, da das Ideal $(p, \sqrt{m}, \frac{m}{p})$ mit p und $\frac{m}{p}$ zwei teilerfremde Zahlen enthält und somit gleich (1) ist.

Sei als nächstes $(d/p) = 1$; dann ist d und wegen $d = m$ oder $d = 4m$ auch m quadratischer Rest modulo p, d.h. es gibt ein $x \in \mathbb{Z}$ mit $x^2 \equiv d \bmod p$. Wir setzen $\mathfrak{p} = (p, x+\sqrt{m})$ und finden $\mathfrak{p}\mathfrak{p}' = (p^2, p(x+\sqrt{m}), p(x-\sqrt{m}), x^2-m) = (p)(p, x+\sqrt{m}, x-\sqrt{m}, (x^2-m)/p)$. Offenbar ist $2\sqrt{m} = x+\sqrt{m}-(x-\sqrt{m})$ und damit auch $4m = (2\sqrt{m})^2$ im letzten Ideal enthalten; da p und $4m$ teilerfremd sind, ist es das Einsideal, und wir haben $\mathfrak{p}\mathfrak{p}' = (p)$. Wäre $\mathfrak{p} = \mathfrak{p}'$, so folgte wie eben $4m \in \mathfrak{p}$ und $\mathfrak{p} = (1)$: Widerspruch.

Sei schließlich $(d/p) = -1$. Gäbe es ein Ideal $\mathfrak{p}$ der Norm p, so hätte es nach Proposition 4.2 die Gestalt $\mathfrak{p} = (p, b + \omega)$ und $p \mid N(b + \omega)$. Ist $\omega = \sqrt{m}$, bedeutet dies $b^2 - m \equiv 0 \bmod p$, $(d/p) = (4m/p) = (m/p) = +1$ im Widerspruch zur Voraussetzung. Ist $\omega = \frac{1}{2}(1 + \sqrt{m})$, so haben wir $(2b + 1)^2 \equiv m \bmod p$, und der Widerspruch folgt wie eben. □

Man kann die beiden Fälle $p = 2$ und $p \neq 2$ zusammenfassen, indem man das *Kronecker-Symbol* (d/p) einführt. Dieses stimmt für ungerade p mit dem Legendre-Symbol überein und ist für $p = 2$ und $d \equiv 1 \bmod 4$ durch $(d/2) = (-1)^{(d-1)/4}$ definiert; für $d \not\equiv 1 \bmod 4$ setzt man $(d/2) = 0$.

4.3 Die Idealklassengruppe

Definition

Wir haben gesehen, daß die Menge der ganzen Ideale $\neq (0)$ in $\mathcal{O}_K$ eine Halbgruppe mit Kürzungsregel bilden. Solche Gruppen kann man (nach dem Vorbild der Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$) formal zu einer Gruppe I_K machen, die dann die Gruppe der Hauptideale $H_K = \{(\alpha) : \alpha \in K^\times\}$ als Untergruppe enthält. Die Faktorgruppe $\mathrm{Cl}(K) = I_K/H_K$ nennt man dann die *Idealklassengruppe* von K (genauer: von $\mathcal{O}_K$).

Wer diesen formalen Weg nicht schätzt, kann die "gebrochenen Ideale" als Mengen einführen: man schreibt $\mathfrak{a}\mathfrak{b}^{-1}$ als $\mathfrak{a}\mathfrak{b}'(\mathfrak{b}\mathfrak{b}')^{-1} = \frac{1}{b}\mathfrak{a}\mathfrak{b}$, wo $b = N\mathfrak{b}$ die Norm von $\mathfrak{b}$ bezeichnet, und definiert ganz allgemein $\frac{1}{\alpha}\mathfrak{c} := \{\frac{\gamma}{\alpha} : \gamma \in \mathfrak{c}\}$. Auf der Menge gebrochener Ideale $\neq 0$ definiert man dann die Multiplikation wie bei ganzen Idealen, und zeigt dann, daß diese eine Gruppe bilden (man muß also $\mathfrak{a}\mathfrak{a}^{-1} = (1)$ zeigen, was angesichts $\mathfrak{a}\mathfrak{a}^{-1} = \frac{1}{a}\mathfrak{a}\mathfrak{a}' = \frac{1}{a}(a) = (1)$ mit $a = N\mathfrak{a}$ aber klar ist).

Wir gehen einen dritten Weg und verzichten ganz auf gebrochene Ideale. Aus der obigen "Definition" der Idealklassengruppe folgt nämlich, daß zwei Ideale $\mathfrak{a}$ und $\mathfrak{b}$ genau dann in der selben Klasse modulo H_K liegen, wenn $\mathfrak{a} = \xi\mathfrak{b}$ für ein $\xi \in K^\times$ ist. Schreibt man $\xi = \beta/\alpha$ mit $\alpha, \beta \in \mathcal{O}_K$, so ist dies gleichbedeutend mit $\alpha\mathfrak{a} = \beta\mathfrak{b}$. Umgekehrt können wir so eine Äquivalenzrelation auf der Menge der (ganzen) Ideale einführen: wir nennen $\mathfrak{a}$ und $\mathfrak{b}$ äquivalent (in Zeichen: $\mathfrak{a} \sim \mathfrak{b}$), wenn es $\alpha, \beta \in \mathcal{O}_K$ gibt mit $\alpha\mathfrak{a} = \beta\mathfrak{b}$. Natürlich muß man die üblichen Axiome nachrechnen: Symmetrie, Reflexivität und Transitivität (Übung).

Auf der Menge der Äquivalenzklassen von Idealen führen wir eine Multiplikation ein wie folgt: sind c und d solche Klassen, so wählen wir Vertreter $\mathfrak{a} \in c$ und $\mathfrak{b} \in d$, und nennen die Klasse $cd = [\mathfrak{a}\mathfrak{b}]$ das Produkt von c und d. Hier ist nachzuweisen, daß diese Definition nicht von der Wahl der Vertreter abhängt (Übung). Offenbar ist die Klasse des Einsideals ein neutrales Element; die Assoziativität folgt aus der Assoziativität der Idealmultiplikation,

und die Existenz des Inversen aus der Tatsache, daß $\mathfrak{a}\mathfrak{a}' = (a)$ ein Hauptideal ist; mit anderen Worten: es ist $[\mathfrak{a}]^{-1} = [\mathfrak{a}']$.

Damit haben wir gezeigt, daß die Idealklassen eine Gruppe bilden; diese heißt die *Idealklassengruppe* von K, wird mit $\mathrm{Cl}(K)$ bezeichnet, und ist zusammen mit der Einheitengruppe die wichtigste Invariante eines Zahlkörpers. Wesentliches Ziel dieses Abschnittes ist es zu zeigen, daß die *Klassenzahl* $h_K = \#\mathrm{Cl}(K)$ *endlich* ist. Da der Beweis konstruktiv ist, wird er die Berechnung von Idealklassengruppen gegebener quadratischer Zahlkörper ermöglichen.

Eine Idealklasse wird immer von den Hauptidealen gebildet; ist $h_K = 1$, gibt es keine andere Klasse, d.h. jedes Ideal ist Hauptideal. Damit haben wir mit der Klassenzahlberechnung ein Verfahren an der Hand, mit dessen Hilfe wir entscheiden können, ob ein vorgelegter Ganzheitsring ein Hauptidealring ist oder nicht, ganz unabhängig davon, ob dieser Ring euklidisch ist oder nicht.

Betrachten wir das Beispiel $R = \mathbb{Z}[\sqrt{-5}\,]$; hier gibt es die Klassen $1 = [(1)]$ und $c = [\mathfrak{a}]$ mit $\mathfrak{a} = (2, 1 + \sqrt{-5}\,)$. Wegen $\mathfrak{a}^2 = (2)$ ist $c^2 = 1$, d.h. c hat die Ordnung 2. Weiter ist $\mathfrak{a} \sim \mathfrak{b}$: aus $\mathfrak{a}\mathfrak{b} = (1 + \sqrt{-5}\,)$ folgt nämlich $\mathfrak{a}\mathfrak{b} \sim (1)$, also $[\mathfrak{b}] = [\mathfrak{a}]^{-1} = [\mathfrak{a}]$. Ebenso zeigt man $\mathfrak{c} \sim \mathfrak{a}$. Die Ideale scheinen sich hier also auf zwei Klassen zu verteilen, und in der Tat werden wir unten sehen, daß R die Klassenzahl 2 hat.

Endlichkeit der Klassenzahl

Wir werden zeigen, daß jede Idealklasse ein ganzes Ideal mit beschränkter Norm besitzt, woraus die Endlichkeit dann sofort folgt. Wir werden dabei der Bequemlichkeit halber den Begriff eines primitiven Ideals benutzen. Ein Ideal $\mathfrak{a}$ in $\mathcal{O}_K$ heißt *primitiv*, wenn es durch kein Ideal der Form $(m) \neq (1)$ mit $m \in \mathbb{Z}$ teilbar ist. Offenbar wird jede Idealklasse von einem primitiven Ideal erzeugt: notfalls kann man durch das Hauptideal (m) dividieren.

Ein Ideal $\mathfrak{a}$ besitzt nach Proposition 4.2 eine $\mathbb{Z}$-Basis der Form $\{n, m(b + \omega)\}$ mit $m \mid n$; insbesondere ist $\mathfrak{a}$ primitiv genau dann, wenn $m = 1$ ist, mit anderen Worten: ist $\mathfrak{a}$ primitiv, so gibt es $n \in \mathbb{N}$ und $b \in \mathbb{Z}$ mit $\mathfrak{a} = n\mathbb{Z} \oplus (b + \omega)\mathbb{Z}$, und es gilt $N\mathfrak{a} = n$. Jetzt behaupten wir:

Satz 4.9. *Sei $m \in \mathbb{Z}$ quadratfrei, $K = \mathbb{Q}(\sqrt{m}\,)$ ein quadratischer Zahlkörper mit Ganzheitsring $\mathcal{O}_K = \mathbb{Z}[\omega]$ und Diskriminante d. Die Gauß-Schranke μ_K*

sei gegeben durch

$$\mu_K = \begin{cases} \sqrt{d/5}, & \text{falls } d > 0, \\ \sqrt{-d/3}, & \text{falls } d < 0. \end{cases}$$

Dann enthält jede Idealklasse von K ein ganzes Ideal $\neq (0)$ mit Norm $\leq \mu_K$; insbesondere ist die Anzahl h aller Idealklassen endlich.

Offensichtlich ist der Satz bestmöglich: für $d = 5$, bzw. $d = -3$ sind die Schranken nämlich scharf. Ist $\mu_K \leq 2$, so enthält jede Idealklasse ein ganzes Ideal $\neq (0)$ der Norm < 2, d.h. der Norm 1; mit anderen Worten: jede Idealklasse enthält das Einsideal. Dann kann es aber nur eine Idealklasse geben, d.h. $\mathcal{O}_K$ ist dann notwendig ZPE-Ring. Satz 4.9 besagt (ganz ohne Rechnung!), daß dies für alle K mit $-12 \leq d \leq 20$ richtig ist, d.h. für $m \in \{-11, -7, -3, -2, -1, 2, 3, 5, 13, 17\}$.

Übung. Ist $d \equiv 5 \bmod 8$, so ist (2) prim, und es gibt keine Ideale der Norm 2 in $\mathcal{O}_K$. Zeige, daß daraus folgt, daß die Körper mit $d = -19, 21, 29, 37$ Klassenzahl 1 haben. Welche Körper erhält man, wenn man zusätzlich noch $d \equiv 2 \bmod 3$ fordert?

Betrachten wir als nächstes $R = \mathbb{Z}[\sqrt{-5}\,]$ mit $d = -20$; nach Satz 4.9 enthält jede Idealklasse ein Ideal der Norm $< \sqrt{20/3}$, also ≤ 2. Da es nur zwei solcher Ideale gibt, nämlich das Hauptideal (1) und das Nichthauptideal $(2, 1 + \sqrt{-5}\,)$, hat R Klassenzahl 2.

Eine wichtige Konsequenz aus Satz 4.9 ist folgende Beobachtungen, die unsere Erkenntnisse über Darstellungen von Primzahlen in der Form $x^2 + y^2$ oder $x^2 + 3y^2$ etc. auf einen Schlag verallgemeinert:

Korollar 4.10. *Ist $K = \mathbb{Q}(\sqrt{m}\,)$ ein quadratischer Zahlkörper mit Klassenzahl h, und ist $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$ in $\mathcal{O}_K$ zerlegt, so gibt es $x, y \in \mathbb{N}$ mit $\pm 4p^h = x^2 - my^2$.*

Beweis. Die h-te Potenz jedes Ideals in $K = \mathbb{Q}(\sqrt{m}\,)$ ist ein Hauptideal. Insbesondere ist $\mathfrak{p}^h = (\frac{x+y\sqrt{m}}{2})$, und Normbildung liefert nun sofort $p^h = |\frac{x^2-my^2}{4}|$. □

Beweis von Satz 4.9. Sei $c = [\mathfrak{a}]$ eine von einem Ideal $\mathfrak{a}$ erzeugte Idealklasse. Ohne Einschränkung der Allgemeinheit dürfen wir annehmen, daß $\mathfrak{a}$ primitiv ist. Also ist $\mathfrak{a} = (a, \alpha)$ mit $a = N\mathfrak{a}$ und $\alpha = b + \omega = s + \frac{1}{2}\sqrt{d}$ für ein $s \in \mathbb{Q}$ mit $2s \in \mathbb{Z}$. Ist $a^2 \leq \mu_K$, so sind wir fertig; andernfalls wendet man den

Euklidischen Algorithmus auf das Paar (s,a) an und findet ein $q \in \mathbb{Z}$ mit $s - qa = r$ und

$$|r| \leq \frac{a}{2} \quad \text{falls } d < 0,$$
$$\frac{a}{2} \leq |r| \leq a \quad \text{falls } d > 0.$$

Mit $\alpha_1 = r + \frac{1}{2}\sqrt{d}$ ist dann $\alpha_1 \in \mathfrak{a}$, $|N\alpha_1| \leq \frac{1}{4}(a^2 - d) < a^2$, sowie $\mathfrak{a}_1 := \frac{1}{a}\alpha_1'\mathfrak{a} \sim \mathfrak{a}$ ein ganzes Ideal mit $[\mathfrak{a}_1] = [\mathfrak{a}]$ und $N\mathfrak{a}_1 < N\mathfrak{a}$. Wir wiederholen diesen Schritt solange, bis wir ein Ideal mit Norm $\leq \mu_K$ gefunden haben; da die Norm bei jedem Schritt um mindestens 1 kleiner wird, ist man nach endlich vielen Schritten fertig.

Der Beweis der Ungleichung $|N\alpha_1| \leq \frac{1}{4}(a^2 - d) < a^2$ ist einfach: im Falle $d < 0$ ist $|N\alpha_1| = |r^2 - \frac{d}{4}| \leq \frac{a^2+|d|}{4} < 1$ wegen $a^2 > \mu_K = \frac{|d|}{3}$, während für $d > 0$ sicher $-a^2 = \frac{a^2-5a^2}{4} < r^2 - \frac{d}{4} < a^2$ ist.

Zu zeigen ist auch noch, daß das Ideal $\mathfrak{a}_1$ ganz ist; wegen $\frac{1}{a}\alpha_1'\mathfrak{a} \subseteq \mathcal{O}_K \iff \alpha'\mathfrak{a} \subseteq (a) = \mathfrak{a}\mathfrak{a}' \iff (\alpha') \subseteq \mathfrak{a}'$ ist das aber klar. □

Beispiele

Eine Tabelle mit Klassenzahlen für kleine Diskriminanten zum Üben:

d	-52	-23	-20	-15	40	60
h	2	3	2	2	2	2

Es folgen einige Beispiele der Klassengruppenberechnung.

1. $K = \mathbb{Q}(\sqrt{-21}\,)$, $d = -84$; die Gauß-Schranke ist $\mu_K = \sqrt{84/3}$, d.h. wir haben Ideale der Norm ≤ 5 zu untersuchen. Wegen $2 \mid d$ ist 2 verzweigt: $(2) = \mathfrak{a}^2$ mit $\mathfrak{a} = (2, 1 + \sqrt{-21}\,)$. Ebenso ist $(3) = \mathfrak{b}^2$ mit $\mathfrak{b} = (3, \sqrt{-21}\,)$. Schließlich ist $(-21/5) = 1$, folglich $(5) = \mathfrak{c}\mathfrak{c}'$ mit $\mathfrak{c} = (5, 2 + \sqrt{-21}\,)$. Die Ideale mit Norm ≤ 5 sind also (1), $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{a}^2 = (2)$, $\mathfrak{c}$ und $\mathfrak{c}'$ ($\mathfrak{a}\mathfrak{b}$ hat bereits Norm 6). Da $\mathfrak{a}^2 \sim (1)$ ist, bleiben $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ und $\mathfrak{c}'$ zu untersuchen. Offenbar ist keines dieser Ideale Hauptideal, da es in $\mathcal{O}_K$ keine Elemente der Normen 2, 3 oder 5 gibt. Ebenso ist $\mathfrak{a} \not\sim \mathfrak{b}$, da sonst $(2) = \mathfrak{a}^2 \sim \mathfrak{a}\mathfrak{b}$ wäre und es ein Element der Norm 6 geben müßte; ein solches gibt es aber nicht.

Nun ist $\mathfrak{a}\mathfrak{b}\mathfrak{c}$ ein Ideal der Norm 30; die Elemente $3 \pm \sqrt{-21}$ haben ebenfalls Norm 30. In der Tat ist $(3 + \sqrt{-21}\,) = \mathfrak{a}\mathfrak{b}\mathfrak{c}'$: die Faktoren $\mathfrak{a}$ und $\mathfrak{b}$ sind klar, zu entscheiden ist lediglich, ob $3 + \sqrt{-21}$ durch $\mathfrak{c}$ oder $\mathfrak{c}'$ teilbar ist. Dies

macht man so: wegen $2+\sqrt{-21} \in \mathfrak{c}$ ist $\sqrt{-21} \equiv -2 \equiv 3 \bmod \mathfrak{c}$, und also $3+\sqrt{-21} \equiv 3-2 \equiv 1 \bmod \mathfrak{c}$ und $3+\sqrt{-21}$ daher sicher nicht durch $\mathfrak{c}$ teilbar. Also ist $\mathfrak{a}\mathfrak{b}\mathfrak{c}' \sim 1$, wegen $\mathfrak{c}' \sim \mathfrak{c}^{-1}$ also $\mathfrak{a}\mathfrak{b} \sim \mathfrak{c}$.

Schließlich ist $\mathfrak{c}' \sim \mathfrak{c}^{-1} \sim \mathfrak{a}^{-1}\mathfrak{b}^{-1} \sim \mathfrak{a}\mathfrak{b}$, da $\mathfrak{a}^2 \sim \mathfrak{b}^2 \sim 1$ ist. Also gibt es genau vier Idealklassen: die Hauptidealklasse, und die Klassen $[\mathfrak{a}]$, $[\mathfrak{b}]$ und $[\mathfrak{a}][\mathfrak{b}]$ der Ordnung 2. Die Idealklassengruppe ist damit isomorph zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, der Kleinschen Vierergruppe.

2. $K = \mathbb{Q}(\sqrt{-17})$ hat $d = -68$, somit sind alle Ideale mit Norm ≤ 4 zu untersuchen. Wir haben $(2) = \mathfrak{a}^2$ mit $\mathfrak{a} = (2, 1+\sqrt{-17})$ und $(3) = \mathfrak{b}\mathfrak{b}'$ mit $\mathfrak{b} = (3, 1+\sqrt{-17})$. Die Ideale mit Norm ≤ 4 sind also (1), $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{b}'$ und $(2) = \mathfrak{a}^2$.

Nun kann $\mathfrak{b}^2$ kein Hauptideal sein, weil es kein Element der Norm 9 gibt; dagegen zeigt $(1+\sqrt{-17}) = \mathfrak{a}\mathfrak{b}^2$, daß $\mathfrak{b}^2 \sim \mathfrak{a}^{-1} \sim \mathfrak{a}$ ist. Schließlich ist $\mathfrak{b}' \sim \mathfrak{b}^{-1}$, und wir sehen, daß die Klasse $[\mathfrak{b}]$ die ganze Idealklassengruppe erzeugt: $\mathfrak{b}^2 \sim \mathfrak{a}$, $\mathfrak{b}^4 \sim \mathfrak{a}^2 \sim 1$ und somit $\mathfrak{b}^3 \sim \mathfrak{b}^{-1} \sim \mathfrak{b}'$. Die Idealklassengruppe hat hier also ebenfalls Ordnung 4, ist aber im Gegensatz zu oben zyklisch, d.h. $\simeq \mathbb{Z}/4\mathbb{Z}$.

Übung. Sei $d = \operatorname{disc} K < 0$ die Diskriminante eines imaginärquadratischen Zahlkörpers K. Für einige kleine Werte von d berechne man die Summe

$$h = \frac{w}{2d} \sum_{r=1}^{|d|-1} \left(\frac{d}{r}\right) r,$$

wobei w die Anzahl der in K enthaltenen Einheitswurzeln (also hier gleich der Ordnung der Einheitengruppe) und (d/r) das Kroneckersymbol ist. Vergleiche h mit der Klassenzahl von K und stelle eine Vermutung auf.

Übung. Zeige, daß die imaginärquadratischen Zahlkörper $\mathbb{Q}(\sqrt{m})$ für $m = -1, -2, -3, -7, -11, -19, -43, -67$, und -163 Klassenzahl 1 haben.

Eine weitere hübsche Anwendung betrifft den Körper $K = \mathbb{Q}(\sqrt{-5})$. Wir haben gesehen, daß die Idealklassengruppe $\mathrm{Cl}(K)$ von den Klassen von (1) und $\mathfrak{a} = (2, 1+\sqrt{-5})$ erzeugt wird. Sei nun $\mathfrak{p}$ ein Primideal der Norm p, welches in $\mathcal{O}_K$ zerlegt ist (also $(-5/p) = +1$ und $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$). Dann ist entweder $\mathfrak{p} = (a+b\sqrt{-5})$ ein Hauptideal und damit $p = a^2+5b^2$, oder aber $\mathfrak{p} \sim \mathfrak{a}$ und damit $\mathfrak{a}\mathfrak{p} = (C+d\sqrt{-5})$ Hauptideal. Im letzteren Falle folgt $2p = C^2+5d^2$; da aber C und d ungerade sind, können wir $C = 2c+d$ für ein $c \in \mathbb{Z}$ schreiben und finden $2p = (2c+d)^2+5d^2 = 4c^2+4cd+6d^2$, also

$p = 2c^2 + 2cd + 3d^2$. Mit anderen Worten: ist $(-5/p) = +1$, so besitzt p eine Darstellung der Form $p = a^2 + 5b^2$ oder $p = 2c^2 + 2cd + 3d^2$.

Nun nennt man ein Polynom $Ax^2 + Bxy + Cy^2 \in \mathbb{Z}[x, y]$ eine binäre quadratische Form; ihre Diskriminante ist definiert als $B^2 - 4AC$. Insbesondere haben die beiden quadratischen Formen $x^2 + 5y^2$ und $2x^2 + 2xy + 3y^2$ dieselbe Diskriminante $d = -20$. Dies ist kein Zufall: Gauß hat die binären quadratischen Formen derselben Diskriminanten in Klassen eingeteilt, und Dirichlet und Dedekind haben gezeigt, daß diese Einteilung genau den Idealklassen quadratischer Zahlkörper entsprechen. Für Diskriminante -20 gibt es genau zwei verschiedene Klassen, nämlich diejenigen, zu denen $x^2 + 5y^2$ und $2x^2 + 2xy + 3y^2$ gehören.

Nach dem quadratischen Reziprozitätsgesetz ist übrigens $(-5/p) = +1 \iff p \equiv 1, 3, 7, 9 \bmod 20$; untersucht man, welche Primzahlen von welcher der obigen Formen dargestellt wird, so stellt man fest: genau dann ist $p = x^2 + 5y^2$, wenn $p \equiv 1, 9 \bmod 20$ ist, und genau dann ist $p = 2x^2 + 2xy + 3y^2$, wenn $p \equiv 3, 7 \bmod 20$ ist. Beispiele: $29 = 3^2 + 5 \cdot 2^2$, $41 = 6^2 + 5 \cdot 1^2$, $3 = 2 \cdot 1^2 + 2 \cdot 1 \cdot (-1) + 3 \cdot (-1)^2$, $7 = 2 \cdot 1^2 + 2 \cdot 1 \cdot 1 + 3 \cdot 1^2$, usw. Diese Bemerkung kann man übrigens leicht beweisen: es ist nämlich $p = x^2 + 5y^2 \equiv x^2 + y^2 \equiv 0, 1 \bmod 4$; soll p prim sein, muß also $p \equiv 1 \bmod 4$ sein, und dies ist gerade für $p \equiv 1, 9 \bmod 20$ der Fall. Ist dagegen $p = 2x^2 + 2xy + 3y^2$, so ist y ungerade, und damit $p \equiv 2x^2 + 2x + 3 = 2x(x+1) + 3 \equiv 3 \bmod 4$ (denn $x(x+1)$ ist immer gerade).

Diese hübsche Beobachtung ist ein Spezialfall der Theorie der Geschlechter, der wir uns im nächsten Kapitel widmen werden.

4.4 Die diophantische Gleichung $y^2 = x^3 - d$

Wir wollen sehen, was wir nun über die Lösungen der Gleichung $y^2 = x^3 - d$ sagen können, wobei wir uns vorbehalten, an d im Laufe der Rechnungen diverse Bedingungen zu stellen.

Der Anfang ist klar: wir schreiben $x^3 = y^2 + d = (y + \sqrt{-d}\,)(y - \sqrt{-d}\,)$. Wir möchten gerne haben, daß die Ideale $\mathfrak{a} = (y + \sqrt{-d}\,)$ und $\mathfrak{a}'$ teilerfremd sind. Offenbar teilt jeder gemeinsame Primidealfaktor $\mathfrak{p}$ (mit $\mathfrak{p} \mid p$) auch $2\sqrt{-d}$; da $\mathfrak{p} \mid \sqrt{-d}$ (und $p \neq 2$) sofort auf $p \mid d$, $p \mid y$, $p \mid x$ und schließlich $p^2 \mid d$ führt, können wir diesen Fall ausschließen, wenn wir voraussetzen, daß $\boxed{d \text{ quadratfrei}}$ ist. Damit bleibt noch die Möglichkeit $\mathfrak{p} \mid 2$; hier gibt es folgende Möglichkeiten:

- $d \equiv 2 \bmod 4$: dann ist $\mathfrak{p} \mid (\sqrt{-d})$ (wegen $\mathfrak{p} = (2, \sqrt{-d})$), somit $\mathfrak{p} \mid y$, $p \mid y$ und schließlich $x^3 = y^2 + d \equiv 2 \bmod 4$: Widerspruch, da eine dritte Potenz nicht genau durch 2 teilbar sein kann.

- $d \equiv 1 \bmod 4$: hier ist $\mathfrak{p} = (2, 1 + \sqrt{-d})$, somit $\mathfrak{p} \mid (y + \sqrt{-d})$ genau dann, wenn y ungerade ist. Damit folgt $x^3 = y^2 + d \equiv 1 + 1 \equiv 2 \bmod 4$, und das ist wie eben ein Widerspruch.

- $d \equiv 3 \bmod 4$: hier ist $y + \sqrt{-d}$ genau dann durch $\mathfrak{p}$ (sogar durch 2) teilbar, wenn y ungerade ist. Aus $d = x^3 - y^2$ folgt, daß x gerade sein muß, somit ist $d \equiv -y^2 \equiv -1 \bmod 8$. Wenn wir also voraussetzen, daß $\boxed{d \not\equiv 7 \bmod 8}$ gilt, kann auch hier nicht $\mathfrak{p} \mid 2$ ein gemeinsamer Teiler von $\mathfrak{a}$ und $\mathfrak{a}'$ sein.

Damit sind $\mathfrak{a}$ und $\mathfrak{a}'$ in der Tat teilerfremd. Da ihr Produkt eine dritte Potenz ist, gibt es ein Ideal $\mathfrak{b}$ mit $\mathfrak{a} = \mathfrak{b}^3$ (und, nach Konjugation, mit $\mathfrak{a}'^3 = \mathfrak{b}'^3$). Jetzt kommt die nächste Voraussetzung: bezeichnet h die Klassenzahl von $\mathbb{Q}(\sqrt{-d})$, so möge $\boxed{3 \nmid h}$ gelten. Denn in diesem Fall ist sowohl $\mathfrak{b}^3$, als auch $f b^h$ Hauptideal, damit auch alle $\mathfrak{b}^{3a+hb}$, und wegen der Teilerfremdheit von 3 und h folgt nach Bezout, daß $\mathfrak{b}$ selbst Hauptideal ist, also $\mathfrak{b} = (\frac{r+s\sqrt{-d}}{2})$ mit $r \equiv s \bmod 2$.

Im Falle $\boxed{d > 0,\ d \neq 1, 3}$ sind ± 1 die einzigen Einheiten, und wir erhalten aus der obigen Idealgleichung die Gleichung von Elementen

$$y + \sqrt{-d} = \left(\frac{r + s\sqrt{-d}}{2} \right)^3,$$

wobei wir das Vorzeichen in die dritte Potenz hineingezogen haben. Koeffizientenvergleich liefert jetzt $1 = \frac{1}{8}(3r^2 s - d s^3)$, also $8 = 3r^2 s - d s^3 = s(3r^2 - d s^2)$. Offenbar muß $s \mid 8$ gelten, also $s = \pm 1$ oder $r \equiv s \equiv 0 \bmod 2$. Im ersten Fall folgt $\pm 8 = 3r^2 - d$, also $d = 3r^2 \mp 8$, im zweiten Fall setzen wir $r = 2t$, $s = 2u$ und finden $1 = u(3t^2 - du^2)$, also $u = \pm 1$ und $d = 3t^2 \mp 1$.

Damit haben wir gezeigt: hat d (unter den gemachten Voraussetzungen) nicht die Form $3t^2 \pm 1$ oder $3t^2 \pm 8$, dann besitzt die diophantische Gleichung $y^2 = x^3 - d$ keine ganzzahlige Lösung.

Was passiert, wenn d von dieser Form ist? Sei z.B. $d = 3r^2 - 8$; dann liefert ein zweiter Koeffizientenvergleich (unter Beachtung von $s = 1$) sofort $8y = r^3 - 3dr = r^3 - 9r^3 + 24r = 24r - 8r^3$, also $y = (3 - r^2)r$, sowie $y^2 + d = r^6 - 6r^4 + 12r^2 - 8 = (r-2)^3$, also $x = r - 2$. Daher entspricht eine Darstellung $d =$

$3r^2-8$ dem Lösungspaar $(r-2, \pm(3-r^2)r)$ unserer diophantischen Gleichung. Ganz entsprechend führen die andern Darstellungen auf solche Lösungspaare: die Werte $d = 3r^2 + 8$, $3t^2 + 1$, $3t^2 - 1$ entsprechen den Lösungspaaren $(r^2 + 2, \pm r(r^2 + 3))$, $(4t^2 + 1, \pm t(8t^2 + 3))$, $(4t^2 - 1, \pm t(8t^2 - 3))$.

Die einzige Frage, die noch zu klären ist, ist folgende: kann ein d mehrere solcher Darstellungen besitzen? Die Antwort ist: $d = 11$ besitzt genau zwei Darstellungen, alle andern höchstens eine. Der Beweis ist einfach: Gleichungen wie $3r^2 - 8 = 3t^2 - 1$ können schon modulo 3 nicht auftreten; es bleiben $3r^2 - 8 = 3t^2 + 1$ (dies führt auf $3(r^2 - t^2) = 9$, also auf $r^2 - t^2 = (r - t)(r + t) = 3$, deren einzige Lösung $r = \pm 2$, $t = \pm 1$ ist und daher auf $d = 4$ führt, was aber nicht quadratfrei ist) und $3r^2 + 8 = 3t^2 - 1$ (dies liefert entsprechend $3 = t^2 - r^2$, also $t = \pm 2$, $r = \pm 1$ und somit $d = 3 + 8 = 3 \cdot 2^2 - 1 = 11$).

Damit haben wir bewiesen:

Satz 4.11. *Sei $d \neq 1, 3$ quadratfreie natürliche Zahl, und $d \neq 7 \bmod 8$. Ist die Klassenzahl von $\mathbb{Q}(\sqrt{-d}\,)$ nicht durch 3 teilbar, so hat die diophantische Gleichung $y^2 = x^3 - d$*

1. *genau zwei Lösungspaare $(3, \pm 4)$ und $(58, \pm 3364)$ für $d = 11$;*
2. *genau ein Lösungspaar, wenn $d \neq 11$ die Form $d = 3t^2 \pm 1$ oder $d = 3t^2 \pm 8$ hat;*
3. *keine ganzzahligen Lösungen sonst.*

Man beachte, daß Satz 4.11 fast alle unserer bisherigen Ergebnisse enthält: wegen $2 = 3 \cdot 1^2 - 1$ hat z.B. $y^2 = x^3 - 2$ genau die Lösungen $(3, \pm 5)$.

Man betrachte auch den Fall $d = 26 = 3 \cdot 3^2 - 1$: man stellt fest, daß $y^2 = x^3 - 26$ außer dem Lösungspaar $(207, \pm 42849)$, das obiger Satz liefert, auch noch die Lösungen $(3, \pm 1)$ hat. Dies ist kein Widerspruch: aus dem Satz folgt dann zwangsläufig, daß die Klassenzahl von $\mathbb{Q}(\sqrt{-26}\,)$ durch 3 teilbar sein muß. In der Tat ist die Klassenzahl gleich 6.

Ganz ähnlich kann man die ganzzahligen Lösungen von $x^p + y^p = z^p$ bestimmen, wenn p die Klassenzahl von $\mathbb{Q}(\zeta_p)$ nicht teilt – dies ist Kummers Zugang zum Fermatschen Problem.

Zusammenfassung

Dieses Kapitel enthält die wesentlichen Ergebnisse der Vorlesung:

- Ideale in Ganzheitsringen $\mathcal{O}_K$ quadratischer Zahlkörper bilden eine Halbgruppe mit Kürzungsregel;
- in $\mathcal{O}_K$ ist die Primidealzerlegung eindeutig;
- rationale Primzahlen sind in $\mathcal{O}_K$ verzweigt, zerlegt oder träge, je nachdem $(d/p) = 0$, $+1$ oder -1 ist;
- Ideale $\mathfrak{a}$ und $\mathfrak{b}$ heißen äquivalent, wenn es $\alpha, \beta \in \mathcal{O}_K \setminus \{0\}$ gibt mit $\alpha\mathfrak{a} = \beta\mathfrak{b}$. Die Äquivalenzklassen von Idealen bilden eine Gruppe, die Idealklassengruppe.
- die Idealklassengruppe von K ist endlich.

Kapitel 5

Geschlechtertheorie und quadratische Reziprozität

5.1 Klassenzahl im engeren Sinne

Die ursprüngliche Form der Äquivalenz von Idealklassen, die von Gauß im Zusammenhang mit binären quadratischen Formen eingeführt wurde, unterscheidet sich von der (bisher behandelten) gewöhnlichen Äquivalenz. Die Einführung einer Äquivalenz im engeren Sinne ist aber für die Geschlechtertheorie nur unter großen Opfern zu vermeiden.

Sei also $k = \mathbb{Q}(\sqrt{m}\,)$ ein quadratischer Zahlkörper. Ein $\alpha \in k^\times$ heißt *total positiv* (in Zeichen: $\alpha \gg 0$), wenn $m < 0$ oder aber $m > 0$, $\alpha > 0$ und $\alpha' > 0$ gilt (unter der Identifizierung von $\sqrt{m}$ mit der positiven Quadratwurzel von m). Entsprechend heißt α *total negativ*, wenn $-\alpha$ total positiv ist. Statt α' schreiben wir auch manchmal α^σ, wo $\sigma : \sqrt{m} \longmapsto -\sqrt{m}$ der nicht-triviale Automorphismus von $k/\mathbb{Q}$ ist.

Beispiel. In imaginärquadratischen Zahlkörpern sind alle von 0 verschiedenen Zahlen totalpositiv; so ist z.B. $-1 \gg 0$ in $\mathbb{Q}(\sqrt{-1}\,)$, aber $-1 \ll 0$ in $\mathbb{Q}(\sqrt{2}\,)$. Weiter ist $1 + \sqrt{2}$ nicht total positiv in $\mathbb{Q}(\sqrt{2}\,)$ wegen $1 - \sqrt{2} < 0$; dagegen ist $3 + \sqrt{2} \gg 0$.

Hilfssatz 5.1. *Ist $\alpha \in k^\times$, so ist $N\alpha > 0$ genau dann, wenn $\alpha \gg 0$ oder $\alpha \ll 0$ gilt.*

Beweis. Ist $\alpha \gg 0$ oder $\alpha \ll 0$, so ist offenbar $N\alpha = \alpha\alpha' > 0$. Ist umgekehrt $N\alpha > 0$, so haben α und α' dasselbe Vorzeichen, folglich ist entweder α oder $-\alpha$ total positiv. □

Wir erinnern uns daran, daß zwei Ideale $\mathfrak{a}$ und $\mathfrak{b}$ äquivalent im gewöhnlichen Sinne heißen, wenn $\mathfrak{a} = \lambda\mathfrak{b}$ für ein $\lambda \in k^\times$ gilt. Wir nennen sie äquivalent im engeren Sinne (in Zeichen: $\mathfrak{a} \overset{+}{\sim} \mathfrak{b}$), wenn $\mathfrak{a} = \lambda\mathfrak{b}$ für ein $\lambda \gg 0$ ist. Da in imaginärquadratischen Zahlkörpern alle Zahlen $\neq 0$ totalpositiv sind, fallen dort beide Äquivalenzbegriffe zusammen.

Auch die Äquivalenzklassen im engeren Sinne bilden eine (wie wir gleich sehen werden, endliche) Gruppe, die mit $\mathrm{Cl}^+(k)$ bezeichnet wird; deren Ordnung h^+ nennt man die Klassenzahl im engeren Sinne.

In reell-quadratischen Zahlkörpern $k = \mathbb{Q}(\sqrt{d}\,)$ dagegen sind beide Begriffe im allgemeinen verschieden: die von dem Ideal $(\sqrt{d}\,)$ erzeugte Idealklasse ist offenbar ein Hauptideal im gewöhnlichen Sinne; sie ist aber Hauptideal im engeren Sinne nur dann, wenn es ein $\lambda \gg 0$ gibt mit $(\sqrt{d}\,) = \lambda(1)$, d.h. wenn das Ideal $(\sqrt{d}\,)$ von einem total positiven Element erzeugt wird. Die Zahl $\alpha = \sqrt{d}$ ist wegen $\alpha' = -\sqrt{d}$ natürlich nicht total positiv.

Im folgenden wollen wir einige Unterschiede, bzw. Gemeinsamkeiten dieser beiden Klassengruppen untersuchen. Dazu stellen wir erstens fest, daß es eine kanonische Projektion $\mathrm{Cl}^+(k) \longrightarrow \mathrm{Cl}(k)$ gibt: man ordnet der von $\mathfrak{a}$ erzeugten Idealklasse $[\mathfrak{a}]^+$ im engeren Sinne die Idealklasse $[\mathfrak{a}]$ im gewöhnlichen Sinne zu (die "Umkehrabbildung" $\mathrm{Cl}(k) \longrightarrow \mathrm{Cl}^+(k) : [\mathfrak{a}] \longmapsto [\mathfrak{a}]^+$ ist i.a. nicht wohldefiniert, weil $\mathfrak{a} \sim \mathfrak{b}$ sein kann, ohne dass $\mathfrak{a} \overset{+}{\sim} \mathfrak{b}$ gilt; mit anderen Worten: man kann $\mathrm{Cl}(k)$ *nicht* als Untergruppe von $\mathrm{Cl}^+(k)$ auffassen). Genauer gilt nun:

Proposition 5.2. *Es bezeichne $\langle\sqrt{d}\,\rangle$ die Untergruppe $\{1, [(\sqrt{d}\,)]_+\}$ der Klassengruppe $\mathrm{Cl}^+(k)$ im engeren Sinne; dann ist die folgende Sequenz abelscher Gruppen exakt:*

$$1 \longrightarrow \langle\sqrt{d}\,\rangle \xrightarrow{\ \iota\ } \mathrm{Cl}^+(k) \xrightarrow{\ \pi\ } \mathrm{Cl}(k) \longrightarrow 1. \tag{5.1}$$

Beweis. Es ist klar, daß $\iota : \langle\sqrt{d}\,\rangle \longrightarrow \mathrm{Cl}^+(k)$ injektiv, daß $\pi : \mathrm{Cl}^+(k) \longrightarrow \mathrm{Cl}(k)$ surjektiv, und daß $\mathrm{im}\,\iota \subseteq \ker\pi$ ist. Es bleibt also $\ker\pi \subseteq \mathrm{im}\,\iota$ zu zeigen.

Sei dazu $[\mathfrak{a}]_+ \in \ker\pi$. Dann ist $\mathfrak{a} = \alpha\mathcal{O}_k$ für ein $\alpha \in k^\times$. Falls $N\alpha > 0$, so können wir $\alpha \gg 0$ wählen und finden $[\mathfrak{a}]_+ = 1$. Ist dagegen $N\alpha < 0$, also z.B. $\alpha > 0$ und $\alpha^\sigma < 0$, und jetzt ist $\alpha/\sqrt{d} \gg 0$, d.h. $[\mathfrak{a}]_+ = [(\sqrt{d}\,)]_+$. In beiden Fällen ist $[\mathfrak{a}]_+ \in \mathrm{im}\,\iota$. □

Als Folgerung halten wir fest: es ist entweder $h^+ = h$ oder $h^+ = 2h$. Insbesondere ist auch $\mathrm{Cl}^+(k)$ endlich.

Beispiel. In $k = \mathbb{Q}(\sqrt{3}\,)$ hat das Ideal $(\sqrt{3}\,)$ Ordnung 2 in $\mathrm{Cl}^+(k)$, obwohl es Hauptideal im gewöhnlichen Sinne ist. Wäre es Hauptideal im engeren Sinne, müßte es ein ganzes Element der Norm $+3$ geben: $x^2 - 3y^2 = 3$ impliziert aber $3z^2 - y^2 = 1$, also $y^2 \equiv -1 \bmod 3$: Widerspruch.

In $k = \mathbb{Q}(\sqrt{5}\,)$ dagegen ist auch $(\sqrt{5}\,)$ Hauptideal im engeren Sinne: ein total positives Erzeugendes ist $\frac{1+\sqrt{5}}{2}\sqrt{5}$. Diese Beobachtung läßt sich verallgemeinern:

Korollar 5.3. *Für quadratische Zahlkörper k gilt $h^+(k) = 2h(k)$, falls $d = \operatorname{disc} k > 0$ und die Fundamentaleinheit ε Norm $+1$ hat, und $h^+(k) = h(k)$ sonst.*

Beweis. Aus Proposition 5.2 folgt, daß $h^+(k) = h(k)$ genau dann gilt, wenn die Idealklasse $[(\sqrt{d})]_+$ trivial ist. Aber $(\sqrt{d})$ ist Hauptideal im engeren Sinne genau dann, wenn es eine Einheit $\eta \in \mathcal{O}_K^\times$ gibt mit $\eta\sqrt{d} \gg 0$. Für $d < 0$ können wir $\eta = 1$ nehmen; ist aber $d > 0$ und $\eta\sqrt{d} \gg 0$, dann zeigt $N\sqrt{d} < 0$, daß $N\eta < 0$ (also $N\eta = -1$) sein muß. Daher ist $[(\sqrt{d}\,)]_+ = 1$ genau dann, wenn es eine Einheit η mit Norm -1 gibt; eine solche wiederum existiert genau dann, wenn $N\varepsilon = -1$ ist. □

5.2 Geschlechter

Im folgenden bezeichne k immer einen quadratischen Zahlkörper $k = \mathbb{Q}(\sqrt{m}\,)$. An weiteren Vorbereitungen benötigen wir Hilberts Satz 90 (dieser Name kommt daher, weil der Satz in Hilberts Zahlbericht von 1897 die Nummer 90 hat). Hilberts Satz 90 gibt es in zwei Versionen: für Elemente und für Ideale:

- Ist $\alpha \in k^\times$, so gilt $N\alpha = 1$ genau dann, wenn α die Form $\alpha = \beta^{\sigma-1}$ hat.
- Ist $\mathfrak{a}$ ein gebrochenes Ideal in $\mathcal{O}_k$, so gilt $N\mathfrak{a} = 1$ genau dann, wenn $\mathfrak{a}$ die Form $\mathfrak{a} = \mathfrak{b}^{\sigma-1}$ für ein ganzes Ideal $\mathfrak{b}$ hat.

Die Richtungen "$\Longleftarrow$" sind in beiden Fällen trivial. Sei also zuerst $N\alpha = 1$. Ist $\alpha = -1$, so genügt $\beta = \sqrt{m}$; ist $\alpha \neq -1$, so setze man $\beta = \alpha^\sigma + 1$: damit ist dann $\beta^{\sigma-1} = \frac{\alpha+1}{\alpha'+1} = \frac{\alpha(\alpha+1)}{\alpha\alpha'+\alpha} = \frac{\alpha(\alpha+1)}{1+\alpha} = \alpha$.

Sei nun $N\mathfrak{a} = 1$ (also $\mathfrak{a} = \mathfrak{c}\mathfrak{d}^{-1}$ Quotient zweier ganzer Ideale derselben Norm). Wegen der Eindeutigkeit der Primidealzerlegung dürfen wir annehmen, daß $\mathfrak{c}$ und $\mathfrak{d}$ teilerfremd sind. Daraus folgt sofort, daß $\mathfrak{c}$ und $\mathfrak{d}$ nicht durch

träge Primideale teilbar sein können: wäre z.B. $(q) \mid \mathfrak{c}$, so müßte q^2 auch in der Faktorisierung von $N\mathfrak{d}$ vorkommen, folglich $\mathfrak{d}$ durch (q) teilbar sein: Widerspruch. Aus demselben Grund können in $\mathfrak{cd}$ keine verzweigten Primideale aufgehen. Also sind $\mathfrak{c}$ und $\mathfrak{d}$ Produkte zerlegter Primideale; ist $\mathfrak{p}^t || \mathfrak{c}$, so folgt $p^t || \mathfrak{d}$, wegen der Teilerfremdheit also $\mathfrak{p}'^t || \mathfrak{d}$. Dies zeigt, daß $\mathfrak{c} = \mathfrak{d}'$ ist; damit gilt $\mathfrak{a} = \mathfrak{d}'\mathfrak{d}^{-1} = \mathfrak{d}^{\sigma-1}$.

Ist die Einteilung in Idealklassen im engeren Sinne feiner als die im gewöhnlichen, so ist die Einteilung in Geschlechter sehr grob. Wir sagen, zwei Ideale $\mathfrak{a}$ und $\mathfrak{b}$ seien *ähnlich* (in Zeichen: $\mathfrak{a} \overset{+}{\approx} \mathfrak{b}$), wenn $N\mathfrak{a} = N\lambda N\mathfrak{b}$ für ein $\lambda \in k^\times$ mit $\lambda \gg 0$ gilt. Die dazugehörigen Äquivalenzklassen nennt man Geschlechter; das Geschlecht, welches das Einsideal enthält, heißt das Hauptgeschlecht. Die Menge aller Geschlechter bildet eine Gruppe, die Geschlechterklassengruppe $\mathrm{Cl}^+_{\mathrm{gen}}(k)$. Tatsächlich lassen sich die Geschlechter recht einfach beschreiben:

Proposition 5.4. *Für Ideale $\mathfrak{a}, \mathfrak{b}$ in $\mathcal{O}_k$ gilt $\mathfrak{a} \overset{+}{\approx} \mathfrak{b}$ genau dann, wenn $\mathfrak{a} \overset{+}{\sim} \mathfrak{bc}^2$ für ein Ideal $\mathfrak{c}$ gilt, d.h. wenn sich ihre Idealklassen im engeren Sinne um ein Quadrat unterscheiden.*

Beweis. Offenbar genügt es zu zeigen, daß $\mathfrak{a} \overset{+}{\approx} (1)$ zu $\mathfrak{a} \overset{+}{\sim} \mathfrak{c}^2$ äquivalent ist. Sei daher $N\mathfrak{a} = N(\lambda)$ für ein $\lambda \gg 0$. Dann ist $N(\lambda^{-1}\mathfrak{a}) = (1)$, und Hilberts Satz 90 für Ideale zeigt, daß es ein Ideal $\mathfrak{c}$ gibt mit $\lambda^{-1}\mathfrak{a} = \mathfrak{c}^{\sigma-1}$. Wegen $\mathfrak{c}^\sigma \overset{+}{\sim} \mathfrak{c}^{-1}$ folgt jetzt $\mathfrak{a} \overset{+}{\sim} \lambda\mathfrak{c}^2$ wie behauptet.

Ist umgekehrt $\mathfrak{a} \overset{+}{\sim} \mathfrak{c}^2$, so gilt $\mathfrak{a} = \lambda\mathfrak{c}^2$ für ein $\lambda \gg 0$, und Bilden der Norm zeigt $N\mathfrak{a} = N(c\lambda)$ mit $c = N\mathfrak{c}$. □

Dies zeigt, daß $\mathrm{Cl}^+_{\mathrm{gen}}(k) \simeq C_+/C_+^2$ ist, wo $C_+ = \mathrm{Cl}^+(k)$ die Idealklassengruppe im engeren Sinne bezeichnet. Das erste Hauptziel der Geschlechtertheorie ist die Berechnung der Geschlechterklassenzahl, also der Ordnung von $\mathrm{Cl}^+_{\mathrm{gen}}(k)$. Wir werden dazu einen neuen Begriff einführen: ein Ideal $\mathfrak{a}$ heißt *ambig*, wenn $\mathfrak{a} = \mathfrak{a}^\sigma$ ist (wenn also $\mathfrak{a}$ gleich seinem Konjugierten ist); eine Idealklasse $c = [\mathfrak{a}]^+$ heißt *ambig*, wenn sie unter der Galoisoperation fest bleibt, wenn also $c = c^\sigma$ gilt (wenn also $\mathfrak{a} \overset{+}{\sim} \mathfrak{a}'$ gilt). Die ambigen Idealklassen bilden eine Untergruppe Am^+ von $\mathrm{Cl}^+(k)$, die Gruppe der ambigen Idealklassen. Direkt aus der Definition erhält man die exakte Sequenz

$$1 \longrightarrow \mathrm{Am}^+ \longrightarrow C_+ \xrightarrow{1-\sigma} C_+^{1-\sigma} \longrightarrow 1, \tag{5.2}$$

wobei der Homomorphismus $C_+ \longrightarrow C_+^{1-\sigma}$ durch $c \longmapsto c^{1-\sigma}$ definiert ist.

Einen dazu analogen Begriff gibt es natürlich auch für gewöhnliche Idealklassen – der Unterschied und gleichzeitig der Hauptgrund für die Einführung der Klassengruppe im engeren Sinne besteht darain, daß das nächste Ergebnis nur für engere Aquivalenz richtig ist:

Proposition 5.5. *Die ambigen Idealklassen in* $\mathrm{Cl}^+(k)$ *sind genau diejenigen, die von ambigen Idealklassen erzeugt werden.*

Beweis. Sei $c = [\mathfrak{a}]_+$ ambig, also $\mathfrak{a}^\sigma = \lambda\mathfrak{a}$ für ein $\lambda \gg 0$. Bilden der Norm zeigt, daß $N\lambda = \pm 1$ sein muß; wegen $\lambda \gg 0$ ist also $N\lambda = +1$. Hilberts Satz 90 gibt $\lambda = \alpha^{1-\sigma}$ für ein $\alpha \in k^\times$. An $0 \ll \lambda\alpha^{2\sigma} = N\alpha$ lesen wir ab, daß $N\alpha > 0$ ist (ist k komplex, so ist die Norm ohnehin ≥ 0, ist k reell, so ist ein $n \in \mathbb{Z}$ genau dann > 0, wenn $n \gg 0$ in k gilt). Also ist α oder $-\alpha$ total positiv, und wir dürfen oBdA $\alpha \gg 0$ annehmen. Damit ist $\mathfrak{a} \overset{+}{\sim} \alpha\mathfrak{a}$. Aber das Ideal $\alpha\mathfrak{a}$ ist ambig wegen $(\alpha\mathfrak{a})^\sigma = \alpha^\sigma\mathfrak{a}^\sigma = \alpha^\sigma\lambda\mathfrak{a} = \alpha\mathfrak{a}$. Wir haben damit gezeigt, daß c von einem ambigen Ideal erzeugt wird. Da die andere Richtung trivial ist, ist der Beweis komplett. □

Beispiel. In $k = \mathbb{Q}(\sqrt{3})$ wird die Idealklasse $[(\sqrt{3})]^+$ der Ordnung 2 in $\mathrm{Cl}^+(k)$ von dem ambigen Ideal $(\sqrt{3})$ erzeugt. Das Beispiel $k = \mathbb{Q}(\sqrt{34})$ zeigt, daß der entsprechende Satz für die gewöhnliche Klassengruppe falsch ist: k hat Klassenzahl 2, die Klasse von $\mathfrak{p} = (3, 5 + \sqrt{34})$ hat Ordnung 2 (denn $x^2 - 34y^2 = \pm 3$ liefert einen Widerspruch modulo 17, während $\mathfrak{p}^2 = (5 + \sqrt{34})$ Hauptideal im gewöhnlichen Sinne ist) und ist damit automatisch ambig, wird aber von keinem ambigen Ideal erzeugt, da alle ambigen Ideale Hauptideale sind: es ist nämlich $(2, \sqrt{34}) = (6 + \sqrt{34})$ und $(17, \sqrt{34}) = (17 + 3\sqrt{34})$. In $\mathrm{Cl}^+(k)$ dagegen ist die Idealklasse $[\mathfrak{p}^2]^+$ nicht trivial, da $(5 + \sqrt{34})$ keinen total positiven Erzeuger hat.

Unser nächstes Ziel ist die Berechnung der Anzahl der Geschlechter. Dazu führen wir einige Gruppen ein:

- $E = \mathcal{O}_k^\times$ ist die Einheitengruppe von $\mathcal{O}_k$;
- $E^+ = \{\varepsilon \in E : \varepsilon \gg 0\}$ ist deren Untergruppe total positiver Einheiten;
- $E^{1-\sigma} = \{\varepsilon^{1-\sigma} : \varepsilon \in E\}$;
- $U = E^+/(E^+ \cap E^{1-\sigma})$;
- A, die Gruppe der (gebrochenen) ambigen Ideale;

- I, die Untergruppe von A, die aus Idealen besteht, die von rationalen Zahlen erzeugt werden;
- $R = A/I$ schließlich ist deren Faktorgruppe.

Jetzt behaupten wir

Satz 5.6. *Sei k quadratischer Zahlkörper und t die Anzahl der verzweigten Primzahlen. Dann existiert eine exakte Sequenz*

$$1 \longrightarrow U \xrightarrow{\phi} R \xrightarrow{cl} Am^+ \longrightarrow 1, \tag{5.3}$$

und es gilt $U \simeq \mathbb{Z}/2\mathbb{Z}$ und $R = A/I \simeq (\mathbb{Z}/2\mathbb{Z})^t$. Insbesondere ist $C_+/C_+^2 \simeq (\mathbb{Z}/2\mathbb{Z})^{t-1}$.

Bevor wir diesen Satz beweisen, notieren wir einige Folgerungen:

Proposition 5.7. *Ist k ein quadratischer Zahlkörper, dessen Diskriminante eine Primzahlpotenz ist, dann hat k ungerade Klassenzahl (sogar im engeren Sinne).*

Beweis. Da genau ein Primideal verzweigt, ist $t = 1$, folglich C_+/C_+^2 trivial und damit $C_+ = C_+^2$. Also ist Quadrieren ein Automorphismus auf der endlichen Gruppe C_+, und dies impliziert, daß deren Ordnung ungerade sein muß (andernfalls gäbe es nach Cauchy ein Element der Ordnung 2, und dieses läge im Kern con $c \longmapsto c^2$). □

Korollar 5.8. *Ist* $\operatorname{disc} k$ *eine Primzahlpotenz, so hat k ungerade Klassenzahl im engeren Sinne. Ist $d = pq$, wo $p \equiv 2, 3 \bmod 4$ und $q \equiv 3 \bmod 4$ prim sind, dann sind alle ambigen Ideale Hauptideale im gewöhnlichen Sinne.*

Beweis. Ist $\operatorname{disc} k$ eine Primzahlpotenz, also $t = 1$, so folgt $C_+ = C_+^2$; also ist Quadrieren ein Automorphismus von C_+, und damit hat C_+ ungerade Ordnung.

Ist $d = pq$, so gilt $t = 2$ und $\#\mathrm{Am}^+(k) = 2$; dabei ist $[(\sqrt{pq}\,)]_+$ die ambige Idealklasse der Ordnung 2, denn die Fundamentaleinheit ε von k hat positive Norm (eine Gleichung $t^2 - pqy^2 = -4$ würde modulo p auf den Widerspruch $(t/2)^2 \equiv -1 \bmod p$ führen). Da die von $\mathfrak{p} = (p, \sqrt{pq}\,)$ und $\mathfrak{q} = (q, \sqrt{pq}\,)$ erzeugten Idealklassen im engeren Sinne ebenfalls ambig sind, müssen sie zu $[(1)]_+$ oder $[(\sqrt{pq}\,)]_+$ im engeren Sinne äquivalent sein; insbesondere sind es damit Hauptideale im gewöhnlichen Sinne. □

Beweis von Satz 5.6. Wir beginnen mit der Definition der Homomorphismen $\phi : U \longrightarrow R$ und $\mathrm{cl} : R \longrightarrow Am^+$. Dazu beobachten wir, daß für alle $\varepsilon \in E^+$ per definitionem $N\varepsilon = +1$ gilt; nach Hilberts Satz 90 ist also $\varepsilon = \alpha^{1-\sigma}$ für ein $\alpha \in k^\times$. Aber dann ist das Ideal $\alpha\mathcal{O}_k$ sicher ambig, und die Abbildung $\phi : \varepsilon \longmapsto \alpha\mathcal{O}_k$ induziert einen Homomorphismus $U \longrightarrow R$, den wir ebenfalls mit ϕ bezeichnen wollen.

Der Homomorphismus cl wird definiert, indem man $\mathfrak{a}I$ auf die Idealklasse $[\mathfrak{a}]_+$ abbildet. Damit bleibt noch die Exaktheit zu zeigen.

1. $\ker\phi = 1$: sei dazu $\phi(\varepsilon) = (a)$ für ein $a \in \mathbb{Z}$. Dann folgt aus $x^{\sigma-1} = \varepsilon$ und $x\mathcal{O}_k = a\mathcal{O}_k$, daß $a = \eta x$ für eine Einheit $\eta \in x$ gilt. Aber jetzt zeigt $1 = a^{\sigma-1} = x^{\sigma-1}\eta^{\sigma-1} = \varepsilon\eta^{\sigma-1}$, daß $\varepsilon = \eta^{1-\sigma} \gg 0$ ist.

2. $\mathrm{im}\,\phi \subseteq \ker \mathrm{cl}$: das ist klar, denn es gilt $\phi(\varepsilon) = (x)$ für ein $x \gg 0$.

3. $\mathrm{im}\,\phi \supseteq \ker \mathrm{cl}$: sei dazu $\mathfrak{a}^\sigma = \mathfrak{a}$ und $\mathfrak{a} = \lambda\mathcal{O}_k$ für ein $\lambda \gg 0$. Dann ist $\lambda^{\sigma-1} = \varepsilon$ eine total positive Einheit mit $\phi(\varepsilon) = \lambda\mathcal{O}_k$.

4. cl ist surjektiv: sei $c \in \mathrm{Am}^+$; then $c = [\mathfrak{a}]_+$ für ein ambiges Ideal $\mathfrak{a}$ (Proposition 5.5), und wir haben $c = \mathrm{cl}\,(\mathfrak{a}I)$.

Damit ist die Exaktheit nachgewiesen.

Nun zeigt man leicht, daß R eine 2-Gruppe ist, die von den Klassen $\mathfrak{p}_j I$ erzeugt wird, und daß $R \simeq (\mathbb{Z}/2\mathbb{Z})^t$ gilt. In der Tat: jedes ambige Ideal hat die Form $(m)\prod \mathfrak{p}_i^{e_i}$, wobei die $\mathfrak{p}_i$ verzweigt sind. Wegen $\mathfrak{p}_i^2 = (p_i)$ kann man Quadrate in das Ideal (m) hineinziehen und darf annehmen, daß $e_i \in \{0, 1\}$ ist. Jetzt setzt man

$$\phi : A/I \longrightarrow (\mathbb{Z}/2\mathbb{Z})^t : (m)\prod \mathfrak{p}_i^{e_i} \longmapsto (e_1, \ldots, e_t)$$

und zeigt, daß ϕ ein Gruppenisomorphismus ist. Als nächstes zeigen wir $U \simeq \mathbb{Z}/2\mathbb{Z}$.

Ist $d < 0$, so operiert σ wie -1 auf den Einheitswurzeln ε, die E erzeugen, folglich ist hier $E/E^{1-\sigma} = E/E^2 \simeq \mathbb{Z}/2\mathbb{Z}$. Ist $d > 0$, so sei ε die Fundamentaleinheit von k. Ist $N\varepsilon = +1$, so folgt $\varepsilon^{1-\sigma} = \varepsilon^2$ und $E^+ = E$, also $U = \langle\varepsilon\rangle/\langle\varepsilon^2\rangle \simeq \mathbb{Z}/2\mathbb{Z}$. Ist dagegen $N\varepsilon = -1$, dann ist $E^+ = \langle\varepsilon^2\rangle$ und $\varepsilon^{1-\sigma} = \langle-\varepsilon^2\rangle$, somit $E^+ \cap E^{1-\sigma} = \langle\varepsilon^4\rangle$ und schließlich $U \simeq \mathbb{Z}/2\mathbb{Z}$.

Zum Schluß müssen wir noch zeigen, daß $C_+/C_+^2 \simeq (\mathbb{Z}/2\mathbb{Z})^{t-1}$. Aber C_+/C_+^2 ist offenbar eine elementar-abelsche 2-Gruppe; nach (5.2) und (5.3) ist ihre Ordnung $(R : U)$, und dieser Index ist 2^{t-1}, wie wir gerade gezeigt haben. □

5.3 Das quadratische Reziprozitätsgesetz

Ein Korollar von Korollar 5.8 ist das quadratische Reziprozitätsgesetz:

Satz 5.9. *Sind p und q ungerade Primzahlen, so ist*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Darüberhinaus gelten die Ergänzungssätze $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ und $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

Beweis. Wir beginnen mit dem ersten Ergänzungssatz. Ist $p \equiv 1 \bmod 4$, so hat $k = \mathbb{Q}(\sqrt{p}\,)$ ungerade Klassenzahl im engeren Sinne, folglich ist $N\varepsilon_p = -1$; schreibt man $\varepsilon = \frac{1}{2}(t + u\sqrt{p}\,)$, so folgt $x^2 - py^2 = -4$, und daraus $(-4/p) = (-1/p) = 1$. Ist umgekehrt $(-1/p) = 1$, so ist p in $k = \mathbb{Q}(i)$ zerlegt; also ist $p = (a + bi)(a - bi)$, und Normenbildung liefert $p = a^2 + b^2$. Dies gibt aber sofort $p \equiv 1 \bmod 4$.

Ganz entsprechend zeigt man den zweiten Ergänzungssatz: wir setzen $p^* = (-1)^{(p-1)/2}p$; dann ist $p^* \equiv 1 \bmod 4$, und $k = \mathbb{Q}(\sqrt{p^*}\,)$ hat ungerade Klassenzahl h. Ist $p \equiv \pm 1 \bmod 8$, so ist 2 in $k/\mathbb{Q}$ zerlegt, also $2\mathcal{O}_k = \mathfrak{p}\mathfrak{p}'$. Da $\mathfrak{p}^h = \frac{1}{2}(x + y\sqrt{p^*}\,)$ Hauptideal ist, liefert Normenbildung $x^2 - p^*y^2 = \pm 4 \cdot 2^h$; tatsächlich dürfen wir annehmen, daß das positive Vorzeichen gilt: ist $p^* = p \equiv 1 \bmod 4$, so hat die Fundamentaleinheit Norm -1, und wir können $x + y\sqrt{p}\,)$ ggf. mit ε multiplizieren; ist aber $p \equiv 3 \bmod 4$, so ist $p^* < 0$ und die Norm ohnehin positiv. Also ist $x^2 - p^*y^2 = 2^{h+2}$, und damit $+1 = (2^{h+2}/p) = (2/p)$.

Jetzt zum eigentlichen Reziprozitätsgesetz: wir behandeln zuerst den Fall, daß eine der beiden Primzahlen, sagen wir p, kongruent $1 \bmod 4$ ist. Wir werden zeigen, daß $\left(\frac{p}{q}\right) = +1 \iff \left(\frac{q}{p}\right) = +1$ gilt.

Dazu stellen wir fest, daß $\left(\frac{p}{q}\right) = +1$ impliziert, daß q in $k = \mathbb{Q}(\sqrt{p}\,)$ zerlegt ist. Also ist $q\mathcal{O}_k = \mathfrak{q}\mathfrak{q}'$ und $\mathfrak{q}^h = \frac{1}{2}(x + y\sqrt{p}\,)$ Hauptideal, wobei $h = h^+$ nach Proposition 5.7 ungerade ist. Normenbildung liefert $\pm 4q^h = x^2 - py^2$. Dies wiederum gibt die Kongruenz $\pm 4q^h \equiv x^2 \bmod p$, also wegen $\left(\frac{-1}{p}\right) = +1$ auch $\left(\frac{q}{p}\right) = +1$ wie behauptet.

Ist dagegen $\left(\frac{q}{p}\right) = +1$, so hat $k = \mathbb{Q}(\sqrt{q^*}\,)$ ungerade Klassenzahl h, wobei wir $q^* = (-1)^{(q-1)/2}q$ gesetzt haben. Wieder folgt aus der Tatsache, daß p in $\mathcal{O}_k$ zerlegt ist, die Gleichung $\pm 4p^h = x^2 - q^*y^2$ und damit $\left(\frac{\pm p}{q}\right) = +1$. Da

entweder $q \equiv 1 \bmod 4$ und $(-1/q) = +1$ oder aber $q \equiv 3 \bmod 4$, q^* negativ und das Vorzeichen damit positive ist, folgt in der Tat $\left(\frac{p}{q}\right) = +1$.

Schließlich sei $p \equiv q \equiv 3 \bmod 4$. Zu zeigen ist, daß $\left(\frac{p}{q}\right) = +1 \iff \left(\frac{q}{p}\right) = -1$. Wir betrachten $k = \mathbb{Q}(\sqrt{pq})$. Nach Korollar 5.8 ist $\mathfrak{p} = (p, \sqrt{pq})$ ein Hauptideal, also $\mathfrak{p} = \frac{1}{2}(x + y\sqrt{pq})$. Dann ist $\pm 4p = x^2 - pqy^2$, also $x = pz$ und $\pm 4 = pz^2 - qy^2$. Gilt das positive Vorzeichen, so folgt durch Reduzieren modulo q und p, daß $(\frac{p}{q}) = +1$ und $(q/p) = -1$ ist; gilt das negative, so folgt entsprechend $(\frac{p}{q}) = -1$ und $(q/p) = +1$. Dies beendet den Beweis. □

Zusammenfassung

In diesem Kapitel ging es um

- Idealklassen im engeren Sinne,
- die Definition der Geschlechterklassengruppe $\mathrm{Cl}^+_{\mathrm{gen}}(k)$,
- der Bestimmung ihrer Struktur,
- und der Anwendung auf das quadratische Reziprozitätsgesetz.

Anhang A

Euler und die diophantische Gleichung $y^2 = x^3 - 2$

Dieser Anhang wurde nachträglich (Juli 1999) eingefügt.

Euler hat die diophantische Gleichung $y^2 = x^3 - 2$ (nebst vielen anderen) in seiner "Anleitung zur Algebra" behandelt. Im folgenden wollen wir einige Abschnitte daraus zitieren.

Euler beschäftigt sich mit der Lösung von $x^2 + cy^2 = z^3$; dazu schreibt er $z^3 = (x + y\sqrt{-c})(x - y\sqrt{-c})$ und folgert $x + y\sqrt{-c} = (p + q\sqrt{-c})^3$. Dies begründet er so:

191.

> Die hier gebrauchte Methode ist um so viel merckwürdiger, da wir durch Hülfe irrationaler und so gar imaginärer Formeln solche Auflösungen gefunden haben, wozu einig und allein rationale und so gar gantze Zahlen erfordert wurden. Noch merckwürdiger aber ist es, daß in denjenigen Fällen wo die Irrationalität verschwindet, unsere Methode nicht mehr statt findet: dann wann z.E. $xx + cyy$ ein Cubus seyn soll, so kann man sicher schließen daß auch die beyden irrationalen Factoren davon, nemlich $x + y\sqrt{-c}$ und $x - y\sqrt{-c}$, Cubos seyn müßen; weil dieselben unter sich untheilbar sind indem die Zahlen x und y keinen gemeinsamen Theiler haben. Fiele aber die Irrationalität $\sqrt{-c}$ weg, als wann z.E. $c = -1$ wäre, so würde dieser Grund nicht mehr stattfinden, weil alsdann die beyden Factoren nemlich $x + y$ und

$x - y$ allerdings gemeinsame Theiler haben könnten, ohngeacht x und y dergleichen nicht haben, z.E. wann beyde ungerade Zahlen wären.

Wann demnach $xx - yy$ ein Cubus seyn soll, so ist nicht nöthig daß sowohl $x + y$ als auch $x - y$ fürt sich ein Cubus sey, sondern man könnte wohl setzen $x + y = 2p^3$ und $x - y = 4q^3$, da dann $xx - yy$ ohnstreitig ein Cubus würde nemlich $8p^3q^3$, davon die Cubic-Wurzel ist $2pq$; alsdann aber wird $x = p^3 + 2q^3$, und $y = p^3 - 2q^3$. Wann aber die Formel $axx + cyy$ sich nicht in zwey rationale Factores zertheilen läßt, so finden auch keine andere Auflösungen statt, als die hier gegeben worden.

193.

II. Frage: Man verlangt solche Quadrate in gantzen Zahlen, welche wann zu 2 addirt wird Cubi werden, wie bey dem Quadrat 25 geschieht: ob es nun noch mehr dergleichen giebt wird hier gefragt?

Da also $xx + 2$ ein Cubus seyn soll, und 2 ein doppeltes Quadrat ist, so suche man erstlich die Fälle, wo die Formel $xx + 2yy$ ein Cubus wird, welches aus dem obige Articul 188, wo $a = 1$ und $c = 2$, geschieht, wann $x = p^3 - 6pqq$ und $y = 3ppq - 2q^3$; da nun hier $y = \pm 1$ so muß seyn $3ppq - 2q^3 = q(3pp - 2qq) = \pm 1$, und also q ein Theiler von 1; es sey demnach $q = 1$, so wird $3pp - 2 = \pm 1$; gilt das obere Zeichen, so wird $3pp = 3$ und $p = 1$, folglich $x = 5$; das untere Zeichen aber giebt vor p einen irrationalen Werth, welcher hier nicht statt findet; woraus folgt, daß nur das einzige Quadrat 25 in gantzen Zahlen die verlangte Eigenschaft habe.

195.

IV. Frage: Man suche solche Quadrate in gantzen Zahlen, welche doppelt genommen wann davon 5 subtrahirt wird, daß ein Cubus heraus komme; oder $2xx - 5$ soll ein Cubus seyn.

Man suche erstlich diejenigen Fälle da $2xx - 5yy$ ein Cubus wird, welches nach dem 188ten Articul, wo $a = 2$ und $c = -5$, geschieht,

> wann $x = 2p^3 + 15pqq$ und $y = 6ppq + 5q^3$. Hier aber muß seyn $y = \pm 1$, und folglich
>
> $$4ppq + 5q^3 = q(6pp + 5qq) = \pm 1,$$
>
> welches in gantzen Zahlen nicht geschehen kann, und auch nicht einmahl in Brüchen; dahero dieser Fall sehr merckwürdig ist, da gleichwohl ein Auflösung statt findet, wann nemlich $x = 4$, dann da wird $2xx - 5 = 27$, welches der Cubus ist von 3; und hievon ist es von der größten Wichtigkeit den Grund zu untersuchen.

Mit anderen Worten: Euler hat zu seiner Methode ein Gegenbeispiel gefunden, sieht aber nicht, wo die Lücke in seiner Argumentation ist. Tatsächlich gibt es deren zwwi: einmal die nicht eindeutige Faktorisierung in irreduzible Elemente in quadratischen Zahlringen, zum andern die Existenz nicht trivialer Einheiten.