Franz Lemmermeyer

Quadratische Zahlkörper
Schnupperkurs

Franz Lemmermeyer
hb3@ix.rzuser.uni-heidelberg.de
http://www.rzuser.uni-heidelberg.de/~hb3

Vorwort

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

Als Voraussetzungen reichen Kenntnisse der linearen Algebra (Vektorräume, lineare Abbildungen, Matrizenrechnung), sowie eine Vertrautheit mit Begriffen der elementaren Zahlentheorie (eindeutige Primfaktorzerlegung, Kongruenzrechung, quadratische Reste); nur im letzten Kapitel über Geschlechter wird etwas abstrakte Algebra auf dem Niveau der Isomorphiesätze verwendet. Mit * gekennzeichnete Abschnitte sind für das Verständnis der nachfolgenden Kapitel entbehrlich.

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 für Zahlen, die nicht von einer besonderen Form sind (wie z.B. die bereits oben erwähnten Mersenne-Zahlen $2^p - 1$), ist das 'number field sieve', das auf der Arithmetik allgemeiner Zahlkörper aufbaut.

P.S. (2011)

Ich habe, auch wenn ich heute manches anders machen würde, den Text nicht wesentlich abgeändert; eine Ausnahme ist der Beweis der Unlösbarkeit der kubischen Fermatgleichung $x^3 + y^3 = z^3$ in von 0 verschiedenen ganzen Zahlen, der ursprünglich zwar direkter, aber auch viel verwickelter war als der jetzt gegebene. Außerdem habe ich zwei verschiedene Lösungen der diophantischen Gleichung $y^2 = x^3 + 1$ aufgenommen, und in Kapitel 5 die Einführung der Idealklassengruppe im engeren Sinne vermieden. Neben einigen eher kosmetischen Ergänzungen habe ich bei einigen Punkten zusätzliche Literaturhinweise gegeben, und ein Anhang enthält eine kleine Einführung in das Rechnen mit `pari` und `sage`.

Franz Lemmermeyer — Jagstzell 2011

[1] Dieser wurde 1999 als zweistündige Vorlesung an der Universität des Saarlands in Saarbrücken "vor kleinem Hause" gehalten.)

Einige Lehrbücher

[Ar] M. Artin, *Algebra*, Birkhäuser Verlag (1993)

Eine wunderschöne Einführung in die Algebra von Emil Artins Sohn Michael, in der viel Wert auf Anschaulichkeit, Intuition und Beispiele gelegt wird.

[BS] Z. Borewicz, I. Shafarevich, *Zahlentheorie*, Birkhäuser 1966

Ebenfalls ein Klassiker; die algebraische Zahlentheorie wird hin bis zu den Klassenzahlformeln entwickelt.

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

Eine Einführung in die algebraische Zahlentheorie mit vielen Dingen, die man anderswo nicht findet. Der Anhang enthält Artins Vorlesungen zur Klassenkörpertheorie.

[C2] H. Cohn, *Advanced number theory*, Dover Publications (1980); Original: *A second course in number theory*, John Wiley and Sons (1962).

Eine der wenigen Einführungen in die algebraische Zahlentheorie, die binäre quadratische Formen ernstnimmt.

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

Eine kurze und knappe Einführung in die elementare Zahlentheorie und p-adische Zahlen, die von [BS] inspiriert ist.

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

Der Klassiker. Neben vielem anderen findet man dort auch eine Einführung in die Theorie quadratischer Zahlkörper.

[He] E. Hecke, *Vorlesungen über die Theorie der algebraische Zahlen*, 1. Aufl. 1923

Ein Musterbeispiel an gelungenem Aufbau und Tiefe – besser geht es nicht. Es verlangt den Lesern aber Einiges ab und geht zum Schluss in die Klassenkörpertheorie über.

[IR] K. Ireland, K. Rosen, *A classical introduction to modern number theory*, Springer-Verlag (1990)

Vielleicht die beste Einführung in die Zahlentheorie überhaupt. An Breite ist es vergleichbar mit Hardy und Wright, aber die Themenauswahl ist sehr viel moderner: Zetafunktionen, Funktionenkörper, elliptische Kurven, ...

[Ko] A.I. Kostrikin, *Introduction to algebra*, Universitext, Springer-Verlag (1982)

Neben Artins Buch war dieses Algebrabuch wegen seiner ungewöhnlichen Beispiele mein Favorit.

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

Eine historische Einführung in die Zahlentheorie – absolut empfehlenswert!

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

Eines der ersten Lehrbücher zur algebraischen Zahlentheorie, entstanden unter dem Eindruck von Hilberts Zahlbericht. Es enthält sehr viele Beispiele und ist sehr viel Anfänger-freundlicher als das weitaus tiefere Buch von Hecke.

[ST] I. Stewart, D. Tall, *Algebraic number theory*, 2nd ed. Chapman and Hall (1987)

Eine Einführung in die algebraische Zahlentheorie, die es nicht eilig hat.

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

Auch dieses Buch ist ein absolutes Muss: hier wird der Zugang über die analytische Seite der algebraischen Zahlentheorie gesucht; sogar die Theorie der binären quadratischen Formen wird mustergültig abgehandelt.

Inhaltsverzeichnis

Vorwort v

Lehrbücher vi

1. Motivation und Vorstellung der Akteure 3
1.1 Identitäten 3
1.2 * Fibonacci-Zahlen 4
1.3 * Die elliptische Kurve $y^2 = x^3 - 2$. 5
1.4 Quadratische Zahlkörper 8

2. Teilbarkeit in Integritätsbereichen 12
2.1 Einheiten, prime und irreduzible Elemente 12
2.2 ZPE-Ringe 16
2.3 Hauptidealringe 18
2.4 Euklidische Ringe 21
2.5 * Die Fermatgleichung $x^4 + y^4 = z^4$ 23
2.6 * Die diophantische Gleichung $y^2 = x^3 + 1$ 24

3. Arithmetik in einigen quadratischen Zahlkörpern 26
3.1 Die Gaußschen Zahlen 26
3.2 Die Eisensteinschen Zahlen 31
3.3 * Die Fermatgleichung $x^3 + y^3 + z^3 = 0$ 33
3.4 Die Pellsche Gleichung 37
3.5 * Welche Zahlen sind Normen? 39
3.6 * Der Lucas-Lehmer-Test 41
3.7 * Euklidische Quadratische Zahlkörper 45

4. Idealarithmetik in quadratischen Zahlkörpern 48
4.1 Motivation 48
4.2 Eindeutige Primidealzerlegung 50
4.3 Die Idealklassengruppe 55
4.4 * Die diophantische Gleichung $y^2 = x^3 - d$ 59

5. Ambige Idealklassen und quadratische Reziprozität 64
5.1 Ambige Idealklassen 64
5.2 Die ambige Klassenzahlformel 66
5.3 Das Quadratische Reziprozitätsgesetz 70

A. Satz von Delaunay und Nagell 72
A.1 Der Diskriminantentrick von Trost 72
A.2 Einheiten in kubischen Zahlringen 72

B. Rechnungen mit pari und sage 74
B.1 Pari 74
B.2 sage 77

Namensverzeichnis 80

Sachverzeichnis 81

1. Motivation und Vorstellung der Akteure

Quadratische Zahlkörper gehören naturgemäß zur algebraischen Zahlentheorie, also der Theorie der algebraischen Zahlen. Quadratische Zahlkörper wie Zahlkörper höheren Grades treten bei der Untersuchung mancher Probleme der elementaren Zahlentheorie ganz natürlich auf, wie die folgenden Beispiele zeigen. Eine formale Definition von quadratischen Zahlkörpern folgt am Ende dieses Kapitels; in den darauffolgenden Kapiteln wird die Theorie dann so weit entwickelt, wie es zum vollen Verständnis der nun folgenden Probleme notwendig ist.

1.1 Identitäten

Ein Reihe von Problemen bei Schülerolympiaden basiert auf folgender Beobachtung: sind die natürlichen Zahlen m und n Summen zweier Quadrate, dann auch ihr Produkt mn. Der Beweis besteht einfach aus dem Nachrechnen der Identität

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2. \tag{1.1}$$

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[1].

Man sieht also, dass die Einführung von Zahlen der Form $x + y\sqrt{m}$ mit rationalen Zahlen x, y das Auffinden von Identitäten[2] wie den obigen erleichtert.

[1] Bereits Brahmagupta benutzte diese Identität zur Lösung von Gleichungen $x^2 = my^2 + 1$ in ganzen Zahlen.

[2] Eine Identität analog zu (1.1) für Summen von drei Quadraten gibt es nicht: so sind $3 = 1^2 + 1^2 + 1^2$ und $5 = 0^2 + 1^2 + 2^2$ Summen von drei Quadraten, $15 = 3 \cdot 5$ dagegen nicht. Eine Produktformel für Summen von vier Quadraten wurde von Euler gefunden; diese verdankt ihre Existenz den Quaternionen: das sind Zahlen der Form $\alpha = a + bi + cj + dk$ mit $i^2 = j^2 = k^2 = -1$, die wegen $ij = -ji$, $jk = -kj$ und $ik = -ki$ aber einen nichtkommutativen Ring bilden. Setzt man $\alpha' = a - bi - cj - dk$ und definiert $N\alpha = \alpha\alpha'$, so rechnet man leicht nach, dass $N\alpha = a^2 + b^2 + c^2 + d^2$ ist. Die Produktformel folgt dann leicht aus $N(\alpha\beta) = N\alpha N\beta$. Den Zusammenhang mit Summen von vier Quadraten hat Hurwitz ausgenutzt, um den Euler-Lagrangeschen Beweis des Vierquadratesatzes ("jede natürliche Zahl ist Summe von höchstens vier Quadratzahlen") in die Sprache der Quaternionen zu übersetzen.

1.2 * Fibonacci-Zahlen

Die Fibonacci-Zahlen[3] 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:

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

Wie kann man das beweisen? Eine Möglichkeit ist via der Binetschen[4] 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:

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 Zahlen 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

$$\alpha^p \equiv \frac{1^p + \sqrt{5}^p}{2^p} = \frac{1 + 5^{(p-1)/2}\sqrt{5}}{2} \bmod p, \tag{1.2}$$

[3] 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.

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

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 (1.2) 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.[5]

Zeige, dass in beliebigen Ringen $(a+b)^p \equiv a^p + b^p \bmod p$ gilt.

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

Fermat[6] hat behauptet, dass $x = 3$, $y = \pm 5$ die einzigen ganzzahlige Lösungen der diophantischen Gleichung $y^2 = x^3 - 2$ sind; Euler[7] hat sich an einem Beweis versucht, der zwar lückenhaft ist, aber doch Eulers Originalität unterstreicht. Kleinere Lücken im folgenden Beweis werden im Laufe der Vorlesung geschlossen werden.

Das Motiv hinter Fermats Beweis wird uns in dieser Vorlesung auf Schritt und Tritt begegnen: es ist die Umwandlung eines additiven Problems in ein multiplikatives. Ein ganz klassisches, auf die Griechen zurückgehendes Beispiel hierfür ist die

[5] Joseph Louis Lagrange (1736–1813), italienisch-französischer Mathematiker, der in der Zahlentheorie vor allem für seine Beweise des Vierquadratesatzes (jede natürliche Zahl ist Summe von höchstens vier Quadratzahlen) und der Lösbarkeit der Pellschen Gleichung, sowie für seine Theorie der Reduktion binärer quadratischer Formen bekannt ist.

[6] Pièrre Fermat (1607–1665) wurde durch das Studium der von Bachet herausgegebenen Bücher Diophants zur Untersuchung zahlentheoretischer Probleme angeregt; in eines dieser Bücher trug er die berüchtigte Vermutung ein, dass die Gleichung $x^n + y^n = z^n$ für kein $n \geq 3$ 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 später 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).

Was das Geburtsjahr von Fermat angeht, vergleiche man K. Barner [*How old did Fermat become?*, NTM (N.S.) **9** (2001), 209–228] und [*Das Leben Fermats*, Mitt. Dtsch. Math.-Ver. 2001, no. 3, 12–26].

[7] 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.

Klassifikation primitiver pythagoreischer Tripel (von Fermat und seinen Zeitgenossen auch der Fundamentalsatz über rechtwinklige Dreiecke genannt). Dazu erinnern wir daran, dass ein Tripel (x, y, z) natürlicher Zahlen ein primitives pythagoreisches Tripel heißt, 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 1.1. *Ist (x, y, z) ein primitives pythagoreisches 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. Wir schreiben die additive Gleichung $x^2 + y^2 = z^2$ in der Form $x^2 = z^2 - y^2 = (z - y)(z + y)$; 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 2.9 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 kehren wir zu unserer Gleichung $y^2 = x^3 - 2$ zurück. Zuerst beachten wir, 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. In Prop. 2.8 werden wir sehen, wie mit der ZPE-Eigenschaft die Behauptung folgt.). 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 $\pm 1 = s(3r^2 - 2s^2)$. Aus der letzten folgt $s = \pm 1$, damit $r = \pm 1$, und schließlich $y = \pm 5$, also Fermat's Behauptung[8].

Diophantische Gleichungen der Form $E : y^2 = x^3 + ax + b$ mit $a, b \in \mathbb{Z}$ heißen (unter ganz schwachen Voraussetzungen[9] an $a, b \in \mathbb{Z}$) *elliptische Kurven.* Die

[8] Es ist meines Wissens unbekannt, ob sich dieser Fermatsche Satz mit Mitteln der elementaren Zahlentheorie beweisen lässt. Undenkbar ist das nicht: beispielsweise könnte man die Gleichung in der Form $(y-5)(y+5) = y^2 - 25 = x^3 - 27 = (x-3)(x^2+3x+9)$ schreiben und zu beweisen versuchen, dass diese Gleichung nur ganzzahlige Lösungen hat, wenn einer der vier Faktoren verschwindet. Gelungen ist mir in dieser Richtung aber bisher noch nichts. Was die Schwierigkeit eines Beweises nach unten begrenzt ist die schon von Bachet und Fermat beobachtete Tatsache, dass die Gleichung $y^2 = x^3 - 2$ unendlich viele rationale Lösungen besitzt.

[9] Das Polynom $f(x) = x^3 + ax + b$ darf keine mehrfachen Nullstellen in einem algebraischen Abschluss des betrachteten Körpers haben.

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. 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[10] 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

[10] Heute ist der Wiles'sche Beweis Allgemeingut und die Episode weit weniger aufregend als 1995. Ich war am Tag der dritten Vorlesung von Wiles in Heidelberg, wo auf einem kleinen Symposium, wenn ich mich recht erinnere, auch Paolo Ribenboim vorgetragen hat und die email per Aushang an der Tür des Mathematischen Instituts in einer Vortragspause bekannt gemacht wurde.

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

Tatsächlich war das Drama damit noch nicht zu Ende: eine genaue Durchsicht des Manuskriptes zeigte, dass der Beweis eine wesentliche Lücke hatte. Es sollte noch einmal etwa ein Jahr dauern, bis Wiles (zusammen mit Taylor) diese Lücke geschlossen hatte.

1.4 Quadratische Zahlkörper

Sei $m \in \mathbb{Z}\backslash\{0,1\}$ 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

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

Ursprünglicher Sinn und Zweck der Einführung quadratischer Zahlringe waren zahlentheoretische Probleme in den gewöhnlichen ganzen Zahlen. Um von Aussagen in quadratischen Zahlringen R auf solche in $\mathbb{Z}$ zu kommen, sind natürlich Abbildungen $R \longrightarrow \mathbb{Z}$ wichtig. Da wir vor allem multiplikative Strukturen betrachten werden (Zerlegung in Faktoren, Einheiten), sind multiplikative Abbildungen wie die Norm besonders wichtig.

Proposition 1.2. *Für alle $\alpha, \beta \in k$ gilt*

$$N(\alpha\beta) = N\alpha\, N\beta \quad \textit{und} \quad \mathrm{Tr}\,(\alpha + \beta) = \mathrm{Tr}\,\alpha + \mathrm{Tr}\,\beta.$$

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. □

Übung. Zeige, dass genau dann $\mathrm{Tr}\,(\alpha) = 0$ ist, wenn $\alpha \in \sqrt{m} \cdot \mathbb{Q}$ ist, d.h. wenn α ein rationales Vielfaches von $\sqrt{m}$ ist.

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.

Wegen $\sigma \circ \sigma = \mathrm{id}$ (die identische Abbildung) ist $\{\mathrm{id}, \sigma\}$ eine Gruppe der Ordnung 2, die man die *Galoisgruppe*[11] von $k/\mathbb{Q}$ nennt und mit $\mathrm{Gal}\,(k/\mathbb{Q})$ bezeichnet.

Quadratische Körpererweiterungen als Vektorräume

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.

Übung. Sei $K/\mathbb{Q}$ eine quadratische Erweiterung. Verifiziere, dass K ein k-Vektorraum ist.

Zeige, dass die Multiplikation mit $\alpha = a + b\sqrt{m} \in K$ eine lineare Abbildung $K \longrightarrow K$ ist, welche in Matrixdarstellung bezüglich der $\mathbb{Q}$-Basis $\{1, \sqrt{m}\,\}$ von K durch $x \to Ax$ gegeben ist, wobei $x = \left(\begin{smallmatrix} r \\ s \end{smallmatrix}\right)$ das Element $r + s\sqrt{m}$ beschreibt und A gegeben ist durch $A = \left(\begin{smallmatrix} a & mb \\ b & a \end{smallmatrix}\right)$.

Zeige, dass $N\alpha = \det A$ und $\mathrm{Tr}\,\alpha = \mathrm{Tr}\,A$ gilt, und dass Norm und Spur nicht von der Wahl der Basis abhängen.

Ganze Algebraische Zahlen.

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 $\mathcal{O}_k$.

Übung. Zeige, dass α genau dann ganz ist, wenn auch $\sigma(\alpha)$ ganz ist.

Nun gilt

Satz 1.3. *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* $m \equiv 1 \bmod 4$.

[11] Nach Évariste Galois (1811–1832), einem französischen Mathematiker, der nach einem Duell im Alter von 20 Jahren starb. Galois revolutioniert die Mathematik durch Einführung von Hilfsmitteln in die Theorie der Auflösung von Gleichungen durch Radikale. Diese "Galoistheorie" verwandelte sich erst im Laufe der Zeit (mit Steinitz, um einen Namen zu nennen) von einer Theorie der Polynome zu einer Theorie der Körpererweiterungen.

Beweis. Sei $\alpha = r + s\sqrt{m}$ ganz mit $r, s \in \mathbb{Q}$; damit sind $\operatorname{Tr}\alpha = 2r$ 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 $\operatorname{ggT}(x, y) = 1$ 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.
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 1.4. *Es gilt $\mathcal{O}_k = \mathbb{Z} \oplus \omega\mathbb{Z}$ mit*

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

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 1.3 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 1.5. *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 1.5 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 $\in \mathbb{Z}[x]$ und 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. 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 $G = \mathrm{Gal}\,(k/\mathbb{Q})$ auf den abelschen Gruppen k, $k^\times$ und $\mathcal{O}_k$ via $(\sigma, \alpha) \longmapsto \sigma(\alpha)$ operiert.

Übung. Löse die Gleichung $x^2 + y^2 = 2z^2$ mit "Eulers Trick": schreibe die Gleichung in der Form $(x + y)^2 + (x - y)^2 = (2z)^2$.

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 $\mathrm{disc}\, k$ 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

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 bezüglich 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 $\mathbb{Z}$).

Übung. Zeige: gilt im Ring $\mathbb{Z}[\sqrt{-2}]$ die Relation $\sqrt{-2} \mid y$ für ein $y \in \mathbb{Z}$, dann ist $2 \mid y$.

Zeige allgemeiner, dass aus $\sqrt{m} \mid y$ immer auch $m \mid y$ folgt.

Finde ein Gegenbeispiel zur Behauptung, aus $\alpha \mid y$ würde immer $N\alpha \mid y$ folgen.

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

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 1.5 zeigt $\gamma \in \mathbb{Z}$, also $a \equiv b \bmod m\mathbb{Z}$ in $\mathbb{Z}$. $\square$

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.

Übung. Ist $R = K$ ein Körper, so gilt $K^\times = K \setminus \{0\}$.

Übung. Ist R ein Integritätsbereich (also nullteilerfreier kommutativer Ring mit Eins) und $R[X]$ der Polynomring in einer Variablen mit Koeffizienten aus R, dann ist $R[X]^\times = R^\times$, d.h. die Einheiten in diesem Polynomring sind alle konstant.

Zeige andererseits, dass das Polynom $2X + 1$ in $(\mathbb{Z}/4\mathbb{Z})[X]$ eine Einheit ist.

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 Ring $\mathbb{Z}[i]$ der Gaußschen Zahlen $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ $N\alpha = 1$ 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*

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

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.*

[1] John Pell (1611–1685), englischer Mathematiker. Der Name 'Pellsche' Gleichung geht auf einen Fehler Eulers zurück, der in seiner Algebra Pell mit dem englischen Mathematiker Brouncker verwechselt hat. Dieser hatte auf Verlangen Fermats ein Verfahren angegeben, mit dessen Hilfe man solche Gleichungen lösen konnte – den Beweis, dass dieses Verfahren für alle Nichtquadrate $m > 1$ auch funktioniert, konnte erst Lagrange erbringen.

Ein ganz ähnliches Lösungsverfahren war übrigens bereits indischen Mathematikern wie Brahmagupta und Bhaskara bekannt; deren Beiträge wurden in Europa aber erst lange nach Fermat bekannt.

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.

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 $R = \mathbb{Z}[\sqrt{-5}\,]$).

Zusammenfassend sind

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}\,)(1 - \sqrt{-5}\,) \tag{2.1}$$

zwei wesentlich verschiedene Zerlegungen der Zahl 6 in irreduzible Elemente. Wir haben das deswegen genau nachgerechnet, weil Zerlegungen, die verschieden aussehen, nicht notwendig auch wirklich verschieden sind. Beispielsweise ist

$$6 = 2 \cdot 3 = (2 + \sqrt{-2}\,)(2 - \sqrt{-2}\,)$$

in $\mathbb{Z}[\sqrt{-2}\,]$; in diesem Ring lassen sich die beiden Faktorisierungen aber erklären, da die einzelnen Faktoren nicht irreduzibel sind:

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

Die beiden Faktorisierungen kommen also dadurch zustande, dass man die irreduziblen Faktoren in der Zerlegung

$$6 = -\sqrt{-2}^2 (1 + \sqrt{-2}\,)(1 - \sqrt{-2}\,)$$

auf verschiedene Arten gruppiert.

Übung. Sei S der Ring, den man erhält, wenn man zu $R = \mathbb{Z}[\sqrt{-5}\,]$ das Element $\omega = \frac{1}{2}(1 + \sqrt{-5}\,)$ hinzunimmt. Zeige, dass $S = R[\frac{1}{2}]$ und $S \cap \mathbb{Z} = \mathbb{Z}[\frac{1}{2}]$ ist.

Zeige weiter, dass die Zerlegung (2.1) kein Beispiel für eine nichteindeutige Zerlegung in irreduzible Elemente ist. Tatsächlich überzeuge man sich davon, dass

$$3 = \frac{1}{2}(1 - \sqrt{-5}\,)(1 + \sqrt{-5}\,)$$

eine Zerlegung von 3 in die Einheit $\frac{1}{2}$ und die beiden irreduziblen (sogar primen) Elemente $1 \pm \sqrt{-5}$ ist. Löse auch die Gleichung $3 \cdot 3 = (2 - \sqrt{-5}\,)(2 + \sqrt{-5}\,)$ in irreduzible Elemente auf.

Übung. Ebenso wie das Beispiel (2.1) 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. 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?

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.)

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[2] sind solche π aber sogar prim:

Proposition 2.6. *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 (sh. den nächsten Abschnitt), 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 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 $\beta \equiv B = 0 \bmod \pi$.

2.2 ZPE-Ringe

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

[2] Wir werden diese Aussage später ganz zwanglos aus der Idealtheorie erhalten. An dieser Stelle wollte ich nur zeigen, dass es auch direkt geht, auch wenn der Beweis im wesentlichen idealtheoretischen Charakter hat: wir zeigen, dass π prim ist, indem wir nachweisen, dass $\mathcal{O}_k/(\pi)$ nullteilerfrei, also (π) ein Primideal ist.

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 2.7. *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 einen solchen Beweis erstmals geführt haben[3], 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.

[3] Will man historisch etwas genauer sein, muss man diese Aussage vorsichtiger formulieren. Vgl. Lemmermeyer, *Zur Zahlentheorie der Griechen. I: Euklids Fundamentalsatz der Arithmetik*, Math. Semesterber. **55** (2008), 181–195.

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! Zum einen braucht es in Ringen ohne eindeutige Primfaktorzerlegung keinen größten gemeinsamen Teiler zu geben, zum andern hat dann, selbst wenn $d = \mathrm{ggT}\,(a, b)$ existiert, dieser nicht die Eigenschaften, die wir von ihm erwarten, wie z.B. $\mathrm{ggT}\,(a, b)^2 = \mathrm{ggT}\,(a^2, b^2)$.

Übung. Zeige, dass in $R = \mathbb{Z}[\sqrt{-5}\,]$ die beiden Zahlen $a = 1+\sqrt{-5}$ und $b = 1-\sqrt{-5}$ keinen gemeinsamen Teiler außer ± 1 haben, dass aber 2 ein gemeinsamer Teiler von a^2 und b^2 ist.

Proposition 2.8. *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 $b = e_2 d^n$. Dabei gilt $cd = x$ und $e_1 e_2 = e$.*

Beweis. Wir führen 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 2.9. *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 2.8 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.

Übung. Zeige, dass die geraden Zahlen $2\mathbb{Z}$ ein Ideal in $\mathbb{Z}$ bilden. Allgemeiner sind die Mengen $m\mathbb{Z}$ für beliebiges $m \in \mathbb{Z}$ Ideale in $\mathbb{Z}$.

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.

Übung. Zeige, dass die Menge $2\mathbb{Z} + \sqrt{2}\,\mathbb{Z}$ ein Ideal in $\mathbb{Z}[\sqrt{2}\,]$ ist, das genau aus den Vielfachen von $\sqrt{2}$ besteht. Zeige weiter, dass $\mathbb{Z} + 2\sqrt{2}\,\mathbb{Z}$ zwar ein Teilring von $\mathbb{Z}[\sqrt{2}\,]$ ist, aber kein Ideal.

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 – für mehr über euklidische Ringe sh. Abschnitt 2.4), 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.

Übung. Sei R der Ring aller ganzen algebraischen Zahlen. Zeige, dass 2 keine Zerlegung in irreduzible Elemente besitzt: $2 = \sqrt{2}^2 = \sqrt[4]{2}^4 = \ldots$. Zeige auch, dass das Ideal $(2, \sqrt{2}, \sqrt[4]{2}, \sqrt[8]{2}, \ldots)$ kein Hauptideal, ja nicht einmal endlich erzeugt ist.

Satz 2.10. *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 $a_2 \mid a_1$, $a_3 \mid a_2, \ldots$, 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'[4] 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.

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

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 anfangs 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 2.11. *Euklidische Ringe sind Hauptidealringe.*

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

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

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. Man versuche, mit dem in Kapitel 1 vorgestellten Verfahren etwas über die ganzzahligen Lösungen der diophantischen Gleichung $y^2 = x^3 + k^2$ für ein festes $k \in \mathbb{Z}$ herauszubekommen. Die Bezeichnung offenes Problem ist hier aber eher angebracht; wer keine vollständige Lösung hinbekommt, sollte also nicht verzweifeln (und wer eine findet, sollte den Fehler suchen).

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.

Übung. Die Bemerkungen aus der vorhergehenden Übung gelten auch hier: man untersuche für $k \in \mathbb{Z}$ die Gleichung $y^2 = x^3 - k^2$. Man sollte auf jeden Fall herausbekommen, dass diese Gleichung lösbar ist, wenn $k = b(3a^2 - b^2)$ oder $k = 2(a^3 + 3a^2b - 3ab^2 - b^3)$ ist. Für $k = 88$ gibt es zwei verschiedene Darstellungen $k = b(3a^2 - b^2)$, also mindestens zwei Lösungen der Gleichung $y^2 = x^3 - k^2$. Kann die Anzahl der Lösungen beliebig groß werden?

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

Einer der wenigen Beweise von Fermat, die überlebt[5] haben, ist der von

Satz 2.12. *Die diophantische Gleichung $x^4+y^4 = z^2$ hat nur die trivialen Lösungen (das sind solche mit $xy = 0$).*

Insbesondere hat auch die Gleichung[6] $x^4 + y^4 = z^4$ keine nicht-trivialen Lösungen. Der Beweis beruht auf der Idee des unendlichen Abstiegs (descente infinie; infinite descent): ausgehend von einer Lösung $(x, y, z) \in \mathbb{N}^3$ konstruiert 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.

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 1.1 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 1.1 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 $c^2 + d^2$ 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 2.8 (zuerst auf das Paar cd und $c^2 + d^2$, dann auf das Paar c und d) folgt, dass diese Faktoren bis auf

[5] In diesem Fall hat nicht nur Fermat eine Beweisskizze gegeben; vielmehr hat auch sein Korrespondenzpartner Frenicle de Bessy eine detaillierte Ausarbeitung des Beweises veröffentlicht. Wie groß der Fermatsche Anteil an Frenicles Beweis ist, ist auch (oder gerade) unter Experten umstritten.

[6] Erstaunlicherweise ist es nicht einfacher, sondern schwieriger, die Unlösbarkeit der spezielleren Gleichung $x^4 + y^4 = z^4$ zu zeigen als die von $x^4 + y^4 = z^2$. Der Grund dafür ist folgender: die Gleichung $x^4 + y^4 = z^2$ beschreibt, wie wir unten zeigen werden, eine elliptische Kurve; die Arithmetik solcher Kurven ist im Vergleich zu derjenigen von Kurven wie $x^4 + y^4 = z^4$ deutlich einfacher.

eine Einheit ± 1 selbst Quadrate sein 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 2.8!

Der Diskriminantentrick von Trost

Der folgende Trick von Trost (*Eine Bemerkung zur diophantischen Analysis*, 60–61) ist zwar simpel, aber manchmal erstaunlich nützlich. Ist eine diophantische Gleichung

$$aX^2 + bX + c = 0$$

gegeben und hat diese eine rationale Lösung X, dann muss selbstverständlich die Diskrminante $b^2 - 4ac$ ein Quadrat sein.

Aus dieser fast trivialen Tatsache wird durch folgenden Trick eine hilfreiche Methode: ist $x^4 - 4y^4 = z^2$ in ganzen (oder auch rationalen) Zahlen lösbar, dann hat die quadratische Gleichung $x^4 - tz^2 - 4y^4t^2$ eine rationale Lösung für $t = 1$; d.h. die Diskriminante Δ des in t quadratischen Polynoms muss ein Quadrat werden, also $\Delta = z^4 + 16x^4z^4 = w^2$ lösbar sein. Nun hat diese Gleichung aber nur die trivialen Lösungen $x = 0$ und $z = 0$; deshalb kann auch die Ausgangsgleichung nur diese Lösungen haben.

Auf ähnliche Art und Weise kann man so zeigen, dass die Gleichung $x^4 - 2y^2 = 1$ nur triviale Lösungen in $\mathbb{Z}$ hat. Ist $y^2 = x^3 - dx$ lösbar, so auch (via $dxt^2 + y^2t - x^3t^2$) die Gleichung $y^4 + 4dx^4 = w^2$ usw.

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 2.8 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 $\operatorname{ggT}(y+1, y-1) = 2$, und nach Proposition 2.8 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 nicht ganz leicht 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).

Der Übergang zum kubischen Zahlkörper $\mathbb{Q}(\sqrt[3]{2})$ lässt sich vermeiden, wenn man die Gleichung $a^3 - 2b^3 = 1$ in der Form

$$2b^3 = a^3 - 1 = (a - 1)(a - \rho)(a - \rho^2)$$

mit $\rho = \frac{-1+\sqrt{-3}}{2}$ schreibt und die Arithmetik in $\mathbb{Z}[\rho]$ verwendet, die wir im nächsten Kapitel vorstellen werden.

Die andere Möglichkeit ist, die Gleichung $y^2 = x^3 + 1$ gleich von Anfang an in der Form

$$y^2 = (x + 1)(x + \rho)(x + \rho^2)$$

zu schreiben und dann in $\mathbb{Z}[\rho]$ zu rechnen.

In jedem Fall muss man aber in einen algebraischen Zahlkörper $\neq \mathbb{Q}$ gehen, um die Gleichung zu lösen. Dies werden wir im nächsten Kapitel nachholen.

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.

3. Arithmetik in einigen quadratischen Zahlkörpern

Obwohl bereits Euler versucht[1] hat, mit Zahlen der Form $a+b\sqrt{-2}$ zu rechnen, um damit die Fermatsche Behauptung zu beweisen, dass die diophantische Gleichung $y^2+2=x^3$ die einzige Lösung $(x,y)=(3,\pm 5)$ hat, wurden die Grundlagen der Arithmetik eines quadratischen Zahlrings erst von Gauß gelegt, und zwar im Zusammenhang mit seinen Arbeiten über das biquadratische Reziprozitätsgesetzes. Zu dessen Formulierung hat es sich nämlich als notwendig herausgestellt, den Bereich der ganzen Zahlen erheblich zu erweitern und in dem Ring $\mathbb{Z}[i]=\{a+bi : a,b\in\mathbb{Z}\}$ zu arbeiten. Die eindeutige Zerlegung in Primelemente hat Gauß dabei nicht wie wir mit Hilfe des euklidischen Algorithmus bewiesen (die Einsicht, dass alle euklidischen Ringe ZPE-Ringe sind, hat erst Dirichlet explizit hingeschrieben), sondern mit Hilfe der Theorie der binären quadratischen Formen der Diskriminante -4.

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

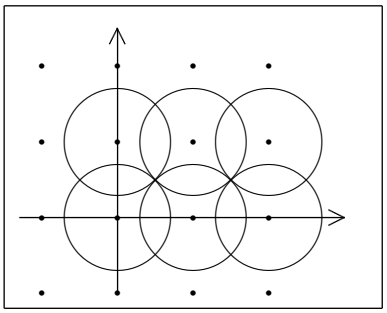
$$N(\xi-\gamma)<1. \tag{3.2}$$

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 $|x|,|y|\le\frac{1}{2}$ haben. Wir behaupten, dass für alle solchen ξ ein einziger Wert von γ

[1] Beim Versuch ist es geblieben, weil Euler die Arithmetik quadratischer Zahlringe nicht wirklich verstanden hat. Insbesondere meinte er, zwei Zahlen $x+y\sqrt{m}$ und $x-y\sqrt{m}$ seien teilerfremd, wenn die ganzen rationalen Zahlen x und y teilerfremd sind. Als Übung überlege man sich, dass das nicht notwendig der Fall ist.

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.



Die Menge aller $\xi \in \mathbb{Q}(i)$ mit $N(\xi) \leq \frac{1}{2}$ liegen in einem Kreis mit Radius $\frac{1}{\sqrt{2}}$ um den Ursprung. Legt man um jeden Gitterpunkt, also jeden Punkt $a+bi$ mit $a, b \in \mathbb{Z}$, einen solchen Kreis, so wird ganz $\mathbb{Q}(i)$ dadurch überdeckt. Dies bedeutet, dass zu jedem $\xi \in \mathbb{Q}(i)$ ein $\gamma \in \mathbb{Z}[i]$ mit (3.2) und sogar stärker mit $N(\xi - \gamma) \leq \frac{1}{2}$ gibt!

Um beispielsweise denn ggT von $1+12i$ und $7+4i$ zu berechnen, bestimmt man die nächste ganze Zahl an

$$\frac{1+12i}{7+4i} = \frac{(1+12i)(7-4i)}{(7+4i)(7-4i)} = \frac{55+80i}{65},$$

nämlich $1+i$, und hat als ersten Schritt im euklidischen Algorithmus die Gleichung

$$1 + 12i = (1+i)(7+4i) + (-2+i).$$

Im nächsten Schritt stellt man fest, dass $-2+i \sim 1+2i$ ein größter gemeinsamer Teiler von $1+12i$ und $7+4i$ ist.

Übung. Bestimme ggT $(26 - 29i, 13 + 4i)$ mit dem euklidischen Algorithmus in $\mathbb{Z}[i]$. Kontrolliere das Ergebnis durch Primfaktorzerlegung. 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[2] 1828 in seiner zweiten Abhandlung über biquadratische Reste getan.[3]

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

[2] 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.

[3] 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.

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 $\operatorname{ggT}(p, q) = 1$ teilen und wäre 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 Fall 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. Sei $p = a^2 + b^2$ eine ungerade Primzahl. Zeige, dass sich a und b aus einer Lösung der Kongruenz $x^2 \equiv -1 \bmod p$ mit Hilfe des euklidischen Algorithmus berechnen lassen, indem man den größten gemeinsamen Teiler von p und $x + i$ in $\mathbb{Z}[i]$ berechnet.

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. Löse die Pythagoreische Gleichung $x^2 + y^2 = z^2$ durch Zerlegen der linken Seite und Ausnutzen der Arithmetik in $\mathbb{Z}[i]$.

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

Wer mag, kann sich nun an der Gleichung $y^2 = x^3 - 4$ (Fermat) versuchen, oder gleich an der allgemeineren Gleichung $y^2 = x^3 - k^2$. Diese "Bachet-Mordell"-Gleichungen wurden ausführlichst untersucht, und es ist wenig wahrscheinlich, dass man mit den hier bereitgestellten Mitteln noch etwas Überraschendes findet – ausgeschlossen ist es aber auch nicht.

Quadratische Reste

Wir geben noch, ohne den einfachen Beweis, den kleinen Fermatschen Satz in $\mathbb{Z}[i]$ an: zuerst rechnet man nach, dass für ungerade Primzahlen p

$$(a+bi)^p \equiv \begin{cases} a+bi \bmod p, & \text{falls } p \equiv 1 \bmod 4, \\ a-bi \bmod p, & \text{falls } p \equiv 3 \bmod 4 \end{cases}$$

gilt. Daraus folgt dann sofort

Satz 3.4 (Kleiner Fermatscher Satz)**.** *Sei $\pi \in \mathbb{Z}[i]$ prim. Dann gilt für alle nicht durch π teilbaren $\alpha \in \mathbb{Z}[i]$ die Kongruenz*

$$\alpha^{N\pi-1} \equiv 1 \bmod \pi.$$

In Analogie zum Fall der gewöhnlichen ganzen Zahlen gilt auch hier

Proposition 3.5 (Eulersches Kriterium)**.** *Ist $\pi \in \mathbb{Z}[i]$ prim mit ungerader Norm und $\alpha \in \mathbb{Z}[i]$ nicht durch π teilbar, dann ist genau dann α quadratischer Rest modulo π, also die Kongruenz $\alpha \equiv \xi^2 \bmod \pi$ lösbar mit $\xi \in \mathbb{Z}[i]$, wenn*

$$\alpha^{(N\pi-1)/2} \equiv 1 \bmod \pi$$

gilt.

Dies erlaubt dann die Einführung des quadratischen Restsymbols $[\frac{\alpha}{\pi}]$ mit Werten aus $\{\pm 1\}$, das durch die Kongruenz

$$\alpha^{(N\pi-1)/2} \equiv \left[\frac{\alpha}{\pi}\right] \bmod \pi$$

festgelegt wird. Dirichlet hat gezeigt, wie man das quadratische Reziprozitätsgesetz in $\mathbb{Z}[i]$, das Gauß zuerst ausgesprochen hat, ganz einfach[4] aus demjenigen für $\mathbb{Z}$ herleiten kann:

Satz 3.6 (Quadratisches Reziprozitätsgesetz)**.** *Sind π und λ nicht assoziierte Primzahlen mit ungerader Norm aus $\mathbb{Z}[i]$, und ist $\pi \equiv \lambda \equiv 1 \bmod 2$, dann gilt*

$$\left[\frac{\lambda}{\pi}\right] = \left[\frac{\pi}{\lambda}\right],$$

Übung. Berechne $[\frac{1+2i}{3+2i}]$.

Übung. 1. Zeige durch Vergleich der Definitionen der quadratischen Restsymbole, dass für prime $\pi \in \mathbb{Z}[i]$ mit ungerader primer Norm p und $a \in \mathbb{Z}$ immer $[\frac{a}{\pi}] = (\frac{a}{p})$ gilt.

Zeige weiter, dass $[\frac{a}{q}] = 1$ ist für alle $a \in \mathbb{Z}$, die nicht durch $q \equiv 3 \bmod 4$ teilbar sind.

2. Ist $\pi = a + bi$ prim mit a ungerade und b gerade, dann gilt $[\frac{a}{a+bi}] = 1$.

[4] Sh. Lemmermeyer, *Reciprocity Laws*, Springer-Verlag 2000

3. Seien $\pi = a + bi$ und $\lambda = c + di$ prim mit ungeraden Normen $N\pi = p$ und $\lambda = q$. Benutze die Kongruenz $ci \equiv d \bmod (c+di)$ und $(\frac{c}{q}) = 1$, um $[\frac{a+bi}{c+di}] = (\frac{ac+bd}{q})$ zu beweisen.

4. Benutze das quadratische Reziprozitätsgesetz in $\mathbb{Z}$ und eine Variation von (1.1), um $(\frac{ac+bd}{pq}) = 1$ nachzurechnen.

5. Beweise das quadratische Reziprozitätsgesetz in $\mathbb{Z}[i]$.

Die Verallgemeinerung des quadratischen Reziprozitätsgesetzes auf beliebige quadratische Zahlkörper ist technisch um Einiges aufwendiger, verläuft aber im wesentlichen analog. Dagegen erfordert der Beweis des quadratischen Reziprozitätsgesetzes in beliebigen Zahlkörpern, wie Hilbert gezeigt hat, viel tiefere Hilfsmittel und führt direkt in die Klassenkörpertheorie. Ein Beweis dieses Satzes findet man in Heckes Lehrbuch [He].

3.2 Die Eisensteinschen Zahlen

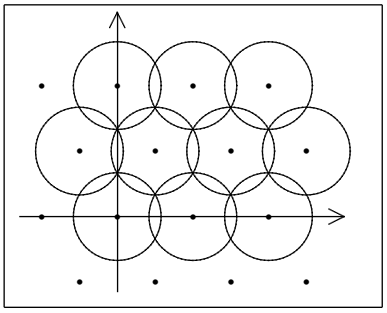
Den Ring $\mathbb{Z}[\rho]$, wo $\rho = \frac{-1+\sqrt{-3}}{2}$ eine primitive dritte Einheitswurzel ist, nennt man auch den Ring der Eisensteinschen Zahlen; Eisenstein[5] hat diesen Ring bei seinem Beweis des kubischen Reziprozitätsgesetzes benutzt.

$\mathbb{Z}[\rho]$ 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 $|2y - b| \leq \frac{1}{2}$ 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 $|2x-a| \leq 1$ erreichen (die nächste ganze Zahl mit vorgegebener Parität hat höchstens Abstand 1 von $2x$). Damit ist dann $N(\xi - \gamma) \leq \frac{1}{4}(1 + \frac{3}{4}) = \frac{7}{16} < 1$.

Im folgenden Diagramm wurde jeder Zahl $x + y\sqrt{-3}$ der Punkt $(x, y\sqrt{3})$ im $\mathbb{R}^2$ zugeordnet; der Ring $\mathbb{Z}[\rho]$ ist dann ein zweidimensionales Gitter.

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.



Im Diagramm nebenan ist um jeden Gitterpunkt ein Kreis mit Radius $1/\sqrt{3}$ gezeichnet. Diese überdecken die Ebene, folglich können wir wirklich immer $N(\xi - \gamma) \leq \frac{1}{3}$ erreichen. Die Skizze zeigt ebenfalls, dass dies bestmöglich ist: für kleinere Radien verliert man z.B. den Punkt, der der Zahl $\xi = \frac{1}{3}\sqrt{-3}$ entspricht.

[5] 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 Modulformen.

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

Proposition 3.7. *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 3.8. *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 Lesern 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 3.9. *Der Ring $\mathbb{Z}[\rho]$ ist euklidisch und damit ZPE-Ring. Die Primelemente sind 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 Folgerung hieraus notieren wir den kleinen Fermatschen Satz

$$\alpha^{N\pi-1} \equiv 1 \bmod \pi$$

für alle $\alpha \in \mathbb{Z}[\rho]$, die nicht durch das Primelement π teilbar sind. Insbesondere gilt im Falle $\pi = 2$ die wichtige Beobachtung

$$\alpha^3 \equiv 1 \bmod 2$$

für alle nicht durch 2 teilbaren $\alpha \in \mathbb{Z}[\rho]$.

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

3.3 * 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[6]. 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 $(x, y, z, \ldots)$ in ganzen Zahlen und zeigt dann, dass es zu jeder Lösung eine 'kleinere' Lösung $(u, v, w, \ldots)$ 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 3.10. *Die diophantische Gleichung $x^3 + y^3 + z^3 = 0$ besitzt in $\mathbb{Z}$ nur triviale Lösungen, also solche mit $xyz = 0$.*

Anstatt diesen Satz nur für Zahlen $x, y, z \in \mathbb{Z}$ zu beweisen, zeigen wir (wie Gauß) stärker, dass die kubische Fermatgleichung nicht einmal im Ring $\mathbb{Z}[\rho]$ eine nichttriviale Lösung besitzt. Dies folgt sofort, wenn man in folgendem Satz $\alpha = x^3$, $\beta = y^3$ und $\gamma = z^3$ setzt:

Satz 3.11. *Seien $\alpha, \beta, \gamma \in \mathbb{Z}[\rho] \setminus \{0\}$. Ist dann $\alpha + \beta + \gamma = 0$ und $\alpha\beta\gamma = \mu^3$, dann ist $\alpha\beta\gamma = 0$.*

Beweis. Wir dürfen annehmen, dass α, β und γ paarweise teilerfremd sind. Unter allen Gegenbeispielen nehmen wir uns jetzt eines her, in dem $N(\alpha\beta\gamma)$ minimal ist. Dann ist

[6] Eulers Beweis enthielt eine Lücke, da er den folgenden Hilfssatz nur unzureichend begründete: ist $c^2 + 3d^2 = r^3$, dann gibt es Zahlen p und q mit $c = p(p^2 - 9q^2)$ und $d = 3q(p^2 - q^2)$. Sh. auch C. Bergmann, *Über Eulers Beweis des großen Fermatschen Satzes für den Exponenten* 3, Math. Ann. **164** (1966), 159–175.

$$\alpha = \rho^a A_1^3, \quad \beta = \rho^b B_1^3, \quad \gamma = \rho^c C_1^3$$

für Elemente $A_1, B_1, C_1 \in \mathbb{Z}[\rho]$. Mit (α, β, γ) ist auch $(\alpha/\rho^a, \beta/\rho^a, \gamma/\rho^a)$ ein Lösungstripel; folglich dürfen wir $a = 0$ annehmen.

Da $\alpha\beta\gamma = \mu^3$ ist, muss $b + c \equiv 0 \bmod 3$ sein, und es bleiben die Möglichkeiten $(b, c) = (0, 0), (1, 2), (2, 1)$. In den beiden letzten Fällen ergibt sich aber ein Widerspruch, wenn man die Gleichung $\alpha + \beta + \gamma = 0$ modulo 2 betrachtet.

Daher ist $a = b = c = 0$, also

$$\alpha = A_1^3, \quad \beta = B_1^3, \quad \gamma = C_1^3.$$

Wir setzen $\alpha_1 = B_1 + C_1$, $\beta_1 = \rho B_1 + \rho^2 C_1$ und $\gamma_1 = \rho^2 B_1 + \rho C_1$. Dann ist

- $\alpha_1 + \beta_1 + \gamma_1 = B_1(1 + \rho + \rho^2) + C_1(1 + \rho + \rho^2) = 0$;
- $\alpha_1\beta_1\gamma_1 = B_1^3 + C_1^3 = \beta + \gamma = -\alpha = (-A_1)^3$;
- $\beta_1 + \gamma_1 = (B_1 + C_1)(\rho + \rho^2) = -(B_1 + C_1) \neq 0$ wegen $\beta + \gamma = -\alpha \neq 0$.
- $N(\alpha_1\beta_1\gamma_1) = N(\alpha) \mid N(\alpha\beta\gamma)$; hätten wir Gleichheit, müsste $N(\beta) = N(\gamma) = 1$ sein. Also sind B_1 und C_1 Einheiten, folglich $\beta, \gamma = \pm 1$. Dies geht nur, wenn (α, β, γ) bis auf eine Permutation gleich $(0, 1, -1)$ ist, was aber unserer Annahme widerspricht.

Also ist $(\alpha_1, \beta_1, \gamma_1)$ ein Lösungstripel mit $N(\alpha_1) < N(\alpha)$ entgegen unserer Annahme über die Minimalität von $N\alpha$. Dieser Widerspruch beendet den Beweis. □

Diese glatte Formulierung des Beweises habe ich von Paul Monsky[7] gelernt.

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[8], 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 nahe, 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 $2 + 6(v/u)^2 = 1/u^3$. Multipliziert man dies mit 6^3 und setzt $Y = 36v/u$, $X = 6/u$, so ergibt sich die elliptische Kurve $Y^2 = X^3 - 432$.

[7] Vgl. `math overflow` Frage # 39561.

[8] 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.

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

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

Betrachten wir noch einmal die ganzzahligen Lösungen der Gleichung $y^2 = x^3 + 1$, die wir im Licht der bisher erlangten Kenntnisse mutig in der Form

$$y^2 = (x+1)(x+\rho)(x+\rho^2)$$

schreiben. Die drei Faktoren auf der rechten Seite sind etweder teilerfremd oder haben einen gemeinsamen Faktor $1-\rho$, da jeder gemeinsame Teiler zweier Faktoren deren Differenz teilt, die bis auf eine Potenz von ρ gleich $1-\rho$ ist.

Im ersten Fall ist $x+1 = \pm a^2$ und $x+\rho = (-\rho)^e(a+b\rho)^2$, woraus durch Konjugation die dritte Gleichung $x+\rho^2 = (-\rho^2)^e(a+b\rho^2)^2$ folgt. Da $\rho = (1+\rho)^2$ ein Quadrat ist, können wir die Potenzen von ρ in das Quadrat ziehen und erhalten $x+\rho = \pm(a+b\rho)^2$ und $x+\rho^2 = \pm(a+b\rho^2)^2$. Subtraktion beider Gleichungen und Division durch $\rho-\rho^2$ ergibt $1 = \pm b(2a-b)$, was auf $b = \pm 1$ und damit letztlich auf die Lösungen $(a,b) = (0,\pm 1)$, $(\pm 1, \pm 1)$ führt. Dies liefert dann $(x,y) = (0,\pm 1)$ und $(-1,0)$.

Im zweiten Fall dagegen ist, wenn wir die Potenzen von ρ wieder in die Quadrate ziehen,

$$\begin{cases} x+1 &= \pm 3a^2, \\ x+\rho &= \pm(1-\rho)(a+b\rho)^2, \\ x+\rho^2 &= \pm(1-\rho^2)(a+b\rho^2)^2 \end{cases} \tag{3.4}$$

Subtraktion der beiden letzten Gleichungen und Division durch $\rho-\rho^2$ liefert[9] diesmal $\pm 1 = a^2 - 4ab + b^2 = \pm(a-2b)^2 - 3b^2$. Die Gleichung $t^2 - 3u^2 = 1$ hat, wie wir weiter unten sehen werden, unendlich viele Lösungen; sehr wenige davon sind aber mit der ersten Gleichung $x+1 = \pm 3a^2$ kompatibel.

Wenn wir die beiden letzten Gleichungen in (3.4) addieren anstatt sie wie eben zu subtrahieren, erhalten wir $2x - 1 = \pm 3(a^2 - b^2)$. Eliminieren wir x aus dieser und der ersten Gleichung, ergeben sich folgende Möglichkeiten:

- $a^2 + b^2 = 1$, also $(a,b) = (\pm 1, 0)$ und $(0, \pm 1)$, was auf $x = 0$ und $x = 2$, also auf die Lösungen $(x,y) = (0,\pm 1)$ und $(x,y) = (2,\pm 3)$ führt.
- Die Vorzeichenwahl $2x-1 = 3a^2-3b^2$ und $x+1 = -3a^2$ liefert die Gleichung $1 = b^2 - 3a^2$. Damit sind wir wieder in die Pellsche Gleichung $1 = b^2 - 3a^2$ gelaufen, an der kein Weg vorbei zu führen scheint. Allerdings hat man manchmal das Glück, das Problem gelöst zu haben, ohne dass man es bemerkt hat. Aus $x+1 = -3a^2$ und $a \neq 0$ folgt $x \leq -4$, was wegen $y^2 = x^3 + 1 > 0$ aber nicht sein kann.

Alles in allem haben wir damit gezeigt:

Satz 3.12. *Die ganzzahligen Lösungen der diophantischen Gleichung* $y^2 = x^3 + 1$ *sind* $(x,y) = (-1,0), (0,\pm 1), (2,\pm 3)$.

[9] Um ehrlich zu sein, mache ich solche Rechnungen lieber in `pari` als von Hand: mit $w = -$`quadgen`(-3) definiert man eine primitive dritte Einheitswurzel, und dann muss man nur noch $(a+b*w)^3 - (a-b*w)^3$ eintippen und das Ergebnis durch $w - w^2$ teilen.

Wie wir gesehen haben, ist der Versuch, Rechnungen in Zahlkörpern $\neq \mathbb{Q}$ zu vermeiden, nicht immer von Erfolg gekrönt: zerlegt man $y^2 - 1 = x^3$ in $\mathbb{Z}$, kommt man vom Regen (dem Rechnen in $\mathbb{Z}[\rho]$, das man so zu vermeiden sucht) in die Traufe, nämlich in den kubischen Zahlkörper $\mathbb{Q}(\sqrt[3]{2}\,)$.

Einen schönen Beweis[10] des obigen Satzes von Paul Monsky möchten wir den Lesern nicht vorenthalten.

Satz 3.13. *Seien $\alpha, \beta, \gamma \in \mathbb{Z}[\rho] \setminus \{0\}$. Ist dann $\alpha + \beta + \gamma = 0$ und $\alpha\beta\gamma = 2\mu^3$, dann ist nach einer geeigneten Permutation der drei Zahlen $\alpha = 0$ oder $\beta = \gamma$.*

Wenn wir in diesem Satz $\alpha = 1 - y$, $\beta = 1 + y$ und $\gamma = -2$ setzen, erhalten wir Satz 3.12 zurück.

Beweis. Sei (α, β, γ) ein Gegenbeispiel. Dann sind α, β und γ paarweise teilerfremd in $\mathbb{Z}[\rho]$, und wir können, notfalls durch eine Permutation, sicherstellen, dass

$$\alpha = 2\rho^a A_1^3, \quad \beta = \rho^b B_1^3, \quad \gamma = \rho^c C_1^3$$

gilt. Unter allen solchen Gegenbeispielen nehmen wir uns jetzt eines her, in dem $N\alpha$ minimal ist. Dividieren wir alle drei Elemente durch ρ^a, folgt $a = 0$.

Jetzt bemerken wir, dass alle Kuben in $\mathbb{Z}[\rho]$ entweder $\equiv 0 \bmod 2$ oder $\equiv 1 \bmod 2$ sind. Dies impliziert, dass $0 \equiv \alpha \equiv \beta + \gamma \equiv \rho^b + \rho^c \bmod 2$ ist, was nur geht, wenn $b = c$ ist. Da $\alpha\beta\gamma$ eine dritte Potenz ist, muss sogar $a = b = c$ und damit $a = b = c = 0$ sein.

Wir haben daher

$$\alpha = 2A_1^3, \quad \beta = B_1^3, \quad \gamma = C_1^3.$$

Da $B_1^3 \equiv C_1^3 \equiv 1 \bmod 2$ ist, dürfen wir nach Prop. 3.8 annehmen, dass $B_1 \equiv C_1 \equiv 1 \bmod 2$ gilt.

Jetzt setzen wir $\alpha_1 = B_1 + C_1$, $\beta_1 = \rho B_1 + \rho^2 C_1$ und $\gamma_1 = \rho^2 B_1 + \rho C_1$. Dann ist

- $\alpha_1 + \beta_1 + \gamma_1 = B_1(1 + \rho + \rho^2) + C_1(1 + \rho + \rho^2) = 0.$
- $\alpha_1\beta_1\gamma_1 = B_1^3 + C_1^3 = \beta + \gamma = -\alpha = 2(-A_1)^3.$
- $\beta_1 + \gamma_1 = (B_1 + C_1)(\rho + \rho^2) = -(B_1 + C_1) \neq 0$ wegen $\beta + \gamma = -\alpha \neq 0$.

[10] Dass es im Falle $y^2 = x^3 + 1$ zwei derart verschiedene Beweise gibt hat seinen tieferen Grund in der Arithmetik elliptischer Kurven. Besitzt die Gruppe der rationalen Punkte einer elliptischen Kurve eine Untergruppe der Ordnung n, so kann man diese Gruppe mit Hilfe einer sogenannten n-Isogenie zu bestimmen versuchen. In unserem Falle bilden die fünf rationalen Punkte aus Satz 3.12 zusammen mit dem ominösen unendlich fernen Punkt eine zyklische Gruppe der Ordnung 6: also hat man die Wahl zwischen einem 2-Abstieg und einem 3-Abstieg. Der 2-Abstieg benutzt Quadrate wie in (3.4), der 3-Abstieg dagegen dritte Potenzen. Hat eine elliptische Kurve gar keine rationalen Punkte außer dem unendlich fernen Punkt, kann man einen 2- oder 3-Abstieg erzwingen, indem man in einen geeigneten Zahlkörper höheren Grades geht. Beispielsweise hat die kubische Fermatgleichung $x^3 + y^3 + z^3 = 0$ eine Lösung $(1, 1, -\sqrt[3]{2}\,)$ im kubischen Zahlkörper $\mathbb{Q}(\sqrt[3]{2}\,)$, und diese Tatsache ermöglicht einen Beweis der kubischen Fermatvermutung durch einen 2-Abstieg über diesem Zahlkörper. Diese Bemerkungen zeigen, dass die Arithmetik elliptischer Kurven unglaublich reichhaltig ist, selbst wenn man nur an diophantischen Aspekten interessiert ist.

- $N(\alpha_1\beta_1\gamma_1) = N\alpha \mid N(\alpha\beta\gamma)$; hätten wir Gleichheit, müsste $N(\beta) = N(\gamma) = 1$ und damit $\beta, \gamma = \pm 1$ sein. Dies liefert aber $\beta = 1$, $\gamma = -1$ und $\alpha = 0$ gegen unsere Annahme.

Also ist $(\alpha_1, \beta_1, \gamma_1)$ ein Lösungstripel mit $N(\alpha_1\beta_1\gamma_1) < N(\alpha\beta\gamma)$, was unserer Annahme über die Minimalität von $N\alpha$ widerspricht. Dieser Widerspruch beendet den Beweis. □

Dass bei der Lösung von $y^2 = x^3 + 1$ eine Variation der kubischen Fermatgleichung auftaucht hätte uns nicht überraschen sollen: bereits bei unserem ersten Lösungsversuch stolperten wir über die Gleichung $a^3 - 2b^3 = 1$. Schreibt man diese in der Form $a^3 + (-1)^3 = 2b^3$, so wird der Zusammenhang mit der Gleichung $x^3 + y^3 = 2z^3$ klar.

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 3.14. *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[11] 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

[11] Der folgende Beweis geht auf Lagrange zurück, der die notwendigen Hilfssätze konstruktiv aus der Theorie der Kettenbrüche entwickelte. Dirichlet hat diese durch einfache Anwendungen seines Schubfachprinzips ersetzt und den Beweis dadurch stark vereinfacht – auf Kosten der Konstruktivität.

Hilfssatz 3.15. *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:*

$$|A\xi_1 + B\xi_2| \leq \tfrac{1}{N}(|\xi_1| + |\xi_2|), \quad |A| \leq N,\ |B| \leq N. \tag{3.5}$$

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

$$f : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{R} : (a, b) \longmapsto a\xi_1 + b\xi_2 \tag{3.6}$$

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 3.16. *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

$$|A - B\sqrt{m}\,| \ \leq \tfrac{1}{N}(1 + \sqrt{m}\,),\ |A| \leq N,\ |B| \leq N \tag{3.7}$$

genügen. Die Dreiecksungleichung liefert

$$|A + B\sqrt{m}\,| \ \leq |A| + |B\sqrt{m}\,| \leq N(1 + \sqrt{m}\,), \tag{3.8}$$

und Multiplikation von (3.7) und (3.8) gibt

$$|A^2 - mB^2| \ \leq (1 + \sqrt{m}\,)^2. \tag{3.9}$$

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 (3.7) aber nicht sein kann.

Da aber $|A^2 - mB^2|$ durch (3.7) 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 3.14 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 Satz 3.14 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 3.17. *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 3.17 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 3.17 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 aber ein recht gutes Verfahren zur Berechnung von Fundamentaleinheiten quadratischer Körper mit bescheidener Diskriminante, das auf der Kettenbruchentwicklung von $\sqrt{m}$ beruht. Für Zahlkörper höheren Grades wird die Berechnung der Einheitengruppe mit wachsender Diskriminante sehr schnell zu einem Problem.

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 in der Regel 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 (mit dem Chinesischen Restsatz), 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:

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

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

$$\begin{aligned} |2a| &= |\beta + \beta'| \leq |\beta| + |\beta'| < |\varepsilon| + c, \\ |2b|\sqrt{m} &= |\beta - \beta'| \leq |\beta| + |\beta'| < |\varepsilon| + c. \end{aligned} \tag{3.10}$$

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 3.18. *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 $0 < (r-x)(r-y) = r^2 - r(x+y) + xy \le r^2 + s - r(x+y)$, 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[12]:

Satz 3.19. *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:*

$$\begin{aligned} |a| &\le \frac{1}{2}\sqrt{c}\big(\sqrt{|\varepsilon|} + \tfrac{1}{\sqrt{|\varepsilon|}}\big) \\ |b| &\le \frac{1}{2\sqrt{m}}\sqrt{c}\big(\sqrt{|\varepsilon|} + \tfrac{1}{\sqrt{|\varepsilon|}}\big) \end{aligned} \tag{3.11}$$

Wenn es beispielsweise ein $\alpha \in \mathbb{Z}[\sqrt{79}\,]$ mit Norm ± 3 gibt, dann gibt es (man setze $m = 79$, $\varepsilon = 80 + 9\sqrt{79}$ und $c = 3$) auch ein Element $a + b\sqrt{79}$ der Norm ± 3 mit $|b| \le 1.24....$ Also 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 Norm ± 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.[13]

[12] Der folgende Satz geht auf Chebyshev (Tschebischeff) zurück (*Sur les formes quadratiques*, J. Math. Pures Appl. **16** (1851), 257–282), der die ersten Schritte in Richtung Primzahlsatzgetan hat. Dieser behauptet, dass die Anzahl $\pi(x)$ aller Primzahlen $\le x$ ungefähr $\frac{x}{\log x}$ ist, wo $\log x$ den natürlichen Logarithmus bezeichnet. Chebyshev hat u.A. gezeigt, dass der Grenzwert $\frac{\pi(x)}{x/\log x}$ für $x \to \infty$, wenn er existiert, gleich 1 sein muss.

[13] Marin Mersenne (1588–1648) war Priester. Er stand mit vielen Mathematikern seiner Zeit 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 (dies sind übrigens lauter Zahlen, die sich um höchstens 3 von einer Zweierpotenz unterscheiden) die einzigen Primzahlen ≤ 257 sind, für die $2^p - 1$ prim ist. Tatsächlich führen aber $p = 67$ 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 (zumindest hat dies E.T. Bell behauptet, der in seinen Büchern einige Anekdoten ausgeschmückt, um nicht zu sagen erfunden hat). Heute liefert ein gutes Faktorisierungsprogramm das Ergebnis $2^{67} - 1 = 193707721 \cdot 761838257287$ in Sekundenschnelle. Sogar die Faktorisierung von $2^{257} - 1 = 535006138814359 \cdot 1155685395246619182673033 \cdot$

Es ist leicht zu zeigen, dass $2^p - 1$ nur dann prim sein kann, wenn p selbst prim ist: dies folgt leicht aus der 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[14] und Lehmer[15]), 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 3.20. *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[16]; dieser wollen wir uns jetzt näher widmen.

37455059850181093658177663009631318139 3 kann man mit pari heute in weniger als einer Minute erledigen. Eine Tabelle mit allen bekannten Faktoren von Mersenne-Zahlen $2^n - 1$ findet man durch googeln nach GIMPS. Das kleinste n, für das $2^n - 1$ im Jahre 1999 nicht vollständig faktorisiert war, ist $n = 571$; nach Abdivision der beiden Faktoren 5711 und 27409 blieb eine zusammengesetzte Zahl mit 164 Dezimalstellen.

Der technische Fortschritt hat auch vor M_{571} nicht haltgemacht: inzwischen wurde diese Zahl in ihre Primfaktoren zerlegt. Die 164-stellige Zahl ist das Produkt von

$$6969336604531667168509871230100794095801832527002849548226132675916172927$$

und einer Primzahl mit 91 Dezimalstellen. Die kleinste nicht ganz faktorisierte Mersenne-Zahl ist heute M_{929}.

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

[15] D. Lehmer, amerikanischer Mathematiker.

[16] Der Kern der Angelegenheit ist die Gruppenstruktur der Einheitengruppe; diese bekommt eine geometrische Interpretation, wenn man die Gleichung $x^2 - 3y^2 = 1$ als Kegelschnitt auffasst. Diese Interpretation hat den Vorteil, dass analoge Tests, die mit der Gruppenstruktur von $(\mathbb{Z}/p\mathbb{Z})^\times$ oder derjenigen der Punkte auf einer elliptischen Kurve arbeiten, sich ganz analog darstellen lassen.

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.

Die geometrische Interpretation ist hier nicht mehr ganz so übersichtlich, da das Bild aller $\xi = x + y\sqrt{3}$ mit $N\xi < 1$ unter der Abbildung $\xi \to (x, y\sqrt{3}\,)$ hier kein Kreis, sondern eine Hyperbel $x^2 - 3y^2 < 1$ ist. Die Überdeckung der Ebene durch solche nichtkompakten Teilmengen ist deutlich schwieriger, aber eben auch reizvoller als im imaginärquadratischen Fall.

Proposition 3.21. *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 3.22. *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 3.9, 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 3.23. *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 3.24. *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.*

Auch in $\mathbb{Z}[\sqrt{3}\,]$ gilt der kleine Fermatsche Satz; wie in andern quadratischen Zahlringen auch ist er eine Folgerung der folgenden allgemeinen und elementaren Beobachtung:

Proposition 3.25. *Sei* $p \nmid 4m$ *prim und* $k = \mathbb{Q}(\sqrt{m})$*; dann gilt für alle* $\alpha \in \mathcal{O}_k$

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

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 $2^p \equiv 2 \bmod p$. $\square$

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 $q \ge 5$ 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 3.22 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 3.25, 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[17] 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 3.26. *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.

[17] Dieses Ergebnis geht auf T. Motzkin [*The Euclidean algorithm*, Bull. Am. Math. Soc. **55** (1949), 1142–1146] zurück. Es ist sehr leicht zu beweisen und hat in der Folge eine große Rolle gespielt. Vgl. auch Lemmermeyer [*The Euclidean Algorithm in Algebraic Number Fields*, Expositiones Math. **13** (1995), 385–416].

Der einzige, der in obiger Liste nicht auftaucht und für den man dies wirklich zeigen kann[18], ist[19] $\mathbb{Q}(\sqrt{69})$.

Dass die in Satz 3.26 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[20].

Ein direkter Nachweis der ZPE-Eigenschaft quadratischer Zahlringe wird durch ein auf Dedekind[21] und Hasse[22] zurückgehendes Kriterium[23] ermöglicht:

Satz 3.27. *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:

Satz 3.28. *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.

Übung. Zeige, dass der Ring $R = \mathbb{Z}[\sqrt{-5}, \frac{1}{2}] = \{2^{-n}(a + b\sqrt{-5}) : a, b, n \in \mathbb{Z}\}$ euklidisch bezüglich derjenigen Norm N_u ist, die man erhält, wenn man von der

[18] Inzwischen ist man weiter. Vgl. insbesondere M. Harper [*A proof that $\mathbb{Z}[\sqrt{14}]$ is Euclidean*, Ph.D. thesis, McGill University, 2000] und [$\mathbb{Z}[\sqrt{14}]$ *is Euclidean*, Can. J. Math. **56** (2004), 55–70].

[19] Vgl. die Diplomarbeit *Quadratic Number Fields that are Euclidean but not Norm-Euclidean* von B. Lutzmann; Univ. Wien 2009.

[20] Dreh- und Angelpunkt ist eine Arbeit von Davenport, die die Sprache der binären quadratischen Formen benutzt und ziemlich verwickelt ist. Für eine deutsche Version sh. *Euklidische Zahlkörper*, Diplomarbeit von K. Halupczok, Univ. Konstanz 1997.

[21] Richard Dedekind (1831–1916) war der erste Algebraiker; Begriffe wie Ring, Körper und insbesondere Ideal gehen auf ihn zurück. Die Invasion der Algebra durch diese originär zahlentheoretischen Begriffe setzten in den 1920er Jahren unter dem maßgeblichen Einfluss von Emmy Noether ein.

[22] 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.

[23] Das Kriterium von Dedekind-Hasse wurde von H. Hasse [*Über eindeutige Zerlegung in Primelemente oder in Primhauptideale in Integritätsbereichen*, J. Reine Angew. Math. **159** (1928), 3–12] veröffentlicht. Emmy Noether hat das Kriterium später bei der Herausgabe von Dedekinds Werken in dessen Nachlass gefunden und hat es in dessen Werke (II, Nr. 38) aufgenommen. Vgl. auch [*Helmut Hasse und Emmy Noether – Die Korrespondenz 1925 – 1935*], (F. Lemmermeyer, P. Roquette (Hrsgb.)), Univ.-Verlag Göttingen, Anmerkung 1 auf S. 60].

gewöhnlichen Norm $N(x + y\sqrt{-5}\,) = x^2 + 5y^2$ nur den ungeraden Faktor nimmt; beispielsweise ist $N_u(1 + \sqrt{-5}\,) = 3$.

Zeige auch, dass die Einheitengruppe von R gleich $R^\times = \langle -1, 2\rangle$ und damit isomorph zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ ist.

Die Ringe aus der vorhergehenden Übung nennt man Ringe S-ganzer Zahlen (im Beispiel war $S = \{2\}$). Sie werden bisweilen herangezogen, wenn man gerne Sätze über Hauptidealringe benutzen möchte. Der Preis dafür ist allerdings eine größere Einheitengruppe, die bei fast allen arithmetischen Problemen den Vorteil der ZPE-Ringe wieder zunichte macht.

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.

4. Idealarithmetik in quadratischen Zahlkörpern

In diesem Kapitel wollen wir zeigen, wie man mit Idealen rechnet, und wie man sie zur Lösung von Problemen in der elementaren Zahlentheorie einsetzt.

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: aus $(2, 1+\sqrt{-5}\,) = (\alpha)$, folgte nämlich $\alpha \sim \mathrm{ggT}\,(2, 1+\sqrt{-5}\,)$:

Übung. Sei R Hauptidealring und $(d) = (a, b)$ für $a, b, d \in R$. Dann ist d ein größter gemeinsamer Teiler von a und b, d.h.:

- d ist gemeinsamer Teiler: $d \mid a$, $d \mid b$.
- jeder gemeinsame Teiler teilt d: aus $e \mid a$ und $e \mid b$ folgt $e \mid d$.

Nun ist aber R kein Hauptidealring, und $(2, 1+\sqrt{-5}\,)$ ist kein Hauptideal. Dedekinds Idee[1] 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 deren Produkt $AB = \{\alpha_1\beta_1 + \ldots + \alpha_m\beta_m : \alpha_j \in A, \beta_j \in B\}$, 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 $AR = A(1) = A$.*

[1] Kummer hatte in Kreisteilungskörpern ideale Zahlen eingeführt; in unserem Fall entsprechen diese surjektiven Homomorphismen $\phi : \mathcal{O}_K \longrightarrow \mathbb{F}_q$ auf endliche Körper. Dedekind hat diese Epimorphismen durch ihre Kerne ersetzt; vgl. F. Lemmermeyer, *Jacobi and Kummer's ideal numbers*, Abh. Math. Sem. Hamburg **79** (2009), 165–187.

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 $(\mathfrak{a}\mathfrak{b})^\sigma = \mathfrak{a}^\sigma\mathfrak{b}^\sigma$ 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 $\mathfrak{c} = \mathfrak{b}^\sigma = (3, 1-\sqrt{-5}\,)$. 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

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

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 $\mathfrak{a}\mathfrak{b} = (1+\sqrt{-5}\,)$, $\mathfrak{a}\mathfrak{c} = (1-\sqrt{-5}\,)$, und $\mathfrak{c}^2 = (2-\sqrt{-5}\,)$.

Übung. Sei $m = a^2 + b^2$ Summe zweier Quadrate und a ungerade. Zeige, dass $(a, b+\sqrt{m}\,)^2 = (b+\sqrt{m}\,)$ gilt.

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 $(3) = \mathfrak{b}\mathfrak{c}$ ein, so folgt die Idealgleichung $(6) = \mathfrak{a}^2\mathfrak{b}\mathfrak{c}$; gruppiert man die Faktoren in der Form $\mathfrak{a}^2\cdot(\mathfrak{b}\mathfrak{c})$, so erhält man die Zerlegung $(6) = (2)(3)$ in zwei Hauptideale; dagegen liefert $(\mathfrak{a}\mathfrak{b})(\mathfrak{a}\mathfrak{c}) = (1+\sqrt{-5}\,)(1-\sqrt{-5}\,)$ 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?

Übung. Zeige, dass es in $R = \mathbb{Z}[\sqrt{-5}]$ Homomorphismen $\phi_2 : R \longrightarrow \mathbb{F}_2$, $\phi_3 : R \longrightarrow \mathbb{F}_3$ und $\phi_3' : R \longrightarrow \mathbb{F}_3$ gibt, deren Kerne genau die oben betrachteten Primideale $\mathfrak{a}$, $\mathfrak{b}$ und $\mathfrak{c}$ sind.

4.2 Eindeutige Primidealzerlegung

Die Idealnorm

Wir beginnen mit der Beobachtung, dass jedes Ideal in $\mathcal{O}_K$ von höchstens zwei Elementen[2] erzeugt wird:

Proposition 4.2. *Sei $\mathfrak{a} \subset \mathcal{O}_K$ ein $\mathbb{Z}$-Modul in $\mathcal{O}_K$, also eine und 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 "Enthalten bedeutet Teilen" und der Umkehrung "Teilen bedeutet Enthalten" – auf Englisch: "to contain is to divide", sowie "to divide is to contain" – 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 $a + my \in H$ 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. $\square$

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.

[2] In allgemeinen Ringen 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 4.3. *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[3] 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
  $$\begin{aligned}\mathfrak{a}\mathfrak{a}' &= (n^2, mn(b + \omega'), mn(b + \omega), m^2 N(b + \omega)) \\ &= (mn)\Big(\frac{n}{m}, b + \omega, b + \omega', \frac{1}{n} N(b + \omega)\Big).\end{aligned}$$
  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 $A \mid nm$.

[3] Dieser Hilfssatz ist verwandt mit dem "Prager Satz" von Dedekind; sh. Lemmermeyer, *Zur Zahlentheorie der Griechen. II: Gaußsche Lemmas und Rieszsche Ringe*, Math. Sem.ber. **56** (2009), 39–51. An dieser Stelle geht ganz wesentlich ein, dass der Ring $\mathcal{O}_k$ ganz abgeschlossen ist, also gleich der Maximalordnung ist.

Die Kürzungsregel

Jetzt wenden wir uns dem Satz von 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. Sei zuerst $\mathfrak{a} = (\alpha)$ ein Hauptideal; dann ist $\mathfrak{a}\mathfrak{b} = \alpha\mathfrak{b}$, also $\mathfrak{b} = \alpha^{-1}\mathfrak{a}\mathfrak{b}$ und $\mathfrak{c} = \alpha^{-1}\mathfrak{a}\mathfrak{c} = \alpha^{-1}\mathfrak{a}\mathfrak{b} = \mathfrak{b}$.

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. □

Übung. Zeige, dass im Ring $R = \mathbb{Z}[\sqrt{-3}\,]$ die Idealgleichung

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

gilt, aber wegen $(2, 1 + \sqrt{-3}\,) \neq (2)$ die Kürzungsregel falsch ist.

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 algebraischen 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 $\mathfrak{a} \neq (0), (1)$ 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 (mit der manchmal lästigen Ausnahme des Nullideals, das zwar prim, aber natürlich nicht maximal ist); irreduzible und maximale Ideale sind in unseren Ringen 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 $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ 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, $\mathfrak{a} \mid \mathfrak{b}\mathfrak{c}$ 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 $\beta\gamma \in \mathfrak{b}\mathfrak{c} \subseteq \mathfrak{a}$, 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 $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ 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 $\mathfrak{a} = \mathfrak{c}\mathfrak{d}$ und $\mathfrak{c} = \mathfrak{a}\mathfrak{e}$, also $\mathfrak{a} = \mathfrak{d}\mathfrak{e}\mathfrak{a}$. Hieraus kann man aber (ohne Kürzungsregel) nicht auf $\mathfrak{d}\mathfrak{e} = (1)$ 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 $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$; 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 $\mathfrak{a} = n\mathbb{Z} \oplus m(b+\omega)\mathbb{Z}$ wie in Prop. 4.2 und rechne nach, dass $\{r + s\omega : 0 \leq r < n, 0 \leq s < m\}$ 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 Zerlegung in Primideale gilt (solche Ringe heißen *Dedekind-Ringe*). Zeige: sind $\mathfrak{A}$ und $\mathfrak{B}$ teilerfremde Ideale mit $\mathfrak{A}\mathfrak{B} = \mathfrak{c}^n$, 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 $\mathfrak{a} \cap \mathfrak{b} \supseteq \mathfrak{a}\mathfrak{b}$, 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 $\mathfrak{p} \mid \mathfrak{p}\mathfrak{p}' = (N\mathfrak{p})$; 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 $m \equiv 1 \bmod 8$. Gerät man ins Stocken, orientiere man sich am Beweis des folgenden Satzes für ungerade p:

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[4] 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

Wir haben gesehen, dass die Menge der ganzen Ideale $\neq (0)$ in $\mathcal{O}_K$ eine Halbgruppe mit Kürzungsregel bildet. Solche Halbgruppen 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 gebrochenen[5] 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 setzt ganz allgemein $\frac{1}{\alpha}\mathfrak{c} := \{\frac{\gamma}{\alpha} : \gamma \in \mathfrak{c}\}$. Auf der Menge gebrochener Ideale $\neq 0$ definiert man 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: $\mathfrak{a} \sim \mathfrak{b}$),

[4] Das Legendre-Symbol $(\frac{a}{p})$ hat für ungerade Primzahlen p den Wert $+1$ oder -1, für den $a^{(p-1)/2} \equiv (\frac{a}{p}) \bmod p$ gilt.

[5] Ein Hauptideal der Form (α), wo $\alpha \in K^\times$ nicht notwendig ganz ist, heißt gebrochenes Hauptideal (fractional principal ideal im Englischen), und es ist $(\alpha) = \alpha\mathcal{O}_K$.

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 $\neq (0)$ 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[6] $\mathfrak{a} \sim \mathfrak{b}$: 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:

Proposition 4.9. *Ist das Ideal $\mathfrak{a}$ 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 $N\mathfrak{a} = n$. Insbesondere ist in diesem Fall $\mathfrak{a} \cap \mathbb{Z} = (N\mathfrak{a})$.*

Jetzt behaupten wir:

Satz 4.10. *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*

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

[6] Mit den Bezeichnungen aus dem Beispiel nach Prop. 4.1.

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 $\mu_K < 2$, 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 4.10 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 4.10 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 4.10 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 4.11. *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 4.10. Sei $c = [\mathfrak{a}]$ eine von einem Ideal $\mathfrak{a}$ erzeugte Idealklasse. Ohne Beschränkung 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. Zeige, dass die Klassenzahl von $\mathbb{Q}(\sqrt{-m})$ für jedes $m \equiv 1 \bmod 4$ mit $m > 1$ gerade ist. Dazu rechne man nach, dass $(2, 1 + \sqrt{-m})$ kein Hauptideal ist, $(2, 1 + \sqrt{-m})^2$ dagegen schon.

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[7] 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 (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 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).

Proposition 4.12. *Die quadratische Form $Q_0(x, y) = x^2 + 5y^2$ stellt alle Primzahlen p mit $(\frac{-1}{p}) = (\frac{-5}{p}) = +1$ dar, die Form $Q_1(x, y) = 2x^2 + 2xy + 3y^2$ alle mit $(\frac{-5}{p}) = +1$ und $(\frac{-1}{p}) = -1$.*

Diese hübsche Beobachtung ist ein Spezialfall der Theorie der Geschlechter, der wir uns im nächsten Kapitel widmen werden. In ihr spiegelt sich auch wieder, dass der Geschlechterklassenkörper von $k = \mathbb{Q}(\sqrt{-5})$ die biquadratische Erweiterung $\mathbb{Q}(\sqrt{-1}, \sqrt{5})$ ist; für mehr in diese Richtung schaue man in das schöne Buch von D. Cox, *Prime numbers of the form $x^2 + ny^2$*, John Wiley & Sons 1989.

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

Wir wollen sehen, was wir nun über die Lösungen der Gleichung $y^2 = x^3 - d$ für ganze $d > 0$ sagen können, wobei wir uns vorbehalten, an d im Laufe der Rechnungen diverse Bedingungen zu stellen.

[7] Dass dies alle sind, hat im wesentlichen bereits Gauß vermutet. Der Beweis gelang unabhängig voneinander Heegner, Stark und Baker; alle Beweise benutzen übrigens diophantische Gleichungen.

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 $\mathfrak{b}^h$ Hauptideal, damit auch $\mathfrak{b}^{3a+hb}$ für alle $a, b \in \mathbb{Z}$, 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 $1 = \frac{1}{8}(3r^2 s - ds^3)$, also $8 = 3r^2 s - ds^3 = s(3r^2 - ds^2)$. 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

$$y^2 + d = r^6 - 6r^4 + 12r^2 - 8 = (r^2 - 2)^3,$$

also $x = r^2 - 2$. Daher entspricht eine Darstellung $d = 3r^2 - 8$ dem Lösungspaar $(r^2 - 2, \pm(3 - r^2)r)$ 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[8]:

Satz 4.13. *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:*

d	(x, y)	d	(x, y)
$3t^2 - 1$	$(4t^2 - 1, \pm t(8t^2 - 3))$	$3t^2 - 8$	$(t^2 - 2, \pm t(3 - t^2))$
$3t^2 + 1$	$(4t^2 + 1, \pm t(8t^2 + 3))$	$3t^2 + 8$	$(t^2 + 2, \pm t(3 + t^2))$

3. *keine ganzzahligen Lösungen sonst.*

Man beachte, dass Satz 4.13 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.

Dieses Beispiel lässt sich leicht verallgemeinern:

Übung. Zeige, dass die Gleichung $y^2 = x^3 - d$ für alle $d = 3t^2 - 1$ mit $t = 3c^3$ eine ganzzahlige Lösung hat, die nicht in Satz 4.13 angegeben ist. Folgere daraus, dass die Klassenzahl von $\mathbb{Q}(\sqrt{d}\,)$ für alle $d = 27c^6 - 1$, für welche d eine quadratische Diskriminante ist (also z.B. quadratfrei), eine durch 3 teilbare Klassenzahl hat.

Wie oft ein Polynom wie $f(x) = 27x^6 - 1$ quadratfreie Werte annimmt, ist ein offenes Problem, sogar schon für Polynome vom Grad 4.

[8] Ganz ähnlich kann man zeigen, dass die Fermatgleichung $x^p + y^p = z^p$ für prime p nur triviale ganzzahlige Lösungen mit $xyz = 0$ besitzt, wenn p die Klassenzahl des Körpers $\mathbb{Q}(\zeta_p)$ der p-ten Einheitswurzeln nicht teilt – dies ist Kummers Zugang zum Fermatschen Problem.

Es stellt sich natürlich die Frage, ob die beiden für $d = 26$ gefundenen Lösungen die einzigen sind. Wir werden diese Frage hier nicht beantworten können, aber doch zeigen, wie man eine entsprechende Untersuchung beginnt.

Wie oben finden wir $(y + \sqrt{-26}\,)(y - \sqrt{-26}\,) = x^3$, und da die beiden Faktoren auf der linken Seite teilerfremd sind, muss $(y + \sqrt{-26}\,) = \mathfrak{a}^3$ für ein geeignetes Ideal $\mathfrak{a}$ sein. Ist $\mathfrak{a} = (\alpha)$ ein Hauptideal, so ergibt sich, wie wir gesehen haben, die Lösung $(x, y) = (207, \pm 42849)$. Ist $\mathfrak{a}$ kein Hauptideal, dann liegt es in einer Idealklasse der Ordnung 3. Eine solche wird vom Ideal $\mathfrak{p} = (3, 1 + \sqrt{-26}\,)$ erzeugt, denn es gilt $\mathfrak{p}^3 = (1 + \sqrt{-26}\,)$, und natürlich kann $\mathfrak{p}$ kein Hauptideal sein. Also ist $\mathfrak{p}\mathfrak{a} = (\alpha)$ oder $\mathfrak{p}'\mathfrak{a} = (\alpha)$ Hauptideal. Im ersten Fall folgt aus $(y + \sqrt{-26}\,) = \mathfrak{a}^3$ durch Multiplikation mit $(1 + \sqrt{-26}\,)$ die Gleichung

$$(1 + \sqrt{-26}\,)(y + \sqrt{-26}\,) = (\mathfrak{p}\mathfrak{a})^3 = (\alpha)^3,$$

also

$$\begin{aligned} y - 26 + (y + 1)\sqrt{-26} &= (a + b\sqrt{-26}\,)^3, \\ y - 26 - (y + 1)\sqrt{-26} &= (a - b\sqrt{-26}\,)^3, \end{aligned}$$

woraus durch Addition und Subtraktion die beiden Gleichungen

$$\begin{aligned} y - 26 &= a(a^2 - 78b^2) \\ y + 1 &= b(3a^2 - 26b^2) \end{aligned}$$

folgen. Elimination von y führt schließlich zur Gleichung

$$27 = -a^3 + 3a^2b + 78ab^2 - 26b^3.$$

Die Substitution $a = -3A + b$ macht daraus

$$A^3 - 9Ab^2 + 2b^3 = 1. \tag{4.1}$$

Die Darstellbarkeit von ganzen Zahlen durch eine binäre kubische Form wie (4.1) ist ein nichttriviales Problem (für quadratische Formen ist es im wesentlichen die Pellsche Gleichung): Thue konnte 1909 zeigen, dass eine Gleichung $F(U, V) = m$, wo $F(U, V) = AU^3 + BU^2V + CUV^2 + DV^3$ eine irreduzible kubische Form ist, nur endlich viele Lösungen hat.

Nachdem wir uns davon überzeugt haben, dass eine Lösung der diophantischen Gleichung $y^2 = x^3 - 26$ in ganzen Zahlen zumindest nicht ganz auf der Hand liegt, möchten wir noch eine etwas allgemeiner gehaltene Bemerkung zum Zusammenhang von Klassenzahlen und elliptischen Kurven der Form $y^2 = x^3 - m$ machen. Schreibt man diese Gleichung in der Form $y^2 + m = x^3$, so sieht man, dass für jeden ganzzahligen Punkt (x, y) auf dieser elliptischen Kurve das Hauptideal $(y + \sqrt{-m}\,)$ bis auf Faktoren, die von gemeinsamen Teilern mit dem konjugierten Ideal $(y - \sqrt{-m}\,)$ herrühren, eine dritte Idealpotenz ist. Ideale, deren dritte Potenzen Hauptideale sind, sind natürlich Quellen für Idealklassen der Ordnung 3 in $\mathbb{Q}(\sqrt{-m}\,)$. Etwas allgemeiner führt die Gleichung $y^2 = x^3 - mz^2$ auf Ideale $(y + z\sqrt{-m}\,)$, die oft eine dritte Idealpotenz sind. Genaueres über den Zusammenhang zwischen dieser Gleichung und der 3-Klassengruppe[9] quadratischer Zahlkörper kann man nachlesen in

[9] Das ist die 3-Sylowgruppe der Idealklassengruppe, die also aus allen Idealklassen besteht, deren Ordnung eine Potenz von 3 ist.

S. Hambleton und F. Lemmermeyer, *Arithmetic of Pell Surfaces*, Acta Arith. **146** (2011), 1–12, und in der dort angegebenen Literatur.

Faktorisiert man die Gleichung $y^2 = x^3 - m$ dagegen auf der rechten Seite, ergeben sich Zusammenhänge mit der 2-Klassengruppe von rein kubischen Zahlkörpern $\mathbb{Q}(\sqrt[3]{m}\,)$. Um diese Dinge goutieren zu können, sind allerdings breitere Kenntnisse der algebraischen Zahlentheorie und die Anfangsgründe der Theorie elliptischer Kurven unerlässlich.

Wir wollen uns an dieser Stelle von der diophantischen Analysis verabschieden; das nächste und letzte Kapitel ist dann der Struktur der 2-Klassengruppe gewidmet.

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.

5. Ambige Idealklassen und quadratische Reziprozität

Klassenzahlen von Zahlkörpern sind, selbst im einfachsten Fall quadratischer Zahlkörper, im Falle großer Diskriminanten sehr schwierig zu bestimmen. Dagegen lassen sich darüber, ob diese Klassenzahlen gerade oder ungerade sind, im Falle quadratischer Zahlkörper sehr genaue Aussagen machen. Die dahinter steckende Theorie ist die Geschlechtertheorie, die im Falle quadratischer Zahlkörper – im Gewande der Geschlechtertheorie für binäre quadratische Formen – auf Gauß zurückgeht, und die sich auf zyklische Körpererweiterungen verallgemeinern lässt: es geht nämlich im wesentlichen darum, wie die Galoisgruppe einer Erweiterung auf den Idealklassen operiert. In diesem Kapitel begnügen wir uns mit den allerersten Anfängen, nämlich der ambigen Klassenzahlformel.

5.1 Ambige Idealklassen

Die Bestimmung der Ordnung von $\mathrm{Cl}(k)/\mathrm{Cl}(k)^2$, also des 2-Rangs der Idealklassengruppe, geht im wesentlichen auf Gauss zurück, der dies in der Sprache der binären quadratischen Formen erledigt hat. Man kann die zentralen Fragen dieser Theorie kaum umgehen, wenn man anfängt, die Operation der Galoisgruppe $G = \{1, \sigma\}$ von $k/\mathbb{Q}$ auf der Idealklassengruppe zu untersuchen.

Für eine Idealklasse $c = [\mathfrak{a}]$ setzen wir $c^\sigma = [\mathfrak{a}^\sigma]$. Damit ist $c^{1+\sigma} = [\mathfrak{a}^{1+\sigma}] = [(N\mathfrak{a})] = 1$, also $c^\sigma = c^{-1}$; man sagt auch, σ operiere auf $\mathrm{Cl}(k)$ wie -1. Insbesondere ist $\mathrm{Cl}(k)^{1-\sigma} = \mathrm{Cl}(k)^2$.

Wir nennen eine Idealkasse $c \in \mathrm{Cl}(k)$ ambig, wenn $c^\sigma = c$ ist. Ein Ideal $\mathfrak{a}$ heißt ambig, wenn $\mathfrak{a}^\sigma = \mathfrak{a}$ ist. Ist ein Ideal $\mathfrak{a}$ ambig, dann auch die von ihr erzeugte Idealklasse $[\mathfrak{a}]$; die Umkehrung ist dagegen nicht richtig: da $\mathbb{Q}(\sqrt{34}\,)$ Klassenzahl 2 hat, ist die Idealklasse c der Ordnung 2 ambig. Diese wird aber nicht von einem ambigen Ideal erzeugt, da alle ambigen Ideale Hauptideale sind. Wir wir weiter unten sehen werden, ist jedes ambige Ideal Produkt von verzweigten Primidealen und Idealen der Form (a) mit $a \in \mathbb{Q}^\times$. Die in $\mathbb{Q}(\sqrt{34}\,)$ verzweigten Primideale sind $(2, \sqrt{34}\,) = (6 + \sqrt{34}\,)$ und $(17, \sqrt{34}\,) = (17 + 3\sqrt{34}\,)$.

Übung. Zeige: ist k ein quadratischer Zahlkörper mit Klassenzahl 2, dann ist $\mathrm{Am}(k) = \mathrm{Cl}(k)$.

Übung. Zeige: ist k ein quadratischer Zahlkörper mit ungerader Klassenzahl, dann ist $\mathrm{Am}(k) = 1$.

Die ambigen Idealklassen bilden eine Gruppe $\mathrm{Am}(k)$, in der die von ambigen Idealen erzeugten Idealklassen eine Untergruppe bilden, nämlich die Gruppe

$\mathrm{Am}_{\mathrm{st}}(k)$ der stark ambigen Idealklassen. Unser Ziel ist die Bestimmung der Struktur der Gruppe $\mathrm{Am}(k)$.

Lemma 5.1. *Der nichttriviale Automorphismus $\sigma : \sqrt{m} \to -\sqrt{m}$ von $k = \mathbb{Q}(\sqrt{m})$ operiert wie -1 auf der Idealklassengruppe $\mathrm{Cl}(k)$. Insbesondere ist eine Idealklasse c genau dann ambig, wenn $c^2 = 1$ ist.*

Beweis. Mit $c = [\mathfrak{a}]$ ist $\mathfrak{a}^{1+\sigma} = \mathfrak{a}\mathfrak{a}' = (N\mathfrak{a})$ ein Hauptideal, also $c^{1+\sigma} = 1$ und damit $c^\sigma = c^{-1}$.

Ist c ambig, also $c = c^\sigma$, so ist $c^2 = c^{1+\sigma} = 1$. Ist umgekehrt $c^2 = 1$, so folgt $c^\sigma = c^{-1} = c$. □

Die Gruppe $\mathrm{Am}_{\mathrm{st}}(k)$ der stark ambigen Idealklassen ist nach Definition gleich $\mathrm{Am}_{\mathrm{st}}(k) = AH/H \simeq A/A \cap H$, wo A die Gruppe der von (0) verschiedenen ambigen Ideale bezeichnet und H die Gruppe der Hauptideale. Offenbar ist $A \cap H = H^G$ die Gruppe der ambigen Hauptideale, d.h. wir haben $\mathrm{Am}_{\mathrm{st}}(k) \simeq A/H^G$. Diese Beobachtung liefert uns die exakte Sequenz[1]

$$1 \longrightarrow H^G/I \xrightarrow{\iota} A/I \xrightarrow{\pi} \mathrm{Am}_{\mathrm{st}}(k) \longrightarrow 1. \tag{5.1}$$

Übung. Zeige, dass die "Inklusion" $\iota : H^G/I \longrightarrow A/I$ injektiv und die durch $\pi(\mathfrak{a}I) = [\mathfrak{a}]$ definierte Abbildung $\pi : A/I \longrightarrow \mathrm{Am}_{\mathrm{st}}(k)$ wohldefiniert und surjektiv ist, und weise nach, dass $\ker \pi = \mathrm{im}\ \iota$ ist.

Da $\mathrm{Am}(k)$ elementar-abelsch ist, d.h. $c^2 = 1$ für jede ambige Idealklasse c gilt, ist zur Bestimmung der Struktur von $\mathrm{Am}(k)$ und $\mathrm{Am}_{\mathrm{st}}(k)$ nur die Ordnung dieser Gruppen zu berechnen. Die exakte Sequenz (5.1) ist ein erster Schritt in diese Richtung; die nächsten Schritte bestehen in der Berechnung der Ordnung von H^G/I und A/I.

Zuvor stellen wir ein einfaches aber äußerst nützliches Hilfsmittel vor:

Hilberts Satz 90

Hilberts Satz 90 (dieser Name kommt daher, weil der Satz in Hilberts Zahlbericht von 1897 die Nummer 90 hat) gibt es in zwei Versionen, nämlich für Elemente und für Ideale:

[1] Eine kurze Sequenz abelscher Gruppen A, B, C besteht aus Gruppenhomomorphismen $\alpha : A \longrightarrow B$ und $\beta : B \longrightarrow C$, die man wie folgt zusammenfasst:

$$1 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 1.$$

Die Abbildung $1 \longrightarrow A$ ist diejenige, die das Element der trivialen Gruppe $\{1\}$ auf das neutrale Element von A abbildet; analog ist $C \longrightarrow 1$ derjenige Homomorphismus, der alle Elemente von C auf das neutrale Element der trivialen Gruppe $\{1\}$ abbildet.

Eine Sequenz abelscher Gruppen heißt exakt, wenn der Kern jeder Abbildung dieser Sequenz gleich dem Bild der vorhergehenden Abbildung ist; in unserem Beispiel muss also $\ker \alpha = \mathrm{im}\ (1 \longrightarrow A) = \{1\}$ (und damit α injektiv), $C = \ker(C \longrightarrow 1) = \mathrm{im}\ \beta$ (und damit β surjektiv), sowie $\ker \beta = \mathrm{im}\ \alpha$ sein. Im wesentlichen enthält diese kurze exakte Sequenz die gleiche Information wie der Homomorphiesatz $C \simeq B/\mathrm{im}\ A$, hat aber den Vorteil, dass die dazugehörigen Abbildungen explizit im Diagramm auftauchen. Unter Umständen wird man diesen Vorteil erst dann zu würdigen wissen, wenn man sich näher mit homologischer Algebra oder Galoiskohomologie beschäftigt. Ein Ziel dieses Kapitels ist der Nachweis, dass dies gerade für an Zahlentheorie Interessierte durchaus lohnend ist.

Satz 5.2 (Hilberts Satz 90)**.** *Ist k ein quadratischer Zahlkörper und $\alpha \in k^\times$, so gilt $N\alpha = 1$ genau dann, wenn α die Form $\alpha = \beta^{\sigma-1}$ hat.*

Hierzu äquivalente Formulierungen von Hilberts Satz 90 sind:

1. Es gibt eine exakte Sequenz

$$1 \longrightarrow (k^\times)^{1-\sigma} \longrightarrow k^\times \xrightarrow{N} k^\times,$$

   wo N die Normabbildung $N_{k/\mathbb{Q}} : k^\times \longrightarrow \mathbb{Q}^\times$ bezeichnet.

2. Die Gruppe $k^\times[N]/(k^\times)^{1-\sigma}$ ist trivial.

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

Die entsprechende Aussage für Ideale ist

Satz 5.3 (Hilberts Satz 90 für Ideale)**.** *Ist $\mathfrak{a}$ ein gebrochenes*[2] *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.*

Beweis. Wie oben ist die Richtung "$\Longleftarrow$" trivial. Sei daher $N\mathfrak{a} = 1$ (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 $\mathfrak{c}\mathfrak{d}$ 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 $\mathfrak{a} = \mathfrak{d}'\mathfrak{d}^{-1} = \mathfrak{d}^{\sigma-1}$. □

Übung. Löse die Pythagoreische Gleichung $x^2 + y^2 = z^2$ mit Hilfe von Hilberts Satz 90. Hinweis: $\alpha = \frac{x+yi}{z} \in \mathbb{Q}(i)$ genügt $N\alpha = 1$. Schreibe $\alpha = \frac{m+ni}{m-ni}$ und mache den Nenner rational.

5.2 Die ambige Klassenzahlformel

Als Aufwärmübung konstruieren wir uns eine Reihe von exakten Sequenzen. Dazu führen wir einige Gruppen ein:

- $E = \mathcal{O}_k^\times$ ist die Einheitengruppe von $\mathcal{O}_k$;
- $E[N] = \{\varepsilon \in E : N_{k/\mathbb{Q}}(\varepsilon) = 1\}$ ist der Kern der Normabbildung, also die Gruppe der Einheiten mit Norm $+1$;
- $E^{1-\sigma} = \{\varepsilon^{1-\sigma} : \varepsilon \in E\}$;

[2] Für ganze Ideale ist die Aussage trivial, weil dann $N\mathfrak{a} = (1)$ mit $\mathfrak{a} = (1)$ gleichbedeutend ist.

- $H^G = \{(\alpha) : (\alpha)^\sigma = (\alpha)\}$ ist die Gruppe der ambigen Hauptideale;
- $I = \{(a) : a \in \mathbb{Q}^\times\}$ ist diejenige Untergruppe von A, die aus Idealen besteht, welche von rationalen Zahlen erzeugt werden.

Jetzt behaupten wir

Proposition 5.4. *Es gibt eine exakte Sequenz*

$$1 \longrightarrow E^{1-\sigma} \longrightarrow E[N] \xrightarrow{\lambda} H^G/I \longrightarrow 1.$$

Beweis. Die Abbildung $E^{1-\sigma} \longrightarrow E[N]$ ist die Inklusion: jede Einheit $\varepsilon^{1-\sigma}$ hat natürlich Norm 1. Zur Konstruktion von $\lambda : E[N] \longrightarrow H^G/I$ sei $\varepsilon \in E[N]$, also $N\varepsilon = 1$. Nach Hilberts Satz 90 gibt es ein $\alpha \in k^\times$ mit $\varepsilon = \alpha^{1-\sigma}$; offenbar ist $(\alpha) \in H^G$ wegen $(\alpha)^\sigma = (\alpha^\sigma) = (\varepsilon\alpha) = (\alpha)$. Die Abbildung $\varepsilon \to (\alpha)$ ist allerdings nicht wohldefiniert, da mit α auch jedes αa mit $a \in \mathbb{Q}^\times$ die Eigenschaft $(\alpha a)^{1-\sigma} = \varepsilon$ hat. Aus diesem Grunde setzen wir $\lambda(\varepsilon) = (\alpha)I$, und diese Abbildung ist jetzt wirklich wohldefiniert. Offenbar ist $\varepsilon \in \ker\lambda$ genau dann, wenn $\lambda(\varepsilon) = I$ ist; dies ist gleichbedeutend mit $(\alpha) = (a)$, d.h. mit $\alpha = a\eta$ für eine Einheit η. Damit ist dann $\varepsilon = \alpha^{1-\sigma} = \eta^{1-\sigma}$, und dies zeigt $\ker\lambda = E^{1-\sigma}$.

Die Surjektivität von λ ist klar: ist (α) ambig, also $(\alpha)^\sigma = (\alpha)$, dann muss $\varepsilon\alpha^\sigma = \alpha$ für eine Einheit ε sein, also $\varepsilon = \alpha^{1-\sigma}$. □

Den Inhalt dieser Proposition kann man auch als Isomorphismus

$$E[N]/E^{1-\sigma} \simeq H^G/I$$

ausdrücken. Die Faktorgruppe $H^{-1}(G, E) = E[N]/E^{1-\sigma}$ ist eine Kohomologiegruppe; eine solche ist uns schon in Hilberts Satz 90 begegnet, der ja besagt, dass $H^{-1}(G, k^\times) = 1$ ist. Hilberts Satz 90 für Ideale besagt entsprechend, dass $H^{-1}(G, I_k) = 1$ ist, wenn I_k die Gruppe der von (0) verschiedenen gebrochenen Ideale in einem quadratischen Zahlkörper bezeichnet. Solche Kohomologiegruppen für zyklische Galoisgruppen $G = \langle\sigma\rangle$ tauchen in der Klassenkörpertheorie an allen Ecken und Enden auf.

Die exakte Sequenz aus Prop. 5.4 kommt aus der Galois-Kohomologie[3] übrigens andersherum heraus:

Übung. Man zeige: es gibt eine exakte Sequenz

$$1 \longrightarrow I \longrightarrow H^G \longrightarrow E[N]/E^{1-\sigma} \longrightarrow 1.$$

[3] Wer sich mit den Anfangsgründen der Kohomologietheorie vertraut gemacht hat, bekommt die Sequenz geschenkt: aus der trivialen Sequenz

$$1 \longrightarrow E \longrightarrow k^\times \longrightarrow H \longrightarrow 1,$$

in der H die Gruppe der gebrochenen Hauptideale $\neq (0)$ bezeichnet, erhält man die lange exakte Sequenz

$$1 \longrightarrow E^G \longrightarrow (k^\times)^G \longrightarrow H^G \longrightarrow H^1(G, E) \longrightarrow H^1(G, k^\times),$$

aus der die Behauptung mit Hilberts Satz 90 ($H^1(G, k^\times) = 1$), der Periodizität $H^1(G, A) \simeq H^{-1}(G, A)$ für zyklische G, sowie $(k^\times)^G = \mathbb{Q}^\times$, $E^G = \{\pm 1\}$ und $\mathbb{Q}^\times/E^G \simeq I$ folgt.

Die Ordnung der Gruppe $E[N]/E^{1-\sigma}$ können wir leicht bestimmen. Im Falle $d < 0$ besteht E nur aus Einheitswurzeln mit Norm 1. Also ist $\varepsilon^\sigma = \varepsilon^{-1}$, d.h. $E^{1-\sigma} = E^2$ und somit $E[N]/E^{1-\sigma} = E/E^2 \simeq \mathbb{Z}/2\mathbb{Z}$. Im Falle $d > 0$ sei ε die Fundamentaleinheit. Ist $N\varepsilon = +1$, so ist wieder $E[N] = E$ und $E^{1-\sigma} = E^2$, also $E[N]/E^{1-\sigma} = E/E^2 = \langle -1, \varepsilon\rangle/\langle\varepsilon^2\rangle \simeq (\mathbb{Z}/2\mathbb{Z})^2$. Ist dagegen $N\varepsilon = -1$, so ist $E[N] = \langle -1, \varepsilon^2\rangle$ und $E^{1-\sigma} = E^2 = \langle\varepsilon^2\rangle$, also $E[N]/E^{1-\sigma} = E/E^2 \simeq \mathbb{Z}/2\mathbb{Z}$.

Lemma 5.5. *Sei k ein quadratischer Zahlkörper, deren Einheitengruppe E von der Grundeinheit ε erzeugt wird. Dann ist*

$$H^{-1}(G, E) = E[N]/E^{1-\sigma} \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{falls } d < 0, \\ \mathbb{Z}/2\mathbb{Z} & \text{falls } d > 0, N\varepsilon = -1, \\ (\mathbb{Z}/2\mathbb{Z})^2 & \text{falls } d > 0, N\varepsilon = +1. \end{cases}$$

Damit bleibt noch die Ordnung von A/I zu bestimmen. Dazu bemerken wir

Lemma 5.6. *Ein Ideal $\mathfrak{a}$ ist genau dann ambig, wenn $\mathfrak{a}$ Produkt von verzweigten Primidealen und einem Ideal (a) mit $a \in \mathbb{Q}^\times$ ist. Genauer ist*

$$A/I \simeq (\mathbb{Z}/2\mathbb{Z})^t,$$

wo t die Anzahl der in $k/\mathbb{Q}$ verzweigten Primzahlen bezeichnet, also die Anzahl der verschiedenen Primfaktoren, die in der Diskriminante aufgehen.

Beweis. Wir dürfen annehmen, dass $\mathfrak{a}$ ganz ist (sonst multiplizieren wir mit einer geeigneten ganzen Zahl). Unter allen Zerlegungen $\mathfrak{a} = (a)\mathfrak{b}$ mit ganzem $\mathfrak{b}$ suchen wir uns nun eine aus, in der $a \in \mathbb{N}$ maximal ist.

Ist $\mathfrak{p}$ ein Primideal mit $\mathfrak{p}^\sigma \neq \mathfrak{p}$, welches $\mathfrak{b}$ teilt, muss auch $\mathfrak{p}^\sigma \mid \mathfrak{b}$ sein: aus $\mathfrak{p} \mid \mathfrak{a}$ folgt durch Anwenden von σ auch $\mathfrak{p}^\sigma \mid \mathfrak{b}^\sigma = \mathfrak{b}$. Also ist $(p) \mid \mathfrak{b}$ mit $(p) = \mathfrak{p}\mathfrak{p}^\sigma$, was der Maximalität von a widerspricht. Aus dem gleichen Grund kann $\mathfrak{b}$ nicht durch ein träges Primideal (p) teilbar sein. Also ist $\mathfrak{b}$ Produkt verzweigter Primideale. Ist $\mathfrak{p}$ ein solches, so gilt $\mathfrak{p}^2 = (p)$, und die Maximalität von a impliziert, dass wir unser $\mathfrak{a}$ eindeutig in der Form

$$\mathfrak{a} = (a) \prod \mathfrak{p}_j^{e_j}$$

schreiben können, wo $\mathfrak{p}_j$ die verzweigten Primideale durchläuft und $e_j \in \{0, 1\}$ ist. Jetzt setzt man

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

und zeigt, dass ϕ ein Gruppenisomorphismus ist. □

Tragen wir alles zusammen, folgt aus der exakten Sequenz (5.1) nun

Korollar 5.7. *In quadratischen Zahlkörpern k mit Diskriminante d und Grundeinheit ε gilt*

$$\#\operatorname{Am}_{\mathrm{st}}(k) = \begin{cases} 2^{t-1} & \text{falls } d < 0, \\ 2^{t-1} & \text{falls } d > 0, N\varepsilon = -1, \\ 2^{t-2} & \text{falls } d > 0, N\varepsilon = +1. \end{cases}$$

wo t die Anzahl der in k verzweigten Primzahlen bezeichnet.

Damit bleibt nur noch der Unterschied zwischen $\mathrm{Am}(k)$ und $\mathrm{Am}_{\mathrm{st}}(k)$ zu klären:

Proposition 5.8. *Es gibt eine exakte Sequenz*

$$1 \longrightarrow \mathrm{Am}_{\mathrm{st}}(k) \longrightarrow \mathrm{Am}(k) \longrightarrow (E_{\mathbb{Q}} \cap Nk^{\times})/NE_k \longrightarrow 1.$$

Insbesondere ist $\mathrm{Am}(k) = \mathrm{Am}_{\mathrm{st}}(k)$ *außer wenn* -1 *die Norm eines Elements, aber nicht Norm einer Einheit ist: in diesem Fall ist* $\#\,\mathrm{Am}(k) = 2 \cdot \#\,\mathrm{Am}_{\mathrm{st}}(k)$.

Beweis. Sei $c = [\mathfrak{a}]$ ambig. Dann ist $\mathfrak{a}\sigma \sim \mathfrak{a}$, also $\mathfrak{a}^{\sigma} = \alpha\mathfrak{a}$. Normenbildung liefert $(N\alpha) = (1)$, also $N\alpha = \pm 1 \in E_{\mathbb{Q}} \cap Nk^{\times}$. Wir setzen daher $\mu(c) = N\alpha \cdot NE_k$.

Ist $c \in \ker \mu$, so gilt $N\alpha = N\eta$, d.h. $N(\alpha\eta) = 1$. Nach Hilbert 90 ist $\alpha\eta = \beta^{1-\sigma}$, und aus $\mathfrak{a}^{\sigma} = \alpha\mathfrak{a}$ folgt $(\beta\mathfrak{a})^{\sigma}(\beta)\mathfrak{a}$. Also ist $\mathfrak{b} = \beta\mathfrak{a}$ ein ambiges Ideal äquivalent zu $\mathfrak{a}$, folglich $c = [\mathfrak{b}]$ stark ambig. Umgekehrt sind natürlich stark ambige Idealklassen im Kern von μ enthalten.

Um die Surjektivität zu zeigen, müssen wir nachweisen, dass $-1NE_k$ im Bild liegt, wenn -1 Norm eines Elements aus k ist. Sei also $N\alpha = -1$ für $\alpha = x + y\sqrt{m}$. Dann ist $x^2 - my^2 = -1$, also -1 quadratischer Rest modulo jedem ungeraden Primteiler p von m. Die elementare Zahlentheorie (oder die Arithmetik der Gaußschen Zahlen) zeigt, dass dies genau dann der Fall ist, wenn $m = a^2 + b^2$ Summe zweier Quadrate ist (oBdA sei a ungerade). Jetzt rechnen wir nach, dass $\mathfrak{a} = (a, b + \sqrt{m}\,)$ eine ambige Idealklasse $c = [\mathfrak{a}]$ erzeugt, und dass $\mu(c) = -1$ ist. In der Tat ist

$$\begin{aligned}\mathfrak{a}^2 &= (a^2, ab + a\sqrt{m}, b^2 + 2b\sqrt{m} + m) = (a^2, ab + a\sqrt{m}, 2b^2 + 2b\sqrt{m}\,)\\ &= (a^2, a(b + \sqrt{m}\,), 2b(b + \sqrt{m}\,) = (a^2, b + \sqrt{m}\,) = (b + \sqrt{m}\,),\end{aligned}$$

wobei wir $\gcd(a^2, 2b) = 1$ und $(b + \sqrt{m}\,)(b - \sqrt{m}\,) = b^2 - m = -a^2$ benutzt haben. Also ist $\mathfrak{a}^2 = (b + \sqrt{m}\,)$ und $\mathfrak{a}\mathfrak{a}^{\sigma} = N\mathfrak{a} = (a)$, folglich $\mathfrak{a}^{1-\sigma} = \mathfrak{a}^2/\mathfrak{a}^{1+\sigma} = \frac{1}{a}(b + \sqrt{m}\,)$. Dies liefert $\mu(c) = N(\frac{b+\sqrt{m}}{a}) = \frac{b^2-m}{a^2} = -1$ wie behauptet. $\square$

Übung. Die Ideale $(a, b + \sqrt{m}\,)$ liegen nicht für jede Wahl von a und b in derselben Idealklasse. Man weise dies am Beispiel $m = 10 = 1^2 + 3^2 = 3^2 + 1^2$ nach.

Die Gruppe $(E_{\mathbb{Q}} \cap Nk^{\times})/NE_k$ ist sehr klein, da schon $E_{\mathbb{Q}} = \{\pm 1\}$ nur zwei Elemente hat. In der Tat ist $(E_{\mathbb{Q}} \cap Nk^{\times})/NE_k = 1$, falls -1 nicht die Norm eines Elements aus k oder falls $N\varepsilon = -1$ ist, und $(E_{\mathbb{Q}} \cap Nk^{\times})/NE_k \simeq \mathbb{Z}/2\mathbb{Z}$, falls -1 zwar Norm eines Elements, aber nicht Norm einer Einheit ist. Wie wir eben gesehen haben, ist -1 genau dann Norm eines Elements, wenn $d = \square + \square$ Summe zweier Quadrate ist. Damit haben wir

Satz 5.9 (Die Ambige Klassenzahlformel)**.** *In quadratischen Zahlkörpern k mit Diskriminante d und Grundeinheit ε gilt*

$$\#\,\mathrm{Am}(k) = \begin{cases} 2^{t-2} & \textit{falls } d > 0, N\varepsilon = +1,\ d \neq \square + \square,\\ 2^{t-1} & \textit{sonst.}\end{cases}$$

wo t die Anzahl der in k verzweigten Primzahlen bezeichnet.

Beispiele.

d	t	$N\varepsilon$	$\square+\square$	$\#\,\mathrm{Am}_{\mathrm{st}}(k)$	$\#\,\mathrm{Am}(k)$
8	1	-1	1^2+1^2	1	1
10	2	-1	1^2+3^2	2	2
12	2	$+1$	nein	1	1
30	3	$+1$	nein	2	2
34	2	$+1$	3^2+5^2	1	2
-30	3	$-$	nein	4	4

Übung. Sei p eine verzweigte Primzahl, und sei das Primideal $\mathfrak{p}$ über p ein Hauptideal, z.B. $\mathfrak{p}=(\pi)$. Zeige, dass $\varepsilon=\frac{1}{p}\pi^2$ eine Einheit in $\mathcal{O}_k$ ist, die kein Quadrat ist. Verallgemeinere die Behauptung auf Produkte verzweigter Primideale. Berechne damit die Grundeinheit von $\mathbb{Q}(\sqrt{30})$.

Als weitere Folgerung aus der ambigen Klassenzahlformel halten wir fest:

Korollar 5.10. *Die Klassenzahl des quadratischen Zahlkörpers mit Diskrimintante d ist genau in den folgenden Fällen ungerade; dabei möge p für Primzahlen $\equiv 1 \bmod 4$ und q, q' für Primzahlen $\equiv 3 \bmod 4$ stehen:*

1. *d ist Primdiskriminante, also $d=-4,\pm 8,p,-q$;*
2. *$d=4q$, $d=8q$ oder $d=qq'$.*

Beweis. Die Klassenzahl von k ist genau dann gerade, wenn $\#\,\mathrm{Am}(k)\neq 1$, also die Anzahl der ambigen Idealklassen gerade ist: dies folgt aus $\mathrm{Am}(k)\simeq \mathrm{Cl}(k)/\mathrm{Cl}(k)^2$. Ist nämlich $\mathrm{Am}(k)=1$, so ist das Quadrieren ein Automorphismus auf $\mathrm{Cl}(k)$, und dies geht nur dann, wenn $\mathrm{Cl}(k)$ kein Element der Ordnung 2 hat. Alles andere folgt einfach aus der ambigen Klassenzahlformel. $\square$

5.3 Das Quadratische Reziprozitätsgesetz

Ein Korollar des Korollars ist das quadratische Reziprozitätsgesetz:

Satz 5.11 (Das Quadratische Reziprozitätsgesetz)**.** *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 beiden Ergänzungssätze

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}} \quad \textit{und} \quad \left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}.$$

Beweis. Wir beginnen mit dem ersten Ergänzungssatz. Ist $p\equiv 1 \bmod 4$, so ist $(\frac{-1}{p})=(-1)^{(p-1)/2}=1$ nach dem Eulerschen Kriterium. 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, da p ungerade ist, sofort $p\equiv 1 \bmod 4$.

Ganz entsprechend zeigt man den zweiten Ergänzungssatz: sei h die nach Kor. 5.10 ungerade Klassenzahl von $k=\mathbb{Q}(\sqrt{p})$. 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 $x^2-py^2=\pm 4\cdot 2^h$. Reduktion modulo p liefert, dass $\pm 2^h$ und damit

± 2 quadratischer Rest modulo p ist; die Behauptung folgt dann aus dem ersten Ergänzungssatz.

Ist umgekehrt $(\frac{2}{p}) = +1$, so ist p in $\mathbb{Q}(\sqrt{2}\,)$ zerlegt, und es folgt $\pm p = x^2 - 2y^2$; Reduktion modulo 8 liefert $p \equiv \pm 1 \bmod 8$ in allen Fällen.

Jetzt zum eigentlichen Reziprozitätsgesetz: wir behandeln zuerst den Fall, dass eine der beiden Primzahlen, sagen wir p, kongruent 1 mod 4 ist. Wir werden zeigen, dass dann $\left(\frac{p}{q}\right) = +1 \iff \left(\frac{q}{p}\right) = +1$ 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 die Klassenzahl h von $k$nach Kor. 5.10 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. Wieder folgt aus der Tatsache, dass p in $\mathcal{O}_k$ zerlegt ist, die Gleichung $\pm 4p^h = x^2 - qy^2$ und damit $\left(\frac{\pm p}{q}\right) = +1$. Da entweder $q \equiv 1 \bmod 4$ und $(-1/q) = +1$ oder aber $q \equiv 3 \bmod 4$ und das Vorzeichen notwendig positiv (**Übung!**) ist, folgt in der Tat $\left(\frac{p}{q}\right) = +1$.

Schließlich sei $p \equiv q \equiv 3 \bmod 4$. Wir betrachten $k = \mathbb{Q}(\sqrt{pq}\,)$. Nach Korollar 5.10 ist die Klassenzahl von k ungerade; das Primideal $\mathfrak{p} = (p, \sqrt{pq}\,)$ über p ist dann notwendig Hauptideal: es ist ja $\mathfrak{p}^2 \sim (1)$ und $\mathfrak{p}^h \sim 1$, wegen $h = 2j + 1$ also auch $\mathfrak{p} = \mathfrak{p}^{h-2j} \sim (1)$. Sei daher $\mathfrak{p} = \frac{1}{2}(x + y\sqrt{pq}\,)$. 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. $\square$

Übung. Man zeige, dass für prime $p \equiv 1 \bmod 4$ aus $\left(\frac{q}{p}\right) = +1$ immer $\left(\frac{p}{q}\right) = +1$ folgt, indem man statt mit $\mathbb{Q}(\sqrt{q}\,)$ mit $k = \mathbb{Q}(\sqrt{q^*}\,)$ für $q^* = (\frac{-1}{q})q$ rechnet.

A. Der Satz von Delaunay und Nagell

In diesem Anhang wollen wir einen Einblick in die Beweistechniken geben, die dem Satz von Delaunay[1] und Nagell zugrundeliegen, wonach die Gleichung $x^3 + dy^3 = 1$ in ganzen Zahlen $\neq 0$ höchstens eine Lösung hat. Daraus folgt insbesondere, dass die einzige Lösung von $x^3 - 2y^3 = -1$ durch $x = y = 1$ gegeben ist.

Die Rechnungen laufen in reinen kubischen Zahlkörpern ab, von deren Arithmetik wir allerdings fast überhaupt nichts benutzen werden. Im wesentlichen halten wir uns im folgenden wie auch das Buch *Topics in Number Theory*, vol. II von W.J. LeVesque an das Original: T. Nagell, *Solution compléte de quelques équations cubiques á deux indéterminées*, J. Math. Pures Appl. **4** (1925), 209–270.

A.1 Einheiten in kubischen Zahlringen

Ein reiner kubischer Zahlkörper hat die Form $K = \mathbb{Q}(\sqrt[3]{m}\,)$ für ein $m > 0$, das nicht durch eine dritte Potenz $\neq \pm 1$ teilbar ist. Die Elemente von K haben die Form $x + y\sqrt[3]{m} + zy\sqrt[3]{m}^2$ mit $x, y, z \in \mathbb{Q}$. Wir wollen uns nicht damit aufhalten, die ganzen Elemente in K zu bestimmen, und bemerken nur folgendes: ist $m = ab^2$ mit quadratfreien Zahlen $a, b \in \mathbb{N}$, dann ist $\sqrt[3]{m}^2 = b\sqrt[3]{a^2b}$. Sind $r, s, t \in \mathbb{Z}$, so gehören die Elemente $r + s\sqrt[3]{ab^2} + t\sqrt[3]{a^2b}$ zu den ganzen algebraischen Zahlen in K.

Außerdem brauchen wir noch die Norm eines Elements $\alpha = r + s\sqrt[3]{ab^2} + t\sqrt[3]{a^2b}$; diese ist definiert als das Produkt $N\alpha = \alpha\alpha'\alpha''$ der Konjugierten von α, wobei

$$\alpha' = r + s\rho\sqrt[3]{ab^2} + t\rho^2\sqrt[3]{a^2b}, \quad \alpha'' = r + s\rho^2\sqrt[3]{ab^2} + t\rho\sqrt[3]{a^2b}$$

ist. Eine kleine Rechung liefert

$$N\alpha = r^3 + ab^2s^3 + a^2bt^3 - 3abrst.$$

Wie in quadratischen Zahlkörpern haben Einheiten Norm ± 1.

Ist $x^3 + dy^3 = 1$, so ist $x + y\sqrt[3]{d}$ eine Einheit in $\mathbb{Z}[\sqrt[3]{d}\,]$. Dieser Ring besitzt nach einem Satz von Dirichlet wie reelle quadratische Zahlkörper eine Grundeinheit ε, so dass sich alle Einheiten in der Form $\eta = \pm\varepsilon^n$ für ein $n \in \mathbb{Z}$ schreiben lassen. Der nichttriviale Teil des Dirichletschen Satzes behauptet die Lösbarkeit der Gleichung

$$r^3 + ab^2s^3 + a^2bt^3 - 3abrst = 1,$$

[1] Eine andere geläufige Transliteration ist Delone; Delaunay ist die "französische" Variante. Delaunay hatte seinen Satz 1915 auf russisch publiziert und 1920 durch eine Veröffentlichung in Frankreich bekannt gemacht.

während die Aussage, dass jede Einheit bis auf das Vorzeichen eine Potenz einer Grundeinheit ist, wie im reellquadratischen Fall folgt, wenn man statt $|r+s\sqrt{m}\,|$ den analogen Betrag $|r+s\sqrt[3]{ab^2}+t\sqrt[3]{a^2b}\,|$ betrachtet. Hätte die Gleichung $x^3+dy^3=1$ zwei Lösungen, so müssten zwei verschiedene Potenzen der Grundeinheit eine Einheit $r+s\sqrt[3]{ab^2}+t\sqrt[3]{a^2b}$ mit $t=0$ (im folgenden auch Binomialeinheit genannt) ergeben.

Wir wollen die Bestimmung der Grundeinheit in dem Spezialfall, der uns vor allem interessiert, vorführen, also für $\mathbb{Q}(\sqrt[3]{2}\,)$. Hier ist $\sqrt[3]{2}-1$ Einheit wegen

$$(\sqrt[3]{2}-1)(1+\sqrt[3]{2}+\sqrt[3]{4})=1.$$

Fassen wir $\sqrt[3]{2}$ als reelle Zahl auf, ist $\varepsilon=1+\sqrt[3]{2}+\sqrt[3]{4}>1$. Wir behaupten nun:

Lemma A.1. *Jede Einheit $\eta>1$ in $\mathbb{Z}[\sqrt[3]{2}\,]$ hat die Form $\eta=\varepsilon^n$ für ein ganzes $n\geq 1$.*

Beweis. Die Einheiten ε^n für $n\geq 1$ haben alle Betrag >1. Gibt es eine Einheit $\eta>1$, die nicht von dieser Form ist, so liegt η zwischen zwei Potenzen von ε:

$$\varepsilon^m<\eta<\varepsilon^{m+1}.$$

Also ist $\eta_1=\eta\varepsilon^{-m}$ eine Einheit mit $1<\eta_1<\varepsilon$. Wegen

$$1=|\eta_1\eta_1'\eta_1''|=\eta_1|\eta_1'|^2$$

folgt daraus

$$\frac{1}{\sqrt{\varepsilon}}<|\eta_1'|<1.$$

Schreiben wir $\eta_1=r+s\sqrt[3]{2}+t\sqrt[3]{4}$, so ist nach der Dreiecksungleichung

$$3|r|=|\eta_1+\eta_1'+\eta_1''|\leq|\eta_1|+|\eta_1'|+|\eta_1''|\leq\varepsilon+\frac{2}{\sqrt{\varepsilon}}<4.2,$$

also $|r|\leq 1$. Ganz analog folgt

$$3|s|\sqrt[3]{2}=|\eta_1+\rho^2\eta_1'+\rho\eta_1''|<4.2,$$

also $|s|\leq 1$, und endlich

$$3|t|\sqrt[3]{4}=|\eta_1+\rho\eta_1'+\rho^2\eta_1''|<4.2,$$

woraus $t=0$ folgt. Durchprobieren aller Möglichkeiten liefert dann den gewünschten Widerspruch. □

Ist $0<\eta<1$, so ist $1/\eta=\varepsilon^n$ für ein $n\geq 1$, also $\eta=\varepsilon^n$ für ein $n\in\mathbb{Z}$. Ist endlich $\eta<0$, muss $-\eta$ diese Form haben. Damit haben wir gezeigt:

Proposition A.2. *Jede Einheit von $\mathbb{Z}[\sqrt[3]{2}\,]$ lässt sich eindeutig in der Form*

$$\eta=(-1)^m\varepsilon^n$$

für $m\in\{0,1\}$ und $n\in\mathbb{Z}$ schreiben, wo $\varepsilon=1+\sqrt[3]{2}+\sqrt[3]{2}$ die Grundeinheit von $\mathbb{Z}[\sqrt[3]{2}\,]$ ist.

Diese Aussage bleibt richtig, wenn man ε durch $\varepsilon^{-1}=\sqrt[3]{2}-1$ ersetzt.

A.2 Die Gleichung $x^3 + 2y^3 = 1$

Betrachten wir nun als speziellen Fall die Gleichung

$$(1 - \sqrt[3]{2})^n = x + y\sqrt[3]{2}. \tag{1.1}$$

Für $n \geq 2$ ergibt die Binomialentwicklung der linken Seite die Gleichung

$$\binom{n}{2} - \binom{n}{5} + \binom{n}{8} \mp \ldots = 0.$$

Division durch $\binom{n}{2}$ ergibt

$$-1 = \sum_{k\geq 1} \binom{n-2}{3k} \frac{2(-2)^k}{(3k+1)(3k+2)}.$$

Reduktion modulo 3 liefert wegen $-2 \equiv 1 \bmod 3$ und $(3k+1)(3k+2) \equiv 2 \bmod 3$ die Kongruenz

$$1 + \binom{n-2}{3} + \binom{n-2}{6} + \ldots \equiv 0 \bmod 3.$$

Das folgende Lemma zeigt, dass dies nicht möglich ist:

Lemma A.3. *Für jede positive Zahl m ist*

$$\binom{m}{0} + \binom{m}{3} + \binom{m}{6} + \ldots \not\equiv 0 \bmod 3.$$

Beweis. Wir setzen

$$\begin{aligned} S_0 &= \binom{m}{0} + \binom{m}{3} + \binom{m}{6} + \ldots, \\ S_1 &= \binom{m}{1} + \binom{m}{4} + \binom{m}{7} + \ldots, \\ S_2 &= \binom{m}{2} + \binom{m}{5} + \binom{m}{8} + \ldots; \end{aligned}$$

dann ist

$$S_0 + S_1 + S_2 = 2^m \equiv (-1)^m \bmod 3,$$

sowie

$$\begin{aligned} S_1 &= \binom{m}{0}\frac{m}{1} + \binom{m}{3}\frac{m-3}{4} + \ldots \equiv mS_0 \bmod 3, \\ S_2 &= \binom{m}{1}\frac{m-1}{2} + \binom{m}{4}\frac{m-4}{5} + \ldots \equiv -mS_1 + S_1 \bmod 3, \end{aligned}$$

und daher

$$(-1)^m \equiv S_0 + S_1 + S_2 \equiv (1 + 2m - m^2)S_0 \bmod 3.$$

Die Behauptung folgt. □

Für negative Exponenten läuft (1.1) wegen

$$(\sqrt[3]{2}-1)^{-1} = 1 + \sqrt[3]{2} + \sqrt[3]{4}$$

auf die Gleichung

$$(1 + \sqrt[3]{2} + \sqrt[3]{4})^n = x + y\sqrt[3]{2}$$

hinaus. Diese erkennt man für $n \geq 1$ aber sofort als unmöglich, weil der Koeffizient von $\sqrt[3]{4}$ in der Multinomialentwicklung der linken Seite nur positive Summanden besitzt.

Damit haben wir bewiesen:

Proposition A.4. *Die einzigen ganzzahligen Lösungen der Gleichung (1.1) sind* $n = 0$ *und* $n = 1$.

Ist nun $x^3 + 2y^3 = 1$, so ist $x + y\sqrt[3]{2}$ eine Einheit in $\mathbb{Z}[\sqrt[3]{2}]$ wegen $N(x + y\sqrt[3]{2}) = x^3 + 2y^3$. Also gilt $x + y\sqrt[3]{2} = \pm(1 - \sqrt[3]{2})^n$ nach Prop. A.2, was nach Prop. A.4 nur für $n = 0$ und $n = 1$ möglich ist. Also sind $(x, y) = (1, 0)$ und $(x, y) = (-1, 1)$ die beiden einzigen ganzzahligen Lösungen der Gleichung $x^3 + 2y^3 = 1$.

A.3 Binomialeinheiten als Quadrate

Im allgemeinen Fall hat die Grundeinheit von $\mathbb{Q}(\sqrt[3]{d})$ für $d = ab^2$ die Form $r + s\sqrt[3]{ab^2} + t\sqrt[3]{a^2b}$, und zur Lösung der Gleichung $x^3 + dy^3 = 1$ müssen wir untersuchen, für welche Exponenten n die Einheit η^n eine Binomialeinheit ist. Der folgende Satz befasst sich mit dem einfachsten Fall, in dem das Quadrat einer Einheit eine Binomialeinheit ist; sein Beweis entbehrt, wie ich finde, nicht einer gewissen Komik:

Satz A.5. *Sei K ein reiner kubischer Zahlkörper und*

$$\eta = r + s\sqrt[3]{ab^2} + t\sqrt[3]{a^2b}$$

mit $r, s, t \in \mathbb{Z}$ eine Einheit $\neq 1$ im Ring $\mathbb{Z}[\sqrt[3]{ab^2}, \sqrt[3]{a^2b}]$. Ist dann $\eta^2 = x + y\sqrt[3]{ab^2}$, so gilt

$$\eta = 1 + \sqrt[3]{20} - \sqrt[3]{50}.$$

Beweis. Wir wissen, dass

$$r^3 + ab^2s^3 + a^2bt^3 - 3abrst = 1 \tag{1.2}$$

und wegen

$$\eta^2 = r^2 + 2abst + (2rs + at^2)\sqrt[3]{ab^2} + (2rt + bs^2)\sqrt[3]{a^2b} \tag{1.3}$$

auch

$$2rt + bs^2 = 0$$

gilt. Wäre $r = 0$, so folgte aus (1.2) der Widerspruch $ab = \pm 1$. Also ist $r \neq 0$, und damit wegen (1.3)

$$t = -\frac{bs^2}{2r}.$$

Setzt man dies in (1.2) ein, so findet man mit $d = ab^2$

$$d^2s^6 - 20dr^3s^3 - 8(r^6 - r^3) = 0.$$

Dies ist ein quadratisches Polynom in ds^3; also muss die Diskriminante $\Delta = 16r^2(27r^4 - 2r)$ ein Quadrat sein, und es folgt

$$(27r^3 - 2)r = u^2.$$

Jetzt unterscheiden wir zwei Fälle:

1. r ist gerade: dann ist

$$27r^3 - 2 = \pm 2v^2, \quad r = \pm 2w^2.$$

Reduktion modulo 3 zeigt, dass das positive Vorzeichen nicht gelten kann; setzt man $r = -2v^2$ in die erste Gleichung ein, so erhält man

$$108w^6 + 1 = v^2, \quad \text{also} \quad (v-1)(v+1) = 108w^6.$$

Wegen $\operatorname{ggT}(v-1, v+1) = 2$ ist daher

$$v \pm 1 = 54x^6, \quad v \mp 1 = 2y^6;$$

dies liefert

$$27x^6 - y^6 = (3x^2)^3 + (-y^2)^3 = (\pm 1)^3,$$

und nach dem Fermatschen Satz 3.11 ist dies nur möglich, wenn $x = 0$ oder $y = 0$ ist. Dies ergibt $v = 0$ und $r = s = 0$, was aber nicht sein kann, weil $t\sqrt[3]{a^2b}$ keine Einheit ist.

2. r ist ungerade: dann folgt entsprechend

$$27r^3 - 2 = \pm v^2, \quad r = \pm w^2.$$

Reduktion modulo 3 zeigt, dass das obere Vorzeichen gelten muss, und wir finden

$$(3r)^3 = v^2 + 2,$$

was nach Abschnitt 1.3 die einzige ganzzahlige Lösung $r = 1$ und $v = \pm 5$ hat. Einsetzen liefert $ds^3 = 10 \pm 10$, also $d = 20$ und $s = 1$ (die Möglichkeit $s = 0$ führt auf $rt = 0$, was der Annahme $\eta \neq \pm 1$ widerspricht), was endlich auf

$$(1 + \sqrt[3]{20} - \sqrt[3]{50}\,)^2 = -19 + 7\sqrt[3]{20}$$

als der einzigen Lösung führt.

Damit ist alles bewiesen. □

Zum vollständigen Beweis des Satzes von Delaunay und Nagell sind nun die Fälle zu untersuchen, in denen η^3, η^4 und η^p für prime $p \geq 5$ Binomialeinheiten sind. Die wesentlichen Beweisideen sind dabei schon in obigen Spezialfällen ans Licht getreten. Eine detaillierte Durchführung des Beweises findet sich in den Büchern von Nagell (sh. oben) und Mordell (*Diophantine Equations*, Academic Press 1969).

B. Rechnungen mit pari und sage

B.1 Pari

Pari[1] ist sehr leicht zu bedienen, und die Grundversion braucht man nicht einmal zu installieren, sondern kann nach dem Herunterladen sofort mit dem Rechnen loslegen.

Arithmetik in den ganzen Zahlen

Mit Restklassen rechnet man so: um den Wert von $3^{N-1} \bmod N$ für $N = 2^{67} - 1$ zu finden, tippt man

```
N = 2^67-1; Mod(3,N)^(N-1)
```

(Man beachte, dass der Befehl

```
Mod(3^(N-1),N)
```

etwas ganz anderes tut!) und liest an der Antwort

```
Mod(95591506202441271281, 147573952589676412927)
```

ab, dass $3^{N-1} \equiv 95591506202441271281 \bmod N$ und damit N keine Primzahl ist. Der Befehl

```
factor(2^67-1)
```

liefert sofort die Zerlegung in Primfaktoren in der Form

```
[193707721 1]

[761838257287 1]
```

Die Bedeutung dieser "Vektoren" erklärt sich von selbst, wenn man z.B. die Zahl 48 in Primfaktoren zerlegen lässt.

Einfache Programme lassen sich in `pari` ganz leicht realisieren. Um z.B. den Lucas-Lehmer-Test zu implementieren, tippen wir eine Befehlfolge zwischen zwei geschweiften Klammern ein (genauer tippt man das Programm in ein Text-File und kopiert es dann durch Rechtsklick auf den oberen Balken in das pari-Fenster hinein):

[1] `pari` wurde ursprünglich an der Universität Bordeaux unter der Leitung von Henri Cohen entwickelt.

```
{p=61; N=2^p-1; S=Mod(4,N);
 for(n=1,p-2,S=S^2-2);
 print(lift(S)) }
```

Der Befehl `lift` wandelt eine Restklasse `Mod(2,127)` in den Repräsentanten 2 um und hat den einzigen Zweck, die Ausgabe etwas übersichtlicher zu gestalten. Andere Methoden, um Schleifen zu realisieren, findet man unter `?11`; beispielsweise erklärt `?while`, wie man eine while-Schleife programmiert.

Dass das Ergebnis der obigen Rechnung 0 ist, bedeutet, dass $2^{61}-1$ prim ist. Mit einer Schleife außenrum kann man sich die kleinen Mersenne-Primzahlen ausdrucken lassen:

```
{forstep(p=3,2000,2,if(isprime(p),
  N=2^p-1; S=Mod(4,N);
  for(n=1,p-2,S=S^2-2);
  if(S,,print(p)))) }
```

In Sekundenschnelle gibt `pari` dann folgende Werte aus:

$$p = 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279.$$

Arithmetik in quadratischen Zahlkörpern

Eine Erzeugende des Rings ganzer Zahlen im quadratischen Zahlkörper der Diskriminante $d = 12$ erhält man mit

```
w = quadgen(12)
```

Durch Quadrieren kann man leicht bestätigen, dass $w^2 = 3$ ist. Mit

```
 w = quadgen(13)
```

dagegen wird $w^2 = 3 + w$, also $w = \frac{1+\sqrt{13}}{2}$. Die Grundrechenarten $+$, $-$, $\cdot$ und $:$ lassen sich auf diese Art und Weise leicht beherrschen.

In dieser Ganzheitsbasis werden auch die Lösungen der Pellschen Gleichung angegeben:

```
quadunit(4*67)
```

liefert `48842 + 5967*w`, also die Grundeinheit $\varepsilon = 48842 + 5967\sqrt{67}$, während
`quadunit(21)`
auf das Ergebnis $\varepsilon = 2 + w = 2 + \frac{1+\sqrt{21}}{2} = \frac{5+\sqrt{21}}{2}$ führt. Norm und Spur der Grundeinheit kann man mit

```
eps = quadunit(21); print(norm(eps),"   ",trace(eps))
```

berechnen.

Klassenzahlen und die Klassengruppe quadratischer Zahlkörper erhält man ebenso einfach:

```
quadclassunit(-84)[1]
```

liefert die Klassenzahl 4 von $\mathbb{Q}(\sqrt{-21}\,)$, während

```
quadclassunit(-84)[2]
```

die Struktur der Idealklassengruppe angibt: $[2,2]$ steht beispielsweise für die Gruppe $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Restklassenarithmetik modulo rationaler Primzahlen lässt sich realisieren, indem man

```
w = quadgen(21)*Mod(1,7)
```

eintippt; mit

```
(3-2*w)^7
```

erhält man dann $(3 - 2\frac{1+\sqrt{21}}{2})^7 \equiv 2 \bmod 7$.

Für weitergehende Rechnungen, z.B. mit Idealen, muss man quadratische Zahlkörper "definieren". Dies geschieht am einfachsten durch

```
nf = bnfinit(x^2-79);
```

Dieser Befehl berechnet die grundlegenden Daten, um im quadratischen Zahlkörper $K = \mathbb{Q}(\sqrt{79}\,)$ rechnen zu können. Das Semikolon hat dabei die Funktion, den langen Ausdruck zu unterdrücken. Eine Ganzheitsbasis findet man durch

```
nf.zk
```

Dabei bezeichnet $[1, x]$ die Ganzheitsbasis $\{1, x\}$, wo x die Nullstelle des eingegebenen Polynoms $x^2 - 79$ ist.

Die Idealklassengruppe dieses Zahlkörpers erhält man mit

```
nf.clgp
```

zurück; der Ausdruck

```
[3, [3], [[3, 2; 0, 1]]]
```

gibt die Klassenzahl 3, die Struktur der Idealklassengruppe [3], und ein Ideal (hier ein Primideal $\mathfrak{q}$ über 3), welches die Idealklassengruppe erzeugt.

Mit

```
idealfactor(nf,5)
```

erhält man die beiden Idealfaktoren von 5 in K. Mit

```
p = %[1,1]
```

wählt man sich das erste Primideal aus, das wir im folgenden mit $\mathfrak{p}$ bezeichnen wollen; der Befehl

```
bnfisprincipal(nf,p)
```

liefert dann mit

```
[[2]~, [19/9, -2/9]~]
```

die Aussage, dass das Primideal $\mathfrak{p}$ in der Idealklasse $\mathfrak{q}^2$ liegt, wo $\mathfrak{q}$ das oben gefundene Primideal über der 3 ist, und dass das Hauptideal $\mathfrak{p}\mathfrak{q}^{-2}$ von $\frac{19}{9} - \frac{2}{9}\sqrt{79}$ erzeugt wird, dass also $9\mathfrak{p} = (19-2\sqrt{79}\,)\mathfrak{q}^2$ ist. Die Idealzerlegung von $19-2\sqrt{79}$ kann man durch

```
idealfactor(nf,19-2*x)
```

kontrollieren.

B.2 sage

In `pari` sind nur ganz elementare Funktionen über elliptische Kurven implementiert, sodass für derartige Rechnungen an `sage`[2] kein Weg vorbeiführt. Allerdings ist `sage` auch für Rechnungen in Zahlkörpern um einiges komfortabler als `pari`, und im Zweifelsfall kann man auch von `sage` aus auf `pari` zugreifen.

Zahlkörper

Einen Zahlkörper definiert man in sage mit

```
K.<a> = NumberField(x^2-79)
```

Damit ist a die Nullstelle des Polynoms $x^2 - 79$ im Zahlkörper, also $a^2 = \sqrt{79}$. Mit

```
K.class_group()
```

erhält man die Information
`Class group of order 3 with structure C3 of Number Field`,
und

```
K.units()
```

liefert die Grundeinheit $9\sqrt{79} - 80$. Der Befehl

```
K.integral_basis()
```

versteht sich von selbst. Das Ideal $I = [5, 2 + \sqrt{79}]\,]$ definiert man durch

```
I = K.ideal([5,2+a])
```

und die Ordnung der von I erzeugten Idealklasse findet man mit

```
C = K.class_group()
order(C(I))
```

Für alles weitere müssen wir auf diverse Einführungen in `sage` verweisen, die man im www leicht findet.

[2] Das Programm `sage` geht auf William Stein zurück, verwendet aber Vorarbeit, die in viele Computeralgebrasysteme wie `pari`, `mwrank` oder `GAP` geflossen ist, um nur einige zu nennen.

Elliptische Kurven

In Sage definiert man die elliptische Kurve $y^2 = x^3 + ax + b$ durch den Befehl

```
E = EllipticCurve([a,b])
```

Um die ganzzahligen Lösungen der Gleichung $y^2 = x^3 - 26$ zu finden, definieren wir also zuerst

```
E = EllipticCurve([0,-26])
```

Der Befehl

```
E.rank()
```

zeigt, dass die Gruppe der rationalen Punkte auf dieser Kurve Rang 2 hat; mit

```
E.gens()
```

findet man die erzeugenden Punkte

```
(3 : 1 : 1), (35 : 207 : 1)
```

die im Affinen den Punkten $(x, y) = (3, 1)$ und $(35 : 207)$ entsprechen. Endlich zeigt

```
E.integral_points()
```

dass diese beiden Punkte die einzigen ganzzahligen Lösungen der Gleichung $y^2 = x^3 - 26$ sind. Kopiert man

```
for a in [1..30]:
E = EllipticCurve([0,-a])
print a, E.integral_points()
```

in das Sage-Fenster und drückt enter, erhält man die folgende Tabelle mit allen ganzzahligen Lösungen der Gleichungen $y^2 = x^3 - d$ für $1 \leq d \leq 30$:

d	$y^2 = x^3 - d$	d	$y^2 = x^3 - d$
1	$(1, 0)$	16	
2	$(3, 5)$	17	
3		18	$(3, 3)$
4	$(2, 2), (5, 11)$	19	$(7, 18)$
5		20	$(6, 14)$
6		21	
7	$(2, 1), (32, 181)$	22	
8	$(2, 0)$	23	$(3, 2)$
9		24	
10		25	$(5, 10)$
11	$(3, 4), (15, 58)$	26	$(3, 1), (35, 207)$
12		27	$(3, 0)$
13	$(17, 70)$	28	$(4, 6), (8, 22), (37, 225)$
14		29	
15	$(4, 7)$	30	

Um Satz 4.13 zu testen, lassen wir `sage` folgendes Programm abspulen:

```
for t in [2,4,..20]:
d = 3*t^2+1
E = EllipticCurve([0,-d])
K.<a> = QuadraticField(-d)
print d, K.class_number(), E.integral_points()
```

und erhalten

d	h	Lösungen
13	2	$(17, 70)$
49	1	$(65, 524)$
109	6	$(5, 4), (145, 1746)$
193	4	$(257, 4120)$
301	8	$(401, 8030)$
433	12	$(13, 42), (577, 13860)$
589	16	$(785, 21994)$
769	20	$(1025, 32816)$
973	12	$(1297, 46710)$
1201	16	$(1601, 64060)$

Dass auch `sage` Grenzen gesetzt sind, merkt man, wenn man die Schleife oben bis $t = 20$ verlängert: bei $t = 14$ und $d = 2353$ steigt `sage` aus. Der Grund dafür ist, dass entweder die Erzeugenden der Gruppe der rationalen Punkte auf E zu groß sind oder dass die elliptische Kurve eine nichttriviale Tate-Shafarevich-Gruppe besitzt.

Mit etwas Gespür für Muster kann man anhand der Tabelle übrigens vermuten, dass die Klassenzahl von $\mathbb{Q}(\sqrt{m})$ für alle $m = 12t^2 + 1$ durch 3 teilbar ist, wenn t ein Vielfaches von 3 ist. Dies ist in der Tat der Fall, dürfte aber ohne Klassenkörpertheorie etwas schwierig zu beweisen sein.

Namensverzeichnis

Baker, 69
Bell, 49
Bergmann, 39
Binet, 4

Cassels, 41
Chebyshev, 48
Coleman, 49

Dedekind, 54, 56
Delaunay, 84
Dirichlet, 85

Eisenstein, 37
Euler, 6, 31

Fermat, 6

Gauss, 31, 33, 36, 39

Halupczok, 54
Harper, 54
Hasse, 54
Heegner, 69
Hilbert, 77
Hurwitz, 59

Kummer, 56, 72

Legendre, 40
Lehmer, D., 50
Lucas, 49
Lutzmann, 54

Mersenne, 49
Monsky, 40, 42
Mordell, 89
Motzkin, 53

Nagell, 41, 84
Noether, E., 54

Pepin, 40

Ribet, 8
Rubin, 8

Stark, 69

Thue, 73
Trost, 28

Wiles, 8

Sachverzeichnis

algebraische Zahl, 12
    ganze, 11
assoziiert, 17
Automorphismus, 10

Bezout-Eigenschaft, 25

Dedekind-Hasse Kriterium, 54
Dedekindringe, 63
Diskriminante, 9
Diskriminantentrick, 28

Einheit, 15
Einheitengruppe, 15
elliptische Kurven, 6, 7
euklidische Ringe, 22, 24, 53
Eulers Kriterium, 34
Eulersches Kriterium, 36
exakte Sequenz, 76

Fermatgleichung
    $n = 3$, 39
    $n = 4$, 27
Fibonacci-Zahlen, 4
Fundamentaleinheit, 46

G-Modul, 13
Galoisgruppe, 10
Ganzheitsbasis, 11
    normale, 13
größter gemeinsamer Teiler, 20

Hauptidealring, 22
Hilberts Satz 90, 77

Ideal, 22
    ambiges, 75
    irreduzibles, 61
    maximales, 61
    primes, 61
    primitives, 66
Idealklasse
    ambige, 75
    stark ambige, 76
Idealklassengruppe, 65
Integritätsbereich, 14

irreduzibel, 17

Klassenzahl, 65
Kronecker-Symbol, 64
Kürzungsregel, 60

Legendre-Symbol, 64
Lucas-Lehmer Test, 52

Maximalordnung, 12
Mersenne-Zahlen, 49

Norm, 9
nullteilerfrei, 14

Ordnung, 12

Pellsche Gleichung, 17, 44
prim, 17
Primidealzerlegung
    eindeutige, 58
Primzahl
    träge, 33, 64
    verzweigte, 64
    zerlegte, 64
Produkt von Idealen, 56
pythagoreisches Tripel, 6

quadratische Zahlkörper, 9

Reziprozitätsgesetz, 36, 82

Spur, 9
Summe von Quadraten, 3

teilbar, 14
teilerfremd, 21

unendlicher Abstieg, 27

ZPE-Ringe, 20