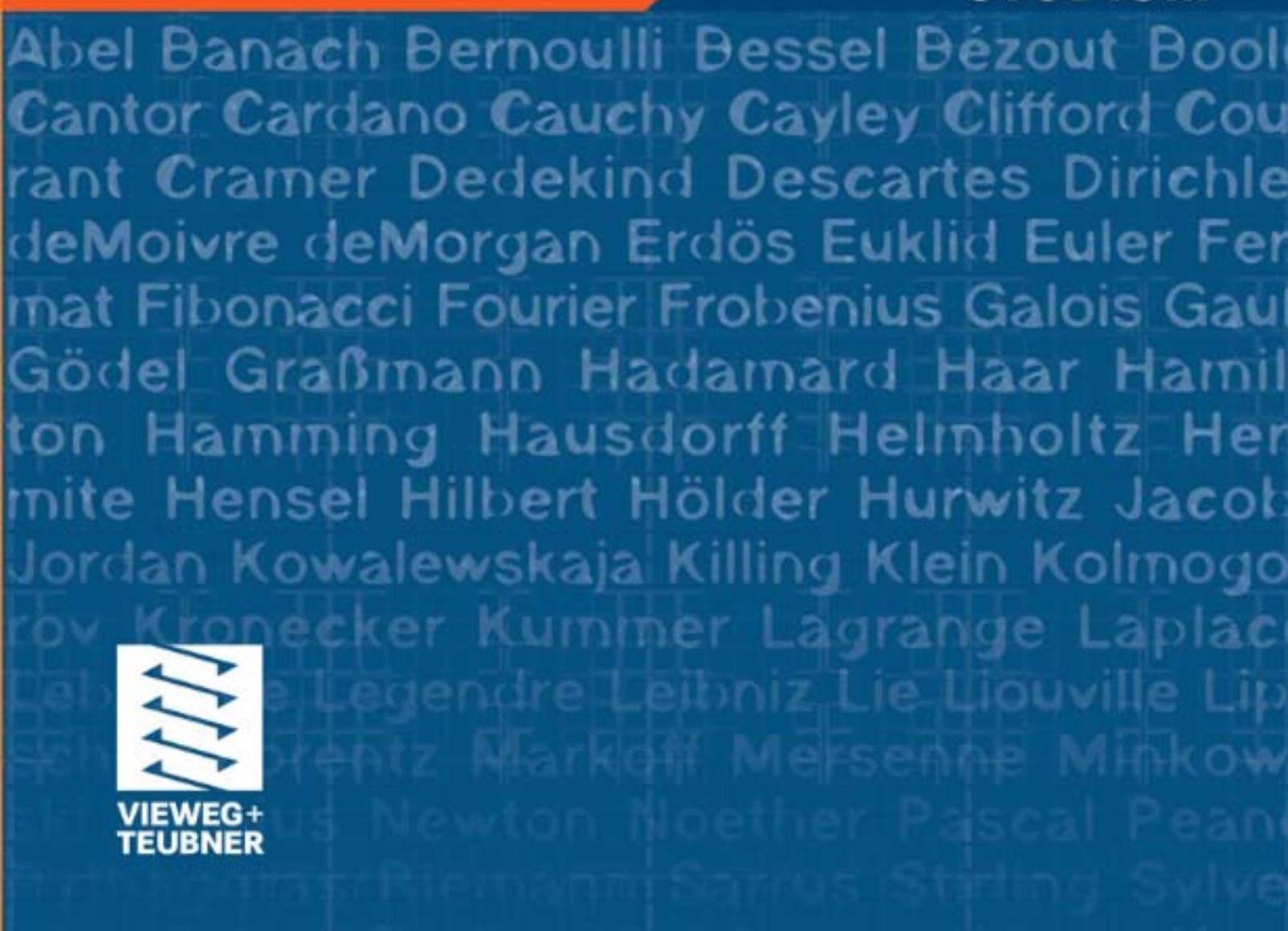
Stefan Müller-Stach | Jens Piontkowski

Elementare und algebraische Zahlentheorie

Ein moderner Zugang zu klassischen Themen

2. Auflage

STUDIUM



VIEWEG+
TEUBNER

Stefan Müller-Stach | Jens Piontkowski

Elementare und algebraische Zahlentheorie

Stefan Müller-Stach | Jens Piontkowski

Elementare und algebraische Zahlentheorie

Ein moderner Zugang zu klassischen Themen

2., erweiterte Auflage

STUDIUM

VIEWEG+
TEUBNER

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der
Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über
<http://dnb.d-nb.de> abrufbar.

Prof. Dr. Stefan Müller-Stach
Johannes Gutenberg-Universität Mainz
Institut für Mathematik
Staudinger Weg 9
55099 Mainz

stach@uni-mainz.de

Priv.-Doz. Dr. Jens Piontkowski
Heinrich-Heine-Universität Düsseldorf
Mathematisches Institut
Universitätsstraße 1
40225 Düsseldorf

piontkow@uni-duesseldorf.de

1. Auflage 2006
2., erweiterte Auflage 2011

Lektorat: Ulrike Schmickler-Hirzebruch | Barbara Gerlach

Vieweg+Teubner Verlag ist eine Marke von Springer Fachmedien.
Springer Fachmedien ist Teil der Fachverlagsgruppe Springer Science+Business Media.
www.viewegteubner.de

Umschlaggestaltung: KünkelLopka Medienentwicklung, Heidelberg
Druck und buchbinderische Verarbeitung: AZ Druck und Datentechnik, Berlin
Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier
Printed in Germany

ISBN 978-3-8348-1256-8

Für unsere Eltern, Evija und Siggi

Vorwort

Der Ausgangspunkt dieses Buches war ein gemeinsam entwickeltes Vorlesungsskript der beiden Autoren, das eine anschauliche Darstellung der Grundbegriffe der elementaren und algebraischen Zahlentheorie zum Ziel hatte. Dabei standen die theoretischen Aspekte zwar im Vordergrund, aber der Stoff sollte immer durch Beispiele und explizite Algorithmen konkretisiert werden.

Der rote Faden dieses Buches ist die Lösungstheorie diophantischer Gleichungen, d.h. die Suche nach ganzzahligen oder rationalen Lösungen von Polynomgleichungen in mehreren Variablen. Dabei stehen die quadratischen Gleichungen im Mittelpunkt, um den Stoff elementar zu halten. Das Buch führt dazu in mehrere Techniken ein. In der Kongruenzrechnung versucht man, eine Gleichung zuerst modulo einer natürlichen Zahl n zu lösen. Dabei bietet es sich an, für n eine Primzahlpotenz p^k zu wählen, weil man die Lösungen zu verschiedenen Primzahlpotenzen mit dem chinesischen Restsatz zusammensetzen kann. Der Grenzübergang von k nach unendlich führt zu den p–adischen Zahlen. An Hand der quadratischen Formen wird demonstriert, wie aus Lösungen über den p–adischen Zahlen auf eine Lösung über den rationalen Zahlen geschlossen werden kann. Einige diophantische Gleichungen werden durch spezielle Techniken effektiver gelöst, so helfen Kettenbrüche bei der Lösung der Pellschen Gleichung $x^2 \quad dy^2 \quad 1$ für $d \quad$.

Eine andere Methode neben der Kongruenzrechnung besteht darin, solche Gleichungen zunächst nicht über den ganzen Zahlen, sondern über einem etwas größeren Ring zu betrachten. Zum Beispiel faktorisiert die Pellsche Gleichung bereits über dem Zahlring $\sqrt{d}$ als $x \quad \sqrt{d}y \quad x \quad \sqrt{d}y \quad 1$. Durch die Beobachtung, dass beide Faktoren Einheiten sind, wird aus der Suche nach Lösungen eine Suche nach Einheiten in $\sqrt{d}$. Welche Erweiterungsringe von $\quad$ für solche Betrachtungen geeignet sind und welche Eigenschaften diese haben, wird in der algebraischen Zahlentheorie studiert. Der Schwerpunkt liegt darauf zu bestimmen, welche dieser algebraischen Erweiterungsringe faktoriell sind, bzw. ihre Abweichung davon mit Hilfe der Klassengruppe zu messen.

Das vorliegende Buch kann auf verschiedene Weisen gelesen und zu Vorlesungen benutzt werden. Die Abschnitte 1– 9 bilden die Grundlage der elementaren Zahlentheorie und sollten auf jeden Fall gründlich bearbeitet werden. Anschließend kann auf drei verschiedene Weisen fortgefahren werden, wenn man eine Auswahl treffen will: Eine Möglichkeit besteht darin, direkt quadratische Formen bis zum Satz von Hasse–Minkowski zu behandeln (13– 15). Andererseits kann man auch Kettenbrüche (10) erarbeiten und darauf aufbauend entweder mit Primzahltests und Faktorisierungsalgorithmen (11– 12) oder mit den Grundbegriffen der algebraischen Zahlentheorie (16– 19) fortfahren. Die Kombination 1– 9 zusammen

mit 10– 12 bietet sich für eine einsemestrige Vorlesung (Modul) im Bachelor–Studiengang an; man kann den Rest des Buches dann für einen Vertiefungsmodul im Rahmen des Master–Studienganges nutzen. Soll der Schwerpunkt schon früh auf die algebraische Zahlentheorie gelegt werden, so liest man 1– 10 mit 16– 19, was aber nur mit einigen Vorkenntnissen in einem Semester behandelt werden kann.

Im Anhang des Buches können Grundkenntnisse über Gruppen, Ringe und Körper nachgeschlagen werden. Eine kurze Einführung in das freie Computeralgebrasystem PARI/GP lädt zu zahlentheoretischen Experimenten ein. Ebenso befinden sich dort die Lösungshinweise zu den Aufgaben.

Wir bedanken uns bei Ralf Gerkmann, Jens Mandavid und Oliver Petras für viele wertvolle Hinweise zu vorläufigen Fassungen des Textes und die tatkräftige Unterstützung beim Übungsbetrieb zu den beiden Vorlesungsreihen in 2004/2005 und 2005/2006. Allen unseren Studenten sind wir sehr dankbar für die aktive Teilnahme an den vier Veranstaltungen und für ihre zahlreichen Korrekturhinweise.

Mainz
September 2006

STEFAN MÜLLER–STACH
JENS PIONTKOWSKI

Vorwort zur zweiten Auflage

In der zweiten Auflage wurden Druckfehler der ersten Auflage berichtigt und weitere Verbesserungen im Text vorgenommen. Außerdem haben wir zahlreiche neue Aufgaben aus Vorlesungen und Staatsexamensklausuren zusammen mit Lösungshinweisen aufgenommen. Wir danken Henning Hollborn und allen anderen, die uns dabei unterstützt haben. Darüber hinaus haben wir einen Anhang über Minkowskitheorie hinzugefügt, um die bisher fehlenden Beweise der Endlichkeit der Klassenzahl sowie des Satzes von Dirichlet geben zu können.

Mainz und Düsseldorf
April 2011

STEFAN MÜLLER–STACH
JENS PIONTKOWSKI

Inhaltsverzeichnis

1 Primzahlen

Einer der Hauptgegenstände der Zahlentheorie sind die Primzahlen, die wir als die natürlichen Zahlen ungleich 1 definieren können, die nur durch 1 und sich selbst teilbar sind. Die wichtigsten Fragen über Primzahlen sind:

1. Wie kann man feststellen, ob eine natürliche Zahl p eine Primzahl ist?
2. Kann man auf einfache Weise eine sehr große Primzahl finden?
3. Wie viele Primzahlen gibt es?
4. Wie sind die Primzahlen in den natürlichen Zahlen verteilt?

Wir wollen in diesem ersten Abschnitt diese Fragen ansprechen — in späteren Abschnitten werden wir die Antworten dann noch weiter vertiefen.

Falls eine natürliche Zahl n keine Primzahl ist, also in ein Produkt $n \quad ab$ mit $a \ b \quad 1$ zerfällt, dann muss a oder b größer gleich $\sqrt{n}$ sein. Diese Überlegung führt zu einem ersten Primzahltest:

Naiver Primzahltest

Sei n gegeben. Teste, ob n durch eine der ganzen Zahlen zwischen 2 und $\sqrt{n}$ teilbar ist. Falls nein, ist n prim. Falls ja, ist n nicht prim.

Wir werden später im Abschnitt 11 wesentlich schnellere Primzahltests kennenlernen.

Um alle Primzahlen von 2 bis zu einer Zahl N zu finden, benutzt man das folgende Verfahren:

Sieb des Eratosthenes

1. Schreibe alle Zahlen von 2 bis N auf.
2. Betrachte jede Zahl n zwischen 2 und N in aufsteigender Reihenfolge: Falls die Zahl nicht gestrichen ist, streiche alle Vielfachen der Zahl mit Ausnahme der Zahl selber.
3. Die verbleibenden nicht–gestrichenen Zahlen sind die Primzahlen.

S. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie,*
DOI 10.1007/978-3-8348-8263-9_1,

Dieses Sieb funktioniert aus zwei Gründen: Erstens werden durch das Streichen der echten Vielfachen von n nur Nicht–Primzahlen entfernt. Zweitens, da man bei den kleinsten Zahlen anfängt, wird eine Nicht–Primzahl gestrichen, sobald n gleich ihrem kleinsten Teiler ungleich 1 ist.

Bestimmen wir als Beispiel die Primzahlen bis 50:

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

Obwohl bei diesem Algorithmus bei den großen Zahlen viel gestrichen wird, gilt doch der folgende Satz:

Satz 1.1 (Euklid) *Es gibt unendlich viele Primzahlen.*

Beweis: Angenommen, es gibt nur die endlich vielen Primzahlen $p_1\ p_2\ \ \ p_n$. Wir setzen $P\ \ \prod_{i\ 1}^{n} p_i\ \ 1$. Nach Definition ist P größer als jede Primzahl, kann also selber keine Primzahl sein. Daher wird P von einer Zahl $1\ \ a\ \ P$ geteilt. Wir wählen das kleinste solche a und behaupten, dass a dann eine Primzahl sein muss. Wäre a nämlich keine Primzahl, so hätte a einen Teiler $1\ \ b\ \ a$. Dieser wäre dann auch ein Teiler von P, im Widerspruch zu Minimalität von a. Also ist der Teiler a von P gleich einem p_j für ein $j\ \ \{1\ \ \ n$. Nun teilt p_j das Produkt $\prod_{i\ 1}^{n} p_i$, aber nicht die 1, somit kann p_j nicht $P\ \ \prod_{i\ 1}^{n} p_i\ \ 1$ teilen. Dieser Widerspruch impliziert die Existenz von unendlich vielen Primzahlen.

Aufgabe 1.2 Modifizieren Sie den Beweis des Satzes von Euklid, um zu zeigen, dass es unendlich viele Primzahlen der Form $4k\ \ 1$ (bzw. $4k\ \ 1$) gibt.

Ganz allgemein gilt der viel tiefer liegende Satz:

Satz 1.3 (Dirichlet) *Seien $a\ b$ teilerfremd. Dann gibt es unendlich viele Primzahlen der Form $ak\ \ b$, wobei k .*

Beweis: Siehe [F, S. 110].

Da man nicht erwarten kann, dass es eine einfache, schnelle Möglichkeit gibt, alle Primzahlen aufzuzählen, sucht man zumindest Funktionen, deren Werte häufig — oder besser immer — Primzahlen sind. Am bekanntesten ist die 1637 von Fermat aufgestellte Vermutung, dass die Zahlen $F_k\ \ 2^{2^k}\ \ 1$ alle Primzahlen sind. Er berechnete damals die ersten fünf Glieder

$$F_0\ \ 3\ \ F_1\ \ 5\ \ F_2\ \ 17\ \ F_3\ \ 257\ \ F_4\ \ 65537$$

und stellte fest, dass diese alle Primzahlen sind. Doch 1732 entdeckte Euler den Teiler 641 von $F_5\ \ 4294967297$. Mittlerweile kennt man die Faktoren der Fermatzahlen bis F_{15} und weiß, dass F_{16} bis F_{36} sowie einige größere Fermatzahlen zusammengesetzt sind. Deshalb

und auch auf Grund eines heuristischen Arguments vermutet man, dass es keine weiteren Primzahlen unter den Fermatzahlen gibt.

Die Tatsache, dass eine doppelte Zweierpotenz bei den Fermatzahlen auftritt, ist kein Zufall.

Lemma 1.4 *Eine Zahl der Form* $b^m - 1 - 2$ *ist höchstens dann prim, wenn* $m - 2^k$ *und* b *gerade ist.*

Beweis: b muss gerade sein, damit $b^m - 1$ ungerade ist. Ist m keine Zweierpotenz, so ist $m - pq$ mit $p - 3$ ungerade. Also gilt $b^m - 1 - b^{pq} - 1 - b^{q\ p} - 1$. Um diesen Term zu faktorisieren, betrachten wir das Polynom $X^p - 1$. Da p ungerade ist, ist $-1\ ^p - 1 - 0$, d.h. -1 ist eine Nullstelle von $X^p - 1$. Daher kann der Term $X - 1$ von $X^p - 1$ abgespalten werden, genauer ist

$$X^p - 1 - X - 1 \ X^{p\ 1} - X^{p\ 2} - X^{p\ 3} - \ - X - 1$$

Setzen wir darin $X - b^q$ ein, so erhalten wir eine Faktorisierung von $b^m - 1$.

Der zweite bekannte Typ von Primzahlen sind die *Mersenneschen Primzahlen*. Dies sind Primzahlen der Form $2^m - 1$.

Lemma 1.5 *Eine Zahl der Form* $2^m - 1$ *ist höchstens dann prim, wenn m prim ist.*

Beweis: Ist $m - pq$ mit $1 - p\ q - m$, so gilt $2^m - 1 - 2^{pq} - 1 - 2^{p\ q} - 1$. Jetzt folgt die Behauptung durch Einsetzen von $X - 2^p$ in die Faktorisierung

$$X^q - 1 - X - 1 \ X^{q\ 1} - \ - X - 1$$

Die Mersenneschen Primzahlen sind deshalb bekannt, weil fast immer die zu einem bestimmten Zeitpunkt bekannte größte Primzahl eine Mersennesche ist. Im Augenblick (März 2011) ist dies $M_{45} - 2^{43\,112\,609} - 1$, eine Zahl mit 12 978 189 Ziffern.

Auch unter den Polynomfunktionen gibt es Funktionen, die viele Primzahlen produzieren. So liefern zum Beispiel

$$f\ n - n^2 - n - 41 \quad \text{und} \quad g\ n - n^2 - 79n - 1601$$

für $0 - n - 39$ bzw. $0 - n - 79$ nur Primzahlen.

Aufgabe 1.6 Zeigen Sie: Es gibt keine Polynomfunktion $f : {}_0 \ $, die nur Primzahlen als Werte hat.

Man kann jedoch Polynome konstruieren, so dass alle deren positiven Werte über $_0$ Primzahlen sind. Tatsächlich hat das folgende Polynom in 26 Variablen,

$$
\begin{aligned}
& k \quad 2 \quad 1 \quad wz \quad h \quad j \quad q^{\,2} \quad gk \quad 2g \quad k \quad 1 \quad h \quad j \quad h \quad z^{\,2} \\
& 2n \quad p \quad q \quad z \quad e^{\,2} \quad 16\, k \quad 1^{\,3} k \quad 2 \quad n \quad 1^{\,2} \quad 1 \quad f^{2\ 2} \\
& e^3 \; e \quad 2 \quad a \quad 1^{\,2} \quad 1 \quad o^{2\ 2} \quad a^2y^2 \quad y^2 \quad 1 \quad x^{2\ 2} \\
& 16r^2y^4 \; a^2 \quad 1 \quad 1 \quad u^{2\ 2} \\
& a \quad u^4 \quad u^2a^{\,2} \quad 1 \quad n \quad 4dy^{\,2} \quad 1 \quad x \quad cu^{\,2\ 2} \\
& n \quad l \quad v \quad y^{\,2} \quad a^2l^2 \quad l^2 \quad 1 \quad m^{2\ 2} \quad ai \quad k \quad 1 \quad l \quad i^{\,2} \\
& p \quad l\, a \quad n \quad 1 \quad b\, 2an \quad 2a \quad n^2 \quad 2n \quad 2 \quad m^{\,2} \\
& q \quad y\, a \quad p \quad 1 \quad s\, 2ap \quad 2a \quad p^2 \quad 2p \quad 2 \quad x^{\,2} \\
& z \quad pl\, a \quad p \quad t\, 2ap \quad p^2 \quad 1 \quad pm^{\,2}
\end{aligned}
$$

die Eigenschaft, dass seine positiven Werte über $^{26}_{0}$ alle Primzahlen sind [R1].

Zusatzaufgaben

Aufgabe 1.7 Sei n ungerade und nicht durch 3 teilbar. Beweisen Sie:

1. 24 teilt n^2 1.
2. Ist n nicht durch 5 teilbar, so wird n^4 1 von 240 geteilt.

Aufgabe 1.8 Bestimmen Sie alle Primzahlen kleiner als 200 ohne Rechner durch die Siebmethode.

Aufgabe 1.9 Zeigen Sie: Ist n 1, so sind die Zahlen n 1 ! k mit 2 k n 1 alle keine Primzahlen. Es gibt also beliebig große Lücken in den Primzahlen.

Aufgabe 1.10 Zeigen Sie: Ist n 4, so können n, n 2, n 4 oder auch n, $2n$ 1, $4n$ 1 nicht alle prim sein.

Aufgabe 1.11 Sei p der kleinste Primfaktor von n und p $\sqrt[3]{n}$, dann ist n p entweder prim oder 1.

Aufgabe 1.12 Sei p_k die k–te Primzahl. Zeigen Sie:

1. $p_{k\ 1}$ p_1p_2 p_k 1.
2. p_k 2^{2^k}.
3. $\pi\, x$ $\#\{p$ p x p prim $\log\log x$.

2 Teilbarkeitstheorie

Im ersten Abschnitt haben wir die Primzahlen als natürliche Zahlen ungleich 1 definiert, die nur 1 und sich selbst als Teiler haben. Dies kann man so verstehen, dass die Primzahlen unzerlegbar sind: Wenn man eine Primzahl p in ein Produkt zweier natürlicher Zahlen zerlegt, ist die eine davon p und die andere 1. Zum Beispiel kann man 13 nur zerlegen als 13 13 1, 6 jedoch als 6 6 1 2 3. Jeder kennt auch noch eine weitere Charakterisierung einer Primzahl p: Falls p das Produkt zweier natürlicher Zahlen teilt, dann teilt p bereits eine dieser Zahlen. Zum Beispiel teilt 13 das Produkt 39 21 und damit (hier) den ersten Faktor 39 3 13, aber obwohl 6 das Produkt 4 9 teilt, teilt sie weder 4 noch 9.

Dass diese Eigenschaften äquivalent sind, ist nicht ganz offensichtlich. Tatsächlich gilt nicht in jedem Ring eine analoge Äquivalenz. In diesem Abschnitt wollen wir dies klären und dabei die Begriffe kennenlernen, die nötig sind, um Teilbarkeitsfragen zu diskutieren.

Definition 2.1 *Sei R ein Integritätsring und a b R.*

> a teilt *b, falls b ac für ein c R. Dies schreibt man als a b. Nicht–Teilbarkeit wird als a b geschrieben.*
>
> *Die* Einheiten *des Ringes sind die Teiler der Eins, R : $\{u$ $R : u$ 1 .*
>
> *Die Elemente a b heißen* assoziiert*, falls sie sich nur um eine Einheit unterscheiden, also a ub für ein u R .*

Erste elementare Aussagen über die Teilbarkeit sind:

Lemma 2.2 *Für Elemente in einem Integritätsring gilt:*

1. *a b a bc.*
2. *a b_1 und a b_2 a c_1b_1 c_2b_2.*
3. *a b ca cb.*
4. *a b und b c a c.*
5. *a b und b a a ub für ein u R .*

Damit interessante Aussagen über die Teilbarkeit möglich sind, muss der Ring noch weitere Eigenschaften haben. Bei den ganzen Zahlen haben wir zum Beispiel die Division mit Rest.

Satz 2.3 (Divisionsalgorithmus) *Seien a b mit b 0. Dann gibt es eindeutig bestimmte ganze Zahlen q r mit a qb r, wobei 0 r b .*

S. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie,*
DOI 10.1007/978-3-8348-8263-9_2,

Aufgabe 2.4 Beweisen Sie diesen Satz.

Ringe, in denen eine Division mit Rest existiert, nennt man *euklidische Ringe*. Die genaue Definition ist wie folgt:

Definition 2.5 *Ein Integritätsring R heißt* euklidisch*, falls eine Norm–Funktion*

$$N : R \setminus \{0\} \to \mathbb{N}_0$$

existiert, so dass gilt:

> *Sind $a, b \in R$ mit $b \neq 0$, dann gibt es $q, r \in R$ mit $a = qb + r$, wobei entweder $r = 0$ oder $r \neq 0$ und $N(r) < N(b)$ gilt.*

Neben den ganzen Zahlen ist der Polynomring $R[X]$ in einer Variablen mit $N(f) = \deg(f)$ das bekannteste Beispiel (Polynomdivision mit Rest). In diesem Beispiel — wie auch vielen anderen — wird N auf eine sinnvolle Weise auf ganz R fortgesetzt, hier mit $N(0) = -\infty$.

Beispiel (Gaußsche Zahlen) Die Gaußschen Zahlen

$$\mathbb{Z}[i] = \{x + iy \mid x, y \in \mathbb{Z}\}$$

sind ein Unterring der komplexen Zahlen mit der Norm–Funktion

$$N(z) = z\overline{z} = |z|^2 \geq 0$$

Ist $z = x + iy$, dann ist $N(z) = x^2 + y^2$. Offensichtlich gilt $N(z) = 0 \Leftrightarrow z = 0$. Die Norm–Funktion ist multiplikativ, d.h. $N(wz) = N(w)N(z)$, denn $N(wz) = wz\overline{wz} = w\overline{w}z\overline{z} = N(w)N(z)$. Mit der Norm–Funktion kann man auch die Einheiten erkennen:

$$z \in \mathbb{Z}[i] \text{ ist Einheit} \Leftrightarrow N(z) = 1 \Leftrightarrow z \in \{1, -1, i, -i\}$$

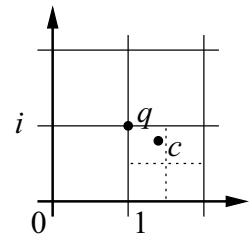
Um dies zu sehen, sei $z \in \mathbb{Z}[i]$. Aus $z \cdot z^{-1} = 1$ folgt $N(z) \cdot N(z^{-1}) = N(1) = 1$. Da die Norm–Funktion nur natürliche Zahlen als Werte annimmt, erhalten wir $N(z) = 1$. Weiter erhalten wir aus $N(z) = x^2 + y^2 = 1$ sofort, dass $x = \pm 1$ oder $y = \pm 1$, d.h. $z \in \{1, -1, i, -i\}$. Dies sind wegen $1^2 = i^2 = (-1)^2 = (-i)^2 = 1$ Einheiten.

Wir zeigen nun, dass $\mathbb{Z}[i]$ euklidisch ist. Seien dazu $a, b \in \mathbb{Z}[i]$ mit $b \neq 0$ gegeben. Wir bezeichnen ihren Quotienten a/b im Körper $\mathbb{Q}[i]$ mit c. Es gilt $c = u + iv$ mit $u, v \in \mathbb{Q}$. Wähle Approximationen $u', v' \in \mathbb{Z}$ mit $|u - u'| \leq 1/2$ und $|v - v'| \leq 1/2$. Wir setzen $q := u' + iv' \in \mathbb{Z}[i]$ und $r := a - bq$. Dann gilt

$$|c - q|^2 = |u - u'|^2 + |v - v'|^2 \leq \left(\tfrac{1}{2}\right)^2 + \left(\tfrac{1}{2}\right)^2 = \tfrac{1}{2} < 1$$

$$N(r) = |r|^2 = |a - bq|^2 = |c - q|^2 \cdot |b|^2 \leq \tfrac{1}{2}|b|^2 = \tfrac{1}{2}N(b) < N(b)$$

Wir rechnen ein Beispiel mit $a = 3 - 2i$ und $b = 1 - 2i$. Dann ist $c = \frac{7}{5} - \frac{4}{5}i$. q ist die Rundung von c zur nächsten Zahl in $\mathbb{Z}[i]$, hier also $q = 1 - i$. Wir bekommen $r = a - bq = 3 - 2i - (1 - 2i)(1 - i) = i$, und es gilt $1 = N(i) < N(b) = 5$. Die Rundung kann man sich am besten graphisch veranschaulichen.



Aufgabe 2.6 Durch die Nicht–Eindeutigkeit der Rundung, falls $u \quad u' \quad 1 \quad 2$ oder $v \quad v' \quad 1 \quad 2$ ist, sind mehrere Divisionen mit Rest möglich. Berechnen Sie alle im Fall $\quad 2 \quad 7i \quad 1 \quad i$.

Aufgabe 2.7 $\sqrt{\ 2}\quad\quad\sqrt{\ 2}$ ist auch euklidisch bezüglich der Norm–Funktion $N\ z \quad z^{\ 2}$, aber $\sqrt{\ 5}$ nicht.

Euklidische Ringe — insbesondere also — sind Hauptidealringe, d.h., die Struktur ihrer Ideale ist ganz einfach.

Definition 2.8 *Ein Integritätsring heißt* Hauptidealring*, falls jedes Ideal I in R ein Hauptideal ist, d.h.,*

$$I \quad a \ : \ Ra : \ \{ra\ r \quad R \quad \text{für ein } a \quad R$$

Satz 2.9 *Jeder euklidische Ring ist ein Hauptidealring.*

Beweis: Sei $I \quad 0$ ein Ideal. Wähle $a \quad I \quad \{0$ mit $N\ a$ minimal. Wir behaupten $I \quad a$. Sei $b \quad I$, dann gibt es $q\ r$ mit $b \quad qa \quad r$ und $r \quad 0$ oder $N\ r \quad N\ a$. Da $r \quad b \quad qa \quad I$ und $N\ a$ minimal ist, muss $r \quad 0$ und $b \quad qa \quad a \quad I$ sein.

Bemerkung 2.10 *Zwei Erzeuger eines Hauptideals in einem Integritätsring sind assoziiert.*

Beweis: Gilt $a \quad b$, so ist $a \quad rb$ und $b \quad sa$ für geeignete $r\ s \quad R$. Also $a \quad rsa$ oder äquivalent dazu $a\ rs \quad 1 \quad 0$. In einem Integritätsring folgt $a \quad 0$ oder $rs \quad 1$. Falls $a \quad 0$, muss auch $b \quad 0$ sein. Falls $rs \quad 1$, sind r und s Einheiten, daher sind a und b assoziiert.

Wir kommen zurück zu den beiden äquivalenten Eigenschaften von Primzahlen. Zuerst formalisieren wir diese:

Definition 2.11 *Sei R ein Integritätsring und* $0 \quad p \quad R \quad R$.

p heißt prim*, falls für alle r s R aus p rs folgt, dass p r oder p s.*

p heißt irreduzibel*, falls aus p rs für r s R folgt, dass p zu r oder s assoziiert ist. (Der andere Faktor ist damit eine Einheit.)*

p heißt reduzibel*, falls p nicht irreduzibel ist.*

Bemerkung 2.12 *Ein primes Element ist immer irreduzibel.*

Beweis: Angenommen für ein primes Element p gilt $p \mid ab$, insbesondere $p \mid ab$. Da p prim ist, teilt p das Element a nach eventueller Vertauschung von a und b. Also gilt $a = pr$ für ein $r \in R$ und daher $p \mid ab = pr\,b = rb\,p$. Weil R ein Integritätsring ist, gilt $rb = 1$, somit sind $r, b \in R$ und $a = pr$ assoziiert zu p.

In einem beliebigen Integritätsring ist jedoch nicht jedes irreduzible Element auch prim.

Aufgabe 2.13 $2 \mid \sqrt{-5}\cdot\sqrt{-5}$ ist irreduzibel, aber nicht prim.

Wenn wir wollen, dass jedes irreduzible Element auch prim ist, müssen wir das als Bedingung an den Ring stellen. Dies führt zur Definition des faktoriellen Ringes, allerdings brauchen wir eine weitere Bedingung, damit die Definition wirklich nützlich ist. Daher nutzen wir hier die von den natürlichen Zahlen bekannte Primfaktorzerlegung in der Definition und zeigen in Satz 2.17 verschiedene äquivalente Charakterisierungen von faktoriellen Ringen.

Definition 2.14 *Ein* faktorieller Ring *ist ein Integritätsring, in dem jedes Element, das weder Null noch eine Einheit ist, in ein Produkt von Primelementen zerlegt werden kann (Primfaktorzerlegung).*

Lemma 2.15 *In einem faktoriellen Ring ist ein irreduzibles Element prim.*
Eine Primfaktorzerlegung eines Elementes ist bis auf Assoziiertheit und Reihenfolge der Faktoren eindeutig.

Beweis: Da sich ein irreduzibles Element nicht weiter in Primfaktoren zerlegen lässt, muss es in einem faktoriellen Ring prim sein. Seien nun zwei Primfaktorzerlegungen eines Elementes

$$r = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m \in R$$

gegeben. Wegen $p_1 \mid r$ teilt p_1 eines der q_j, sei dies nach eventueller Umnummerierung q_1. Aus $p_1 \mid q_1$, also $q_1 = sp_1$ für $s \in R$, und der Irreduzibilität von q_1 folgt, dass $s \in R^\times$ und q_1 zu p_1 assoziiert ist. Wir kürzen die Produktzerlegung zu

$$p_2 p_3 \cdots p_n = sq_2\, q_3 \cdots q_m \in R$$

und wiederholen das Verfahren bis alle Faktoren abgebaut sind.

Definition 2.16 *Ein Element $a \neq 0$ eines faktoriellen Ringes R heißt* quadratfrei*, falls für alle $0 \neq r \in R$, $R \neq R^\times$ gilt: $r^2 \nmid a$.*

Nach dem Lemma werden in $\mathbb{Z}$ also die Zerlegungen $12 = 2\cdot 3 = 2\cdot 2\cdot 2 = -3$ als im Wesentlichen gleich betrachtet. Wir sehen auch, dass 12 nicht quadratfrei ist.

Hier sind andere mögliche Definitionen von faktoriellen Ringen:

Satz 2.17 *Für einen Integritätsring sind äquivalent:*

1. *R ist faktoriell.*
2. *Jedes Element, das weder die Null noch eine Einheit ist, kann in ein* Produkt von Primelementen *zerlegt werden, wobei die Faktoren bis auf Assoziiertheit und Reihenfolge der Faktoren eindeutig sind.*
3. *Jedes Element, das weder die Null noch eine Einheit ist, kann in ein* Produkt von irreduziblen Elementen *zerlegt werden, wobei die Faktoren bis auf Assoziiertheit und Reihenfolge der Faktoren eindeutig sind.*
4. *Jedes Element, das weder die Null noch eine Einheit ist, kann in ein* Produkt von irreduziblen Elementen *zerlegt werden. Weiter ist jedes irreduzible Element prim.*

Beweis: 1 2 ist Lemma 2.15. 2 3 folgt aus Bemerkung 2.12. 4 1 ist trivial. Bleibt bei 3 4 zu zeigen, dass jedes irreduzible Element prim ist. Sei also p irreduzibel, und p teile ab. Dann gibt es c mit $pc = ab$. Wir zerlegen a b c in ihre irreduziblen Faktoren $a = \prod_i a_i$, $b = \prod_j b_j$, $c = \prod_k c_k$. Dann sind

$$p\prod_k c_k = \prod_i a_i \prod_j b_j$$

zwei Zerlegungen des Elements ab in irreduzible Faktoren. Wegen der Eindeutigkeit der Zerlegung muss p zu einem der a_i oder b_j assoziiert sein, also teilt p entweder a oder b.

Nun wollen wir zeigen, dass die ganzen Zahlen — oder allgemeiner jeder Hauptidealring — ein faktorieller Ring ist.

Satz 2.18 *Jeder Hauptidealring ist faktoriell.*

Beweis: Wir zeigen zuerst, dass jedes irreduzible Element prim ist. Sei p irreduzibel und $p \mid ab$, aber $p \nmid a$. Wir müssen $p \mid b$ zeigen. Betrachte $I = \{pa + x : x \in I\}$. I ist ein Hauptideal $I = (r)$, wobei $r \mid p$ und $r \mid a$. Da p irreduzibel ist, ist r entweder eine Einheit oder assoziiert zu p. Das zweite ist unmöglich, da $p \nmid a$, aber $r \mid a$. Also ist $r \in R^\times$ und $I = (r) = R$. Wir finden daher $x, y \in R$ mit $xp + ya = 1 \in R = \{pa + x : x \in I\}$. Multiplikation mit b ergibt $xpb + yab = b$, aus $p \mid ab$ folgt schließlich $p \mid b$.

Wir müssen noch zeigen, dass jedes Element in ein Produkt von irreduziblen Elementen zerlegt werden kann. Sei $0 \neq r \in R \setminus R^\times$ beliebig. Falls r nicht irreduzibel ist, zerlegen wir es in ein Produkt zweier Elemente. Falls diese nicht irreduzibel sind, zerlegen wir sie wieder usw. Wir müssen uns überlegen, dass dieser Prozess abbricht. Falls nicht, bekommen wir eine Folge von Elementen r_i mit $r_{i+1} \mid r_i$ und damit eine Kette von Idealen $(r_1) \subset (r_2) \subset (r_3) \subset \ldots$. Daher ist auch $I = \bigcup_i (r_i)$ ein Ideal. Da R ein Hauptidealring ist, ist $I = (r_\infty)$ für ein $r_\infty \in I$. Aus $r_\infty \in I$ folgt $r_\infty \in (r_i)$ für ein geeignetes $i \in \mathbb{N}$. Dann ist aber $(r_i) \subset (r_\infty)$ und damit $r_i \mid r_{i+1} \mid \ldots \mid r_\infty$. Somit sind r_i und r_{i+1} assoziiert, und die Zerlegung in der i–ten Stufe war keine echte Zerlegung.

Die positiven Primelemente der ganzen Zahlen heißen *Primzahlen*, in Zeichen $\mathbb{P}$. Man nennt die reduziblen ganzen Zahlen auch *zusammengesetzte Zahlen*.

Beispiel (Gaußsche Zahlen) Was sind die Primelemente in i ? Wir erinnern uns, dass nur die Einheiten 1 i in i die Norm eins haben. Wir werden die Primelemente — genauso wie die Einheiten — über ihre Norm finden. Sei also π i prim. Wegen $N\ \pi$ $\pi\overline{\pi}$ teilt π eine Primzahl p . Sei πz p, dann ist $N\ \pi$ $N\ z$ $N\ p$ p^2. Also gilt entweder $N\ \pi$ p oder π ist assoziiert zu p.

Alle Elemente π mit $N\ \pi$ p müssen prim sein. Denn aus π ab folgt p $N\ \pi$ $N\ a$ $N\ b$, daher muss $N\ a$ oder $N\ b$ eins und a oder b eine Einheit sein.

Nun betrachten wir eine Primzahl p . Wegen 2 1 i 1 i ist 2 nicht prim in i . Sei p eine ungerade Primzahl. Wir wollen zeigen, dass p genau dann prim in i ist, wenn p nicht die Summe der Quadrate zweier natürlicher Zahlen ist. In Abschnitt 9 werden wir sehen, dass dies genau die Primzahlen der Form $4k$ 3 sind. Sei also p x^2 y^2 die Summe zweier Quadrate, dann ist p wegen p x iy x iy und $N\ x$ iy p 1 nicht prim. Andererseits sollte p nicht prim sein, so gibt es Nichteinheiten $a\ b$ i mit p ab. Wegen p^2 $N\ p$ $N\ a\ N\ b$ und $N\ a$ $N\ b$ 1 folgt $N\ a$ $N\ b$ p. Falls a x iy ist, ist p $N\ a$ x^2 y^2 die Summe zweier Quadrate.

Zusammenfassend sind die Primelemente in i bis auf Assoziiertheit die Zahlen mit einer Norm, die eine Primzahl in ist, und die Primzahlen in der Form p $4k$ 3.

Faktorielle Ringe haben viele gute Eigenschaften, zum Beispiel gilt:

Satz 2.19 *Sei R ein faktorieller Ring, dann ist auch der Polynomring $R\ X$ ein faktorieller Ring.*

Beweis: Siehe [Wü, Satz 12.18].

Zusatzaufgaben

Aufgabe 2.20 Faktorisieren Sie die Zahl 47355 ohne Rechner.

Aufgabe 2.21 Nutzen Sie Satz 2.19, um zu zeigen, dass X ein faktorieller Ring ist, der jedoch kein Hauptidealring ist.

Aufgabe 2.22 Bestimmen Sie alle multiplikativen Einheiten im Ring der stetigen, reellen Funktionen f : mit der punktweisen Addition und Multiplikation. Welche Funktionen sind die irreduziblen Elemente?

Aufgabe 2.23 Finden Sie für die folgenden Ringe R und Ideale I R jeweils ein Element a R mit I a :

1. R : , I : $8\ 14\ 36$.
2. R : $\mathbb{Q}\ X$, I : $2X^3$ X^2 $2X$ $1\ 6X^2$ $13X$ 5 .

Aufgabe 2.24 Entscheiden Sie, ob die folgenden Ideale in X Hauptideale sind:

$$I_1 : \quad 3\ X \qquad \text{und} \qquad I_2 : \quad X \quad 7\ 2X \quad 13$$

Aufgabe 2.25 Sei K ein Körper und $0 \quad f \quad K\,X$.

1. Ist $a \quad K$ eine Nullstelle von f, dann gibt es ein $g \quad K\,X$ mit $f \quad X \quad a\,g$.
2. Ist $n \quad \deg f$ der Grad von f, dann hat f höchstens n Nullstellen in K.
3. Bestimmen Sie alle Nullstellen von $f : \quad X^4 \quad 8X^3 \quad 14X^2 \quad 8X \quad 15$ über $\mathbb{Q}$.

Aufgabe 2.26 Zeigen Sie: $\sqrt{2}$ und $\sqrt{3}$ sind euklidische Ringe.

Aufgabe 2.27 Zeigen Sie: $1 \quad \sqrt{\ 7\ } \quad 2$ ist euklidisch, aber $\sqrt{\ 7\ } \quad 1 \quad \sqrt{\ 7\ }$ noch nicht einmal faktoriell.

Aufgabe 2.28 Sei R ein euklidischer Ring mit euklidischer Funktion $N : R \quad \{0$. Definieren Sie die neue Abbildung $N' : R \quad \{0$ durch $N'\ a \quad \min\{N\ ax \quad x \quad R \quad \{0$. Zeigen Sie, dass $R\ N'$ ein euklidischer Ring ist und N' die Eigenschaft $N'\ a \quad N'\ ab$ erfüllt für alle $a\ b \quad R \quad \{0$.

Aufgabe 2.29 Welche der Zahlen $1, i, 1 \quad i, 1 \quad i, 3 \quad i, 2 \quad 4i, 4 \quad 2i, 8 \quad 6i$ und $11i \quad 10$ sind assoziiert bzw. teilen einander in i ?

Aufgabe 2.30 Zerlegen Sie die natürlichen Zahlen 101, 103 und 2310 in Primfaktoren innerhalb i .

3 Der ggT und der euklidische Algorithmus

Definition 3.1 *Sei R ein faktorieller Ring und a b R, nicht beide* 0*. Dann ist* der größte gemeinsame Teiler ggT *a b ein Element c, so dass gilt*

c a und c b.

Jedes Element d, das a und b teilt, teilt auch c.

Die Existenz werden wir gleich beweisen. Der ggT kann nur eindeutig bis auf Assoziiertheit sein. Es ist üblich, das in der Schreibweise zu ignorieren, so kann man sowohl ggT 4 6 2 als auch ggT 4 6 2 schreiben. Natürlich darf man nicht 2 2 folgern.

Der größte gemeinsame Teiler von drei oder mehr Elementen ist analog definiert. Zwei Elemente heißen *teilerfremd*, falls ihr ggT eins ist. Drei oder mehr Elemente können keinen gemeinsamen Teiler haben, obwohl sie paarweise nicht teilerfremd sind, zum Beispiel 6 10 15.

Bevor wir die Existenz des größten gemeinsamen Teilers beweisen, wollen wir einige elementare Eigenschaften zeigen.

Lemma 3.2 *Seien a, b und c Elemente eines faktoriellen Ringes.*

1. ggT *a b* ggT *b a* .
2. ggT *a* 0 *a und* ggT *a* 1 1.
3. ggT *ca cb* *c* ggT *a b* .
4. ggT *a b* *a* *a b.*
5. ggT *a b* ggT *a bc* .
6. ggT *a b* *ca* ggT *a b* .
7. ggT *a b c* ggT *a* ggT *b c* .
8. ggT *a b* 1 ggT a^i b^j 1 *für i j* .
9. *a bc und* ggT *a b* 1 *a c.*
10. ggT *a b* 1 ggT *a bc* ggT *a c* .

S. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie,*
DOI 10.1007/978-3-8348-8263-9_3,

Beweis: Die Eigenschaften 1)–7) sind elementar. Für 8) reicht es zu zeigen, dass kein Primelement ggT $a^i\ b^j$ teilt. Nehmen wir also an, dass es ein Primelement p gibt mit p ggT $a^i\ b^j$. Dann gilt $p\ a^i$ und $p\ b^j$. Nach der Primeigenschaft gilt auch $p\ a$ und $p\ b$, also p ggT $a\ b$. Wegen ggT $a\ b$ 1 ist p eine Einheit im Widerspruch zu p prim. Für 9) stellen wir uns a, b und c zerlegt in ihre Primfaktoren vor. Wegen ggT $a\ b$ 1 können keine der Primfaktoren von a und b assoziiert sein. Also müssen sämtliche der Primfaktoren von a mit der entsprechenden Multiplizität unter den Primfaktoren von c vorkommen, d.h., a teilt c. Bei 10) gilt ggT $a\ c$ ggT $a\ bc$ nach 5). Wir müssen die umgekehrte Teilbarkeit zeigen. Sei d ggT $a\ bc$, dann gilt $d\ a$ und $d\ bc$. Aus $d\ a$ und ggT $a\ b$ 1 folgt ggT $d\ b$ 1 nach 5). Mit 9) ergibt sich $d\ c$ und somit auch d ggT $a\ c$.

Eine Art der Berechnung des ggT bei den ganzen Zahlen ist wohlbekannt. Betrachten wir als Beispiel die Zahlen 132 und 504. Zuerst zerlegen wir diese Zahlen in Primfaktoren: 132 $2^2\ 3\ 11$ und 504 $2^3\ 3^2\ 7$. Da der ggT beide Zahlen teilt, muss er ein Produkt der in beiden Primfaktorzerlegungen auftretenden Primzahlen sein. Damit er möglichst groß wird, wählen wir die Potenzen möglichst groß, also gleich dem Minimum der beiden Potenzen in den Zerlegungen — in unserem Beispiel ggT 132 504 $2^2\ 3$ 12. Genau wie in diesem Beispiel kann man allgemein die Existenz des ggT zeigen.

Satz 3.3 *In einem faktoriellen Ring existiert der größte gemeinsame Teiler und ist eindeutig bis auf Assoziiertheit.*

Beweis: Für die Eindeutigkeit nehmen wir an, dass c und c' größte gemeinsame Teiler von a und b sind. Insbesondere teilen beide also a und b, daher muss nach der zweiten Eigenschaft des ggT $c\ c'$ und $c'\ c$ gelten. Nach Lemma 2.2 sind c und c' daher assoziiert.

Wir zeigen nun die Existenz. Nach dem Lemma 3.2 können wir $a\ b$ 0 annehmen. Sei P die Menge aller Primfaktoren, die in den Primfaktorzerlegungen der zwei Elemente a und b auftreten. Falls es in P zwei assoziierte Primelemente gibt, entfernen wir eins von beiden. Jetzt gibt es nach Lemma 2.15 eindeutig bestimmte $n_p\ m_p$ 0 für p P und $u\ v$ R mit

$$a \quad u \prod_{p\ P} p^{n_p} \qquad\qquad b \quad v \prod_{p\ P} p^{m_p}$$

Dann ist

$$c \quad \prod_{p\ P} p^{\min\ n_p\ m_p}$$

der ggT von a und b. Denn offensichtlich gilt $c\ a$ und $c\ b$. Weiter ergibt sich aus der Eindeutigkeit der Primfaktorzerlegung, dass jeder Teiler von a und b als $w \prod_{p\ P} p^{k_p}$ mit k_p 0 und w R schreibbar ist. Offenbar ist dann c das „größte Element“, das a und b teilt.

Aufgabe 3.4 Berechnen Sie ggT 3080 7956 , indem Sie den Schritten des Beweises folgen.

In Hauptidealringen kann ggT $a\ b$ als Linearkombination von a und b dargestellt werden.

Satz 3.5 *Sei R ein Hauptidealring und a b R. Dann existieren x y R mit*

$$\text{ggT}\ a\ b \quad xa \quad yb$$

Beweis: Betrachte das Ideal $I = a\ b = \{xa + yb \mid x, y \in R\}$. Weil R ein Hauptidealring ist, gibt es ein c mit $I = c$. Wir behaupten $c = \mathrm{ggT}(a, b)$. Da a und b in I sind, teilt c beide. Ist d ein Teiler von a und b, so teilt d jedes Element in I und damit auch c. Also ist c der ggT von a und b. Wegen $c \in I = a\ b$ existieren die in der Aussage verlangten $x, y \in R$.

Die Elemente x, y sind nicht eindeutig, so erfüllt neben x, y zum Beispiel auch $x + b, y - a$ die Gleichung. Im Allgemeinen ist es auch nicht offensichtlich, wie man x, y zu gegebenen a, b finden kann. Erst in euklidischen Ringen gibt es einen schnellen Algorithmus, um den ggT zu berechnen und x und y zu finden.

Aufgabe 3.6 Finden Sie alle Elemente $x, y \in \mathbb{Z}^2$ mit $2x + 3y = 1$.

Satz 3.7 (Euklidischer Algorithmus) *Seien a_0 und a_1 Elemente eines euklidischen Ringes. Man berechne a_{i+1} als Rest der Division von a_{i-1} durch a_i, d.h.*

$$a_{i-1} = q_{i-1}a_i + a_{i+1} \quad \text{mit } N(a_{i+1}) < N(a_i) \text{ oder } a_{i+1} = 0$$

solange bis $a_{k+1} = 0$. Dann ist $\mathrm{ggT}(a_0, a_1) = a_k$.

Beweis: Wegen $N(a_1) > N(a_2) > N(a_3) > \ldots$ muss nach endlich vielen Schritten die 0 erreicht werden. Nach Lemma 3.2 ist für $0 \le i \le k$

$$\mathrm{ggT}(a_{i-1}, a_i) = \mathrm{ggT}(q_{i-1}a_i + a_{i+1}, a_i) = \mathrm{ggT}(a_{i+1}, a_i) = \mathrm{ggT}(a_i, a_{i+1})$$

und daher

$$\mathrm{ggT}(a_0, a_1) = \mathrm{ggT}(a_1, a_2) = \ldots = \mathrm{ggT}(a_k, a_{k+1}) = \mathrm{ggT}(a_k, 0) = a_k$$

Beispiel Berechnen wir hier als Beispiel $\mathrm{ggT}(93, 42) = 3$:

$$\begin{aligned} 93 &= 2 \cdot 42 + 9 \\ 42 &= 4 \cdot 9 + 6 \\ 9 &= 1 \cdot 6 + 3 \\ 6 &= 2 \cdot \underline{3} + 0 \end{aligned}$$

Aufgabe 3.8 Berechnen Sie jetzt $\mathrm{ggT}(3080, 7956)$ mit dem euklidischen Algorithmus.

Mit etwas Mehraufwand lassen sich auch die Elemente x, y aus Satz 3.5 finden. In unserem Beispiel geht das durch die folgende Rückwärtsrechnung, beginnend bei der vorletzten Zeile:

$$\begin{aligned} 3 &= 9 - 1 \cdot 6 & 9 &= 1 \cdot 42 - 4 \cdot 9 \\ 1 &= 42 - 5 \cdot 9 & 1 &= 42 - 5 \cdot 93 + 2 \cdot 42 \\ 5 &= 93 - 11 \cdot 42 \end{aligned}$$

Jetzt formalisieren wir diese Rechnung.

Satz 3.9 (Erweiterter euklidischer Algorithmus) *Seien a und b Elemente eines euklidischen Ringes.*

Man setze $a_0 \quad a, a_1 \quad b, x_0 \quad 1, y_0 \quad 0, x_1 \quad 0$ *und* $y_1 \quad 1$ *und berechne* $a_{i\ 1}\ q_{i\ 1}\ x_{i\ 1}\ y_{i\ 1}$ *für* $i \quad 1$ *wie folgt*

$$a_{i\ 1} \quad q_{i\ 1}a_i \quad a_{i\ 1} \qquad \textit{mit } N\ a_{i\ 1} \quad N\ a_i \ \textit{ oder } a_{i\ 1} \quad 0$$
$$x_{i\ 1} \quad x_{i\ 1} \quad q_{i\ 1}x_i$$
$$y_{i\ 1} \quad y_{i\ 1} \quad q_{i\ 1}y_i$$

solange bis $a_{k\ 1} \quad 0$.

Dann ist ggT $a\ b \quad a_k \quad x_k a \quad y_k b$.

Beweis: Nach dem vorangegangenen Satz reicht es aus, per Induktion zu zeigen, dass für alle i

$$a_i \quad x_i a \quad y_i b$$

gilt. Der Induktionsanfang für $i \quad 0\ 1$ wird durch die Definition von $x_0\ x_1\ y_0\ y_1$ gesichert. Der Induktionsschluss läuft wie folgt

$$a_{i\ 1} \quad a_{i\ 1} \quad q_{i\ 1}a_i \quad x_{i\ 1}a \quad y_{i\ 1}b \quad q_{i\ 1}\ x_i a \quad y_i b$$
$$x_{i\ 1} \quad q_{i\ 1}x_i\ a \quad y_{i\ 1} \quad q_{i\ 1}y_i\ b \quad x_{i\ 1}a \quad y_{i\ 1}b$$

Beispiel Wir nutzen wieder die Zahlen $a \quad 93$ und $b \quad 42$ als Beispiel:

i	a_i	q_i	x_i	y_i
0	93	—	1	0
1	42	—	0	1
2	9	2	1	2
3	6	4	4	9
4	3	1	5	11
5	0	2		

Daher gilt $3 \quad \text{ggT } 93\ 42 \quad 5\ 93 \quad 11 \quad 42$.

Aufgabe 3.10 Berechnen Sie jetzt x und y für die Zahlen $a \quad 3080$ und $b \quad 7956$.

Aufgabe 3.11 Programmieren Sie den Algorithmus in einer beliebigen Programmiersprache.

Analog zum größten gemeinsamen Teiler ist das kleinste gemeinsame Vielfache definiert:

Definition 3.12 *Sei R ein faktorieller Ring und* $a\ b \quad R$. *Dann ist* das kleinste gemeinsame Vielfache kgV $a\ b$ *ein Element c, so dass gilt*

a c und b c.

Jedes Element d, das von a und b geteilt wird, wird auch von c geteilt.

Analog zum ggT können wir die Existenz des kgV über die Primfaktorzerlegung beweisen. Falls

$$a \quad u \prod_{p \ P} p^{n_p} \qquad\qquad b \quad v \prod_{p \ P} p^{m_p}$$

wie im Beweis von Satz 3.3, dann ist

$$\text{kgV } a \ b \quad \prod_{p \ P} p^{\max \ n_p \ m_p}$$

In unserem obigen Beispiel mit $a \quad 132 \quad 2^2 \ 3 \ 11$ und $b \quad 504 \quad 2^3 \ 3^2 \ 7$ ist kgV $a \ b$ $2^3 \ 3^2 \ 7 \ 11 \quad 5544$.

Wir beweisen jetzt einen Zusammenhang zwischen ggT und kgV, der auch die schnelle Berechenbarkeit im Falle von euklidischen Ringen sichert.

Satz 3.13 *Für zwei Elemente $a \ b \quad 0$ eines faktoriellen Ringes gilt (bis auf Assoziiertheit)*

$$\text{kgV } a \ b \quad \frac{ab}{\text{ggT } a \ b}$$

Beweis: Sei wie im Beweis von Satz 3.3 und obiger Bemerkung $a \quad u \prod_{p \ P} p^{n_p}$ und b $v \prod_{p \ P} p^{m_p}$, also ggT $a \ b \quad \prod_{p \ P} p^{\min \ n_p \ m_p}$ und kgV $a \ b \quad \prod_{p \ P} p^{\max \ n_p \ m_p}$. Dann ist

$$ab \quad uv \prod_{p \ P} p^{n_p \ \ m_p} \quad uv \prod_{p \ P} p^{\min \ n_p \ m_p \quad \max \ n_p \ m_p} \quad uv \ \text{ggT } a \ b \quad \text{kgV } a \ b$$

daher gilt die behauptete Gleichheit bis auf Assoziiertheit.

Zusatzaufgaben

Aufgabe 3.14 Berechnen Sie den ggT der folgenden Zahlenpaare und schreiben Sie ihn als Linearkombination: 681 361 und 12345 54321 .

Aufgabe 3.15 Bestimmen Sie den ggT der Polynome

$$f: \quad x^3 \quad 4x^2 \quad x \quad 6 \qquad \text{und} \qquad g: \quad x^4 \quad 14x^3 \quad 59x^2 \quad 46x \quad 120$$

Aufgabe 3.16 Bestimmen Sie ggT $2^{250} \quad 1 \ 2^{100} \quad 1$.

Aufgabe 3.17 Sei $R \qquad i$ der Ring der Gaußschen Zahlen.

1. Seien $a \ b \quad R$ teilerfremd, und es gelte $ab \quad \varepsilon c^n$ für ein $n \qquad$ und Elemente $c \quad R$, $\varepsilon \quad R$. Zeigen Sie: Dann gibt es Einheiten $\varepsilon' \ \varepsilon'' \quad R$ und $r \ s \quad R$ mit $a \quad \varepsilon' r^n$ und $b \quad \varepsilon'' s^n$.

2. Ein *primitives Pythagoräisches Tripel* (PPT) ist ein Tripel $x \ y \ z$ teilerfremder natürlicher Zahlen mit $x^2 \quad y^2 \quad z^2$. Sei $x \ y \ z$ ein PPT und $a: \quad x \quad iy \quad R$. Beweisen Sie mit Hilfe von Teil 1, dass dann $r \quad R$ und $\varepsilon \quad R$ existieren mit $a \quad \varepsilon r^2$.

3. Sei $x\ y\ z$ ein PPT. Zeigen Sie: Nach eventueller Vertauschung von x und y gibt es ein Paar $u\ v$ teilerfremder natürlicher Zahlen, $u\ v$ nicht beide ungerade, $u \quad v$, mit

$$x \quad u^2 \quad v^2 \quad y \quad 2uv \quad z \quad u^2 \quad v^2$$

Aufgabe 3.18 Berechnen Sie jeweils $z \quad \text{ggT}\ a\ b$ in $\quad i$ und geben Sie eine Linearkombination $z \quad xa \quad yb$ an:

1. $a \quad 208 \quad i,\ b \quad 509.$
2. $a \quad 1 \quad 3i,\ b \quad 5i \quad 1.$
3. $a \quad 5i \quad 1,\ b \quad 1 \quad 8i.$

Aufgabe 3.19 Welche Paare aus den folgenden Zahlen besitzen einen gemeinsamen Teiler in $\quad i$?

$$101 \quad 2^{100} \quad 1 \quad 10 \quad i \quad 2^{50} \quad 1 \quad 2^{50} \quad i \quad 2^{100} \quad i \quad 2^{100} \quad i \quad 2^{100} \quad 1 \quad 2^{150} \quad 1$$

Aufgabe 3.20 Sei $R \quad \sqrt{3}$ und $a \quad 47 \quad 17\sqrt{3}$ sowie $b \quad 36 \quad 16\sqrt{3}$ gegeben. Bestimmen Sie $z \quad \text{ggT}\ a\ b$ in $\quad \sqrt{3}$ und geben Sie eine Linearkombination $z \quad xa \quad yb$ an. Benutzen Sie hierbei, dass $\quad \sqrt{3}$ euklidisch ist mit der Normfunktion $N\ a \quad b\sqrt{3} \quad a^2 \quad 3b^2$ (siehe Aufgabe 2.26).

4 Kongruenzrechnung

Bei der Kongruenzrechnung betrachten wir die ganzen Zahlen „bis auf Vielfache“ einer natürlichen Zahl n .

Definition 4.1 *Seien a b und n . Dann ist a* kongruent *zu b modulo n, in Zeichen a $b \bmod n$, falls n a b*

Falls a nicht kongruent zu b ist, schreibt man das als a $b \bmod n$.

Also heißt a $b \bmod n$, dass a und b die gleichen Reste bei einer Division durch n haben.

Beispiele 2 5 12 mod 7; a gerade a 0 mod 2; a ungerade a 1 mod 2.

Was die Kongruenzen so nützlich macht, ist, dass man mit ihnen rechnen kann wie mit ganzen Zahlen, aber zusätzlich an jeder Stelle Vielfache von n subtrahieren kann. So darf man zum Beispiel

$$6 \quad 3 \; 4 \quad 5 \quad 6 \quad 12 \quad 5 \quad 6 \; 17 \quad 102 \mod 7$$

aber auch

$$6 \quad 3 \; 4 \quad 5 \quad 1 \quad 2 \quad 5 \quad 1 \quad 3 \quad 3 \quad 4 \mod 7$$

rechnen. Dies ist gerechtfertigt durch den folgenden Satz:

Satz 4.2 *Sei a $b \bmod n$ und c $d \bmod n$, dann gilt*

$$a \quad c \quad b \quad d \bmod n \quad \textit{und} \quad a \; c \quad b \; d \bmod n$$

Beweis: Nach Voraussetzung gilt a b kn und c d ln für gewisse k l . Daher ist

$$a \quad c \quad b \quad d \quad k \quad l \; n \qquad a \quad c \quad b \quad d \bmod n.$$

$$ac \quad bd \quad bl \quad dk \quad kln \; n \qquad ac \quad bd \bmod n.$$

Mit Induktion folgt aus dem Satz auch a^m $b^m \bmod n$ für alle m $_0$, falls a $b \bmod n$. Dies hat die folgende schöne Anwendung:

Beispiel (Teilbarkeitstests) Jeder weiß, dass eine Zahl genau dann durch 3 teilbar ist, wenn ihre Quersumme durch 3 teilbar ist. Dies beweist man mit Hilfe der Kongruenzrechnung. Sei $a_m a_{m\ 1} \quad a_0, a_i \quad \{0 \quad 9$, eine Zehnerdarstellung der Zahl $a \quad \sum_{i\ 0}^{m} a_i 10^i$. Ihre Quersumme ist $\sum_{i\ 0}^{m} a_i$. Aus $10 \quad 1 \bmod 3$ folgt $10^i \quad 1 \bmod 3$ und daher

$$a \quad \sum_{i\ 0}^{m} a_i 10^i \quad \sum_{i\ 0}^{m} a_i \mod 3$$

S. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie,*
DOI 10.1007/978-3-8348-8263-9_4,

Also ist a genau dann durch 3 teilbar ($a \equiv 0 \bmod 3$), wenn es die Quersumme von a ist. Für die Teilbarkeit durch 11 muss man wegen $10 \equiv -1 \bmod 11$, also

$$a \equiv \sum_{i=0}^{m} a_i 10^i \equiv \sum_{i=0}^{m} a_i (-1)^i \bmod 11$$

die alternierende Quersumme betrachten.

Aufgabe 4.3 Die Zahl 531958 ist durch 7 teilbar, denn es ist

$$\begin{aligned} 531958 &\equiv \underline{8}\cdot 10^0 + \underline{5}\cdot 10^1 + \underline{9}\cdot 10^2 + \underline{1}\cdot 10^3 + \underline{3}\cdot 10^4 + \underline{5}\cdot 10^5 \\ &\equiv \underline{8}\cdot 1 + \underline{5}\cdot 3 + \underline{9}\cdot 2 + \underline{1}\cdot(-1) + \underline{3}\cdot(-3) + \underline{5}\cdot(-2) \equiv 0 \bmod 7 \end{aligned}$$

1. Formulieren und beweisen Sie eine allgemeine Regel für Teilbarkeit natürlicher Zahlen durch $n \geq 7$.
2. Entwickeln Sie analoge Teilbarkeitstests für alle $n \in \{2, \ldots, 15\}$.

Man kann die Kongruenzrechnung auch bei alltäglichen Fragestellungen nutzen:

Aufgabe 4.4 Der Geburtstag von Carl F. Gauß ist der 30. April 1777. Auf welchen Wochentag fiel das?

Das Potenzrechnen modulo Primzahlen wird durch den folgenden Satz vereinfacht. Wir werden ihn später auch für einen Primzahltest benutzen.

Satz 4.5 (Kleiner Satz von Fermat) *Sei p eine Primzahl. Dann gilt für alle a*

$$a^p \equiv a \bmod p$$

Diese Aussage ist äquivalent zu $a^{p-1} \equiv 1 \bmod p$ für $a \not\equiv 0 \bmod p$ nach Korollar 4.10. Der Satz ist eine einfache Folgerung aus folgendem Hilfssatz.

Hilfssatz 4.6 *Seien $a, b \in \mathbb{N}$, dann gilt*

$$(a+b)^p \equiv a^p + b^p \bmod p$$

Beweis: Nach der Binomialformel gilt

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i}$$

Für die Behauptung reicht es zu zeigen, dass $\binom{p}{i}$ für $0 < i < p$ durch p teilbar ist. Nun sind die Zahlen $\binom{p}{i}$ gegeben durch

$$\binom{p}{i} = \frac{p!}{i!\,(p-i)!}$$

Beim Kürzen von $p!$ durch $i!\,(p-i)!$ kann der Faktor p nicht weggekürzt werden, da p die größte auftretende Primzahl ist. Daher ist p ein Teiler von $\binom{p}{i}$.

Beweis (Kleiner Satz von Fermat): Wir betrachten zuerst $a \geq 0$ und führen eine Induktion durch. Der Fall $a = 0$ ist klar. Für den Induktionsschritt folgt aus dem Hilfssatz und der Induktionsannahme

$$a+1)^p \equiv a^p + 1^p \equiv a + 1 \mod p$$

Beim Fall $a < 0$ gilt nach dem eben gezeigten $(-a)^p \equiv -a \bmod p$. Für $p = 2$ ist $a \equiv -a \bmod 2$, und die Aussage folgt. Für eine ungerade Primzahl p gilt $a - 1)^p = (-1)^p a^p = -a^p \bmod p$. Durch Multiplikation mit -1 folgt auch hier die Behauptung.

Beispiel Modulo 7 gilt: $3^{100} = 3^{7\cdot 14+2} = (3^7)^{14} \cdot 3^2 \equiv 3^{14} \cdot 3^2 \equiv 3^2 \cdot 3^2 = (3^2)^2 \equiv 2^2 \equiv 4 \bmod 7$. Die äquivalente Aussage $a^p - 1 \equiv 1 \bmod p$ ist noch einfacher zu nutzen: $3^{100} = 3^{6\cdot 16+2\cdot 2} \equiv (3^6)^{16} \cdot 3^{2\cdot 2} \equiv 1^{16} \cdot 2^2 \equiv 4 \bmod 7$.

Eine Gleichung, die modulo 12 wahr ist, ist natürlich auch modulo 2, 3, 4 und 6 wahr. Diese und ähnliche Eigenschaften halten wir im folgenden Lemma fest, das sofort aus der Definition folgt.

Lemma 4.7 *Für a, b und n, m gelten folgende Regeln:*

1. *$a \equiv b \bmod n$ und $m \mid n$ $\Rightarrow$ $a \equiv b \bmod m$.*
2. *$a \equiv b \bmod n$ $\Rightarrow$ $ma \equiv mb \bmod mn$.*

Ein großer Teil der Zahlentheorie beschäftigt sich mit dem Lösen von diophantischen Gleichungen. Eine mögliche Strategie besteht darin, solche Gleichungen zunächst über $\mathbb{F}_p$ zu lösen. Zuerst wollen wir daher lineare Gleichungen mit Kongruenzen lösen:

Satz 4.8 *Gegeben sei die Gleichung*

$$ax \equiv b \mod n \quad \text{mit } a, b \text{ und } n$$

Sei $d = \mathrm{ggT}(a, n)$.

1. *Falls $d \nmid b$, dann besitzt die Gleichung keine Lösung.*
2. *Sei $d \mid b$. Wähle y, z mit $ya + zn = d$ (zum Beispiel mit Hilfe des euklidischen Algorithmus). Dann ist die obige Gleichung äquivalent zu*

$$x \equiv y\tfrac{b}{d} \mod \tfrac{n}{d}$$

und besitzt daher eine Lösung.

Beweis: Falls es eine Lösung x gibt, dann existiert ein $k \in \mathbb{Z}$, so dass $ax = b + kn$. Also teilt $d = \mathrm{ggT}(a, n)$ die Zahl $b = ax - kn$.

Sei also b durch d teilbar. Sei x eine Lösung der Gleichung $ax \equiv b \bmod n$. Es gibt daher ein $k \in \mathbb{Z}$ mit $ax = b + kn$, und wir folgern weiter:

$$\begin{aligned}
yax &= yb + ykn \\
d - zn\,x &= yb + ykn \\
dx &= yb + zx + yk\,n \\
x &= y\tfrac{b}{d} + zx + yk\,\tfrac{n}{d} \\
x &\equiv y\tfrac{b}{d} \mod \tfrac{n}{d}
\end{aligned}$$

Die Rechnung lässt sich leicht umkehren. Aus $x \quad y\frac{b}{d} \bmod \frac{n}{d}$ erhält man die Existenz eines $k \quad$ mit $x \quad y\frac{b}{d} \quad k\frac{n}{d}$ und weiter

$$\begin{aligned} ax \quad & ay\tfrac{b}{d} \quad ak\tfrac{n}{d} \quad d \quad zn \ \tfrac{b}{d} \quad ak\tfrac{n}{d} \\ ax \quad & b \quad z\tfrac{b}{d} \quad \tfrac{a}{d}k \ n \\ ax \quad & b \mod n \end{aligned}$$

Beispiel In der chromatischen Tonleiter besteht eine Oktave aus zwölf Halbtonschritten. Eine Quinte bedeutet 7 Stufen. Wie viele Quinten muss man auf einem Klavier greifen, um von einem C zu einem Fis zu kommen? Ein Fis liegt 6 Halbtonschritte über dem C. Die zu lösende Gleichung lautet also $7x \quad 6 \bmod 12$. Aus dem euklidischen Algorithmus bekommen wir $5 \quad 7 \quad 3 \ 12 \quad 1$. Also ist die obige Kongruenzgleichung äquivalent zu $x \quad 5 \quad 6 \quad 30 \quad 6 \bmod 12$. Man braucht daher $6 \quad 12k, k \quad$, Quinten.

Aufgabe 4.9 Lösen Sie $30x \quad 1 \bmod 101$.

Korollar 4.10 *Seien $a \ b \quad$ und $m \ n \quad$, dann gilt*

$$ma \quad mb \bmod n \quad und \quad \text{ggT} \ n \ m \quad 1 \qquad a \quad b \bmod n$$

Beweis: Aus $ma \quad mb \bmod n$ folgt $m \ a \quad b \quad 0 \bmod n$. Der Satz impliziert nun die Kongruenz $a \quad b \quad 0 \bmod n$.

Wir wollen nun zwei lineare Kongruenzen gleichzeitig lösen:

$$cx \quad a \mod n \quad \text{und} \quad dx \quad b \mod m$$

Wegen des obigen Satzes dürfen wir ohne Einschränkungen $c \quad d \quad 1$ annehmen.

Satz 4.11 (Chinesischer Restsatz, 1. Version) *Gegeben seien $a \ b \quad$ und $n \ m \quad$. Sei d $\text{ggT} \ n \ m$ und $y \ z \quad$, so dass $yn \quad zm \quad d$. Die simultanen Kongruenzen*

$$x \quad a \mod n \quad und \quad x \quad b \mod m$$

sind genau dann lösbar, wenn $a \quad b \bmod d$. In diesem Fall ist die simultane Kongruenz äquivalent zu der einfachen Kongruenz

$$x \quad a \quad yn\tfrac{a \quad b}{d} \mod \tfrac{mn}{d}$$

Beweis: Falls eine Lösung x existiert, ist $x \quad a \bmod d$ und $x \quad b \bmod d$ nach Lemma 4.7, also $a \quad b \bmod d$.

Falls $x \quad a \quad yn\frac{a \quad b}{d} \bmod \frac{mn}{d}$ folgt sofort $x \quad a \bmod n$. Mit $yn \quad d \quad zm$ folgt auch

$$x \quad a \quad d \quad zm \ \tfrac{a \quad b}{d} \quad a \quad a \quad b \quad b \mod m$$

Wir wollen hier noch andeuten, wie man an diese Formel kommt, noch klarer wird das durch den Beweis von Satz 5.5 werden. Wir multiplizieren die Gleichung $yn \quad zm \quad d$ mit $a \quad b \quad d$, um

$$\tfrac{a \quad b}{d} yn \quad \tfrac{a \quad b}{d} zm \quad a \quad b$$

zu erhalten. Aus der umgestellten Gleichung

$$x : \quad a \quad \tfrac{a \quad b}{d} yn \quad b \quad \tfrac{a \quad b}{d} zm$$

sieht man sofort, dass x gerade a mod n und b mod m ist.

Um zu zeigen, dass wir alle Lösungen der simultanen Kongruenz haben, betrachten wir eine weitere Lösung x'. Dann gilt

$$x \quad x' \quad a \quad a \quad 0 \mod n \quad \text{und} \quad x \quad x' \quad b \quad b \quad 0 \mod m$$

d.h. $n \; x \quad x'$ und $m \; x \quad x'$. Nach Definition gilt damit auch kgV $n \; m \; x \quad x'$. Mit kgV $n \; m$ $nm \; d$ (Satz 3.13) folgt $x \quad x' \mod nm \; d$, und wir sehen, dass wir bereits alle Lösungen kennen.

Beispiel Die Mondphasen haben eine Periode von 29 Tagen. Angenommen heute ist Sonntag und Neumond. In wie vielen Tagen fällt Vollmond auf einen Dienstag? Nummerieren wir die Wochentage bei Sonntag mit 0 beginnend, so erhalten wir die folgenden Kongruenzgleichungen

$$x \quad 2 \mod 7 \quad \text{und} \quad x \quad 15 \mod 29$$

Da $4 \quad 7 \quad 1 \; 29 \quad 1$, sind die simultanen Kongruenzen äquivalent zu $x \quad 2 \quad 4 \quad 7 \quad 2$ $15 \quad 1 \mod 7 \; 29$, d.h. $x \quad 362 \quad 44 \mod 203$. Also muss man $44 \quad 203k$ Tage auf einen Vollmond am Dienstag warten, wobei $k \quad _0$.

Korollar 4.12 *Die Lösungsmenge der simultanen Kongruenzen*

$$a_i x \quad b_i \mod n_i \quad \textit{für } i \quad 1 \quad m$$

ist berechenbar.

Beweis: Nach Satz 4.8 können wir ohne Einschränkung $a_i \quad 1$ annehmen. Mit dem vorangehenden Satz können wir jeweils zwei Kongruenzen zusammenfassen. Wir wiederholen das, bis nur noch eine Kongruenz übrig bleibt.

Beispiel (Sun Tsu, 400 AD) Man löse

$$x \quad 2 \mod 3 \quad x \quad 3 \mod 5 \quad \text{und} \quad x \quad 2 \mod 7$$

Wir fassen die ersten beiden Gleichungen mit Hilfe des Satzes zusammen. Es gilt $2 \; 3 \quad 1 \; 5$ 1. Daher sind die ersten beiden Kongruenzen äquivalent zu $x \quad 2 \quad 2 \; 3 \quad 2 \quad 3 \quad 1 \mod 3 \; 5$, d.h. $x \quad 8 \mod 15$. Jetzt fassen wir diese Kongruenz mit $x \quad 2 \mod 7$ zusammen. In diesem Fall ist $1 \; 15 \quad 2 \; 7 \quad 1$. Also ist die simultane Kongruenz äquivalent zu $x \quad 8 \quad 1 \; 15 \quad 8$ $2 \quad 1 \mod 7 \; 15$, d.h. $x \quad 82 \quad 23 \mod 105$.

Zusatzaufgaben

Aufgabe 4.13 Finden Sie eine Formel für die Lösung von mehreren simultanen Kongruenzen analog zu Satz 4.11.

Aufgabe 4.14 Berechnen Sie den eindeutig bestimmten Repräsentanten zwischen 0 und 16 der Kongruenzklasse $3^{3^{100}} \bmod 17$.

Aufgabe 4.15 Bestimmen Sie die letzte Dezimalstelle der Zahlen n^{67839} für $n \quad 7$ und $n \quad 2$.

Aufgabe 4.16 Lösen Sie die folgenden (simultanen) Kongruenzen:

1. $5x \quad 7 \bmod 13$.
2. $6x \quad 14 \bmod 20$.
3. $x \quad 2 \bmod 5 \quad x \quad 7 \bmod 14$ und $x \quad 5 \bmod 18$
4. $2x \quad 7 \bmod 13$ und $5x \quad 12 \bmod 17$.

Aufgabe 4.17 Alice schuldet Bob 210 Euro und Carlo 125 Euro. Alle drei besitzen nur Geldscheine zu 12 oder 30 Euro. Kann Alice ihre Schulden einem oder beiden abbezahlen? Wenn ja, wie?

Aufgabe 4.18 Ein Bienenvolk hat zwischen 200 und 250 Mitglieder. Stellt man sie in 7er Reihen auf, so bleibt eine Biene alleine. Stellt man sie dagegen in 5er Reihen auf, so bleiben drei übrig. Wie viele Bienen sind es genau ?

Aufgabe 4.19 Eine Spielzeugbaukasten enthält etwa 400 bis 500 Bauklötze. Stellt man sie in 13er–Reihen auf, so bleiben 2 übrig. Stellt man sie dagegen in 17er–Reihen auf, so bleiben 11 übrig. Stellen Sie ein geeignetes System von linearen Kongruenzen auf und lösen Sie es, um die wirkliche Anzahl von Bauklötzen zu ermitteln.

Aufgabe 4.20 Sei n eine natürliche Zahl und p eine ungerade Primzahl. Es gelte $2^n \quad 1 \bmod p$ und $2^n \quad 1 \bmod p^2$. Dann ist $2^d \quad 1 \bmod p^2$, wobei d die Ordnung von 2 modulo p ist.

Aufgabe 4.21 (Sophie Germain) Sei p eine Primzahl, so dass auch $2p \quad 1 \quad q \quad 3$ prim ist. Dann hat die Fermatgleichung $x^p \quad y^p \quad z^p \quad 0$ keine Lösung mit $x \; y \; z \quad 0 \bmod p$.

5 Die Ringe n

In diesem Abschnitt wollen wir die Ergebnisse des letzten abstrahieren und vertiefen. Wir starten mit der folgenden offensichtlichen Bemerkung.

Lemma 5.1 *Kongruenz mod n ist eine Äquivalenzrelation auf den ganzen Zahlen, d.h. für alle a b c gilt:*

1. $a \quad a \bmod n.$
2. $a \quad b \bmod n \qquad b \quad a \bmod n.$
3. $a \quad b \bmod n$ *und* $b \quad c \bmod n \qquad a \quad c \bmod n.$

Bei Äquivalenzrelationen betrachtet man immer auch die Äquivalenzklassen. Hier heißen sie Restklassen mod n und sind konkret definiert durch

$$\overline{a}: \quad a \quad n \quad : \quad \{a \quad kn \quad k \qquad \text{für } a$$

Dabei heißt a der Repräsentant der Restklasse $\overline{a}$. Man beachte, dass in der Oberstrichschreibweise das n nicht erscheint und aus dem Zusammenhang erschlossen werden muss. Es gilt $b \quad \overline{a} \qquad \overline{a} \quad \overline{b}$.

Definition 5.2 *Die Menge der* Restklassen mod n *wird mit* $\quad n \quad : \quad \{a \quad n \quad a \qquad$ *bezeichnet.*

In Augenblick mag n noch als recht große Menge erscheinen, dies ist aber nicht der Fall. Am besten versteht man n über ein *vollständiges Repräsentantensystem*, d.h. eine Menge $R \qquad$ mit $\quad n \quad \{r \quad n \quad r \quad R$, so dass zwei $r_1 \; r_2 \quad R$ mit $r_1 \quad r_2$ verschiedene Restklassen $r_1 \quad n \qquad r_2 \quad n$ haben.

Lemma 5.3 $R \quad \{0 \; 1 \qquad n \quad 1$ *ist ein Repräsentantensystem für* $\quad n$ *. Insbesondere besteht* $\quad n \quad$ *aus n Elementen.*

Beweis: Sei $\overline{a} \qquad n$ eine beliebige Restklasse mod n. Dann gibt es nach Division von a durch n mit Rest $q \qquad , r \quad R$ mit $a \quad qn \quad r$, d.h. $a \quad r \bmod n$ und $\overline{a} \quad \overline{r}$.
Seien nun $r_1 \; r_2 \quad R$ mit $r_1 \quad r_2$. Wir müssen $\overline{r_1} \quad \overline{r_2}$ oder äquivalent dazu $r_1 \quad r_2 \bmod n$ zeigen. Dies ist aber klar.

Die ganzen Definitionen wären sinnlos, wenn n nicht eine zusätzliche Struktur trüge:

Satz 5.4 n *ist ein Ring bezüglich der Operationen*

$$\overline{a} \quad \overline{b}: \quad \overline{a \quad b} \quad \textit{und} \quad \overline{a} \; \overline{b}: \quad \overline{a \; b}$$

S. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie,*
DOI 10.1007/978-3-8348-8263-9_5,

Beweis: Die Wohldefiniertheit der Addition und der Multiplikation, d.h. die Unabhängigkeit von der Auswahl der Repräsentanten der Restklassen, ist gerade Satz 4.2. Die Ringgesetze von vererben sich auf n .

Beispiel Hier sind die Verknüpfungstafeln von 2 , 4 und 5 :

2 :

	0	1
0	0	1
1	1	0

	0	1
0	0	0
1	0	1

4 :

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

5 :

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Es gibt natürliche Ringhomomorphismen

$$n \quad x \quad x \quad n$$

$$n \quad m \quad x \quad n \quad x \quad m \quad \text{für } m \; n$$

Die Wohldefiniertheit des letzteren folgt aus dem Lemma 4.7.

Satz 5.5 (Chinesischer Restsatz, 2. Version) *Seien m n zwei teilerfremde Zahlen, dann ist der natürliche Ringhomomorphismus*

$$\Phi : \quad nm \qquad n \quad m$$

$$x \quad nm \qquad x \quad n \quad x \quad m$$

ein Isomorphismus.

Beweis: Da wir bereits bemerkt haben, dass Φ tatsächlich ein Ringhomomorphismus ist, bleibt zu zeigen, dass Φ bijektiv ist. Sprich, zu gegebenen $\overline{a}$ $\overline{b}$ n m muss es ein eindeutig bestimmtes $\overline{x}$ nm geben mit x $a \bmod n$ und x $b \bmod m$. Dies sagt gerade die erste Version des chinesischen Restsatzes 4.11.

Da der Isomorphismus für uns so wichtig ist, wollen wir noch das Inverse von Φ direkt berechnen. Wegen ggT $n \; m$ 1 gibt es nach dem euklidischen Algorithmus $x \; y$ mit $xn \quad ym$ 1. Dann ist

$$\Phi \; \overline{1 \quad xn} \qquad \overline{1 \quad xn} \; \overline{1 \quad xn} \qquad \overline{1} \; \overline{ym} \qquad \overline{1} \; \overline{0}$$

$$\Phi \; \overline{1 \quad ym} \qquad \overline{1 \quad ym} \; \overline{1 \quad ym} \qquad \overline{nx} \; \overline{1} \qquad \overline{0} \; \overline{1}$$

Somit gilt nach Linearität $\Phi\ \overline{a\ 1\quad xn\quad b\ 1\quad ym}\qquad \overline{a}\ \overline{b}$ und daher

$$\Phi\ ^{1}\ \overline{a}\ \overline{b}\qquad \overline{a\ 1\quad xn\quad b\ 1\quad ym}$$

Aufgabe 5.6 Berechnen Sie den Isomorphismus aus Satz 5.5 explizit für die Zahlen $n\quad 13$ und $m\quad 17$.

Aufgabe 5.7 Zeigen Sie, dass auch die Umkehrung des chinesischen Restsatzes gilt: Ist der natürliche Ringhomomorphismus Φ ein Isomorphismus, so gilt ggT $n\ m\quad 1$.

Korollar 5.8 *Seien* $n_1\ n_2\quad n_s\quad$ *paarweise teilerfremde Zahlen, dann gilt*

$$n_1n_2\quad n_s\qquad n_1\qquad n_2\qquad\qquad n_s$$

Beweis: Das Korollar folgt aus dem Satz durch Induktion mit der Klammerung $n_1n_2\quad n_s$ $n_1\ n_2\quad n_s$.

An vielen Stellen in der Mathematik spielen die Einheiten des Ringes n eine wichtige Rolle. Sie erhalten daher eine Standardbezeichnung, und wir werden sie hier und im übernächsten Abschnitt genauer untersuchen.

Definition 5.9 *Die* Einheitengruppe *von* n *wird mit* $U_n\qquad n\quad$ *bezeichnet.*

Satz 5.10

$$U_n\quad \{a\quad n\quad \text{ggT}\ a\ n\quad 1$$

Beweis: $\overline{a}\qquad n$ ist genau dann eine Einheit, falls es ein $\overline{x}\qquad n$ gibt mit $\overline{x}\overline{a}\quad 1$, also die Gleichung $ax\quad 1 \bmod n$ lösbar ist. Dies ist nach Satz 4.8 gerade dann möglich, wenn ggT $a\ n\quad 1$.

Aufgabe 5.11 Berechnen Sie U_n für $2\quad n\quad 15$.

Definition 5.12 *Die* Eulersche φ–Funktion *ist definiert durch*

$$\varphi :\qquad n\qquad \#U_n$$

Wir wollen eine einfache Formel für φ finden.

Lemma 5.13 *Seien* $n\ m\quad$ *zwei teilerfremde Zahlen, dann gilt*

$$U_{nm}\quad U_n\quad U_m\qquad \textit{und}\qquad \varphi\ nm\quad \varphi\ n\quad \varphi\ m$$

Beweis: $nm\qquad n\qquad m\qquad n\qquad m$.

Eine Funktion $\varphi :\qquad$ mit der Eigenschaft $\varphi\ nm\quad \varphi\ n\quad \varphi\ m$ für teilerfremde $n\ m$ wird *multiplikative zahlentheoretische Funktion* genannt.

Lemma 5.14 *Sei p prim und r , dann ist*

$$\varphi\ p^r \quad p^{r\ 1}\ p \quad 1$$

Beweis: Nach Satz 5.10 ist

$$U_{p^r} \quad \{a \quad p^r \quad \text{ggT}\ a\ p^r \quad 1 \quad \{a \quad p^r \quad p \quad a$$

Wir können uns bei der Berechnung von $\#U_{p^r}$ auf die Betrachtung des vollständigen Repräsentantensystems 0 1 p^r 1 von p^r beschränken, damit ist

$$\#U_{p^r} \quad \#\{a \quad \{0 \quad p^r \quad 1 \quad p \quad a \quad p^r \quad \#\{a \quad \{0 \quad p^r \quad 1 \quad p\ a$$

Wegen $p\ a$ gilt $a \quad pb$ für ein passendes $b \quad . 0 \quad a \quad p^r \quad 1$ ist äquivalent zu $0 \quad b \quad p^r \quad 1 \quad p \quad p^{r\ 1} \quad 1$, und daher haben wir $p^{r\ 1}$ Wahlmöglichkeiten für b bzw. a. Insgesamt folgern wir $\varphi\ p^r \quad \#U_{p^r} \quad p^r \quad p^{r\ 1} \quad p^{r\ 1}\ p \quad 1$.

Satz 5.15 *Sei* $n \quad \prod_{i\ 1}^{s} p_i^{r_i}$ *die Primfaktorzerlegung einer natürlichen Zahl, dann ist*

$$\varphi\ n \quad \prod_{i\ 1}^{s} p_i^{r_i\ 1}\ p_i \quad 1$$

Beweis: Nach den beiden Lemmata ist

$$\varphi\ n \quad \prod_{i\ 1}^{s} \varphi\ p_i^{r_i} \quad \prod_{i\ 1}^{s} p_i^{r_i\ 1}\ p_i \quad 1$$

Aufgabe 5.16 Beweisen Sie: $n \quad \sum_{d\ n} \varphi\ d$.

Damit können wir den kleinen Satz von Fermat (Satz 4.5) verallgemeinern:

Satz 5.17 (Euler) *Sei n und a teilerfremd zu n. Dann ist*

$$a^{\varphi\ n} \quad 1 \mod n$$

Beweis: Dies folgt aus dem Satz von Lagrange (siehe Anhang A.9): Ist G eine endliche Gruppe der Ordnung l, so erfüllt jedes Element $g \quad G$ die Gleichung $g^l \quad 1$. Wir wenden das hier auf die Gruppe U_n an.

Die Struktur von n und U_n wird heute in der *Kryptographie* benutzt, wie man in den folgenden zwei Beispielen sieht. Die erste Methode von Diffie und Hellman dient zum Austausch eines Schlüssels, den man dann zur weiteren sicheren Verschlüsselung benutzen kann:

Beispiel *Das Diffie–Hellman Schlüsselaustausch Protokoll (1976)*: Max und Sebastian wollen ein Geheimnis austauschen. Sie vereinbaren eine Primzahl p und eine natürliche Zahl g, die Ordnung $p \quad 1$ modulo p hat. Max und Sebastian merken sich jeweils individuell eine

weitere geheime natürliche Zufallszahl m bzw. n. Dann berechnet Max $g^m \bmod p$ und sendet die Information an Sebastian. Der berechnet $s \quad g^{m\ n} \quad g^{mn} \bmod p$. Dieses s wird *geheimer Schlüssel* genannt. Sebastian sendet nun ebenfalls $g^n \bmod p$ an Max und der berechnet ebenfalls $s \quad g^{n\ m} \quad g^{mn} \bmod p$. Mit diesem Schlüssel s kann man nun z.B. geheime Botschaften austauschen.

Ein möglicher Spion von außen kann die Werte von g^m und g^n sehen, aber daraus nicht $s \quad g^{mn}$ berechnen, weil er auch m und n nicht kennt. Übrigens kennen nicht mal Max und Sebastian die Werte von m und n, die der jeweils andere gewählt hat.

Die Sicherheit dieses Verfahren beruht auf dem *Diskreten Logarithmusproblem:* Gegeben g und g^n modulo p, dann berechne $n \quad \log_g g^n$. Dieses Problem gilt als sehr schwer in den Gruppen $\quad p \quad$, falls p eine große Primzahl ist. Die Potenzfunktion $g \quad g^n$ ist eine sogenannte *Einwegfunktion*, d.h. man kann sie relativ leicht berechnen, aber ihre Umkehrfunktion nur sehr schwer.

Das zweite Beispiel ist das RSA–Verfahren aus der Public–Key Kryptographie:

Beispiel Benannt nach Rivest/Shamir/Adleman ist *RSA*, ein *Public–Key Kryptosystem*. Max und Sebastian wollen wieder Geheimnisse austauschen. Max bestimmt zunächst eine *Einwegfunktion*:

1. Max bestimmt zwei große Primzahlen p und q und berechnet $n \quad pq$.
2. Er berechnet leicht $\varphi\ n \quad p \quad 1 \quad q \quad 1$.
3. Max wählt eine zufällige Zahl $e \quad$ mit $1 \quad e \quad \varphi\ n$ und ggT $e\ \varphi\ n \quad 1$.
4. Max berechnet jetzt eine Lösung d der Gleichung

$$ed \quad 1 \mod \varphi\ n$$

   mit dem erweiterten euklidischen Algorithmus.

5. Die *Kodierungsfunktion* ist nun

$$E : \quad n \qquad n \quad x \quad x^e$$

Man beachte den Unterschied zwischen n und $\varphi\ n$. Wie funktioniert nun die Verschlüsselung? Der *öffentliche Schlüssel* ist das Paar $n\ e$, das öffentlich bekannt ist. Max ist aber der einzige, der d kennt, da er $\varphi\ n$ kennt. Alle anderen kennen die Faktorisierung von n nicht und damit $\varphi\ n$ und also d nicht. Wenn Sebastian eine Nachricht an Max schicken will, so schreibt er die Nachricht als eine Folge von Zahlen $m_1 \quad m_l \quad n$. Die verschlüsselte Nachricht ist $E\ m_1 \quad E\ m_l$. Max *entschlüsselt* die Nachricht, indem er die d–te Potenz berechnet:

$$E\ m_i^{\ d} \quad m_i^{e\ d} \quad m_i^{ed} \quad m_i \mod n$$

Dies folgt aus dem Satz von Euler, weil $ed \quad 1 \bmod \varphi\ n$ ist.

Das folgende konkrete Beispiel dient zur Illustration, die Zahlen sind natürlich viel zu klein, um in der Praxis dienlich zu sein. Sei $p \quad 17$ und $q \quad 19$, also $n \quad 323$. Dann ist $\varphi\ n \quad pq \quad p \quad q \quad 1 \quad 288$. Wähle zufällig $e \quad 95$. Dann berechne $d \quad 191$ mit dem erweiterten

euklidischen Algorithmus. Der öffentliche Schlüssel ist also $323\ 95$. Wir wollen $x \quad 24$ verschlüsseln. Man bekommt

$$E\ x \quad 24^{95} \quad 294 \quad \mathrm{mod}\ 323$$

Das Entschlüsseln erfolgt dann so:

$$E^{\ 1}\ 294 \quad 294^{191} \quad 24 \quad \mathrm{mod}\ 323$$

Ist $\varphi\ n$ bekannt, so kennt man auch eine Faktorisierung von n: Wegen $\varphi\ n \quad pq \quad p \quad q \quad 1 \quad n \quad p \quad q \quad 1$ sind die Koeffizienten des Polynoms

$$x \quad p\ x \quad q \quad x^2 \quad p \quad q\ x \quad pq$$

bekannt, also auch seine Nullstellen $p\ q$. Das RSA–Verfahren gilt als sicher, solange die Faktorisierung großer Zahlen ein schweres Problem ist.

Falls n eine Primzahl ist, ist die Struktur von $\quad n \quad$ besonders einfach.

Satz 5.18 *Sei $p \quad$ eine natürliche Zahl.*

$p \quad$ ist ein Körper genau dann, wenn p eine Primzahl ist.

Beweis: Falls p prim ist, gilt ggT $a\ p \quad 1$ für $p \quad a$. Daher ist nach Satz 5.10 $U_p \quad \{\overline{a} \quad p \quad a \quad \quad p \quad \{\overline{0}$. Da alle Elemente ungleich 0 Einheiten sind, ist $\quad p \quad$ ein Körper.

Falls p nicht prim ist, gibt es $a\ b \quad$ mit $p \quad ab$ und $a\ b \quad p$. Modulo p ist $\overline{a}\overline{b} \quad \overline{0}$, wobei $\overline{a}\ \overline{b} \quad \overline{0}$. $\overline{a}\ \overline{b}$ sind also Nullteiler und damit keine Einheiten, folglich kann auch $\quad p \quad$ kein Körper sein.

Definition 5.19 *Der Körper $\quad p \quad , p \quad \quad ,$ wird mit $\mathbb{F}_p$ bezeichnet.*

Beispiel In Körpern kann man durch beliebige Zahlen ungleich 0 dividieren, so ist zum Beispiel $\overline{1}\ \overline{2} \quad \overline{3}$ in $\mathbb{F}_5$.

Aufgabe 5.20 Berechnen Sie $\overline{3} \quad \overline{4}, \overline{3} \quad \overline{4}, \overline{3}\ \overline{4}$ und $\overline{3}\ \overline{4}$ in $\mathbb{F}_7$.

Warnung Es gibt auch die Körper $\mathbb{F}_{p^r}$ mit p^r Elementen für $r \quad 2$. Diese sind aber *nicht* isomorph zu den $\quad p^r \quad$, die ja nach obigem Satz gar keine Körper sind.

Satz 5.21 (Wilson) *Eine natürliche Zahl p ist eine Primzahl genau dann, wenn*

$$p \quad 1\ ! \quad \quad 1 \quad \mathrm{mod}\ p$$

Beweis: Wenn p nicht prim ist, ist $p = ab$ mit $1 < a, b < p$. Falls $a = b$, gilt offensichtlich $p \mid ab$, $p \mid (p-1)!$ und damit $p \mid (p-1)! + 1$. Für $p = 4$ ist $2^2 = 3! + 1 = 6 + 2 \bmod 4$. Es bleibt, $p = a^2$ mit $a > 2$ zu betrachten. Wegen $2a < p$ gilt $a < 2a < p - 1$, also $a \mid (p-1)!$. Es folgt $p \mid (p-1)! + 1$, also $(p-1)! + 1 \equiv 0 \bmod 2a^2$, insbesondere $(p-1)! + 1 \equiv 0 \bmod a^2$.

Sei nun p prim, dann rechnen wir in dem Körper $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. In einem Körper sind nur die Elemente 1 und -1 ihr eigenes Inverses, denn

$$x = x^{-1} \iff x^2 - 1 = 0 \iff x^2 - 1 = (x-1)(x+1) = 0.$$

In $\mathbb{F}_p$ gilt $1 = \overline{1}$ und $-1 = \overline{p-1}$. Also wird in dem Produkt $\overline{2} \cdot \overline{3} \cdots \overline{p-2}$ jedes Element mit seinem Inversen multipliziert, und es ist daher $\overline{1}$. Somit ist $(p-1)! = p - 1 = -1 \bmod p$.

Beispiel Für $p = 13$ ist die Paarung der Elemente mit ihrem Inversen wie folgt:

$$11! = 2 \cdot 7 \cdot 3 \cdot 9 \cdot 4 \cdot 10 \cdot 5 \cdot 8 \cdot 6 \cdot 11 = -1 \bmod 13$$

Zusatzaufgaben

Aufgabe 5.22 Zeigen Sie: n ist genau dann prim, wenn $n - 1 = \varphi(n)$.

Aufgabe 5.23 Beweisen Sie: $\varphi(n)$ ist gerade für $n > 3$.

Aufgabe 5.24 Zeigen Sie: $\varphi(n)$ ist eine Zweierpotenz genau dann, wenn n das Produkt einer Zweierpotenz mit paarweise verschiedenen Fermatschen Primzahlen ist.

Aufgabe 5.25 Sei $p > 3$ prim und a eine Einheit in $\mathbb{Z}/p\mathbb{Z}$. Hat a die Ordnung 3, so hat $a - 1$ die Ordnung 6.

Aufgabe 5.26 Seien $p = 11$, $q = 13$ und $n = pq = 143$ ihr Produkt. Bestimmen Sie $\varphi(n)$ und finden Sie ein $e > 1$ mit $\mathrm{ggT}(e, \varphi(n)) = 1$. Dann bestimmen Sie d mit $ed \equiv 1 \bmod \varphi(n)$. Kodieren Sie daraufhin $x = 17$ unter der Einwegfunktion $E(x) = x^e$.

Aufgabe 5.27 Sei p eine Primzahl mit $p \equiv 1 \bmod 4$. Zeigen Sie, dass $a = \left(\frac{p-1}{2}\right)!$ die Gleichung $a^2 \equiv -1 \bmod p$ erfüllt. Benutzen Sie das Gezeigte, um die Gleichung $x^2 \equiv -1$ für $p = 5, 13, 17, 29$ zu lösen.

Aufgabe 5.28 Eine *exakte Sequenz abelscher Gruppen* ist ein Diagramm bestehend aus abelschen Gruppen und Homomorphismen der Form

$$0 \xrightarrow{\varphi_0} A_0 \xrightarrow{\varphi_1} A_1 \xrightarrow{\varphi_1} \cdots \xrightarrow{\varphi_n} A_n \xrightarrow{\varphi_{n-1}} 0$$

derart, dass $\mathrm{Im}\,\varphi_{k-1} = \mathrm{Ker}\,\varphi_k$ für $1 < k < n - 1$ gilt. Seien nun n, m beliebige natürliche Zahlen und $\varphi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ der kanonische Homomorphismus. Zeigen Sie, dass eine exakte Sequenz der Gestalt

$$0 \to \mathrm{kgV}(n, m)\,\mathbb{Z}/nm\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathrm{ggT}(n, m)\,\mathbb{Z}/nm\mathbb{Z} \to 0$$

existiert und geben Sie die fehlenden Homomorphismen explizit an.

Aufgabe 5.29 Zeigen Sie, dass $\tau(n) = \sum_{d|n} 1$ und $\sigma(n) = \sum_{d|n} d$ multiplikative zahlentheoretische Funktionen sind.

Aufgabe 5.30 Zeigen Sie: Sind f g multiplikative zahlentheoretische Funktionen, so auch die Faltung $f * g$ mit $(f * g)(n) = \sum_{d|n} f(d)\, g\left(\frac{n}{d}\right)$.

Aufgabe 5.31 Zeigen Sie: Die Funktion $\mu(n)$ mit $\mu(1) = 1$, $\mu(n) = 0$ für n nicht quadratfrei und $\mu(n) = (-1)^k$ für n quadratfrei mit k verschiedenen Primfaktoren, ist eine multiplikative zahlentheoretische Funktion.

Aufgabe 5.32 Zeigen Sie: Sei g eine multiplikative zahlentheoretische Funktion und $f = g * \mu$ mit μ aus Aufgabe 5.31. Dann ist $g(n) = \sum_{d|n} f(d)$.

6 Endlich erzeugte abelsche Gruppen

In den letzten Abschnitten haben wir die Ringe und n kennengelernt, in diesem Abschnitt betrachten wir nur noch ihre additive Gruppenstruktur. Ziel des Abschnittes ist es zu zeigen, dass jede endlich erzeugte abelsche Gruppe ein direktes Produkt aus diesen Gruppen ist. Starten wir mit einigen Definitionen.

Definition 6.1 *Sei G eine Gruppe.*

Für S G bezeichnet S die von S erzeugte Untergruppe, d.h. die kleinste Untergruppe von G, die S enthält. Die Elemente von S heißen Erzeuger von S .

G heißt zyklisch*, falls G von einem einzigen Element erzeugt werden kann, d.h. G g für ein g G.*

G heißt endlich erzeugt*, wenn G von endlich vielen Elementen erzeugt werden kann.*

Im Allgemeinen ist es schwierig zu verstehen, wie die von S erzeugte Untergruppe von G aussieht, jedoch im Fall von abelschen Gruppen ist es recht einfach. Das liegt daran, dass abelsche Gruppen die Struktur eines –Moduls tragen. Schreiben wir die Verknüpfung einer abelschen Gruppe mit , dann definieren wir für g G und n :

$$\begin{aligned} 0 \quad g &: \quad 0 \\ n \quad g &: \quad \underbrace{g \quad \cdots \quad g}_{n \text{ mal}} \\ n \quad g &: \quad n \quad g \end{aligned}$$

Aufgabe 6.2 Zeigen Sie, dass jede abelsche Gruppe G mit dieser Verknüpfung zu einem –Modul wird.

Lemma 6.3 *Sei G eine abelsche Gruppe und S G. Dann gilt*

$$S \quad \sum_{g \ S} n_g g \quad S' \quad S \text{ endlich } n_g$$

Beweis: Bezeichnen wir die rechte Menge mit H. Wir zeigen zuerst, dass S H gilt. Per Definition ist S S . Da eine Untergruppe abgeschlossen bezüglich Addition und Inversenbildung ist, muss neben einem g S auch ng S für n sein. Aus dem gleichen Grund muss S auch endliche Summen $\sum_{g \ S} n_g g$, S' S endlich, enthalten. Daher ist H S .

S. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie,*
DOI 10.1007/978-3-8348-8263-9_6,

Da S die kleinste Gruppe ist, die S enthält, können wir den Beweis abschließen, indem wir beweisen, dass H eine Untergruppe ist. Dazu reicht es die Abgeschlossenheit von H bezüglich der Addition und Inversenbildung zu zeigen. Seien $h_1 \quad \sum_{g \ S} n_g g$ und $h_2 \quad \sum_{g \ S} m_g g$ mit endlichen $S' \ S'' \quad S$ zwei beliebige Elemente aus H. Wir setzen $n_g \quad 0$ für $g \quad S'' \quad S'$ und $m_g \quad 0$ für $g \quad S' \quad S''$. Dann ist

$$h_1 \quad h_2 \quad \sum_{g \ S \ S} n_g g \quad \sum_{g \ S \ S} m_g g \quad \sum_{g \ S \ S} n_g \quad m_g \ g$$

$$h_1 \quad \sum_{g \ S} n_g g \quad \sum_{g \ S} n_g \ g$$

Aufgabe 6.4 Sei G eine beliebige Gruppe, deren Verknüpfung wir multiplikativ schreiben. Zeigen Sie, dass für ein g G gilt: $g \quad \{g^n \quad n \quad .$

Lemma 6.5 *Jede zyklische Gruppe ist abelsch.*

Beweis: Da wir a priori noch nicht wissen, dass eine zyklische Gruppe G abelsch ist, schreiben wir die Verknüpfung in G multiplikativ. Nach der vorangegangenen Aufgabe ist $G \quad \{g^n \quad n \quad .$ Da offensichtlich $g^n g^m \quad g^{n \ m} \quad g^m g^n$ gilt, ist G abelsch.

Beispiele Die Gruppen und n sind zyklische Gruppen mit Erzeuger 1 bzw. $\overline{1}$.

Satz 6.6 *Jede zyklische Gruppe ist isomorph zu oder n für ein n .*

Beweis: Sei G eine zyklische Gruppe mit Erzeuger g. Per Definition ist der Gruppenhomomorphismus

$$\Phi : \quad G \quad m \quad mg$$

surjektiv. Sein Kern, $\mathrm{Ker}\,\Phi$, ist eine Untergruppe von , tatsächlich aber sogar ein – Untermodul von wegen der –Modulstruktur von abelschen Gruppen. Da $\mathrm{Ker}\,\Phi$, muss er sogar ein Ideal sein. Nach Satz 2.9 ist ein Hauptidealring, also existiert ein n mit $\mathrm{Ker}\,\Phi \quad n$. Falls $n \quad 0$ ($\mathrm{Ker}\,\Phi \quad 0$), dann ist Φ ein Isomorphismus, d.h. G . Für $n \quad 1$ ist schließlich nach dem Homomorphiesatz $G \quad n$.

Bemerkung 6.7 *Sei G eine endliche zyklische Gruppe. Ein Element $g \quad G$ erzeugt G genau dann, wenn* $\mathrm{ord}\, g \quad \mathrm{ord}\, G$.

Beweis: Per Definition ist $n : \quad \mathrm{ord}\, g$ die kleinste natürliche Zahl mit $ng \quad 0$. Es folgt $m \quad kn \ g \quad mg$ für alle k . Daher ist

$$g \quad \{mg \quad m \quad \{mg \quad m \quad \{0 \quad n \quad 1$$

Die in der letzten Menge aufgezählten Elemente sind alle paarweise verschieden. Nämlich, falls $mg \quad m'g$ für $0 \quad m' \quad m \quad n \quad 1$, dann ist $m \quad m' \ g \quad 0$ mit $m \quad m' \quad n$ — im Widerspruch zur Minimalität von n mit dieser Eigenschaft.

Wegen $g \quad G$ ist $g \quad G$ äquivalent zu $n \quad \mathrm{ord} \ g \quad \mathrm{ord}\, G$.

Wenden wir uns nun den endlich erzeugten abelschen Gruppen zu. Sei G eine solche. Um mit G arbeiten zu können, benutzen wir eine *Darstellung* von G (als –Modul). Seien dazu $g_1 \quad g_k$ Erzeuger von G, wir schreiben sie als k–Tupel $S \quad g_1 \quad g_k$ und betrachten den surjektiven Homomorphismus

$$\varphi_S : \quad ^k \quad G \quad m_1 \quad m_k \quad \sum_{i \quad 1}^{k} m_i g_i$$

Elemente des Kerns von φ_S werden *Relationen* der Erzeuger S genannt. Wir werden gleich in Lemma 6.8 zeigen, dass auch der Kern von φ_S endlich erzeugt ist. Wir wählen Erzeuger $r_1 \quad r_l$ davon und schreiben sie als Spalten in eine Matrix R. Diese repräsentiert eine Abbildung $R : \quad ^l \quad ^k$, und man bezeichnet

$$^l \; R \quad ^k \; S \; G$$

als eine *Präsentation* oder *Darstellung* der Gruppe G. Nach dem Homomorphiesatz gilt $G \quad ^k \; \mathrm{Ker}\,\varphi_S \quad ^k \; \mathrm{Im}\,R$. Wir können also den Isomorphietyp von G an der Matrix R allein ablesen!

Beispiel Bereits im Beweis von Satz 6.6 haben wir implizit die Darstellungen

$$0 \quad ^1 \quad \text{und} \quad ^n \quad \overline{1} \quad n$$

der zyklischen Gruppen gefunden.

Beispiele Diese Präsentationen sind nicht eindeutig, und manchmal ist es schwierig, den Isomorphietyp der Gruppe aus der Matrix direkt abzulesen. Wir betrachten als Beispiel drei verschiedene Präsentationen von $2 \quad 2$:

$$2 \xrightarrow{\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}} 2 \qquad 2 \xrightarrow{\overline{1}\,0 \quad 0\,\overline{1}} 2 \quad 2$$

$$3 \xrightarrow{\begin{smallmatrix} 2 & 0 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{smallmatrix}} 3 \qquad 3 \xrightarrow{\overline{1}\,0 \quad 0\,\overline{1} \quad \overline{1}\,\overline{1}} 2 \quad 2$$

$$2 \xrightarrow{\begin{smallmatrix} 4 & 2 \\ 2 & 2 \end{smallmatrix}} 2 \qquad 2 \xrightarrow{\overline{1}\,0 \quad \overline{1}\,\overline{1}} 2 \quad 2$$

Lemma 6.8 *Jede Untergruppe von* ^{k} *ist endlich erzeugt.*

Beweis: Sei $H \quad ^k$ eine Untergruppe. Wir führen eine Induktion nach k. Der Fall $k \quad 0$ ist trivial. Für $k \quad 0$ betrachten wir die Projektion $\pi : \quad ^k \quad$ auf den letzten Faktor. $\pi \; H$ ist eine Untergruppe von und damit auch ein Ideal von . Da ein Hauptidealring ist, gilt $\pi \; H$ n für ein $n \quad$. Sei $g \quad \pi \; ^1 \; n \quad H$ und $H' \quad H \quad ^{k \; 1} \quad 0$. Nach Induktionsvoraussetzung ist H' endlich erzeugt.

Wir behaupten, dass g zusammen mit den Erzeugern von H' die Untergruppe H erzeugt. Dafür reicht es zu zeigen, dass es für jedes $h \quad H$ ein $l \quad$ gibt mit $h \quad lg \quad H'$. Sei $m: \quad \pi\ h \quad \pi\ H \quad n$, d.h. $n\ m$. Setze $l: \quad m\ n$. Dann ist

$$\pi\ h \quad lg \quad \pi\ h \quad l\pi\ g \quad m \quad ln \quad 0$$

Also gilt $h \quad lg \quad \mathrm{Ker}\,\pi \quad H \quad H'$.

Nun überlegen wir uns, wie wir durch geschickte Wahl der Erzeuger von G und ihrer Relationen die Matrix R auf besonders einfache Form bringen können. Wir werden später sogar sehen, dass wir R bis auf Diagonalform bringen können.

Falls $g_1 \quad g_k \quad S$ Erzeuger von G sind, sind offensichtlich auch

$g_1 \quad g_i \quad \lambda g_j \quad g_k \quad$ für $\lambda \quad$ und $i \quad j$

$g_1 \quad g_i \quad g_k$

$g_{\pi\ 1} \quad g_{\pi\ 2} \quad g_{\pi\ k} \quad$ für eine Permutation $\pi \quad \mathrm{Perm}\ k$

Erzeuger von G. Diese Operationen nennen wir *Elementaroperationen*. Wir können die Elementaroperationen besser durch Rechtsmultiplikationen von Matrizen an den Zeilenvektor S beschreiben. Die *Elementarmatrizen* sind wie folgt definiert:

$E_{ij}\ \lambda \quad a_{\nu\mu} \quad$ mit $a_{ij} \quad \lambda$ und $a_{\nu\mu} \quad \delta_{\nu\mu}$ sonst.
Einheitsmatrix mit zusätzlichem λ auf einer Position $i\ j$ mit $i \quad j$

$E_i \quad b_{\nu\mu} \quad$ mit $b_{ii} \quad 1$ und $b_{\nu\mu} \quad \delta_{\nu\mu}$ sonst.
Einheitsmatrix, bei der das i–Diagonalelement gegen $\quad 1$ getauscht wurde.

$P\ \pi \quad b_{\nu\mu} \quad$ mit $b_{\nu\mu} \quad \delta_{\pi\ \nu\ \mu}$
Matrix, bei der in der ν–ten Zeile an der $\pi\ \nu$ –ten Stelle eine 1 steht und sonst nur Nullen.

Wir sehen, dass $E_{ij}\ \lambda \quad ^{1} \quad E_{ij} \quad \lambda$, $E_i \quad ^{1} \quad E_i$ und $P\ \pi \quad ^{1} \quad P\ \pi \quad ^{1}$. Zusammen erzeugen diese Matrizen die Gruppe

$$\mathrm{GL}\ k \quad \{M \quad \mathrm{GL}\ k\ \mathbb{Q} \quad M\ M \quad ^{1} \quad \mathrm{Mat}\ k$$

dies werden wir aber nicht weiter benutzen.

Aufgabe 6.9 Beweisen Sie: Für jede Matrix $M \quad \mathrm{GL}\ k \quad$ gilt $\det M \quad 1$.

Aufgabe 6.10 Zeigen Sie, dass $\mathrm{GL}\ k \quad \mathrm{GL}\ k\ \mathbb{Q} \quad \mathrm{Mat}\ k \quad$.

Die obigen drei Elementaroperationen entsprechen Rechtsmultiplikationen von S mit $E_{ji}\ \lambda$, E_i und $P\ \pi \quad ^{1}$. Wenn wir von den Erzeugern S mit der Elementarmatrix E zu den Erzeugern SE wechseln, müssen wir von den Relationen r_i zu den Relationen $E \quad ^{1}r_i$ übergehen, also von R nach $E \quad ^{1}R$, d.h. aus der Darstellung $^{l\ R} \quad ^{k\ S}\ G$ wird die Darstellung $^{l\ E\ ^{1}R} \quad ^{k\ SE}\ G$. Analog zum Erzeugerwechsel für S können wir die Erzeuger von $\mathrm{Ker}\,\varphi_S$ wechseln. Dies entspricht der Rechtsmultiplikation der Relationenmatrix R mit einer Elementarmatrix. Zusammenfassend gilt:

Lemma 6.11 *Sei* $^{l}R^{k}S$ *G eine Darstellung einer endlich erzeugten abelschen Gruppe G. Falls E und E' zwei Elementarmatrizen der Größe k bzw. l sind, dann ist auch*

$$l \xrightarrow{ERE} k \xrightarrow{SE^{-1}} G$$

eine Darstellung von G.

Da der Isomorphietyp von G von der Relationenmatrix R allein bestimmt wird, werden wir jetzt einen Algorithmus vorstellen, der aus R durch Links– und Rechtsmultiplikationen mit Elementarmatrizen eine Diagonalmatrix macht, d.h. eine Matrix von dem Typ

$$R \quad \left(\begin{array}{ccc|c} n_1 & & 0 & 0 \\ & \ddots & & \vdots \\ 0 & & n_r & 0 \\ \hline 0 & & 0 & 0 \end{array}\right)$$

Da die Matrix R nicht notwendig symmetrisch ist, kann die Anzahl der Nullzeilen von der Anzahl der Nullspalten abweichen.

Diagonalisierungsalgorithmus

Während des folgenden Algorithmus werden wir immer wieder schon fertige Zeilen und Spalten an den Rand tauschen und dann für den weiteren Prozess vergessen. Wir bezeichnen die verbleibende Matrix als Restmatrix. Bei Beginn des Prozesses ist die ganze Matrix die Restmatrix.

1. Falls die Restmatrix Nullzeilen oder –spalten enthält, tausche man diese an den unteren bzw. rechten Rand der Matrix.

2. Falls es eine Position $i_0\ j_0$ in der Restmatrix gibt, so dass $r_{i_0 j_0} \quad 0$, aber $r_{i_0 j} \quad 0$ für alle $j \quad j_0$ und $r_{i j_0} \quad 0$ für alle $i \quad i_0$, tausche man die i_0–te Zeile mit der ersten Zeile der Restmatrix und die j_0–te Spalte der Restmatrix mit der ersten Spalte und vergesse diese neue erste Zeile und Spalte der Restmatrix. Diesen Schritt wiederholen wir so oft wie möglich.

3. Falls es keine Restmatrix mehr gibt, sind wir fertig.

4. Suche in der Restmatrix das Element $r_{i_0 j_0}$ mit dem kleinsten Betrag ungleich Null.

   (a) Für jede Zeile $i \quad i_0$ der Restmatrix berechne man q_i durch Division mit Rest, $r_{i j_0} \quad q_i r_{i_0 j_0} \quad r'_{i j_0}$ mit $0 \quad r'_{i j_0} \quad r_{i_0 j_0}$, und subtrahiere das q_i–fache der i_0–ten Zeile von der i–ten Zeile.

   (b) Für jede Spalte $j \quad j_0$ der Restmatrix berechne man q_j durch Division mit Rest, $r_{i_0 j} \quad q_j r_{i_0 j_0} \quad r'_{i_0 j}$ mit $0 \quad r'_{i_0 j} \quad r_{i_0 j_0}$, und subtrahiere das q_j–fache der j_0–ten Spalte von der j–ten Spalte.

5. Zurück zu 1.

Dass der Algorithmus am Ende eine Diagonalmatrix liefert, ist klar. Wir müssen jedoch überlegen, ob er überhaupt terminiert. Dafür behaupten wir, dass bei jedem Erreichen von Punkt 3 (ab dem zweiten Mal) die Restmatrix verkleinert wurde oder das Minimum der Beträge ungleich Null der Restmatrix gesunken ist. Da beides durch natürliche Zahlen beschrieben wird, muss der Algorithmus damit terminieren. Schauen wir uns Schritt 4 darauf hin an. Dort ist vor der Ausführung des Schrittes das Minimum der Beträge ungleich Null $r_{i_0 j_0}$. Jetzt werden Divisionen mit Rest bezüglich $r_{i_0 j_0}$ durchgeführt. Die einzige Möglichkeit, wie das Minimum der Beträge ungleich Null dabei nicht sinken kann, ist, dass alle $r'_{i j_0}$ und $r'_{i_0 j}$ Null sind. Dann wird aber im Schritt 2 i_0 j_0 als eine gesuchte Position erkannt und folglich nach Vertauschungen eine Zeile und Spalte der Restmatrix gestrichen, also die Restmatrix verkleinert.

Die Berechnung des Kokerns, ^{k} ImR, einer Diagonalmatrix und damit des Isomorphietyps der dargestellten Gruppe ist trivial. Halten wir es als Hilfssatz fest:

Hilfssatz 6.12 *Falls* ^{l} R ^{k} S *G eine Darstellung einer endlich erzeugten abelschen Gruppe G ist und*

$$R \quad \left(\begin{array}{ccc|c} n_1 & & 0 & 0 \\ & \ddots & & \vdots \\ 0 & & n_r & 0 \\ \hline 0 & & 0 & 0 \end{array}\right)$$

dann ist G isomorph zu

$$^{k}\ ^{r} \prod_{i\ 1}^{r} n_i$$

Zusammen mit dem Diagonalisierungsalgorithmus erhalten wir den Hauptsatz.

Satz 6.13 *Jede endlich erzeugte abelsche Gruppe ist isomorph zu einem endlichen Produkt von zyklischen Gruppen.*

Beispiel Wir wenden den Algorithmus auf ein einfaches Beispiel an. Schritte, bei denen sich nichts ändert, lassen wir weg und schreiben die Schrittnummer des ausgeführten Schrittes über den Pfeil. Das für den Schritt wichtigste Element ist unterstrichen.

$$\begin{array}{ccc} \begin{array}{ccc} 8 & 15 & 23 \\ 16 & 18 & \underline{4} \\ 0 & 15 & 15 \\ 16 & 30 & 14 \end{array} & \overset{4a}{\longrightarrow} & \begin{array}{ccc} 72 & 105 & 3 \\ 16 & 18 & \underline{4} \\ 48 & 69 & 3 \\ 80 & 102 & 2 \end{array} \\ & \overset{4b}{\longrightarrow} & \\ \begin{array}{ccc} 84 & 117 & 3 \\ 0 & \underline{2} & 4 \\ 60 & 81 & 3 \\ 72 & 94 & 2 \end{array} & \overset{4a}{\longrightarrow} & \begin{array}{ccc} 84 & 1 & 235 \\ 0 & \underline{2} & 4 \\ 60 & 1 & 163 \\ 72 & 0 & 186 \end{array} \\ & \overset{4b}{\longrightarrow} & \\ \begin{array}{ccc} 84 & \underline{1} & 237 \\ 0 & 2 & 0 \\ 60 & 1 & 165 \\ 72 & 0 & 186 \end{array} & \overset{4a}{\longrightarrow} & \begin{array}{ccc} 84 & \underline{1} & 237 \\ 168 & 0 & 474 \\ 24 & 0 & 72 \\ 72 & 0 & 186 \end{array} \\ & \overset{4b}{\longrightarrow} & \\ \begin{array}{ccc} 0 & \underline{1} & 0 \\ 168 & 0 & 474 \\ 24 & 0 & 72 \\ 72 & 0 & 186 \end{array} & \overset{2}{\longrightarrow} & \begin{array}{ccc} 1 & 0 & 0 \\ 0 & 168 & 474 \\ 0 & \underline{24} & 72 \\ 0 & 72 & 186 \end{array} \\ & \overset{4a}{\longrightarrow} & \\ \begin{array}{ccc} 1 & 0 & 0 \\ 0 & 0 & 30 \\ 0 & \underline{24} & 72 \\ 0 & 0 & 30 \end{array} & \overset{4b}{\longrightarrow} & \begin{array}{ccc} 1 & 0 & 0 \\ 0 & 0 & 30 \\ 0 & \underline{24} & 0 \\ 0 & 0 & 30 \end{array} \\ & \overset{2}{\longrightarrow} & \\ \begin{array}{ccc} 1 & 0 & 0 \\ 0 & 24 & 0 \\ 0 & 0 & \underline{30} \\ 0 & 0 & 30 \end{array} & \overset{4a}{\longrightarrow} & \begin{array}{ccc} 1 & 0 & 0 \\ 0 & 24 & 0 \\ 0 & 0 & 30 \\ 0 & 0 & 0 \end{array} \end{array}$$

Damit ist die durch die Matrix dargestellte abelsche Gruppe isomorph zu 24 30

.

Aufgabe 6.14 Diagonalisieren Sie die Matrix

$$\begin{pmatrix} 13 & 16 & 3 & 14 \\ 1 & 0 & 3 & 0 \\ 22 & 24 & 4 & 22 \\ 15 & 16 & 5 & 16 \end{pmatrix}$$

Mit Hilfe des chinesischen Restsatzes lässt sich der Satz umformulieren:

Korollar 6.15 *Jede endlich erzeugte abelsche Gruppe G ist isomorph zu*

$$^{r} \prod_{j=1}^{s} \prod_{i=1}^{s_j} p_j^{r_{ji}}$$

für geeignete Primzahlen p_j *und natürliche Zahlen* $r\ s\ _0; s_j\ r_{ji}$ *. Die Zahl r sowie die Gruppen* $p_j^{r_{ji}}$ *sind bis auf Reihenfolge eindeutig.*

Beweis: Nach dem vorangegangenen Satz ist G isomorph zu $^{r}\ \prod_{i\ 1}^{l}\ n_i$. Falls n_i $\prod_{j\ 1}^{l_i} p_j^{r_{ji}}$, dann ist nach Korollar 5.8

$$n_i \prod_{j=1}^{l_i} p_j^{r_{ji}}$$

Umsortieren der Faktoren ergibt nun die Existenz der Zerlegung. Die Eindeutigkeit kann wie folgt gezeigt werden. Nimmt man eine Primzahl p, die nicht in der Menge $\{p_1 \quad p_s$ vorkommt, so ist die Multiplikation mit p ein Isomorphismus auf den Gruppen $p_j^{r_{ji}}$. Folglich ist

$$G\ pG \qquad p\ ^{r}$$

und damit r festgelegt. Nun beobachten wir, dass für jedes j

$$G_j : \quad g \quad G \quad n \quad _0 : \operatorname{ord} g \quad p_j^n \quad \prod_{i=1}^{s_j} p_j^{r_{ji}}$$

ist. Seien die r_{ji} durch $r_{j1} \quad r_{j2} \qquad r_{r_j s_j}$ geordnet. Wir führen einen Induktionsbeweis nach r_{j1}. Für $r_{j1} \quad 1$ ist G_j ein p_j –Vektorraum der Dimension s_j und muss daher aus s_j Kopien von p_j bestehen. Für $r_{j1} \quad 1$ betrachten wir

$$p_j G_j \quad \prod_{i=1}^{s_j} p_j \quad p_j^{r_{ji}} \qquad \prod_{i=1}^{s_j} \quad p_j^{r_{ji}\ 1}$$

wobei $p^0 \qquad 0$ die triviale Gruppe ist. Durch Anwenden der Induktionsvoraussetzung auf $p_j G_j$ erhalten wir die Eindeutigkeit der Faktoren $p_j^{r_{ji}\ 1}$ in $p_j G_j$ und damit auch die Eindeutigkeit der Faktoren $p_j^{r_{ji}}$ in G_j sowie G.

Korollar 6.16 *Jede endlich erzeugte abelsche Gruppe G ist isomorph zu*

$$^{r} \prod_{i\ 1}^{l} n_i$$

für geeignete natürliche Zahlen n_i 2 *mit* $n_{i\ 1}$ n_i *für* i 1 l 1 *und* r $_0$. *Die Zahlen* n_i *sind eindeutig bestimmt.*

Beweis: Wir dürfen annehmen, dass G ein Produkt ist, wie es im letzten Korollar beschrieben wurde. Weiter nehmen wir an, dass die r_{ji} für festes j absteigend sortiert sind, d.h. r_{j1} r_{j2} r_{j3} . Wir setzen n_i $\prod_{j\ 1}^{s} p_j^{r_{ji}}$, wobei r_{ji} 0 für i s_j. Dann gilt $n_{i\ 1}$ n_i wegen der Sortierung der r_{ij}. Dass G isomorph zu ^{r} $\prod_{i\ 1}^{l}$ n_i ist, folgt dann wieder aus dem Korollar zum chinesischen Restsatz. Die Eindeutigkeit der n_i wird ähnlich wie im Beweis von Korollar 6.15 mit Induktion über n_l bewiesen.

Definition 6.17 *Die Zahl r in dem vorangehenden Korollar ist der* Rang *der abelschen Gruppe G. Die* n_i *heißen* Elementarteiler.

Beispiel Wir führen das obige Beispiel fort. Wir hatten bereits gefunden, dass G isomorph zu 24 30 war. Die Primfaktorzerlegungen sind 24 2^3 3 und 30 2 3 5, und G ist isomorph zu

$$2 \quad 2^3 \quad 3 \quad 3 \quad 5$$

Fassen wir die Faktoren wie im Beweis von Korollar 6.16 zusammen, so erhalten wir n_1 8 3 5 120, n_2 2 3 6, also

$$G \quad 120 \quad 6$$

Aufgabe 6.18 Bringen Sie nun auch die abelsche Gruppe, die durch die Matrix aus Aufgabe 6.14 dargestellt wird, auf die Normalformen der beiden Korollare.

Zusatzaufgaben

Aufgabe 6.19 Klassifizieren Sie alle endlichen, abelschen Gruppen mit 30 vielen Elementen bis auf Isomorphie.

Aufgabe 6.20 Sei G eine endlich erzeugte abelsche Gruppe mit einer Darstellung der Form ^{5} R ^{5} S G, wobei

$$R = \begin{array}{rrrrr} 2 & 2 & 8 & 6 & 10 \\ 2 & 8 & 2 & 6 & 22 \\ 2 & 26 & 1756 & 126 & 688 \\ 6 & 6 & 96 & 48 & 30 \\ 10 & 22 & 392 & 30 & 284 \end{array}$$

1. Bestimmen Sie $r\ l \quad 0$ und natürliche Zahlen $n_1 \quad n_l$ mit $n_i \ 1 \ n_i$ für $1 \quad i \quad l \quad 1$, so dass $G \quad r \ \prod_{i \ 1}^{l} \ n_i$ gilt.
2. Bestimmen Sie $r\ s \quad 0, s_j \ r_{ji}$ und Primzahlen p_j, so dass

$$G \quad r \ \prod_{j \ 1}^{s} \prod_{i \ 1}^{s_j} \ p_j^{r_{ji}}$$

Aufgabe 6.21 Sei R : 14 und φ die R–lineare Abbildung

$$\varphi : R^2 \quad R^2 \quad v \quad \begin{matrix} 4 & 9 \\ 2 & 6 \end{matrix} \quad v$$

Stellen Sie die Untergruppen G : Ker φ und H : Im φ von R^2 mit Hilfe von Erzeugern und Relationen dar.

Aufgabe 6.22 Sei $l \quad k$. Zeigen Sie: $p^l \quad p^k \quad p^{k \ l}$.

Aufgabe 6.23 Sei k . Beweisen Sie: Jede Untergruppe von ^{k} ist isomorph zu ^{l} mit $l \quad k$.

Aufgabe 6.24 Seien G, r und l wie in Korollar 6.16. Zeigen Sie, dass $r \quad l$ die minimale Anzahl von Erzeugern der Gruppe G ist.

Aufgabe 6.25 Zeigen Sie, dass $\mathbb{Q}$ kein endliches oder unendliches Produkt von zyklischen Gruppen ist. Zeigen Sie weiter, dass die multiplikative Gruppe $\mathbb{Q}$ von $\mathbb{Q}$ nicht endlich erzeugt ist.

Aufgabe 6.26 Sei R Mat n GL $n \ \mathbb{Q}$ die Relationenmatrix einer endlich erzeugten abelschen Gruppe G, d.h. es gibt Erzeuger $e_1 \quad e_n$, so dass

$$n \quad R \quad n \ e_1 \ \ldots \ e_n \quad G$$

eine Darstellung von G ist. Zeigen Sie: ord G det R .

Aufgabe 6.27 Folgern Sie aus dem Diagonalisierungsalgorithmus, dass GL k — wie oben behauptet — von den Elementarmatrizen erzeugt ist.

7 Die Struktur der Einheitengruppen U_n

Nachdem wir im letzten Abschnitt sämtliche endlichen abelschen Gruppen kennengelernt haben, stellt sich natürlich die Frage, welche Struktur die Gruppe U_n hat. Wegen des chinesischen Restsatzes in der Form von Lemma 5.13 können wir uns auf den Fall $n = p^r$ beschränken. Wir werden zeigen, dass alle diese Gruppen U_{p^r} zyklisch sind — mit Ausnahme der U_{2^r} für $r \geq 3$.

Beispiele Die Struktur der U_n für kleine n ergibt sich meist schon aus der Anzahl ihrer Elemente, da es nur eine abelsche Gruppe mit dieser Anzahl $\varphi(n)$ gibt:

$$
\begin{array}{ll}
U_2 & \{\overline{1}\} \\
U_3 & \{\overline{1}, \overline{2}\} \cong C_2 \\
U_4 & \{\overline{1}, \overline{3}\} \cong C_2 \\
U_5 & \{\overline{1}, \overline{2}, \overline{4}, \overline{2}^2 = \overline{3}, \overline{2}^3 = \overline{3}\} \cong C_4 \\
U_6 & \{\overline{1}, \overline{5}\} \cong C_2 \\
U_7 & \{\overline{1}, \overline{3}, \overline{2}, \overline{3}^2 = \overline{6}, \overline{3}^3 = \overline{4}, \overline{3}^4 = \overline{5}, \overline{3}^5 = \overline{3}\} \cong C_6 \\
U_8 & \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\} \cong C_2 \times C_2
\end{array}
$$

Dass U_8 isomorph zu $C_2 \times C_2$ und nicht zu C_4 ist, sieht man daran, dass jedes Element in U_8 zum Quadrat eins ist, also Ordnung 1 oder 2 hat.

Wir betrachten zuerst die U_p, die multiplikative Gruppe des Körpers $\mathbb{F}_p$, bevor wir zu den Primzahlpotenzen übergehen.

Satz 7.1 *Die Einheitengruppe $U_p = \mathbb{F}_p^\times$ ist zyklisch, d.h. sie ist isomorph zu der Gruppe C_{p-1}.*

Dies ist eine unmittelbare Folgerung aus dem folgenden allgemeineren Satz:

Satz 7.2 *Jede endliche Untergruppe der multiplikativen Gruppe eines Körpers ist zyklisch.*

Beweis: Wir bezeichnen die Untergruppe der multiplikativen Gruppe $K^\times$ mit G. Nach der Klassifikation der endlichen abelschen Gruppen ist G isomorph zu einem Produkt

$$\prod_{j=1}^{s} \prod_{i=1}^{s_j} p_j^{r_{ji}} \qquad s, s_j, r_{ji} \in \mathbb{N}; \ p_j \text{ paarweise verschieden}$$

S. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie,*
DOI 10.1007/978-3-8348-8263-9_7,

Nach dem Korollar 5.8 zum chinesischen Restsatz ist diese Gruppe zyklisch, falls alle s_j gleich 1 sind. Angenommen eines der s_j wäre größer, ohne Einschränkung sei es s_1. Wir setzen $r :=$ max$\{r_{1i} \mid i = 1, \ldots, s_1\}$. Dann haben die Elemente von

$$\prod_{i=1}^{s_1} p_1^{r_{1i}} \quad 0 \quad : H$$

alle eine Ordnung, die p_1^r teilt. Daher sind die entsprechenden Elemente in G alle Lösungen der Gleichung $x^{p_1^r} = 1$. Über dem Körper K hat das Polynom $x^{p_1^r} - 1$ höchstens p_1^r Nullstellen (siehe Anhang B). Da H aber $\prod_{i=1}^{s_1} p_1^{r_{1i}} > p_1^r$ Elemente hat, ist das ein Widerspruch.

Definition 7.3 *Eine Zahl ζ, die modulo n eine zyklische Einheitengruppe U_n erzeugt, nennt man* Primitivwurzel *modulo n.*

Manchmal reicht es nicht aus, abstrakt zu wissen, dass U_n zyklisch ist, sondern man möchte den Isomorphismus konkret kennen. Wir benötigen also eine Primitivwurzel ζ, damit wir

$$\exp_\zeta : \quad \varphi(n) \quad U_n \quad i \quad \varphi(n) \quad \zeta^i \quad n$$

schreiben können. Zum Auffinden einer Primitivwurzel modulo p ist keine bessere Strategie bekannt als das einfache Durchprobieren der Elemente von U_p. Die Rechengesetze für Ordnungen (siehe Anhang A.10) implizieren die folgende Aussage:

Lemma 7.4 *Sei p eine Primzahl. Für eine Zahl ζ mit $\zeta \not\equiv 0 \bmod p$ sind äquivalent:*

1. *ζ ist Primitivwurzel modulo p.*
2. *$\zeta^{\frac{p-1}{q}} \not\equiv 1 \bmod p$ für alle Primteiler q von $p - 1$.*

Wir werden in Aufgabe 7.11 sehen, dass recht viele Zahlen unter den $1, \ldots, p - 1$ Primitivwurzeln sind, so dass man üblicherweise nicht allzuviele ζ testen muss.

Beispiel Wir wollen beweisen, dass $\zeta = 2$ eine Primitivwurzel modulo 19 ist. Da $19 - 1 = 18 = 2 \cdot 3^2$ ist, reicht es zu zeigen, dass $\zeta^{18/2} = 2^9 \not\equiv 1 \bmod 19$ und $\zeta^{18/3} = 2^6 \not\equiv 1 \bmod 19$ ist. Dazu rechnen wir $\overline{2}^2 = \overline{4}$, $\overline{2}^4 = \overline{2}^{2 \cdot 2} = \overline{4}^2 = \overline{16}$, $\overline{2}^8 = \overline{2}^{4 \cdot 2} = \overline{16}^2 = \overline{3}^2 = \overline{9}$, also $\overline{2}^9 = \overline{2}^8 \cdot \overline{2} = \overline{9} \cdot \overline{2} = \overline{18} = \overline{-1}$ und $\overline{2}^6 = \overline{2}^4 \cdot \overline{2}^2 = \overline{16} \cdot \overline{4} = \overline{-3} \cdot \overline{4} = \overline{-7} = \overline{-1}$.

Jetzt können wir die Struktur der U_{p^r} bestimmen. Für $p > 2$ sind sie alle zyklisch. Wir starten mit einem Hilfssatz.

Hilfssatz 7.5 *Sei $x \in \mathbb{Z}$. Für $2 < p$ und $r > 2$ gilt*

$$x^p \equiv 1 \bmod p^r \quad \Rightarrow \quad x \equiv 1 \bmod p^{r-1}$$

Beweis: Sei zunächst $x \equiv 1 \bmod p^{r-1}$ vorausgesetzt. Wir schreiben $x = 1 + ap^{r-1}$ für ein a und rechnen

$$x^p = 1 + ap^{r-1}{}^p = 1 + pap^{r-1} + \sum_{i=2}^{p} \binom{p}{i} a^i p^{i(r-1)} \equiv 1 \bmod p^r$$

wobei wir $i(r-1) = 2r-1-r = r-1 \geq r$ nutzen.

Sei nun $x^p \equiv 1 \bmod p^r$. Für $r = 2$ folgt die Aussage aus dem kleinen Satz von Fermat 1 $x^p \equiv x \bmod p$. Wir zeigen jetzt den Induktionsschritt von r auf $r+1$. Da die Gleichung $x^p \equiv 1 \bmod p^{r-1}$ auch modulo p^r gilt, erhalten wir durch Anwenden der Induktionsvoraussetzung $x \equiv 1 \bmod p^{r-1}$. Wir schreiben wieder x als $x = 1 + ap^{r-1}$ mit $a \in \mathbb{Z}$. Dann ist

$$1 + x^p = 1 + ap^{r-1}{}^p = 1 + ap^r + \binom{p}{2} a^2 p^{2(r-1)} + \sum_{i=3}^{p} \binom{p}{i} a^i p^{i(r-1)}$$

$$\equiv 1 + ap^r + \frac{p(p-1)}{2} a^2 p^{2r-2} \equiv 1 + ap^r \bmod p^{r+1}$$

weil $i(r-1) \geq 3(r-1) = 3r-3 = r + 2r - 3 \geq r + 1$ und $2r - 1 \geq r + r - 1 = r + r - 1 \geq r + 1$. Wir erhalten $ap^r \equiv 0 \bmod p^{r+1}$. Also muss p die Zahl a teilen und $x \equiv 1 \bmod p^r$ sein.

Aufgabe 7.6 Zeigen Sie, dass der Hilfssatz für $p = 2$ falsch ist. Beweisen Sie auch, dass er richtig wird, wenn man nur x mit $x \equiv 1 \bmod 4$ betrachtet.

Satz 7.7 *Die Einheitengruppe U_{p^r} ist zyklisch für alle Primzahlen $p \geq 3$ und $r \geq 1$, d.h. U_{p^r} hat $\varphi(p^r)$ Elemente. Falls ζ eine Primitivwurzel modulo p ist, dann ist ζ oder $\zeta + p$ eine Primitivwurzel modulo p^r für alle $r \geq 1$, abhängig davon ob $\zeta^{p-1} \not\equiv 1 \bmod p^2$ oder $(\zeta + p)^{p-1} \not\equiv 1 \bmod p^2$.*

Beweis: Wir müssen zeigen, dass ζ oder $\zeta + p$ die maximale Ordnung, $\varphi(p^r) = p^{r-1}(p-1)$, in $\mathbb{Z}/p^r\mathbb{Z}$ hat. Dafür reicht es zu zeigen, dass für alle Primzahlen q mit $q \mid \varphi(p^r)$ immer $\zeta^{\varphi(p^r)/q} \not\equiv 1 \bmod p^r$ oder immer $(\zeta + p)^{\varphi(p^r)/q} \not\equiv 1 \bmod p^r$ ist. Für q mit $q \mid p-1$ gilt nach dem kleinen Satz von Fermat

$$(\zeta + p)^{\varphi(p^r)/q} \equiv \zeta^{\varphi(p^r)/q} \equiv \zeta^{p^{r-1}(p-1)/q} \equiv \zeta^{(p-1)/q} \not\equiv 1 \bmod p$$

dabei folgt die letzte Ungleichung aus der Tatsache, dass ζ eine Primitivwurzel modulo p ist.

Es bleibt nur noch $q = p$ zu betrachten, also zu zeigen, dass

$$\zeta^{p^{r-2}(p-1)} \not\equiv 1 \bmod p^r \quad \text{oder} \quad (\zeta + p)^{p^{r-2}(p-1)} \not\equiv 1 \bmod p^r$$

Dies ist durch $r-2$ –faches Anwenden des Hilfssatzes 7.5 auf $\zeta^{(p-1)p^{r-2}}$ bzw. $(\zeta + p)^{(p-1)p^{r-2}}$ äquivalent zu

$$\zeta^{p-1} \not\equiv 1 \bmod p^2 \quad \text{oder} \quad (\zeta + p)^{p-1} \not\equiv 1 \bmod p^2$$

Nehmen wir das Gegenteil an, also $\zeta^{p-1} \equiv \zeta \equiv p^{p-1} \equiv 1 \bmod p^2$. Dann ist aber

$$1 \equiv \zeta \equiv p^{p-1} \equiv \zeta^{p-1} \equiv p \equiv 1 \quad \zeta^{p-2} p \equiv 1 \equiv p\zeta^{p-2} \bmod p^2$$

also $p\zeta^{p-2} \equiv 0 \bmod p^2$ $\zeta^{p-2} \equiv 0 \bmod p$. Da ζ eine Einheit ist, ist das ein Widerspruch.

Beispiel Wir haben bereits gezeigt, dass 2 eine Primitivwurzel modulo 19 ist, daher ist 2 oder $2 \equiv 19 \equiv 21$ eine Primitivwurzel modulo 19^r, $r \equiv$. Wir müssen dafür nur testen, ob $2^{18} \equiv 1$ oder $21^{18} \equiv 1 \bmod 19^2$ ist. Wir rechnen modulo 19^2: $\overline{2}^2 \equiv \overline{4}, \overline{2}^4 \equiv \overline{4}^2 \equiv \overline{16}, \overline{2}^8 \equiv \overline{16}^2 \equiv \overline{256}, \overline{2}^{16} \equiv \overline{256}^2 \equiv \overline{195}, \overline{2}^{18} \equiv \overline{2}^{16} \overline{2}^2 \equiv \overline{195} \overline{4} \equiv \overline{58} \equiv \overline{1}$. Also ist 2 eine Primitivwurzel modulo 19^r für alle r .

Aufgabe 7.8 Seien p und ζ wie im Satz 7.7. Können sowohl ζ als auch $\zeta \quad p$ eine Primitivwurzel modulo p^r sein?

Wie an so vielen Stellen der Zahlentheorie bildet der Fall für $p \quad 2$ eine Ausnahme. Am Anfang des Abschnittes haben wir bereits $U_2 \quad 0$ und $U_4 \quad 2$ bestimmt. Die restlichen U_{2^r} sind alle nicht zyklisch.

Satz 7.9 *Für $r \quad 3$ ist die folgende Abbildung ein Isomorphismus:*

$$\Psi : \quad 2 \qquad 2^{r-2} \qquad\qquad U_{2^r}$$
$$i \quad 2 \quad j \quad 2^{r-2} \qquad\qquad 1 \quad i5^j \quad 2^r$$

Beweis: Damit die Abbildung überhaupt wohldefiniert ist, muss die Ordnung von 5 in U_{2^r} die Zahl 2^{r-2} teilen. Tatsächlich wollen wir zeigen, dass $\operatorname{ord}\overline{5} \quad 2^{r-2}$. Dazu betrachten wir den natürlichen surjektiven Homomorphismus $U_{2^r} \quad U_4 \quad \{\overline{1}\ \overline{3}$, der die Einschränkung von $2^r \qquad 4$ ist. Sei H sein Kern. Die Ordnung von H ist $\operatorname{ord}U_{2^r} \quad \operatorname{ord}U_4 \quad 2^{r-1} \quad 2 \quad 2^{r-2}$. Wegen $5 \quad 1 \bmod 4$ liegt $\overline{5}$ in H und nach dem Satz von Lagrange gilt $\operatorname{ord}\overline{5} \quad \operatorname{ord}H \quad 2^{r-2}$. Um $\operatorname{ord}\overline{5} \quad 2^{r-2}$ zu beweisen, reicht es $5^{2^{r-3}} \quad 1 \bmod 2^r$ zu zeigen.

Wir führen dafür eine Induktion nach r. Der Anfang für $r \quad 3$ ist klar. Um die Aussage für $r \quad 1$ zu zeigen, starten wir mit $5^{2^{r-3}} \quad 1 \bmod 2^r$, d.h. $5^{2^{r-3}} \quad 1 \quad a2^k$ mit $k \quad r$ und ungeradem a . Da mit $\overline{5} \quad H$ auch die Potenzen $\overline{5}^{2^{r-3}}$ in H liegen, sind sie 1 modulo 4, sprich $k \quad 2$. Durch Quadrieren erhalten wir unter Berücksichtigung von $2k \quad k \quad 1$ die Behauptung

$$5^{2^{r-2}} \quad 5^{2^{r-3} \cdot 2} \quad 1 \quad a2^k \quad 2 \quad 1 \quad a2^{k-1} \quad a^2 2^{2k} \quad 1 \bmod 2^{r-1}$$

Nun da wir wissen, dass Ψ ein wohldefinierter Homomorphismus ist, wollen wir zeigen, dass Ψ injektiv ist. Sei $\Psi\ \overline{i}\ \overline{j} \qquad 1 \quad i5^j \quad 1 \bmod 2^r$. Insbesondere ist dann $1 \qquad 1 \quad i5^j \quad 1 \quad i \bmod 4$ und damit $i \quad 0 \bmod 2 \quad \overline{i} \quad \overline{0}$. Aus $\Psi\ \overline{0}\ \overline{j} \qquad 1 \quad 0 5^j \quad 5^j \quad 1 \bmod 2^r$ folgt wegen $\operatorname{ord}\overline{5} \quad 2^{r-2}$, dass $j \quad 0 \bmod 2^{r-2} \quad \overline{j} \quad \overline{0}$. Somit ist Ψ injektiv. Die Surjektivität folgt nun unmittelbar, weil die beiden Gruppen die gleiche Anzahl von Elementen haben.

Aufgabe 7.10 Zeigen Sie: Die Einheitengruppe U_n ist genau dann zyklisch, wenn $n \quad 4$, $n \quad p^{r-1}$ oder $n \quad 2p^r$ mit $p \qquad \{2$ und $r \qquad 0$ gilt.

Aufgabe 7.11 Sei U_n eine zyklische Einheitengruppe und $\overline{\zeta}$ ein Erzeuger. Zeigen Sie, dass $\{\overline{\zeta}^i \mid i \quad \text{ggT}\ i\ \varphi\ n \quad 1\}$ die Menge aller Erzeuger von U_n ist. Insbesondere hat U_n also $\varphi\ \varphi\ n$ Erzeuger.

Lemma 7.12 *Sei U_n eine zyklische Einheitengruppe und ζ eine Primitivwurzel modulo n. Dann erfüllt die Exponentialfunktion* $\exp_\zeta : \quad \varphi\ n \quad U_n$ *die üblichen Rechengesetze:*

$$\exp_\zeta\ x \quad y \quad \exp_\zeta\ x \quad \exp_\zeta\ y$$
$$\exp_\zeta\ x \quad \exp_\zeta\ mx$$

für $x\ y \quad \varphi\ n$ und m . Folglich gilt für ihre Umkehrfunktion $\log_\zeta : U_n \quad \varphi\ n$ *:*

$$\log_\zeta\ x\ y \quad \log_\zeta\ x \quad \log_\zeta\ y$$
$$\log_\zeta\ x^m \quad m \log_\zeta\ x$$

Beweis: Diese Rechengesetze vererben sich von auf $\varphi\ n$.

Eine der wichtigsten Anwendungen des Isomorphismus $\exp_\zeta$ — oder genauer seiner Umkehrfunktion, des diskreten Logarithmus $\log_\zeta$ — ist das Rückführen von Wurzelziehen auf lineare Gleichungen. Betrachten wir in einem zyklischen U_n die Gleichung

$$x^k \quad a \qquad \text{für } k \qquad \text{und } a \quad U_n$$

Sei ζ eine Primitivwurzel modulo n und $\alpha \quad \log_\zeta a$, d.h. $a \quad \zeta^\alpha \mod n$. Anwenden des diskreten Logarithmus führt zur äquivalenten Gleichung

$$k\ \log_\zeta x \quad \log_\zeta x^k \quad \log_\zeta a \quad \alpha \qquad \text{in} \quad \varphi\ n$$

Die Gleichung $k\ \log_\zeta x \quad \alpha$ können wir jetzt mit Hilfe von Satz 4.8 für $\log_\zeta x$ lösen. Das Anwenden von $\exp_\zeta$ auf alle möglichen Lösungen liefert alle Lösungen für $x^k \quad a$. Wenn man diese Vorgehensweise auf konkrete Zahlen anwendet, ergibt sich das Problem, dass die Berechnung von $\log_\zeta$ schwierig sein kann. Am Ende des Abschnittes stellen wir dafür den „baby steps – giant steps“ Algorithmus vor. Für eine andere — meist schnellere — Methode zur Berechnung der k–ten Wurzeln siehe Aufgabe 8.17.

Beispiel Wir wollen die Gleichung $x^3 \quad \overline{11}$ in $\mathbb{F}_{19}$ lösen. Wir wählen wieder $\zeta \quad 2$ als Primitivwurzel. Um $\log_2 \overline{11}$ zu finden, betrachten wir die Werte der Exponentialfunktion:

i	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\exp_2$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{8}$	$\overline{16}$	$\overline{13}$	$\overline{7}$	$\overline{14}$	$\overline{9}$

i	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{13}$	$\overline{14}$	$\overline{15}$	$\overline{16}$	$\overline{17}$
$\exp_2$	$\overline{18}$	$\overline{17}$	$\overline{15}$	$\overline{11}$	$\overline{3}$	$\overline{6}$	$\overline{12}$	$\overline{5}$	$\overline{10}$

Wir sehen $\log_2 \overline{11} \quad \overline{12}$. Da ggT 3 18 12, hat die Gleichung $3y \quad 12 \mod 18$ nach Satz 4.8 die Lösungen $y \quad 4 \mod 6$. Modulo 18 ist y gleich 4, 10 oder 16. Damit hat die Gleichung $x^3 \quad \overline{11}$ in $\mathbb{F}_{19}$ die Lösungen $\exp_2 \overline{4} \quad \overline{16}$, $\exp_2 \overline{10} \quad \overline{17}$ und $\exp_2 \overline{16} \quad \overline{5}$.

Betrachten wir noch die Gleichung $x^3 \equiv \overline{13}$ in $\mathbb{F}_{19}$. Durch Anwenden von $\log_2$ erhalten wir $3 \log_2 x \equiv \overline{5}$ in $\mathbb{Z}/18\mathbb{Z}$. Da ggT$(3,18) = 5$, gibt es keine Lösungen dieser Gleichung für $\log_2 x$ und somit auch keine Lösungen für $x^3 \equiv \overline{13}$ in $\mathbb{F}_{19}$.

Aufgabe 7.13 Berechnen Sie die Lösungen von $x^3 \equiv 4 \bmod 17$, $x^3 \equiv 8 \bmod 13$ und $x^2 \equiv 1 \bmod 21$.

Die Schwierigkeit der Berechnung des diskreten Logarithmus entfällt bei bestimmten Werten. So ist immer $\log_\zeta \overline{1} \equiv \overline{0}$. Daher lassen sich nach obigem Verfahren schnell alle Einheitswurzeln finden. Suchen wir für zyklisches U_n die Quadratwurzeln von 1. Das sind natürlich zum Beispiel 1 und -1, wir werden auch gleich sehen, dass dies die einzigen sind. Wenden wir das obige Verfahren an. Dann ist $x^2 \equiv 1$ in U_n äquivalent zu $2 \log_\zeta x \equiv \overline{0}$ in $\mathbb{Z}/\varphi(n)\mathbb{Z}$. Wir finden nach Satz 4.8 die Lösungen $\log_\zeta x \in \{\overline{0}, \overline{\frac{\varphi(n)}{2}}\}$, also $\exp_\zeta \overline{0} = \overline{1}$ und $\exp_\zeta \overline{\frac{\varphi(n)}{2}}$ als Lösungen von $x^2 \equiv 1$. Der Vergleich mit den bekannten Lösungen $1, -1$ liefert, dass immer $\exp_\zeta \overline{\frac{\varphi(n)}{2}} = \overline{-1}$ gilt.

Das führt zu dem folgenden bekannten Lemma über die Quadratwurzeln von -1 in dem Körper $\mathbb{F}_p$.

Lemma 7.14 *Sei p eine ungerade Primzahl. Die Kongruenz $x^2 \equiv -1 \bmod p$ ist genau dann lösbar, wenn $p \equiv 1 \bmod 4$ ist.*

Beweis: Nach obigen Bemerkungen ist die Gleichung $x^2 \equiv -1$ in $\mathbb{F}_p$ äquivalent zur Gleichung $2 \log_\zeta x \equiv \log_\zeta \overline{-1} \equiv \overline{\frac{p-1}{2}}$ in $\mathbb{Z}/(p-1)\mathbb{Z}$. Diese besitzt nach Satz 4.8 genau dann Lösungen, falls ggT$(2, p-1) \mid \frac{p-1}{2}$. Da ggT$(2, p-1) = 2$, ist dies äquivalent zu $2 \mid \frac{p-1}{2}$, $4 \mid p-1$, $p \equiv 1 \bmod 4$.

Zum Abschluss wollen wir noch den *„baby steps – giant steps" Algorithmus* beschreiben, mit dem der diskrete Logarithmus $\log_\zeta \overline{a}$ etwas schneller berechnet werden kann als durch Ausrechnen sämtlicher ζ^i, bis endlich $\zeta^i \equiv a \bmod n$ gilt.

Wir suchen also ein α, $0 \leq \alpha \leq n-1$ mit $\zeta^\alpha \equiv a \bmod n$. Sei Q die kleinste natürliche Zahl mit $Q^2 \geq Q(n-1) \geq n$, also $Q \geq \sqrt{n}$. Dann können wir jede natürliche Zahl, die kleiner als $n-1$ ist, — insbesondere α — schreiben als $kQ - l$ mit $0 \leq k \leq Q$ und $0 \leq l \leq Q$. Wir suchen daher jetzt solche k, l mit $\zeta^{kQ-l} \equiv a \bmod n$ oder äquivalent dazu

$$\zeta^{Q \cdot k} \equiv a\zeta^{\cdot l} \bmod n$$

Dies kann man durchführen, indem man eine Liste der möglichen $\zeta^{Q \cdot k}$ erstellt und die $a\zeta^{\cdot l}$ so lange berechnet, bis man ein Element der Liste erhält. Da man die Liste für das schnelle Auffinden eines Elementes sortieren muss, hat der Algorithmus einen Aufwand von $\sqrt{n} \log n$.

Beispiel Berechnen wir $\log_2 \overline{7}$ in $\mathbb{F}_{19}$. Hier ist $Q = 4$. Wir wählen wieder $\zeta = 2$, dann gilt

ζ^{1} 10 mod 19. Die folgende Tabelle enthält die „baby–“und „giant steps“:

k l	$2^{4\,k}$ mod 19	$7\ 2^{\ l}$ mod 19
0	1	7
1	16	13
2	9	16
3	11	8
4	5	4

Wir sehen, dass $2^{4\,1}$ $7\ 2^{\ 2}$ mod 19. Daher ist 2^6 7 mod 19, d.h. $\log_2 \overline{7}$ $\overline{6}$.

Zusatzaufgaben

Aufgabe 7.15 Finden Sie alle Primitivwurzeln zu p 17 31 43. Wie viele gibt es? Drücken Sie alle Primitivwurzeln zu p 17 durch Potenzen von einer gefundenen aus.

Aufgabe 7.16 Berechnen Sie $\log_{\overline{2}} \overline{11}$ in $\mathbb{F}_{37}$ und $\log_{\overline{5}} \overline{65}$ in $\mathbb{F}_{547}$.

Aufgabe 7.17 Bestimmen Sie alle Lösungen von x^3 $\overline{2}$ in U_{43} und von x^4 $\overline{11}$ in U_{35}.

Aufgabe 7.18 Zeigen Sie: Es gibt kein n mit U_n 14 . Gibt es ein n mit U_n 21 ?

Aufgabe 7.19 Bestimmen Sie ein n , so dass U_n eine zu 7 ^{3} isomorphe Untergruppe enthält.

Aufgabe 7.20 Berechnen Sie für eine Primzahl p und k den Kern der natürlichen Abbildung $U_{p^{k\ 1}}$ U_{p^k}, und geben Sie einen expliziten Isomorphismus zur Gruppe p an.

Aufgabe 7.21 Bestimmen Sie für die Gruppen U_n, n {10 27 80 100 300 , jeweils eine Darstellung durch Erzeuger und Relationen. Dabei sind die Erzeuger jeweils explizit als Elemente von U_n anzugeben.

Aufgabe 7.22 Finden Sie alle Primitivwurzeln zu p 19 und p 41. Wie viele gibt es ? Drücken Sie alle Primitivwurzeln zu p 19 durch Potenzen einer gefundenen aus.

Aufgabe 7.23 Sei q eine ungerade Primzahl. Zeigen Sie:

1. Ist p $4q$ 1 prim, so ist 2 eine Primitivwurzel modulo p.
2. Ist p $2q$ 1 prim, so ist 2 oder 2 eine Primitivwurzel modulo p.

Aufgabe 7.24 Für welche a U_{128} hat die Gleichung x^2 a vier verschiedene Lösungen ?

Aufgabe 7.25 Verwenden Sie den *„baby steps – giant steps“ Algorithmus* zur Berechnung von $\log_2$ 29 mod 29, $\log_2$ 100 mod 103,

Aufgabe 7.26 Bestimmen Sie:

1. Einen expliziten Erzeuger ζ von U_7.
2. Einen expliziten Erzeuger ζ von U_{49}.
3. Einen expliziten Erzeuger ζ von U_{98}.
4. Ein a mit ζ^a 47 mod 98 mit dem *„baby steps – giant steps" Algorithmus*.

Aufgabe 7.27 Beschreiben Sie die Struktur der Einheitengruppe U_{192} als abelsche Gruppe. Wieviele Lösungen kann eine Gleichung der Form x^2 a mod 192 für a U_{192} höchstens haben ?

8 Quadratische Reste

In diesem Abschnitt geht es um die Frage, ob zu vorgegebenen p und d , $d \not\equiv 0 \bmod p$, die Gleichung

$$x^2 \equiv d \bmod p$$

eine Lösung hat. Falls ja, dann nennt man d einen *quadratischen Rest* modulo p, sonst *Nichtrest*. Dies ist natürlich äquivalent zur Frage, ob die Gleichung $x^2 = \overline{d}$ in $\mathbb{F}_p$ eine Lösung hat. Wir haben bereits im letzten Abschnitt ein Verfahren erarbeitet, um diese Frage zu beantworten und sogar eine Lösung zu finden. Das war jedoch mit einem hohen Rechenaufwand verbunden; hier wollen wir ein sehr viel schnelleres Verfahren finden.

Aufgabe 8.1 Führen Sie für eine Primzahl $p \geq 3$ die Gleichung

$$ay^2 + by + c \equiv 0 \bmod p$$

mit $a\ b\ c$ und $a \not\equiv 0 \bmod p$ durch quadratische Ergänzung auf eine Gleichung vom Typ $x^2 \equiv d \bmod p$ zurück. Schreiben Sie für $p \geq 2$ alle möglichen quadratischen Gleichungen auf, und lösen Sie sie.

Wie viele Lösungen hat die Kongruenz $x^2 \equiv d \bmod p$ bzw. die Gleichung $x^2 = \overline{d}$ in $\mathbb{F}_p$? Ein quadratisches Polynom über einem Körper kann mit Multiplizität nur entweder keine Nullstelle oder zwei Nullstellen haben. Falls $\overline{d} \neq 0$ ist, gibt es offensichtlich nur die doppelte Lösung 0. Auch $x^2 = \overline{1}$ hat in $\mathbb{F}_2$ eine doppelte Nullstelle, nämlich $\overline{1}$. In allen anderen Fällen gibt es keine oder zwei verschiedene Lösungen, denn falls y eine Lösung ist, dann auch $-y$. Wenn diese zusammenfallen, gilt für $p \geq 3$

$$y = -y \qquad 2y = 0 \qquad y = 0 \text{ in } \mathbb{F}_p$$

Definition 8.2 *Für eine Primzahl p ist das* Legendre–Symbol $\left(\frac{a}{p}\right)$ *definiert durch*

$$\left(\frac{a}{p}\right) \begin{cases} 1 & \text{falls } x^2 \equiv a \bmod p \text{ lösbar ist und } a \not\equiv 0 \bmod p \\ -1 & \text{falls } x^2 \equiv a \bmod p \text{ nicht lösbar ist} \\ 0 & \text{falls } a \equiv 0 \bmod p \end{cases}$$

Lemma 8.3 *Sei p eine ungerade Primzahl und ζ eine Primitivwurzel modulo p. Dann sind die Potenzen ζ^{2l}, $0 \leq l \leq \frac{p-1}{2}$, die quadratischen Reste und die Potenzen ζ^{2l+1}, $0 \leq l \leq \frac{p-1}{2}$, die quadratischen Nichtreste modulo p, d.h.*

$$\left(\frac{\zeta^k}{p}\right) = (-1)^k$$

Insbesondere gilt $\sum_{i=1}^{p-1} \left(\frac{i}{p}\right) = 0$.

S. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie,*
DOI 10.1007/978-3-8348-8263-9_8,

Beweis: Offensichtlich ist $\zeta^{2l} \quad \zeta^{l\ 2}$ ein quadratischer Rest. Zeigen wir nun, dass $\zeta^{2l\ 1}$ kein quadratischer Rest ist. Wir nehmen an, dass $\zeta^{2l\ 1} \quad a^2 \bmod p$ für ein $a \quad$. Schreiben wir $a \quad \zeta^k \bmod p$ für ein geeignetes $k \quad$. Einsetzen ergibt $\zeta^{2l\ 1} \quad \zeta^{2k} \bmod p$. Durch Anwendung von $\log_\zeta$ geht diese Gleichung über in $2l \quad 1 \quad 2k \bmod p \quad 1 \quad 2\ k \quad l \quad 1 \bmod p \quad 1$. Dies ist jedoch unmöglich, weil wegen $2 \quad \text{ggT}\ 2\ p \quad 1 \quad 1$ die Gleichung $2y \quad 1 \bmod p \quad 1$ nach Satz 4.8 keine Lösung besitzt.

Da jeweils die Hälfte der Elemente von U_p — die wir als $\overline{\zeta^l}$, $0 \quad l \quad p \quad 1$, oder als $\overline{i}$, $1 \quad i \quad p$, schreiben können — quadratische Reste und Nichtreste sind, heben sich in der Summe $\sum_{i\ 1}^{p\ 1} \frac{i}{p}$ die 1 und 1 gerade auf.

Aufgabe 8.4 Sei p eine ungerade Primzahl. Zeigen Sie: Eine Zahl $\zeta \quad U_p$ kann nur dann eine Primitivwurzel modulo p sein, wenn $\frac{\zeta}{p} \quad 1$ ist. Dieses notwendige Kriterium schließt bei der Berechnung von Primitivwurzeln die Hälfte der Fälle aus. Zeigen Sie durch ein Beispiel, dass das Kriterium nicht hinreichend ist.

Der folgende Satz beschreibt die einfachsten Eigenschaften des Legendre–Symbols:

Satz 8.5 *Sei p eine ungerade Primzahl und $a \quad b \quad$.*

1. $a \quad b \bmod p \qquad \frac{a}{p} \quad \frac{b}{p}$. *(Gilt auch für $p \quad 2$.)*

2. *(Euler)* $\frac{a}{p} \quad a^{\frac{p\ 1}{2}} \bmod p.$

3. $\frac{1}{p} \quad 1^{\frac{p\ 1}{2}} \quad \begin{cases} 1 & \text{für } p \quad 1 \bmod 4 \\ 1 & \text{für } p \quad 3 \bmod 4 \end{cases}$

4. $\frac{ab}{p} \quad \frac{a}{p} \quad \frac{b}{p}$.

5. $\frac{ab^2}{p} \quad \frac{a}{p}$ *für* $b \quad 0 \bmod p.$

Beweis: Punkt 1) folgt direkt aus der Definition. Die zweite Aussage ist für $a \quad 0 \bmod p$ trivial. Sei also $a \quad 0 \bmod p$. Wir bemerken zuerst, dass nach dem Satz 5.17 von Euler $a^{\frac{p\ 1}{2}\ 2} \quad a^{p\ 1} \quad 1 \bmod p$ gilt. Damit ist $a^{\frac{p\ 1}{2}}$ eine Lösung der Gleichung $x^2 \quad 1 \bmod p$, also 1 oder $\quad 1$ modulo p. Da auch $\frac{a}{p}$ nur die Werte 1 und $\quad 1$ annimmt, reicht es zu untersuchen, wann beide 1 sind.

Sei $a \quad \zeta^l$ für eine Primitivwurzel ζ modulo p und $l \quad$. Dann ist $a^{\frac{p\ 1}{2}} \quad \zeta^{\frac{l\ p\ 1}{2}} \bmod p$. Wegen $\text{ord}\,\zeta \quad p \quad 1$ ist dieser Ausdruck genau dann gleich 1, falls $p \quad 1 \quad \frac{l\ p\ 1}{2}$, also falls l gerade ist. Nach dem vorangegangenen Lemma ist dies äquivalent dazu, dass $\frac{a}{p} \quad 1$ ist.

Eigenschaft 3) ist ein Spezialfall von 2) zusammen mit der Bemerkung, dass die auftretenden Zahlen nur 1 sind und daher die Kongruenz eine Gleichheit ist. Die vierte Aussage folgt mit der gleichen Bemerkung aus

$$\frac{a}{p}\ \frac{b}{p}\quad a^{\frac{p-1}{2}}b^{\frac{p-1}{2}}\quad ab^{\frac{p-1}{2}}\quad \frac{ab}{p}\mod p$$

Die letzte Aussage ergibt sich schließlich aus

$$\frac{ab^2}{p}\quad \frac{a}{p}\ \frac{b}{p}^2\quad \frac{a}{p}$$

Mit Hilfe dieses Satzes kann das Problem der Berechnung des Legendre–Symbols auf den Fall $\frac{q}{p}$ für eine Primzahl q reduziert werden. Wenn $a\quad 1^{\,j}\prod_i q_i^{r_i}$ für $q_i\quad, r_i$ die Primfaktorzerlegung von a ist, gilt nach dem Satz

$$\frac{a}{p}\quad \frac{1}{p}^j\prod_i\ \frac{q_i}{p}^{r_i}$$

Es bleibt also $\frac{q}{p}$ für q prim zu berechnen. Der Fall $q\quad 2$ ist wieder ein Sonderfall.

Lemma 8.6 (Gauß) *Sei p eine ungerade Primzahl. Dann gilt:*

$$\frac{2}{p}\quad 1^{\frac{p^2-1}{8}}\quad \begin{array}{ll} 1 & \text{für } p\quad 1 \bmod 8\\ 1 & \text{für } p\quad 3 \bmod 8\end{array}$$

Beweis: Wir wollen Satz 8.5.2 nutzen und $2^{\frac{p-1}{2}}$ berechnen. Um das möglich zu machen, geht man bei der Berechnung von dem Ring auf den Ring i über. In i ist die Primfaktorzerlegung von 2, nämlich $2\quad i\quad 1\quad i^{\,2}$, also ein Quadrat bis auf eine Einheit. Wir rechnen

$$2^{\frac{p-1}{2}}\quad i^{\frac{p-1}{2}}\ 1\quad i^{\,p\ 1}\quad \frac{i^{\frac{p-1}{2}}}{1\quad i}\ 1\quad i^{\,p}$$

Wenn wir die Gleichung modulo p betrachten (Real– und Imaginärteil separat), gilt $1\quad i^{\,p}\ 1\quad i^p$ nach dem gleichen Argument wie im Beweis von Hilfssatz 4.6. Wir rechnen weiter

$$2^{\frac{p-1}{2}}\quad \frac{i^{\frac{p-1}{2}}\ 1\quad i}{1\quad i\quad 1\quad i}\ 1\quad i^p\quad \frac{i^{\frac{p-1}{2}}\quad i^{\frac{p-1}{2}}}{2}\ 1\quad i^p\mod p$$

Da $i^4\quad i^{\,4}\ 1$ ist, hängt der Wert der rechten Seite nur von p modulo 8 ab. Einsetzen der Werte 1 und 3 liefert 1 bzw. 1. Damit ist gezeigt, dass in der behaupteten Gleichheit in der Aussage der linke Term gleich dem rechten ist.

Wir müssen noch zeigen, dass der mittlere Term gleich dem rechten ist. Dazu bemerken wir zuerst, dass auch der mittlere Term nur von p modulo 8 abhängt, denn Einsetzen von $p\quad 8k$ für p in $1^{\frac{p^2-1}{8}}$ ergibt

$$1^{\frac{p\ 8k^{\,2}-1}{8}}\quad 1^{\frac{p^2\ 16kp\ 64k^2-1}{8}}\quad 1^{\frac{p^2-1}{8}\ 2kp\ 8k^2}$$

$$1^{\frac{p^2-1}{8}}\quad 1^{\,2\ kp\ 4k^2}\quad 1^{\frac{p^2-1}{8}}$$

Jetzt folgt die Gleichheit der beiden Terme in der Aussage wieder durch Einsetzen von 1 3 für p.

Der Schlüssel zur Berechnung von $\frac{q}{p}$ für eine ungerade Primzahl q ist der folgende Satz.

Satz 8.7 (Quadratisches Reziprozitätsgesetz von Gauß) *Seien p q zwei ungerade Primzahlen. Dann gilt*

$$\frac{q}{p} \quad 1 \quad \frac{p\ 1}{2}\cdot\frac{q\ 1}{2} \quad \frac{p}{q}$$

d.h.

$$\frac{q}{p} \quad \begin{cases} \dfrac{p}{q} & \text{für } p \quad q \quad 3 \bmod 4 \\ \dfrac{p}{q} & \text{sonst.} \end{cases}$$

Da das Legendre–Symbol $\frac{p}{q}$ nur von der Restklasse von p und q abhängt, kann man bei seiner Berechnung p durch seinen Rest bei der Division durch q ersetzen. Dadurch erhält man kleinere Werte und man kann die Berechnung nach einigen solchen Schritten abschließen. Wir müssen jedoch unterwegs alle Zahlen faktorisieren, da wir die quadratische Reziprozität nur für Primzahlen kennen.

Beispiel

$$\frac{59}{89} \quad \frac{89}{59} \quad \frac{30}{59} \quad \frac{2\ 3\ 5}{59} \quad \frac{2}{59} \quad \frac{3}{59} \quad \frac{5}{59}$$

$$1 \quad \frac{59}{3} \quad \frac{59}{5} \quad \frac{2}{3} \quad \frac{4}{5} \quad 1 \quad \frac{2\ 2}{5}$$

$$\frac{2}{5}^{\ 2} \quad 1$$

Es gibt zwei bekannte Beweise für das Reziprozitätsgesetz. Einer benützt ein subtiles kombinatorisches Argument und ist zum Beispiel in [F, IV,2] zu finden. Wir führen hier den etwas kürzeren Beweis über das technische Hilfsmittel der Gaußsummen.

Definition 8.8 *Sei p eine ungerade Primzahl und* $\xi \quad \exp\ 2\pi\sqrt{\ 1}\ p$ *eine p–te primitive Einheitswurzel. Dann ist für ein a , a* $0 \bmod p$, *die* Gaußsumme *von a definiert durch*

$$g_a \quad \sum_{i\ 1}^{p\ 1} \quad \frac{i}{p} \quad \xi^{ai}$$

Offensichtlich hängt die Gaußsumme nur von der Restklasse von a modulo p ab. Das nächste Lemma wird zeigen, dass die Gaußsumme g_a das Legendre–Symbol $\frac{a}{p}$ mal dem festen Wert g_1 ist, d.h. im Wesentlichen ist die Gaußsumme das Legendre–Symbol.

Im Folgenden werden wir in dem Ring $\xi \quad {}_{i\ 0}^{p\ 1} \quad \xi^i$ rechnen. Wenn wir ein Element dieses Ringes modulo q betrachten, bedeutet dies, dass wir alle Koeffizienten der ξ^i modulo q betrachten, also im Ring $q \quad \xi \quad {}_{i\ 0}^{p\ 1} \quad q \quad \xi^i$ rechnen.

Lemma 8.9 *Für ungerade Primzahlen $p \quad q \quad$ und $a \quad 0 \bmod p$ gilt:*

1. $g_a \quad \frac{a}{p} \quad g_1$.

2. $g_1^2 \quad \frac{1}{p} \quad p \quad : p$.

3. $g_1^q \quad g_q \bmod q$ *in* $\quad \xi$.

Beweis: Da $\frac{a}{p} \quad \{ \quad 1$ selbstinvers ist, reicht es für die erste Aussage $\frac{a}{p} \quad g_a \quad g_1$ zu zeigen. Nun ist

$$\frac{a}{p} \quad g_a \quad \sum_{i\ 1}^{p\ 1} \quad \frac{a}{p} \quad \frac{i}{p} \quad \xi^{ai} \quad \sum_{i\ 1}^{p\ 1} \quad \frac{ai}{p} \quad \xi^{ai}$$

Da $a \quad 0 \bmod p$, ist $\overline{a} \quad U_p$. Die Linksmultiplikation $\lambda_{\overline{a}} : U_p \quad U_p$ ist ein Isomorphismus mit Inversem $\lambda_{\overline{a}\ 1}$, d.h. wenn $\overline{i}$ alle Elemente $\overline{1}\ \overline{2} \quad \overline{p \quad 1}$ durchläuft, dann durchläuft auch $\overline{ai}$ alle Elemente von U_p. Da sowohl $\frac{ai}{p}$ als auch ξ^{ai} nur von der Restklasse von i modulo p abhängt, können wir die obige Summe umsummieren:

$$\frac{a}{p} \quad g_a \quad \sum_{i\ 1}^{p\ 1} \quad \frac{ai}{p} \quad \xi^{ai} \quad \sum_{l\ 1}^{p\ 1} \quad \frac{l}{p} \quad \xi^l \quad g_1$$

Die zweite Aussage des Satzes folgt durch eine ähnliche Rechnung. Wir bemerken vorweg, dass wegen der Summenformel für die partielle geometrische Reihe für $l \quad 0 \bmod p$ gilt:

$$\sum_{i\ 1}^{p\ 1} \xi^{li} \quad 1 \quad \sum_{i\ 0}^{p\ 1} \xi^{l\ i} \quad 1 \quad \frac{\xi^{l\ p} \quad 1}{\xi^l \quad 1} \quad 1 \quad \frac{\xi^{p\ l} \quad 1}{\xi^l \quad 1} \quad 1$$

Trivialerweise gilt auch

$$\sum_{i\ 1}^{p\ 1} \xi^{pi} \quad \sum_{i\ 1}^{p\ 1} 1 \quad p \quad 1$$

Wir rechnen nun

$$g_1^2 \quad \sum_{i\ 1}^{p\ 1} \frac{i}{p}\ \xi^i \quad \sum_{j\ 1}^{p\ 1} \frac{j}{p}\ \xi^j \quad \sum_{i\ 1}^{p\ 1}\sum_{j\ 1}^{p\ 1} \frac{ij}{p}\ \xi^{i\ j}$$

$$\sum_{i\ 1}^{p\ 1}\sum_{l\ 1}^{p\ 1} \frac{i^2 l}{p}\ \xi^{i\ il} \quad \text{(Umsummierung mit } j \quad il\text{)}$$

$$\sum_{l\ 1}^{p\ 1} \frac{l}{p} \sum_{i\ 1}^{p\ 1} \xi^{i\ 1\ l} \quad \text{(Satz 8.5.5)}$$

$$\sum_{l\ 1}^{p\ 2} \frac{l}{p} \quad 1 \quad \frac{p\ 1}{p} \quad p \quad 1 \quad \text{(Vorangehende Bemerkung)}$$

$$\frac{p\ 1}{p}\ p \sum_{l\ 1}^{p\ 1} \frac{l}{p} \quad \frac{1}{p}\ p \quad \text{(Lemma 8.3).}$$

Um die letzte Aussage des Lemmas zu beweisen, benutzen wir wieder Hilfssatz 4.6 beim Potenzieren von g_1^q modulo q

$$g_1^q \quad \sum_{i\ 1}^{p\ 1} \frac{i}{p}\ \xi^i \Bigg)^q \quad \sum_{i\ 1}^{p\ 1} \frac{i}{p}\ \xi^i \Bigg)^q \quad \sum_{i\ 1}^{p\ 1} \frac{i}{p} \Bigg)^q \xi^{iq}$$

$$\sum_{i\ 1}^{p\ 1} \frac{i}{p}\ \xi^{iq} \quad g_q \mod q$$

Beweis (Reziprozitätsgesetz): Wir berechnen $g_q \bmod q$ auf zwei Arten

$$\frac{q}{p}\ g_1 \quad g_q \quad g_1^q \quad g_1\ g_1^2\ ^{\frac{q\ 1}{2}} \quad g_1\ p\ ^{\frac{q\ 1}{2}} \quad g_1\ \frac{p}{q} \mod q$$

Multiplizieren wir noch mit g_1, so erhalten wir

$$\frac{q}{p}\ p \quad \frac{q}{p}\ g_1^2 \quad \frac{p}{q}\ g_1^2 \quad \frac{p}{q}\ p \mod q$$

Jetzt sind alle auftretenden Terme ganze Zahlen. Wegen $p \quad 0 \bmod q$ können wir es wegkürzen um

$$\frac{q}{p} \quad \frac{p}{q} \quad \frac{1\ ^{\frac{p\ 1}{2}} p}{q} \quad \frac{1}{q}\ ^{\frac{p\ 1}{2}}\ \frac{p}{q} \quad 1\ ^{\frac{q\ 1}{2}\ \frac{p\ 1}{2}}\ \frac{p}{q}$$

$$1\ ^{\frac{p\ 1}{2}\cdot\frac{q\ 1}{2}}\ \frac{p}{q} \mod q$$

zu bekommen. Da sämtliche auftretenden Terme 1 oder 1 sind, handelt es sich hier nicht nur um eine Kongruenz, sondern um eine Gleichheit.

Das Aufwändigste bei der Berechnung des Legendre–Symbols $\frac{59}{89}$ im Beispiel war, dass man alle auftretenden Zahlen faktorisieren musste. Dies vermeidet man durch die Einführung des Jacobi–Symbols.

Definition 8.10 *Sei n eine ungerade natürliche Zahl und $n \quad \prod_{i \ 1}^{s} q_i^{r_i}$ ihre Primfaktorzerlegung. Dann ist das* Jacobi–Symbol *als*

$$\frac{a}{n} \quad \prod_{i \ 1}^{s} \frac{a}{q_i}^{r_i}$$

definiert.

Warnung Falls a ein quadratischer Rest modulo n ist, ist das Jacobi–Symbol 1. Die Umkehrung gilt jedoch nicht!

Aufgabe 8.11 Finden Sie dazu Beispiele.

Die Eigenschaften des Legendre–Symbols vererben sich auf das Jacobi–Symbol. So hängt es nur von a modulo n ab und ist multiplikativ in a. Seine Multiplikativität in n folgt direkt aus der Definition. Es gilt die folgende Version des Reziprozitätsgesetzes:

Satz 8.12 (Reziprozitätsgesetz für das Jacobi–Symbol) *Seien $m \quad n \quad 3$ ungerade natürliche Zahlen. Dann gilt*

1. $\frac{1}{n} \qquad 1 \ ^{\frac{n \ 1}{2}}$.
2. $\frac{2}{n} \qquad 1 \ ^{\frac{n^2 \ 1}{8}}$.
3. $\frac{m}{n} \qquad 1 \ ^{\frac{m \ 1}{2} \cdot \frac{n \ 1}{2}} \ \frac{n}{m}$.

Beweis: Nach den bisherigen Ergebnissen gilt der Satz, falls n und m Primzahlen sind. Da das Jacobi–Symbol $\frac{n}{m}$ multiplikativ in n und m ist, reicht es für den Beweis des Satzes aus, zu zeigen, dass auch $1 \ ^{\frac{n \ 1}{2}}$, $1 \ ^{\frac{n^2 \ 1}{8}}$ und $1 \ ^{\frac{n \ 1}{2} \cdot \frac{m \ 1}{2}}$ für ungerade natürliche Zahlen multiplikativ in n und m sind. Die Multiplikativität von $1 \ ^{\frac{n \ 1}{2}}$ bedeutet

$$1 \ ^{\frac{n_1 n_2 \ 1}{2}} \qquad 1 \ ^{\frac{n_1 \ 1}{2}} \qquad 1 \ ^{\frac{n_2 \ 1}{2}} \qquad 1 \ ^{\frac{n_1 \ n_2 \ 2}{2}}$$

Wir müssen also $n_1 n_2 \quad 1 \quad n_1 \quad n_2 \quad 2 \bmod 4$ für ungerade Zahlen n_1 und n_2 beweisen. Dies ist äquivalent zu $n_1 n_2 \quad n_1 \quad n_2 \quad 1 \quad 0 \bmod 4$ oder $n_1 \quad 1 \quad n_2 \quad 1 \quad 0 \bmod 4$. Letzteres gilt, weil $n_1 \quad 1 \quad n_2 \quad 1 \quad 0 \bmod 2$.

Analog müssen wir für die Multiplikativität von $1 \ ^{\frac{n^2 \ 1}{8}}$, d.h.

$$1 \ ^{\frac{n_1 n_2 \ ^2 \ 1}{8}} \qquad 1 \ ^{\frac{n_1^2 \ 1}{8}} \qquad 1 \ ^{\frac{n_2^2 \ 1}{8}} \qquad 1 \ ^{\frac{n_1^2 \ n_2^2 \ 2}{8}}$$

$n_1^2 n_2^2 \quad 1 \quad n_1^2 \quad n_2^2 \quad 2 \bmod 16$ für ungerade $n_1 \ n_2$ zeigen. Äquivalent dazu sind $n_1^2 n_2^2 \quad n_1^2 \quad n_2^2 \quad 1 \quad 0 \bmod 16$, $n_1^2 \quad 1 \quad n_2^2 \quad 1 \quad 0 \bmod 16$ oder schließlich $n_1 \quad 1 \quad n_1 \quad 1 \quad n_2 \quad 1 \quad n_2 \quad 1 \quad 0 \bmod 16$. Letzteres gilt wiederum, weil $n_1 \quad 1 \quad n_1 \quad 1 \quad n_2 \quad 1 \quad n_2 \quad 1 \quad 0 \bmod 2$.

Die Bimultiplikativität von $1^{\frac{n_1-1}{2}\cdot\frac{m_1-1}{2}}$ folgt aus der Multiplikativität von $1^{\frac{n_1-1}{2}}$.

Die Berechnung des Jacobi–Symbols läuft nun ähnlich wie die Berechnung des größten gemeinsamen Teilers. Man muss höchstens noch die Faktoren -1 und 2 in den Schritten abspalten, um für die Anwendung des Reziprozitätsgesetzes auf ungerade natürliche Zahlen zu kommen.

Beispiel

$$\frac{59}{89}\quad\frac{89}{59}\quad\frac{30}{59}\quad\frac{2\ 15}{59}\quad\frac{2}{59}\quad\frac{15}{59}\quad 1\quad\frac{59}{15}$$

$$\frac{14}{15}\quad\frac{2}{15}\quad\frac{7}{15}\quad 1\quad\frac{15}{7}\quad\frac{1}{7}\quad 1$$

In diesem Beispiel hätte man durch Benutzung von

$$\frac{14}{15}\quad\frac{1}{15}\quad 1$$

die Rechnung abkürzen können.

Aufgabe 8.13 Berechnen Sie die Jacobi–Symbole $\frac{37}{859}$ und $\frac{10270}{25511}$.

Aufgabe 8.14 Zeigen Sie: Es gilt $\frac{41}{51}\quad 1$, aber 41 ist kein quadratischer Rest modulo 51.

Mit Hilfe des Jacobi–Symbols und des Reziprozitätssatzes können wir jetzt schnell entscheiden, ob d ein quadratischer Rest modulo p ist. Natürlich wäre es wünschenswert, wenn wir auch schnell die Wurzel aus d in $\mathbb{F}_p$ ziehen könnten. Bisher können wir die Wurzel finden, indem wir eine Primitivwurzel ζ modulo p suchen und dann $\exp_\zeta\ \frac{1}{2}\log_\zeta d$ berechnen, wobei jedoch die Berechnung von $\log_\zeta d$ sehr langsam ist.

In einem Fall ist das Wurzelziehen sehr einfach:

Lemma 8.15 *Sei p eine Primzahl mit $p \quad 3 \bmod 4$ und d ein quadratischer Rest modulo p. Dann ist $d^{\frac{p-1}{4}}$ eine Lösung von $x^2 \quad d \bmod p$.*

Beweis:

$$d^{\frac{p-1}{4}\ 2} \quad d^{\frac{p-1}{2}} \quad d^{\frac{p-1}{2}}\ d \quad \frac{d}{p}\ d \quad d \mod p$$

Im *Algorithmus von Tonelli und Shanks* wird dieses Lemma auf andere Primzahlen angepasst. Sei $p \quad 1 \quad 2^e\ q$ für $e\ q$ und q ungerade. Man berechnet $a : \quad d^{\frac{q-1}{2}} \bmod p$ als Approximation für die Lösung der Gleichung $x^2 \quad d \bmod p$. (Im Spezialfall ist $\frac{q-1}{2} \quad \frac{p-1}{4}$.)

Welchen Fehler machen wir dabei? Es gilt

$$\frac{d}{a^2} \quad \frac{d}{d^{\frac{q\ 1}{2}\ 2}} \quad d^{1\ \frac{2\ q\ 1}{2}} \quad d^{\ q}$$

Nach dem Satz 5.17 von Euler ist $d\ a^{2\ 2^e} \quad d^{\ 2^e q} \quad 1\ d^{p\ 1} \quad 1 \bmod p$, d.h. die Ordnung von $d\ a^2$ in U_p ist eine Zweierpotenz. Untersuchen wir daher die Elemente in U_p, deren Ordnung eine Zweierpotenz ist. Wir haben die Isomorphismen $U_p \quad p \quad 1 \quad 2^e \quad q$. Da 2 eine Einheit in $\quad q$ ist, kann für ein Element $x\ y \quad 2^e \quad q$ nur dann $2^e \quad x\ y \quad 2^e x\ 2^e y \quad 0$ gelten, wenn $y \quad 0$ ist. Daher liegt jedes Element, dessen Ordnung eine Zweierpotenz ist, in der Untergruppe H von U_p, die unter dem Isomorphismus $\quad 2^e \quad 0$ entspricht. Insbesondere liegt also $d\ a^2$ in H.

Der nächste Schritt ist das Auffinden eines Erzeugers von H. Dies geschieht ähnlich wie bei der Suche nach einer Primitivwurzel modulo p. Man wählt zufällig eine Zahl $x \quad , 0 \quad x \quad p$, und setzt $\vartheta : \quad x^q$. Dann gilt $\operatorname{ord} \vartheta \ 2^e$. Nun testet man, ob ϑ ein Erzeuger von H ist, also ob $\operatorname{ord} \vartheta \quad 2^e$ ist, indem man $\vartheta^{2^{e\ 1}} \quad \exp_\vartheta 2^{e\ 1} \bmod p$ berechnet. Falls dies 1 modulo p ist, ist dies nicht der Fall. Man wählt dann einfach ein neues x und fängt von vorne an. Weil dabei $2^{e\ 1}q$ der $2^e q$ Elemente eine gute Wahl für x sind, wird man dies im Allgemeinen nicht sehr häufig wiederholen müssen.

Da $d\ a^2 \quad H$ ist, gibt es also ein $l \quad , 0 \quad l \quad 2^e$ mit $d\ a^2 \quad \vartheta^l \quad \exp_\vartheta l \bmod p$. Wir könnten das l wie mit dem „baby steps – giant steps“ Algorithmus bestimmen, aber hier gibt es eine bessere Möglichkeit, weil die Ordnung der Gruppe eine Zweierpotenz ist. Wir schreiben nun l in seiner Binärdarstellung $l \quad \sum_{i\ 0}^{e\ 1} l_i 2^i$ mit $l_i \quad \{0\ 1 \quad$ und nehmen an, wir hätten $l_0 \quad l_{s\ 1}$ schon bestimmt. Da $\exp_\vartheta \ 2^{e\ 1}$ in H die Ordnung 2 besitzt, ist es gleich 1. Damit berechnen wir

$$\frac{d}{a^2} \ \exp_\vartheta \quad \sum_{i\ 0}^{s\ 1} l_i 2^i \qquad \exp_\vartheta \quad \sum_{i\ s}^{e\ 1} l_i 2^i$$

$$\exp_\vartheta \ l_s 2^{e\ 1} \quad \exp_\vartheta \quad 2^e \quad \sum_{i\ s\ 1}^{e\ 1} l_i 2^{i\ s\ 1}$$

$$\exp_\vartheta \ 2^{e\ 1\ l_s} \qquad 1^{\ l_s} \quad \bmod p$$

l_s ist genau dann gleich 1, falls dieser Wert ungleich 1 modulo p ist. Auf diese Weise können wir also l bestimmen.

Da $d\ a^2$ ein Quadrat ist, muss l gerade sein. Wir finden damit $d \quad a\vartheta^{\frac{l}{2}\ 2} \bmod p$, d.h $a\vartheta^{\frac{l}{2}}$ ist eine gesuchte Lösung von $x^2 \quad d \bmod p$.

Beispiel Wir wollen $x^2 \quad 5 \bmod 89$ lösen. Es gilt $89 \quad 1 \quad 2^3 \quad 11$. Wir finden $a : \quad 5^{\frac{11\ 1}{2}}$ $5^6 \quad 50 \bmod 89$ als approximative Lösung. Tatsächlich ist $50^2 \quad 8 \bmod 89$. Wir suchen daher nach einem Erzeuger der 8–elementigen Untergruppe von U_{89}, deren Elemente Zweierpotenzen als Ordnungen haben. Versuchen wir es mit $\vartheta : \quad 3^{11} \quad 37 \bmod 89$. Dies ist tatsächlich ein Erzeuger, da $\vartheta^4 \quad 1 \quad 1 \bmod 89$. Als Ansatz für l haben wir $l_0 \quad 2l_1 \quad 4l_2$. Wegen $d\ a^{2\ 4} \quad 5\ 50^{2\ 4} \quad 1 \bmod 89$ ist $l_0 \quad 0$ und a wirklich ein quadratischer Rest. Da

$d\ a^{2\ 2}\quad 1 \bmod 89$, ist $l_1\quad 1$. Schließlich folgt aus $d\quad a^2\vartheta^{2\ 1}\quad 1 \bmod 89$, dass $l_2\quad 0$. Also ist $l\quad 2$ und $a\vartheta^{\frac{2}{2}}\quad 70 \bmod 89$ eine Lösung von $x^2\quad 5 \bmod 89$.

Aufgabe 8.16 Berechnen Sie die Lösungen von $x^2\quad 56 \bmod 113$.

Aufgabe 8.17 Man kann dieses Verfahren anpassen, um auch eine k–te Wurzel aus d zu finden. Dann schreibt man $p\quad 1\quad k^e q$ mit ggT $k\ q\quad 1$. Als Approximation verwendet man $a:\quad d^t$, wobei $t\quad$ so gewählt ist, dass $k\ t\quad 1 \bmod q$. Schließlich verwendet man eine k–Darstellung $l\quad \sum_i^e{}_0^1 l_i k^i$. Führen Sie die Details aus. Wir finden dabei jedoch nur eine k–te Wurzel von d. Zeigen Sie nun: Ist a eine k–te Wurzel von d, dann ist b genau dann eine weitere k–te Wurzel von d, wenn $b\ a$ eine k–te Einheitswurzel ist, also $b\ a^{\ k}\quad 1$ gilt. Die k–ten Einheitswurzeln lassen sich leicht durch die „log–exp" Methode am Ende von Abschnitt 7 finden, da der Logarithmus von 1 Null ist und daher nicht mehr berechnet zu werden braucht.

Zusatzaufgaben

Aufgabe 8.18 Berechnen Sie mit dem Algorithmus von Tonelli und Shanks jeweils eine Lösung der Kongruenzen

$$x^2\quad 6 \mod 43 \qquad \text{bzw.} \qquad x^2\quad 881 \mod 4073$$

Aufgabe 8.19 Sei $p\quad 3$ prim und $a\ b\ c\quad$ mit $p\quad a$. Zeigen Sie: Die Anzahl der Lösungen der Gleichung $ax^2\quad bx\quad c\quad 0 \bmod p$ in $\quad p\quad$ ist (mit geeigneter Vielfachheit) gegeben durch $1\quad \frac{\Delta}{p}$, wobei $\Delta\quad b^2\quad 4ac$.

Aufgabe 8.20 Sei $p\quad 3$ prim. Zeigen Sie: $\frac{3}{p}\quad 1$ genau dann, wenn $p\quad 1 \bmod 6$.

Aufgabe 8.21 Sei $p\quad 3$ prim. Zeigen Sie: $\frac{3}{p}\quad 1$ genau dann, wenn $p\quad 1 \bmod 12$ oder $p\quad 11 \bmod 12$.

Aufgabe 8.22 Sei $p\quad 3$ prim. Zeigen Sie: $\frac{2}{p}\quad 1$ genau dann, wenn $p\quad 1 \bmod 8$ oder $p\quad 3 \bmod 8$.

Aufgabe 8.23 Bestimmen Sie ein $m\quad$ so, dass die Funktion $p\quad \frac{75}{p}\quad$ für $p\quad 3$ prim nur von der Restklasse $p \bmod m$ abhängt.

Aufgabe 8.24 Zeigen Sie: Ist eine Primzahl $p\quad$ von der Form $p\quad 1 \bmod 8$, so gibt es $a\ b\quad$ mit $a^2\quad 2b^2\quad 0 \bmod p$.

Aufgabe 8.25 Bestimmen Sie die Jacobi–Symbole $\frac{3991}{5863}$ und $\frac{1024}{173}$.

Aufgabe 8.26 Überprüfen Sie, ob die Gleichung $x^2\quad 6314 \bmod 10403$ eine Lösung besitzt.

Aufgabe 8.27 Für welche ungeraden Primzahlen p hat die Kongruenz $a^2\quad b^2\quad 1 \bmod p$ eine durch 8 teilbare Anzahl von Lösungen $a\ b\quad U_p\quad U_p$?

9 Quadratsätze

In diesem Abschnitt werden wir zeigen, welche Zahlen als Summe von zwei Quadraten geschrieben werden können. Wir werden sehen, dass auch drei Quadrate nicht ausreichen, um jede Zahl darzustellen, sondern dies erst mit vier Quadraten möglich ist.

Wenden wir uns zuerst bei dem Zwei–Quadrate Problem den Primzahlen zu.

Satz 9.1 *Eine Primzahl p kann genau dann als Summe zweier Quadrate geschrieben werden $p = x^2 + y^2; x, y \in \mathbb{N}_0$, wenn $p \equiv 3 \bmod 4$.*

Beweis: Natürlich ist $2 = 1^2 + 1^2$. Modulo 4 sind alle Quadrate $0^2 \equiv 0$, $1^2 \equiv 3^2 \equiv 1$ und $2^2 \equiv 0$. Daher muss für ein $p = x^2 + y^2$ entweder $p \equiv 1 \bmod 4$ oder $p \equiv 0 \bmod 2$ gelten.

Wir zeigen nun, dass eine Primzahl p mit $p \equiv 1 \bmod 4$ als Summe zweier Quadrate darstellbar ist. Nach Lemma 7.14 gibt es ein a mit $a^2 \equiv -1 \bmod p$. Daher können wir ein k mit $a^2 + 1 = kp$ finden. Schauen wir uns diese Gleichung in dem Ring $\mathbb{Z}[i]$ an. Hier gilt

$$a^2 + 1 = (a + i)(a - i) = kp$$

Sei $x + iy = \text{ggT}(a + i, p)$. Wir behaupten, dass

$$p = N(x + iy) = x^2 + y^2$$

gilt. Damit wäre dann der Satz bewiesen.

Aus $x + iy \mid p$ folgt $N(x + iy) \mid N(p) = p^2$. Wir müssen die Fälle $N(x + iy) = 1$ oder p^2 ausschließen. Nehmen wir $N(x + iy) = p^2$ an. Wegen $x + iy \mid p$ gibt es ein $z = u + iv$ mit $p = (x + iy)z$. Anwenden der Norm–Funktion ergibt

$$p^2 = N(p) = N(x + iy)N(z) = p^2 N(z)$$

Daher ist $N(z) = 1$ und $z = u + iv \in \{1, -1, i, -i\}$. Es folgt $x = 0$ oder $y = 0$, was wegen $x + iy \mid a + i$ unmöglich ist.

Nehmen wir nun $N(x + iy) = 1$ an, d.h. $a + i$ und p sind teilerfremd. Da p keine Einheit ist, hat es einen Primteiler. Nach muss dieser $a + i$ oder $a - i$ teilen. Nach eventueller Konjugation dieses Teilers dürfen wir annehmen, dass er $a + i$ teilt. Dies ist aber ein Widerspruch zur Teilerfremdheit von $a + i$ und p.

Korollar 9.2 (Zwei–Quadrate–Satz) *Eine natürliche Zahl n ist die Summe von zwei Quadraten genau dann, wenn in ihrer Primfaktorzerlegung die Primzahlen p mit $p \equiv 3 \bmod 4$ nur mit geraden Exponenten vorkommen.*

S. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie,*
DOI 10.1007/978-3-8348-8263-9_9,

Beweis: Falls die Bedingung an die Primfaktorzerlegung erfüllt ist, können wir wegen Satz 9.1 und der Formel $p^2 \quad p^2 \quad 0^2$ die Zahl n in ein Produkt von Zahlen zerlegen, die selber alle die Summe von zwei Quadraten sind. Es reicht also aus, zu zeigen: Wenn $n \quad x^2 \quad y^2$ und $m \quad a^2 \quad b^2$, dann ist auch nm die Summe zweier Quadrate. Dies folgt unter Zuhilfenahme des Ringes i und seiner Norm–Funktion sofort:

$$nm \quad x^2 \quad y^2 \quad a^2 \quad b^2 \quad N\, x \quad iy \quad N\, a \quad ib \quad N \quad x \quad iy \quad a \quad ib$$
$$N \quad xa \quad yb \quad i\, ay \quad xb \quad xa \quad yb\ ^2 \quad ay \quad xb\ ^2$$

Nehmen wir nun an, die Bedingung an die Primfaktorzerlegung von n sei nicht erfüllt, aber es gelte trotzdem $n \quad x^2 \quad y^2$. Dann können wir $n \quad mp^{2k \quad 1}$ für ein $p \quad$ mit $p \quad 3 \bmod 4$ und ggT $m\ p \quad 1$ schreiben, also

$$x^2 \quad y^2 \quad mp^{2k \quad 1}$$

Wir dürfen weiter annehmen, dass $p \quad y$ gilt. Denn wenn $p\, y$, dann folgt $p\, x$, und wir können die ganze Gleichung durch p^2 dividieren. Modulo p folgt aus dieser Gleichung jetzt $x^2 \quad y^2 \bmod p$ oder äquivalent dazu $x\ y\ ^2 \quad 1 \bmod p$. Dies ist aber nach Lemma 7.14 unmöglich.

Aufgabe 9.3 Stellen Sie die Zahlen 178, 373 und 4797 als Summe von zwei Quadraten dar, indem sie den obigen konstruktiven Beweisen folgen.

Der folgende Drei–Quadrate–Satz ist wesentlich schwieriger zu beweisen als der Zwei–Quadrate–Satz oder der Vier–Quadrate–Satz, weil hier nicht mehr gilt, dass aus Darstellungen von n und m eine Darstellung von nm gefunden werden kann. Tatsächlich gibt es gar nicht immer eine solche Darstellung.

Satz 9.4 (Drei–Quadrate–Satz) *Eine natürliche Zahl n ist die Summe dreier Quadrate genau dann, wenn sie nicht von der Form* $n \quad 4^i\ 7 \quad 8k$ *für* $i\ k \quad _0$ *ist.*

Beweis: (Hier nur die Notwendigkeit der Bedingung, vollständiger Beweis am Ende des Abschnittes 15.) Wir zeigen zuerst, dass n genau dann die Summe dreier Quadrate ist, wenn $4n$ dies ist. Aus $n \quad x^2 \quad y^2 \quad z^2$ folgt offensichtlich $4n \quad 2x\ ^2 \quad 2y\ ^2 \quad 2z\ ^2$. Nehmen wir nun $4n \quad x^2 \quad y^2 \quad z^2$ an. Wir wollen zeigen, dass x, y und z alle gerade sind. Betrachten wir die Gleichung modulo 8. Die Quadrate modulo 8 sind 0, $1\ ^2 \quad 1$, $2\ ^2 \quad 4$, $3\ ^2 \quad 1$ und $4^2 \quad 0$. Da $4n$ modulo 8 entweder 0 oder 4 ist, können bei den vorhandenen Möglichkeiten für die Quadrate nur Quadrate auftauchen, die 0 oder 4 modulo 8 sind. Also sind diese Quadrate durch 4 teilbar und damit sind die Zahlen gerade.

Wir beweisen nun, dass ein n mit $n \quad 7 \bmod 8$ nicht die Summe dreier Quadrate sein kann. Das folgt wieder durch Betrachten der Gleichung $n \quad x^2 \quad y^2 \quad z^2$ modulo 8. Wie oben bemerkt treten nur die Zahlen 0, 1 und 4 modulo 8 als Quadrate auf. Keine Summe von drei solchen Zahlen kann 7 ergeben, daher muss $n \quad 7 \bmod 8$ sein.

Wir kommen jetzt zum Vier–Quadrate–Satz. Die Zutaten zum Beweis sind die gleichen wie beim Beweis des Zwei–Quadrate–Satzes. Besonders wichtig ist, dass es hier eine Analogie zu

den Gaußschen Zahlen gibt. Anstatt den ganzen Zahlen in den komplexen Zahlen nutzen wir die ganzen Zahlen innerhalb der Quaternionen. Dies ist die von Hamilton entdeckte nicht–kommutative vierdimensionale –Algebra

$$\mathbb{H}: \quad \{x \quad x_0 \quad x_1 i \quad x_2 j \quad x_3 k \quad x_i$$

Die –lineare Multiplikation von Elementen aus $\mathbb{H}$ ist festgelegt durch

$$i^2 \quad j^2 \quad k^2 \qquad 1 \qquad ij \qquad ji \quad k \qquad jk \qquad kj \quad i \quad \text{und} \quad ki \qquad ik \quad j$$

Die Konjugation ist hier erklärt durch

$$\overline{x} \quad x_0 \quad x_1 i \quad x_2 j \quad x_3 k$$

Es gilt $\overline{xy} \quad \overline{y} \ \overline{x}$, da dies für die Basiselemente $1 \ i \ j \ k$ gilt und die Gleichung auf beiden Seiten –bilinear ist. Analog zu den Gaußschen Zahlen erklären wir die Norm als

$$N \ x \qquad x\overline{x} \quad x_0^2 \quad x_1^2 \quad x_2^2 \quad x_3^2$$

Die Norm ist wieder multiplikativ:

$$N \ xy \qquad xy\overline{xy} \quad xy\overline{y}\,\overline{x} \quad x \ y\overline{y} \ \overline{x} \qquad x\overline{x} \ \ y\overline{y} \qquad N \ x \ N \ y$$

wobei wir $y\overline{y} \qquad$ genutzt haben. Ausgeschrieben bedeutet dies:

$$\begin{array}{cccccccc} x_0^2 & x_1^2 & x_2^2 & x_3^2 & y_0^2 & y_1^2 & y_2^2 & y_3^2 \\ x_0y_0 & x_1y_1 & x_2y_2 & x_3y_3 & ^2 & x_0y_1 & x_1y_0 & x_2y_3 \quad x_3y_2 \ ^2 \\ x_0y_2 & x_2y_0 & x_1y_3 & x_3y_1 & ^2 & x_0y_3 & x_3y_0 & x_1y_2 \quad x_2y_1 \ ^2 \end{array}$$

d.h., falls n und m jeweils die Summe von vier Quadraten sind, ist auch nm von diesem Typ.

Anstatt des Lemmas 7.14 benötigen wir:

Lemma 9.5 *Für jede Primzahl p gibt es eine Lösung der Gleichung*

$$x^2 \quad y^2 \qquad 1 \quad \mathrm{mod}\ p$$

mit $x \ y$.

Beweis: Für $p \quad 2$ und $p \quad 1 \bmod 4$ können wir $y \quad 0$ wählen und eine Lösung für x durch das Lemma 7.14 finden.

Sei nun $p \quad 3 \bmod 4$. Nach Lemma 7.14 ist in diesem Fall $\quad 1$ ein quadratischer Nichtrest modulo p. Nun sind die $y^2, y \qquad$, alle quadratischen Nichtreste modulo p. Denn die Multiplikativität des Jacobisymbols impliziert, dass das Produkt zweier quadratischer Nichtreste ein quadratischer Rest ist, daher ist jeder Nichtrest mal $\quad 1$ von der Form y^2 modulo p.

Betrachten wir $x^2 \quad 1$. Falls dies für alle $x \qquad$ quadratische Reste wären, wäre mit jedem quadratischen Rest auch sein Nachfolger ein quadratischer Rest, und es gäbe nur quadratische Reste, was unmöglich ist. Es gibt also ein x, so dass $x^2 \quad 1$ ein quadratischer Nichtrest und daher von der Form $\quad y^2$ modulo p ist. Also gilt $x^2 \quad 1 \qquad y^2 \bmod p$ oder äquivalent dazu $x^2 \quad y^2 \qquad 1 \bmod p$.

Satz 9.6 (Lagrange) *Jede natürliche Zahl ist als Summe von vier Quadraten darstellbar.*

Beweis: Nach den Vorbemerkungen reicht es aus, zu zeigen, dass jede Primzahl p die Summe von vier Quadraten ist. Wir dürfen p ungerade annehmen. Nach Lemma 9.5 hat die Gleichung

$$x_0^2 \quad x_1^2 \quad x_2^2 \quad x_3^2 \quad 0 \mod p \qquad \text{für } x_i$$

eine Lösung des Typs $x\ y\ 1\ 0$ mit $x\ y$. Wir können $x\ y$ so wählen, dass $x \quad y \quad p\ 2$ ist, dann gilt $x^2 \quad y^2 \quad 1^2 \quad 0^2 \quad p^2\ 4 \quad p^2\ 4 \quad 1 \quad p^2$. Dies wollen wir in der folgenden Form festhalten: Es gibt x_i und k mit $0 \quad k \quad p$, so dass

$$x_0^2 \quad x_1^2 \quad x_2^2 \quad x_3^2 \quad kp$$

Wir benutzen nun die Beweismethode des Abstiegs: Falls $k \quad 1$ ist, sind wir fertig. Falls nicht zeigen wir, dass wir die x_i so verändern können, dass die Gleichung auch mit einem kleineren k gilt. Mehrfaches Wiederholen dieses Schrittes führt dann schließlich zu $k \quad 1$.

Sei also $k \quad 1$. Falls k gerade ist, müssen von den x_i keines, zwei oder alle vier gerade sein. Wir nummerieren sie so um, dass x_0 und x_1 bzw. x_2 und x_3 entweder beide gerade oder ungerade sind. Dann erhalten wir die folgende Gleichung mit nur ganzen Zahlen:

$$\frac{x_0 \quad x_1}{2}^2 \quad \frac{x_0 \quad x_1}{2}^2 \quad \frac{x_2 \quad x_3}{2}^2 \quad \frac{x_2 \quad x_3}{2}^2 \quad \frac{k}{2}p$$

Falls k ungerade ist, wählen wir y_i mit

$$y_0 \quad x_0 \mod k \quad y_i \quad x_i \mod k \quad \text{für} \quad 1 \quad i \quad 3 \quad \text{und} \quad y_i \quad k\ 2$$

Es gilt $\sum_i^3 {}_0 y_i^2 \quad k^2$. Mit $\sum y_i^2 \quad \sum x_i^2 \quad 0 \mod k$ folgt $\sum y_i^2 \quad k'k$ mit einem $k' \quad k$. Wir müssen $k' \quad 1$ sicherstellen. Angenommen $k' \quad 0$, dann muss $y_0 \quad y_3 \quad 0$ sein. Folglich gilt $x_i \quad 0 \mod k \quad x_i^2 \quad 0 \mod k^2$, also $0 \quad \sum x_i^2 \quad kp \mod k^2$. Dies impliziert $k \ p$, was aber wegen $1 \quad k \quad p$ und p prim unmöglich ist.

Einsetzen von x_i und y_i in die Formel für die Multiplikativität der Norm ergibt:

$$\begin{aligned} k^2k'p \quad & x_0^2 \quad x_1^2 \quad x_2^2 \quad x_3^2 \quad y_0^2 \quad y_1^2 \quad y_2^2 \quad y_3^2 \\ & x_0y_0 \quad x_1y_1 \quad x_2y_2 \quad x_3y_3^{\ 2} \quad x_0y_1 \quad x_1y_0 \quad x_2y_3 \quad x_3y_2^{\ 2} \\ & x_0y_2 \quad x_2y_0 \quad x_1y_3 \quad x_3y_1^{\ 2} \quad x_0y_3 \quad x_3y_0 \quad x_1y_2 \quad x_2y_1^{\ 2} \end{aligned}$$

Nun gilt wegen der Kongruenzbedingungen zwischen den x_i und y_i

$$\begin{aligned} & x_0y_1 \quad x_1y_0 \quad x_2y_3 \quad x_3y_2 \quad x_0x_1 \quad x_1 \quad x_0 \quad x_2x_3 \quad x_3x_2 \quad 0 \mod k \\ & x_0y_2 \quad x_2y_0 \quad x_1y_3 \quad x_3y_1 \quad x_0x_2 \quad x_2 \quad x_0 \quad x_1x_3 \quad x_3x_1 \quad 0 \mod k \\ & x_0y_3 \quad x_3y_0 \quad x_1y_2 \quad x_2y_1 \quad x_0x_3 \quad x_3 \quad x_0 \quad x_1x_2 \quad x_2x_1 \quad 0 \mod k \end{aligned}$$

daher sind die letzten drei Quadrate in der vorangehenden Formel alle durch k^2 teilbar. Damit ist auch das erste Quadrat durch k^2 teilbar. Wir können also die ganze Gleichung termweise durch k^2 teilen und erhalten eine Gleichung des Typs mit einem $1 \quad k' \quad k$.

Zusatzaufgaben

Aufgabe 9.7 Finden Sie die kleinsten Zahlen n , die sich auf zwei bzw. drei wesentlich verschiedene Weisen als Summe zweier Quadrate darstellen lassen. Warum ist die Quadratsummendarstellung bei zusammengesetzten Zahlen im Allgemeinen nicht eindeutig?

Aufgabe 9.8 Stellen Sie die Zahlen 260, 882, 5525 und 5929 als Summen zweier Quadrate dar.

Aufgabe 9.9 Beweisen Sie auch den Zwei–Quadrate–Satz durch eine Abstiegsmethode.

Aufgabe 9.10 Beweisen Sie den Zwei– und Vier–Quadrate–Satz unter Verwendung des *Gitterpunktsatzes von Minkowski* (siehe Anhang D):

Sei Γ ein vollständiges Gitter in ^{n} mit Fundamentalbereich F. Weiter sei M eine beschränkte, messbare, konvexe und symmetrische Teilmenge im ^{n}. Falls

$$\text{vol } M \quad 2^n \text{vol } F$$

so enthält M einen Punkt aus Γ $\{0$. Die gleiche Aussage gilt auch, falls M kompakt, konvex und symmetrisch ist und

$$\text{vol } M \quad 2^n \text{vol } F$$

Aufgabe 9.11 Bekanntlich besagt die *Vermutung von Fermat*, dass für jede natürliche Zahl n 2 und $x\ y\ z$ gilt

$$x^n \quad y^n \quad z^n \qquad xyz \quad 0$$

Der Satz soll hier für den Fall n 4 bewiesen werden. Genauer gesagt beweisen wir die etwas stärkere Aussage, dass $x^4 \quad y^4 \quad z^2$ nur Lösungen mit $xyz \quad 0$ besitzt.

1. Zeigen Sie zunächst: Gilt die Aussage für jedes *teilerfremde* Tripel $x\ y\ z$ ganzer Zahlen, dann gilt sie auch für beliebige Tripel.

2. Sei nun $x\ y\ z$ ein teilerfremdes Tripel ganzer Zahlen mit $x^4 \quad y^4 \quad z^2, xyz \quad 0$. Dann gibt es nach evtl. Vertauschung von x und y teilerfremde $p\ q$ mit $p \quad q \mod 2$, $p \quad q \quad 0$ und
$$x^2 \quad 2pq \quad y^2 \quad p^2 \quad q^2 \quad z \quad p^2 \quad q^2$$

3. Zeigen Sie, dass für die Zahlen $p\ q$ aus Teil 2 gilt: Es gibt teilerfremde $a\ b$ mit $a \quad b \mod 2$, $a \quad b \quad 0$, so dass
$$q \quad 2ab \quad y \quad a^2 \quad b^2 \quad p \quad a^2 \quad b^2$$

4. Zeigen Sie, dass ab und $a^2 \quad b^2$ und somit auch $a\ b$ Quadrate in sind.

5. Sei $a \quad X^2, b \quad Y^2$ und $a^2 \quad b^2 \quad Z^2$ mit $X\ Y\ Z$. Verwenden Sie das Tripel $X\ Y\ Z$, um durch ein Abstiegsargument die Vermutung von Fermat für n 4 zu beweisen.

6. Zeigen Sie: Ist die Vermutung von Fermat für jede ungerade Primzahl bewiesen, dann gilt sie für alle n 2.

10 Kettenbrüche

Ein endlicher *Kettenbruch* ist ein Ausdruck der Form

$$a_0 \quad \cfrac{1}{a_1 \quad \cfrac{1}{a_2 \quad \cfrac{1}{a_3 \quad \cfrac{1}{a_n}}}}$$

wobei die a_i reelle Zahlen sind. Wir kürzen dies mit $a_0\ a_1 \quad a_n$ ab. Formaler definieren wir einen endlichen Kettenbruch direkt als Symbol $a_0\ a_1 \quad a_n$, dessen Wert durch die folgende rekursive Vorschrift gegeben ist:

$$a_0 \quad : \quad a_0$$

$$a_0 \quad a_n : \quad a_0 \quad a_n \ 1 \quad \frac{1}{a_n} \qquad \text{für } n$$

Meist betrachtet man den Fall, wobei a_0 eine ganze Zahl und die $a_1 \quad a_n$ natürliche Zahlen sind.

Beispiel Wir entwickeln $\frac{48}{11}$ in einen Kettenbruch:

$$\frac{48}{11} \quad 4 \quad \frac{4}{11} \quad 4 \quad \cfrac{1}{\frac{11}{4}} \quad 4 \quad \cfrac{1}{2 \quad \frac{3}{4}} \quad 4 \quad \cfrac{1}{2 \quad \frac{1}{\frac{4}{3}}} \quad 4 \quad \cfrac{1}{2 \quad \cfrac{1}{1 \quad \frac{1}{3}}} \qquad 4\ 2\ 1\ 3$$

Die unendlichen Kettenbrüche werden auf die offensichtliche Weise formal erklärt und durch die Folge $a_0\ a_1 \quad$ dargestellt. Ihr Wert ist als Grenzwert der endlichen Kettenbrüche $a_0\ a_1 \quad a_n$ erklärt. Wir werden bald eine Konvergenzaussage beweisen.

Beispiel Der einfachste unendliche Kettenbruch ist

$$\Phi \quad 1 \quad \cfrac{1}{1 \quad \cfrac{1}{1 \quad \frac{1}{1}}} \qquad 1\ 1\ 1$$

Wenn wir davon ausgehen, dass der Grenzwert existiert, dann muss er $\Phi \quad 1 \quad 1 \quad \Phi$ erfüllen. Das Lösen dieser Gleichung liefert als einzigen positiven Wert den goldenen Schnitt $\frac{1 \quad \sqrt{5}}{2}$.

Wir wollen nun eine beliebige reelle Zahl $x \quad$ in einen Kettenbruch mit $a_0 \quad$ und $a_1\ a_2 \quad$ entwickeln.

S. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie,*
DOI 10.1007/978-3-8348-8263-9_10,

Kettenbruchalgorithmus

1. Man setze $a_0 :$ x und $t_0 :$ x a_0 0 1 .
2. Solange t_n 0 ist, berechne man

$$\xi_n : \frac{1}{t_n} \quad 1 \quad a_{n\ 1} : \quad \xi_n \qquad \text{und} \quad t_{n\ 1} : \quad \xi_n \quad a_{n\ 1} \quad 0\ 1$$

Wir wollen zeigen, dass dieser Algorithmus sinnvoll ist. Dazu behaupten wir, dass

$$x \quad a_0 \qquad a_n\ \xi_n$$

gilt. Man sieht dies durch Induktion. Wir haben im Algorithmus durch die Definition der Anfangswerte

$$x \quad x \qquad a_0 \quad \frac{1}{\xi_0} \qquad a_0\ \xi_0$$

Der Induktionschritt ist wie folgt

$$x \quad a_0 \qquad a_n\ \xi_n \qquad\qquad a_0 \qquad a_n\ a_{n\ 1} \quad t_{n\ 1}$$

$$a_0 \qquad a_n\ a_{n\ 1} \quad \frac{1}{\xi_{n\ 1}} \qquad a_0 \qquad a_{n\ 1}\ \xi_{n\ 1}$$

Aufgabe 10.1 Stellen Sie die Zahl $\alpha :$ $\frac{17}{99}$ als Kettenbruch dar.

Aufgabe 10.2 Berechnen Sie den Wert des Kettenbruchs 1 2 2 2 unter der Annahme, dass der Grenzwert existiert.

Aufgabe 10.3 Zeigen Sie, dass für 0 m n gilt:

$$a_0 \qquad a_n \qquad a_0 \qquad a_{m\ 1} \quad a_m \qquad a_n$$

Folgern Sie durch einen Grenzwertprozess

$$a_0\ a_1 \qquad\qquad a_0 \qquad a_{m\ 1} \quad a_m\ a_{m\ 1}$$

unter der Annahme, dass alle auftretenden Grenzwerte existieren.

Satz 10.4 *Dieser Algorithmus liefert für eine Zahl x einen endlichen Kettenbruch $a_0\ a_1 \qquad a_n$ genau dann, wenn x $\mathbb{Q}$.*
In diesem Fall gilt x $a_0\ a_1 \qquad a_n$.

Beweis: Nach den obigen Bemerkungen gilt, wenn der Kettenbruchalgorithmus abbricht

$$x \quad a_0 \qquad a_n \quad t_n \qquad a_0 \qquad a_n \qquad \text{falls } t_n \quad 0$$

Somit ist x ein endlicher Kettenbruch und damit offensichtlich eine rationale Zahl.

Sei daher nun $x \in \mathbb{Q}$ vorgegeben. Wir wollen zeigen, dass der obige Kettenbruchalgorithmus im Wesentlichen der euklidische Algorithmus ist. Sei $x = \frac{p}{q}$ mit $q > 0$. Wir setzen $r_0 := q$ und definieren mit dem euklidischen Algorithmus die weiteren a'_i, r_i:

$$\begin{array}{llllll}
p = a'_0 \cdot r_0 + r_1 & \text{mit } 0 \leq r_1 < q = r_0 \\
r_0 = a'_1 \cdot r_1 + r_2 & \text{mit } 0 \leq r_2 < r_1 \\
\vdots & \vdots \\
r_{n-2} = a'_{n-1} \cdot r_{n-1} + r_n & \text{mit } 0 \leq r_n < r_{n-1} \\
r_{n-1} = a'_n \cdot r_n + 0 & r_{n-1} = 0
\end{array}$$

Es gilt daher:

$$\begin{array}{llllll}
x = \frac{p}{r_0} = a'_0 + \frac{r_1}{r_0} = a'_0 + \frac{1}{\frac{r_0}{r_1}} & \text{mit } \frac{1}{\frac{r_0}{r_1}} > 0 < 1 \\
\frac{r_{i-1}}{r_i} = a'_i + \frac{r_{i+1}}{r_i} = a'_i + \frac{1}{\frac{r_i}{r_{i+1}}} & \text{mit } \frac{1}{\frac{r_i}{r_{i+1}}} > 0 < 1 & \text{für } i = 1, \ldots, n-1 \\
\frac{r_{n-1}}{r_n} = a'_n + \frac{r_{n+1}}{r_n} = a'_n
\end{array}$$

Ein Vergleich mit den Formeln aus dem Kettenbruchalgorithmus,

$$\begin{array}{llllll}
x = a_0 + t_0 = a_0 + \frac{1}{\xi_0} & \text{mit } \frac{1}{\xi_0} > 0 < 1 \\
\xi_{i-1} = a_i + t_i = a_i + \frac{1}{\xi_i} & \text{mit } \frac{1}{\xi_i} > 0 < 1 & \text{für } i = 1, \ldots, n-1 \\
\xi_{n-1} = a_n + t_n
\end{array}$$

zeigt $a_i = a'_i$ und $t_i = \frac{r_{i+1}}{r_i}$. Insbesondere gilt also $t_n = \frac{0}{r_n} = 0$, d.h. dort bricht der Kettenbruchalgorithmus ab.

Die Kettenbruchdarstellung einer rationalen Zahl ist selbst unter der Bedingung $a_0 \in \mathbb{Z}$, $a_i > 0$ für $i > 0$ nicht ganz eindeutig, denn es gilt

$$[a_0, \ldots, a_{n-1}, a_n] = \begin{cases} [a_0, \ldots, a_{n-1}, a_n - 1, 1] & \text{für } a_n > 1 \text{ oder } n = 0 \\ [a_0, \ldots, a_{n-1} + 1] & \text{für } a_n = 1 \text{ und } n > 1 \end{cases}$$

Aufgabe 10.5 Zeigen Sie, dass die Darstellung einer rationalen Zahl abgesehen von diesen Möglichkeiten eindeutig ist. Zeigen Sie dafür zunächst: Ist

$$[a_0, \ldots, a_n, \xi] = [b_0, \ldots, b_n, \zeta]$$

mit $a_0, b_0 \in \mathbb{Z}$, $a_1, \ldots, a_n, b_1, \ldots, b_n > 0$ und reellen Zahlen $\xi, \zeta > 1$, dann gilt $a_i = b_i$ für alle $i \in \{0, \ldots, n\}$ und $\xi = \zeta$.

Sei nun allgemein eine Folge ganzer Zahlen $a_{n\ n\ 0}$ mit $a_n \quad 1$ für $n \quad 1$ gegeben. Unser nächstes Ziel ist es zu zeigen, dass die endlichen Kettenbrüche $a_0\ a_1 \quad a_n$ immer eine konvergente Folge bilden, deren Grenzwert wir mit $a_0\ a_1 \quad$ bezeichnet haben. Weiter wollen wir auch beweisen, dass die Folge dieser Kettenbrüche gegen x konvergiert, falls die Folge a_n aus der Kettenbruchentwicklung einer Zahl $x \quad \mathbb{Q}$ stammt. Dies zu zeigen wird einige Zeit in Anspruch nehmen und benutzt die folgenden Hilfsfolgen von ganzen Zahlen:

$$\begin{array}{llll} p_{\ 2} & 0 & p_{\ 1} & 1 \\ q_{\ 2} & 1 & q_{\ 1} & 0 \end{array} \qquad \begin{array}{ll} p_n & a_n p_{n\ 1} \quad p_{n\ 2} \\ q_n & a_n q_{n\ 1} \quad q_{n\ 2} \end{array}$$

Die ersten p_n, q_n sehen wie folgt aus

$$\begin{array}{ll} p_0 & a_0 \\ p_1 & a_1 a_0 \quad 1 \\ p_2 & a_2 a_1 a_0 \quad a_2 \quad a_0 \\ p_3 & a_3 a_2 a_1 a_0 \quad a_3 a_2 \quad a_3 a_0 \quad a_1 a_0 \quad 1 \end{array} \qquad \begin{array}{ll} q_0 & 1 \\ q_1 & a_1 \\ q_2 & a_2 a_1 \quad 1 \\ q_3 & a_3 a_2 a_1 \quad a_3 \quad a_1 \end{array}$$

Diese Rekursionsfolgen lassen sich noch einfacher in Matrizenschreibweise ausdrücken:

$$\begin{array}{ll} p_{\ 1} & p_{\ 2} \\ q_{\ 1} & q_{\ 2} \end{array} \qquad \begin{array}{ll} 1 & 0 \\ 0 & 1 \end{array} \qquad \text{und}$$

$$\begin{array}{ll} p_n & p_{n\ 1} \\ q_n & q_{n\ 1} \end{array} \qquad \begin{array}{ll} p_{n\ 1} & p_{n\ 2} \\ q_{n\ 1} & q_{n\ 2} \end{array} \qquad \begin{array}{ll} a_n & 1 \\ 1 & 0 \end{array}$$

Das Auflösen der Rekursion ist in dieser Schreibweise trivial:

$$\begin{array}{ll} p_n & p_{n\ 1} \\ q_n & q_{n\ 1} \end{array} \qquad \begin{array}{ll} a_0 & 1 \\ 1 & 0 \end{array} \qquad \begin{array}{ll} a_1 & 1 \\ 1 & 0 \end{array} \qquad \begin{array}{ll} a_n & 1 \\ 1 & 0 \end{array} \qquad : \prod_{i\ 0}^{n} \begin{array}{ll} a_i & 1 \\ 1 & 0 \end{array}$$

Sie stehen in folgendem Zusammenhang zu den Kettenbrüchen:

Lemma 10.6 *Mit den obigen Bezeichnungen gilt für alle* $n \quad 0$ *und* $\xi \quad 0$*:*

$$a_0\ a_1 \quad a_n \quad \frac{p_n}{q_n} \quad \textit{und} \quad a_0\ a_1 \quad a_n\ \xi \quad \frac{\xi p_n \quad p_{n\ 1}}{\xi q_n \quad q_{n\ 1}}$$

Beweis: Die zweite Formel gilt für $n \quad 0$ nach Definition. Der Induktionsschritt ist die folgende Rechnung:

$$a_0\ a_1 \quad a_n\ \xi \qquad a_0\ a_1 \quad a_n \quad \frac{1}{\xi}$$

$$\frac{a_n \quad \frac{1}{\xi}\ p_{n\ 1} \quad p_{n\ 2}}{a_n \quad \frac{1}{\xi}\ q_{n\ 1} \quad q_{n\ 2}} \qquad \frac{a_n \xi \quad 1\ p_{n\ 1} \quad \xi p_{n\ 2}}{a_n \xi \quad 1\ q_{n\ 1} \quad \xi q_{n\ 2}}$$

$$\frac{\xi\ a_n p_{n\ 1} \quad p_{n\ 2} \quad p_{n\ 1}}{\xi\ a_n q_{n\ 1} \quad q_{n\ 2} \quad q_{n\ 1}} \qquad \frac{\xi p_n \quad p_{n\ 1}}{\xi q_n \quad q_{n\ 1}}$$

Durch Einsetzen von a_n für ξ in diese Formel für $n \quad 1$ statt n und Benutzen der Rekursionsformeln für p_n und q_n erhält man sofort die erste Gleichheit.

Wir beweisen noch einige elementare Eigenschaften der Folgen p_n und q_n, auf die wir häufig zurückgreifen werden.

Lemma 10.7 *Mit den obigen Bezeichnungen gilt:*

1. $q_{n\ 1}\quad q_n$ *für* $n\quad$, *insbesondere ist* $q_n\quad n$. *Weiter ist* $q_1\quad q_0$, *wobei die Gleichheit genau im Fall* $a_1\quad 1$ *gilt.*
2. $p_n q_{n\ 1}\quad p_{n\ 1}q_n\qquad 1\ ^{n\ 1}$ *für* $n\quad 0$.
3. $p_n q_{n\ 2}\quad p_{n\ 2}q_n\qquad 1\ ^n a_n$ *für* $n\quad 0$.
4. ggT $p_n\ q_n\quad 1$.

Beweis: Für die erste Aussage bemerken wir, dass $q_0\quad 1$, $q_1\quad a_1 q_0\quad a_1\quad 1$ und $q_{n\ 1}\quad a_{n\ 1}q_n\quad q_{n\ 1}\quad q_n\quad q_{n\ 1}$. Damit ergibt sich $q_{n\ 1}\quad q_n\quad n$ durch eine offensichtliche Induktion.

Für die zweite Aussage berechnen wir

$$p_n q_{n\ 1}\quad p_{n\ 1}q_n\quad \det\begin{matrix} p_n & p_{n\ 1} \\ q_n & q_{n\ 1}\end{matrix}\qquad \det\prod_{i\ 0}^{n}\begin{matrix} a_i & 1 \\ 1 & 0\end{matrix}$$

$$\prod_{i\ 0}^{n}\det\begin{matrix} a_i & 1 \\ 1 & 0\end{matrix}\qquad \prod_{i\ 0}^{n}\ 1\qquad 1\ ^{n\ 1}$$

Daraus folgt unmittelbar ist dritte Aussage:

$$p_n q_{n\ 2}\quad p_{n\ 2}q_n\qquad a_n p_{n\ 1}\quad p_{n\ 2}\ q_{n\ 2}\quad p_{n\ 2}\ a_n q_{n\ 1}\quad q_{n\ 2}$$
$$a_n\ p_{n\ 1}q_{n\ 2}\quad p_{n\ 2}q_{n\ 1}\qquad 1\ ^n a_n$$

Für die letzte Aussage, ggT $p_n\ q_n\quad 1$, bemerken wir, dass jeder gemeinsame Teiler von p_n und q_n auch $p_n q_{n\ 1}\quad p_{n\ 1}q_n\qquad 1\ ^{n\ 1}$ teilen muss und damit $\quad 1$ ist.

Satz 10.8 (Konvergenz) *Sei* $a_{n\ n\ \ 0}$ *eine Folge ganzer Zahlen mit* $a_n\quad 1$ *für* $n\quad 1$. *Dann bilden die Brüche* $\frac{p_n}{q_n}\qquad a_0\qquad a_n$ *eine konvergente Folge. Genauer gilt: Die Teilfolge* $\frac{p_{2n}}{q_{2n}}$ *wächst streng monoton und die Teilfolge* $\frac{p_{2n\ 1}}{q_{2n\ 1}}$ *fällt streng monoton. Daher sind die Folgenglieder der gesamten Folge abwechselnd größer und kleiner als der Grenzwert.*

Beweis: Nach Lemma 10.7 gilt

$$\frac{p_n}{q_n}\quad \frac{p_{n\ 1}}{q_{n\ 1}}\quad \frac{1\ ^{n\ 1}}{q_n q_{n\ 1}}$$

Folglich ist

$$\frac{p_n}{q_n}\quad \sum_{i\ 1}^{n}\frac{p_i}{q_i}\quad \frac{p_{i\ 1}}{q_{i\ 1}}\qquad \frac{p_0}{q_0}\quad a_0\quad \sum_{i\ 1}^{n}\frac{1\ ^{i\ 1}}{q_i q_{i\ 1}}$$

Da die Terme $\frac{1}{q_i q_{i\ 1}}$ wieder nach Lemma 10.7 eine streng monotone Nullfolge bilden, ist ihre alternierende Reihe eine konvergente Reihe nach dem Leibniz–Kriterium, also konvergieren auch die Brüche $\frac{p_n}{q_n}$.

Um die strenge Monotonie zu beweisen, folgern wir aus Lemma 10.7

$$\frac{p_n}{q_n}\quad \frac{p_{n\ 2}}{q_{n\ 2}}\qquad 1\ ^n\frac{a_n}{q_n q_{n\ 2}}$$

Für $n \quad 2$ ist $a_n \; q_n \; q_{n \; 2} \quad 1$ und daher

$$\frac{p_n}{q_n} \quad \frac{p_{n \; 2}}{q_{n \; 2}} \text{ für } n \text{ gerade} \qquad \text{sowie} \qquad \frac{p_n}{q_n} \quad \frac{p_{n \; 2}}{q_{n \; 2}} \text{ für } n \text{ ungerade}$$

Satz 10.9 (Konvergenz der Kettenbruchentwicklung) *Sei* $x \quad \mathbb{Q}$. *Dann konvergieren die Brüche* $\frac{p_n}{q_n} \quad a_0 \quad a_n$ *gegen* x. *Genauer gilt:*

$$x \quad \frac{p_n}{q_n} \quad \frac{1}{q_n q_{n \; 1}} \quad \frac{1}{n \; n \quad 1}$$

wobei die letzte Abschätzung nur für $n \quad 1$ *gilt.*

Auf Grund dieser Eigenschaft werden die $\frac{p_n}{q_n}$ als *Näherungsbrüche* von x bezeichnet.

Beweis: Nach Lemma 10.6 gilt

$$x \quad a_0 \; a_1 \quad a_n \; \xi_n \quad \frac{\xi_n p_n \quad p_{n \; 1}}{\xi_n q_n \quad q_{n \; 1}}$$

somit ist

$$x \quad \frac{p_n}{q_n} \quad \frac{\xi_n p_n \quad p_{n \; 1} \; q_n \quad p_n \; \xi_n q_n \quad q_{n \; 1}}{q_n \; \xi_n q_n \quad q_{n \; 1}}$$

$$\frac{p_{n \; 1} q_n \quad p_n q_{n \; 1}}{q_n \; \xi_n q_n \quad q_{n \; 1}} \quad \frac{1 \; ^n}{q_n \; \xi_n q_n \quad q_{n \; 1}}$$

Mit $a_{n \; 1} \quad \xi_n$ folgt

$$x \quad \frac{p_n}{q_n} \quad \frac{1}{q_n \; \xi_n q_n \quad q_{n \; 1}} \quad \frac{1}{q_n \; a_{n \; 1} q_n \quad q_{n \; 1}} \quad \frac{1}{q_n q_{n \; 1}} \quad \frac{1}{n \; n \quad 1}$$

wobei die letzte Abschätzung nur für $n \quad 1$ gilt. Wir erkennen insbesondere, dass $\frac{p_n}{q_n}$ gegen x konvergiert.

Beispiel Die Kettenbruchentwicklungen von e und π sind

$$e \quad 2 \; 1 \; 2 \; 1 \; 1 \; 4 \; 1 \; 1 \; 6 \; 1 \; 1 \; 8 \; 1 \; 1 \; 10 \; 1 \; 1 \; 12 \; 1 \; 1 \; 14 \; 1 \; 1 \; 16 \; 1 \; 1 \; 18$$

$$\pi \quad 3 \; 7 \; 15 \; 1 \; 292 \; 1 \; 1 \; 1 \; 2 \; 1 \; 3 \; 1 \; 14 \; 2 \; 1 \; 1 \; 2 \; 2 \; 2 \; 2 \; 1 \; 84 \; 2 \; 1 \; 1 \; 15 \; 3$$

Dass die Kettenbruchentwicklung von e wirklich so regelmäßig ist, wurde schon von Euler [E] mit Hilfe der Riccati-Differentialgleichung gezeigt. Ein elementarer Beweis findet sich in [Ch]. Es mag erstaunen, dass eine transzendente Zahl eine solche einfache Kettenbruchentwicklung besitzt.

Bei π lässt sich in der Kettenbruchentwicklung kein Muster entdecken. Auffällig sind jedoch die manchmal auftretenden großen Zahlen. Solche Zahlen geben immer besonders gute Approximationen von π relativ zu der Nennergröße. Denn falls $a_{n \; 1}$ groß ist, ist q_n relativ klein zu $q_{n \; 1} \quad a_{n \; 1} q_n \quad q_{n \; 1}$ und somit ist der Betrag der Differenz $x \quad \frac{p_n}{q_n} \quad \frac{1}{q_n q_{n \; 1}}$ sehr klein

und $a_0 \quad a_n$ eine daher gute Approximation. Für π erhalten wir die folgenden Approximationen:

$a_0 \quad a_n$	$\frac{p_n}{q_n}$	$\pi \quad \frac{p_n}{q_n}$
3 7	$\frac{22}{7}$	1 26 10 ^{3}
3 7 15	$\frac{333}{106}$	8 32 10 ^{5}
3 7 15 1	$\frac{355}{113}$	2 67 10 ^{7}
3 7 15 1 292	$\frac{103993}{33102}$	5 78 10 ^{10}
3 7 15 1 292 1 1 1 2 1 3 1 14	$\frac{80143857}{25510582}$	5 79 10 ^{16}

Aufgabe 10.10 (Beste Approximation) Zeigen Sie, dass die Näherungsbrüche $p_n \quad q_n$ einer irrationalen Zahl α für $n \quad 2$ die besten Approximationen von α durch Brüche $p \quad q$ mit ggT $p \quad q \quad 1$ und $1 \quad q \quad q_n$ liefern.

Wir wollen nun spezielle Kettenbruchentwicklungen untersuchen.

Definition 10.11 *Eine Kettenbruchentwicklung* $x \quad a_0 \; a_1 \quad$ *heißt* periodisch *(mit Periode* h*), falls es ein* $n \quad , n \quad 1$*, gibt mit* $a_{m \quad h} \quad a_m$ *für alle* $m \quad n \quad 1$*, in Zeichen*

$$x \quad a_0 \; a_1 \quad a_n \; \overline{a_{n \quad 1} \; a_{n \quad 2} \quad a_{n \quad h}}$$

Sie heißt rein periodisch*, falls es keine Vorperiode gibt, d.h.* $n \quad 1$ *gewählt werden kann.*

Wir haben bereits gesehen, dass $\frac{1 \quad \overline{5}}{2}$ rein periodisch ist, allgemein gilt folgender Satz:

Satz 10.12 (Euler/Lagrange) *Der Kettenbruch einer reellen Zahl* x *ist periodisch genau dann, wenn* x *eine quadratische Irrationalzahl ist, d.h.* $x \quad \mathbb{Q}$ *erfüllt eine quadratische Gleichung* $ax^2 \quad bx \quad c \quad 0$ *mit* $a \; b \; c \quad$ *und* $a \quad 0$*.*

Beweis: (Euler) Ist $x \quad a_0 \; a_1 \quad a_n \; \overline{a_{n \quad 1} \; a_{n \quad 2} \quad a_{n \quad h}}$ periodisch, so setzen wir $\xi \quad \overline{a_{n \quad 1} \; a_{n \quad 2} \quad a_{n \quad h}}$. Dann gilt offenbar

$$\xi \quad a_{n \quad 1} \; a_{n \quad 2} \quad a_{n \quad h} \; \xi$$

Wir bezeichnen die zu ξ gehörenden Hilfsfolgen mit $p'_i \; q'_i$. Nach Lemma 10.6 gilt

$$\xi \quad \frac{\xi p'_{h \quad 1} \quad p'_{h \quad 2}}{\xi q'_{h \quad 1} \quad q'_{h \quad 2}}$$

und — äquivalent dazu —

$$q'_{h \quad 1}\xi^2 \quad q'_{h \quad 2} \quad p'_{h \quad 1}\,\xi \quad p'_{h \quad 2} \quad 0$$

Daher erfüllt ξ eine quadratische Gleichung. Nun ist

$$x \quad a_0 \; a_1 \quad a_n \; \xi \quad \frac{\xi p_n \quad p_{n \quad 1}}{\xi q_n \quad q_{n \quad 1}} \qquad \xi \quad \frac{q_{n \quad 1}x \quad p_{n \quad 1}}{q_n x \quad p_n}$$

Einsetzen in die obige quadratische Gleichung und Multiplikation mit $q_n x \quad p_n \; ^2$ liefert eine quadratische Gleichung für x.

(Lagrange) Sei nun umgekehrt x eine quadratische Irrationalzahl mit $ax^2 \quad bx \quad c \quad 0$. Für die Kettenbruchentwicklung $x \quad a_0 \; a_1 \quad a_n \; \xi_n$ von x gilt

$$x \quad \frac{\xi_n p_n \quad p_{n \; 1}}{\xi_n q_n \quad q_{n \; 1}}$$

Setzt man dies in die quadratische Gleichung ein, so ergibt sich

$$A_n \xi_n^2 \quad B_n \xi_n \quad C_n \quad 0$$

mit ganzen Zahlen

$$A_n : \quad a p_n^2 \quad b p_n q_n \quad c q_n^2$$

$$B_n : \quad 2a p_n p_{n \; 1} \quad b \; p_n q_{n \; 1} \quad p_{n \; 1} q_n \quad 2c q_n q_{n \; 1}$$

$$C_n : \quad a p_{n \; 1}^2 \quad b p_{n \; 1} q_{n \; 1} \quad c q_{n \; 1}^2$$

Jetzt erkennt man, dass $C_n \quad A_{n \; 1}$ und dass die Diskriminanten der quadratischen Gleichungen

$$B_n^2 \quad 4A_n C_n \quad b^2 \quad 4ac \quad p_n q_{n \; 1} \quad q_n p_{n \; 1}{}^2 \quad b^2 \quad 4ac$$

alle gleich sind. Aus der Abschätzung

$$x \quad \frac{p_n}{q_n} \quad \frac{1}{q_n q_{n \; 1}} \quad \frac{1}{q_n^2}$$

folgt

$$p_n \quad x q_n \quad \frac{\delta}{q_n}$$

mit $\delta \quad 1$. Das Einsetzen in die Formel für A_n liefert

$$A_n \quad a \; x q_n \quad \frac{\delta}{q_n}{}^2 \quad b q_n \; x q_n \quad \frac{\delta}{q_n} \quad c q_n^2$$

$$q_n^2 \; ax^2 \quad bx \quad c \quad 2ax\delta \quad a\frac{\delta^2}{q_n^2} \quad b\delta$$

$$2ax\delta \quad a\frac{\delta^2}{q_n^2} \quad b\delta \quad 2 \; ax \quad a \quad b$$

Hieraus folgt, dass es nur endlich viele Möglichkeiten für A_n — und somit auch für $C_n \quad A_{n \; 1}$ — gibt. Die Gleichung $B_n^2 \quad 4A_n C_n \quad b^2 \quad 4ac$ impliziert, dass es auch nur endlich viele Möglichkeiten für B_n gibt. Schließlich können wegen $A_n \xi_n^2 \quad B_n \xi_n \quad C_n \quad 0$ auch nur endlich viele verschiedene ξ_n auftreten. Es gibt also ein $m \quad {}_0$ und $h \quad$ mit $\xi_{m \; h} \quad \xi_m$. Damit ist die Kettenbruchentwicklung periodisch.

Nach der Lösungsformel für quadratische Gleichungen hat jede quadratische Irrationalzahl die Form

$$x \quad u \quad v\sqrt{d}$$

wobei $u \; v \; d \quad \mathbb{Q}$ mit $v \; d \quad 0$ und d kein Quadrat. Üblicherweise erweitert man die rationale Zahl d so, dass ihr Nenner ein Quadrat ist und zieht diesen dann aus der Wurzel, d.h. man kann ohne Einschränkung $d \quad$ annehmen.

Wir wollen nun die rein periodischen Kettenbrüche charakterisieren. Dazu benötigen wir folgende Definition.

Definition 10.13 *Sei $x = u + v\sqrt{d}$ mit $u, v \in \mathbb{Q}$ und d kein Quadrat, dann ist die zu x* konjugierte Zahl

$$\overline{x} = u - v\sqrt{d}$$

Dies ist wohldefiniert, da für jedes m gilt

$$\overline{u + v\sqrt{m^2 d}} = u + v\sqrt{m^2 d} = u + vm\sqrt{d} = \overline{u + vm\sqrt{d}}$$

Aufgabe 10.14 Sei d kein Quadrat. Zeigen Sie, dass die Konjugation ein Körperautomorphismus auf $\mathbb{Q}(\sqrt{d}) = \mathbb{Q} \to \mathbb{Q}(\sqrt{d})$ ist. Folgern Sie nun: Falls $x \in \mathbb{Q}$ eine Lösung einer quadratischen Gleichung $ax^2 + bx + c = 0$ mit $a, b, c \in \mathbb{Q}$ ist, dann ist $\overline{x}$ die zweite Lösung.

Satz 10.15 *Eine quadratische Irrationalzahl x hat genau dann eine rein periodische Kettenbruchentwicklung, wenn x reduziert ist, d.h.*

$$x > 1 \quad \textit{und} \quad -1 < \overline{x} < 0$$

Zum Beispiel ist $1 + \sqrt{2}$ reduziert. Im Beweis benötigen wir den folgenden Hilfssatz.

Hilfssatz 10.16 *Sei x eine quadratische Irrationalzahl mit rein periodischer Kettenbruchentwicklung*

$$x = \overline{[a_0, a_1, \ldots, a_{h-1}]}$$

dann gilt

$$-\frac{1}{\overline{x}} = \overline{[a_{h-1}, \ldots, a_1, a_0]}$$

Beweis: Sei $y = \overline{[a_{h-1}, \ldots, a_1, a_0]}$. Weiter sollen $\frac{p_n}{q_n}$ und $\frac{p'_n}{q'_n}$ die Näherungsbrüche in der Kettenbruchentwicklung von x bzw. y bezeichnen. Wegen

$$x = [a_0, a_1, \ldots, a_{h-1}, x] \quad \text{und} \quad y = [a_{h-1}, \ldots, a_1, a_0, y]$$

gilt nach Lemma 10.6

$$x = \frac{xp_{h-1} + p_{h-2}}{xq_{h-1} + q_{h-2}} \quad \text{und} \quad y = \frac{yp'_{h-1} + p'_{h-2}}{yq'_{h-1} + q'_{h-2}}$$

Wir finden also x und y als Lösungen der quadratischen Gleichungen

$$q_{h-1}x^2 + (q_{h-2} - p_{h-1})x - p_{h-2} = 0 \quad \text{und} \quad q'_{h-1}y^2 + (q'_{h-2} - p'_{h-1})y - p'_{h-2} = 0$$

Durch Division der letzten Gleichung durch y^2 erhalten wir eine quadratische Gleichung in $\frac{1}{y}$:

$$p'_{h-2}\left(\frac{1}{y}\right)^2 + (q'_{h-2} - p'_{h-1})\frac{1}{y} - q'_{h-1} = 0$$

Mit Hilfe der Matrizenschreibweise können wir wie folgt ausdrücken: Es gibt $0 \neq \mu, \lambda \in \mathbb{Z}$ mit

$$\mu \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} xp_{h-1} + p_{h-2} \\ xq_{h-1} + q_{h-2} \end{pmatrix} = \begin{pmatrix} p_{h-1} & p_{h-2} \\ q_{h-1} & q_{h-2} \end{pmatrix} \begin{pmatrix} x \\ 1 \end{pmatrix}$$

$$\lambda \begin{pmatrix} y \\ 1 \end{pmatrix} = \begin{pmatrix} yp'_{h-1} + p'_{h-2} \\ yq'_{h-1} + q'_{h-2} \end{pmatrix} = \begin{pmatrix} p'_{h-1} & p'_{h-2} \\ q'_{h-1} & q'_{h-2} \end{pmatrix} \begin{pmatrix} y \\ 1 \end{pmatrix}$$

Nun ist

$$\begin{matrix} p_{h-1} & p_{h-2} \\ q_{h-1} & q_{h-2} \end{matrix} \qquad \begin{matrix} a_0 & 1 \\ 1 & 0 \end{matrix} \qquad \begin{matrix} a_1 & 1 \\ 1 & 0 \end{matrix} \qquad \begin{matrix} a_{h-1} & 1 \\ 1 & 0 \end{matrix}$$

und

$$\begin{matrix} p'_{h-1} & p'_{h-2} \\ q'_{h-1} & q'_{h-2} \end{matrix} \qquad \begin{matrix} a_{h-1} & 1 \\ 1 & 0 \end{matrix} \qquad \begin{matrix} a_{h-2} & 1 \\ 1 & 0 \end{matrix} \qquad \begin{matrix} a_0 & 1 \\ 1 & 0 \end{matrix}$$

somit erhalten wir

$$\begin{matrix} p_{h-1} & p_{h-2} \\ q_{h-1} & q_{h-2} \end{matrix} \qquad \begin{matrix} p'_{h-1} & p'_{h-2} \\ q'_{h-1} & q'_{h-2} \end{matrix}^{t}$$

Als Einzelgleichungen ist dies

$$p_{h-1} \quad p'_{h-1} \quad p_{h-2} \quad q'_{h-1} \quad q_{h-1} \quad p'_{h-2} \quad \text{und} \quad q_{h-2} \quad q'_{h-2}$$

Also sind x und $-1/y$ Lösungen derselben quadratischen Gleichung, es gilt daher $x = -1/y$ oder $\overline{x} = -1/y$. Da rein periodische Kettenbrüche wegen $a_0 \geq a_h \geq 1$ positive Zahlen sind, ist $x \cdot y > 0$ und $-1/y < 0$. Somit muss $\overline{x} = -1/y$ gelten, d.h. $y = -1/\overline{x}$.

Beweis (Satz 10.15): Sei zuerst $x = \overline{a_0\ a_1 \ldots a_{h-1}}$ rein periodisch. Dann ist $x > a_0 \geq a_h \geq 1$. Ebenso ist $-1 < \overline{x} < \overline{a_{h-1} \ldots a_0} < -1$, d.h. $0 < \overline{x} < 1$.

Nehmen wir jetzt umgekehrt an, dass x eine reduzierte quadratische Irrationalzahl ist. Wir wissen, dass x eine periodische Kettenbruchentwicklung besitzt,

$$x = a_0, \ldots, a_n, \overline{a_{n+1}, a_1, \ldots, a_{n+h}}$$

Wir behaupten, dass auch ξ_0 reduziert sind. (Hier sind die ξ_i aus dem Kettenbruchalgorithmus gemeint.) Nach Definition ist $\xi_0 = 1/(x - a_0) = x - a_0 > 1$. Nach Aufgabe 10.14 ist

$$\overline{\xi_0} = -\frac{1}{\overline{x} - a_0}$$

Mit $x - a_0 > 1$ und $-1 < \overline{x} < 0$ folgt wie behauptet $-1 < \overline{\xi_0} < 0$. Mit Induktion über n und der Formel $\xi_n = 1/(\xi_{n-1} - a_n)$ zeigt man genauso, dass alle ξ_n reduziert sind.

Es reicht $a_n = a_{n+h}$ zu beweisen, dann ist

$$x = a_0, \ldots, a_{n-1}, \overline{a_n, a_{n+1}, \ldots, a_{n+h-1}}$$

und der Satz folgt durch Induktion. Wir haben nach Definition und dem Hilfssatz

$$\xi_n = \overline{a_{n-1}, \ldots, a_{n+h}}$$

$$\xi_{n-1} = a_n + \overline{a_{n+1}, a_1, \ldots, a_{n+h}} = a_n + \xi_n = a_n + \frac{1}{\xi_n}$$

$$\frac{1}{\overline{\xi_n}} = \overline{a_{n+h}, \ldots, a_{n+1}}$$

Da ξ_{n-1} reduziert ist, gilt $-1 < \overline{\xi_{n-1}} < 0$. Aus $\xi_{n-1} = a_n + 1/\xi_n$ folgt

$$\frac{1}{\overline{\xi_n}} = a_n - \overline{\xi_{n-1}} \qquad \frac{1}{\overline{\xi_n}} < a_n$$

Nach dem Kettenbruchalgorithmus für die Zahl $1\ \overline{\xi_n}$ gilt auch $1\ \overline{\xi_n}\quad a_{n\ h}$, und wir erhalten schließlich $a_n\quad a_{n\ h}$.

Untersuchen wir nun die Kettenbruchentwicklungen von Quadratwurzeln. Die Kettenbruchentwicklungen der ersten Zahlen sind

$$\begin{array}{ll}
\sqrt{2} & 1\ \overline{2} \\
\sqrt{3} & 1\ \overline{1\ 2} \\
\sqrt{5} & 2\ \overline{4} \\
\sqrt{6} & 2\ \overline{2\ 4} \\
\sqrt{7} & 2\ \overline{1\ 1\ 1\ 4} \\
\vdots & \vdots \\
\sqrt{19} & 4\ \overline{2\ 1\ 3\ 1\ 2\ 8} \\
\sqrt{20} & 4\ \overline{2\ 8} \\
\sqrt{21} & 4\ \overline{1\ 1\ 2\ 1\ 1\ 8}
\end{array}$$

Satz 10.17 *Sei d kein Quadrat. Dann ist die Kettenbruchentwicklung von $\sqrt{d}$ vom Typ*

$$\sqrt{d}\quad a_0\ \overline{a_1\quad a_{h\ 1}\ 2a_0}$$

mit $a_{h\ i}\quad a_i$ für $i\quad 1\quad h\quad 1$.

Beweis: Sei wie im Kettenbruchalgorithmus vorgegeben $a_0\quad \sqrt{d}$. Anstatt $\sqrt{d}$ direkt in einen Kettenbruch zu entwickeln, entwickeln wir $x\quad a_0\quad \sqrt{d}$. Wegen a_0 unterscheiden sich die beiden Kettenbruchentwicklungen nur an der ersten Stelle, an der bei $\sqrt{d}$ die Zahl a_0 und bei x die Zahl $x\quad a_0\quad \sqrt{d}\quad 2a_0$ steht.

x ist reduziert, da $0\quad \overline{x}\quad \sqrt{d}\quad \sqrt{d}\quad 1$ ist. Somit hat x eine rein periodische Kettenbruchentwicklung,

$$x\quad \overline{2a_0\ a_1\quad a_{h\ 1}}$$

Für die Symmetrie in den a_i wendet man auf

$$\frac{1}{x\quad 2a_0}\quad \xi_0\quad \overline{a_1\quad a_{h\ 1}\ 2a_0}$$

den Hilfssatz 10.16 an:

$$\overline{2a_0\ a_{h\ 1}\quad a_2\ a_1}\qquad \frac{1}{\overline{\xi_0}}\qquad \overline{x}\quad 2a_0\quad a_0\quad \sqrt{d}\quad x$$

Durch Vergleich der obigen Kettenbruchentwicklungen ergibt sich $a_i\quad a_{h\ i}$.

Aufgabe 10.18 Sei $m\quad$. Entwickeln Sie $\sqrt{m^2\quad 1}$ in einen Kettenbruch.

Für den Faktorisierungsalgorithmus von Brillhart–Morrison im Abschnitt 12, der mit Kettenbruchentwicklungen arbeitet, stellen wir noch den folgenden Satz bereit.

Satz 10.19 *Sei d kein Quadrat. Seien p_n, q_n, ξ_n und a_n die Näherungsbrüche, Reste und deren ganzzahlige Anteile in der Kettenbruchentwicklung von $\sqrt{d}$. Dann gilt*

$$\xi_n = \frac{b_n + \sqrt{d}}{c_n} \quad \text{mit} \quad \begin{array}{l} b_0 := \sqrt{d} \\ c_{-1} := 1 \quad c_0 := d - b_0^2 \\ b_{n+1} := a_n c_n - b_n \\ c_{n+1} := c_{n-1} + 2a_n b_n - a_n^2 c_n \end{array}$$

sowie

$$p_n^2 - dq_n^2 = (-1)^{n-1} c_n \quad \text{und} \quad 0 < c_n < 2\sqrt{d}$$

für $n > 0$.

Beweis: Wir beweisen zunächst die Gleichung

$$d - b_n^2 = c_{n-1} c_n$$

per Induktion für $n \geq 1$. Für $n = 1$ ist dies die Definition von c_0. Der Induktionsschritt ist

$$d - b_{n+1}^2 = d - (a_n c_n - b_n)^2 = d - b_n^2 + c_n - 2a_n b_n + a_n^2 c_n = c_n c_{n-1} + c_n - c_n + c_n = c_n c_{n-1}$$

Nun beweisen wir ebenfalls durch Induktion die Formel $\xi_n = (b_n + \sqrt{d})/c_n$ für $n \geq 0$. Der Anfang ist

$$\xi_0 = \frac{1}{\sqrt{d} - \sqrt{d}} = \frac{1}{\sqrt{d} - b_0} = \frac{b_0 + \sqrt{d}}{d - b_0^2} = \frac{b_0 + \sqrt{d}}{c_0}$$

und der Schritt

$$\xi_{n+1} = \frac{1}{\xi_n - a_{n-1}} = \frac{c_n}{b_n - \sqrt{d} - a_{n-1} c_n} = \frac{c_n}{\sqrt{d} - b_{n-1}} = \frac{c_n (b_{n-1} + \sqrt{d})}{d - b_{n-1}^2}$$

$$= \frac{c_n (b_{n-1} + \sqrt{d})}{c_n c_{n-1}} = \frac{b_{n-1} + \sqrt{d}}{c_{n-1}}$$

Um die Gleichung $p_n^2 - dq_n^2 = (-1)^{n-1} c_n$ zu beweisen, starten wir mit der Formel aus Lemma 10.6 und setzen den obigen Ausdruck für ξ_n ein:

$$\sqrt{d} = \frac{\xi_n p_n + p_{n-1}}{\xi_n q_n + q_{n-1}} = \frac{(b_n + \sqrt{d}) p_n + c_n p_{n-1}}{(b_n + \sqrt{d}) q_n + c_n q_{n-1}}$$

$$b_n p_n + c_n p_{n-1} + dq_n + \sqrt{d}\, p_n + b_n q_n + c_n q_{n-1} = 0$$

Ein Koeffizientenvergleich liefert

$$b_n p_n + c_n p_{n-1} + dq_n = 0 \quad \text{und} \quad p_n + b_n q_n + c_n q_{n-1} = 0$$

Multiplikation der ersten Gleichung mit q_n, der zweiten mit p_n und Addition beider ergibt

$$p_n^2 + c_n p_{n-1} q_n + p_n q_{n-1} + dq_n^2 = 0$$

Mit Lemma 10.7 ergibt sich die behauptete Gleichheit.

Zum Abschluss beweisen wir die Abschätzung

$$0 \quad c_n \quad 2\sqrt{d}$$

Für $n \quad 0$ folgt dies aus

$$c_0 \quad d \quad \sqrt{d}^{\,2} \quad \sqrt{d} \quad \sqrt{d} \quad \sqrt{d} \quad \sqrt{d}$$

Für $n \quad 1$ besitzt ξ_n nach Satz 10.17 eine rein–periodische Kettenbruchentwicklung. Es gilt daher $\xi_n \quad 1$ und $1 \quad \overline{\xi}_n \quad 0$ nach Satz 10.15. Aus der Rechnung

$$0 \quad \xi_n \quad \overline{\xi}_n \quad \frac{b_n \quad \sqrt{d}}{c_n} \quad \frac{b_n \quad \sqrt{d}}{c_n} \quad \frac{2\sqrt{d}}{c_n}$$

folgt, dass die c_n positiv sind. Dies nutzen wir, um die b_n durch

$$b_n \quad \sqrt{d \quad c_n \; {}_1c_n} \quad \sqrt{d}$$

abzuschätzen. Nun ergibt sich wegen $\xi_n \quad 1$

$$c_n \quad c_n\xi_n \quad b_n \quad \sqrt{d} \quad 2\sqrt{d}$$

Wir wollen nun zeigen, dass die Näherungsbrüche einer Kettenbruchentwicklung die besten rationalen Approximationen sind.

Satz 10.20 *Sei x gegeben. Falls für $\frac{p}{q} \quad \mathbb{Q}$ mit* ggT $p \; q \quad 1$ *und* $q \quad 0$ *gilt*

$$x \quad \frac{p}{q} \quad \frac{1}{2q^2}$$

dann ist $\frac{p}{q}$ ein Näherungsbruch der Kettenbruchentwicklung von x.

Beweis: Wir entwickeln $\frac{p}{q}$ in einen Kettenbruch

$$\frac{p}{q} \quad a_0 \; a_1 \quad a_n$$

Falls $x \quad p \; q$ ist, ist dies die Kettenbruchentwicklung von x, und wir sind fertig. Andernfalls gibt es $\varepsilon \quad \{ \quad 1 \quad$ und $0 \quad \delta \quad 1$ mit

$$x \quad \frac{p}{q} \quad \varepsilon \; \frac{\delta}{2q^2}$$

Wir hatten nach Satz 10.4 bemerkt, dass man die Länge der Kettenbruchentwicklung einer rationalen Zahl um eins variieren kann. Daher dürfen wir ohne Einschränkung annehmen, dass $\varepsilon \quad 1^{\,n}$ ist.

Nun finden wir ein $\xi_n \quad$ mit

$$x \quad a_0 \; a_1 \quad a_n \; \xi_n$$

Wir setzen weiter

$$\xi_i : \quad a_{i\ 1} \quad a_n\ \xi_n \quad \text{für } i \quad 0 \quad n \quad 1 \quad \text{also} \quad \xi_i \quad a_{i\ 1}\ \xi_{i\ 1} \quad a_{i\ 1} \quad \frac{1}{\xi_{i\ 1}}$$

Dann gilt

$$x \quad a_0\ a_1 \quad a_i\ \xi_i$$

Wir wollen zeigen, dass dies Kettenbruchentwicklungen von x sind und damit insbesondere $p\ q$ ein Näherungsbruch von x ist. Dafür müssen wir nur $\xi_i \quad 1$ für $i \quad 0 \quad n$ beweisen, denn dann ist $a_{i\ 1} \quad \xi_i$ — genau wie vom Kettenbruchalgorithmus verlangt. Tatsächlich folgt $\xi_i \quad 1$ für $i \quad 0 \quad n$ bereits aus $\xi_n \quad 1$ durch eine absteigende Induktion auf Grund der Gleichung

$$\xi_i \quad a_{i\ 1} \quad \frac{1}{\xi_{i\ 1}}$$

Berechnen wir jetzt ξ_n. Nach Lemma 10.6 ist

$$\frac{p}{q} \quad \frac{p_n}{q_n} \quad \text{und} \quad x \quad \frac{p_n\xi_n \quad p_{n\ 1}}{q_n\xi_n \quad q_{n\ 1}}$$

Aus ggT $p\ q \quad$ ggT $p_n\ q_n \quad 1$ und $q\ q_n \quad 0$ folgt $p \quad p_n$ und $q \quad q_n$. Wir rechnen nun unter Ausnutzung der Voraussetzung und von Lemma 10.7

$$\frac{1\ ^n\delta}{2q_n^2} \quad x \quad \frac{p}{q} \quad \frac{p_n\xi_n \quad p_{n\ 1}}{q_n\xi_n \quad q_{n\ 1}} \quad \frac{p_n}{q_n} \quad \frac{q_np_{n\ 1} \quad p_nq_{n\ 1}}{q_n\ q_n\xi_n \quad q_{n\ 1}}$$

$$\frac{1\ ^n}{q_n\ q_n\xi_n \quad q_{n\ 1}}$$

$$2q_n \quad \delta\ q_n\xi_n \quad q_{n\ 1} \qquad q_n \quad q_{n\ 1} \quad 2q_n \quad q_n\xi_n \quad q_{n\ 1}$$

woraus schließlich $\xi_n \quad 1$ folgt.

Eine weitere berühmte Anwendung finden die Kettenbruchentwicklungen beim Lösen der *Pellschen Gleichung*,

$$x^2 \quad dy^2 \quad 1 \qquad \text{für } d \qquad \text{kein Quadrat.}$$

Meist ist man an ganzzahligen Lösungen interessiert. Wir wollen etwas allgemeiner die Gleichung

$$x^2 \quad dy^2 \quad c$$

betrachten. Im Augenblick interessieren wir uns für $c \qquad 1$. Im Abschnitt 17 wird dann auch $c \qquad 4$ wichtig werden.

Falls $p\ q \qquad ^2$ eine solche Lösung ist, dann sind auch $p \quad q$ Lösungen. Weiter bemerken wir, dass für jede Lösung $p\ q$ der Gleichung $x^2 \quad dy^2 \qquad 1$ die Zahlen p und q teilerfremd sein müssen, weil jeder gemeinsame Teiler von p und q auch ein Teiler von $p^2 \quad dq^2 \qquad 1$ sein muss. Man kann daher p und q bis auf Vorzeichen aus ihrem Quotienten $\frac{p}{q} \quad \mathbb{Q}$ rekonstruieren.

Satz 10.21 *Sei d kein Quadrat und c eine ganze Zahl mit $c \quad d$ und*

$$2\,c \quad \sqrt{\min\{c\ 0 \quad d} \quad \sqrt{d}$$

Dann tritt jede Lösung $p\ q \quad ^2$ der Pellschen Gleichung $x^2 \quad dy^2 \quad c$ in der Form $\frac{p}{q}$ als Näherungsbruch in der Kettenbruchentwicklung von $\sqrt{d}$ auf.

Beweis: Sei $p\ q$ eine solche Lösung, d.h. $p^2 \quad dq^2 \quad c$. Dann gilt

$$p \quad q\sqrt{d} \quad \frac{c}{p \quad q\sqrt{d}}$$

$$\frac{p}{q} \quad \sqrt{d} \quad \frac{c}{q\ p \quad q\sqrt{d}} \quad \frac{c}{q\ \sqrt{c \quad dq^2} \quad q\sqrt{d}}$$

$$\frac{c}{q^2\ \sqrt{c\ q^2 \quad d} \quad \sqrt{d}} \quad \frac{c}{q^2\ \sqrt{\min\{c\ 0 \quad d} \quad \sqrt{d}} \quad \frac{1}{2q^2}$$

also ist $\frac{p}{q}$ nach Satz 10.20 ein Näherungswert der Kettenbruchentwicklung.

Insbesondere treten nach dem Satz alle Lösungen der Gleichung $x^2 \quad dy^2 \quad 1$ als Näherungsbruch in der Kettenbruchentwicklung auf. Wir wollen noch die Existenz von Lösungen der Pellschen Gleichung sichern. Im folgenden Satz werden unendlich viele Lösungen angegeben. Es wird jedoch nicht gezeigt, dass dies alle Lösungen sind, auch andere Kettenbruchnäherungen kommen als Lösungen in Frage. Die genaue Struktur der Lösungsmenge werden wir in Abschnitt 17 beschreiben.

Satz 10.22 *Sei d kein Quadrat und*

$$\sqrt{d} \quad a_0\ \overline{a_1 \quad a_{h\ 1}\ 2a_0}$$

eine Kettenbruchentwicklung von $\sqrt{d}$. $\frac{p_n}{q_n}$ sollen die Näherungsbrüche der Kettenbruchentwicklung bezeichnen.

Dann sind die Tupel $p_{ih\ 1}\ q_{ih\ 1}$ für $i \quad$ Lösungen der Gleichung

$$x^2 \quad dy^2 \quad 1^{\ ih}$$

Beweis: Aus der Kettenbruchentwicklung von $\sqrt{d}$ folgt, dass $a_0 \quad \sqrt{d}$ die Kettenbruchentwicklung

$$a_0 \quad \sqrt{d} \quad \overline{2a_0\ a_1 \quad a_{h\ 1}}$$

hat. Dies sind auch gerade die Reste $\xi_{ih\ 1}$ bei der Kettenbruchentwicklung von

$$\sqrt{d} \quad a_0 \quad a_{ih\ 1}\ \xi_{ih\ 1}$$

Lemma 10.6 impliziert

$$\sqrt{d} \quad \frac{\xi_{ih\ 1}p_{ih\ 1} \quad p_{ih\ 2}}{\xi_{ih\ 1}q_{ih\ 1} \quad q_{ih\ 2}} \quad \frac{a_0 \quad \sqrt{d}\ p_{ih\ 1} \quad p_{ih\ 2}}{a_0 \quad \sqrt{d}\ q_{ih\ 1} \quad q_{ih\ 2}}$$

Durch Multiplikation mit dem Nenner und Ausmultiplizieren erhalten wir

$$a_0 p_{ih\ 1}\quad p_{ih\ 2}\quad dq_{ih\ 1}\qquad a_0 q_{ih\ 1}\quad q_{ih\ 2}\quad p_{ih\ 1}\sqrt{d}\quad 0$$

Da $\sqrt{d}$ irrational ist, können wir einen Koeffizientenvergleich durchführen. Multiplizieren der Terme mit $q_{ih\ 1}$ bzw. $p_{ih\ 1}$ und Addition führt nach Umsortieren zu

$$p_{ih\ 1}^2\quad dq_{ih\ 1}^2\quad p_{ih\ 1}q_{ih\ 2}\quad p_{ih\ 2}q_{ih\ 1}\qquad 1^{\ ih}$$

wobei die letzte Gleichheit nach Lemma 10.7 gilt.

Beispiel Es gilt $\sqrt{3}\quad 1\ \overline{1\ 2}$ und somit $p_0\quad 1$, $p_1\quad 2$, $q_0\quad 1$, $q_1\quad 1$ und $h\quad 2$. Man bekommt also die Lösung $x\ y\qquad 2\ 1$ für $i\quad 1$.

Zusatzaufgaben

Aufgabe 10.23 Bestimmen Sie die Kettenbruchentwicklungen der reellen Zahlen $1\ 2\quad \sqrt{5}$ und $\sqrt{3}\ 2$.

Aufgabe 10.24 Berechnen Sie für $m\qquad$, $m\quad 2$ die Kettenbruchentwicklung von $x\quad \sqrt{m^2\quad 1}$.

Aufgabe 10.25 Berechnen Sie einige Lösungen der Pellschen Gleichungen $x^2\quad 3y^2\quad 1$ und $x^2\quad 13y^2\quad 1$.

Aufgabe 10.26 Man kann die Pellsche Gleichung, $x^2\quad dy^2\quad 1$, auch schreiben als

$$\det\begin{matrix} x & dy \\ y & x \end{matrix}\qquad 1$$

Zeigen Sie, dass damit die ganzzahligen Lösungen der Pellschen Gleichung zu einer Untergruppe der Gruppe $\mathrm{GL}\ 2\ \mathbb{Q}$ werden.

Aufgabe 10.27 Sei $x\quad 5\quad \sqrt{26}$. Berechnen Sie die Kettenbruchentwicklung von x sowie einen Näherungsbruch $\frac{p_n}{q_n}$ zu x, der um weniger als $10^{\ 9}$ von x abweicht.

Aufgabe 10.28 Sei $n\quad 1$ eine natürliche Zahl und $z\quad n$ eine reelle Zahl, die die Gleichung $z^2\quad 1\quad nz$ erfüllt. Bestimmen Sie die Kettenbruchentwicklung von z in Abhängigkeit von n und berechnen Sie z für $n\quad 3$ als quadratische Irrationalzahl. Geben Sie damit eine Lösung $x\ y$ der Pellschen Gleichung $x^2\quad 13y^2\qquad 4$ an.

Aufgabe 10.29 In der Kettenbruchentwicklung einer reellen, positiven Zahl α ist bei zwei aufeinanderfolgenden Näherungsbrüchen $\frac{p_n}{q_n}$ wenigstens eine der zwei folgenden Abschätzungen richtig:

$$\alpha\quad \frac{p_n}{q_n}\quad \frac{1}{2q_n^2}\qquad \alpha\quad \frac{p_{n\ 1}}{q_{n\ 1}}\quad \frac{1}{2q_{n\ 1}^2}$$

Bei drei aufeinanderfolgenden Näherungsbrüchen ist wenigstens eine der drei folgenden Abschätzungen richtig:

$$\alpha \quad \frac{p_n}{q_n} \quad \frac{1}{\sqrt{5}q_n^2} \qquad \alpha \quad \frac{p_{n\ 1}}{q_{n\ 1}} \quad \frac{1}{\sqrt{5}q_{n\ 1}^2} \qquad \alpha \quad \frac{p_{n\ 2}}{q_{n\ 2}} \quad \frac{1}{\sqrt{5}q_{n\ 2}^2}$$

Aufgabe 10.30 Finden Sie die Kettenbruchentwicklung von $x \quad 1 \quad 2\sin \pi \ 3$, indem Sie eine quadratische Gleichung für x aufstellen.

11 Primzahltests

In diesem Abschnitt wollen wir diskutieren, wie man entscheiden kann, ob eine gegebene Zahl n prim ist. Dazu könnte man natürlich auch die Faktorisierungsalgorithmen des nächsten Abschnittes verwenden, diese haben jedoch eine wesentlich schlechtere Laufzeit.

Wie schon im Abschnitt 1 erwähnt, ist meistens die zu einem bestimmten Zeitpunkt größte bekannte Primzahl eine Mersennesche. Das liegt daran, dass es für diese den folgenden einfach durchzuführenden Test gibt:

Satz 11.1 (Lucas–Lehmer Test) *Sei* $n \quad 2^p \quad 1$ *für eine ungerade Primzahl* p . *Die Folge* S_k *sei rekursiv definiert durch* $S_1 \quad 4$ *und* $S_k \quad S_{k \quad 1}^2 \quad 2$. *Dann ist* n *genau dann prim, falls* n *die Zahl* $S_{p \quad 1}$ *teilt.*

Beweis: Wir rechnen im Ring $\sqrt{3}$, der additiv als $\sqrt{3}$ geschrieben werden kann. Sei $\omega \quad 2 \quad \sqrt{3}$ und $\overline{\omega} \quad 2 \quad \sqrt{3}$. Wir behaupten, dass

$$S_k \quad \omega^{2^{k \quad 1}} \quad \overline{\omega}^{2^{k \quad 1}}$$

Wir zeigen dies durch Induktion. Der Anfang ist $\omega^{2^0} \quad \overline{\omega}^{2^0} \quad \omega \quad \overline{\omega} \quad 4$, und der Induktionschritt ist die Rechnung

$$S_k \quad S_{k \quad 1}^2 \quad 2 \quad \omega^{2^{k \quad 2}} \quad \overline{\omega}^{2^{k \quad 2} \quad 2} \quad 2 \quad \omega^{2^{k \quad 1}} \quad \overline{\omega}^{2^{k \quad 1}} \quad 2 \ \omega\overline{\omega}^{\ 2^{k \quad 2}} \quad 2$$
$$\omega^{2^{k \quad 1}} \quad \overline{\omega}^{2^{k \quad 1}} \qquad \text{da} \quad \omega\overline{\omega} \quad 1$$

Nun setzen wir voraus, dass n eine Primzahl ist und zeigen zunächst, dass

$$\omega^{2^{p \quad 1}} \qquad 1 \mod n$$

Dazu bemerken wir, dass

$$\omega \qquad \frac{1 \quad \sqrt{3}}{\sqrt{2}}^{\ 2}$$

Unter Ausnutzung von

$$2^{\frac{n \quad 1}{2}} \qquad \frac{2}{n} \qquad 1 \mod n$$

und

$$3^{\frac{n \quad 1}{2}} \qquad \frac{3}{n} \qquad \frac{n}{3} \qquad \frac{1^{\ p} \quad 1}{3} \qquad \frac{2}{3} \qquad 1 \mod n$$

S. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie,*
DOI 10.1007/978-3-8348-8263-9_11,

sowie des Hilfssatzes 4.6 rechnen wir

$$\omega^{2^{p-1}} \equiv \omega^{\frac{n-1}{2}} \equiv \frac{\left(1+\sqrt{3}\right)^{n-1}}{2^{\frac{n-1}{2}}} \equiv \frac{\left(1+\sqrt{3}\right)^{n}}{2^{\frac{n-1}{2}}} \cdot \frac{1+\sqrt{3}}{2} \equiv 1 \cdot \sqrt{3}^{n} \cdot \frac{1+\sqrt{3}}{2}$$

$$\equiv 1 \cdot 3^{\frac{n-1}{2}}\sqrt{3} \cdot \frac{1+\sqrt{3}}{2} \equiv 1 \cdot \sqrt{3} \cdot \frac{1+\sqrt{3}}{2} \equiv -1 \bmod n$$

Durch Multiplikation der äquivalenten Gleichung $\omega^{2^{p-1}} \equiv -1 \equiv 0 \bmod n$ mit $\overline{\omega}^{2^{p-2}}$ erhalten wir wegen $\omega\overline{\omega} \equiv 1$

$$0 \equiv \omega^{2^{p-1}}\overline{\omega}^{2^{p-2}} \equiv \overline{\omega}^{2^{p-2}} \equiv \omega^{2^{p-2}} \equiv \overline{\omega}^{2^{p-2}} \equiv S_{p-1} \bmod n$$

d.h. n teilt S_{p-1}.

Setzen wir dies umgekehrt voraus, dann finden wir ein $c \in \mathbb{Z}$ mit $S_{p-1} = cn$. Einsetzen in die Formel für S_{p-1} liefert

$$cn \equiv \omega^{2^{p-2}} \equiv \overline{\omega}^{2^{p-2}}$$

Durch Multiplikation mit $\omega^{2^{p-2}}$ erhalten wir wegen $\omega\overline{\omega} \equiv 1$

$$\omega^{2^{p-1}} \equiv -1 \equiv cn\omega^{2^{p-2}} \equiv 1$$

Angenommen, n wäre nicht prim. Dann finden wir einen Primfaktor q mit $3 \leq q \leq \sqrt{n}$. Modulo q lautet die obige Gleichung

$$\omega^{2^{p-1}} \equiv -1 \bmod q \quad \text{und daher} \quad \omega^{2^p} \equiv 1 \bmod q$$

Also ist ω im Ring $R = \mathbb{Z}[\sqrt{3}]/q\mathbb{Z}[\sqrt{3}] = \mathbb{Z}/q\mathbb{Z}[\sqrt{3}]$ eine Einheit, und seine Ordnung in der Einheitengruppe R^* ist 2^p. Da $R^* = R \setminus \{0\}$ höchstens $q^2 - 1$ Elemente hat, gilt $2^p \leq q^2 - 1$. Dies widerspricht jedoch der Wahl von q als Primzahl mit $q^2 \leq n = 2^p - 1$.

Beispiel Wir wollen mit Hilfe dieses Tests beweisen, dass $n = 2^5 - 1 = 31$ eine Primzahl ist. Um $n \mid S_4$, d.h. $S_4 \equiv 0 \bmod n$, zu zeigen, rechnen wir die S_k direkt modulo n aus:

$$S_1 = 4 \quad S_2 = 4^2 - 2 = 14 \quad S_3 = 14^2 - 2 = 194 \equiv 8 \bmod 31$$
$$S_4 \equiv 8^2 - 2 = 62 \equiv 0 \bmod 31$$

Aufgabe 11.2 Zeigen Sie mit dem Lucas–Lehmer Test, dass $n = 2^7 - 1 = 127$ eine Primzahl ist.

Mittlerweile gibt es im Internet das GIMPS–Projekt (Great Internet Mersenne Prime Search). Dort wurde die Suche nach den Mersenneschen Primzahlen parallelisiert. Leute, die zu dieser Suche beitragen möchten, können sich dort ein Programm herunterladen und auf ihrem Computer ausführen. Dieses Programm holt sich dann von einem Server immer neue Teilaufgaben für die Berechnung der nächsten Mersenneschen Primzahl, löst diese und schickt

sie wieder zum Server zurück. Durch die Beteiligung vieler Rechner konnten bereits im Mai 2004 vierzehn Billionen (14 10^{12}) Rechenoperation pro Sekunde durchgeführt werden.

Die anderen bereits erwähnten berühmten Primzahlen sind die Fermatschen Primzahlen, obwohl man davon nur 5 Stück kennt und vermutet, dass es keine weiteren gibt. Auch für diese Zahlen gibt es einen speziellen Test, den Pepin Test. Er beruht auf dem folgenden Test, der immer anwendbar ist, wenn man die Primteiler von n 1 kennt.

Satz 11.3 (Lucas Test) *Eine natürliche Zahl n ist genau dann eine Primzahl, wenn es eine natürliche Zahl* 0 a *n gibt mit*

$$a^{n\ 1} \quad 1 \mod n \qquad \text{aber } a^{\frac{n\ 1}{q}} \quad 1 \mod n$$

für alle Primteiler q von n 1.

Beweis: Falls n eine Primzahl ist, hat jede Primitivwurzel modulo n diese Eigenschaft nach Lemma 7.4. Falls umgekehrt die Zahl a die Voraussetzungen erfüllt, dann hat a die Ordnung n 1 in n U_n. Insbesondere gilt also n 1 $\varphi\ n$. Wegen $\varphi\ n$ n bedeutet dies $\varphi\ n$ n 1. Damit ist n prim nach Aufgabe 5.22.

Wir wollen zeigen, dass n 61 prim ist. Wegen n 1 60 2^2 3 5 folgt dies aus

$$2^{\frac{60}{2}} \quad 2^{30} \qquad 2^{6\ 5} \qquad 64^5 \qquad 3^5 \quad 60 \quad 1 \mod 61$$

$$2^{\frac{60}{3}} \quad 2^{20} \qquad 2^{6\ 3\ 2^2} \qquad 64\ ^3\ 2^2 \qquad 3^3\ 4 \quad 47 \quad 1 \mod 61$$

$$2^{\frac{60}{5}} \quad 2^{12} \qquad 2^{6\ 2} \qquad 64^2 \qquad 3^2 \quad 9 \quad 1 \mod 61$$

Aufgabe 11.4 Zeigen Sie mit dem Lucas Test, dass n 71 prim ist.

Eine direkte Verallgemeinerung des Lucas Tests ist der Pocklington Test:

Satz 11.5 (Pocklington) *Sei n eine natürliche Zahl, so dass n* 1 *eine Faktorisierung der Form n* 1 R F *besitzt, wobei alle Primteiler von F bekannt sind. Weiterhin gebe es eine natürliche Zahl* 0 a *n mit*

$$a^{n\ 1} \quad 1 \mod n \quad \textit{und} \quad \text{ggT}\left(a^{\frac{n\ 1}{q}} \quad 1, n\right) \quad 1$$

für alle Primteiler q von F. Ist dann F $\sqrt{n}$*, so ist n eine Primzahl.*

Beweis: Sei p ein Primteiler von n. Wir berechnen die Ordnung d von a^R modulo p. Wegen $a^{R\ F}$ $a^{n\ 1}$ 1 mod n und p n ist diese ein Teiler von F. Tatsächlich sind d und F gleich. Denn gäbe es einen Primteiler q von F d, also d F q , so folgte

$$1 \quad a^{R\ d} \quad a^{R\ \frac{F}{q}} \quad a^{\frac{n\ 1}{q}} \mod p \qquad p\ a^{\frac{n\ 1}{q}} \quad 1$$

im Widerspruch zu $\text{ggT}\left(a^{\frac{n\ 1}{q}} \quad 1, n\right)$ 1.

Somit teilt d F die Gruppenordnung p 1 von p , insbesondere ist p F $\sqrt{n}$. Wir haben damit gezeigt, dass n nur Primteiler größer als $\sqrt{n}$ besitzt, was für eine zusammengesetzte Zahl unmöglich ist.

Brillhart, Lehmer und Selfridge haben diesen Test noch weiter verbessert [CP, Thm. 4.1.5]. Für die Fermatschen Primzahlen reicht es aus, im Lucas Test die Zahl a 3 zu überprüfen:

Satz 11.6 (Pepin Test) *Die Zahl* $F_k = 2^{2^k} + 1$, $k \geq 1$, *ist genau dann eine Primzahl, falls*

$$3^{(F_k - 1)/2} \equiv -1 \mod F_k$$

Beweis: Da $F_k - 1$ eine Zweierpotenz ist, sind

$$3^{\frac{F_k - 1}{2}} \equiv -1 \mod F_k \qquad 3^{F_k - 1} \equiv 1 \mod F_k$$

gerade die nötigen Kongruenzen, um mit Hilfe des vorangegangenen Satzes schließen zu können, dass F_k eine Primzahl ist.

Sei nun umgekehrt vorausgesetzt, dass F_k eine Primzahl ist, dann ist nach Satz 8.5.2 von Euler und dem Gaußschen Reziprozitätsgesetz

$$3^{\frac{F_k - 1}{2}} \equiv \frac{3}{F_k} \equiv \frac{F_k}{3} \mod F_k$$

Mit $F_k = 2^{2^k} + 1 \equiv (-1)^{2^k} + 1 = 2 \equiv -1 \bmod 3$ folgt

$$3^{\frac{F_k - 1}{2}} \equiv \frac{F_k}{3} \equiv \frac{-1}{3} \equiv -1 \mod F_k$$

Beispiel Da F_k doppelt exponentiell in k wächst, kann man den Test per Hand nur für sehr kleine k durchführen. Wir betrachten hier $F_2 = 2^{2^2} + 1 = 2^4 + 1 = 17$. Diese Zahl ist prim, weil

$$3^{(F_2 - 1)/2} = 3^{2^3} = 3^8 = 3^{4 \cdot 2} = 13^2 \equiv -1 \mod 17$$

Aufgabe 11.7 Zeigen Sie mit dem Pepin Test, dass $F_3 = 257$ prim ist.

Bei der Anwendung des Lucas Tests auf eine beliebige Zahl n gibt es zwei Probleme:

1. Man muss die Primteiler von $n - 1$ kennen. Dies ist ein Faktorisierungsproblem und damit im Allgemeinen schwierig.

2. Man muss alle $n - 1$ Werte für a überprüfen. Dies bedeutet einen sehr hohen Rechenaufwand. (Die Anzahl könnte man verkleinern, wenn man berücksichtigt, dass es $\varphi(n - 1)$ Primitivwurzeln modulo n für n prim gibt. Man bleibt aber in der gleichen Größenordnung für den Rechenaufwand.)

Um das erste Problem in den Griff zu bekommen, könnte man hoffen, dass ein n bereits prim ist, falls $a^{n-1} \equiv 1 \bmod n$ ist für alle zu n teilerfremden a im Bereich von 1 bis $n - 1$. Das ist aber leider nicht richtig.

Definition 11.8 *Eine natürliche Zahl* $n \geq 2$ *heißt* Carmichael–Zahl, *falls n keine Primzahl ist und für alle* a *mit* ggT$(a, n) = 1$ *gilt:* $a^{n-1} \equiv 1 \bmod n$

Wir wollen zeigen, dass die Carmichael–Zahlen jedoch sehr speziell sind. Wir starten mit dem folgenden Satz.

Satz 11.9 *Sei n eine natürliche Zahl und n* $2^r \prod_{i=1}^{s} p_i^{r_i}$ *ihre Primfaktorzerlegung. Weiter sei*

$$G: \quad x \quad U_n \quad x^{n-1} \quad 1$$

Dann ist

$$U_n \; G \quad U_{2^r} \quad \prod_{i=1}^{s} \quad m_i \qquad mit \; m_i \quad \frac{p_i^{r_i-1} \; p_i \quad 1}{\text{ggT} \; p_i \quad 1 \; n \quad 1}$$

Beweis: Nach dem chinesischen Restsatz in Form von Lemma 5.13 und dem Satz 7.7 gilt

$$\Phi : U_n \quad U_{2^r} \quad \prod_{i=1}^{s} \quad \varphi \; p_i^{r_i}$$

Die Gruppe G besteht aus den Elementen, deren Ordnung $n \quad 1$ teilt. Dies gilt auch für das Bild von G unter dem Isomorphismus Φ. Für gerades n ist $n \quad 1$ ungerade. Da alle Elemente von U_{2^r} als Ordnung eine Zweierpotenz haben, hat nur $1 \quad U_{2^r}$ eine Ordnung, die $n \quad 1$ teilt. Daher liegt $\Phi \; G$ in $\{1 \quad \prod_{i=1}^{s} \quad \varphi \; p_i^{r_i}$. Nun heißt für $x \quad \overline{x_i} \quad \prod_{i=1}^{s} \quad \varphi \; p_i^{r_i}$ die Bedingung ord$x \; n \quad 1$ gerade

$$n \quad 1 \; x_i \quad 0 \mod \varphi \; p_i^{r_i} \qquad \text{für } i \quad 1 \quad s$$

Nach Satz 4.8 ist das äquivalent zu

$$x_i \quad 0 \mod \varphi \; p_i^{r_i} \quad \text{ggT} \; n \quad 1 \; \varphi \; p_i^{r_i}$$

Wegen $\varphi \; p_i^{r_i} \quad p_i^{r_i-1} \; p_i \quad 1$ und $p_i \quad n \quad 1$ ist

$$\text{ggT} \; n \quad 1 \; \varphi \; p_i^{r_i} \quad \text{ggT} \; n \quad 1 \; p_i \quad 1$$

Somit ist das Bild von G mit m_i wie in der Aussage des Satzes

$$\Phi \; G \quad \{1 \quad \prod_{i=1}^{s} m_i \quad \varphi \; p_i^{r_i}$$

und für $U_n \; G$ ergibt sich das Behauptete.

Korollar 11.10 *Sei n* 2 *eine natürliche Zahl, die keine Primzahl ist.*

1. *n ist eine Carmichael–Zahl genau dann, wenn n keine mehrfachen Primteiler hat und* $p \quad 1 \; n \quad 1$ *für jeden Primteiler p von n gilt.*
2. *Jede Carmichael–Zahl ist ungerade und das Produkt von mindestens drei verschiedenen Primzahlen.*

Beweis: n ist eine Carmichael–Zahl genau dann, wenn im vorangegangenen Satz $U_n \quad G$ gilt. Damit $U_n \; G$ trivial ist, muss $r \quad 0, r_i \quad 1$ und $p_i \quad 1 \quad \text{ggT} \; p_i \quad 1 \; n \quad 1$, d.h. $p_i \quad 1 \; n \quad 1$ für alle i gelten.

Eine gerade Zahl kann keine Carmichael–Zahl sein, weil für jeden ungeraden Primfaktor p die gerade Zahl $p \quad 1$ nicht die ungerade Zahl $n \quad 1$ teilen kann. Es bleibt zu zeigen, dass

$n = pq$ mit $p < q$ keine Carmichael–Zahl sein kann. Aus $q - 1 \mid n - 1$ folgt

$$0 \equiv n - 1 \equiv pq - 1 \equiv p(q-1) + (p-1) \equiv p - 1 \bmod q - 1$$

Wegen $0 < p - 1 < q - 1$ folgt $p = 1$, was unmöglich ist.

Die kleinsten Carmichael–Zahlen sind

$561 = 3 \cdot 11 \cdot 17$	$1105 = 5 \cdot 13 \cdot 17$	$1729 = 7 \cdot 13 \cdot 19$
$2465 = 5 \cdot 17 \cdot 29$	$2821 = 7 \cdot 13 \cdot 31$	$6601 = 7 \cdot 23 \cdot 41$
$8911 = 7 \cdot 19 \cdot 67$	$10585 = 5 \cdot 29 \cdot 73$	$15841 = 7 \cdot 31 \cdot 73$

Aufgabe 11.11 Zeigen Sie: Eine Zahl der Form $n = (6k+1)(12k+1)(18k+1)$ ist eine Carmichael–Zahl, falls alle drei Faktoren prim sind.

Alford, Granville und Pomerance haben gezeigt, dass es unendlich viele Carmichael–Zahlen gibt [AGP].

Die Untersuchung der Carmichael–Zahlen zeigt, dass man nicht einfach $a^{n-1} \equiv 1 \bmod n$ testen kann, um zu entscheiden, ob n prim ist. Wir müssen diese Bedingung also verschärfen. Genau dies geschieht im folgenden Satz.

Satz 11.12 (Solovay–Strassen Test) *Sei $n \geq 3$ ungerade. Dann ist n genau dann prim, wenn für jedes $0 < a < n$ mit $\mathrm{ggT}(a, n) = 1$ gilt*

$$a^{\frac{n-1}{2}} \equiv \frac{a}{n} \bmod n$$

Falls n nicht prim ist, ist die Kongruenz für mindestens die Hälfte aller a nicht erfüllt.

Beweis: Für n prim ist die Kongruenzbedingung der Satz 8.5.2 von Euler. Sei daher n nicht prim. Durch Quadrieren der Bedingung in der Voraussetzung erhalten wir $a^{n-1} \equiv 1 \bmod n$, somit ist n eine Carmichael–Zahl. Ihre Primfaktorzerlegung ist nach Korollar 11.10 von der Form $n = \prod_{i=1}^{s} p_i$ mit $s \geq 3$. Nach dem chinesischen Restsatz gilt

$$\Phi : U_n \cong \prod_{i=1}^{s} U_{p_i}$$

Sei nun ζ eine Primitivwurzel modulo p_1 und a , so dass $\Phi(a) = (\zeta, 1, \ldots, 1)$. Wir berechnen das Jacobi–Symbol

$$\frac{a}{n} = \frac{a}{\prod_{i=1}^{s} p_i} = \prod_{i=1}^{s} \frac{a}{p_i} = \frac{\zeta}{p_1} \prod_{i=2}^{s} \frac{1}{p_i} = -1$$

weil ζ als Primitivwurzel modulo p_1 kein Quadrat modulo p_1 ist.

Andererseits entspricht $a^{\frac{n-1}{2}}$ unter dem Isomorphismus Φ dem Element $(\zeta^{\frac{n-1}{2}}, 1, \ldots, 1)$ und kann damit niemals $(-1, 1, \ldots, 1)$ sein. Somit ist für dieses a die Bedingung in der Aussage nicht erfüllt.

Um die Größe der Menge

$$A: \quad a \quad U_n \quad a^{\frac{n-1}{2}} \quad \frac{a}{n} \mod n$$

abzuschätzen, beobachten wir, dass A gerade der Kern des Homomorphismus

$$\psi : U_n \quad U_n \quad a \quad a^{\frac{n-1}{2}} \quad \frac{a}{n}$$

ist. Wir haben eben gezeigt, dass $A \quad U_n$, also ψ nicht konstant, ist. Daher gilt

$$\frac{\#A}{\#U_n} \quad \frac{1}{\#\psi \; U_n} \quad \frac{1}{2}$$

Es bleibt das Problem, dass wir fast $n \; 2$ Zahlen a überprüfen müssen, um sicher zu entscheiden, ob n eine Primzahl ist. Für praktische Anwendungen löst man das Problem dadurch, dass man darauf verzichtet, sicher zu wissen, ob n prim ist, und nur testet, ob n sehr wahrscheinlich prim ist. Falls ein zufälliges a die Bedingung des Solovay–Strassen Tests erfüllt, dann ist n mit Wahrscheinlichkeit $\; 1 \; 2$ nicht prim. Wiederholt man dies für k verschiedene zufällige a und ist die Bedingung jedesmal erfüllt, dann ist n nur noch mit einer Wahrscheinlichkeit von $1 \; 2^k$ nicht prim. Bei genügend vielen Wiederholungen wird die Fehlerwahrscheinlichkeit schnell sehr klein, zum Beispiel kleiner als die Möglichkeit eines Soft– oder Hardwarefehlers des Computers, auf dem dieser Test implementiert ist.

Solche Tests, bei denen man nur mit großer Wahrscheinlichkeit feststellt, ob n prim ist, werden *probabilistische Tests* im Gegensatz zu den *deterministischen Primzahltests* genannt. In der Praxis sind sie sehr beliebt, weil sie meist viel schneller als deterministische sind.

Beispiel Wir wollen zeigen, dass der Test mit mindestens 75% Wahrscheinlichkeit ergibt, dass 89 prim ist. Wegen ggT $3 \; 89 \quad$ ggT $5 \; 89 \quad 1$ können wir im Solovay–Strassen Test $a \quad 3$ und $a \quad 5$ verwenden. Es gilt

$$3^{\frac{88}{2}} \quad 3^{44} \quad 1 \mod 89 \quad \text{bzw.} \quad 5^{\frac{88}{2}} \quad 5^{44} \quad 1 \mod 89$$

sowie

$$\frac{3}{89} \quad \frac{89}{3} \quad \frac{1}{3} \quad 1 \quad \text{bzw.} \quad \frac{5}{89} \quad \frac{89}{5} \quad \frac{1}{5} \quad 1$$

Daher ist für $a \quad \{3 \; 5$ die Bedingung des Solovay–Strassen Tests erfüllt und die Wahrscheinlichkeit, dass 89 nicht prim ist, kleiner als $\; 1 \; 2^{\; 2} \quad 1 \; 4$.

Aufgabe 11.13 Zeigen Sie auf geeignete Weise, dass der Solovay–Strassen Test die Zahl 73 mit einer Wahrscheinlichkeit von mindestens 85% als prim erklärt. Zeigen Sie mit diesem Test auch, dass 91 nicht prim ist.

Der Solovay–Strassen Test wurde unabhängig von Miller und Rabin verbessert, indem sie die Notwendigkeit der Berechnung des Jacobi–Symbols in der Bedingung eliminierten.

Satz 11.14 (Miller–Rabin Test) *Sei n 3 ungerade und n 1 $2^t m$ für m ungerade. n ist genau dann eine Primzahl, wenn für jede zu n teilerfremde natürliche Zahl* 0 a n *gilt*

$$a^m \quad 1 \mod n \qquad \textit{oder} \qquad a^{2^s m} \quad 1 \mod n \textit{ für ein } s \quad \{0\ 1 \quad t \quad 1$$

Ist n keine Primzahl, so erfüllt höchstens ein Viertel aller Zahlen a eine der Bedingungen.

Beweis: Falls n eine Primzahl ist, dann ist n $\mathbb{F}_n$ ein Körper und $\mathbb{F}_n$ eine zyklische Gruppe. Insbesondere ist $a^{n\ 1}$ $a^{2^t m}$ 1 mod n für a 0 mod n. Wählt man s $_0$ minimal mit $a^{2^{s\ 1}m}$ 1 mod n, dann ist entweder s 0 und a^m 1 mod n oder $a^{2^s m}$ 1 eine Quadratwurzel von 1. Da in einem Körper nur 1 Quadratwurzeln von 1 sind, muss dann $a^{2^s m}$ 1 mod n gelten.

Sei nun n keine Primzahl und n $\prod_{i\ 1}^{r} p_i^{r_i}$ seine Primfaktorzerlegung. Neben der Menge

$$A: \quad a \quad U_n \quad a^m \quad 1 \text{ oder } \quad 0 \quad s \quad t \quad 1 : a^{2^s m} \quad 1$$

betrachten wir noch die folgenden Untergruppen von U_n

$$G: \quad x \quad U_n \quad x^{n\ 1} \quad 1 \qquad \text{und} \qquad H: \quad \{x \quad U_n \quad x^m \quad 1$$

Offensichtlich gilt H A G und H A A, also ist A die Vereinigung von Restklassen von H. Wir wollen A H G H identifizieren.

Seien t_i m_i definiert durch φ $p_i^{r_i}$ $p_i^{r_i\ 1}$ p_i 1 $2^{t_i} m_i$ mit m_i ungerade. Wir betrachten die Abbildung

$$\pi : U_n \quad \prod_{i\ 1}^{r} U_{p_i^{r_i}} \quad \prod_{i\ 1}^{r} \quad \varphi\ p_i^{r_i} \qquad \prod_{i\ 1}^{r} \quad 2^{t_i} \quad : Q$$

wobei die letzte Abbildung aus den Projektionen φ $p_i^{r_i}$ m_i 2^{t_i} 2^{t_i} besteht. Somit gilt Ker π $\prod_{i\ 1}^{r}$ m_i . Elemente des Kerns haben also eine Ordnung, die $\prod m_i$ teilt, insbesondere also ungerade ist. Somit gilt für ein x G Ker π mit $x^{2^s m}$ 1, also auch $x^{2^{s\ 1}m}$ 1, bereits x^m 1. Folglich ist der Kern der Einschränkung von π auf G gleich der Untergruppe H.

Was ist das Bild von π? G besteht aus den Elementen von U_n, deren Ordnung n 1 $2^t m$ teilt, somit haben auch die Bilder von G unter π eine solche Ordnung. Wir können aber auch Q auf die offensichtliche Weise mit einer Abbildung $\varepsilon : Q$ U_n in U_n einbetten, so dass ε π id gilt. Daher gilt

$$\pi\ G \quad \{x \quad Q \quad \text{ord} x\ 2^t m \quad \{x \quad Q \quad \text{ord} x\ 2^t$$

Die Elemente von 2^{t_i} , deren Ordnung 2^t teilt, finden wir durch das Lösen der Gleichung $2^t x$ 0 mod 2^{t_i}. Nach Satz 4.8 ist das äquivalent zu x 0 mod 2^{k_i} mit k_i : max$\{t_i \quad t\ 0$. Für t_i' : t_i k_i min$\{t_i\ t$ gilt 2^{k_i} 2^{t_i} 2^{t_i} und insgesamt

$$G\ H \quad \prod_{i\ 1}^{r} 2^{k_i} \quad 2^{t_i} \qquad \prod_{i\ 1}^{r} \quad 2^{t_i} \quad : Q'$$

Dabei wird 1 H unter dem ersten Isomorphismus auf

$$\varphi\ p_1^{r_1}\ \ 2\qquad \varphi\ p_s^{r_s}\ \ 2\qquad 2^{t_1}\ \ 1\qquad 2^{t_s}\ \ 1$$

und damit unter dem zweiten auf

$$2^{t_1}\ \ 1\qquad 2^{t_s}\ \ 1$$

abgebildet — siehe die Diskussion nach Lemma 7.12. Nun entspricht $A\ \ H\quad G\ \ H$ unter dem Isomorphismus $G\ \ H\quad Q'$ der Menge

$$A':\qquad x_i\quad \prod\quad p_i^{r_i}\qquad 0\quad s\quad t\quad 1:\ 2^s x_i\qquad 2^{t_i}\ \ 1\qquad \{0$$

Aus der Bedingung $2^s x_i\quad 2^{t_i}\ \ 1\quad 0$ in 2^{t_i} folgt $2^s\ \ ^1 x_i\quad 0$, also bedeutet die Bedingung gerade, dass jedes x_i die Ordnung $2^s\ \ 1$ in 2^{t_i} hat. Somit können wir A' auch schreiben als

$$A':\qquad x_i\quad \prod\quad p_i^{r_i}\quad \mathrm{ord}\,x_1\qquad\qquad \mathrm{ord}\,x_r$$

Wir müssen nun die Elemente in Q' zählen, die in jeder Komponente die gleiche Ordnung haben. Die Gruppe 2^{t_i} hat ein Element der Ordnung 0 und $2^s\ \ 1$ Elemente der Ordnung 2^s für $0\quad s\quad t_i'$, nämlich die Restklassen von $2^{t_i}\ \ ^s u$ mit $1\quad u\quad 2^s$ ungerade. Somit erhalten wir mit $T:\quad \min\{t_i'$

$$\#A'\quad 1\quad \sum_{s\ \ 1}^{T} 2^{s\ \ 1\ \ r}\quad 1\quad \sum_{s\ \ 0}^{T\ \ 1} 2^{r\ \ s}\quad 1\quad \frac{2^{rT}\quad 1}{2^r\quad 1}$$

Unsere Aufgabe ist zu zeigen, dass der Quotient $\#U_n\ \#A\quad \#\ U_n\ G\quad \#G\ \#A\quad \#\ U_n\ G\quad \#Q'\ \#A'$ mindestens 4 ist. Wir behaupten, dass

$$\#Q'\quad 2^{r\ \ 1}\#A'$$

und zeigen sogar $2^{rT}\quad 2^{r\ \ 1}\#A'$ durch die folgende Rechnung

$$\begin{aligned}
&2^{rT}\quad 2^{r\ \ 1}\ \ 1\quad \frac{2^{rT}\quad 1}{2^r\quad 1}\\
&2^r\quad 1\ 2^{rT}\quad 2^{r\ \ 1}\ 2^r\quad 1\quad 2^{r\ \ 1}\ 2^{rT}\quad 1\\
&2^r\quad 1\ 2^{rT}\quad 2^{r\ \ 1} 2^{rT}\quad 2^{r\ \ 1}\ \ 1\ 2^r\\
&2^{r\ \ 1}\ \ 1\ 2^{rT}\quad 2^{r\ \ 1}\ \ 1\ 2^r\\
&2^{r\ \ T\ \ 1}\quad 1
\end{aligned}$$

was wegen $r\ \ T\quad 1$ wahr ist.

Somit gilt für $r\quad 3$ bereits $\#U_n\ \#A\quad \#Q'\ \#A'\quad 4$. Für $r\quad 2$ erhalten wir nur $\#Q'\ \#A'\quad 2$. Nun kann bei $r\quad 2$ die Zahl n nach Korollar 11.10 keine Carmichael–Zahl sein, daher gilt $\#\ U_n\ G\quad 2$, und wir finden wiederum $\#U_n\ \#A\quad \#\ U_n\ G\quad \#Q'\ \#A'\quad 2\ \ 2\quad 4$.

Wir sehen, dass der Miller–Rabin Test dem Solovay–Strassen Test auch insofern überlegen ist, als die Fehlerwahrscheinlichkeit mit dem Test jeder Zahl a um $1\ \ 4$ statt nur um $1\ \ 2$ fällt. Tatsächlich gilt sogar das Folgende:

Aufgabe 11.15 Zeigen Sie, dass ein a, das die Bedingung des Miller–Rabin Tests erfüllt, auch die Bedingung des Solovay–Strassen Tests erfüllt.

Beispiel Wir überprüfen 89 auch mit dem Miller–Rabin Test. Es gilt $n \quad 1 \quad 88 \quad 2^3 \quad 11$, also $t \quad 3$. Für die Testzahlen $a \quad 3$ und $a \quad 5$ erhalten wir:

$$\begin{array}{llll} 3^{11} & 37 & \bmod n & 5^{11} \quad 55 \quad \bmod n \\ 3^{2\cdot 11} & 37^2 & 34 \bmod n & 5^{2\cdot 11} \quad 55^2 \quad 1 \bmod n \\ 3^{4\cdot 11} & 34^2 & 1 \bmod n & \end{array}$$

Da zwei zufällige Zahlen die Testbedingung erfüllen, ist 89 mit einer Wahrscheinlichkeit von mindestens $1 \quad 1 \; 4^{\,2} \quad 15 \; 16$ prim.

Aufgabe 11.16 Zeigen Sie durch den Miller–Rabin Test, dass 73 mit einer Wahrscheinlichkeit von mindestens 98% prim ist. Zeigen Sie damit auch, dass 91 nicht prim ist.

Unter Annahme einer naheliegenden Verallgemeinerung der Riemannschen Vermutung [N] kann man zeigen, dass für ein zusammengesetztes n ein $0 \quad a \quad 2\log^2 n$ existiert, das die Bedingung des Miller–Rabin Tests nicht erfüllt. Dann wird der Miller–Rabin Test angewandt auf alle $0 \quad a \quad 2\log^2 n$ zu einem deterministischen Test, der in polynomialer Zeit arbeitet.

Agrawal, Kayal und Saxena haben im Jahr 2002 ohne Annahme der Riemannschen Vermutung gezeigt, dass man in polynomialer Zeit entscheiden kann, ob eine gegebene Zahl prim ist [AKS]. Im Verhältnis zu den probabilistischen Tests ist der Algorithmus langsam, liefert dafür aber ein sicheres Ergebnis. Die Grundlage der AKS–Methode ist der folgende Satz.

Satz 11.17 *Eine natürliche Zahl n ist genau dann prim, wenn im Polynomring* X

$$X \quad a^{\,n} \quad X^n \quad a \mod n$$

für alle a *gilt.*

Beweis: Falls n prim ist, folgt die Kongruenz genau wie im Beweis von Hilfssatz 4.6 unter Ausnutzung des kleinen Satzes von Fermat. Falls n nicht prim ist, schreiben wir $n \quad p^l m$ mit einer Primzahl p und einer zu p teilerfremden Zahl m . Der Koeffizient von X^p in $X \quad 1^{\,n}$ ist

$$\binom{n}{p} \quad \frac{n!}{p!\; n \quad p\;!} \quad \frac{n\; n \quad 1 \quad n \quad p \quad 1}{p\; p \quad 1 \quad 1}$$

Da im Zähler p aufeinanderfolgende Zahlen stehen, ist genau eine von ihnen durch die Primzahl p teilbar. Diese muss also von der Form $n \quad p^l m$ sein. Im Nenner steht auch noch ein p, daher ist $\binom{n}{p} \quad p^{l \quad 1} m'$ für ein $m' \quad$ mit ggT $p \; m' \quad 1$. Folglich ist $\binom{n}{p} \quad 0 \bmod p^l$ und somit nach Lemma 4.7 auch $\binom{n}{p} \quad 0 \bmod n$. Also ist die Kongruenz $X \quad 1^{\,n} \quad X^n \quad 1 \bmod n$ nicht erfüllt.

Die wesentliche Idee des AKS Tests ist, diese Bedingung nicht in $n \quad X$ zu testen, sondern noch modulo eines Polynoms $X^r \quad 1$, wobei r in der Größenordnung von $\log n^{\,15/2}$ gewählt werden kann [AKS]. Die folgende Version des Satzes geht auf Bernstein und Pomerance zurück, siehe [P, B].

Satz 11.18 (Agrawal/Kayal/Saxena) *Sei n eine natürliche Zahl. Wir setzen voraus, dass es eine Primzahl r gibt, die n nicht teilt, sowie einen Primfaktor q $r-1$ mit $q \geq 2\sqrt{r}\log_2 n$ und*

$$n^{\frac{r-1}{q}} \not\equiv 1 \mod r$$

Falls dann für alle $0 \leq a \leq l$ gilt

$$(X+a)^n \equiv X^n + a \mod (n, X^r - 1)$$

und n keine Primfaktoren $\leq l$ besitzt, so ist n eine Primzahlpotenz.

Die Unterscheidung, ob eine Zahl n eine Primzahl oder eine Primzahlpotenz ist, ist einfach. Man berechnet für $2 \leq k \leq \log_2 n$ numerisch $\sqrt[k]{n}$ und überprüft, ob die k–te Potenz mit n übereinstimmt.

Beweis: Aus den Voraussetzungen folgt, dass ein Primteiler p von n existiert mit

$$p^{\frac{r-1}{q}} \not\equiv 1 \mod r$$

Da r kein Teiler von n ist, ist ggT$(r, p) = 1$ und damit $p \in U_r$. Sei $d = \mathrm{ord}_{U_r} p$. Aus folgt $q \mid d$ und damit $d \geq l$.

Wir betrachten nun die Einheitengruppe R^* des endlichen Ringes $R = \mathbb{F}_p[X]/(X^r - 1)$. Auf R haben wir für jedes m die Endomorphismen (siehe Aufgabe 11.19)

$$\Phi_m : R \to R,\quad \overline{f} \mapsto \overline{f}^m$$
$$\sigma_m : R \to R,\quad \overline{f} \mapsto \overline{f(X^m)}$$

Für die Homomorphismen gilt

$$\Phi_{mk} = \Phi_m \circ \Phi_k \quad \text{bzw.} \quad \sigma_{mk} = \sigma_m \circ \sigma_k$$

weil

$$\Phi_{mk}(\overline{f}) = \overline{f}^{mk} = (\overline{f}^k)^m = (\Phi_k(\overline{f}))^m = (\Phi_m \circ \Phi_k)(\overline{f})$$
$$\sigma_{mk}(\overline{f}) = \overline{f(X^{mk})} = \overline{f(X^{mk})} = \sigma_m(\overline{f(X^k)}) = (\sigma_m \circ \sigma_k)(\overline{f})$$

Sei G die von den linearen Polynomen $\overline{X+a}$, $0 \leq a \leq l$, erzeugte Untergruppe von R^*. Offensichtlich gilt $\Phi_m(G) \subseteq G$. Weiter sei

$$I = \{m \mid \Phi_m(g) = \sigma_m(g)\ \forall g \in G\}$$

In dieser Menge I liegt die Zahl n nach Voraussetzung und die Primzahl p nach Satz 11.17. Die Menge I ist auch multiplikativ abgeschlossen, denn für $m, k \in I$ ist mit $g \in G$ auch $\Phi_k(g) = \sigma_k(g) \in G$ und somit folgt

$$\Phi_{mk}(g) = \Phi_m(\Phi_k(g)) = \Phi_m(\sigma_k(g)) = \sigma_m(\sigma_k(g)) = \sigma_{mk}(g)$$

Insbesondere enthält I also die Elemente der Form $n^i p^j$.

Das Polynom $X^r - 1$ zerfällt in $\mathbb{F}_p[X]$ in den irreduziblen Faktor $X - 1$ und $r - 1$ d irreduzible Faktoren vom Grad d [MS, 3.2.3]. Sei h ein solcher Faktor, dann ist $\mathbb{F}_p[X]/(h)$ der endliche Körper, $\mathbb{F}_{p^d}$, mit p^d Elementen.

Sei nun H das Bild von G unter der Projektion $\pi : R \to \mathbb{F}_p[X]/(h) \cong \mathbb{F}_{p^d}$. Wegen der Voraussetzung $p \nmid l$ sind die Bilder von $\overline{X - a}$ unter π alle verschieden. Selbst alle 2^l Produkte von bis zu l verschiedenen Faktoren aus den $\pi(\overline{X - a})$ sind verschieden in H, weil $d \le \deg h \le l$. Somit folgt

$$\#H \ge 2^l \ge 2^{2\lfloor \overline{r} \log_2 n \rfloor} \ge n^{2\lfloor \overline{r} \rfloor}$$

Seien nun $m_1, m_2 \in I$ mit $m_1 \equiv m_2 \bmod r$. Wir behaupten, dass dann sogar $m_1 \equiv m_2 \bmod \#H$ gilt. Wir schreiben $m_2 = m_1 + kr$ für ein $k \ge 0$ und rechnen unter Ausnutzung von $\overline{X}^r = 1$ in R für ein $\overline{g} \in G$

$$\begin{aligned}\Phi_{m_2}(\overline{g}) &= \Phi_{m_1+kr}(\overline{g}) = \sigma_{m_1+kr}(\overline{g}) = g(\overline{X})^{m_1+kr} \\ &= g(\overline{X})^{m_1}(\overline{X}^r)^k = g(\overline{X})^{m_1} = \sigma_{m_1}(\overline{g}) = \Phi_{m_1}(\overline{g}) \\ &\\ &= \overline{g}^{m_1+kr} = \overline{g}^{m_1}\end{aligned}$$

Die analoge Gleichung gilt dann auch nach der Projektion unter π in $H \subseteq \mathbb{F}_{p^d}$. In dem Körper können wir kürzen und erhalten $x^{kr} = 1$ für alle $x \in H$. Da H als endliche multiplikative Untergruppe eines Körpers zyklisch ist (Satz 7.2), folgt $\#H \mid kr = m_2 - m_1$, also $m_1 \equiv m_2 \bmod \#H$.

Wir betrachten nun die Elemente $n^i p^j \in I$ für natürliche Zahlen $0 \le i, j \le \sqrt{r}$. Da es davon $(\lfloor \sqrt{r} \rfloor + 1)^2 > r$ Stück gibt, finden wir $i, j \neq i', j'$ mit $n^i p^j \equiv n^{i'} p^{j'} \bmod r$. Nach dem eben Gezeigten folgt $n^i p^j \equiv n^{i'} p^{j'} \bmod \#H$. Da $n^i p^j, n^{i'} p^{j'} \le n^{\lfloor \overline{r} \rfloor} p^{\lfloor \overline{r} \rfloor} \le n^{2\lfloor \overline{r} \rfloor} \le \#H$ ist, gilt sogar $n^i p^j = n^{i'} p^{j'}$. Aus der Eindeutigkeit der Primfaktorzerlegung folgt, dass n eine Potenz der Primzahl p ist.

Aufgabe 11.19 Beweisen Sie, dass die Abbildungen Φ_m und σ_m im Beweis des Satzes 11.18 wohldefinierte Homomorphismen sind.

Zusatzaufgaben

Aufgabe 11.20 Wenden Sie den Lucas Test jeweils auf $n = 701$ und 7001 an.

Aufgabe 11.21 Zeigen Sie, dass der Pepin Test auch mit 5 statt 3 als Basis funktioniert.

Aufgabe 11.22 (Proth) Sei $n = 1 \cdot 2^k n + 1$, $2^k > \sqrt{n}$ und $a^{(n-1)/2} \equiv -1 \bmod n$ für ein a. Zeigen Sie: n ist prim.

Aufgabe 11.23 Untersuchen Sie mit dem Pepin Test, ob die Zahlen $F_3 = 257$ und $F_4 = 65537$ prim sind. Bei F_4 sollten Sie dazu nach Möglichkeit ein Computeralgebrasystem benutzen.

Aufgabe 11.24 Untersuchen Sie mit dem Lucas–Lehmer Test, ob die Zahl $n = 2^{11} - 1$ prim ist.

12 Faktorisierungsalgorithmen

Sei n eine zusammengesetzte natürliche Zahl. In diesem Abschnitt wollen wir diskutieren, wie man möglichst schnell die Primfaktorzerlegung von n finden kann. Dafür reicht es aus, Algorithmen zu entwickeln, bei denen n nicht–trivial in ein Produkt zweier natürlicher Zahlen zerlegt werden kann. Die rekursive Anwendung des Algorithmus auf die einzelnen Faktoren liefert schließlich die vollständige Zerlegung von n. Die Frage, wie viel Zeit es kostet, eine große Zahl zu faktorisieren, ist hochgradig aktuell, weil viele moderne kryptographische Verfahren auf der Annahme beruhen, dass man bei sehr großen Zahlen die großen Primfaktoren nur mit sehr großem Zeitaufwand finden kann.

Wir werden zwei grundsätzlich verschiedene Ansätze zur Lösung dieses Problems erläutern. Einer davon ist von Shor so weit entwickelt worden, dass er auf Quantencomputern in polynomialer Zeit läuft, jedoch steckt deren praktische Entwicklung noch in den Anfängen [Sh].

Die Probedivision ist das einfachste Verfahren, um einen Faktor zu finden. Dabei teilt man die Zahl n durch die natürlichen Zahlen $a \quad \sqrt{n}$, bis man einen Faktor findet. Diese Methode ist jedoch sehr langsam. Trotzdem führt man häufig eine Probedivision mit $a \quad \log n$ bei einer Zahl n durch, um kleine Primfaktoren zu finden, bevor man einen komplizierten Faktorisierungsalgorithmus benutzt. Schließlich hat eine zufällig gewählte Zahl n mit hoher Wahrscheinlichkeit einen kleinen Primfaktor.

Bereits Fermat entwarf einen Faktorisierungsalgorithmus, der auf der folgenden Beobachtung beruht.

Lemma 12.1 *Sei n eine natürliche Zahl.*

1. *Ist n eine ungerade zusammengesetzte Zahl, dann ist n die Differenz zweier Quadrate, d.h.* $n \quad x^2 \quad y^2$ *mit* $x \; y \quad$ *, wobei* $x \quad y \bmod n$ *gilt.*
2. *Sei* $x^2 \quad y^2 \quad cn$ *mit* $x \; y \; c \quad$ *und* $x \quad y \bmod n$*, dann sind* $a : \quad \mathrm{ggT}\; x \quad y \; n$ *und* $b : \quad \mathrm{ggT}\; x \quad y \; n$ *echte Teiler von n.*

Beweis: Falls $n \quad ab$ mit ungeraden Zahlen $a \quad b \quad 3$ ist, setzen wir

$$x : \quad \frac{a \quad b}{2} \qquad \text{und} \qquad y : \quad \frac{a \quad b}{2}$$

Dann ist $x^2 \quad y^2 \quad n$ und $n \quad x \quad y \quad 0$. Sollte x kongruent zu y sein, so folgt $x \quad y$. Dies ist aber äquivalent zu $b \quad 0$ im Widerspruch zu $b \quad 3$.

S. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie,*
DOI 10.1007/978-3-8348-8263-9_12,

Um den zweiten Teil der Aussage zu beweisen, bemerken wir, dass $x \not\equiv y \bmod n$ äquivalent zu $x - y \not\equiv 0 \bmod n$ ist. Somit gilt $a \nmid b - n$. Aus der Zerlegung

$$x^2 - y^2 = x - y\ x + y = cn$$

und der Existenz und Eindeutigkeit der Primfaktorzerlegung folgt, dass wir c und n so in ganze Zahlen zerlegen können, dass $c = de$ und $n = ml$ mit $x - y = dm$ und $x + y = el$ gilt. Damit sind m und l Teiler von a bzw. b. Wegen $a \nmid b - n$ muss $m \neq n$ sein, also auch $m \neq 1$. Folglich sind auch a und b echte Teiler von n.

Warnung Die Voraussetzung $x \not\equiv y \bmod n$ im zweiten Teil des Lemmas ist wichtig, denn für jede ungerade Zahl n gilt mit

$$x = \frac{n-1}{2} \quad \text{und} \quad y = \frac{n-1}{2}$$

die Gleichung $x^2 \equiv y^2 \bmod n$, jedoch ist $x - y = n$ und $x + y = 1$. Man findet daher durch ggT $x - y, n$ oder ggT $x + y, n$ keinen echten Teiler.

Um eine Zahl n zu faktorisieren, suchen wir also x, y mit $x^2 \equiv y^2 \bmod n$, aber $x \not\equiv \pm y \bmod n$. Wir beschreiben nun verschiedene Möglichkeiten, solche x, y zu finden. Die einfachste Möglichkeit ist der folgende Algorithmus von Fermat:

1. Man berechne $x := \lceil \sqrt{n} \rceil$ und $z := x^2 - n$.
2. Falls $z = y^2$ ein Quadrat ist, bestimmt man ggT $x - y, n$ und findet damit Teiler von n. Falls ein echter Teiler von n dabei ist, ist man fertig.
3. Andernfalls erhöhe man x um eins, $x := x + 1$, und setze entsprechend $z := z + 2x + 1$, so dass weiter $z = x^2 - n$ gilt. Man fahre mit 2 fort.

Aufgabe 12.2 Zeigen Sie, dass der Algorithmus nach endlich vielen Schritten einen echten Teiler von n findet.

Beispiel Sei $n = 1649$. Wir starten den Algorithmus also mit $x = 41$. Es gilt

x	z	$x^2 - n$
41	32	2^5
42	115	$5 \cdot 23$
43	200	$2^3 \cdot 5^2$
44	287	$7 \cdot 41$
45	376	$2^3 \cdot 47$
$\vdots$		$\vdots$
57	1600	$2^6 \cdot 5^2 = 40^2$

Wir finden somit die Teiler ggT $57 - 40, 1649 = 17$ und ggT $57 + 40, 1649 = 97$. Tatsächlich gilt $17 \cdot 97 = 1649$.

Hierbei haben wir 17 Schritte benötigt, also einen mehr als beim Probedivisionsverfahren nötig gewesen wäre, um den Teiler 17 zu finden. Tatsächlich ist der Fermat Algorithmus in

dieser einfachen Form im Allgemeinen langsamer als das Probedivisionsverfahren. Wir hätten aber schon früher (diese) Teiler von n finden können, wenn wir die Primfaktorzerlegungen der z betrachtet hätten. Denn aus $41^2 \equiv 2^5 \bmod n$ und $43^2 \equiv 2^3 \cdot 5^2 \bmod n$ erhalten wir $41^2 \cdot 43^2 \equiv 2^8 \cdot 5^2 \bmod n$, also

$$114^2 \equiv 41 \cdot 43^2 \equiv 2^4 \cdot 5^2 \equiv 80^2 \bmod n$$

Nach dem Lemma erhalten wir dann die Faktoren ggT$(1649, 114 - 80) = 17$ und ggT$(1649, 114 + 80) = 97$.

Aus diesem Beispiel erhalten wir eine neue Faktorisierungsstrategie. Wähle geschickt Zahlen x_i, $i \in I$, berechne $z_i \equiv x_i^2 \bmod n$. Der Fermat Algorithmus suggeriert die Wahl $x_i := \sqrt{n} + i$ und $z_i := x_i^2 - n$ für ein Intervall $I = [0, c]$. (Hier könnte man auch andere Repräsentanten von x_i^2 modulo n wählen, z.B. z_i mit $|z_i| < n/2$. Diese Wahl hat aber einen entscheidenden Vorteil, wie wir gleich sehen werden.) Danach faktorisieren wir die z_i und suchen eine Teilmenge $J \subseteq I$, so dass $\prod_{i \in J} z_i = y^2$ ein Quadrat ist. Nach Definition der z_i gilt

$$\prod_{i \in J} x_i^2 \equiv y^2 \bmod n$$

Mit etwas Glück ist $\prod_{i \in J} x_i \neq \pm y \bmod n$, und wir finden nach dem Lemma echte Teiler von n.

Hier müssen noch einige Details geklärt werden, zum Beispiel die Faktorisierung der z_i. Da bereits am Anfang $z_i \approx 2\sqrt{n}i$ gilt, sind die z_i auch noch recht groß. Man scheint daher aus einem Faktorisierungsproblem sehr viele etwas kleinere gemacht zu haben. Man löst dies dadurch, dass man nur solche z_i betrachtet, die das Produkt von vielen kleinen Primzahlen sind. Sollte dies nicht der Fall sein, verwirft man dieses z_i und x_i einfach. Die erlaubten z_i werden durch die folgende Definition festgelegt:

Definition 12.3 *Eine* Faktorbasis *B ist eine endliche Teilmenge von $\{-1\}$. Für eine Zahl $b \neq \pm 1$ ist*

$$B = \{-1\} \cup \{p \mid p \text{ prim}, p \mid b\}$$

die Faktorbasis zu *b. Eine Zahl n heißt B–*glatt*, falls sie ein Produkt von Potenzen von Elementen aus B ist, d.h.*

$$n = \prod_{p \in B} p^{r_p} \quad \text{mit } r_p \geq 0$$

*Entsprechend heißt die Zahl n auch b–*glatt*, falls sie B–glatt ist, wobei B die Faktorbasis zu b ist.*

Wir wählen nun eine Zahl $b \neq \pm 1$. Die Faktorisierung der b–glatten Zahlen wird nun durch Probedivision mit den $p \mid b$ realisiert. Die nicht b–glatten z_i werden verworfen. Nun müssen wir eine Teilmenge J von I bestimmen, so dass $\prod_{i \in J} z_i$ ein Quadrat ist. Sei dafür

$$B = \{-1, p_1, \ldots, p_s\} \quad \text{und} \quad z_i = \prod_{j=1}^{s} p_j^{r_{ij}}$$

Wir definieren die Exponentenmatrix modulo 2 als

$$E \qquad \begin{matrix} r_{i0} \\ r_{i1} \\ \vdots \\ r_{is} \end{matrix} \qquad \text{Mat } s \quad \#I \ \mathbb{F}_2$$

Sei $f \quad \overline{f}_i \quad \mathbb{F}_2^{\#I}, f_i \quad \{0\ 1$, ein Element des Kerns von E, d.h. $\sum_i f_i r_{ij} \quad 0 \bmod 2$ für alle $j \quad 1 \quad s$. Dann ist

$$z : \quad \prod_{i \ I} z_i^{f_i} \quad \prod_{j \ 1}^{s} p_j^{\sum_i f_i r_{ij}}$$

ein Quadrat, da alle Exponenten der p_j gerade sind.

Natürlich sind wir nur an nicht–trivialen Elementen des Kerns interessiert. Diese können wir zum Beispiel mit dem Gauß Algorithmus aus der Linearen Algebra bestimmen, es gibt jedoch dafür auch noch schnellere Algorithmen. Der Kern ist mit Sicherheit nicht–trivial, sobald $\#I \quad s \quad 1$ ist. Wir produzieren also solange x_i und z_i, bis diese Bedingung erfüllt ist. Sollten wir Pech haben und aus

$$\prod_{i \ I} x_i^{f_i} \qquad z \quad y^2 \mod n$$

mit dem Lemma 12.1 keine nicht–trivialen Teiler von n bekommen, so produzieren wir einfach weitere x_i und z_i und suchen neue Elemente des Kerns der vergrößerten Exponentenmatrix E.

Wir haben bereits angedeutet, dass die Wahl des Repräsentanten $z_i : \quad x_i^2 \quad n$ für die Restklasse von x_i^2 modulo n besondere Vorteile bietet. Bei dieser Wahl können nämlich nicht alle Primzahlen in der Primfaktorzerlegung von z_i auftreten. Um das einzusehen, sei p ein Primfaktor von z_i, dann folgt aus $z_i \quad x_i^2 \quad n$, dass $x_i^2 \quad n \bmod p$ ist. Wir dürfen annehmen, dass wir die relativ wenigen Primzahlen in der Faktorbasis darauf getestet haben, ob sie Teiler von n sind. Falls wir einen gefunden hätten, wären wir fertig gewesen. Also gilt $n \quad 0 \bmod p$ und $x_i^2 \quad n \bmod p$ bedeutet, dass n ein quadratischer Rest modulo p ist. Folglich brauchen wir in die Faktorbasis nur Primzahlen aufnehmen, für die

$$\frac{n}{p} \qquad 1$$

gilt. Dies schließt etwa die Hälfte aller Primzahlen aus.

Für die praktische Ausführung ist die Wahl der Schranke b, bis zu der man Primzahlen in die Faktorbasis B aufnimmt, von entscheidender Bedeutung. Ein zu kleines b bedeutet, dass nur sehr wenige der produzierten Zahlen z_i b–glatt sein werden; ein zu großes b bedeutet einen hohen Aufwand bei der Faktorisierung und der Berechnung des Kerns von E. Durch Untersuchungen über die Dichte von b–glatten Zahlen kommt man zur optimalen Wahl dieses b als

$$b \quad \exp \quad \log n \log\log n \ ^{1/2} \quad 2$$

Bei dieser Wahl muss man etwa $b^{2}\ \log\log b$ von den x_i produzieren, um genügend b–glatte Zahlen zu finden [CP, 6.1]. Weiter ist es bei dieser Wahl so, dass die z_i kleiner als $n\ 2$ sind, also vom Betrag her die kleinsten Repräsentanten von x_i^2 modulo n sind.

Bei dem obigen Algorithmus liegen die z_i in der Größenordnung von $n^{1/2\ \varepsilon}$ mit $0\quad\varepsilon\quad 1\ 2$, dadurch entsteht ein hoher Aufwand bei der Faktorisierung durch Probedivision mit den Elementen der Faktorbasis. Man kann auf zwei Arten diesen Aufwand reduzieren: Man produziert durch eine neue Methode nur kleinere z_i oder man verbessert den Teilbarkeitstest durch die Elemente von B. Das erste führt zum *Kettenbruchalgorithmus von Brillhart–Morrison* und das zweite zum *quadratischen Sieb*.

Der Kettenbruchalgorithmus geht auf Methoden von Gauß und Legendre zurück, um Quadrate modulo n zu finden. Sei $p_i\ q_i$ ein Näherungsbruch in der Kettenbruchentwicklung von $\sqrt{n}$. Diese erfüllen nach Satz 10.19 die Gleichung

$$p_i^2 \qquad 1\ ^{i}\ ^{1}c_i \mod n$$

wobei die c_i natürliche Zahlen mit $c_i\quad 2\sqrt{n}$ sind. Wir wählen also $x_i:\quad p_i$ und $z_i:\qquad 1\ ^{i}\ ^{1}c_i$ als Repräsentanten von x_i^2 mod n und erhalten damit relativ kleine z_i.

Auch hier brauchen wir eine Primzahl p nur dann in die Faktorbasis aufnehmen, wenn für sie $\frac{n}{p}\qquad 1$ gilt. Der Grund ist ein ähnlicher wie beim Fermat Algorithmus. Sei p ein Teiler von z_i, von dem wir auch wieder annehmen, dass er n nicht teilt. Dann folgt aus $z_i\quad p_i^2\quad nq_i^2$ die Kongruenz $p_i^2\quad nq_i^2 \mod p$. Da p_i und q_i teilerfremd sind, kann p nicht beide teilen; wegen der Kongruenz damit sogar keinen. q_i ist daher eine Einheit modulo p, und wir erhalten, dass $n\quad p_i\ q_i\ ^{2} \mod p$ ein quadratischer Rest modulo p ist. Wir haben damit wieder $\frac{n}{p}\qquad 1$.

Falls die Periode der Kettenbruchentwicklung von $\sqrt{n}$ klein ist, bekommt man eventuell nicht genügend viele $x_i\ z_i$, damit die Exponentenmatrix einen nicht–trivialen Kern hat. In diesem Fall benutzt man zusätzlich die Näherungsbrüche der Kettenbruchentwicklungen von $\sqrt{kn}$ für $k\quad$, denn schließlich folgt aus $p_i^2\quad knq_i^2\qquad 1\ ^{i}\ ^{1}c_i$ ebenfalls $p_i^2\qquad 1\ ^{i}\ ^{1}c_i \mod n$. Hier entsteht aber ein neues Problem, man kann nicht mehr wie oben folgern, dass in der Primfaktorzerlegung der $z_i\qquad 1\ ^{i}\ ^{1}c_i$ nur Primzahlen auftreten, modulo denen n ein quadratischer Rest ist. Man muss daher jetzt die komplette Faktorbasis zur Schranke b benutzen.

Beispiel Wir wollen hier mit dem Kettenbruchalgorithmus von Brillhart–Morrison die Zahl $n\quad 4309$ faktorisieren. Einsetzen von n in die obige Formel für b liefert $b\quad 8\ 2$. Wir nehmen also in die Faktorbasis $\quad 1, 2$ und die Primzahlen $3\quad p\quad 8$ mit $\frac{n}{p}\qquad 1$ auf, also B $\{\ 1\ 2\ 3\ 5\ 7\ .$ Nun starten wir die Kettenbruchentwicklung von $\sqrt{n}$. Wir berechnen dabei neben den a_i für $\sqrt{n}\qquad a_0\ a_1\qquad$ auch p_i, q_i und $z_i:\quad p_i^2\quad nq_i^2$. Die z_i zerlegen wir in ein Produkt von Potenzen von Zahlen aus B und einem Rest, der teilerfremd zu den Zahlen aus B ist. Die ersten Schritte sehen wie folgt aus

i	a_i	p_i	q_i	z_i
0	65	65	1	$84\qquad 1\quad 2^2\ 3\ 7$
1	1	66	1	$47\quad 47$
2	1	131	2	$75\qquad 1\quad 3\ 5^2$
3	1	197	3	$28\quad 2^2\ 7$

Wir sehen sofort, dass $z_0z_2z_3 \quad 1\ ^2 2^4 3^2 5^2 7^2 \quad 420^2$ ein Quadrat ist. Mit $z_i \quad p_i^2 \bmod n$ erhalten wir die Relation

$$p_0p_2p_3\ ^2 \quad z_0z_2z_3 \mod n \qquad 1254^2 \quad 420^2 \mod n$$

Damit finden wir die Teiler ggT $1254 \quad 420\ n \quad 31\ 139$ von n, tatsächlich ist $n \quad 4309 \quad 31\ 139$.

Wir können auch die Technik mit der Exponentenmatrix an diesem Beispiel demonstrieren. Da wir z_1 nicht mit unserer Faktorbasis faktorisieren konnten, tragen wir nur die Exponenten von $z_0\ z_2\ z_3$ als Spalten in der Matrix ein:

$$E \quad \begin{matrix} 1 & 1 & 0 \\ 2 & 0 & 2 \\ 1 & 1 & 0 \\ 0 & 2 & 0 \\ 1 & 0 & 1 \end{matrix} \qquad \begin{matrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{matrix} \mod 2$$

Der Kern von E modulo 2 ist aufgespannt von $f: \quad 1\ 1\ 1\ ^t$. Dies bedeutet, dass $z: \quad \prod z_i^{f_i}$ $z_0z_2z_3$ — die Zahl z_1 wurde ja weggelassen — ein Quadrat ist, was wir oben bereits direkt gesehen haben.

Aufgabe 12.4 Faktorisieren Sie mit dem Kettenbruchalgorithmus von Brillhart–Morrison die Zahl $n \quad 7729$.

Beim *quadratischen Sieb* versucht man anstatt der Wahl der x_i die Faktorisierung der b–glatten Zahlen z_i zu optimieren. Im Fermat Algorithmus hängen die z_i polynomial von den x_i ab, genauer ist $z_i \quad f\ x_i$ mit $f \quad X^2 \quad n$. Nun gilt $p^r\ f\ x$ genau dann, wenn $f\ x \quad 0 \bmod p^r$ ist, insbesondere hängt dies nur von der Restklasse von x modulo p^r ab! Wir haben bereits in Abschnitt 7 diskutiert, wie man die Nullstellen x_{p^r} von f, also die Wurzeln von n, in U_{p^r} finden kann. Die Techniken des folgenden Abschnittes werden eine schnellere Berechnung von x_{p^r} ermöglichen: Zunächst berechnet man die Wurzeln von n modulo p mit dem Verfahren von Tonelli–Shanks — sie existieren wegen $\frac{n}{p} \quad 1$. Danach liftet man sie sukzessive zu Wurzeln modulo p^k durch Benutzung des Hilfssatzes 13.14. Zusammenfassend haben wir für $p \quad 2$

$$p^r\ x^2 \quad n \qquad x \quad x_{p^r} \text{ oder } x \quad x_{p^r} \mod p^r$$

Für die Teilbarkeit durch 2^r kann man ähnlich vorgehen, man erhält jedoch auf Grund von $U_{2^r} \quad 2 \quad 2^r\ ^2$ für $r \quad 3$ keine oder vier Wurzeln von n modulo 2^r.

Aufgabe 12.5 Geben Sie einen Algorithmus an, mit dem man alle Wurzeln von n modulo 2^r finden kann.

Das Faktorisieren der b–glatten Zahlen findet jetzt durch einen Siebprozess statt. Man schreibt für ein Intervall $I \quad 0\ c\ , c \quad b^2 \ \log\log b\ $, die $x_i \quad \sqrt{n} \quad i$ und dazu gehörenden $z_i \quad x_i^2 \quad n$ auf. Für jede Primzahl p in der Faktorbasis B zu b und $r \quad$ mit $r \quad \log_p z_c$ berechnet man die Lösungen x_{p^r} von $x^2 \quad n \bmod p^r$ (für $p \quad 2$ gibt es hier bis zu vier Lösungen zu berücksichtigen). Dann ist ein z_i durch p^r teilbar, wenn $x_i \quad x_{p^r} \bmod p^r$ gilt.

Da die x_i $\sqrt{n}$ i linear von i abhängen, können wir diese x_i auf die folgende Weise finden: Zuerst suchen wir den kleinsten Repräsentanten von x_{p^r} (bzw. x_{p^r}) der größer oder gleich $\sqrt{n}$ ist — dies ist das erste x_i mit x_i x_{p^r} mod p^r. Die restlichen solchen x_i finden wir durch wiederholte Addition von p^r. So können wir für jedes z_i die maximale Potenz von p herausfinden, durch die z_i teilbar ist.

Wir notieren uns diese Potenzen für alle z_i und alle Primzahlen der Faktorbasis. Zum Schluss überprüfen wir, ob z_i das Produkt dieser Potenzen ist. Falls ja, dann ist z_i b–glatt und wir haben auch seine Primfaktorzerlegung; falls nein, ist z_i nicht b–glatt. Nun fährt man wie im Fermat Algorithmus fort. Sollte man nicht genügend b–glatte Zahlen gefunden haben, wird das Intervall nachträglich vergrößert.

Beispiel Wir wollen auch das quadratische Sieb an der Zahl n 4309 illustrieren. Aus den Überlegungen für dieses n bei dem Kettenbruchfaktorisierungsalgorithmus wissen wir, dass wir die Faktorbasis B { 1 2 3 5 7 benutzen können. Als Nächstes sollen wir eine Liste der x_i z_i anlegen mit i 0 b^2 $\log\log b$ 0 90 . Für dieses Beispiel wird bereits eine Liste mit elf Zeilen genügen:

i	x_i $\sqrt{n}$ i	z_i x_i^2 n
0	66	47
1	67	180
2	68	315
3	69	452
4	70	591
5	71	732
6	72	875
7	73	1020
8	74	1167
9	75	1316
10	76	1467

Für die Teilbarkeitstests p^r z_i x_i^2 n benötigen wir nun die Quadratwurzeln von n modulo p^r für p B und r $\log_p z_{10}$. Diese sind modulo den entsprechenden p^r

p r	1	2	3	4	5	6
2	1	1	—	—	—	—
3	1	4	4	4	85	85
5	2	3	53	303		
7	2	12	86			

Nach dem oben Gesagten ist die Bedeutung der Tabelle die folgende: Ein z_i x_i^2 n ist genau dann durch p^r teilbar, falls x_i modulo p^r gleich einem Eintrag der Tabelle an der Stelle p r ist. Nun benötigen wir den jeweils kleinsten Repräsentanten in diesen Restklassen, der größer gleich x_0 66 ist. Diese sind

p r	1	2	3	4	5	6
2	67	67 69	—	—	—	—
3	67 68	67 68	77 85	77 85	85 158	85 644
5	67 68	72 78	72 178	303 322		
7	68 72	86 110	86 257			

Für unsere Liste ergeben sich damit die folgenden Teilbarkeiten:

i	x_i	z_i	teilbar durch	partielle Faktorisierung
0	66	47		47
1	67	180	$2\ 2^2\ 3\ 3^2\ 5$	$2^2\ 3^2\ 5$
2	68	315	$3\ 3^2\ 5\ 7$	$3^2\ 5\ 7$
3	69	452	$2\ 2^2$	$2^2\ 113$
4	70	591	3	$3\ 197$
5	71	732	$2\ 2^2\ 3$	$2^2\ 3\ 61$
6	72	875	$5\ 5^2\ 5^3\ 7$	$5^3\ 7$
7	73	1020	$2\ 2^2\ 3\ 5$	$2^2\ 3\ 5\ 17$
8	74	1167	3	$3\ 389$
9	75	1316	$2\ 2^2\ 7$	$2^2\ 7\ 47$
10	76	1467	$3\ 3^2$	$3^2\ 163$

Wir können also mit unserer Faktorbasis $z_1\ z_2\ z_6$ faktorisieren und sehen auch sofort, dass $z_2 z_6 \quad 3^2 5^4 7^2 \quad 525^2$ ein Quadrat ist. Wir erhalten die Relation

$$x_2 x_6\ ^2 \quad z_2 z_6 \mod n \qquad\qquad 587^2 \quad 525^2 \mod n$$

und damit die Faktoren ggT $587 \quad 525\ n \quad 31\ 139$ von $n \quad 4309 \quad 31\ 139$.

Aufgabe 12.6 Faktorisieren Sie mit dem quadratischen Sieb die Zahl $n \quad 7729$.

Das quadratische Sieb ist der schnellste bekannte Faktorisierungsalgorithmus für Zahlen im Bereich von 10^{20} bis 10^{120}, falls sie keine relativ kleinen Primfaktoren enthalten. Für Zahlen mit kleinen Primteilern ist das *Lenstra–Verfahren* schneller, das elliptische Kurven benutzt und dessen Grundprinzip wir weiter unten andeuten. Für Zahlen über 10^{120} ist das *Zahlkörpersieb* schneller, das eine Weiterentwicklung des quadratischen Siebes ist.

Der modernste Faktorisierungsalgorithmus, der auf dem Lemma 12.1 beruht, ist der Algorithmus von Shor, der in polynomialer Zeit auf dem noch zu entwickelnden Quantencomputer läuft. Hier wählt man sogar fest $y \quad 1$. Man sucht also $x \quad$ mit $x^2 \quad 1 \mod n$. Dies macht man, indem man die Ordnung d eines zufälligen Elementes $\overline{a} \quad U_n$ ausrechnet. Es gilt dann $\overline{a}^d \quad 1$. Falls d ungerade ist, versucht man es mit einem anderen zufälligen Element $\overline{a} \quad U_n$. Sollte d gerade sein, setzt man $x : \quad a^{d/2}$. Dann ist $x^2 \quad 1 \mod n$. Sollte auch noch $x \quad 1 \mod n$ gelten, finden wir mit dem Lemma Teiler von n.

Das Auffinden der Ordnung von $\overline{a} \quad U_n$ ist normalerweise eine aufwendige Rechnung, sie lässt sich aber auf einem Quantencomputer mit Hilfe der diskreten Fouriertransformation und geeigneten Algorithmen in polynomialer Zeit durchführen. Das Auftreten der Fouriertransformierten ist deshalb verständlich, weil man an Hand von Fouriertransformierten die Periodizität von Funktionen untersucht und wir ein d mit $x^i \quad x^{d\ i} \mod n$ für alle i suchen.

Wir wollen hier am Ende des Abschnittes noch eine weitere Grundstrategie zur Faktorisierung diskutieren, die nicht auf dem Lemma 12.1 aufbaut. Man muss dafür jeder natürlichen Zahl

n eine Gruppe G_n zuordnen können, so dass für einen Primteiler p von n ein kanonischer Homomorphismus

$$\pi : G_n \quad G_p$$

existiert. Weiter muss eine Möglichkeit gegeben sein, aus einem nicht–trivialen Element des Kerns von π einen Faktor von n konstruieren zu können — ohne das p selbst zu kennen. Sei dann

$$\#G_p \quad \prod_{i \ 1}^{s} p_i^{r_i}$$

die Primfaktorzerlegung der Ordnung einer Gruppe G_p mit $p \ n$. Damit die Methode funktioniert, müssen wir voraussetzen, dass $p_i^{r_i} \quad b$ für alle i mit einem nicht allzu großen b gilt. Man setzt dann

$$C : \quad \text{kgV } 1 \ 2 \ 3 \quad b \quad \prod_{p^r \ b} p^r$$

wobei das Produkt über alle Primzahlpotenzen kleiner gleich b läuft. Wegen $\#G_p \ C$ folgt, dass für jedes zufällig gewählte Element $g \quad G$ das Element g^C im Kern von π liegt, weil $\pi \ g^C \quad \pi \ g \ ^C \quad e$. Sollte noch $g^C \quad e$ gelten, können wir nach unserer Annahme einen Teiler von n konstruieren.

Wir illustrieren diese Methode am *Pollardschen* $p \quad 1$ *–Verfahren* Hier ist $G_n : \quad U_n$ und $\pi : U_n \quad U_p$ die kanonische Projektion für $p \ n$. Falls wir ein nicht–triviales Element $\overline{a}$ des Kerns haben, bedeutet dies

$$a \quad 1 \mod p \qquad \text{und} \qquad a \quad 1 \mod n$$

d.h. $p \ a \quad 1$ und $n \quad a \quad 1$. Daher ist der Teiler $q \quad \text{ggT } a \quad 1 \ n \quad n$ von n ein Vielfaches von p, insbesondere also nicht–trivial. Damit haben wir die Voraussetzungen überprüft, um das obige allgemeine Verfahren anwenden zu können.

Der Nachteil der Pollardschen $p \quad 1$ –Methode ist, dass man voraussetzen muss, dass es zumindest einen Primteiler p von n geben muss, so dass $p \quad 1$ nicht allzu große Primzahlpotenzen als Teiler hat. Falls der Algorithmus in der Praxis scheitert, wiederholt man ihn einfach mit einem größeren b nochmal. Dies hilft dann noch in einigen Fällen. Es ist bekannt, dass etwa 15% der Zahlen in der Größenordnung von 10^{15} mit $b \quad 10^6$ faktorisiert werden können.

Das $p \quad 1$ *–Verfahren von Williams* benutzt für die Gruppen G_n Untergruppen der Einheitengruppen von $n \quad \sqrt{d} \quad n \quad n \quad \sqrt{d}, d$ mit $\text{ggT } n \ d \quad 1$. Für eine Primzahl p hat G_p gerade $p \quad 1$ Elemente. Zum erfolgreichen Faktorisieren muss man auch hier voraussetzen, dass $p \quad 1$ nur durch kleine Primzahlpotenzen teilbar ist.

Lenstra hatte die Idee, eine elliptische Kurve über n für die Gruppen G_n zu benutzen. Eine elliptische Kurve ist eine ebene glatte Kurve vom Grad 3. Sie trägt auf kanonische Weise eine Gruppenstruktur. Der entscheidende Vorteil ist, dass die elliptischen Kurven von einem Parameter λ abhängen und dass die Anzahl ihrer Punkte, also $\#G_p$, mit diesem Parameter variiert. Wenn man also das Pech hatte, dass $\#G_p$ durch eine große Primzahlpotenz teilbar ist, kann man den Parameter λ variieren und es nochmal versuchen. Die Laufzeit des Algorithmus hängt erstaunlicherweise nicht von n, sondern von dem kleinsten Primteiler p von n ab.

Er ist daher besonders gut geeignet, Primfaktoren in der Größenordnung von 10^{10} bis 10^{20} zu finden, größere als 10^{30} werden selten gefunden. Für diese kleinen Primfaktoren ist der Algorithmus der schnellste bekannte [R1].

Zusatzaufgaben

Aufgabe 12.7 Faktorisieren Sie die Zahl 23205 mit der Probedivision.

Aufgabe 12.8 Faktorisieren Sie die Zahl 13199 mit der Fermat–Methode.

Aufgabe 12.9 Sei n ungerade, zusammengesetzt und keine Primzahlpotenz. Zeigen Sie: Mindestens die Hälfte aller Paare $x\ y$ mit $0 \quad x\ y \quad n$ und $x^2 \quad y^2 \bmod n$ erfüllt die Ungleichung $1 \quad \mathrm{ggT}\ x \quad y\ n \quad n$.

Aufgabe 12.10 Faktorisieren Sie die Zahl 7429 mit dem quadratischen Sieb zur Faktorbasis $B \quad \{ \ 1\ 2\ 3\ 5\ 7\ .$

Aufgabe 12.11 Faktorisieren Sie die Zahl $2^{118} \quad 1$, indem Sie zuerst das Polynom $X^{4a \ 2}$ $X^{2a \ 2} \quad 2X^{2a \ 1} \quad 1$ in zwei Polynome vom Grad $2a \quad 1$ zerlegen und dann $X \quad 2$ setzen.

Aufgabe 12.12 Zeigen Sie, dass man mit der Fermat–Methode die RSA–Zahlen $n \quad pq$ leicht faktorisieren kann, wenn $p \quad q$ klein ist.

13 p–adische Zahlen

Im Abschnitt 8 haben wir quadratische Gleichungen im Körper $\mathbb{F}_p$ p gelöst. Wie kann man Gleichungen in den Ringen p^k, die ja noch nicht einmal Integritätsringe sind, lösen?

Betrachten wir als Beispiel die Gleichung

$$X^2 \quad 2 \quad 0 \mod 7^k$$

Falls es eine Lösung x gibt, erfüllt diese auch

$$x^2 \quad 2 \quad 0 \mod 7^l \qquad \text{für alle } l \quad k$$

Um die Lösung der Ursprungsgleichung zu finden, suchen wir zuerst Lösungen von $X^2 \quad 2$ 0 mod 7. Mit den Methoden aus Abschnitt 8 finden wir $x \quad 3 \mod 7$. Wir setzen $x_0 \quad a_0$ 3. (Mit $x_0 \quad 3$ könnten wir eine analoge Rechnung durchführen.) Nun versuchen wir die Lösung nach 7^2 zu liften, d.h. wir suchen x_1 mit

$$x_1^2 \quad 2 \quad 0 \mod 7^2 \qquad \text{und} \qquad x_1 \quad x_0 \mod 7$$

Die zweite Bedingung legt den Ansatz $x_1 \quad x_0 \quad a_1 7$ nahe. Einsetzen in die erste Gleichung ergibt

$$\begin{aligned} x_1^2 \quad 2 \quad 3 \quad a_1 7^{\,2} \quad 2 \quad 7 \quad 6 \; 7a_1 \quad a_1^2 7^2 \quad 7 \; 1 \quad 6a_1 \quad 0 \mod 7^2 \\ 1 \quad 6a_1 \quad 0 \mod 7 \qquad\qquad a_1 \quad 1 \mod 7 \\ x_1 \quad 3 \quad 1 \; 7 \quad 10 \mod 7^2 \end{aligned}$$

Die Eindeutigkeit der Lösung der linearen Gleichung in a_1 ist eine Konsequenz daraus, dass nur noch modulo 7, also eigentlich im Körper $\mathbb{F}_7$, gerechnet wird.

Führen wir nun den allgemeinen Schritt durch. Wir nehmen an, wir haben bereits ein x_k $\sum_{i \quad 0}^{k} a_i 7^i$ gefunden mit $x_k^2 \quad 2 \quad 0 \mod 7^{k \quad 1}$. Dann suchen wir ein $x_{k \quad 1}$ mit

$$x_{k \quad 1}^2 \quad 2 \quad 0 \mod 7^{k \quad 2} \qquad \text{und} \qquad x_{k \quad 1} \quad x_k \mod 7^{k \quad 1}$$

Der Ansatz $x_{k \quad 1} \quad x_k \quad a_{k \quad 1} 7^{k \quad 1}$ führt zur Gleichung

$$\begin{aligned} 0 \quad x_{k \quad 1}^2 \quad 2 \quad x_k \quad a_{k \quad 1} 7^{k \quad 1 \; 2} \quad 2 \quad x_k^2 \quad 2 \quad 2a_{k \quad 1} x_k 7^{k \quad 1} \quad a_{k \quad 1}^2 7^{2k \quad 2} \\ x_k^2 \quad 2 \quad 2a_{k \quad 1} x_k 7^{k \quad 1} \mod 7^{k \quad 2} \end{aligned}$$

S. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie,*
DOI 10.1007/978-3-8348-8263-9_13,

Nun haben wir $x_k^2 \equiv 2 \equiv 0 \bmod 7^{k-1}$ vorausgesetzt. Es gibt also ein b_{k-1} mit $x_k^2 - 2 = b_{k-1}7^{k-1}$. Setzen wir das noch oben ein, bekommen wir

$$0 \equiv b_{k-1}7^{k-1} - 2a_{k-1}x_k 7^{k-1} + 7^{k-1}b_{k-1} - 2a_{k-1}x_k \bmod 7^{k-2}$$

$$b_{k-1} - 2a_{k-1}x_k \equiv 0 \bmod 7 \qquad b_{k-1} - 2a_{k-1}x_0 \equiv 0 \bmod 7$$

$$b_{k-1} - 6a_{k-1} \equiv 0 \bmod 7 \qquad a_{k-1} \equiv 6^{-1}b_{k-1} \equiv b_{k-1} \bmod 7$$

Wir können also ein eindeutiges $a_{k-1} \in \{0, \ldots, 6\}$ finden, so dass $x_{k-1} = \sum_{i=0}^{k-1} a_i 7^i$ die Gleichung $x^2 - 2 \equiv 0 \bmod 7^{k-2}$ löst. Insgesamt erhalten wir eine Folge $(x_k)_{k \in \mathbb{N}_0}$ von ganzen Zahlen mit $x_{k-1} \equiv x_k \bmod 7^{k-1}$, die $x_k^2 - 2 \equiv 0 \bmod 7^{k-1}$ erfüllen. Ihr Anfang ist

$$\begin{aligned}
x_0 &= 3\\
x_1 &= 3 + 1 \cdot 7 = 10\\
x_2 &= 3 + 1 \cdot 7 + 2 \cdot 7^2 = 108\\
x_3 &= 3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 = 2166\\
x_4 &= 3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + 1 \cdot 7^4 = 4567\\
x_5 &= 3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + 1 \cdot 7^4 + 2 \cdot 7^5 = 38181
\end{aligned}$$

Wir würden natürlich gerne k gegen unendlich laufen lassen und $x_\infty = \lim_{k \to \infty} x_k = \sum_{i=0}^{\infty} a_i 7^i$ setzen. Damit hätten wir dann sämtliche Gleichungen $X^2 - 2 \equiv 0 \bmod 7^{k-1}$ gleichzeitig gelöst. Es ist jedoch nicht zu erwarten, dass der Grenzwert $\lim_{k \to \infty} x_k$ in $\mathbb{Q}$ existiert, schließlich löst keine Zahl in $\mathbb{Q}$ die Gleichung $X^2 - 2 = 0$. Genau um diese Probleme in den Griff zu bekommen, wurden die p–adischen Zahlen eingeführt.

Definition 13.1 *Die* ganzen p–adischen Zahlen *für eine Primzahl p sind definiert durch*

$$\mathbb{Z}_p := \left\{ (\overline{x_k}) \in \prod_{k=0}^{\infty} \mathbb{Z}/p^{k+1}\mathbb{Z} \;\middle|\; x_{k+1} \equiv x_k \bmod p^{k+1} \right\}$$

Mit der komponentenweisen Verknüpfung wird $\mathbb{Z}_p$ zu einem kommutativen Ring mit $0 := (\overline{0}_{k+1})_{k \in \mathbb{N}_0}$ und $1 := (\overline{1}_{k+1})_{k \in \mathbb{N}_0}$. Wir haben die kanonische Abbildung

$$\varepsilon_p : \mathbb{Z} \to \mathbb{Z}_p, \quad x \mapsto (\overline{x}_{k+1})_{k \in \mathbb{N}_0} = (\overline{x}, \overline{x}, \overline{x}, \ldots)$$

Beispiel In $\mathbb{Z}_7$ ist unter Weglassen der Oberstriche:

$$\begin{aligned}
\varepsilon_7(173) &= (173, 173, 173, \ldots) = (5, 26, 173, 173, \ldots)\\
\varepsilon_7(1) &= (1, 1, 1, \ldots) = (6, 48, 342, 2400, \ldots)\\
\sqrt{\varepsilon_7(2)} &= (3, 10, 108, 2166, \ldots)
\end{aligned}$$

Eine Darstellung $x = (\overline{x_k}) \in \mathbb{Z}_p$ heißt *reduziert*, falls $0 \le x_k < p^{k+1}$. Häufiger noch nutzt man die *Potenzreihendarstellung*. Um diese für x abzuleiten, sei $(\overline{x_k})$ eine reduzierte Darstellung von x. Zur Vereinfachung der Notation setzen wir $x_{-1} := 0$. Aus $x_k \equiv x_{k-1} \bmod p^k$ folgt $p^k \mid x_k - x_{k-1}$. Wir setzen

$$a_k := \frac{x_k - x_{k-1}}{p^k}$$

Dann ist $x_k \quad a_k p^k \quad x_{k\ 1}$, und wegen $0 \quad x_k \quad p^{k\ 1}$ ist $a_k \quad \{0 \quad p \quad 1$. Das Auflösen der Rekursion führt zu

$$x_k \quad \sum_{i\ 0}^{k} a_i p^i$$

und man schreibt x formal als Potenzreihe in p

$$x \quad \sum_{i\ 0}^{\infty} a_i p^i \qquad \text{mit } a_i \quad \{0 \quad p \quad 1$$

Die Addition und Multiplikation in $_p$ ist so erklärt, dass man die Potenzreihen wie üblich addiert und multipliziert. Man muss jedoch anschließend noch „Überträge“ durchführen, damit die Koeffizienten wieder kleiner als p werden. Betrachten wir ein Beispiel:

$$\begin{array}{l}
3\ 7^0 \quad 4\ 7^1 \quad 2\ 7^2 \quad\quad 5\ 7^0 \quad 3\ 7^1 \\
\quad 3 \quad 5 \quad 7^0 \quad 4 \quad 3 \quad 7^1 \quad\quad\quad 2\ 7^2 \\
\quad 7 \quad 1 \quad 7^0 \quad\quad 7 \quad 7^1 \quad\quad\quad 2\ 7^2 \\
\quad\quad 1 \quad 7^0 \quad 7 \quad 1 \quad 7^1 \quad\quad\quad 2\ 7^2 \\
\quad\quad 1 \quad 7^0 \quad\quad\quad 1 \quad 7^1 \quad 2 \quad 1 \quad 7^2 \\
\quad\quad 1 \quad 7^0 \quad\quad\quad 1 \quad 7^1 \quad\quad\quad 3 \quad 7^2
\end{array}$$

$$\begin{array}{l}
3\ 7^0 \quad 4\ 7^1 \quad 2\ 7^2 \quad\quad 5\ 7^0 \quad 3\ 7^1 \\
\quad\quad 3\ 5 \quad 7^0 \quad 3\ 3 \quad 4\ 5 \quad 7^1 \quad 4\ 3 \quad 2\ 5 \quad 7^2 \quad\quad 2\ 3 \quad 7^3 \\
\quad\quad\quad 15 \quad 7^0 \quad\quad\quad 29 \quad 7^1 \quad\quad\quad 22 \quad 7^2 \quad\quad\quad 6 \quad 7^3 \\
\quad 2\ 7 \quad 1 \quad 7^0 \quad\quad 4\ 7 \quad 1 \quad 7^1 \quad\quad 3\ 7 \quad 1 \quad 7^2 \quad\quad\quad 6 \quad 7^3 \\
\quad\quad\quad 1 \quad 7^0 \quad\quad\quad 1 \quad 2 \quad 7^1 \quad\quad\quad 1 \quad 4 \quad 7^2 \quad 6 \quad 3 \quad 7^3 \\
\quad\quad\quad 1 \quad 7^0 \quad\quad\quad\quad 3 \quad 7^1 \quad\quad\quad\quad 5 \quad 7^2 \quad\quad\quad 2 \quad 7^3 \quad 1 \quad 7^4
\end{array}$$

Besonders interessant mag sein, dass für jede Primzahl p

$$\varepsilon_p \quad 1 \quad \sum_{i\ 0}^{\infty} p \quad 1\ p^i$$

gilt. Dies verifiziert man durch die Addition von $\varepsilon_p\ 1 \quad\quad 1$.

Der Ring $_p$ besitzt die folgenden Eigenschaften:

Satz 13.2 *Für den Ring $_p$, $p \quad$, gilt:*

1. *Der Ring $_p$ ist ein Hauptidealring, insbesondere ein Integritätsring.*
2. *Die Abbildung ε_p : $\quad\quad _p$ ist eine Einbettung. Man fasst damit $\quad$ als Teilmenge von $_p$ auf.*

3. *Die Einheiten des Ringes sind* $_p \quad p \quad p \quad _p$*, d.h. die Potenzreihen mit konstantem Term ungleich* 0*.*

4. *Jedes Element* $x \quad _p \setminus \{0$ *besitzt eine eindeutige Zerlegung*

$$x \quad p^n u \qquad \text{mit } n \quad _0 \text{ und } u \quad _p$$

Insbesondere ist p das einzige Primelement bis auf Assoziiertheit.

5. $_p$ *besitzt nur die Ideale* 0 *und* $p^n \quad _p$ *für* $n \quad _0$*. Es gilt* $_{n \quad _0} p^n \quad _p \quad 0$ *und*

$$_p \; p^n \quad _p \qquad p^n$$

Insbesondere ist $p \quad _p$ *das einzige maximale Ideal.*

Beweis: Für 1) zeigen wir, dass $_p$ ein Integritätsring ist. Dass $_p$ sogar ein Hauptidealring ist, folgt dann, sobald wir 5) bewiesen haben. Sei also $x \quad \overline{x_k} \quad y \quad \overline{y_k} \quad _p \setminus \{0$ und $z \quad \overline{z_k} \quad xy \quad \overline{x_k y_k}$. Wegen $x \; y \quad 0$ existieren $n \; m \quad _0$ mit $x_n \quad 0 \bmod p^{n \; 1}$ und $y_m \quad 0 \bmod p^{m \; 1}$. Wir setzen $l : \quad n \quad m$. Aus $x_l \quad x_n \bmod p^{n \; 1}$ und $y_l \quad y_m \bmod p^{m \; 1}$ leiten wir die Existenz der Zerlegungen $x_l \quad u \; p^n$ bzw. $y_l \quad v \; p^m$ mit ggT $u \; p \quad$ ggT $v \; p \quad 1$, $n' \quad n$ und $m' \quad m$ ab. Dann ist wegen $n' \quad m' \quad l$ auch

$$z_l \quad uvp^{n \quad m} \quad 0 \mod p^{l \; 1}$$

und damit $z \quad 0$.

Um 2) zu beweisen, sei $x \quad$ mit $\varepsilon_p \; x \quad \overline{x}_{\; k} \quad 0$, d.h. $x \quad 0 \bmod p^{k \; 1}$ für alle $k \quad _0$. Die einzige ganze Zahl, die durch beliebig hohe p–Potenzen teilbar ist, ist die Null, also gilt $x \quad 0$. Somit ist ε_p eine Einbettung.

Für 3) bemerken wir zuerst, dass ein Element $x \quad \overline{x_k} \quad p \quad _p$ keine Einheit sein kann. Für ein solches x gilt nämlich $x_0 \quad 0 \bmod p$. Somit hat für jedes $y \quad \overline{y_k} \quad _p$ das Produkt xy als 0–te Komponente $\overline{x_0 y_0} \quad \overline{0 y_0} \quad 0 \quad 1$ und ist damit ungleich 1. Folglich kann x keine Einheit sein.

Sei nun $x \quad \overline{x_k} \quad _p \quad p \quad _p$, d.h. $\overline{x_0} \quad 0$. Nach der Definition der ganzen p–adischen Zahlen ist damit $x_k \quad x_0 \quad 0 \bmod p$. Wegen $p \quad x_k$ ist $\overline{x_k} \quad p^{k \; 1}$. Es gibt also eindeutig bestimmte $\overline{y_k} \quad p^{k \; 1}$ mit $\overline{x_k y_k} \quad \overline{1}$ in $p^{k \; 1}$. Nun impliziert $x_{k \; 1} y_{k \; 1} \quad 1 \bmod p^{k \; 2}$ zusammen mit $x_{k \; 1} \quad x_k \bmod p^{k \; 1}$, dass $x_k y_{k \; 1} \quad 1 \bmod p^{k \; 1}$. Aus der Eindeutigkeit von $\overline{y_k}$ folgt nun $y_{k \; 1} \quad y_k \bmod p^{k \; 1}$. Daher ist $y \quad \overline{y_k} \quad _p$ und nach Wahl der $\overline{y_k}$ gilt $xy \quad \overline{x_k y_k} \quad 1$

Wir beweisen zuerst für 5) das Teilresultat, dass $_{n \quad _0} p^n \quad _p \quad 0$ ist. Falls $x \quad \overline{x_k} \quad p^n \quad _p$, dann ist $0 \quad x_k \quad p^{k \; 1}$ für $k \quad n$. Folglich gilt für ein x im Schnitt $x_k \quad 0$ für alle $k \quad _0$, also $x \quad 0$.

Für 4) sei nun ein Element $x \quad _p \setminus \{0$ gegeben. Wegen $_{n \quad _0} p^n \quad _p \quad 0$ gibt es ein eindeutig bestimmtes $n \quad _0$ mit $x \quad p^n \quad _p \quad p^{n \; 1} \quad _p$. Man kann also $x \quad p^n u$ schreiben, wobei $u \quad _p \quad p \quad _p \quad _p$ sein muss. Da n eindeutig ist, ist auch u eindeutig, weil $_p$ ein Integritätsring ist.

Wir überlegen nun, dass p prim in $_p$ ist. Sei p ein Teiler von xy mit $x \; y \quad _p$. Dann ist $xy \quad p \quad _p$ und liegt damit nicht in den Einheiten $_p \quad _p \quad p \quad _p$. Also ist auch x oder y keine

Einheit und entsprechend ein Element von p_p und durch p teilbar. Es kann neben dem Primelement p keine weiteren Primelemente geben, da jedes Element ein Produkt von einer p–Potenz und einer Einheit ist.

Schließlich sei für 5) ein beliebiges Ideal $I \neq 0$ gegeben. Aus $\bigcap_{n \geq 0} p^n{}_p = 0$ folgt auch $\bigcap_{n \geq 0} I + p^n{}_p = 0$. Wegen $I \subseteq p^0{}_p = I$ gibt es ein minimales $n \geq 0$ mit $I \subseteq p^n{}_p = I$, aber $I \not\subseteq p^{n-1}{}_p = I$. Wir behaupten $I = p^n{}_p$. Aus $I \not\subseteq p^{n-1}{}_p = I$ folgt die Existenz eines $x = p^n u \in I$ mit $u \in {}_p$. Damit ist auch $p^n \in I$ und somit $p^n{}_p \subseteq I$. Da die andere Inklusion nach Wahl von n gilt, ist $I = p^n{}_p$.

Zum Schluss betrachten wir die kanonische Projektion

$$\pi : {}_p \to \prod_{k \geq 0} p^{k-1} \qquad p^n$$

Sie ist offensichtlich surjektiv, weil $\overline{x_{n-1}} \qquad p^n$ das Bild von $x_{n-1} \qquad {}_p$ ist. Der Kern von π ist ein Ideal und somit von der Form $\mathrm{Ker}\,\pi = p^l{}_p$. Da $\pi\ p^k = 0$ genau dann, wenn $k \geq n$ ist, gilt $\mathrm{Ker}\,\pi = p^n{}_p$. Mit dem Homomorphiesatz erhalten wir ${}_p / p^n{}_p \cong p^n$.

Aufgabe 13.3 Zeigen Sie, dass $\frac{1}{2}$ und $\frac{7}{4}$ Elemente in ${}_5$ sind, und berechnen Sie die ersten vier Stellen der Potenzreihenentwicklung.

Aufgabe 13.4 Entscheiden Sie, ob die folgenden Gleichungen eine Lösung besitzen und berechnen Sie gegebenenfalls die ersten drei Stellen einer Lösung.

$$X^2 \equiv 7 \text{ in } {}_3 \qquad X^2 \equiv 17 \text{ in } {}_{5003} \qquad X^2 \equiv -1 \text{ in } {}_2$$

Definition 13.5 *Die p–adischen Zahlen sind der Quotientenkörper der ganzen p–adischen Zahlen*

$$\mathbb{Q}_p : \quad \frac{r}{s} \quad r \quad {}_p \ s \quad {}_p \setminus \{0 \qquad \frac{r}{p^n} \quad r \quad {}_p \ n \quad 0$$
$$p^m u \quad u \quad {}_p \ m \qquad \setminus \{0$$

Die Gleichheit der Mengen ist eine direkte Folgerung aus Satz 13.2.4. Aus der Einbettung von in ${}_p$ erhalten wir eine Einbettung von $\mathbb{Q}$ in $\mathbb{Q}_p$. Satz 13.2.4 impliziert auch, dass die Zerlegung einer Zahl $x = p^m u \in \mathbb{Q}_p \setminus \{0$ eindeutig ist. Dies ermöglicht die folgende Definition.

Definition 13.6 *Die p–*adische Bewertung *auf $\mathbb{Q}_p$ ist die Abbildung*

$$v_p : \quad \mathbb{Q}_p \qquad \{\infty$$
$$p^m u \qquad m \qquad \text{für } m \qquad u \quad {}_p$$
$$0 \qquad \infty$$

Lemma 13.7 *Für die p–adische Bewertung auf $\mathbb{Q}_p$ und $x\ y \in \mathbb{Q}_p$ gilt:*

1. $v_p\ x \neq \infty \qquad x \neq 0$

2. $v_p\ xy \quad v_p\ x \quad v_p\ y$

3. $v_p\ x \quad y \quad \min\{v_p\ x \quad v_p\ y$

   Für $v_p\ x \quad v_p\ y$ *gilt Gleichheit in der obigen Ungleichung.*

4. $_p \quad \{z \quad \mathbb{Q}_p \quad v_p\ z \quad 0$

5. $_p \quad \{z \quad \mathbb{Q}_p \quad v_p\ z \quad 0$

Allgemein ist eine Bewertung eine Abbildung von einem Körper nach $\{\infty$, die die ersten drei Aussagen des Lemmas erfüllt. Die Bewertung, die alle Elemente ungleich 0 auf 0 abbildet, wird dabei als trivial bezeichnet.

Beweis: Die Aussagen sind alle offensichtlich bis vielleicht auf 3). Wir können uns beim Beweis auf $x\ y \quad 0$ beschränken. Sei $x \quad p^n u$ und $y \quad p^m v$ mit $n\ m$ und $u\ v \quad _p$. Wir nehmen ohne Einschränkung $n \quad m$ an. Dann ist

$$x \quad y \quad p^n u \quad p^m v \quad p^n\ u \quad p^m\ ^n v$$

Wegen $m \quad n \quad 0$ ist $u \quad p^m\ ^n v \quad _p$ und hat eine Bewertung größer oder gleich Null, daher gilt $v_p\ x \quad y \quad n \quad v_p\ x$. Falls $n \quad v_p\ x \quad v_p\ y \quad m$ ist, ist $p^m\ ^n v \quad p \quad _p$ und damit $u \quad p^m\ ^n v \quad _p$. Somit ist $v_p\ u \quad p^m\ ^n v \quad 0$ und $v_p\ x \quad y \quad n \quad v_p\ x$.

Neben der p–adischen Bewertung nutzt man auch den äquivalenten Begriff der p–Norm.

Definition 13.8 *Auf* $\mathbb{Q}_p$ *ist die* p–Norm *definiert durch*

$$_p\colon \quad \mathbb{Q}_p$$

$$x \qquad\qquad p^{\ v_p\ x}$$

wobei man $p^{\ \infty}\colon \quad 0$ *setzt.*

Etwas gewöhnungsbedürftig ist, dass die p–Norm genau „verkehrt herum“ ist, $p^n\ _p \quad 1 \quad p^n$. Die Umformulierung des vorangehenden Lemmas für die p–Norm lautet:

Lemma 13.9 *Für die* p–*Norm auf* $\mathbb{Q}_p$ *und* $x\ y \quad \mathbb{Q}_p$ *gilt:*

1. $x\ _p \quad 0;\ x\ _p \quad 0 \qquad\qquad x \quad 0.$

2. $xy\ _p \quad x\ _p\ \ y\ _p$

3. $x \quad y\ _p \quad \max\{\ x\ _p\ \ y\ _p \qquad x\ _p \quad y\ _p$

   Für $x\ _p \quad y\ _p$ *gilt* $x \quad y\ _p \quad \max\{\ x\ _p\ \ y\ _p$.

4. $_p \quad \{z \quad \mathbb{Q}_p \quad z\ _p \quad 1$

5. $_p \quad \{z \quad \mathbb{Q}_p \quad z\ _p \quad 1$

Insbesondere ist die p–*Norm tatsächlich eine Norm.*

Von der üblichen Betragsnorm auf $\mathbb{Q}$ sind wir gewohnt, dass für jedes r ein n existiert, so dass $n \geq r$ gilt. Die Norm auf wird deshalb als *archimedisch* bezeichnet. Die p–Normen sind alle nicht archimedisch. Denn nach Lemma 13.9.4 ist $n \leq 1$, aber es gilt $p^n_p = p^n$ für n .

Die $\mathbb{Q}_p$ teilen mit die folgende wichtige Eigenschaft.

Satz 13.10 *Die p–adischen Zahlen sind vollständig bezüglich der p–Norm, d.h. jede Cauchy–Folge konvergiert.*

Beweis: Sei x_i eine Cauchy–Folge in $\mathbb{Q}_p$. Wir wollen zuerst dafür argumentieren, dass wir ohne Einschränkung $x_i \leq 1$ annehmen dürfen. Betrachten wir dazu die Menge $\{ x_i \mid i \}$. Wir behaupten, dass sie nach oben beschränkt ist. Falls nicht, gibt es für alle m und N zwei Indizes $i, j \geq N$ mit $x_i > p^m$ und $x_j \leq p^m$. Nach Lemma 13.9.3 ist somit $x_i = x_j + x_i - x_j \leq p^m$. Dies ist jedoch für eine Cauchy–Folge unmöglich. Nun wählen wir m mit $p^m \geq \max\{ x_i \mid i \geq 0 \}$. Dann ist $p^m x_i$ eine Cauchy–Folge mit $p^m x_i \leq 1$ und $p^m x_i \neq 0$. Sie konvergiert genau dann, wenn x_i konvergiert.

Wir brauchen daher nur noch eine Cauchy–Folge x_i in zu betrachten. Wir wollen zeigen, dass sie konvergiert und ihren Grenzwert z bestimmen. Für jedes k wählen wir ein N_k , so dass

$$x_i - x_j \leq p^{-k} \quad \text{für } i, j \geq N_k$$

Wir dürfen annehmen, dass N_k eine aufsteigende Folge ist. Die obige Ungleichung können wir auch als $v_p(x_i - x_j) \geq k$ oder $x_i \equiv x_j \pmod{p^k}$ lesen. Wir finden daher ein z_k mit

$$z_k \equiv x_i \equiv x_j \pmod{p^{k-1}} \quad \text{für } i, j \geq N_k$$

Wegen $N_{k-1} \leq N_k$ ist

$$z_{k-1} \equiv x_{N_{k-1}} \equiv x_{N_k} \equiv z_k \pmod{p^{k-1}}$$

d.h. $z = (\overline{z_k})_k \in \prod p^{k-1}$ ist ein Element aus . Weiter gilt für $i \geq N_k$

$$x_i \equiv z_k \equiv z \pmod{p^{k-1}} \qquad x_i - z \leq p^{-k}$$

also konvergieren die x_i gegen z.

Durch die Einbettung $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ erben die rationalen Zahlen die p–Norm. Zur Vereinheitlichung bezeichnet man den Absolutbetrag auch als ∞–Norm und schreibt ∞ : .

Die p–adischen Zahlen können auch analog zur Konstruktion der reellen Zahlen als Cauchy–Folgen in $\mathbb{Q}$ bezüglich der p–Norm modulo den Nullfolgen definiert werden. Dies bezeichnet man als Vervollständigung der rationalen Zahlen bezüglich der p–Norm. Dann folgt bereits aus der Definition, dass die p–adischen Zahlen vollständig sind.

Nachdem wir so viele neue Normen gefunden haben, stellt sich natürlich die Frage, ob es noch weitere Normen auf $\mathbb{Q}$ gibt. Wir erinnern, dass zwei Normen und auf einem Körper K äquivalent sind, wenn es $0 < c \leq C$ gibt mit $c \cdot x \leq x \leq C \cdot x$ für alle $x \in K$. Eine Norm heißt trivial, falls sie äquivalent ist zu der Norm mit $x = 1$ für alle $x \neq 0$.

Satz 13.11 (Ostrowski) *Jede nicht–triviale Norm auf $\mathbb{Q}$ ist äquivalent zu einer der p–Normen oder dem Absolutbetrag.*

Beweis: [F, Satz 6.5].

Man weiß, dass es bis auf Äquivalenz nur eine nicht–triviale Norm auf und $\mathbb{Q}_p$ gibt. Man bezeichnet sie deshalb als *lokale Körper*.Weil und die $\mathbb{Q}_p$ alle Körper sind, die aus den rationalen Zahlen durch Vervollständigung entstehen, nennt man sie die lokalen Körper zum *globalen Körper* $\mathbb{Q}$.

Schließen wir die Normbetrachtungen mit einer fast trivialen Bemerkung ab.

Bemerkung 13.12 *Sei x $\mathbb{Q}$, dann gilt*

$$\prod_{p \quad \infty} x_p \quad 1$$

Beweis: Wir schreiben

$$x \qquad \prod_{i \quad 1}^{s} p_i^{n_i} \qquad \text{mit } n_i \qquad \text{und } p_i \qquad \text{paarweise verschieden.}$$

Somit sind die Normen von x

$$x_{\infty} \quad \prod_{i \quad 1}^{s} p_i^{n_i} \qquad x_{p_i} \quad p_i^{\,n_i} \quad \text{und} \quad x_p \quad 1 \text{ für alle } p \qquad \{p_1 \qquad p_s$$

Damit ist die Behauptung offensichtlich.

Kehren wir zu unserer ursprünglichen Motivation für die Betrachtung der p–adischen Zahlen zurück, dem Lösen von Gleichungen modulo Potenzen von Primzahlen. Leider funktioniert das nicht immer so gut wie im Eingangsbeispiel, wo die Lösungen modulo p auf eindeutige Weise zu Lösungen modulo p^k geliftet werden konnten.

Betrachten wir zum Beispiel unsere Ursprungsgleichung $X^2 \quad 2 \quad 0$ modulo 2^k. Diese hat modulo 2 die Lösung 0, aber keine Lösung modulo 2^k für $k \quad 2$, weil

$$x^2 \quad 2 \quad 0 \bmod 2^k \qquad x^2 \quad 2 \quad 0 \bmod 2$$

$$x \quad 0 \bmod 2 \qquad x^2 \quad 0 \bmod 4 \qquad x^2 \quad 2 \quad 0 \bmod 2^k$$

Noch schlimmer ist die Situation für die Gleichung

$$X^2 \quad 7 \quad 0 \mod 2^k$$

Hier gibt es die Lösungen

k	Lösungen mod 2^k	Zahlen links mod 2^{k-1}
1	1	
2	1 3	1 1
3	1 3 5 7	1 3 1 3
4	3 5 11 13	3 5 3 5
5	5 11 21 27	5 11 5 11
6	11 21 43 53	11 21 11 21
7	11 53 75 117	11 53 11 53
8	53 75 181 203	53 75 53 75
9	75 181 331 437	75 181 75 181
10	181 331 693 843	181 331 181 331

Das Bemerkenswerte ist, dass es für $k \geq 3$ immer vier Lösungen gibt. Diese sind jeweils zwei Liftungen von zwei Lösungen modulo 2^{k-1}. Das bedeutet, dass wir in $\mathbb{Z}_2$ nur zwei Lösungen erhalten. Schließlich ist $x = x_k \in \mathbb{Z}_2$ eine Lösung von $X^2 - 7 = 0$, wenn neben $x_k^2 - 7 \equiv 0 \bmod 2^{k-1}$ auch noch $x_k \equiv x_{k-1} \bmod 2^k$ gilt. So können wir zwei Lösungen mit $x = 1\,1\ldots$ und $y = 1\,3\ldots$ beginnen. Die 1 (bzw. 3) können wir zu der Lösung 1 oder 5 (bzw. 3 oder 7) von $X^2 - 7 \equiv 0 \bmod 8$ liften. Wir sehen jedoch am rechten Eintrag der vierten Zeile der Tabelle, dass nur 5 (bzw. 3) weiter geliftet werden kann. Also müssen die Lösungen weitergehen als $x = 1\,1\,5\ldots$ und $y = 1\,3\,3\ldots$. Mehrfaches Wiederholen dieses Argumentes führt zu

$$x = 1\,1\,5\,5\,21\,53\,53\,181\,181\ldots$$
$$y = 1\,3\,3\,11\,11\,11\,75\,75\,331\ldots$$

Wir hätten direkt von Anfang an sehen können, dass es nur zwei Lösungen von $X^2 - 7 = 0$ über $\mathbb{Z}_2$ geben kann, denn ein quadratisches Polynom kann über dem Körper $\mathbb{Q}_2$ — und damit auch über $\mathbb{Z}_2$ — höchstens zwei Nullstellen haben.

Wir wollen das oben beschriebene Verhalten beweisen: Dass eine Lösung entweder gar nicht oder gleich zu zwei Lösungen geliftet werden kann, ist leicht zu sehen. Nehmen wir an, dass $x \in \mathbb{Z}$ die Kongruenz $x^2 - 7 \equiv 0 \bmod 2^{k-1}$ erfüllt. x kann nur zu x oder $x + 2^{k-1}$ modulo 2^k geliftet werden. Es gilt

$$x + 2^{k-1}\big)^2 - 7 = x^2 + 2^k x + 2^{2k-2} - 7 \equiv x^2 - 7 \bmod 2^k \quad \text{für } k \geq 2$$

somit ist entweder x und $x + 2^{k-1}$ eine Lösung oder keins von beiden.

Wir wollen dafür argumentieren, dass es für $k \geq 3$ immer genau vier Lösungen gibt. Sobald wir das gezeigt haben, folgt das oben beschriebene Verhalten unmittelbar. Wir machen das mit einem ad hoc Argument, eine etwas systematischere Vorgehensweise würde den nachfolgenden Satz und Hilfssatz nutzen. Untersuchen wir $\overline{7} \in U_{2^k}$. Wegen $7^2 \equiv 1 \bmod 16$ ist $\operatorname{ord}_{U_{2^4}} \overline{7} = 2$. Aufgabe 7.6 zeigt, dass $\operatorname{ord}_{U_{2^r}} \overline{x} = 2\operatorname{ord}_{U_{2^{r-1}}} \overline{x}$ für alle x mit $x \equiv 1 \bmod 4$ und weiter $\operatorname{ord}_{U_{2^r}} \overline{x} = 2\operatorname{ord}_{U_{2^{r-1}}} \overline{x}x$ für x mit $2 \nmid \operatorname{ord}_{U_{2^{r-1}}} \overline{x}$. Folglich ist $\operatorname{ord}_{U_{2^k}} \overline{7} = 2^{k-3}$. Aus dem Beweis von Satz 7.9 folgt, dass $\overline{7}$ unter dem Isomorphismus $U_{2^k} \cong \{\pm 1\} \times \langle 2 \rangle \cong \{\pm 1\} \times \mathbb{Z}/2^{k-2}\mathbb{Z}$ einem Element entspricht, das in der vorderen Komponente eine $\overline{0}$ hat. Auf Grund der Ordnung muss es von der Form $(\overline{0}, \overline{2x})$ mit $2 \nmid x$ sein. Dem Wurzelziehen aus $\overline{7} \in U_{2^k}$ entspricht das

Teilen von $\overline{0}\ \overline{2x}$ durch 2 in $2 \qquad 2^{k\ 2}$. Nach Satz 4.8 finden wir je zwei Lösungen in den Komponenten und somit insgesamt vier Lösungen.

Die Hoffnung, dass das oben an Beispielen gezeigte Ausnahmeverhalten nur bei der Primzahl 2 auftritt, trügt leider, wie die folgende Aufgabe zeigt.

Aufgabe 13.13 Beschreiben Sie die Lösungen von

$$X^4 \quad 3X^2 \quad 27 \quad 0 \mod 5^k \qquad \text{bzw.} \qquad X^4 \quad X^3 \quad 8 \quad 0 \mod 5^k$$

Berechnen Sie Lösungen zumindest bis $k \quad 5$. Um das allgemeine Schema zu beweisen, mag der folgende Hilfssatz und Satz hilfreich sein.

Das wirkliche Problem bei diesen Beispielen ist, dass die Ableitung der Polynome an den approximativen Lösungen gleich 0 modulo p ist. Falls dies nicht der Fall ist, läuft das Verfahren wie am Anfang des Abschnittes. Dies wollen wir jetzt beweisen. Ein einzelner Liftungsschritt wird durch den folgenden Hilfssatz beschrieben. Dabei bezeichnet f' die formale Ableitung von f.

Hilfssatz 13.14 *Sei* $f \qquad {}_p X$ *und* $\tilde{x} \qquad {}_p$ *mit*

$$f\ \tilde{x} \qquad 0 \mod p^k \quad \textit{für ein } k$$

Weiter sei $l \qquad$ *mit* $l \quad k$. *Dann gilt für* a

$$f\ \tilde{x} \quad ap^k \qquad 0 \bmod p^{k\ l} \qquad\qquad f'\ \tilde{x}\ a \quad \frac{f\ \tilde{x}}{p^k} \bmod p^l$$

Beweis: Wir schreiben f als Polynom in $X \quad \tilde{x}$,

$$f \quad \sum_{i\ 0}^{d} c_i\ X \quad \tilde{x}\ ^i \quad \text{mit } c_i \qquad {}_p$$

Per Definition ist $c_0 \quad f\ \tilde{x}$ und $c_1 \quad f'\ \tilde{x}$, damit ist

$$f\ \tilde{x} \quad ap^k \qquad \sum_{i\ 0}^{d} c_i\ ap^{k\ i} \quad f\ \tilde{x} \quad f'\ \tilde{x}\ ap^k \quad p^{2k} \sum_{i\ 2}^{d} c_i a^i p^{i\ 2\ k}$$

Modulo $p^{k\ l}$ ergibt das

$$f\ \tilde{x} \quad ap^k \qquad f\ \tilde{x} \quad f'\ \tilde{x}\ ap^k \quad \bmod p^{k\ l}$$

Folglich gilt

$$\begin{aligned} f\ \tilde{x} \quad ap^k \qquad & 0 \quad \bmod p^{k\ l} \\ f\ \tilde{x} \quad f'\ \tilde{x}\ ap^k \quad & 0 \quad \bmod p^{k\ l} \\ \frac{f\ \tilde{x}}{p^k} \quad f'\ \tilde{x}\ a \quad p^k \quad & 0 \quad \bmod p^{k\ l} \\ f'\ \tilde{x}\ a \qquad \frac{f\ \tilde{x}}{p^k} \quad & \bmod p^l \end{aligned}$$

Satz 13.15 (Henselsches Lemma) *Sei $f \in \mathbb{Z}_p[X]$ ein Polynom und $\tilde{x} \in \mathbb{Z}_p$. Weiter sei $l \geq 1$: $v_p(f'(\tilde{x})) = l$. Falls $f(\tilde{x}) \equiv 0 \bmod p^{2l+1}$, dann existiert ein eindeutig bestimmtes $x \in \mathbb{Z}_p$ mit*

$$f(x) = 0 \quad \text{und} \quad x \equiv \tilde{x} \bmod p^{l+1}$$

Beweis: Wir konstruieren $x \in \mathbb{Z}_p$ als Folge $x = \overline{x_k}_{k \geq 0}$, $x_k \in \mathbb{Z}$, mit

1. $x_k \equiv \tilde{x} \bmod p^{\min(l+1,k+1)}$.
2. $x_k \equiv x_{k-1} \bmod p^k$.
3. $f(x_k) \equiv 0 \bmod p^{k+l+1}$.

Nach dem Isomorphismus aus Satz 13.2 gibt es ein $z \in \mathbb{Z}$ mit $z \equiv \tilde{x} \bmod p^{2l+1}$. Um $x_k \equiv \tilde{x} \bmod p^{\min(l+1,k+1)}$ zu erfüllen, setzen wir $x_0 := x_1 := \ldots := x_l := z$. Diese Bedingung bestimmt diese x_k auch eindeutig modulo p^{k+1}.

Nehmen wir nun an, wir hätten x_{k-1} mit $k \geq l$ schon gefunden, dann machen wir den Ansatz $x_k = x_{k-1} + ap^k$ mit $a \in \mathbb{Z}$. Nach dem Hilfssatz folgt

$$f(x_k) = f(x_{k-1} + ap^k) \equiv 0 \bmod p^{k+l+1}$$

aus

$$f'(x_{k-1})\, a \equiv \frac{f(x_{k-1})}{p^k} \bmod p^{l+1}$$

Nach Konstruktion ist $x_{k-1} \equiv \tilde{x} \bmod p^{l+1}$. Es folgt $f'(x_{k-1}) \equiv f'(\tilde{x}) \not\equiv 0 \bmod p^{l+1}$ und $f'(x_{k-1}) \equiv f'(\tilde{x}) \not\equiv 0 \bmod p^{l+1}$, also $v_p(f'(x_{k-1})) = l$. Da $f(x_{k-1}) \equiv 0 \bmod p^{k+l}$, gilt $p^k \mid f'(x_{k-1})\, f(x_{k-1})$. Daher sind nach dem Satz 4.8 die Lösungen für a in der obigen Kongruenz

$$a \equiv \frac{f(x_{k-1})}{f'(x_{k-1})\, p^k} \bmod p$$

Dies bestimmt das gesuchte $x_k = x_{k-1} + ap^k$ eindeutig modulo p^{k+1}. Insgesamt erhalten wir ein eindeutiges $x \in \mathbb{Z}_p$ mit den geforderten Eigenschaften.

Fast immer wird das Henselsche Lemma für $l = 0$ benutzt, also in der Form:

Korollar 13.16 *Sei $f \in \mathbb{Z}_p[X]$ ein Polynom und $\tilde{x} \in \mathbb{Z}_p$ mit $f(\tilde{x}) \equiv 0 \bmod p$ und $f'(\tilde{x}) \not\equiv 0 \bmod p$. Dann existiert ein eindeutig bestimmtes $x \in \mathbb{Z}_p$ mit*

$$f(x) = 0 \quad \text{und} \quad x \equiv \tilde{x} \bmod p$$

Die Interpretation des Korollars ist klar: Jede einfache Nullstelle von f modulo p lässt sich eindeutig zu einer einfachen Nullstelle von f in $\mathbb{Z}_p$ liften. Den allgemeinen Satz kann man so verstehen: Gegeben ein $\tilde{x} \in \mathbb{Z}_p$ mit $l = v_p(f'(\tilde{x}))$. Dann lässt sich aus $\tilde{x}$ genau dann eine Lösung $x \in \mathbb{Z}_p$ von f mit $x \equiv \tilde{x} \bmod p^{l+1}$ konstruieren, wenn man aus $\tilde{x}$ eine Lösung z von f modulo p^{2l+1} mit $z \equiv \tilde{x} \bmod p^{l+1}$ konstruieren kann.

Das Unbefriedigende an dieser Aussage ist, dass man schon fordern muss, dass $x \equiv \tilde{x} \bmod p^{l+1}$ gelten soll. Vielleicht wäre man ja schon mit einer schlechteren Annäherung an $\tilde{x}$ zufrieden gewesen. Jedoch ist es gerade diese Bedingung, die $v_p(f'(x_{k-1})) = v_p(f'(\tilde{x}))$

während der Konstruktion von x sichert. Falls man sie weg lässt, könnte $v_p\ f'\ x_{k\ 1}$ größer werden und der entsprechende Konstruktionsschritt wäre eventuell unmöglich.

Wir kehren zu einem unserer Hauptthemen zurück:

Lösen von Polynomgleichungen modulo n

Sei ein $f\quad X$ und ein $n\quad$ gegeben. Wir suchen Lösungen von f modulo n. Dazu zerlegen wir n in seine Primfaktoren $n\quad\prod_{i\ 1}^{s} p_i^{r_i}$. Nach dem chinesischen Restsatz ist $f\ x\quad 0 \bmod n$ genau dann, wenn $f\ x\quad 0 \bmod p_i^{r_i}$ für alle $i\quad 1\quad s$. Um diese Gleichungen zu lösen, suchen wir zunächst $\tilde{x}_i$ mit $f\ \tilde{x}_i\quad 0 \bmod p_i$. Dies ist der schwierigste Schritt. Falls keines der bisher beschriebenen Verfahren anwendbar ist, muss man alle Zahlen $0\ 1\quad p_i\quad 1$ ausprobieren. Dann wenden wir einige Liftungsschritte wie im Hilfssatz 13.14 beschrieben an, um Lösungen x_i von $f\ x_i\quad 0 \bmod p_i^{r_i}$ zu finden. Durch den chinesischen Restsatz erhalten wir ein $x\quad$ mit $x\quad x_i \bmod p_i^{r_i}$, dieses erfüllt damit $f\ x\quad 0 \bmod n$.

Beispiel Wir lösen

$$f:\quad X^4\quad 8X^3\quad 6X^2\quad 16X\quad 16\quad 0\quad \bmod 50\quad 2\ 5^2$$

Betrachten wir diese Gleichung zuerst modulo 2, also $X^4\quad 0 \bmod 2$. Dies hat nur die Lösung $x_1\quad 0 \bmod 2$.

Modulo 5 haben wir das Polynom $X^4\quad 3X^3\quad 4X^2\quad X\quad 4$. Da uns im Augenblick kein Verfahren zur Lösung dieser Gleichung einfällt, setzen wir die Werte $0\ 1\ 2\ 3\ 4$ ein:

x	0	1	2	3	4
$f\ x\ \bmod 5$	4	3	2	0	0

Wir finden daher $x_2\quad 3 \bmod 5$ und $x_2\quad 4 \bmod 5$ als Lösungen von f modulo 5. Es gilt $f'\ 3\quad 4 \bmod 5$ und $f'\ 4\quad 3 \bmod 5$, damit wird das Liften nach dem Hilfsatz 13.14 einfach. Wir liften 3 zu $3\quad a5$, wobei a festgelegt ist durch

$$f'\ 3\ a\quad f\ 3\quad 5 \bmod 5\qquad 4a\quad 275\ \ 5 \bmod 5\qquad a\quad 0 \bmod 5$$

Daher können wir als Liftung der Lösung 3 von f modulo 5 wieder 3 als Lösung von f modulo 25 wählen. Analog liften wir die Lösung 4 von f modulo 5 zu 14 als Lösung von f modulo 25.

Jetzt finden wir alle Lösungen von f modulo 50, indem wir mit dem chinesischen Restsatz die Kongruenzen

$$x\quad 0 \bmod 2\ \text{und}\ x\quad 3 \bmod 25\quad \text{bzw.}\quad x\quad 0 \bmod 2\ \text{und}\ x\quad 14 \bmod 25$$

lösen. Die Lösungen sind $x\quad 28 \bmod 50$ bzw. $x\quad 14 \bmod 50$.

Da wir nicht in einem Körper rechnen, wären auch a priori mehr als vier Lösungen von f möglich gewesen.

Zusatzaufgaben

Aufgabe 13.17 Untersuchen Sie die folgenden quadratischen Kongruenzen auf ihre Lösbarkeit:

1. $x^2 \quad 811 \bmod 851$.
2. $x^2 \quad 27x \quad 52 \quad 0 \bmod 13^3$.

Aufgabe 13.18 Gegeben sei das Polynom $f : \quad X^3 \quad 3X \quad 5$. Bestimmen Sie alle Lösungen der Kongruenz $f\ x \quad 0 \bmod 7^4$.

Aufgabe 13.19 Sei $n \quad , n \quad 2$. Wir definieren den Ring der n–adischen Zahlen durch

$$_n \qquad \bar{x_k} \qquad \prod_{k \ 0}^{\infty} \quad n^{k \ 1} \quad x_{k \ 1} \quad x_k \mod n^{k \ 1}$$

1. Zeigen Sie: Sind $n \ m \quad 2$ teilerfremde natürliche Zahlen, dann ist $_{nm} \qquad _n \qquad _m$.
2. Beweisen Sie, dass für jede natürliche Zahl $n \quad 2$ und jedes $r \qquad$ ein natürlicher Isomorphismus $_{n^r} \qquad _n$ existiert.

Aufgabe 13.20 Gegeben seien die Polynome

$$f : \quad X^3 \quad X^2 \quad 20X \quad 3 \qquad \text{und} \qquad g : \quad X^4 \quad X^3 \quad 8$$

in X. Zeigen Sie:

1. Das Polynom f besitzt zwei Nullstellen modulo 5, sechs Nullstellen modulo 25 und 11 Nullstellen modulo 5^k für $k \quad 3$, aber nur drei Nullstellen in $_5$.
2. Das Polynom g besitzt eine Nullstelle modulo 5, fünf Nullstellen modulo 25 und 10 Nullstellen modulo 5^k für $k \quad 3$, aber nur zwei Nullstellen in $_5$.

Aufgabe 13.21 Zeigen Sie: Ist $x_{i \ i}$ eine Nullfolge in $\mathbb{Q}_p$, dann ist die Reihe $\sum_{i \ 0}^{\infty} x_i$ konvergent.

Aufgabe 13.22 Sei K ein Körper, der $\mathbb{Q}$ enthält. Eine *Anordnung* auf K ist eine Teilmenge $P \quad K$ mit den Eigenschaften

1. $0 \quad P$ und $x \quad P \qquad x \quad P$ für alle $x \quad K \quad \{0$.
2. Sind $x \ y \quad P$, dann auch $x \quad y$ und xy.

Die Schreibweise $x \quad y$ ist gleichbedeutend mit $y \quad x \quad P$.

1. Zeigen Sie: Existiert ein $m \qquad$, so dass $\quad m$ ein Quadrat in K ist, dann gibt es auf K keine Anordnung.
2. Beweisen Sie, dass der Körper $\mathbb{Q}_p$ für keine Primzahl p eine Anordnung besitzt.

Aufgabe 13.23 Zeigen Sie, dass das Polynom

$$f: \quad X^2 \quad 13 \quad X^2 \quad 17 \quad X^2 \quad 13 \quad 17 \qquad X$$

modulo jeder natürlichen Zahl n eine Nullstelle hat, aber keine Nullstelle in besitzt.

Aufgabe 13.24 Zeigen Sie, dass $\frac{1}{2}$ und $\frac{5}{3}$ Elemente in $_7$ sind und berechnen Sie jeweils die ersten vier Stellen der Potenzreihenentwicklung.

Aufgabe 13.25 Berechnen Sie den p–adischen Absolutbetrag von $\frac{1}{p^7 \quad p^5 \quad p^3}$.

Aufgabe 13.26 Sei p eine Primzahl und $b \quad p^n u \quad \mathbb{Q}_p$ mit $u \qquad _p$ und $n \qquad$. Zeigen Sie:

1. Die Gleichung $x^3 \quad b$ besitzt genau dann eine Lösung in $\mathbb{Q}_p$, wenn n durch 3 teilbar ist und $x^3 \quad u$ eine Lösung in $_p$ besitzt.
2. Sei $p \quad 3$. Die Gleichung $x^3 \quad u$ ist genau dann in $_p$ lösbar, wenn $x^3 \quad u \bmod p$ eine Lösung besitzt.

Aufgabe 13.27 Sei $m \qquad$. Zeigen Sie, dass es unendlich viele Primzahlen p gibt, so dass $\sqrt{m} \quad \mathbb{Q}_p$. Ist umgekehrt $p \qquad$ eine feste ungerade Primzahl, so zeige man, dass es unendlich viele $m \qquad$ gibt, so dass $\sqrt{m} \quad \mathbb{Q}_p$. Hinweis: Sie dürfen benutzen, dass in jeder arithmetischen Progression unendlich viele Primzahlen existieren (*Satz von Dirichlet*).

Aufgabe 13.28 Sei n eine natürliche Zahl und $n \quad a_0 \quad a_1 p \qquad a_{r \ 1} p^{r \ 1}$ ihre p–adische Entwicklung, wobei $0 \quad a_i \quad p$. Zeigen Sie, dass

$$v_p \ n! \quad \frac{n \quad a_0 \quad a_1 \qquad a_{r \ 1}}{p \quad 1}$$

Aufgabe 13.29 Für welche Primzahlen p hat die Gleichung $x^2 \quad 75y^2 \quad 0$ eine nicht–triviale Lösung in $_p \quad _p$?

Aufgabe 13.30 Zeigen Sie, dass $_p$ als metrischer Raum mit der p–adischen Metrik kompakt ist. Zeigen Sie auch, dass $\mathbb{Q}_p$ lokalkompakt ist, d.h. jeder Punkt eine kompakte Umgebung besitzt.

14 Quadratrestklassen und Hilbert–Symbole

In Abschnitt 8 haben wir das Legendre– und Jacobi–Symbol eingeführt, um zu entscheiden, ob die Gleichung

$$X^2 \quad d \qquad \text{mit } d \quad \mathbb{F}_p$$

eine Lösung in $\mathbb{F}_p$ hat. Eine Besonderheit dieser Körper ist, dass in ihnen das Produkt zweier quadratischer Nichtreste immer ein quadratischer Rest ist. Das ist in $\mathbb{Q}$ und $\mathbb{Q}_p$ zum Beispiel nicht der Fall, deshalb kann man in diesen Körpern das Legendre–Symbol nicht einfach analog einführen. Wir gehen daher einen anderen Weg.

Für einen Körper K bezeichnen wir die Menge seiner Quadrate mit

$$K^{\ 2}: \quad a^2 \ \ a \quad K \qquad K$$

Diese bilden eine Untergruppe von K , und wir können daher die Quotientengruppe $K \quad K^{\ 2}$ betrachten. Ihre Elemente sind die Mengen

$$bK^{\ 2} \qquad ba^2 \quad K \quad a \quad K \qquad K$$

Die Verknüpfung dieser Elemente geschieht über die Repräsentanten.

Die Frage, ob ein $d \quad K$ ein Quadrat ist, ist nun äquivalent zur Frage, ob die Restklasse $dK^{\ 2}$ von d gleich der Einheitsklasse $1 \ K^{\ 2} \quad K^{\ 2}$ ist, denn

$$dK^{\ 2} \quad K^{\ 2} \qquad\qquad d \quad K^{\ 2}$$

Die Elemente von $K \quad K^{\ 2}$ entsprechen den verschiedenen Arten, kein Quadrat zu sein.

Wir wollen diese Gruppe $K \quad K^{\ 2}$ für alle bisher aufgetretenen Körper bestimmen. Dazu definieren wir den folgenden Isomorphismus von Gruppen:

$$\log_{\ 1}: \{ \ 1 \qquad\qquad 2 \qquad\qquad 1 \qquad \overline{0} \quad 1 \qquad \overline{1}$$

Satz 14.1 *Für jede ungerade Primzahl p ist*

$$\Phi_{\ p}: \mathbb{F}_p \quad \mathbb{F}_p^{\ 2} \qquad 2 \qquad x\mathbb{F}_p^{\ 2} \qquad \log_{\ 1} \ \frac{x}{p}$$

ein Isomorphismus. Für $p \quad 2$ ist $\mathbb{F}_2 \quad \mathbb{F}_2^{\ 2} \quad \{1$.

S. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie,*
DOI 10.1007/978-3-8348-8263-9_14,

Beweis: Wegen $\mathbb{F}_2 = \{1\}$ ist die Aussage für $p = 2$ trivial. Für $p \geq 3$ betrachten wir zuerst die Abbildung $\log_1 \left(\frac{\cdot}{p}\right) : \mathbb{F}_p^* \to \{\pm 1\}$. Per Definition liegt $\mathbb{F}_p^{*2}$ in ihrem Kern. Da nach Lemma 8.3 jeweils die Hälfte der Elemente von $\mathbb{F}_p^*$ Quadrate und Nichtquadrate sind, ist die Abbildung surjektiv und $\#\mathbb{F}_p^* / \mathbb{F}_p^{*2} = 2$. Also ist die induzierte Abbildung $\Phi_p : \mathbb{F}_p^* / \mathbb{F}_p^{*2} \to \{\pm 1\}$ ein Isomorphismus.

Auch für reelle Zahlen ist die Situation einfach.

Satz 14.2 *Die Abbildung*

$$\Phi : \mathbb{R}^* \to \{\pm 1\}, \quad x \mapsto \log_1 \operatorname{sgn} x$$

ist ein Isomorphismus. Insbesondere ist $\{\pm 1\}$ ein vollständiges Repräsentantensystem von $\mathbb{R}^*/\mathbb{R}^{*2}$.

Beweis: Die Aussage ist offensichtlich, da -1 in $\mathbb{R}^{*2}$ kein Quadrat ist und jedes $x \in \mathbb{R}^*$ sich schreiben lässt als $x = \operatorname{sgn} x \cdot \sqrt{x^2}$.

In Analogie zu den Körpern $\mathbb{F}_p$ definiert man daher auch auf $\mathbb{Q}_\infty$ ein Legendre–Symbol

$$\left(\frac{\cdot}{\infty}\right) : \mathbb{Q}_\infty^* \to \{\pm 1\}, \quad x \mapsto \operatorname{sgn} x$$

Für die rationalen Zahlen ist die Gruppe $\mathbb{Q}^*/\mathbb{Q}^{*2}$ sehr groß.

Satz 14.3 *Die Abbildung*

$$\Phi : \mathbb{Q}^*/\mathbb{Q}^{*2} \to \{\pm 1\} \times \bigoplus_p \mathbb{Z}/2\mathbb{Z}, \quad x\mathbb{Q}^{*2} \mapsto \left(\log_1 \operatorname{sgn} x, \; v_p(x) \bmod 2\right)_p$$

ist ein Isomorphismus.

Wir erinnern uns, dass die direkte Summe von Gruppen G_i, $i \in I$, definiert ist durch

$$\bigoplus_{i \in I} G_i = \{(g_i) \in \prod_{i \in I} G_i \mid \text{nur endlich viele } g_i \neq 0\}$$

Beweis: Wir betrachten zunächst die Abbildung $\tilde{\Phi} : \mathbb{Q}^* \to \{\pm 1\} \times \bigoplus_p \mathbb{Z}/2\mathbb{Z}$, die analog zu Φ definiert ist. $\tilde{\Phi}$ bildet tatsächlich in die direkte Summe ab und nicht nur in das direkte Produkt, weil nur endlich viele verschiedene Primzahlen in den Primfaktorzerlegungen des Nenners und Zählers der rationalen Zahl x vorkommen. Dass $\tilde{\Phi}$ ein Homomorphismus ist, ist eine Folge der Rechengesetze für die p–adischen Bewertungen. Auch die Surjektivität ist klar. Ein gegebenes $i \cdot \prod_p p^{r_p}$ ist das Bild von $(-1)^i \prod_p p^{r_p}$.

Berechnen wir den Kern von $\tilde{\Phi}$. Es gilt $\mathbb{Q}^{\ 2}$ $\mathrm{Ker}\tilde{\Phi}$, da x^2 0 und $v_p\ x^2$ $2v_p\ x$. Tatsächlich ist $\mathrm{Ker}\tilde{\Phi}$ $\mathbb{Q}^{\ 2}$. Für ein x $\mathrm{Ker}\tilde{\Phi}$ gilt x 0 und in einer Primfaktorzerlegung x $\prod_p$ p^{r_p} von x müssen alle Exponenten r_p gerade sein. Daher ist

$$x \quad \prod_p p^{\frac{r_p}{2}}{}^2$$

ein Quadrat. Die Anwendung des Homomorphiesatzes liefert die Behauptung.

Wenden wir uns schließlich den p–adischen Zahlen zu.

Satz 14.4 *Für eine ungerade Primzahl p ist*

$$\Phi_p : \mathbb{Q}_p \quad \mathbb{Q}_p^{\ 2} \qquad 2 \qquad 2$$

$$up^n\mathbb{Q}_p^{\ 2} \qquad \log_{\ 1}\frac{u}{p} \quad n \quad 2 \qquad \textit{mit } u \quad {}_p$$

ein Isomorphismus. Insbesondere gilt, dass für jedes ε ${}_p$ mit $\frac{\varepsilon}{p}$ 1 die Menge $\{1\ \varepsilon\ p\ \varepsilon p$ ein vollständiges Repräsentantensystem von $\mathbb{Q}_p$ $\mathbb{Q}_p^{\ 2}$ ist.

Dabei ist das Symbol $\frac{u}{p}$ für u ${}_p$ so zu verstehen, dass man u modulo p betrachtet und somit als Element von p auffasst.

Beweis: Wir betrachten wieder zuerst den Homomorphismus $\tilde{\Phi}_p : \mathbb{Q}_p$ 2 2 , der genau wie in der Aussage nur direkt auf den Elementen statt auf den Restklassen definiert ist. Für die Surjektivität von $\tilde{\Phi}_p$ brauchen wir nur zu merken, dass $\tilde{\Phi}_p\ p$ $\overline{0}\ \overline{1}$ und $\tilde{\Phi}_p\ \varepsilon$ $\overline{1}\ \overline{0}$ für jedes ε ${}_p$ mit $\frac{\varepsilon}{p}$ 1 gilt.

Berechnen wir nun den Kern von $\tilde{\Phi}_p$. Zuerst bemerken wir, dass $\mathbb{Q}_p^{\ 2}$ $\mathrm{Ker}\tilde{\Phi}_p$. Nämlich für ein x up^n ist x^2 u^2p^{2n} und damit

$$\tilde{\Phi}_p\ x^2 \qquad \log_{\ 1}\frac{u^2}{p} \quad 2n \quad 2 \qquad \log_{\ 1}1\ \overline{0} \qquad \overline{0}\ \overline{0}$$

Sei nun up^n ein Element des Kerns von $\tilde{\Phi}_p$. Dann ist $\frac{u}{p}$ 1 und 2 n. u ist damit ein Quadrat modulo p. Es gibt also eine Lösung $\tilde{v}$ $\{0$ der Gleichung X^2 u $0 \bmod p$. Nach dem Henselschen Lemma kann $\tilde{v}$ zu einer Lösung v ${}_p$ von X^2 u 0 geliftet werden. Nun gilt $vp^{n/2\ 2}$ v^2p^n up^n, d.h. jedes Element des Kerns ist ein Quadrat. Mit Hilfe des Homomorphiesatzes ergibt sich die Aussage.

Satz 14.5 *Die Abbildung*

$$\Phi_2 : \mathbb{Q}_2 \quad \mathbb{Q}_2^{\ 2} \qquad U_8 \qquad 2 \qquad 2 \qquad 2 \qquad 2$$

$$u2^n\mathbb{Q}_2^{\ 2} \qquad u \bmod 8 \quad n \quad 2 \qquad \textit{mit } u \quad {}_2$$

ist ein Isomorphismus. Insbesondere ist $\{$ 1 5 2 10 ein vollständiges Repräsentantensystem von $\mathbb{Q}_2$ $\mathbb{Q}_2^{\ 2}$.

Beweis: Wie immer betrachten wir zuerst die analog definierte Abbildung

$$\tilde{\Phi}_2 : \mathbb{Q}_2 \quad U_8 \quad 2$$

$\tilde{\Phi}_2$ ist offensichtlich surjektiv. Man sieht fast genauso einfach, dass jedes Quadrat im Kern von $\tilde{\Phi}_2$ liegt, schließlich ist jedes Quadrat in U_8 gleich 1 wegen $U_8 \quad 2 \quad 2$.

Sei nun ein Element $u2^n$ des Kerns gegeben, d.h. $u \quad 1 \bmod 8$ und $2 \; n$. Wir wollen zeigen, dass es ein Quadrat ist. Dazu suchen wir eine Quadratwurzel mit dem Henselschen Lemma. Für das Polynom

$$f \quad X^2 \quad u \quad {}_2 X$$

gilt $l : \quad \nu_2 \; f' \; u \quad \nu_2 \; 2u \quad 1$ und $f \; u \quad u^2 \quad u \quad u \; u \quad 1 \quad 0 \bmod 2^{2l \; 1} \quad 8$. Somit gibt es nach dem Henselschen Lemma ein $w \quad {}_2$ mit $w^2 \quad u$. Folglich ist das Element $u2^n$ des Kerns von $\tilde{\Phi}_2$ das Quadrat von $w2^{n/2}$. Wir haben somit $\mathrm{Ker} \; \tilde{\Phi}_2 \quad \mathbb{Q}_2^{\;2}$ gezeigt und der Homomorphiesatz impliziert jetzt die Aussage.

Aufgabe 14.6 Eine Quadratwurzel von u lässt sich im obigen Beweis auch durch die Benutzung des Korollars 13.16 aus dem Henselschen Lemmas mit $l \quad 0$ konstruieren. Dazu muss man jedoch das Polynom $f \quad 2X^2 \quad X \quad \frac{u \; 1}{8} \quad {}_2 X$ an der Stelle 0 betrachten. Falls w eine Lösung von f in ${}_2$ ist, so ist $4w \quad 1$ eine Quadratwurzel von u. Arbeiten Sie das aus.

Beispiel Wir wollen entscheiden, ob $x \quad 833$ ein Quadrat in $\mathbb{Q}_7$ ist. Es gilt $x \quad 7^2 \; 17$ und

$$\frac{17}{7} \quad \frac{3}{7} \quad \frac{7}{3} \quad \frac{1}{3} \quad 1$$

Daher ist $\Phi_7 \quad \overline{1} \; \overline{0}$ und x kein Quadrat in $\mathbb{Q}_7$.

Wir haben jetzt $K \quad K^{\;2}$ für alle uns bekannten Körper ausgerechnet. Auffällig ist, dass dies alles recht einfache Gruppen sind — mit Ausnahme von $\mathbb{Q} \quad \mathbb{Q}^{\;2}$. Dies ist wieder ein Merkmal der lokal–global Beziehung von $\mathbb{Q}$ zu $\mathbb{Q}_p$ und . Typisch ist auch der folgende Satz.

Satz 14.7 (Hasse–Minkowski, Teil 0) *Die Gleichung*

$$X^2 \quad d \quad \textit{mit } d \quad \mathbb{Q}$$

hat eine Lösung in $\mathbb{Q}$ genau dann, wenn sie eine Lösung in allen Körpern und $\mathbb{Q}_p$, p , hat.

Beweis: Wegen $\mathbb{Q} \quad \mathbb{Q}_p$ ist eine Lösung in $\mathbb{Q}$ auch eine Lösung in den anderen Körpern. Die Eigenschaft von d in den Körpern und $\mathbb{Q}_p$, p , ein Quadrat zu sein, impliziert nach den Sätzen 14.2, 14.4 und 14.5, dass $2 \; \nu_p \; d$ und $d \quad 0$. Nach Satz 14.3 folgt nun, dass d ein Quadrat in $\mathbb{Q}$ ist.

Anstatt nach der Lösbarkeit von $X^2 \quad d, d \quad 0$, zu fragen, hätten wir auch nach der Existenz einer nicht–trivialen Lösung $y \; z \quad 0$ von $dY^2 \quad Z^2$ fragen können. Schließlich bekommen

wir aus $x^2 \quad d$ die Gleichung $d \ 1^2 \quad x^2$ und umgekehrt aus $dy^2 \quad z^2$ die Gleichung $z \ y^{\ 2}$ d, weil wegen $d \quad 0$ sowohl y als auch z ungleich Null sein müssen.

In dieser Form verallgemeinern sich die Ergebnisse besser. Wir werden die Lösbarkeit von

$$aX^2 \quad bY^2 \quad Z^2$$

untersuchen.

Definition 14.8 *Sei* $p \qquad \{\infty$ *und* $a \ b \quad \mathbb{Q}_p$, *wobei* $\mathbb{Q}_\infty : \quad .$ *Dann ist das* Hilbert–Symbol

$$\frac{a \ b}{p} \qquad \{ \quad 1 \quad 1$$

genau dann gleich 1, *wenn die Gleichung*

$$aX^2 \quad bY^2 \quad Z^2$$

ein Lösung $0 \quad x \ y \ z \quad \mathbb{Q}_p^{\ 3}$ *besitzt.*

Obwohl das quadratische Polynom $aX^2 \quad bY^2 \quad Z^2$ recht einfach ist, stellt sich die Frage, warum wir gerade seine Nullstellen untersuchen. Tatsächlich ist das aber gar keine Einschränkung. Aus der linearen Algebra ist der folgende Satz bekannt [L, XIV, 3].

Satz 14.9 *Sei* $Q \quad \sum_{i \ j \ 1}^{n} a_{ij}X_iX_j$, $a_{ij} \quad a_{ji} \quad K$, *eine quadratische Form in n Variablen über einem Körper* K *mit* $2 \quad 0$. *Dann gibt es eine lineare Transformation der Koordinaten, so dass anschließend* Q *die Form*

$$Q \quad \sum_{i \ 1}^{r} a_i X_i^2 \quad \text{mit } a_i \quad 0 \text{ für } i \quad 1 \qquad r$$

hat. Die Invariante r *ist dabei der Rang der quadratischen Form* Q.

Also kann jede quadratische Form vom Rang 3 über $\mathbb{Q} \ \mathbb{Q}_p$ durch lineare Koordinatentransformation auf die Form $aX^2 \quad bY^2 \quad cZ^2$ mit $abc \quad 0$ gebracht werden. Wenn uns nur die Nullstellen von Q interessieren, können wir auch

$$\frac{1}{c}Q \qquad \frac{a}{c}X^2 \quad \frac{b}{c}Y^2 \quad Z^2$$

betrachten, und dies ist gerade die in der Definition des Hilbert–Symbols verwendete Form.

Für die reellen Zahlen lässt sich das Hilbert–Symbol unmittelbar berechnen.

Lemma 14.10 *Für* $a \ b \qquad$ *gilt*

$$\frac{a \ b}{\infty} \qquad 1 \qquad\qquad a \quad 0 \text{ oder } b \quad 0$$

Beweis: Für $a \quad 0$ gilt

$$a \ 1^2 \quad b \ 0^2 \quad \sqrt{a}^{\,2} \qquad \frac{a \ b}{\infty} \qquad 1$$

Für $b \quad 0$ argumentiert man analog. Wenn $a \quad 0$ und $b \quad 0$ gilt, ist der Ausdruck $ax^2 \quad by^2$ für jedes $x \ y \quad 0$ negativ und damit kein Quadrat. Somit besitzt $aX^2 \quad bY^2 \quad Z^2$ in diesem Fall keine nicht–triviale Lösung.

Um das Hilbert–Symbol für die Körper $\mathbb{Q}_p$ berechnen zu können, benötigen wir einige elementare Eigenschaften:

Lemma 14.11 *Für $p \qquad \{\infty$ und $a \ b \ c \ d \quad \mathbb{Q}_p$ gilt:*

1. $\dfrac{a \ b}{p} \qquad \dfrac{b \ a}{p}$.
2. $\dfrac{a \ 1}{p} \qquad \dfrac{a \quad a}{p} \qquad 1.$
3. $\dfrac{a \ 1 \quad a}{p} \qquad 1$ *für* $a \quad 1.$
4. $\dfrac{a \ b}{p} \qquad \dfrac{ac^2 \ bd^2}{p}$,

   d.h. das Hilbert–Symbol hängt nur von den Restklassen von a und b in $\mathbb{Q}_p \quad \mathbb{Q}_p{}^2$ *ab.*
5. $\dfrac{ab \ ac}{p} \qquad \dfrac{ab \quad bc}{p}$.
6. *Für* $\dfrac{a \ c}{p} \qquad 1$ *gilt* $\dfrac{a \ b}{p} \qquad \dfrac{a \ bc}{p}$.

Beweis: Die Symmetrie des Hilbert–Symbols folgt unmittelbar aus seiner Definition. Die Punkte 2) und 3) sind durch die Gleichungen

$$a \ 0^2 \quad 1 \ 1^2 \quad 1^2 \quad a \ 1^2 \qquad a \quad 1^2 \quad 0^2 \quad \text{und} \quad a \ 1^2 \quad 1 \quad a \quad 1^2 \quad 1^2$$

bewiesen. Für 4) bemerken wir, dass die Gleichung

$$ac^2X^2 \quad bd^2Y^2 \quad a \ cX^{\,2} \quad b \ dY^{\,2} \quad Z^2$$

durch die Variablensubstitution $\tilde{X} \quad cX$ und $\tilde{Y} \quad dY$ in die Gleichung $a\tilde{X}^2 \quad b\tilde{Y}^2 \quad Z^2$ übergeht. Daher können die Lösungen der beiden Gleichungen ineinander umgerechnet werden.

Für 5) formen wir die Gleichung $abX^2 \quad acY^2 \quad Z^2$ äquivalent um:

$$abX^2 \quad acY^2 \quad Z^2 \qquad Z^2 \quad acY^2 \qquad abX^2 \qquad \tfrac{1}{ab}Z^2 \quad \tfrac{c}{b}Y^2 \quad X^2$$

Somit gilt mit Hilfe von 4)

$$\frac{ab\ ac}{p} \qquad \frac{\frac{1}{ab}\quad \frac{c}{b}}{p} \qquad \frac{ab\quad bc}{p}$$

Da die Hilbert–Symbole nur zwei Werte annehmen, können wir die Gleichheit in Aussage 6) auch formulieren als

$$\frac{a\ b}{p} \quad 1 \qquad \frac{a\ bc}{p} \quad 1$$

Sei zunächst neben $\frac{a\ c}{p} \quad 1$ auch $\frac{a\ b}{p} \quad 1$. Wir finden daher $x\ y\ z \quad 0$ und $\tilde{x}\ \tilde{y}\ \tilde{z} \quad 0$ mit

$$ax^2 \quad by^2 \quad z^2 \quad \text{und} \quad a\tilde{x}^2 \quad c\tilde{y}^2 \quad \tilde{z}^2$$

Sollte $y \quad 0$ oder $\tilde{y} \quad 0$ sein, so haben wir sofort die gesuchte Lösung von $aX^2 \quad bcY^2 \quad Z^2$. Wir könnten nun direkt nachrechnen, dass sonst $x\tilde{z} \quad \tilde{x}z\ y\tilde{y}\ ax\tilde{x} \quad z\tilde{z}$ eine nicht–triviale Lösung dieser Gleichung ist. Jedoch wäre dann immer noch unklar, woher diese Lösung kommt. Wir gehen daher einen anderen Weg. Nach Division der Gleichungen durch y^2 bzw. $\tilde{y}^2$ können wir annehmen, dass ohne Einschränkung $y \quad \tilde{y} \quad 1$ gilt. Wir haben also $b \quad z^2 \quad ax^2$ und $c \quad \tilde{z}^2 \quad a\tilde{x}^2$. Wir rechnen in dem Erweiterungskörper $\mathbb{Q}_p\ \sqrt{a} \quad \mathbb{Q}_p \quad \mathbb{Q}_p\sqrt{a}$ (Diese Summe kann auch $\mathbb{Q}_p$ sein.):

$$\begin{aligned}
bc \quad & z^2 \quad ax^2 \quad \tilde{z}^2 \quad a\tilde{x}^2 \\
& z \quad \sqrt{a}x \quad z \quad \sqrt{a}x \quad \tilde{z} \quad \sqrt{a}\tilde{x} \quad \tilde{z} \quad \sqrt{a}\tilde{x} \\
& z \quad \sqrt{a}x \quad \tilde{z} \quad \sqrt{a}\tilde{x} \quad z \quad \sqrt{a}x \quad \tilde{z} \quad \sqrt{a}\tilde{x} \\
& z\tilde{z} \quad ax\tilde{x} \quad \sqrt{a}\,x\tilde{z} \quad \tilde{x}z \quad z\tilde{z} \quad ax\tilde{x} \quad \sqrt{a}\,x\tilde{z} \quad \tilde{x}z \\
& z\tilde{z} \quad ax\tilde{x}^{\,2} \quad a\,x\tilde{z} \quad \tilde{x}z^{\,2}
\end{aligned}$$

$$a\,x\tilde{z} \quad \tilde{x}z^{\,2} \quad bc \quad 1^2 \quad z\tilde{z} \quad ax\tilde{x}^{\,2} \qquad \frac{a\ bc}{p} \quad 1$$

Falls umgekehrt $\frac{a\ bc}{p} \quad 1$ ist, nutzen wir das gerade Bewiesene um

$$1 \quad \frac{a\ bc}{p} \qquad \frac{a\ bcc}{p} \qquad \frac{a\ b}{p}$$

zu folgern.

Nun sind wir bereit, die Hilbert–Symbole zu berechnen.

Satz 14.12 *Sei p eine ungerade Primzahl, $n\ m$ und $u\ v$ $_p$. Dann gilt:*

$$\frac{u\ v}{p} \quad 1 \quad \frac{u\ vp}{p} \qquad \frac{vp\ u}{p} \qquad \frac{u}{p} \quad \textit{und} \quad \frac{up\ vp}{p} \qquad \frac{uv}{p}$$

In geschlossener Form ist das

$$\frac{up^n \quad vp^m}{p} \qquad 1 \ ^{nm\frac{p\ 1}{2}} \quad \frac{u}{p} \quad ^m \quad \frac{v}{p} \quad ^n$$

oder in Tabellenform

$p \quad 1 \bmod 4$

	1	ε	p	εp
1	1	1	1	1
ε	1	1	1	1
p	1	1	1	1
εp	1	1	1	1

$p \quad 3 \bmod 4$

	1	ε	p	εp
1	1	1	1	1
ε	1	1	1	1
p	1	1	1	1
εp	1	1	1	1

wobei $1 \ \varepsilon \ p \ \varepsilon p$ *das Repräsentantensystem von* $\mathbb{Q}_p \quad \mathbb{Q}_p \ ^2$ *aus Satz 14.4 ist.*

Beweis: Wir zeigen zuerst $\frac{u\ v}{p} \quad 1$. Wir suchen daher nach einer Lösung $x \ y \ z \quad 0$ von $uX^2 \quad vY^2 \quad Z^2$. Schränken wir uns auf Lösungen mit $y \quad 1$ ein und suchen zunächst Lösungen in $\mathbb{F}_p$. Wir betrachten die folgenden Mengen in $\mathbb{F}_p$

$$M_1 \quad \{u\tilde{x}^2 \quad v \bmod p \quad \tilde{x} \quad \mathbb{F}_p \quad \mathbb{F}_p$$
$$M_2 \quad \{ \quad \tilde{z}^2 \bmod p \quad \tilde{z} \quad \mathbb{F}_p \quad \mathbb{F}_p$$

Da wir wissen, dass $\#\mathbb{F}_p \ ^2 \quad \frac{p\ 1}{2}$ ist, gilt $\#M_1 \quad \#M_2 \quad 1 \quad \#\mathbb{F}_p \ ^2 \quad \frac{p\ 1}{2}$. Also ist $\#M_1 \quad \#M_2 \quad p \quad 1 \quad \#\mathbb{F}_p$, d.h. M_1 und M_2 haben ein gemeinsames Element $w \quad \mathbb{F}_p$, für das es $\tilde{x} \ \tilde{z} \quad \mathbb{F}_p$ gibt mit

$$u\tilde{x}^2 \quad v \quad w \quad \tilde{z}^2 \mod p$$

$\tilde{x}$ und $\tilde{z}$ können nicht beide 0 sein. Nehmen wir $\tilde{x} \quad 0$ an, andernfalls führt man das Argument mit vertauschten Rollen von $\tilde{x}$ und $\tilde{z}$. Für $\tilde{z}$ wählen wir irgendeine Liftung nach $\ _p$. Eine passende Liftung x für $\tilde{x}$ finden wir durch die Anwendung des Henselschen Lemmas auf das Polynom $f \quad uX^2 \quad v \quad z^2$, weil $\tilde{x}$ eine Nullstelle von f modulo p ist und $f' \ \tilde{x} \quad 2u\tilde{x} \quad 0 \bmod p$ ist. Insgesamt gilt nun $u \ x^2 \quad v \ 1^2 \quad z^2$, und das Hilbert–Symbol $\frac{u\ v}{p}$ ist eins.

Wenden wir uns jetzt $\frac{u\ vp}{p} \quad \frac{u}{p}$ zu. Angenommen es gibt eine nicht–triviale Lösung $x \ y \ z$ von

$$uX^2 \quad vpY^2 \quad Z^2$$

Wenn wir $x \ y \ z$ mit dem gleichen Faktor multiplizieren, erhalten wir eine weitere Lösung. Wir dürfen daher nach Multiplikation mit der richtigen p–Potenz annehmen, dass $x \ y \ z$ in $\ _p$ und mindestens eins davon in $\ _p$ liegt. Wir wollen zeigen, dass $x \quad _p$ gilt. Sollte $x \quad p \ _p$ sein, teilt p^2 den Term $z^2 \quad vpy^2$. Insbesondere teilt p dann z und damit teilt p^2 auch vpy^2. Dies führt zu $p \ y$ und $x \ y \ z \quad p \ _p$ und somit zu einem Widerspruch.

Betrachten wir jetzt die Gleichung modulo p, also $0 \quad ux^2 \quad z^2 \bmod p$. Insbesondere ist also auch $z \quad _p$. Wir folgern weiter $u \quad z \ x \ ^2 \bmod p$, damit ist $u \bmod p$ ein quadratischer Rest, d.h. $\frac{u}{p} \quad 1$.

Wenn wir damit starten, dass u ein quadratischer Rest modulo p ist, können wir die obige Rechnung umkehren. Zunächst finden wir $\tilde{z} \quad \mathbb{F}_p$ mit $u \quad \tilde{z}^2 \bmod p$. Dieses $\tilde{z}$ liften wir mit dem Henselschen Lemma zu einem $z \quad {}_p$ mit $z^2 \quad u$, somit gilt die Gleichung $u \ 1^2 \quad vp \ 0^2 \quad z^2$. Damit ist das Hilbert–Symbol $\frac{u\ vp}{p}$ gleich eins.

Bei $\frac{up\ vp}{p} \qquad \frac{uv}{p}$ nutzen wir Lemma 14.11.5 und das eben Gezeigte

$$\frac{up\ vp}{p} \qquad \frac{up \quad uv}{p} \qquad \frac{uv}{p}$$

Die geschlossene Form und die Tabelle verifiziert man durch die Betrachtung aller möglichen Fälle unter Ausnutzung von $\frac{1}{p} \qquad 1 \ \frac{p\ 1}{2}$.

Satz 14.13 *Für $u2^n \ v2^m \quad \mathbb{Q}_2$ mit $u \ v \quad {}_2$ gilt*

$$\frac{u2^n \ v2^m}{2} \qquad 1 \ \frac{u\ 1}{2}\cdot\frac{v\ 1}{2} \quad 1 \ n\frac{v^2\ 1}{8} \quad 1 \ m\frac{u^2\ 1}{8}$$

wobei die Ausdrücke $\frac{u\ 1}{2}$ $\frac{v\ 1}{2}$ $\frac{v^2\ 1}{8}$ $\frac{u^2\ 1}{8}$ jeweils modulo 2 zu verstehen sind. Mit dem vollständigen Repräsentantensystem $\{ \ 1 \quad 5 \quad 2 \quad 10$ von $\mathbb{Q}_2 \quad \mathbb{Q}_2{}^2$ lässt sich das durch die folgende Tabelle ausdrücken:

	1	1	5	5	2	2	10	10
1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1
5	1	1	1	1	1	1	1	1
5	1	1	1	1	1	1	1	1
2	1	1	1	1	1	1	1	1
2	1	1	1	1	1	1	1	1
10	1	1	1	1	1	1	1	1
10	1	1	1	1	1	1	1	1

Beweis: Während des Beweises nutzen wir die kompaktere Schreibweise $a \ b \ {}_2$ für das Hilbert–Symbol. Unsere Aufgabe ist die Tabelle zu verifizieren. Die Symmetrie der Hilbert–Symbole reduziert den Aufwand um fast die Hälfte. Die erste Zeile ist Lemma 14.11.2. Für die zweite Zeile beweisen wir die 1 durch Hinschreiben der entsprechenden Gleichheiten:

$$1 \ 2 \ {}_2 \quad 1 \quad \text{weil} \quad 1 \ 1^2 \quad 2 \ 1^2 \quad 1^2$$
$$1 \ 5 \ {}_2 \quad 1 \quad \text{weil} \quad 1 \ 1^2 \quad 5 \ 1^2 \quad 2^2$$
$$1 \ 10 \ {}_2 \quad 1 \quad \text{weil} \quad 1 \ 1^2 \quad 10 \ 1^2 \quad 3^2$$

Wir zeigen nun $1 \quad 2 \ {}_2 \quad 1$. Angenommen, das gelte nicht und wir hätten eine nicht–triviale Lösung $x \ y \ z$ der Gleichung

$$X^2 \quad 2Y^2 \quad Z^2$$

Wir können wie im Beweis vorher bei der Gleichung $uX^2 \quad vpY^2 \quad Z^2$ zeigen, dass wir $x\ y\ z \quad _2$ und $x\ z \quad _2$ annehmen dürfen. Nun folgt $x^2 \quad z^2 \quad 1 \bmod 8$ wegen $U_8 \quad 2 \quad 2$. Daher gilt

$$2y^2 \quad z^2 \quad x^2 \quad 2 \mod 8 \qquad y^2 \quad 1 \mod 4$$

was unmöglich ist.

Nun folgen die weiteren Einträge der zweiten Zeile aus Lemma 14.11.6:

$$\begin{array}{lll} 1 \quad 1 \ _2 & 1 \quad 4 \ _2 & 1 \quad 2 \ 2 \ _2 \quad 1 \quad 2 \ _2 \quad 1 \\ 1 \quad 5 \ _2 & 1 \quad 1 \ 5 \ _2 & 1 \quad 1 \ _2 \quad 1 \\ 1 \quad 10 \ _2 & 1 \quad 1 \ 10 \ _2 & 1 \quad 1 \ _2 \quad 1 \end{array}$$

Die restlichen Einträge der Tabelle sind nun einfach zu berechnen. Nach Lemma 14.11.2 haben wir

$$5 \quad 5 \ _2 \quad 2 \quad 2 \ _2 \quad 10 \quad 10 \ _2 \quad 1$$

Nach Satz 14.5 gilt $5\mathbb{Q}_2^{\ 2} \quad 3\mathbb{Q}_2^{\ 2} \quad 11\mathbb{Q}_2^{\ 2}$ in $\mathbb{Q}_2 \quad \mathbb{Q}_2^{\ 2}$, und mit Lemma 14.11.3 folgt

$$5 \quad 2 \ _2 \quad 3 \quad 2 \ _2 \quad 1 \quad \text{und} \quad 5 \quad 10 \ _2 \quad 11 \quad 10 \ _2 \quad 1$$

Mit Lemma 14.11.5 erhalten wir

$$2 \quad 10 \ _2 \qquad 2 \ 1 \quad 2 \ 5 \ _2 \qquad 2 \quad 5 \ _2 \quad 1$$

Nun können wir die Hilbert–Symbole, die sich von den obigen nur um ein Vorzeichen unterscheiden, durch Anwendung von Lemma 14.11.6 mit den Hilbert–Symbolen der zweiten Zeile berechnen:

$$\begin{array}{lll} 5\ 5 \ _2 & 5 \quad 1 \quad 5 \ _2 & 5 \quad 1 \ _2 \quad 1 \\ 5 \quad 5 \ _2 & 1 \ 5 \quad 5 \ _2 & 1 \quad 5 \ _2 \quad 1 \\ 2\ 2 \ _2 & 2 \quad 1 \quad 2 \ _2 & 2 \quad 1 \ _2 \quad 1 \\ 2 \quad 2 \ _2 & 1 \ 2 \quad 2 \ _2 & 1 \quad 2 \ _2 \quad 1 \\ 10\ 10 \ _2 & 10 \quad 1 \quad 10 \ _2 & 10 \quad 1 \ _2 \quad 1 \\ 10 \quad 10 \ _2 & 1 \ 10 \quad 10 \ _2 & 1 \quad 10 \ _2 \quad 1 \\ 5\ 2 \ _2 & 5 \quad 1 \quad 2 \ _2 & 5 \quad 1 \ _2 \quad 1 \\ 5 \quad 2 \ _2 & 1 \quad 5 \quad 2 \ _2 & 1 \quad 2 \ _2 \quad 1 \\ 5 \quad 10 \ _2 & 1 \quad 5 \quad 10 \ _2 & 1 \quad 10 \ _2 \quad 1 \\ 5\ 10 \ _2 & 5 \quad 1 \quad 10 \ _2 & 5 \quad 1 \ _2 \quad 1 \\ 2 \quad 10 \ _2 & 1 \quad 2 \quad 10 \ _2 & 1 \quad 10 \ _2 \quad 1 \\ 2\ 10 \ _2 & 2 \quad 1 \quad 10 \ _2 & 2 \quad 1 \ _2 \quad 1 \end{array}$$

Die letzten drei Einträge der Tabelle berechnen wir mit Hilfe von Lemma 14.11.5

$$\begin{array}{lll} 2\ 10_2 & 2\ 1\ 2\ 5_2 & 2\ \ 5_2 \quad 1 \\ 2\ 5_2 & 1\ 2\ 1\ 5_2 & 2\ \ 10_2 \quad 1 \\ 5\ 10_2 & 5\ 1\ 5\ 2_2 & 5\ \ 2_2 \quad 1 \end{array}$$

Die geschlossene Form für das Hilbert–Symbol wird an Hand der Tabelle verifiziert.

Korollar 14.14 *Das Hilbert–Symbol ist bimultiplikativ.*

Beweis: Für p ergibt sich das unmittelbar aus den geschlossenen Formen für die Hilbert–Symbole. Wir haben nämlich bereits im Beweis von Satz 8.12 gezeigt, dass deren Faktoren multiplikativ bzw. bimultiplikativ sind.

Für $p \quad \infty$, also für den Körper , reicht es den Fall

$$\frac{1\ \ 1}{\infty} \qquad \frac{1\ \ 1}{\infty} \qquad 1 \quad 1 \quad 1 \qquad \frac{1\ 1}{\infty} \qquad \frac{1\ \ 1\ \ 1}{\infty}$$

nachzurechnen — die restlichen folgen durch Symmetrie und aus Lemma 14.11.6.

Satz 14.15 *Für $a\ b$ $\mathbb{Q}$ gilt die Produktformel*

$$\prod_{p \quad \infty} \frac{a\ b}{p} \quad 1$$

Beweis: Das Hilbert–Symbol hängt nur von den Klassen von a und b in $\mathbb{Q}_p \quad \mathbb{Q}_p{}^2$ ab. Wir dürfen nach Multiplikation mit den Quadraten der Nenner annehmen, dass a und b Elemente von sind. Wir bemerken nun, dass nur endlich viele der Faktoren in dem Produkt der Hilbert–Symbole ungleich 1 sind. Dies liegt daran, dass nach Satz 14.12 für alle $p \quad \{2\ ,$ die nicht in der Primfaktorzerlegung von a und b auftreten, das Hilbert–Symbol $\frac{a\ b}{p}$ eins ist.

Wegen der Bimultiplikativität der Symbole und $\frac{1\ a}{p} \quad 1$ können wir uns beim Beweis der Aussage auf die Fälle

$$a\ b \qquad 1 \quad 1 \qquad 1\ 2 \qquad 1\ q \quad 2\ 2 \quad 2\ q \quad q\ q \quad q\ r$$

mit ungeraden $q \quad r$ beschränken. Mit Lemma 14.11.5 können wir noch die Fälle $2\ 2$ und $q\ q$ auf die anderen zurückführen:

$$\frac{2\ 2}{p} \qquad \frac{2\ 1\ 2\ 1}{p} \qquad \frac{2\ \ 1}{p} \quad \text{und} \quad \frac{q\ q}{p} \qquad \frac{q\ 1\ q\ 1}{p} \qquad \frac{q\ \ 1}{p}$$

Es bleiben also 5 Fälle übrig:

$a\ b$	$\frac{a\ b}{\infty}$	$\frac{a\ b}{2}$	$\frac{a\ b}{q}$	$\frac{a\ b}{r}$
$1\quad 1$	1	1	1	1
$1\ 2$	1	1	1	1
$1\ q$	1	$1^{\frac{q\ 1}{2}}$	$\frac{1}{q}$	1
$2\ q$	1	$1^{\frac{q^2\ 1}{8}}$	$\frac{2}{q}$	1
$q\ r$	1	$1^{\frac{q\ 1}{2}\frac{r\ 1}{2}}$	$\frac{r}{q}$	$\frac{q}{r}$

Nun folgt die Behauptung aus dem quadratischen Reziprozitätsgesetz.

Als unmittelbare Folgerung erhalten wir:

Korollar 14.16 *Die quadratische Gleichung* $aX^2 \quad bY^2 \quad Z^2$ *habe Lösungen in* $\quad$ *und* $\mathbb{Q}_p$ *für alle Primzahlen p bis auf q. Dann hat sie auch eine Lösung in* $\mathbb{Q}_q$.

Die Bilinearität des Hilbert–Symbols kann noch anders interpretiert und verschärft werden. Wir haben gesehen, dass $\mathbb{Q}_p \quad {\mathbb{Q}_p}^2$ isomorph zu $\quad 2 \quad ^n$ mit $n \quad \{1\ 2\ 3$ ist. Wir erinnern uns, dass wir abelsche Gruppen als $\quad$–Modul betrachten können. Da hier alle Elemente multipliziert mit 2 das neutrale Element ergeben, haben wir eigentlich eine Operation von $\quad 2 \quad \mathbb{F}_2$ auf diesen abelschen Gruppen, d.h. wir haben $\mathbb{F}_2$–Vektorräume. Da bei den Isomorphismen $\mathbb{Q}_p \quad {\mathbb{Q}_p}^2 \quad \mathbb{F}_2^n$ aus den Multiplikationen Additionen werden, bedeutet das vorangehende Korollar, dass das Hilbert–Symbol additiv in beiden Argumenten und somit auch automatisch $\mathbb{F}_2$–bilinear ist.

Korollar 14.17 *Für jedes* $p \quad \{\infty$ *ist das Hilbert–Symbol eine nicht–degenerierte symmetrische Bilinearform auf dem* $\mathbb{F}_2$*–Vektorraum* $\mathbb{Q}_p \quad {\mathbb{Q}_p}^2$.

Beweis: Es bleibt nur noch die Nicht–Degeneriertheit zu zeigen, d.h. wir müssen zeigen, dass die zur symmetrischen Bilinearform gehörende symmetrische Matrix den maximalen Rang hat. Dazu schreiben wir einfach die Matrizen für das Hilbert–Symbol in einer Basis von $\mathbb{Q}_p \quad {\mathbb{Q}_p}^2$ hin. Wir müssen nur beachten, dass wir im Augenblick wegen den Isomorphismen in die Tabelle $\log_1 \frac{a\ b}{p}$ und nicht $\frac{a\ b}{p}$ selbst schreiben.

$p \quad \infty$

	1
1	1

$p \quad \{2$

	ε	p
ε	0	1
p	1	$\log_1 \frac{1}{p}$

$p \quad 2$

	1	5	2
1	1	0	0
5	0	0	1
2	0	1	0

Man sieht sofort, dass die Determinante sämtlicher Matrizen $\quad 1$ ist, somit haben diese Matrizen alle den vollen Rang.

Wir kommen zum abschließenden Höhepunkt des Abschnittes.

Satz 14.18 (Hasse–Minkowski, Teil 1) *Die Gleichung*

$$aX^2 \quad bY^2 \quad Z^2 \qquad \text{mit } a\ b \quad \mathbb{Q}$$

hat genau dann eine nicht–triviale Lösung über $\mathbb{Q}$*, wenn sie nicht–triviale Lösungen für und alle* $\mathbb{Q}_p$*,* p *, besitzt.*

Beweis: Wegen $\mathbb{Q} \quad \mathbb{Q}_p$ ist jede Lösung über $\mathbb{Q}$ auch eine Lösung in den anderen Körpern. Zum Beweis der anderen Richtung können wir wieder annehmen, dass $a\ b$ quadratfreie ganze Zahlen sind, da ja das Hilbert–Symbol nur von den Restklassen von $a\ b$ in $\mathbb{Q} \quad \mathbb{Q}^{\ 2}$ abhängt. Weiter setzen wir $a \qquad b$ voraus. Der Beweis ist nun eine Induktion nach $n \quad a \quad b$.

Beim Induktionsanfang für $n \quad 2$ sind bis auf Symmetrie nur die Gleichungen

$$X^2 \quad Y^2 \quad Z^2 \qquad X^2 \quad Y^2 \quad Z^2 \quad \text{und} \qquad X^2 \quad Y^2 \quad Z^2$$

möglich. Die letzte Gleichung hat keine nicht–triviale Lösung über und erfüllt daher unsere Voraussetzungen nicht. Die beiden anderen haben die nicht–triviale Lösung $1\ 0\ 1$ über $\mathbb{Q}$.

Für $n \quad 3$ ist $b \quad 2$ und damit insbesondere $b \qquad 1$. Wir wollen zeigen, dass a ein Quadrat modulo b ist. Dazu zeigen wir zuerst, dass a ein Quadrat modulo jedem Primteiler p von b ist. Sei $x\ y\ z$ eine nicht–triviale Lösung der Gleichung über $\mathbb{Q}_p$. Mit den gleichen Argumenten wie im Beweis von Satz 14.12 sehen wir, dass wir $x\ y\ z \qquad _p$ und $x\ z \qquad _p$ annehmen dürfen. Modulo p ist also

$$ax^2 \quad z^2 \mod p \qquad a \quad \left(\frac{z}{x}\right)^2 \quad 0 \mod p$$

Somit ist a ein Quadrat modulo p. Da b quadratfrei ist, ist seine Primfaktorzerlegung b $\prod_{i\ 1}^{s} p_i$ mit paarweise verschiedenen $p_i \qquad$. Daher gilt nach dem chinesischen Restsatz

$$b \quad \prod_{i\ 1}^{s} p_i$$

Da a ein Quadrat in allen p_i ist, ist es auch ein Quadrat modulo b. Wir finden daher $t\ b'$ mit

$$t^2 \quad a \quad bb' \quad \text{und} \quad t \quad \frac{b}{2}$$

Sollte $b' \quad 0$ sein, also $a \quad t^2$ gelten, haben wir schon mit $1\ 0\ t$ die gesuchte Lösung der Ausgangsgleichung gefunden. Ansonsten zerlegen wir b' in $b' \quad b''c^2$ mit $b'' \ c$ und b'' quadratfrei. Wir können die obige Gleichung sehen als

$$a\ 1^2 \quad bb''\ c^2 \quad t^2 \qquad \frac{a\ bb''}{p} \qquad 1 \quad \text{für alle } p \qquad \{\infty$$

Mit der Voraussetzung $\frac{a\ b}{p} \qquad 1$ und der Multiplikativität des Hilbert–Symbols bekommen wir

$$\frac{a\ b''}{p} \qquad \frac{a\ bb''}{p} \qquad 1$$

Nun gilt

$$b'' \quad b' \quad \frac{t^2 \quad a}{b} \quad \frac{t^{\,2}}{b} \quad \frac{a}{b} \quad \frac{b}{4} \quad 1 \quad b$$

also gibt es nach Induktionsvoraussetzung rationale Zahlen $\tilde{x}\ \tilde{y}\ \tilde{z}$, nicht alle gleich 0, mit

$$a\tilde{x}^2 \quad b''\tilde{y}^2 \quad \tilde{z}^2$$

Sollte hierbei $\tilde{y} \quad 0$ sein, ist $\tilde{x}\ \tilde{y}\ \tilde{z} \quad \mathbb{Q}^3$ schon eine nicht–triviale Lösung der Ausgangsgleichung. Ansonsten gewinnen wir genau wie im Beweis von Lemma 14.11.6 aus dieser Gleichung und der Gleichung $a \quad 1^2 \quad bb'' \quad c^2 \quad t^2$ die nicht–triviale Lösung $t\tilde{x} \quad \tilde{z}\ c\tilde{y}\ a\tilde{x} \quad t\tilde{z}$ von

$$aX^2 \quad b\ b''\ ^2Y^2 \quad Z^2$$

und somit ist $t\tilde{x} \quad \tilde{z}\ b''c\tilde{y}\ a\tilde{x} \quad t\tilde{z}$ eine nicht–triviale Lösung der Ausgangsgleichung.

Beispiel Wir wollen zeigen, dass die Gleichung

$$\frac{1}{8}X^2 \quad \frac{23}{9}Y^2 \quad Z^2$$

eine nicht–triviale Lösung über $\mathbb{Q}$ besitzt. Da diese Frage nur von den Quadratrestklassen abhängt, können wir wegen $1\ \ 8 \quad 2\ \ 4^2$ und $23\ \ 9 \quad 23\ \ 3^2$ auch die Gleichung

$$2X^2 \quad 23Y^2 \quad Z^2$$

betrachten. Offensichtlich ist die Gleichung über $\quad$ lösbar, zum Beispiel nach Lemma 14.10. Die Hilbert–Symbole $\frac{2\ 23}{p}$ für $p \qquad \{2\ 23$ sind alle eins nach Satz 14.12. Die zwei verbleibenden können wir auch leicht berechnen: Nach Satz 14.12 und Lemma 8.6 gilt

$$\frac{2\ \ 23}{23} \qquad \frac{2}{23} \qquad 1$$

und nach Satz 14.5 und der Tabelle in Satz 14.13 ist auch

$$\frac{2\ \ 23}{2} \qquad \frac{2 \quad 1}{2} \qquad 1$$

Da alle Hilbert–Symbole eins sind, besitzt die Gleichung über allen Körpern $\mathbb{Q}_p \quad$ eine nicht–triviale Lösung, folglich nach dem Satz von Hasse–Minkowski auch über $\mathbb{Q}$. Hier in diesem einfachen Beispiel sieht man die Lösung $1\ \ 1\ \ 5$ von $2X^2 \quad 23Y^2 \quad Z^2$ natürlich auch direkt, und somit auch die Lösung $4\ \ 3\ \ 5$ von $\frac{1}{8}X^2 \quad \frac{23}{9}Y^2 \quad Z^2$.

Tatsächlich hätten wir gar nicht alle Hilbert–Symbole ausrechnen müssen, denn es reicht nach Satz 14.15 zu zeigen, dass alle Symbole bis auf eins $\quad 1$ sind — das letzte ist dann auch

1. Im obigen Fall hätte es sich angeboten, das Hilbert–Symbol für $p \quad 2$ oder $p \quad 23$ nicht auszurechnen, sondern zu erschließen.

Zusatzaufgaben

Aufgabe 14.19 Bestimmen Sie für die Zahlen $r \in \{ 1, 2, 6, \frac{4}{5} \}$ jeweils die Menge der Primzahlen p, so dass r ein Quadrat im Körper $\mathbb{Q}_p$ ist.

Aufgabe 14.20 Zeigen Sie direkt — ohne Verwendung von Sätzen: Die Gleichung $X^2 + bX + c = 0$ mit $b, c \in \mathbb{Q}$ hat eine Lösung in $\mathbb{Q}$ genau dann, wenn sie eine reelle Lösung sowie eine Lösung in $\mathbb{Q}_p$ für alle p besitzt.

Aufgabe 14.21 Zwei der folgenden Gleichungen besitzen nur die triviale Lösung $x, y, z = 0, 0, 0$ über $\mathbb{Q}$. Welche sind das? Bestimmen Sie eine nicht–triviale Lösung der dritten.

$$3x^2 + 5y^2 + 7z^2 = 0 \qquad 5x^2 + 7y^2 + 3z^2 = 0 \qquad 3x^2 + 7y^2 + 5z^2 = 0$$

Aufgabe 14.22 Zeigen Sie: Sind p und q zwei verschiedene Primzahlen, dann sind $\mathbb{Q}_p$ und $\mathbb{Q}_q$ nicht isomorph.

Aufgabe 14.23 Sei p eine ungerade Primzahl. Zeigen Sie:

1. Ein Element $x \in \mathbb{Q}_p$ ist genau dann in $\mathbb{Z}_p$ enthalten, wenn $1 + px^2$ ein Quadrat in $\mathbb{Q}_p$ ist.
2. Der Körper $\mathbb{Q}_p$ besitzt keine Automorphismen außer der Identität.
3. Auch der Körper $\mathbb{Q}_2$ besitzt keine nicht–trivialen Automorphismen.

Aufgabe 14.24 Beweisen Sie durch Verwendung von Hilbert–Symbolen und ohne auf den Zwei–Quadrate–Satz 9.2 zurückzugreifen, dass eine Zahl $n \in \mathbb{N}$ genau dann als Summe von zwei Quadraten in $\mathbb{Q}$ darstellbar ist, wenn alle Primteiler p von n mit $p \equiv 3 \bmod 4$ nur mit geradem Exponenten vorkommen.

Aufgabe 14.25 Sei K ein Körper, in dem $2 \neq 0$ ist, $a, b \in K^*$ und $x_0, y_0 \in K^2$ eine Lösung der Gleichung

$$aX^2 + bY^2 = 1$$

Zeigen Sie, dass dann für jede weitere, von x_0, y_0 verschiedene Lösung x, y der Gleichung eine der folgenden Aussagen zutrifft:

1. Es gibt ein $t \in K$, so dass $at^2 + b \neq 0$ und
$$\begin{pmatrix} x \\ y \end{pmatrix} - \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = 2 \frac{ax_0t + by_0}{at^2 + b} \begin{pmatrix} t \\ 1 \end{pmatrix}$$
2. Es ist $x = x_0$ und $y = y_0$.

Aufgabe 14.26 Untersuchen Sie, ob die folgenden Gleichungen Lösungen $x, y \in \mathbb{Z}_p^*$ besitzen, so dass $x \not\equiv y \equiv 0 \bmod p$ gilt:

1. $x^4 + y^3 = p^2$.
2. $y^2 = x^3 + p$.

Aufgabe 14.27 Sei $l \geq 3$ eine Primzahl. Untersuchen Sie, ob die *Fermatsche Gleichung* $X^l + Y^l = Z^l$ (mit $XYZ \neq 0$) Lösungen in $\mathbb{Z}$ und $\mathbb{Q}_p$ besitzt.

15 Der Satz von Hasse–Minkowski

In diesem Abschnitt wollen wir die quadratischen Formen vom Rang größer als drei untersuchen und insbesondere den Satz von Hasse–Minkowski für sie beweisen. Nach Satz 14.9 können wir immer annehmen, dass die quadratische Form von dem Typ

$$Q \quad a_1X_1^2 \quad a_2X_2^2 \qquad a_rX_r^2 \qquad \text{mit } a_i \quad 0$$

ist, wobei r der Rang von Q ist.

In der Theorie der quadratischen Formen sind die folgenden Definitionen üblich:

Definition 15.1 *Sei Q eine quadratische Form über K vom Rang r in r Variablen. Ein $b \quad K$ wird von Q* dargestellt*, wenn es ein $0 \quad x \quad K^r$ gibt mit $Q\ x \quad b$. Q heißt* isotrop*, falls 0 von Q dargestellt wird, sonst* anisotrop*.*

Bemerkung Für ein Q in der Form $Q \quad \sum_{i \ 1}^{r} a_iX_i^2$ hängen die Fragen nach der Isotropie oder der Darstellbarkeit von Elementen nur von den Quadratrestklassen der a_i in $K \quad K^{\ 2}$ ab, weil wir für $a_ic_i^2X_i^2$ auch $a_i \ c_iX_i^{\ 2}$ schreiben können. Ebenso hängt die Darstellbarkeit eines $b \quad 0$ nur von seiner Quadratrestklasse ab, da $Q\ \lambda x_1 \ \lambda x_2 \qquad \lambda x_r \quad \lambda^2 Q\ x_1 \qquad x_r$ für $\lambda \quad K$.

Bemerkung 15.2 *Offensichtlich ist die quadratische Form $Q \quad \sum_{i \ 1}^{r} a_iX_i^2$ über genau dann isotrop, wenn nicht alle a_i das gleiche Vorzeichen haben.*

Satz 15.3 *Sei $Q \quad \sum_{i \ 1}^{r} a_iX_i^2$ eine isotrope quadratische Form über einem Körper mit $2 \quad 0$, dann ist jedes $b \quad K$ von Q darstellbar.*

Beweis: Sei $Q\ x_1 \qquad x_r \quad 0$ für geeignete $x_i \quad K$ und ohne Einschränkung $x_1 \quad 0$. Mit $\lambda \quad K$ machen wir den Ansatz

$$y_1 : \quad x_1 \ 1 \quad \lambda \quad \text{und} \quad y_i : \quad x_i \ 1 \quad \lambda \quad \text{für } i \quad 2 \qquad r$$

Dann gilt

$$\begin{aligned}\sum_{i \ 1}^{r} a_iy_i^2 \quad & a_1x_1^2 \ 1 \quad \lambda \ ^2 \quad a_1x_1^2 \ 1 \quad \lambda \ ^2 \quad 1 \quad \lambda \ ^2 \sum_{i \ 1}^{r} a_ix_i^2 \\ & a_1x_1^2 \quad 1 \quad \lambda \ ^2 \quad 1 \quad \lambda \ ^2 \qquad 1 \quad \lambda \ ^2 \ 0 \\ & 4a_1x_1^2\lambda\end{aligned}$$

Mit $\lambda \quad b \quad 4a_1x_1^2$ erhalten wir $Q\ y_1 \qquad y_r \quad b$.

S. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie,*
DOI 10.1007/978-3-8348-8263-9_15,

Machmal braucht man nicht nur eine nicht–triviale Nullstelle $x \quad x_i \quad 0$ einer quadratischen Form, sondern man will auch noch, dass bestimmte x_i ungleich 0 sind. Dabei hilft das folgende Lemma.

Lemma 15.4 *Jede isotrope quadratische Form* $Q \quad \sum_{i \quad 1}^{r} a_i X_i^2$ *über einem Körper* K *mit* $\#K \quad 6$ *besitzt eine Nullstelle* $x \quad x_i$ *mit* $x_i \quad 0$ *für alle* $i \quad 1 \quad r$.

Beweis: Da Q isotrop ist, gibt es zumindest eine Nullstelle $y_1 \quad y_r \quad 0$. Nach Umnummerierung können wir annehmen, dass $y_1 \quad y_n \quad 0$ und $y_{n \quad 1} \quad y_r \quad 0$. Es reicht zu zeigen, dass wir für $n \quad r$ eine Nullstelle $x \quad x_1 \quad x_r$ mit $x_1 \quad x_{n \quad 1} \quad 0$ finden können, dann folgt die Aussage durch Induktion.

Wir wählen $x_i \quad y_i$ für $i \quad \{1 \quad r \quad \{n \; n \quad 1$ und suchen $x_n \; x_{n \quad 1} \quad 0$ mit

$$a_n x_n^2 \quad a_{n \quad 1} x_{n \quad 1}^2 \quad a_n y_n^2 \quad a_n y_n^2 \quad a_{n \quad 1} y_{n \quad 1}^2$$

dann ist x offensichtlich die gesuchte Nullstelle von Q mit $n \quad 1$ Einträgen ungleich Null.

Diese $x_n \; x_{n \quad 1}$ finden wir ausgehend von der Gleichung

$$\frac{1 \quad \lambda^{\quad 2}}{1 \quad \lambda^{\quad 2}} \quad \frac{4\lambda}{1 \quad \lambda^{\quad 2}} \quad 1$$

Multiplikation mit $a_n y_n^2$ führt zu

$$a_n y_n^2 \quad a_n \left(\frac{1 \quad \lambda \; y_n}{1 \quad \lambda} \right)^{\quad 2} \quad a_n \lambda \left(\frac{2 y_n}{1 \quad \lambda} \right)^{\quad 2}$$

$$a_n \left(\frac{1 \quad \lambda \; y_n}{1 \quad \lambda} \right)^{\quad 2} \quad a_{n \quad 1} \frac{a_n \lambda}{a_{n \quad 1}} \left(\frac{2 y_n}{1 \quad \lambda} \right)^{\quad 2}$$

Nun setzt man $\lambda \quad \mu^2 a_{n \quad 1} \; a_n$, wobei μ ein Element aus K mit $\mu \quad 0$ und $\mu^2 \quad a_n \; a_{n \quad 1}$ ist. Dies existiert, da $\#K \quad 6$, und garantiert, dass $\lambda \quad 1$ ist. Nun gilt für

$$x_n : \quad \frac{1 \quad \lambda \; y_n}{1 \quad \lambda} \quad 0 \qquad \text{und} \qquad x_{n \quad 1} : \quad \frac{2 y_n \mu}{1 \quad \lambda} \quad 0$$

die gewünschte Gleichheit $a_n x_n^2 \quad a_{n \quad 1} x_{n \quad 1}^2 \quad a_n y_n^2$.

Eine typische Anwendung des Lemmas ist, eine Nullstelle von Q zu finden, wobei eines der x_i gleich 1 ist. Wenn wir zum Beispiel eine Nullstelle $x_1 \quad x_r$ mit $x_r \quad 1$ haben wollen, garantiert das Lemma zumindest eine Nullstelle $y_1 \quad y_r$ mit $y_r \quad 0$, dann ist aber $y_1 \; y_r \quad y_{r \quad 1} \; y_r \; 1$ die gesuchte Nullstelle.

Jetzt wollen wir untersuchen, wann die quadratischen Formen über $\mathbb{Q}_p$ isotrop sind.

Lemma 15.5 *Sei* p *eine ungerade Primzahl und* $Q \quad \sum_{i \quad 1}^{r} a_i X_i^2$ *eine quadratische Form über* $\mathbb{Q}_p$. *Falls* $r \quad 3$ *und* $a_1 \; a_2 \; a_3 \quad {}_p$ *gilt, ist* Q *isotrop.*

Beweis: Es ist zu zeigen, dass $a_1X_1^2 \quad a_2X_2^2 \quad a_3X_3^2 \quad 0$ eine nicht–triviale Lösung besitzt. Diese Gleichung ist äquivalent zu

$$\frac{a_1}{a_3}X_1^2 \quad \frac{a_2}{a_3}X_2^2 \quad X_3^2$$

Wegen $a_1 \ a_3 \quad a_2 \ a_3 \quad _p$ besitzt sie nach Satz 14.12 eine nicht–triviale Lösung.

Satz 15.6 *Für jede Primzahl p ist jede quadratische Form vom Rang 5 über $\mathbb{Q}_p$ isotrop.*

Beweis: Sei $Q \quad \sum_i^r {}_1 \, a_iX_i^2$ eine quadratische Form vom Rang 5 über $\mathbb{Q}_p$. Da die Isotropie nur von den Quadratrestklassen der a_i abhängt, dürfen wir annehmen, dass die a_i in $_p$ liegen und quadratfrei sind, d.h. $a_i \quad u_i$ oder $a_i \quad u_ip$ mit $u_i \quad _p$. Nach eventueller Multiplikation von Q mit p können wir auch noch annehmen, dass mindestens die Hälfte der a_i von der Form u_i sind, also nach Umnummerierung

$$Q \quad u_1X_1^2 \quad u_2X_2^2 \qquad u_sX_s^2 \quad p \ u_s \ {}_1X_s^2 \ {}_1 \qquad u_rX_r^2 \quad \text{mit } s \quad 3$$

Für $p \quad 2$ ist nach dem vorangegangenen Lemma bereits $u_1X_1^2 \quad u_2X_2^2 \quad u_3X_3^2$ isotrop und damit auch Q.

Sei daher für den Rest des Beweises $p \quad 2$. Wir versuchen zuerst eine Nullstelle modulo 8 zu finden. Wir müssen dabei zwei Fälle unterscheiden:

Im ersten Fall ist $s \quad 4 \quad r$. Wir setzen $\tilde{x}_1 \quad x_2 \quad 1$ und $x_4 \qquad x_r \ {}_1 \quad 0$. Wegen $u_i \quad {}_2$ ist $u_i \quad 1 \bmod 2$. Insbesondere ist $u_1 \quad u_2 \quad 0 \bmod 2$ und daher $x_r : \quad u_1 \quad u_2 \quad 2 \quad {}_2$. Schließlich setzen wir noch $x_3 : \quad x_r \quad u_rx_r^2 \quad {}_2$. Da $x_r \quad x_r^2 \bmod 2$, gilt sogar $x_3 \quad 2 \quad {}_2$. Wir rechnen

$$\begin{aligned} Q \ \tilde{x}_1 \ x_2 \qquad x_r \quad & u_1\tilde{x}_1^2 \quad u_2x_2^2 \quad u_3x_3^2 \quad 2u_rx_r^2 \\ & u_1 \quad u_2 \quad u_3x_3^2 \quad 2u_rx_r^2 \\ & 2x_r \quad 2u_rx_r^2 \quad u_3x_3^2 \\ & 2x_3 \quad u_3x_3^2 \quad x_3 \ 2 \quad u_3x_3 \end{aligned}$$

Wir behaupten, dass dieser Term Null modulo 8 ist. Wir wissen bereits, dass $x_3 \quad 2 \quad _2$ ist. Sollte sogar $x_3 \quad 4 \quad _2$ gelten, ist $x_3 \ 2 \quad u_3x_3 \quad 0 \bmod 8$ offensichtlich. Falls $x_3 \quad 2 \quad _2 \quad 4 \quad _2$ gilt, dann ist $x_3 \quad 2 \quad 4x_3'$ mit $x_3' \quad _2$ und somit

$$x_3 \ 2 \quad u_3x_3 \quad 2 \quad 4x_3' \ 2 \quad u_3 \ 2 \quad 4x_3' \quad 4 \quad 4u_3 \quad 0 \mod 8$$

da $u_3 \quad 1 \bmod 2$.

Im zweiten Fall ist $s \quad 5$. Da die Isotropie von Q nur von den Quadratrestklassen der u_i abhängt, dürfen wir $u_i \quad \{ \ 1 \quad 5$ annehmen, d.h. $u_i \quad 1 \bmod 4$. Wir finden daher $\tilde{x}_1 \ x_2 \ x_3 \ x_4 \quad \{0 \ 1$, nicht alle gleich 0, so dass

$$u_1\tilde{x}_1^2 \quad u_2x_2^2 \quad u_3x_3^2 \quad u_4x_4^2 \quad 0 \mod 4$$

Nach Umnummerierung können wir $\tilde{x}_1 \quad 1$ voraussetzen. Wir setzen

$$b : \quad u_1\tilde{x}_1^2 \quad u_2x_2^2 \quad u_3x_3^2 \quad u_4x_4^2 \quad 4 \quad _2 \qquad \text{und} \qquad x_5 : \quad 2b$$

Dann gilt

$$u_1\tilde{x}_1^2 \quad u_2x_2^2 \qquad u_5x_5^2 \quad 4b \quad u_54b^2 \quad 4b\ 1 \quad u_5b \quad \mod 8$$

Dieser Term ist wieder 0, weil für $b \quad 1 \mod 2$ der Term $1 \quad u_5b \quad 0 \mod 2$ ist.

Wir haben daher in beiden Fällen eine nicht–triviale Nullstelle $\tilde{x}_1\ x_2 \qquad x_r$ von Q modulo 8 mit $\tilde{x}_1 \quad 1$ gefunden. Wenn wir

$$c: \quad \frac{1}{u_1} \quad \sum_{i\ 2}^{r} a_i x_i^2$$

setzen, gilt $c \quad \tilde{x}_1^2 \quad 1 \mod 8$. Wir können daher nach Satz 14.5 die Wurzel von c in $\mathbb{Q}_2$ ziehen, nennen wir sie x_1. Dann gilt schließlich $0 \quad \sum_{i\ 1}^{r} a_i x_i^2 \quad Q\ x_1 \qquad x_r$.

Korollar 15.7 *Jede quadratische Form vom Rang* 4 *über* $\mathbb{Q}_p$, $p \qquad$, *stellt jedes Element von* $\mathbb{Q}_p$ *dar.*

Beweis: Sei $Q \quad \sum_{i\ 1}^{4} a_i X_i^2$ die quadratische Form und $b \quad \mathbb{Q}_p$. Dann hat die quadratische Form $Q \quad bX_5^2$ Rang 5 und ist damit isotrop. Nach Lemma 15.4 finden wir auch eine Nullstelle $x_1 \qquad x_5$ mit $x_5 \quad 0$, somit ist

$$Q\ x_1\ x_5\ x_2\ x_5\ x_3\ x_5\ x_4\ x_5 \qquad b$$

Satz 15.8 (Hasse–Minkowski) *Eine quadratische Form über* $\mathbb{Q}$ *ist genau dann isotrop über* $\mathbb{Q}$, *wenn sie isotrop über* $\quad$ *und allen* $\mathbb{Q}_p$, $p \qquad$, *ist.*

Beweis: Falls die quadratische Form über $\mathbb{Q}$ eine nicht–triviale Nullstelle besitzt, dann ist diese Nullstelle auch eine Nullstelle in allen anderen Körpern, weil $\mathbb{Q} \qquad \mathbb{Q}_p$. Starten wir also mit einer quadratischen Form Q, die isotrop über $\quad$ und allen $\mathbb{Q}_p$ ist. Wir können wieder ohne Einschränkung annehmen, dass Q von der Form

$$Q \quad a_1X_1^2 \quad a_2X_2^2 \qquad a_rX_r^2 \quad \text{mit } a_i \quad 0$$

ist. Der Fall $r \quad 1$ ist trivial, da $a_1X_1^2$ über keinem der Körper $\mathbb{Q}\ \mathbb{Q}_p \qquad$ eine Nullstelle hat. Die Fälle $r \quad 2$ und $r \quad 3$ sind die Sätze 14.7 und 14.18. Wir werden daher $r \quad 4$ annehmen.

Da Q über $\quad$ eine nicht–triviale Nullstelle besitzt, können die a_i nicht alle das gleiche Vorzeichen haben. Durch Umnummerierung können wir erreichen, dass $a_1 \quad 0$ und $a_3 \quad 0$ ist. Der Grundgedanke des Beweises ist, die quadratische Form Q in zwei Teile zu teilen, auf die dann der Satz per Induktion nach r angewendet werden kann. Sei daher

$$f: \quad a_1X_1^2 \quad a_2X_2^2 \quad \text{und} \quad g: \qquad a_3X_3^2 \quad a_4X_4^2 \qquad a_rX_r^2$$

Unser Ziel ist ein $b \quad \mathbb{Q}$ und $0 \qquad x_1 \qquad x_r \quad \mathbb{Q}^r$ zu finden mit

$$b \quad f\ x_1\ x_2 \quad g\ x_3 \qquad x_r$$

weil wir dann wegen $Q\ x_1 \qquad x_r \quad f\ x_1\ x_2 \quad g\ x_3 \qquad x_r \quad 0$ eine nicht–triviale Nullstelle von Q gefunden haben.

Sei P die Menge aller ungeraden Primzahlen, die Teiler eines der $a_1 \ldots a_r$ sind. Für jede Primzahl $p \in P \cup \{2\}$ finden wir eine nicht–triviale Nullstelle $0 \neq y_1 \ldots y_r \in \mathbb{Q}_p^r$ von Q, d.h.

$$b_p : = f(y_1, y_2) + a_1 y_1^2 + a_2 y_2^2 = a_3 y_3^2 + \ldots + a_r y_r^2 = g(y_3, \ldots, y_r)$$

Nach Lemma 15.4 können wir $y_1 y_2 \neq 0$ und $y_3 \ldots y_r \neq 0$ annehmen. Weiter soll $b_p \neq 0$ sein. Sollte zufällig $b_p = 0$ sein, sind die quadratischen Formen f, g isotrop und stellen nach Satz 15.3 alle Elemente von $\mathbb{Q}_p$ dar, zum Beispiel auch $b_p = 1$. Schließlich wollen wir auch noch $b_p \in \mathbb{Z}_p \setminus p\mathbb{Z}_p^2$ voraussetzen. Dies ist möglich, da die Darstellbarkeit von b_p nur von seiner Quadratrestklasse in $\mathbb{Q}_p / \mathbb{Q}_p^2$ abhängt.

Nach dem chinesischen Restsatz 4.11 besitzen die simultanen Kongruenzen

$$x \equiv b_2 \bmod 16 \quad \text{und} \quad x \equiv b_p \bmod p^2 \text{ für } p \in P$$

eine eindeutige Lösung b modulo $m : = 16 \prod_{p \in P} p^2$. Wir wählen $b \neq 0$.

Betrachten wir nun die quadratischen Formen

$$F = bY^2 - f \quad \text{und} \quad G = bY^2 - g$$

Wir wollen zeigen, dass diese Formen isotrop sind. Dann können wir nämlich nach Lemma 15.4 Nullstellen $y \neq x_1 \ldots x_2$ und $z \neq x_3 \ldots x_r$ von F und G finden mit $y \neq z$. Es gilt dann wie gefordert $b = f(x_1, x_2) + g(x_3, \ldots, x_r)$, und der Satz ist bewiesen. Um diese Nullstellen von F und G über $\mathbb{Q}$ zu finden, können wir Induktion benutzen, da F und G kleineren Rang als Q haben. Wir müssen daher nur zeigen, dass F und G isotrop über $\mathbb{R}$ und $\mathbb{Q}_p$, $p \in P$, sind.

Über $\mathbb{R}$ ist das klar, weil $b \neq 0$ und $a_1 \ldots a_3 \neq 0$. Für die Körper $\mathbb{Q}_p$, $p \in P \cup \{2\}$, folgt das aus der Wahl von b: Nach den Konstruktionsbedingungen und $b_p \in \mathbb{Z}_p \setminus p\mathbb{Z}_p^2$ gilt nämlich

$$b_2 b^{-1} \equiv 1 \bmod 8 \quad \text{und} \quad b_p b^{-1} \equiv 1 \bmod p \text{ für } p \in P$$

Nach den Sätzen 14.5 und 14.4 sind die $b_p b^{-1} \in \mathbb{Q}_p$ Quadrate, also mit der ursprünglichen Nullstelle $y_1 \ldots y_r$ von Q über $\mathbb{Q}_p$ gilt

$$b \sqrt{b_p b^{-1}}^2 = f(y_1, y_2) = b_p = f(y_1, y_2) = 0$$
$$b \sqrt{b_p b^{-1}}^2 = g(y_3, \ldots, y_r) = b_p = g(y_3, \ldots, y_r) = 0$$

d.h. F und G sind isotrop über $\mathbb{Q}_p$ für $p \in P \cup \{2\}$.

Es bleibt, die Körper $\mathbb{Q}_p$ für die Primzahlen $p \in P \cup \{2\}$ zu betrachten. Teilt eine solche Primzahl p die Zahl b nicht, dann sind F und G nach Lemma 15.5 isotrop. Für $r \geq 5$ ist der Rang von g gleich oder größer als 3, und wir können das Lemma 15.5 auf g anwenden, somit ist g — und damit auch G — isotrop.

Der verbleibende Problemfall sind Primzahlen $p \in P \cup \{2\}$ mit $p \mid b$ für die Form F. (Im Fall $r \geq 4$ wird die Form G analog behandelt.) Die Idee ist nun, die Zahl b, die nur eindeutig modulo m ist, so geschickt zu wählen, dass nur eine Problemprimzahl q übrig bleibt und diese mit dem Lokal–Global–Prinzip abzuhandeln.

Sei $d : = \text{ggT}(b, m)$, dann sind b/d und m/d teilerfremd. Nach dem Primzahlsatz 1.3 von Dirichlet gibt es ein $k \in \mathbb{N}$, so dass $b/d + k \cdot m/d : = q$ eine Primzahl ist. Somit ist $dq = b + km$,

und wir dürfen annehmen, dass wir dieses dq schon ursprünglich für b gewählt haben. Es gibt also nur einen Primteiler, nämlich q, der b teilt, aber nicht in P $\{2$ liegt. Nun wissen wir, dass F b Y^2 $\frac{a_1}{b}X_1^2$ $\frac{a_2}{b}X_2^2$ isotrop über allen Körpern und $\mathbb{Q}_p$, p $\{q$, ist, und damit auch über $\mathbb{Q}_q$ nach Korollar 14.16.

Zusammenfassend haben wir gesehen, dass F und G isotrop über allen $\mathbb{Q}_p$ und sind, und somit auch über $\mathbb{Q}$. Nach den bereits gemachten Bemerkungen schließt das den Beweis ab.

Korollar 15.9 *Eine quadratische Form über $\mathbb{Q}$ vom Rang größer oder gleich 5 ist isotrop über $\mathbb{Q}$ genau dann, wenn sie isotrop über ist.*

Beweis: Das folgt unmittelbar aus Satz 15.6.

Warnung Für Formen vom höheren Grad gilt kein analoger Satz zum Satz von Hasse–Minkowski.

Aufgabe 15.10 (Selmer) Zeigen Sie: Das Polynom $3X^3$ $4Y^3$ $5Z^3$ hat eine nicht–triviale Nullstelle in und in allen $\mathbb{Q}_p$. Es hat jedoch keine nicht–triviale Nullstelle in $\mathbb{Q}$, dies ist aber viel schwieriger zu beweisen. Eine zum Satz von Hasse–Minkowski analoge Aussage gilt daher nicht für kubische Polynome.

Wir wollen nun mit dem Satz von Hasse–Minkowski den Drei–Quadrate–Satz 9.4 beweisen. Wir müssen zeigen, dass die quadratische Form Q X_1^2 X_2^2 X_3^2 über alle natürlichen Zahlen — außer denen von der Form 4^i 7 $8k$ — darstellt.

Überlegen wir zuerst, welche Zahlen Q über den Körpern , $\mathbb{Q}_p$ und $\mathbb{Q}$ darstellt. Offensichtlich stellt Q über alle positiven Zahlen dar. Für die $\mathbb{Q}_p$, p $\{2$, ist die Form nach Lemma 15.5 isotrop und stellt somit jedes Element von $\mathbb{Q}_p$ dar. Für $\mathbb{Q}_2$ ist die Situation komplizierter.

Hilfssatz 15.11 *Ein Element b $\mathbb{Q}_2$ wird genau dann von Q X_1^2 X_2^2 X_3^2 dargestellt, wenn $b\mathbb{Q}_2{}^2$ $7\mathbb{Q}_2{}^2$ in $\mathbb{Q}_2$ $\mathbb{Q}_2{}^2$ ist.*

Beweis: Ob b darstellbar ist, hängt nur von seiner Quadratrestklasse in $\mathbb{Q}_2$ $\mathbb{Q}_2{}^2$ ab. Wir können uns also nach dem Satz 14.5 auf b $u2^n$ mit u $\{1\ 3\ 5\ 7$ und n $\{0\ 1$ beschränken. Wir sehen sofort

$$\begin{array}{cccc} 1 & 1^2 & 0^2 & 0^2 \\ 3 & 1^2 & 1^2 & 1^2 \\ 5 & 2^2 & 1^2 & 0^2 \end{array} \qquad \begin{array}{cccc} 2 & 1^2 & 1^2 & 0^2 \\ 6 & 2^2 & 1^2 & 1^2 \\ 10 & 3^2 & 1^2 & 0^2 \\ 14 & 3^2 & 2^2 & 1^2 \end{array}$$

Wir müssen noch zeigen, dass 7 nicht darstellbar ist. Angenommen, es gelte x_1^2 x_2^2 x_3^2 7 in $\mathbb{Q}_2$. Sei 4^i, i $_0$, der Hauptnenner der x_1^2 x_2^2 x_3^2. Multiplikation der vorherigen Gleichung mit diesem führt zu einer Gleichung

$$z_1^2 \quad z_2^2 \quad z_3^2 \quad 7 \quad 4^i \quad \text{mit } z_1\ z_2\ z_3 \quad {}_2$$

Nach den Eigenschaften des Hauptnenners muss mindestens eines der $z_1^2\ z_2^2\ z_3^2\ 7\ 4^i$ in $_2$ liegen. Tatsächlich müssen mindestens zwei davon in $_2$ liegen, denn, wenn wir die Gleichung modulo 2 betrachten, muss es eine gerade Anzahl von Termen geben, die gleich 1 modulo 2 sind. Insbesondere liegt eins der $z_1^2\ z_2^2\ z_3^2$ in $_2$, sagen wir ohne Einschränkung z_1^2. Schauen wir uns nun die Gleichung modulo 8 an, also

$$z_1^2 \quad z_2^2 \quad z_3^2 \quad 7\ 4^i \quad \text{mod } 8$$

wobei $7\ 4^i$ modulo 8 gleich 7, 4 oder 0 ist. Die Quadrate modulo 8 sind nur $1^{\ 2}\quad 1$, $2^{\ 2}\quad 4$, $3^{\ 2}\quad 1$, $4^2\quad 0$. Insbesondere ist daher $z_1^2\quad 1 \bmod 8$. Nun ist es aber offensichtlich, dass

$$1 \quad z_2^2 \quad z_3^2 \quad \{0\ 4\ 7 \quad \text{modulo } 8$$

mit $z_2^2\ z_3^2 \quad \{0\ 1\ 4$ keine Nullstelle hat.

Mit dem Satz von Hasse–Minkowski können wir nun den Körper $\mathbb{Q}$ behandeln.

Lemma 15.12 *Eine Zahl $b \quad \mathbb{Q}$ ist genau dann durch die quadratische Form $Q \quad X_1^2 \quad X_2^2 \quad X_3^2$ darstellbar, wenn $b \quad 0$ und $b\mathbb{Q}_2^{\ 2} \quad 7\mathbb{Q}_2^{\ 2}$ in $\mathbb{Q}_2 \quad \mathbb{Q}_2^{\ 2}$ gilt.*

Beweis: $b \quad K$ kann genau dann von Q über K dargestellt werden, wenn die quadratische Form $Q \quad bY^2$ isotrop über K ist, denn nach Lemma 15.4 können wir für eine Nullstelle $0 \quad x_1\ x_2\ x_3\ y \quad K^4$ dieser quadratischen Form ohne Einschränkung $y \quad 1$ annehmen. Jetzt folgt das Lemma aus dem Satz von Hasse–Minkowski und den vorangegangenen Untersuchungen von Q über den Körpern $\quad$ und $\mathbb{Q}_p$.

Nun müssen wir von der Darstellbarkeit über den rationalen Zahlen zu der Darstellbarkeit über den ganzen Zahlen kommen. Dies geht in unserem Fall mit dem folgenden Lemma:

Lemma 15.13 (Davenport–Cassels) *Sei $B\ X\ Y \quad \sum_{i\ j\ \ 1}^{r} a_{ij}X_iY_j$ eine positiv definite symmetrische Bilinearform über $\quad$. Die zugehörige quadratische Form $Q\ X \quad B\ X\ X$ besitze die folgende Eigenschaft:*

Für jedes $x \quad \mathbb{Q}^r$ existiert ein $y \quad ^r$ mit $Q\ x \quad y \quad 1$.

Dann stellt Q jedes Element $b \quad$, das über $\mathbb{Q}$ darstellbar ist, auch über $\quad$ dar.

Beweis: Sei $x \quad x_i \quad \mathbb{Q}^r \quad \{0$ mit $Q\ x \quad b$ und $k \quad$ der Hauptnenner der x_i. Wir benutzen die Beweismethode des Abstiegs nach k. Falls $k \quad 1$ ist, sind wir fertig. Andernfalls versuchen wir ein x' zu finden, so dass der Hauptnenner der Komponenten von x' kleiner als k ist.

Nach Voraussetzung existiert ein $y \quad ^r$ mit $Q\ x \quad y \quad 1$. Sei $z : \quad x \quad y \quad \mathbb{Q}^r \quad ^r$. Da B positiv definit ist, gilt $0 \quad Q\ z \quad 1$. Wir setzen

$$n \quad Q\ y \quad b \qquad m \quad 2k\ b \quad B\ x\ y \quad 2kb \quad 2B\ kx\ y$$

$$k' \quad nk \quad m \qquad x' \quad \frac{nkx \quad my}{k'} \text{ wobei } nkx \quad my \quad ^r$$

Wir werden gleich zeigen, dass $k' \neq 0$ und x' damit definiert ist. Zunächst bemerken wir aber, dass $Q(x') \neq b$ gilt, weil

$$\begin{aligned} Q(x') &= B(x', x')\, n^2 k^2 Q(x) + 2knmB(x, y) + m^2 Q(y) = k'^2 \\ n^2 k^2 b &+ 2knm\, b\, \frac{m}{2k} + m^2 n\, b = k'^2 \\ n^2 k^2 b &+ 2knmb + m^2 b = k'^2 \\ b\,(nk + m)^2 &= k'^2 \neq b \end{aligned}$$

Wegen $nkx + my \in r$ ist der Hauptnenner von x' ein Teiler von k'. Zur Vervollständigung des Arguments reicht es daher zu zeigen, dass $0 < k' < k$ gilt. Dies ergibt sich aus

$$\begin{aligned} k' &< k \Leftrightarrow nk + m < k \Leftrightarrow Q(y) + b < 2b \Leftrightarrow B(x, y) + b < 2B(x, y) + Q(y) \\ &\Leftrightarrow Q(x) < 2B(x, y) + Q(y) \Leftrightarrow Q(x) + y < Q(z) \Leftrightarrow 0 < 1 \end{aligned}$$

Beweis (Drei–Quadrate–Satz): Nach Lemma 15.12 ist eine natürliche Zahl n durch $Q = X_1^2 + X_2^2 + X_3^2$ über $\mathbb{Q}$ darstellbar, falls $n \in \mathbb{Q}_2^{\times 2}$ oder $7\mathbb{Q}_2^{\times 2}$ in $\mathbb{Q}_2 / \mathbb{Q}_2^{\times 2}$ gilt. Diese Bedingung ist nach Satz 14.5 äquivalent zu $n = 4^i(7 + 8k)$ für alle $i, k \in \mathbb{N}_0$.

Es bleibt zu überprüfen, dass $B(X, Y) = X_1Y_1 + X_2Y_2 + X_3Y_3$ die Voraussetzungen des vorangegangenen Lemmas erfüllt. Dies ist aber klar: Zu gegebenen $x_1, x_2, x_3 \in \mathbb{Q}^3$ wählen wir $y = (y_i) \in \mathbb{Q}^3$ mit $x_i = y_i + 1/2$, dann gilt

$$Q(x - y) = (x_1 - y_1)^2 + (x_2 - y_2)^2 + (x_3 - y_3)^2 = 3 \cdot \tfrac{1}{4} < 1$$

Den Vier–Quadrate–Satz kann man nicht direkt aus Satz 15.6 mit dem Davenport–Cassels–Lemma beweisen, weil hier die analoge Abschätzung nicht gilt, aber wir können den Vier–Quadrate–Satz unmittelbar aus dem Drei–Quadrate–Satz folgern.

Beweis (Vier–Quadrate–Satz): Wir schreiben $n = 4^i m$ mit $i \in \mathbb{N}_0$, $m \in \mathbb{N}$ und $4 \nmid m$. Falls $m \equiv 7 \bmod 8$ ist, sind m und damit n die Summe dreier Quadrate. Ansonsten ist $m - 1$ die Summe dreier Quadrate und somit $m = 1^2 + (m - 1)$ sowie n die Summe vierer Quadrate.

Zusatzaufgaben

Aufgabe 15.14 Geben Sie eine Beschreibung aller rationalen Zahlen, die sich durch die Form $2x^2 + 5y^2$ darstellen lassen.

Aufgabe 15.15 (Legendre) Seien a, b, c paarweise teilerfremde, quadratfreie ganze Zahlen, die nicht alle positiv oder alle negativ sind. Dann ist die Gleichung $aX^2 + bY^2 + cZ^2 = 0$ in $\mathbb{Q}$ nicht–trivial lösbar genau dann, wenn die Kongruenzen $u^2 \equiv -bc \bmod a$, $v^2 \equiv -ac \bmod b$ und $w^2 \equiv -ab \bmod c$ lösbar sind.

Aufgabe 15.16 Untersuchen Sie die Isotropie der quadratischen Formen vom Rang 4 über $\mathbb{Q}_p$, $p \in \{2, \ldots$

16 Zahlkörper

Zahlkörper sind der Hauptgegenstand für Überlegungen in der algebraischen Zahlentheorie.

Definition 16.1 *Ein* Zahlkörper *K ist ein Zwischenkörper $\mathbb{Q}$ K , so dass die Dimension von K als $\mathbb{Q}$–Vektorraum endlich ist. Die Zahlkörper K $\mathbb{Q}\sqrt{d}$ $\mathbb{Q}$ $\mathbb{Q}\sqrt{d}$ für ein d , d kein Quadrat, werden* quadratische Zahlkörper *genannt.*

Aufgabe 16.2 Zeigen Sie, dass die quadratischen Zahlkörper genau die Zahlkörper sind, deren Dimension als $\mathbb{Q}$–Vektorraum zwei ist.

Zu jedem Zahlkörper K gehört sein Ring der ganzen Zahlen $\mathcal{O}_K$, der der eigentliche Gegenstand bei der Untersuchung von Zahlkörpern ist. Bevor wir diesen definieren, wollen wir an einem Beispiel zeigen, wie die zu entwickelnde Theorie zur Lösung von diophantischen Gleichungen benutzt werden kann. In diesem Beispiel ist der benutzte Zahlkörper K $\mathbb{Q}\sqrt{2}$. Sein Ring der ganzen Zahlen ist $\mathcal{O}_K$ $\sqrt{2}$, von dem wir bereits in Aufgabe 2.7 gezeigt haben, dass er euklidisch ist.

Satz 16.3 (Fermat) *Die einzigen ganzzahligen Lösungen der Gleichung*

$$x^2 \quad 2 \quad y^3$$

sind x y 5 3 .

Beweis: Angenommen wir haben eine ganzzahlige Lösung x y der Gleichung, dann faktorisieren wir diese Gleichung in $\sqrt{2}$ folgendermaßen

$$x \quad \sqrt{2} \; x \quad \sqrt{2} \quad y^3$$

Wir behaupten, dass x $\sqrt{2}$ und x $\sqrt{2}$ teilerfremd sind. Ein gemeinsamer Teiler w a $b\sqrt{2}$ $\sqrt{2}$ würde auch die Summe und Differenz von x $\sqrt{2}$ und x $\sqrt{2}$, also $2x$ und $2\sqrt{2}$, teilen. Somit teilt seine Norm N w a^2 $2b^2$ die Normen N $2x$ $4x^2$ und N $2\sqrt{2}$ 8.

Jetzt bemerken wir, dass x nicht gerade sein kann. Nämlich, für gerades x muss wegen y^3 x^2 2 auch y gerade sein. Dann wird aus x^2 2 y^3 modulo 4 die Kongruenz 2 0 mod 4, was ein Widerspruch ist.

Folglich ist ggT $4x^2$ 8 4 und N w a^2 $2b^2$ teilt somit 4. Für a b ergeben sich daraus die Möglichkeiten 1 0 , 2 0 und 0 1 . Entsprechend haben wir w { 1 2 $\sqrt{2}$. Dies sind jedoch keine echten Teiler von x $\sqrt{2}$, daher sind x $\sqrt{2}$ und x $\sqrt{2}$ teilerfremd.

S. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie,*
DOI 10.1007/978-3-8348-8263-9_16,

Nun kann in einem faktoriellen Ring wegen der Eindeutigkeit der Primfaktorzerlegung das Produkt zweier teilerfremder Zahlen nur dann eine dritte Potenz sein, wenn bereits die einzelnen Faktoren dritte Potenzen sind, d.h. also hier

$$x \quad \sqrt{2} \quad c \quad d\sqrt{2}^{\,3} \qquad \text{mit } c \; d$$

Ausrechnen führt zu

$$x \quad \sqrt{2} \quad c^3 \quad 6cd^2 \quad 3c^2d \quad 2d^3\sqrt{2}$$
$$x \quad c\,c^2 \quad 6d^2 \quad \text{und} \quad 1 \quad d\;3c^2 \quad 2d^2$$

Wir finden $c \; d \qquad 1 \; 1$ und somit $x \qquad 5$. Schließlich ergibt sich $y \quad 3$.

Das wesentliche Element des vorangehenden Beweises war, dass $\mathcal{O}_K \qquad \sqrt{2}$ ein faktorieller Ring ist. Allgemein soll der Ring der ganzen Zahlen $\mathcal{O}_K$ eines Zahlkörpers K ein Unterring von K mit möglichst guten Eigenschaften sein, so dass in etwa die gleiche Beziehung wie im Fall $\mathbb{Q}$ besteht. $\mathcal{O}_K$ soll also möglichst viele Primelemente besitzen und sein Quotientenkörper soll K sein. Bei einem quadratischen Zahlkörper denkt man wohl zuerst daran, einfach immer $\mathcal{O}_K \qquad \sqrt{d}$ zu setzen; dies war schließlich bei $d \qquad 2$ erfolgreich. Wir haben jedoch bereits in Aufgabe 2.27 gezeigt, dass $\sqrt{7}$ kein faktorieller Ring ist, aber der minimal größere Ring $1 \quad \sqrt{7} \quad 2$ faktoriell ist. Dieser wäre also wesentlich nützlicher. Die richtige Definition ist die folgende:

Definition 16.4 *Seien $R \quad S$ zwei Ringe.*

Ein Element $x \quad S$ heißt ganz *über R, falls es eine Nullstelle eines normierten Polynoms über R ist, d.h.*

$$x^n \quad r_{n\ 1}x^{n\ 1} \qquad r_0 \quad 0 \qquad \text{für } n \qquad r_i \quad R \text{ geeignet.}$$

Der Ring S heißt ganz *über R, wenn jedes seiner Elemente ganz über R ist.*

Die Menge aller ganzen Elemente über R heißt der ganze Abschluss $\overline{R}$ *von R in S.*

Ein Integritätsring heißt ganz–abgeschlossen*, wenn er gleich seinem ganzen Abschluss in seinem Quotientenkörper ist.*

Der Ring der ganzen Zahlen $\mathcal{O}_K$ *eines Zahlkörpers K ist der ganze Abschluss von in K.*

Natürlich ist jedes Element $x \quad R$ ganz über R, weil es die Gleichung $x \quad r_0 \quad 0$ mit $r_0 \qquad x \; R$ erfüllt.

Damit die Bezeichnung von $\mathcal{O}_K$ als Ring gerechtfertigt ist, wollen wir zeigen, dass der ganze Abschluss eines Ringes wirklich ein Ring ist. Dafür benötigen wir jedoch noch eine andere Beschreibung für die Ganzheit eines Elementes.

Satz 16.5 *Seien $R \quad S$ zwei Ringe. Für ein Element $x \quad S$ sind äquivalent:*

1. *Das Element x ist ganz über R.*

2. *Der Ring*

$$R\,x\,:\quad \sum_{j\ 0}^{m}\lambda_j x^j\ \ m\qquad \lambda_j\quad R\qquad S$$

ist als R–Modul endlich erzeugt.

3. *Das Element x ist in einem Unterring T S enthalten, der als R–Modul endlich erzeugt ist.*

Beweis: Falls x ganz mit Ganzheitsgleichung

$$x^n\quad \sum_{i\ 0}^{n\ \ 1} r_i x^j\quad 0$$

ist, ist der R–Modul $R\,x$ von $1\ \ x\qquad x^{n\ \ 1}$ erzeugt. Denn in einer Summe $\sum\lambda_j x^j$ können wir die Potenzen mit einem Exponenten größer gleich n mit Hilfe der Gleichung

$$x^n\qquad \sum_{i\ 0}^{n\ \ 1} r_i x^i$$

durch kleinere ersetzen. Nach genügend vielen Wiederholungen erhält man eine Summe, die nur noch Potenzen mit Exponenten kleiner als n enthält.

Für die Folgerung von 2) nach 3) reicht es, für T den Ring $R\,x$ zu wählen.

Schließlich folgern wir 1) aus 3). Seien $e_1\quad 1\ \ e_2\qquad e_n$ die Erzeuger des Ringes T als R–Modul. Dann gibt es $\lambda_{kl}\quad R$ mit

$$x\ \ e_k\quad \sum_{l\ 1}^{n}\lambda_{kl}e_l\qquad \text{für } k\quad 1\qquad n$$

Mit dem Kronecker δ–Symbol ist dies

$$\sum_{l\ 1}^{n}\delta_{kl}x\quad \lambda_{kl}\ e_l\quad 0\qquad \text{für } k\quad 1\qquad n$$

Wir bezeichen die Koeffizientenmatrix $\delta_{kl}x\quad \lambda_{kl\ \ kl}$ dieses linearen Gleichungssystems mit A. Dann gilt mit $e\qquad e_1\qquad e_n\ ^t$ und der zu A adjungierten Matrix $A\ $ nach der Cramerschen Regel

$$A\ \ e\quad 0\qquad\qquad A\quad A\ \ e\quad 0\qquad\qquad \det A\ \ e\quad 0$$

Da $e_1\quad 1$ ist, folgt $\det A\quad 0$. Die Entwicklung der Determinante von A führt zu einer Ganzheitsgleichung $x^n\qquad 0$ für x.

Insbesondere ist also mit x auch jedes Element aus $R\,x$ ganz.

Aufgabe 16.6 Benutzen Sie das Verfahren des Beweises, um zu zeigen, dass neben $\sqrt{3}$ und $\sqrt[3]{2}$ auch $\sqrt{3}\quad\sqrt[3]{2}$ ganz über ist.

Korollar 16.7 *Seien $T \quad S \quad R$ drei Ringe. Dann ist T ganz über R genau dann, wenn T über S und S über R ganz ist.*

Beweis: Falls T ganz über R ist, ist auch S ganz über R, einfach weil $S \quad T$ ist. Ebenso ist die Erweiterung $S \quad T$ ganz, weil eine Ganzheitsgleichung für ein Element $x \quad T$ über R auch eine Ganzheitsgleichung von x über $S \quad R$ ist.

Beweisen wir nun die Umkehrung. Sei $x \quad T$ und

$$x^n \quad \sum_{i \quad 0}^{n \quad 1} s_i x^i \quad 0 \qquad \text{mit } s_i \quad S$$

seine Ganzheitsgleichung über S. Weiter seien

$$s_i \ ^{m_i} \quad \sum_{j \quad 0}^{m_i \quad 1} r_{ij} \ s_i \ ^j \quad 0 \qquad \text{mit } r_{ij} \quad R$$

die Ganzheitsgleichungen der s_i über R. Wir behaupten jetzt, dass der Ring

$$R \ s_0 \qquad s_n \ _1 \ x \ : \qquad \sum_{\text{endl.}} \lambda_{l_0 \ldots l_n \ _1 k} s_0^{l_0} \quad s_n^{l_n \ 1} {}_1 x^k \ \lambda_{l_0 \ldots l_n \ _1 k} \quad R$$

als R–Modul endlich erzeugt ist. Damit ist dann x ganz über R.

Tatsächlich ist $R \ s_0 \qquad s_n \ _1 \ x$ von den Elementen

$$s_0^{l_0} \quad s_n^{l_n \ 1} {}_1 x^k \qquad \text{mit } 0 \quad l_i \quad m_i \quad 0 \quad k \quad n$$

erzeugt. Das zeigen wir mit dem gleichen Argument wie im Beweis des Satzes. Wenn wir eine Summe

$$\sum_{\text{endl.}} \lambda_{l_0 \ldots l_n \ _1 k} s_0^{l_0} \quad s_n^{l_n \ 1} {}_1 x^k$$

haben, können wir unter Ausnutzung der Gleichung

$$x^n \qquad \sum_{i \quad 0}^{n \quad 1} s_i x^i$$

die Potenzen von x mit Exponenten größer gleich n durch kleinere Potenzen ersetzen. Nach genügend vielen Wiederholungen sind schließlich nur noch Potenzen von x mit Exponenten kleiner als n übrig. Danach machen wir dasselbe mit den Potenzen der s_i mit Hilfe der Gleichungen

$$s_i \ ^{m_i} \qquad \sum_{j \quad 0}^{m_i \quad 1} r_{ij} \ s_i \ ^j$$

Am Ende erhalten wir eine R–Linearkombination mit den oben beschriebenen Erzeugern.

Korollar 16.8 *Seien $R \quad S$ zwei Ringe. Dann ist der ganze Abschluss $\overline{R}$ von R in S ein Ring.*

Beweis: Wir müssen zeigen: Wenn $x\ y \quad \overline{R}$, dann liegen auch $x \quad y$ und xy in $\overline{R}$. Da x ganz über R ist, ist $R\ x$ ganz über R. Weil y ganz über R — und damit auch über $R\ x$ — ist, ist $R\ x\ y \quad R\ x\ y$ dann ganz über $R\ x$. Nach dem vorangehenden Korollar ist $R\ x\ y$ ganz über R, insbesondere sind seine Elemente $x \quad y$ und xy ganz über R.

Korollar 16.9 *Seien $R \quad S$ zwei Ringe und $\overline{R}$ der ganze Abschluss von R in S. Dann ist der ganze Abschluss von $\overline{R}$ in S wieder $\overline{R}$.*

Beweis: Sei $\overline{\overline{R}}$ der ganze Abschluss von $\overline{R}$ in S. Nach Korollar 16.7 ist $\overline{\overline{R}}$ ganz über R. Dann sind die Elemente von $\overline{\overline{R}}$ ganz über R und per Definition in $\overline{R}$ enthalten.

Angewandt auf die Situation bei den Zahlkörpern ergibt sich:

Satz 16.10 *Sei K ein Zahlkörper. Dann ist K der Quotientenkörper des Ringes $\mathcal{O}_K$ der ganzen Zahlen von K. Der Ring $\mathcal{O}_K$ ist ganz–abgeschlossen. Weiter gibt es für jedes Element $x \quad K$ eine natürliche Zahl k, so dass kx ganz über $\quad$ ist.*

Beweis: Wir zeigen zunächst die letzte Aussage. Sei $0 \quad x \quad K$ beliebig. Setzen wir n dim K. Dann sind die $n \quad 1$ Elemente

$$x^n \ x^{n \ 1} \qquad x^2 \ x \ 1$$

linear abhängig über $\mathbb{Q}$. Es gibt daher ein $m \qquad$ und $\lambda_i \quad \mathbb{Q}$ mit

$$x^m \quad \sum_{i \ 0}^{m \ 1} \lambda_i x^i \quad 0$$

Sei k der Hauptnenner der λ_i. Multiplikation der obigen Gleichung mit k^m ergibt

$$kx^{\ m} \quad \sum_{i \ 0}^{m \ 1} k^{m \ i} \lambda_i \quad kx^{\ i} \quad 0$$

Wegen $k^{m \ i} \lambda_i \qquad$ ist dies eine Ganzheitsgleichung von kx über $\quad$. Insbesondere liegt kx in $\mathcal{O}_K$.

Wir können also jedes $x \quad K$ schreiben als $x \qquad kx \quad k$ mit $kx \quad \mathcal{O}_K$ und $k \qquad \mathcal{O}_K$. Also liegt K im Quotientenkörper von $\mathcal{O}_K$. Da K bereits ein Körper ist, muss der Quotientenkörper von $\mathcal{O}_K$ der Zahlkörper K sein.

Nach Korollar 16.9 ist $\mathcal{O}_K$ ganz–abgeschlossen.

Dass sich die teilbarkeitstheoretischen Eigenschaften eines Ringes durch Abschluss verbessern, deutet der folgende Satz an:

Satz 16.11 *Jeder faktorielle Ring ist ganz–abgeschlossen.*

Beweis: Wir bezeichnen den Ring wieder mit R. Sei x ein ganzes Element des Quotientenkörpers. Wir schreiben $x = a\ b$ mit teilerfremden $a\ b \in R$. Für $a\ b$ haben wir eine Ganzheitsgleichung

$$\frac{a}{b}^{n} \quad r_{n-1}\frac{a}{b}^{n-1} \quad r_1\frac{a}{b} \quad r_0 = 0$$

Multiplikation mit b^n führt zu

$$a^n + r_{n-1}ba^{n-1} + r_1b^{n-1}a + r_0b^n = 0$$

$$a^n = b\,(-r_{n-1}a^{n-1} - r_1b^{n-2}a - r_0b^{n-1})$$

Wegen ggT$(a\ b) = 1$ muss b eine Einheit in R sein, also ist $a\ b \in R$. Folglich ist R abgeschlossen in seinem Quotientenkörper.

Im Allgemeinen ist es nicht einfach zu entscheiden, ob ein Element ganz ist. Im Fall von Zahlkörpern gibt es jedoch eine einfache Möglichkeit. Wir erinnern uns daran, dass das Minimalpolynom über $\mathbb{Q}$ eines Elementes $x \in K$ das normierte Polynom kleinsten Grades ist, welches x als Nullstelle hat. Man kann es leicht durch Betrachten der linearen Abhängigkeiten unter den Potenzen von x finden.

Aufgabe 16.12 Zeigen Sie: Das Minimalpolynom von x ist der eindeutig bestimmte normierte Erzeuger des Ideals

$$I = \{f \in \mathbb{Q}X \mid f(x) = 0\}$$

Satz 16.13 *Ein Element eines Zahlkörpers ist genau dann ganz über , wenn die Koeffizienten seines Minimalpolynoms in liegen.*

Beweis: Für die nicht–triviale Richtung sei $f \in X$ das normierte Polynom aus der Ganzheitsbedingung für x. Nach der vorangegangenen Aufgabe liegt f in dem vom Minimalpolynom m erzeugten Ideal. Es gibt also ein notwendigerweise normiertes Polynom $g \in \mathbb{Q}X$ mit $f = mg$. Der Satz von Gauß [Wü, Satz 12.17] besagt nun, dass wegen $f \in X$ auch $g\ m$ in X liegen.

Für den Spezialfall der quadratischen Zahlkörper kann man das Minimalpolynom direkt angeben. Wir bezeichen mit σ den Körperautomorphismus

$$\sigma : \mathbb{Q}\sqrt{d} \to \mathbb{Q}\sqrt{d} \qquad a + b\sqrt{d} \mapsto a - b\sqrt{d}$$

Aufgabe 16.14 Zeigen Sie: Ein quadratischer Zahlkörper $\mathbb{Q}\sqrt{d}$ hat nur zwei Einbettungen $\mathbb{Q}\sqrt{d}$ in den Körper der komplexen Zahlen, die Identität auf $\mathbb{Q}\sqrt{d}$ und σ verknüpft mit der Inklusion $\mathbb{Q}\sqrt{d}$.

Wir definieren die *Spur–* und *Norm–*Abbildung als

$$\mathrm{Sp} : \mathbb{Q}\sqrt{d} \to \mathbb{Q} \qquad x \mapsto x + \sigma x$$
$$N : \mathbb{Q}\sqrt{d} \to \mathbb{Q} \qquad x \mapsto x\,\sigma x$$

Dass die Bilder dieser Abbildungen wirklich in $\mathbb{Q}$ liegen, erkennt man aus der folgenden alternativen Darstellung dieser Abbildungen

$$\begin{array}{llllllllll} \mathrm{Sp}\ a\quad b\sqrt{d} & a\quad b\sqrt{d} & \sigma\ a\quad b\sqrt{d} & a\quad b\sqrt{d} & a\quad b\sqrt{d} & 2a \\ N\ a\quad b\sqrt{d} & a\quad b\sqrt{d} & \sigma\ a\quad b\sqrt{d} & a\quad b\sqrt{d} & a\quad b\sqrt{d} & a^2\quad db^2 \end{array}$$

Offensichtlich ist die Spur additiv und die Norm multiplikativ.

Lemma 16.15 *Sei* $x\quad \mathbb{Q}\ \sqrt{d}\quad \mathbb{Q}$. *Dann ist sein Minimalpolynom über* $\mathbb{Q}$*:*

$$X^2\quad \mathrm{Sp}\ x\ X\quad N\ x$$

Insbesondere ist x genau dann ganz, wenn $\mathrm{Sp}\ x$ *und* $N\ x$ *in liegen.*

Beweis: Das Minimalpolynom von x kann nicht linear sein, weil $x\quad \mathbb{Q}$. Da x eine Nullstelle von

$$X\quad x\ X\quad \sigma\ x\qquad X^2\quad x\quad \sigma\ x\ X\quad x\sigma\ x\quad X^2\quad \mathrm{Sp}\ x\ X\quad N\ x\quad \mathbb{Q}\ X$$

ist, muss dies bereits das Minimalpolynom sein.

Aus der Galois–Theorie ist die Verallgemeinerung dieses Satzes auf beliebige Zahlkörper bekannt. Sei K ein Zahlkörper, aber nicht notwendig galoissch, und

$$\mathrm{Hom}\ K\qquad \{\sigma : K\qquad \sigma\ \text{Körperhomomorphismus}$$

die Menge der Einbettungen von K in . Es gibt davon genau dim K Stück. Das Minimalpolynom eines Elementes $x\quad K$ kann dann berechnet werden als

$$\prod_{y\ S} X\quad y\qquad \text{mit}\ S\quad \{\sigma\ x\quad \sigma\quad \mathrm{Hom}\ K$$

Man beachte, dass diese Formel auch richtig ist, wenn der von x erzeugt Unterkörper von K nicht mit K übereinstimmt. Die *Spur* und *Norm* eines Elementes sind definiert durch

$$\mathrm{Sp}\ x\ :\quad \sum_{\sigma\ \mathrm{Hom}\ K}\quad \sigma\ x\quad \mathbb{Q}\quad \text{und}\quad N\ x\ :\quad \prod_{\sigma\ \mathrm{Hom}\ K}\quad \sigma\ x\quad \mathbb{Q}$$

Etwas allgemeiner definiert man für zwei Zahlkörper $L\quad K\quad \mathbb{Q}$ Norm und Spur eines Elementes $x\quad L$ durch

$$\mathrm{Sp}_{L/K}\ x\ :\quad \sum_{\sigma\ \mathrm{Hom}_K\ L}\quad \sigma\ x\quad K\quad \text{und}\quad N_{L/K}\ x\ :\quad \prod_{\sigma\ \mathrm{Hom}_K\ L}\quad \sigma\ x\quad K$$

wobei die Menge $\mathrm{Hom}_K\ L$ diejenigen Körperhomomorphismen $\sigma : L$ bezeichnet, die auf K die Identität sind. Es gilt $N\quad N_{K/}$ und $\mathrm{Sp}\quad \mathrm{Sp}_{K/}$.

Aufgabe 16.16 Sei $K\quad \mathbb{Q}\ \sqrt[4]{3}$. Berechnen Sie nach der oben beschriebenen Methode das Minimalpolynom, die Spur und die Norm von

$$\sqrt{3}\qquad \text{und}\qquad 3\sqrt[4]{3}\quad 2\sqrt{27}$$

Lemma 16.17 *Sei x ein ganzes Element in einem Zahlkörper K. Dann ist auch $\sigma\ x$ für jedes σ Hom K ganz. Weiter ist*

$$\text{Sp } x \qquad \textit{und} \qquad N\ x$$

Beweis: Sei

$$x^n \quad \sum_{i\ 0}^{n\ 1} r_i x^i \quad 0 \qquad \text{mit } r_i$$

eine Ganzheitsgleichung von x. Dann ergibt sich durch Anwenden eines Körperhomomorphismus σ Hom K wegen σ id

$$\sigma\ x\ ^n \quad \sum_{i\ 0}^{n\ 1} r_i\ \sigma\ x\ ^i \quad 0$$

Dies ist eine Ganzheitsgleichung für $\sigma\ x$.

Da die ganzen Zahlen einen Ring bilden, sind auch Sp x und $N\ x$ als algebraische Ausdrücke in den $\sigma\ x$ ganz über . Weil Sp x und $N\ x$ bereits in $\mathbb{Q}$ liegen, folgt aus Satz 16.11, dass sie ganzzahlig sind.

Für späteren Gebrauch beweisen wir noch das folgende Korollar.

Korollar 16.18 *Sei K ein Zahlkörper und x 0 ein Element des Ringes ganzer Zahlen von K. Dann gilt:*

$$N\ x \qquad \mathcal{O}_K x$$

Insbesondere enthält jedes nicht–triviale Ideal eine ganze Zahl ungleich Null.

Beweis: Nach Definition der Norm gilt:

$$N\ x \qquad x \qquad \prod_{\substack{\sigma \text{ Hom } K \\ \sigma \text{ id}}} \sigma\ x$$

Wegen $N\ x$ K und x K ist

$$y: \qquad \prod_{\substack{\sigma \text{ Hom } K \\ \sigma \text{ id}}} \sigma\ x \qquad \frac{N\ x}{x} \qquad K$$

Da die $\sigma\ x$ ganz über sind, ist auch y ganz, d.h. y $\mathcal{O}_K$. Somit ist $N\ x$ yx $\mathcal{O}_K x$.

Für die Zusatzaussage wählen wir in einem Ideal I 0 ein Element 0 x I, dann gilt $N\ x$ $\mathcal{O}_K x$ I.

Für nicht–quadratische Zahlkörper sind die Bedingungen Sp x $N\ x$ nicht mehr hinreichend für die Ganzheit von x.

Aufgabe 16.19 Finden Sie einen Zahlkörper K, der ein Element enthält, dessen Spur und Norm ganzzahlig ist, es selbst jedoch nicht ganz ist.

Für quadratische Zahlkörper können wir die Ringe der ganzen Zahlen allgemein bestimmen:

Satz 16.20 *Sei* $K \quad \mathbb{Q}\sqrt{d}$, d *quadratfrei, ein quadratischer Zahlkörper. Dann ist der Ring der ganzen Zahlen*

$$\mathcal{O}_K \quad \begin{cases} \sqrt{d} & \text{für } d \quad 2 \ 3 \bmod 4 \\ \frac{1 \quad \sqrt{d}}{2} & \text{für } d \quad 1 \bmod 4 \end{cases}$$

Ein beliebiges Element aus $1 \quad \sqrt{d} \quad 2$ ist von der Form

$$a \ 1 \quad b \ \frac{1 \quad \sqrt{d}}{2} \quad \frac{2a \quad b \quad b\sqrt{d}}{2} \qquad \text{mit } a \ b$$

Daher kann man die Elemente auch schreiben als

$$\frac{c \quad b\sqrt{d}}{2} \qquad \text{mit } c \ b \qquad \text{und } b \quad c \bmod 2$$

Beweis: Offensichtlich ist $\sqrt{d}$ als Nullstelle des Polynoms $X^2 \quad d \qquad X$ immer ganz. Im Fall $d \quad 1 \bmod 4$ ist auch $\omega : \quad 1 \quad \sqrt{d} \quad 2$ ganz, weil

$$\text{Sp } \omega \quad \frac{1 \quad \sqrt{d}}{2} \quad \frac{1 \quad \sqrt{d}}{2} \quad 1$$

$$N \ \omega \quad \frac{1 \quad \sqrt{d}}{2} \ \frac{1 \quad \sqrt{d}}{2} \quad \frac{1 \quad d}{4}$$

Da die ganzen Zahlen einen Ring bilden, folgt jetzt $\sqrt{d} \quad \mathcal{O}_K$ bzw. $\omega \quad \mathcal{O}_K$.

Sei nun umgekehrt $x \quad a \quad b\sqrt{d}$ mit $a \ b \quad \mathbb{Q}$ eine ganze Zahl, d.h.

$$\text{Sp } x \quad 2a \qquad \text{und} \qquad N \ x \quad a^2 \quad db^2$$

Dann ist auch $4N \ x \quad 2a \ ^2 \quad d \ 2b \ ^2$, also $d \ 2b \ ^2$. Da d quadratfrei ist, folgt $2b$. Falls a , folgt aus $a^2 \quad db^2$ wie eben db^2 und b .

Bleibt der Fall $a \quad c \ 2$ mit ungeradem c zu betrachten. Hier ist

$$N \ x \quad \frac{c^2 \quad d \ 2b \ ^2}{4} \qquad\qquad c^2 \quad d \ 2b \ ^2 \quad 0 \mod 4$$

Aus c ungerade folgt $1 \quad c^2 \quad d \ 2b \ ^2 \bmod 4$. Somit muss $2b \quad 1 \bmod 2$ sein, d.h. auch b ist von der Form $e \ 2$ mit e ungerade. Aus $2b \quad 1 \bmod 2$ erhalten wir auch $2b \ ^2 \quad 1 \bmod 4$. Einsetzen in $1 \quad d \ 2b \ ^2 \bmod 4$ zeigt, dass dies nur mit $d \quad 1 \bmod 4$ möglich ist.

Wir sehen insbesondere, dass der Ring der ganzen Zahlen eines quadratischen Zahlkörpers als abelsche Gruppe isomorph zu ^{2} ist. Ein analoger Satz gilt auch für beliebige Zahlkörper. Um dies zu beweisen, führen wir die Diskriminante ein.

Definition 16.21 *Sei* $B \quad b_1 \quad b_n$ *eine* $\mathbb{Q}$*–Basis eines Zahlkörpers* K *und*

$$\text{Hom}\ K \qquad \{\sigma_1 \quad \text{id}_K\ \sigma_2 \qquad \sigma_n$$

die Menge seiner Einbettungen in . *Dann ist die* Diskriminante *der Basis* B

$$\Delta\ B \qquad \det \begin{matrix} b_1 & \sigma_2\ b_1 & & \sigma_n\ b_1 \\ b_2 & \sigma_2\ b_2 & & \sigma_n\ b_2 \\ \vdots & & & \vdots \\ b_n & \sigma_2\ b_n & & \sigma_n\ b_n \end{matrix}^2$$

Wir berechnen zunächst die Abhängigkeit der Diskriminante von der Wahl der Basis.

Lemma 16.22 *Seien* B *und* B' *zwei* $\mathbb{Q}$*–Basen eines Zahlkörpers* K *der* $\mathbb{Q}$*–Dimension* n*. Weiter sei* $T \quad \text{GL}\ n\ \mathbb{Q}$ *die Transformationsmatrix, die die Basis* B *in die Basis* B' *überführt. Dann gilt*

$$\Delta\ B' \qquad \det T^{\,2}\ \Delta\ B$$

Beweis: Scheiben wir die Basen als $B \quad b_1 \quad b_n$ und $B' \quad b'_1 \quad b'_n$, dann gilt per Definition

$$\begin{matrix} b'_1 \\ \vdots \\ b'_n \end{matrix} \qquad T \qquad \begin{matrix} b_1 \\ \vdots \\ b_n \end{matrix}$$

Da ein $\sigma \quad \text{Hom}\ K \quad$ linear über $\mathbb{Q}$ ist, folgt

$$\begin{matrix} \sigma\ b'_1 \\ \vdots \\ \sigma\ b'_n \end{matrix} \qquad T \qquad \begin{matrix} \sigma\ b_1 \\ \vdots \\ \sigma\ b_n \end{matrix}$$

und schließlich wegen der Multiplikativität der Determinante

$$\Delta\ B' \qquad \det \quad T \qquad \begin{matrix} b_1 & \sigma_2\ b_1 & & \sigma_n\ b_1 \\ b_2 & \sigma_2\ b_2 & & \sigma_n\ b_2 \\ \vdots & & & \vdots \\ b_n & \sigma_2\ b_n & & \sigma_n\ b_n \end{matrix}^2 \qquad \det T^{\,2}\ \Delta\ B$$

Lemma 16.23 *Sei* $B \quad b_1 \quad b_n$ *eine* $\mathbb{Q}$*–Basis eines Zahlkörpers* K*. Dann gilt*

$$\Delta\ B \qquad \mathbb{Q}$$

Falls alle b_i *ganz sind, dann gilt sogar*

$$\Delta\ B \qquad \{0$$

Beweis: Für zwei $\mathbb{Q}$–Basen eines Zahlkörpers K unterscheiden sich nach Lemma 16.22 die Diskriminanten nur um einen Faktor aus $\mathbb{Q}$, daher reicht es, die erste Aussage für eine spezielle Basis des Zahlkörpers zu beweisen.

Sei wieder n die $\mathbb{Q}$–Dimension von K. Nach dem Satz vom primitiven Element [Wü, Satz 14.11] gibt es ein α K, so dass K $\mathbb{Q}$ α . Also ist B 1 α α^2 $\alpha^{n\ 1}$ eine $\mathbb{Q}$–Basis von K. Per Definition ist

$$\Delta\ B \quad \det \begin{matrix} 1 & 1 & & 1 \\ \alpha & \sigma_2\ \alpha & & \sigma_n\ \alpha \\ \alpha^2 & \sigma_2\ \alpha^{\ 2} & & \sigma_n\ \alpha^{\ 2} \\ \vdots & \vdots & & \vdots \\ \alpha^{n\ 1} & \sigma_2\ \alpha^{\ n\ 1} & & \sigma_n\ \alpha^{\ n\ 1} \end{matrix}^2$$

Dies ist das Quadrat einer *Vandermondeschen Determinante*, also

$$\Delta\ B \quad \prod_{1\ i\ j\ n} \sigma_i\ \alpha \quad \sigma_j\ \alpha^{\ 2} \quad 1^{\ \frac{n\ n\ 1}{2}} \prod_{i\ j} \sigma_i\ \alpha \quad \sigma_j\ \alpha$$

Zuerst beweisen wir $\Delta\ B$ 0, d.h., wir müssen $\sigma_i\ \alpha$ $\sigma_j\ \alpha$ für i j zeigen. Nun ist der Grad des Minimalpolynoms von α gleich der $\mathbb{Q}$–Dimension von K $\mathbb{Q}$ α , also n. Wir haben bereits vorher bemerkt, dass das Minimalpolynom von α als

$$\prod_{y\ S} X\ \ y \qquad \text{mit} \qquad \begin{matrix} S & \{\sigma\ \alpha\ \ \sigma & \text{Hom}\ K \\ & \{\sigma_1\ \alpha \quad \alpha\ \sigma_2\ \alpha & \sigma_n\ \alpha \end{matrix}$$

berechnet werden kann. Es folgt $\#S$ n. Dies zeigt, dass die $\sigma_i\ \alpha$ alle paarweise verschieden sind.

Der Ausdruck für $\Delta\ B$ ist symmetrisch in den $\sigma_i\ \alpha$, d.h. invariant unter Permutationen der $\sigma_i\ \alpha$. Dann folgt sofort aus der Galois–Theorie, dass $\Delta\ B$ im Grundkörper $\mathbb{Q}$ liegt.

Nehmen wir nun zusätzlich an, dass die b_i alle ganz sind. Nach Lemma 16.17 sind damit auch die $\sigma\ b_i$ mit σ Hom K ganz. Also sind alle Einträge der Matrix, die zur Berechnung der Diskriminante benutzt werden, ganz. Somit ist auch $\Delta\ B$, das Quadrat ihrer Determinante, als algebraischer Ausdruck in den Einträgen ganz über . Da nach Satz 16.11 ganz–abgeschlossen in $\mathbb{Q}$ ist, folgt $\Delta\ B$ $\{0$.

Mit Hilfe der Diskriminante studieren wir die Struktur von $\mathcal{O}_K$ als abelsche Gruppe.

Satz 16.24 *Sei K ein Zahlkörper und n* dim *K. Dann ist der Ring ganzer Zahlen $\mathcal{O}_K$ als abelsche Gruppe isomorph zu* ^{n}.

Beweis: Wir bemerken zuerst, dass es $\mathbb{Q}$–Basen von K gibt, deren Elemente in $\mathcal{O}_K$ liegen. Denn sei b_1 b_n eine $\mathbb{Q}$–Basis von K, dann existieren nach Satz 16.10 ganze Zahlen 0 k_i , so dass $k_i b_i$ Elemente von $\mathcal{O}_K$ sind. Natürlich ist auch $k_1 b_1$ $k_n b_n$ eine $\mathbb{Q}$–Basis von K.

Sei daher nun B b_1 b_n eine $\mathbb{Q}$–Basis von K mit b_i $\mathcal{O}_K$. Wir betrachten die von b_1 b_n erzeugte additive Untergruppe Γ von $\mathcal{O}_K$. Da die b_i über $\mathbb{Q}$ linear unabhängig sind,

sind sie es auch über , d.h. aus $\sum \lambda_i b_i$ 0 folgt λ_i 0 für alle i. Dies bedeutet, dass der per Definition surjektive Homomorphismus

$$^{n} \quad \Gamma \quad \lambda_i \quad \sum_{i\ 1}^{n} \lambda_i b_i$$

auch injektiv ist. Somit ist Γ ^{n}.

Wir betrachten jetzt unter allen Basen B b_1 b_n mit b_i $\mathcal{O}_K$ eine, deren Diskriminante vom Betrag her minimal ist. Wir behaupten, dass die von dieser Basis erzeugte Untergruppe Γ bereits ganz $\mathcal{O}_K$ ist, und somit $\mathcal{O}_K$ Γ ^{n} ist.

Angenommen, $\mathcal{O}_K$ Γ. Sei dann x $\mathcal{O}_K$ Γ. Da B über $\mathbb{Q}$ ganz K erzeugt, gibt es λ_i $\mathbb{Q}$ mit

$$x \quad \sum_{i\ 1}^{n} \lambda_i b_i$$

Wegen x Γ können nicht alle λ_i ganzzahlig sein. Sei ohne Einschränkung λ_1 . Wir setzen α : λ_1 λ_1 0 1 und betrachten die Basis

$$B' \quad x \quad \lambda_1 \ b_1 \ b_2 \ b_3 \quad b_n$$

Die Transformationsmatrix, die die Basis B in die Basis B' überführt, ist

$$T \quad \begin{matrix} \alpha & \lambda_2 & & \lambda_n \\ & 1 & & 0 \\ & & \ddots & \\ 0 & & & 1 \end{matrix}$$

Ihre Determinante ist $\det T$ α. Nach der Formel aus Lemma 16.22 gilt für die Beträge der Diskriminanten

$$\Delta\ B' \quad \alpha^2 \ \Delta\ B \quad \Delta\ B$$

im Widerspruch zur Wahl von B. Somit ist $\mathcal{O}_K$ Γ ^{n}.

Korollar 16.25 *In der Situation des Satzes ist auch jedes Ideal I* 0 *von* $\mathcal{O}_K$ *isomorph zu* ^{n}.

Beweis: Da I $\mathcal{O}_K$ ^{n} ist, gilt für jede natürliche Zahl m 2, dass für jedes x I ungleich 0 auch mx ungleich 0 ist. I kann also keine zu m isomorphe Untergruppe enthalten und muss daher nach der Klassifikation der endlich erzeugten abelschen Gruppen isomorph zu ^{k} für ein k $_0$ sein. Nun enthält I die Untergruppe $x\mathcal{O}_K$ ^{n} für ein 0 x I und ist selbst in $\mathcal{O}_K$ ^{n} enthalten, daher muss k n sein, also I ^{n}.

Somit ist die Inklusion 0 I $\mathcal{O}_K$ eine Einbettung einer zu ^{n} isomorphen Gruppe in eine zu ^{n} isomorphe Gruppe. Folglich ist $\mathcal{O}_K$ I eine endliche Gruppe.

Definition 16.26 *Sei* $\mathcal{O}_K$ *der Ring der ganzen Zahlen eines Zahlkörpers K und I* 0 *ein Ideal darin. Dann ist die* Norm $N\ I$ *des Ideal I gleich* $\#\mathcal{O}_K\ I$.

Die Norm ist eine wichtige Invariante, die jedoch in diesem Buch wenig gebraucht wird, weil wir hauptsächlich quadratische Zahlkörper betrachten. Wir begnügen uns daher mit einer Zusammenstellung ihrer Eigenschaften — teilweise ohne Beweis.

Satz 16.27 *Seien $I\ J\quad 0$ zwei Ideale in einem Ring ganzer Zahlen eines Zahlkörpers K. Dann gilt:*

1. *$N\ I\quad 1\qquad I\quad \mathcal{O}_K$.*
2. *$N\ I$ ist eine Primzahl $\qquad$ I ist ein Primideal.*
3. *Die Norm ist multiplikativ, d.h. $N\ I\ J\quad N\ I\quad N\ J$.*
4. *Falls I ein Hauptideal ist, also $I\quad x$ für ein $0\quad x\quad \mathcal{O}_K$, dann ist die Norm von I gleich dem Betrag der Körpernorm von x, d.h.*

$$N\ I\quad N\ x$$

Beweis: Wegen $N\ I\quad \#\mathcal{O}_K\ I$ ist 1) klar nach Definition. Für 2) betrachten wir den Ringhomomorphimus

$$\varphi:\qquad \mathcal{O}_K\ I$$

Mit $p:\ N\ I\quad \#\mathcal{O}_K\ I$ gilt $p\quad \operatorname{Ker}\varphi$, weil $p\quad \mathcal{O}_K\ I\quad 0$. Nun ist ein Hauptidealring, somit wird $\operatorname{Ker}\varphi$ von einem Element x erzeugt. Aus $p\quad \operatorname{Ker}\varphi$ folgt $x\ p$. Weil p nach Voraussetzung eine Primzahl ist, ergibt sich $x\quad p$ oder $x\quad 1$. Letztes ist unmöglich, da $\operatorname{Ker}\varphi$ bedeutet, dass φ die Nullabbildung ist. Somit ist $\mathcal{O}_K\ I\qquad x\qquad p$ ein Körper und I ein (maximales) Primideal.

Für 3) und 4) verweisen wir auf Satz D.2 in Anhang D

Zu ^{n} isomorphe Gruppen erhalten eine besondere Bezeichnung.

Definition 16.28 *Eine abelsche Gruppe G, die isomorph zu ^{n} für ein $n\quad 0$ ist, heißt* freie abelsche Gruppe vom Rang *n. Eine* –Basis *von G ist ein n–Tupel $B\quad b_1\qquad b_n$ mit $b_i\quad G$, so dass die $b_1\qquad b_n$ die Gruppe G erzeugen.*

Jede freie abelsche Gruppe G besitzt eine –Basis, nämlich die Bilder der Einheitsvektoren von ^{n} unter dem Isomorphismus $^n\quad G$. Seien nun zwei –Basen $B\quad b_1\qquad b_n$ und $B'\quad b'_1\qquad b'_n$ einer freien abelschen Gruppe G gegeben. Weil beide die Gruppe G erzeugen, gibt es Matrizen $T\ S\quad \mathrm{Mat}\ n\quad$ mit

$$\begin{matrix} b'_1 \\ \vdots \\ b'_n \end{matrix}\quad T\quad \begin{matrix} b_1 \\ \vdots \\ b_n \end{matrix}\qquad \text{und}\qquad \begin{matrix} b_1 \\ \vdots \\ b_n \end{matrix}\quad S\quad \begin{matrix} b'_1 \\ \vdots \\ b'_n \end{matrix}$$

Durch ineinander Einsetzen folgt $T\,S\quad ST\quad E_n$, also $T\quad S^{\ 1}\quad \mathrm{GL}\ n$. Die –Basen einer freien abelschen Gruppe werden also durch Elemente von $\mathrm{GL}\ n$ aufeinander abgebildet. Für eine Matrix $T\quad \mathrm{GL}\ n$ folgt aus $T\ T^{\ 1}\quad E_n$ die Gleichung $\det T\ \det T^{\ 1}\quad 1$. Wegen $\det T\ \det T^{\ 1}$ ist also $\det T\quad 1$. Dies können wir jetzt nutzen, um die Diskriminante des Zahlkörpers selbst, also nicht nur von einer Basis desselben, zu definieren.

Definition 16.29 *Sei $B \quad b_1 \quad b_n$ eine –Basis des Ringes der ganzen Zahlen eines Zahlkörpers K. Dann heißt*

$$\Delta_K \quad \Delta \; B$$

die Diskriminante des Zahlkörpers K.

Die Definition ist nach Lemma 16.22 unabhängig von der Wahl der Basis B.

Für die quadratischen Zahlkörper ist die Berechnung der Diskriminante einfach und führt zu einer einheitlichen Beschreibung des Ringes der ganzen Zahlen.

Lemma 16.30 *Für einen quadratischen Zahlkörper $K \quad \mathbb{Q}\sqrt{d}$, d quadratfrei, ist die Diskriminante*

$$\Delta \quad \begin{array}{ll} 4d & \text{für } d \quad 2 \; 3 \bmod 4 \\ d & \text{für } d \quad 1 \bmod 4 \end{array}$$

Beweis: Der Körper K hat neben der Identität nur σ mit $\sigma \; a \quad b\sqrt{d} \quad a \quad b\sqrt{d}$ als Einbettung in . Für $d \quad 2 \; 3 \bmod 4$ ist $1 \; \sqrt{d}$ eine Basis von $\mathcal{O}_K \quad \sqrt{d}$, und wir berechnen

$$\Delta \quad \det \begin{array}{cc} 1 & 1 \\ \sqrt{d} & \sqrt{d} \end{array}^2 \quad \sqrt{d} \quad \sqrt{d}^{\,2} \quad 4d$$

Analog ergibt sich bei $d \quad 1 \bmod 4$ mit der Basis $1 \quad 1 \quad \sqrt{d} \quad 2$ für $\mathcal{O}_K \quad 1 \quad \sqrt{d} \quad 2$

$$\Delta \quad \det \begin{array}{cc} 1 & 1 \\ \frac{1 \quad \overline{d}}{2} & \frac{1 \quad \overline{d}}{2} \end{array}^2 \quad \frac{1 \quad \sqrt{d}}{2} \quad \frac{1 \quad \sqrt{d}}{2}^{\,2} \quad d$$

Korollar 16.31 *Für einen quadratischen Zahlkörper K und seine Diskriminante Δ gilt:*

$$K \quad \mathbb{Q}\sqrt{\Delta} \qquad \textit{und} \qquad \mathcal{O}_K \quad \frac{\Delta \quad \sqrt{\Delta}}{2}$$

Beweis: Wir nutzen die Bezeichnungen wie im Lemma. Wegen $\Delta \quad \{d \; 4d$ ist $K \quad \mathbb{Q}\sqrt{d} \quad \mathbb{Q}\sqrt{\Delta}$ offensichtlich. Wir berechnen

$$\frac{\Delta \quad \sqrt{\Delta}}{2} \quad \begin{cases} \dfrac{4d \quad \sqrt{4d}}{2} \quad 2d \quad \sqrt{d} & \text{für } d \quad 2 \; 3 \bmod 4 \\ \dfrac{d \quad \sqrt{d}}{2} \qquad \dfrac{d \quad 1}{2} \quad \dfrac{1 \quad \sqrt{d}}{2} & \text{für } d \quad 1 \bmod 4 \end{cases}$$

Modulo ist dies $\sqrt{d}$ bzw. $1 \quad \sqrt{d} \quad 2$, also hat $\mathcal{O}_K$ die behauptete Form.

Zum Abschluss des Abschnittes wollen wir einen Algorithmus beschreiben, mit dem der Ring ganzer Zahlen eines beliebigen Zahlkörpers bestimmt werden kann. Sei $n \quad \dim \; K$. Die Grundidee des Algorithmus ist, dass man n linear unabhängige Elemente $b_1 \qquad b_n \quad : B$

aus $\mathcal{O}_K$ wählt, von denen man hofft, dass sie eine –Basis von $\mathcal{O}_K$ bilden. Zumindest ist die von ihnen erzeugte Untergruppe Γ eine freie abelsche Gruppe vom Rang n, so dass $\mathcal{O}_K$ Γ endlich ist. Man versucht dann ein x $\mathcal{O}_K$ Γ zu finden. Wenn es das nicht gibt, ist man fertig, sonst vergrößert man Γ mit Hilfe von x und wiederholt das Verfahren.

Wir werden die Diskriminante von B als Maß für die Größe von $\mathcal{O}_K$ Γ verwenden.

Satz 16.32 *Sei K ein Zahlkörper mit n* dim *K und $\mathcal{O}_K$ sein Ring ganzer Zahlen. Sei Γ eine freie additive Untergruppe von $\mathcal{O}_K$ mit –Basis*

$$B \quad b_1 \quad b_n$$

Dann gilt für die Diskriminanten von B und des Zahlkörpers:

$$\Delta\ B \quad \Delta_K \quad \#\mathcal{O}_K\ \Gamma\ ^2$$

Beweis: Wir wenden auf die Inklusion

$$\Gamma \quad ^n \quad \mathcal{O}_K \quad ^n$$

den Diagonalisierungsalgorithmus aus Abschnitt 6 an. Dadurch erhalten wir eine Basis $B' \quad b'_1 \quad b'_n$ von Γ und eine Basis $C \quad c_1 \quad c_n$ von $\mathcal{O}_K$, so dass die Inklusion als Diagonalmatrix

$$\begin{matrix} m_1 & & 0 \\ & \ddots & \\ 0 & & m_n \end{matrix} \qquad \text{mit } m_i \quad \{0$$

gegeben ist, d.h. $b'_i \quad m_i c_i$. Somit ist einerseits

$$\mathcal{O}_K\ \Gamma \quad \prod_{i\ 1}^{n} \quad m_i \qquad \text{also } \#\mathcal{O}_K\ \Gamma \quad \prod_{i\ 1}^{n} m_i$$

und andererseits

$$\Delta\ B \quad \Delta\ B' \quad \det\ \sigma_i\ b'_j\ ^2 \quad \det\ \sigma_i\ m_j c_j\ ^2$$

$$\det \begin{matrix} m_1 c_1 & m_1 \sigma_2\ c_1 & & m_1 \sigma_n\ c_1 \\ m_2 c_2 & m_2 \sigma_2\ c_2 & & m_2 \sigma_n\ c_2 \\ \vdots & & & \vdots \\ m_n c_n & m_n \sigma_2\ c_n & & m_n \sigma_n\ c_n \end{matrix}^2$$

$$\prod_{j\ 1}^{n} m_j^2 \quad \det\ \sigma_i\ c_j\ ^2 \qquad \prod_{j\ 1}^{n} m_j^2 \quad \Delta_K$$

Beides zusammen impliziert die Aussage.

Das folgende Korollar zeigt, wo wir nach Elementen von $\mathcal{O}_K$ Γ suchen müssen.

Korollar 16.33 *Sei K ein Zahlkörper mit n dim K und $\mathcal{O}_K$ sein Ring ganzer Zahlen. Sei Γ eine freie additive Untergruppe von $\mathcal{O}_K$ mit –Basis B b_1 b_n . Falls Γ $\mathcal{O}_K$ ist, dann existiert eine Primzahl p mit p^2 Δ B zusammen mit einem Element*

$$x \quad \frac{1}{p}\sum_{i\ 1}^{n}\lambda_i b_i \qquad \text{mit } \lambda_i \qquad 0 \quad \lambda_i \quad p$$

so dass ein i_0 $\{1$ n existiert mit λ_{i_0} 1. Weiter ist

$$B' : \quad b_1 \qquad b_{i_0\ 1}\ x\ b_{i_0\ 1} \qquad b_n$$

die –Basis einer Untergruppe Γ' von $\mathcal{O}_K$, die Γ echt enthält.

Beweis: Sei p ein Teiler der Gruppenordnung von $\mathcal{O}_K$ Γ. Nach dem Satz teilt dann p^2 die Diskriminante Δ B . Die Gruppe $\mathcal{O}_K$ Γ enthält ein Element y Γ der Ordnung p, also py Γ, aber y Γ. Wir schreiben

$$py \quad \sum_{i\ 1}^{n}\mu_i b_i$$

für geeignete μ_i . Wegen y Γ existiert ein i_0 $\{1$ n mit p μ_{i_0}. Wir wählen α β mit

$$\alpha\mu_{i_0} \quad \beta p \quad \text{ggT } \mu_{i_0}\ p \quad 1$$

und betrachten

$$p\alpha y \quad \sum_{i\ 1}^{n}\alpha\mu_i\ b_i$$

Die Koeffizienten $\alpha\mu_i$ werden zerlegt als

$$\alpha\mu_i \quad \gamma_i p \quad \lambda_i \qquad \text{mit } \gamma_i\ \lambda_i \qquad 0 \quad \lambda_i \quad p$$

Auf Grund von $\alpha\mu_{i_0}$ 1 mod p ist λ_{i_0} 1. Schließlich definieren wir

$$x : \quad \frac{1}{p}\sum_{i\ 1}^{n}\lambda_i b_i \quad \alpha y \quad \sum_{i\ 1}^{n}\gamma_i b_i \quad \mathcal{O}_K \quad \Gamma$$

und setzen B' wie in der Aussage des Korollars. Da

$$b_{i_0} \quad px \quad \sum_{\substack{i\ 1\\ i\ i_0}}^{n}\lambda_i b_i$$

ist, enthält die von B' erzeugte Untergruppe Γ' die Untergruppe Γ. Sie ist echt größer, weil x Γ' Γ.

Das Korollar liefert den Korrektheitsbeweis des folgenden

Algorithmus zur Bestimmung von $\mathcal{O}_K$

1. Errate eine –Basis B b_1 b_n einer Untergruppe Γ $\mathcal{O}_K$ vom Rang n dim K.

2. Für alle Primzahlen p mit $p^2 \Delta B$ überprüfe die Elemente

$$x \quad \frac{1}{p}\sum_{i\ 1}^{n} \lambda_i b_i$$

wobei $\lambda_i \quad \{0 \quad p \quad 1$ und eines davon 1 ist, auf Ganzheit.

Falls keins gefunden wird, gilt $\Gamma \quad \mathcal{O}_K$, und wir sind fertig. Ansonsten bildet man wie im Korollar mit Hilfe von x eine neue größere Untergruppe, mit der man diesen Schritt wiederholt.

Aufgabe 16.34 Beweisen Sie Satz 16.20 nochmal, indem Sie den Algorithmus anwenden.

Beispiel Wir bestimmen den Ring der ganzen Zahlen von $K \quad \mathbb{Q}\ \sqrt{2}\ i$. Die offensichtliche Wahl für eine –Basis einer Untergruppe $\Gamma \quad \mathcal{O}_K$ vom Rang 4 ist:

$$B \quad 1\ \sqrt{2}\ i\ i\sqrt{2}$$

Die Einbettungen von K nach sind bestimmt durch

$$\sigma_1 : \begin{matrix}\sqrt{2} & \sqrt{2}\\ i & i\end{matrix} \qquad \sigma_2 : \begin{matrix}\sqrt{2} & \sqrt{2}\\ i & i\end{matrix} \qquad \sigma_3 : \begin{matrix}\sqrt{2} & \sqrt{2}\\ i & i\end{matrix} \qquad \sigma_4 : \begin{matrix}\sqrt{2} & \sqrt{2}\\ i & i\end{matrix}$$

Somit ist die Diskriminante von B

$$\Delta\ B \quad \det \begin{matrix}1 & 1 & 1 & 1\\ \sqrt{2} & \sqrt{2} & \sqrt{2} & \sqrt{2}\\ i & i & i & i\\ i\sqrt{2} & i\sqrt{2} & i\sqrt{2} & i\sqrt{2}\end{matrix}^{2} \quad 32^{\ 2} \quad 1024$$

Wir suchen nach Elementen $x \quad \mathcal{O}_K \quad \Gamma$ der Form

$$x \quad \frac{1}{2}\ \lambda_1 1 \quad \lambda_2\sqrt{2} \quad \lambda_3 i \quad \lambda_4 i\sqrt{2}$$

mit $\lambda_j \quad \{0\ 1$. Da x ganz sein soll, müssen insbesondere seine Spur und Norm ganzzahlig sein:

$$\mathrm{Sp}\ x \quad 2\lambda_1$$

$$N\ x \quad \tfrac{1}{16} \quad \lambda_1^2 \quad 2\lambda_2^2 \quad \lambda_3^2 \quad 2\lambda_4^{2\ 2} \quad 4\ \lambda_1\lambda_3 \quad 2\lambda_2\lambda_4^{\ 2}$$

Durch Probieren findet man, dass die Norm für $\lambda_1 \quad \lambda_3 \quad 0$ und $\lambda_2 \quad \lambda_4 \quad 1$ ganzzahlig ist. Dies entspricht

$$x \quad \frac{\sqrt{2}}{2}\ 1 \quad i$$

Wegen $x^4 \quad 1$ ist x tatsächlich ganz, und wir erhalten

$$B' \quad 1\ \sqrt{2}\ i\ \frac{\sqrt{2}}{2}\ 1 \quad i$$

als Basis einer größeren Untergruppe Γ' von $\mathcal{O}_K$. Weil Γ' Γ isomorph zu 2 ist, gilt

$$\Delta\ B' \quad \Delta\ B \quad 4 \quad 256$$

nach Satz 16.32, angewandt auf B und B'. Jetzt sucht man nach Elementen

$$x \quad \frac{1}{2} \quad \lambda_1 1 \quad \lambda_2\sqrt{2} \quad \lambda_3 i \quad \lambda_4\frac{\sqrt{2}}{2}\ 1 \quad i$$

mit $\lambda_j \quad \{0\ 1$. Eine Rechnung analog zur bisherigen zeigt, dass keines dieser Elemente ungleich 0 eine ganzzahlige Norm besitzt, somit ist B' eine –Basis von $\mathcal{O}_K$.

Zusatzaufgaben

Aufgabe 16.35 Zeigen Sie, dass die Zahl $z \quad \sum_{k\ 1}^{\infty} 10^{\ k!} \quad 0\ 110001000$ keine algebraische Zahl über $\mathbb{Q}$ ist.

Aufgabe 16.36 Untersuchen Sie die folgenden komplexen Zahlen darauf, ob sie ganz über oder zumindest algebraisch über $\mathbb{Q}$ sind:

$$\frac{23}{5} \quad \frac{1 \quad \sqrt[3]{5}}{3} \quad \frac{1 \quad \sqrt{7}}{\sqrt{5}} \quad \exp\ 2\pi i\ 13$$

Aufgabe 16.37 Sei $B \quad b_1 \quad b_n$ eine Basis eines Zahlkörpers K mit $b_i \quad \mathcal{O}_K$. Zeigen Sie: Falls $\Delta\ B$ eine quadratfreie ganze Zahl ist, dann ist B eine –Basis von $\mathcal{O}_K$.

Aufgabe 16.38 Bestimmen Sie den Ring der ganzen Zahlen des Zahlkörpers $K \quad \mathbb{Q}\ \sqrt[3]{5}$.

Aufgabe 16.39 Sei $K \quad \mathbb{Q}\ \alpha$ mit $\alpha \quad \sqrt[3]{2}$. Berechnen Sie die Spur von α und α^2.

Aufgabe 16.40 Seien p und q Primzahlen mit $p \quad 1 \bmod 4$ und $q \quad 3 \bmod 4$. Bestimmen Sie den Ganzheitsring von $\mathbb{Q}\ \sqrt{p}\ \sqrt{q}$.

Aufgabe 16.41 Sei $\mathcal{O}_K$ der Ring ganzer Zahlen des quadratischen Zahlkörpers $K \quad \mathbb{Q}\ \sqrt{d}$. Sei $N\ x \quad x\sigma\ x$ wie üblich die Norm auf K. Sei $d\ x \ : \quad N\ x$. Zeigen Sie: Falls es für jedes $x \quad K$ ein $y \quad \mathcal{O}_K$ gibt mit $d\ x \quad y \quad 1$, dann ist $\mathcal{O}_K$ euklidisch mit Norm–Funktion d.

Aufgabe 16.42 Sei $\mathcal{O}_K$ der Ring ganzer Zahlen des quadratischen Zahlkörpers K mit Diskriminante Δ. Sei B eine –Basis eines Ideals $I \quad 0$ in $\mathcal{O}_K$. Zeigen Sie: Die Norm des Ideals I ist

$$N\ I \quad \frac{\sqrt{\Delta\ B}}{\Delta}$$

Aufgabe 16.43 Sei $1 \quad \zeta_p$ eine Nullstelle des Polynoms $X^p \quad 1$ für p . Der Körper $K \quad \mathbb{Q}\ \zeta_p$ heißt Kreisteilungskörper. Zeigen Sie, dass der Ring ganzer Zahlen von K gleich ζ_p ist. Folgern Sie, dass die Diskriminante Δ gleich $1^{\ p\ 1\ /2} p^{p\ 2}$ ist.

Aufgabe 16.44 Sei $K \quad \mathbb{Q} \ \alpha$ ein Zahlkörper, wobei α das irreduzible Minimalpolynom $f \quad X^3 \quad X \quad 4$ besitzt. Berechnen Sie:

1. Norm und Spur von α.
2. Die Diskriminante der $\mathbb{Q}$-Basis $1 \ \alpha \ \alpha^2$.
3. Eine Ganzheitsbasis von $\mathcal{O}_K$.
4. Die Diskriminante Δ_K von K.

Aufgabe 16.45 Ist $a \quad \mathbb{Q}$ und K ein Zahlkörper der Dimension n, so gilt $N \ a \quad a^n$ und Sp $a \quad na$.

Aufgabe 16.46 Sind $L \quad K \quad \mathbb{Q}$ Zahlkörper, so gilt

$$N_{K/} \quad N_{L/K} \quad N_{L/} \qquad \mathrm{Spur}_{K/} \quad \mathrm{Spur}_{L/K} \quad \mathrm{Spur}_{L/}$$

Aufgabe 16.47 Sei K ein Zahlkörper und $\alpha \quad \mathcal{O}_K$. Weiterhin sei $m : \mathcal{O}_K \quad \mathcal{O}_K$ die –lineare Abbildung, die durch Multiplikation mit α gegeben ist. Bezüglich einer –Basis von $\mathcal{O}_K$ sei M die darstellende Matrix von m. Zeigen Sie, dass $N \ \alpha \quad \det M$ und Sp $\alpha \quad \mathrm{Spur}\ M$ gilt und dies nicht von der Wahl der –Basis abhängt.

17 Teilertheorie im Ring ganzer Zahlen

In diesem Abschnitt wollen wir die Einheiten des Ringes ganzer Zahlen eines Zahlkörpers bestimmen — oder zumindest Aussagen über die Struktur dieser Gruppe machen. Wir werden das für quadratische Zahlkörper genau durchführen und die Ergebnisse über beliebige Zahlkörper zitieren.

Lemma 17.1 *Für ein Element $x \quad \mathcal{O}_K$ des Ringes der ganzen Zahlen eines Zahlkörpers K gilt:*

$$x \quad \mathcal{O}_K \qquad N\,x \qquad 1$$

Beweis: Falls x invertierbar ist, folgt

$$1 \quad N\,1 \quad N\,x\;x^{\,1} \quad N\,x \quad N\,x^{\,1}$$

Nach Lemma 16.17 sind die Werte $N\,x$ und $N\,x^{\,1}$ ganzzahlig. Daher muss $N\,x$ $N\,x^{\,1}$ 1 sein.

Setzen wir nun $1 \quad N\,x$ voraus. Nach Definition ist

$$1 \quad N\,x \quad x\prod_{\sigma}\sigma\,x$$

wobei σ die Menge Hom K $\{\mathrm{id}$ durchläuft. Also ist zunächst $\prod_\sigma \sigma\,x$ das Inverse zu x im Körper K. Weil mit x auch die $\sigma\,x$ ganz sind, liegt $\prod_\sigma \sigma\,x$ sogar in $\mathcal{O}_K$.

Für die genauere Bestimmung der Einheiten eines quadratischen Zahlkörpers $\mathbb{Q}\,\sqrt{d}$ wird das Vorzeichen von d wichtig.

Definition 17.2 *Ein quadratischer Zahlkörper $K \quad \mathbb{Q}\,\sqrt{d}$ heißt*

$$\begin{array}{ll} \text{reell–quadratisch,} & \textit{falls } d \quad 0, \\ \text{imaginär–quadratisch,} & \textit{falls } d \quad 0. \end{array}$$

Satz 17.3 *Die Einheiten $\mathcal{O}_K$ des Ringes der ganzen Zahlen eines imaginär–quadratischen Zahlkörpers $K \quad \mathbb{Q}\,\sqrt{d}$, d quadratfrei, sind*

$$\mathcal{O}_K \quad \begin{cases} \{ \quad 1 \quad i & & & & \textit{für } d \quad 1 \\ \{ \quad 1 \quad \rho \quad \rho^2 & \textit{mit } \rho & \exp\frac{2\pi i}{3} & & \textit{für } d \quad 3 \\ \{ \quad 1 & & & & \textit{sonst.} \end{cases}$$

S. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie,*
DOI 10.1007/978-3-8348-8263-9_17,

Beweis: Nach dem Lemma müssen wir die $x \in \mathcal{O}_K$ mit $N(x) \leq 1$ bestimmen. Wir schreiben $x = a + b\sqrt{d}$ mit $a, b \in \frac{1}{2}\mathbb{Z}$. Dann ist $N(x) = a^2 - db^2 \geq 0$, weil $d < 0$. Es gibt also keine x mit $N(x) < 1$, und wir müssen nur die Gleichung

$$1 = N(x) = a^2 + |d| b^2$$

betrachten.

Wir haben immer die Lösungen $(a, b) = (1, 0)$, also $x = 1$. Sind $a, b \in \mathbb{Z}$, so können nur noch für $d = -1$ die Lösungen $(a, b) = (0, \pm 1)$, entsprechend $x = \pm i$, hinzukommen. Es bleibt, den Fall $a, b \in \frac{1}{2} + \mathbb{Z}$ für $d \equiv 1 \bmod 4$ zu betrachten. Hier setzen wir $A = 2a$ und $B = 2b$ und betrachten nun die Gleichung

$$A^2 + |d| B^2 = 4$$

Für $d < -5$ muss $B = 0$ sein und $A = \pm 2$, entsprechend den bekannten $x = \pm 1$. Im Falle $d = -5$ impliziert $d \equiv 1 \bmod 4$ bereits $d \leq -3$. Dafür kann B auch noch ± 1 sein. Somit finden wir $A = \pm\sqrt{4 - |d|B^2} = \pm 1$. Insgesamt erhalten wir für $K = \mathbb{Q}(\sqrt{-3})$

$$\mathcal{O}_K = \left\{ \pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2} \right\}$$

Dies sind gerade die sechsten Einheitswurzeln in $\mathbb{C}$.

Satz 17.4 *Sei $K = \mathbb{Q}(\sqrt{d})$ ein reell–quadratischer Zahlkörper. Dann existiert ein eindeutiges Element $\eta \in \mathcal{O}_K$, $\eta > 1$, im Ring der ganzen Zahlen, so dass jede Einheit dieses Ringes auf eindeutige Weise als $\pm\eta^n$ mit $n \in \mathbb{Z}$ geschrieben werden kann.*

Insbesondere ist $\mathcal{O}_K^\times$ isomorph zu $\{\pm 1\} \times \mathbb{Z}$.

Das η im vorangehenden Satz wird *Fundamentaleinheit* genannt. Manche Autoren verzichten auf die Bedingung $\eta > 1$. Dann ist die Fundamentaleinheit nicht ganz eindeutig. Neben η sind auch $-\eta, \eta^{-1}$ und $-\eta^{-1}$ Fundamentaleinheiten.

Beweis: Wir haben im Satz 10.22 gesehen, dass die Gleichung $x^2 - dy^2 = \pm 1$ eine ganzzahlige Lösung (a, b) mit $a, b > 0$ hat. Also ist $x = a + b\sqrt{d}$ wegen $N(x) = \pm 1$ eine Einheit und die Einheitengruppe besteht nicht nur aus ± 1.

Nun behaupten wir, dass die Menge $\mathcal{O}_K^\times \cap \{1 \leq x \leq 2\}$ keinen Häufungspunkt bei 1 hat. Angenommen, 1 wäre ein Häufungspunkt. Sei

$$x_n = \frac{a_n + b_n\sqrt{d}}{2} \in \mathcal{O}_K \quad \text{mit } a_n, b_n \in \mathbb{Z}$$

eine Folge in $\mathcal{O}_K^\times \cap \{1 < x \leq 2\}$, die dagegen konvergiert. Die Folgen a_n und b_n können nicht beschränkt sein, weil sonst nur endlich viele verschiedene Werte in der Folge auftreten und die Folge damit gegen einen dieser Werte ungleich 1 konvergiert. Es gibt also eine Teilfolge, bei der a_n, b_n gegen $+\infty$ oder $-\infty$ konvergiert. Auf dieser Teilfolge konvergiert aber $\sigma(x_n) = a_n - b_n\sqrt{d} \geq 2$ gegen $+\infty$ bzw. $-\infty$. Dies widerspricht

$$\sigma(x_n) = \frac{N(x_n)}{x_n} = \left(\frac{1}{x_n}\right)^n \to 1$$

Da 1 kein Häufungspunkt von $\mathcal{O}_K \quad \{1$ ist, gibt es ein minimales $\eta \quad \mathcal{O}_K$ mit $\eta \quad 1$. Wir müssen zeigen, dass jedes Element von $\mathcal{O}_K$ auf eindeutige Weise als η^n mit n geschrieben werden kann. Da diese Elemente offensichtlich alle verschieden sind, ist die Eindeutigkeit klar. Sei nun $x \quad \mathcal{O}_K$ gegeben. Wir können ohne Einschränkung $x \quad 0$ annehmen. Da die Folge η^n streng monoton wächst und für $n \quad \infty$ gegen 0 sowie für $n \quad \infty$ gegen ∞ konvergiert, gibt es ein n mit

$$\eta^n \quad x \quad \eta^{n \ 1}$$

Jetzt folgt $1 \quad x \ \eta^n \quad \eta$. Weil das Element $x \ \eta^n$ wieder in $\mathcal{O}_K$ liegt, muss es nach Wahl von η sogar 1 sein, d.h. $x \quad \eta^n$.

Insgesamt erhalten wir folgenden Isomorphismus

$$2 \qquad \mathcal{O}_K \qquad \bar{j} \ n \qquad 1 \ ^j\eta^n$$

Die Eindeutigkeit von η ist einfach. Sei η' ein weiteres Element mit den Eigenschaften der Aussage. Sei ohne Einschränkung $\eta' \quad \eta \quad 1$. Es gibt ein n mit $\eta'^{\ n} \quad \eta$. Wegen $\eta'^{\ n} \quad \eta \quad 1$ folgt $n \quad 1$. Aus der strengen Monotonie von $\eta'^{\ n}$ und $\eta' \quad \eta$ folgt $n \quad 1$ und somit $\eta \quad \eta'$.

Wir wollen nun einen Algorithmus zum Auffinden der Fundamentaleinheit beschreiben. Zunächst beschreiben wir die allgemeine Form einer Einheit, die größer als 1 ist.

Lemma 17.5 *Für eine Einheit*

$$\varepsilon \quad \frac{a \quad b\sqrt{\Delta}}{2} \quad 1$$

im Ring ganzer Zahlen eines reell–quadratischen Zahlkörpers mit Diskriminante Δ gilt:

$$a \quad 1 \qquad \textit{und} \qquad b \quad 1$$

Beweis: Auf Grund von $\varepsilon \quad 1$ sind die vier Zahlen $\varepsilon \quad \varepsilon^{\ 1}$ paarweise verschieden. Wegen $\varepsilon^{\ 1} \quad N \ \varepsilon \quad \sigma \ \varepsilon$ haben sie die Form

$$\frac{a \quad b\sqrt{\Delta}}{2}$$

Die einzige Zahl größer als eins — und somit die größte — unter ihnen ist ε selbst. Folglich muss $a \ b \quad 1$ sein.

Satz 17.6 *Sei K ein reell–quadratischer Zahlkörper mit Diskriminante Δ und $\mathcal{O}_K \qquad \omega$ mit $\omega \quad \Delta \quad \sqrt{\Delta} \quad 2$ sein Ring ganzer Zahlen. Sei schließlich*

$$\vartheta \quad \frac{1}{\omega \quad \omega}$$

Dann ist ϑ reduziert, d.h. $\vartheta \quad 1$ und $1 \quad \sigma \ \vartheta \quad 0$, und hat somit eine rein–periodische Kettenbruchentwicklung

$$\vartheta \quad \overline{a_0 \qquad a_{h \ 1}}$$

wobei die Periodenlänge minimal gewählt sein soll. Die Folge q_n sei wie im Abschnitt 10 definiert. Dann ist

$$\eta \quad q_{h\ 1}\vartheta \quad q_{h\ 2}$$

die Fundamentaleinheit von $\mathcal{O}_K$.

Beweis: Wir zeigen zuerst, dass ϑ reduziert ist. Wegen $0 \quad \omega \quad \omega \quad 1$ ist $\vartheta \quad 1$. Aus $\Delta \quad 4$ folgt

$$\sigma\ \omega \quad \omega \quad \sigma\ \omega \quad \omega \quad \omega \quad \sqrt{\Delta} \quad \omega \quad \omega \quad \omega \quad 2 \quad 1$$

und somit auch $0 \quad \sigma\ \vartheta \quad 1$.

Als Nächstes beweisen wir, dass η wirklich in $\mathcal{O}_K$ liegt und eine Einheit ist. Aus der Periodizität der Kettenbruchentwicklung folgt mit Lemma 10.6

$$\vartheta \quad a_0 \quad a_{h\ 1}\ \vartheta \quad \frac{\vartheta p_{h\ 1} \quad p_{h\ 2}}{\vartheta q_{h\ 1} \quad q_{h\ 2}}$$

und weiter

$$q_{h\ 1}\vartheta^2 \quad q_{h\ 2} \quad p_{h\ 1}\ \vartheta \quad p_{h\ 2} \quad 0$$

Multiplizieren dieser Gleichung mit $q_{h\ 1}$ und substituieren mit $\vartheta \quad \eta \quad q_{h\ 2} \quad q_{h\ 1}$ führt zu

$$\eta^2 \quad q_{h\ 2} \quad p_{h\ 1}\ \eta \quad p_{h\ 1}q_{h\ 2} \quad p_{h\ 2}q_{h\ 1} \quad 0$$

Mit dem Lemma 10.7 ergibt sich

$$\eta^2 \quad q_{h\ 2} \quad p_{h\ 1}\ \eta \quad 1^{\ h} \quad 0$$

Dies ist eine Ganzheitsgleichung für η. Wenn wir sie als

$$\eta\ \eta \quad q_{h\ 2} \quad p_{h\ 1} \quad 1^{\ h}$$

schreiben, erkennen wir, dass η eine Einheit im Ring ganzer Zahlen ist.

Wir zeigen nun, dass η die Fundamentaleinheit ist. Dafür müssen wir zeigen, dass für jede Einheit $\varepsilon \quad \mathcal{O}_K$ mit $\varepsilon \quad 1$ eine natürliche Zahl n existiert mit $\varepsilon \quad \eta^n$.

Wir schreiben gemäß Lemma 17.5

$$\varepsilon \quad \frac{r \quad s\sqrt{\Delta}}{2} \qquad \text{mit } r\ s$$

Wir wollen ε und $\vartheta\varepsilon$ in der Form

$$\begin{matrix} \vartheta\varepsilon & p\vartheta & p' \\ \varepsilon & q\vartheta & q' \end{matrix} \qquad \text{also} \qquad \begin{matrix} \vartheta\varepsilon & p & p' & \vartheta \\ \varepsilon & q & q' & 1 \end{matrix}$$

darstellen. Dazu suchen wir ein Polynom in X mit ϑ als Nullstelle. Für $\omega \quad \omega$ haben wir nach Lemma 16.15

$$\omega \quad \omega^{\ 2} \quad 2\ \omega \quad \Delta\ \omega \quad \omega \quad \frac{2\ \omega \quad \Delta^{\ 2} \quad \Delta}{4} \quad 0$$

Wir teilen diese Gleichung durch $\omega \quad \omega^{\ 2}$ und substituieren $\omega \quad \omega \quad 1\ \vartheta$

$$\frac{\Delta \quad 2\ \omega \quad \Delta^{\ 2}}{4}\vartheta^2 \quad 2\ \omega \quad \Delta\ \vartheta \quad 1 \quad 0$$

Zur Abkürzung setzen wir

$$\beta : \quad 2\ \omega \quad \Delta$$

$$\alpha : \quad \frac{\Delta \quad \beta^2}{4}$$

Insbesondere gilt also $\Delta \quad \beta^2 \quad 4\alpha$ und die obige Gleichung ist nun

$$\alpha\vartheta^2 \quad \beta\vartheta \quad 1 \quad 0$$

Aus

$$\beta \quad 2\ \frac{\Delta \quad \sqrt{\Delta}}{2} \qquad \Delta$$

erhalten wir die Abschätzungen

$$0 \quad \beta \quad \sqrt{\Delta} \qquad \text{und somit} \qquad \alpha \quad \frac{\Delta \quad \beta^2}{4} \quad 0$$

Multiplikation der Gleichung mit α führt zu

$$\alpha\vartheta^{\ 2} \quad \beta\ \alpha\vartheta \qquad \alpha \quad 0$$

Durch das Lösen dieser Gleichung unter Berücksichtigung von $\alpha \quad 0$ und $\vartheta \quad 1$ erhalten wir

$$\alpha\vartheta \quad \frac{\beta \quad \sqrt{\beta^2 \quad 4\alpha}}{2} \quad \frac{\beta \quad \sqrt{\Delta}}{2}$$

Lesen wir dies als $\sqrt{\Delta}\ 2 \quad \alpha\vartheta \quad \beta\ 2$, dann ergibt sich unmittelbar die Darstellung

$$\varepsilon \quad \frac{r \quad s\sqrt{\Delta}}{2} \quad \frac{r}{2} \quad s \quad \alpha\vartheta \quad \frac{\beta}{2} \qquad \alpha s\vartheta \quad \frac{r \quad \beta s}{2}$$

$$q\vartheta \quad q' \qquad \text{mit } q \quad \alpha s \qquad \text{und } q' \quad \frac{r \quad \beta s}{2}$$

sowie auch mit Hilfe von

$$\varepsilon\vartheta \qquad \alpha s\vartheta \quad \frac{r \quad \beta s}{2} \quad \vartheta \quad \alpha s\vartheta^2 \quad \frac{r \quad \beta s}{2}\vartheta$$

$$s\ \beta\vartheta \quad 1 \quad \frac{r \quad \beta s}{2}\vartheta \quad \frac{r \quad \beta s}{2}\vartheta \quad s$$

$$p\vartheta \quad p' \qquad \text{mit } p \quad \frac{r \quad \beta s}{2} \qquad \text{und } p' \quad s$$

Durch Division der beiden Darstellungen erhalten wir

$$\vartheta \quad \frac{p\vartheta \quad p'}{q\vartheta \quad q'}$$

Dies sieht genau wie die Formel aus, die wir von der Kettenbruchentwicklung kennen. Angenommen, dies ist wirklich der Fall, d.h. es gibt ein k-Tupel von natürlichen Zahlen $B \quad b_0\ b_1 \quad b_{k\ 1}$, so dass für die zugehörigen Folgen der $\overline{p}_i$ und $\overline{q}_i$ gilt

$$\overline{p}_{k\ 1} \quad p \quad \overline{p}_{k\ 2} \quad p' \quad \overline{q}_{k\ 1} \quad q \quad \text{und} \quad \overline{q}_{k\ 2} \quad q'$$

Dann gilt nach Lemma 10.6

$$\vartheta \quad b_0 \quad b_{k\ 1}\ \vartheta$$

Aus der Eindeutigkeit der Kettenbruchentwicklung von ϑ folgt, dass das k–Tupel B gerade aus $k\ \ h$–Kopien des h–Tupels $a_0 \quad a_{h\ 1}$ besteht. Es folgt in der Matrizenschreibweise

$$\begin{matrix} p & p' \\ q & q' \end{matrix} \quad \prod_{n\ 0}^{k\ 1} \begin{matrix} b_n & 1 \\ 1 & 0 \end{matrix} \quad \prod_{n\ 0}^{h\ 1} \begin{matrix} a_n & 1 \\ 1 & 0 \end{matrix}^{k/h} \quad \begin{matrix} p_{h\ 1} & p_{h\ 2} \\ q_{h\ 1} & q_{h\ 2} \end{matrix}^{k/h}$$

Aus erhalten wir

$$\begin{matrix} p_{h\ 1} & p_{h\ 2} \\ q_{h\ 1} & q_{h\ 2} \end{matrix} \begin{matrix} \vartheta \\ 1 \end{matrix} \quad \begin{matrix} p_{h\ 1}\vartheta & p_{h\ 2} \\ q_{h\ 1}\vartheta & q_{h\ 2} \end{matrix} \quad q_{h\ 1}\vartheta \quad q_{h\ 2} \quad \begin{matrix} \vartheta \\ 1 \end{matrix}$$

$$\eta \quad \begin{matrix} \vartheta \\ 1 \end{matrix}$$

und weiter

$$\varepsilon \quad \begin{matrix} \vartheta \\ 1 \end{matrix} \quad \begin{matrix} p & p' \\ q & q' \end{matrix} \quad \begin{matrix} \vartheta \\ 1 \end{matrix} \quad \begin{matrix} p_{h\ 1} & p_{h\ 2} \\ q_{h\ 1} & q_{h\ 2} \end{matrix}^{k/h} \quad \begin{matrix} \vartheta \\ 1 \end{matrix} \quad \eta^{k/h} \quad \begin{matrix} \vartheta \\ 1 \end{matrix}$$

Insbesondere folgt die gewünschte Gleichung $\varepsilon \quad \eta^{k/h}$.

Wir wollen nun die ganzen Zahlen $p\ p'\ q\ q'$ abschätzen. Dazu starten wir mit den Abschätzungen

$$\sqrt{\Delta} \quad 2\alpha\vartheta \quad \beta \quad 2\alpha \quad \beta \qquad \text{aus } \vartheta \quad 1$$

$$\sqrt{\Delta} \quad 2\alpha\sigma\ \vartheta \quad \beta \quad 2\alpha \quad \beta \qquad \text{aus } 0 \quad \sigma\ \vartheta \quad 1$$

Wir erkennen, dass $\sqrt{\Delta}$ in dem offenen Intervall $2\alpha \quad \beta\ 2\alpha \quad \beta$ liegt. Damit erhalten wir nun

$$q' \quad \frac{r \quad s\beta}{2} \quad \frac{r \quad s\sqrt{\Delta}}{2} \quad \sigma\ \varepsilon \quad N\ \varepsilon\ \varepsilon^{\ 1} \quad 1$$

$$q \quad q' \quad \frac{r \quad s\ 2\alpha \quad \beta}{2} \quad \frac{r \quad s\sqrt{\Delta}}{2} \quad \sigma\ \varepsilon \quad N\ \varepsilon\ \varepsilon^{\ 1} \quad 1$$

$$p \quad q \quad \frac{r \quad s\ 2\alpha \quad \beta}{2} \quad \frac{r \quad s\sqrt{\Delta}}{2} \quad \sigma\ \varepsilon \quad N\ \varepsilon\ \varepsilon^{\ 1} \quad 1$$

Mit der Ganzzahligkeit der Werte ergibt sich

$$q \quad q' \quad 0 \quad \text{und} \quad p \quad q$$

Des Weiteren haben wir die Gleichheit

$$pq' \quad qp' \quad \frac{r \quad s\beta}{2} \; \frac{r \quad s\beta}{2} \quad \alpha s^2 \quad \frac{r^2 \quad \beta^2 \quad 4\alpha \; s^2}{4} \quad \frac{r^2 \quad s^2\Delta}{4} \quad N \; \varepsilon$$

insbesondere sind p und q teilerfremd.

Wir behandeln zunächst einige Spezialfälle. Für $q' \quad 0$ folgt aus $1 \quad N \; \varepsilon \quad pq' \quad qp'$ qp' bereits $q \quad p' \quad 1$. Benutzen wir für B das 1–Tupel p so ergibt sich wie gefordert

$$\overline{p}_{\;1} \quad 1 \quad p' \quad \overline{p}_0 \quad p \quad \overline{q}_{\;1} \quad 0 \quad q' \quad \overline{q}_0 \quad 1 \quad q$$

Für $q \quad q' \quad 1$ folgt aus $1 \quad N \; \varepsilon \quad pq' \quad qp' \quad q \; p \quad p'$ diesmal $q \quad q' \quad 1$ und $p \quad p' \quad 1$. Aus $1 \quad q \quad \alpha s$ folgt $p' \quad s \quad 1$ und damit $p \quad p' \quad 1 \quad 2$. Hier benutzen wir für B das 2–Tupel $1 \; 1$, dann ist wie gewünscht

$$\overline{p}_0 \quad 1 \quad \overline{p}_1 \quad 1 \; \overline{p}_0 \quad 1 \quad 2 \quad p \quad \overline{q}_0 \quad 1 \quad q' \quad \overline{q}_1 \quad 1 \; \overline{q}_0 \quad 1 \quad q$$

Als letzten Spezialfall betrachten wir $p \quad q$. Wegen der Teilerfremdheit muss nun $p \quad q \quad 1$ gelten. Aus $1 \quad q \quad q' \quad 0$ folgt $q \quad q'$ oder $q' \quad 0$. Beides haben wir schon behandelt.

Wir dürfen nun die folgende Situation annehmen

$$q \quad q' \quad 0 \qquad \text{und} \qquad \frac{p}{q} \quad 1$$

Wir entwickeln nun $p \; q$ in einen Kettenbruch

$$\frac{p}{q} \quad b_0 \qquad b_{k \;\; 1}$$

und wählen natürlich $B \quad b_0 \qquad b_{k \;\; 1}$. Wegen $q \quad 2$ ist $k \quad 2$. Auf Grund der Bemerkung nach Satz 10.4 können wir die Kettenbruchentwicklung entweder um eins verlängern oder verkürzen und dürfen daher $1 \;^{k} \quad N \; \varepsilon$ annehmen. Dann gilt nach Lemma 10.7

$$pq' \quad qp' \quad N \; \varepsilon \qquad 1 \;^{k} \quad \overline{p}_{k \;\; 1}\overline{q}_{k \;\; 2} \quad \overline{p}_{k \;\; 2}\overline{q}_{k \;\; 1} \qquad \dagger$$

und nach Lemma 10.6

$$\frac{p}{q} \quad \frac{\overline{p}_{k \;\; 1}}{\overline{q}_{k \;\; 1}}$$

Da sowohl p und q sowie $\overline{p}_{k \;\; 1}$ und $\overline{q}_{k \;\; 1}$ teilerfremd sind, folgt

$$p \quad \overline{p}_{k \;\; 1} \qquad \text{und} \qquad q \quad \overline{q}_{k \;\; 1}$$

Einsetzen in $\dagger$ ergibt

$$p \; q' \quad \overline{q}_{k \;\; 2} \quad q \; p' \quad \overline{p}_{k \;\; 2} \qquad\qquad q \; q' \quad \overline{q}_{k \;\; 2}$$

Mit $q \quad \overline{q}_{k \;\; 1} \quad q' \; \overline{q}_{k \;\; 2} \quad 0$ folgt $q' \quad \overline{q}_{k \;\; 2}$. Einsetzen der drei bisher gefundenen Gleichheiten in $\dagger$ impliziert schließlich auch die letzte $p' \quad \overline{p}_{k \;\; 2}$.

Beispiel Wir bestimmen die Fundamentaleinheit des Ringes ganzer Zahlen des reell–quadratischen Zahlkörpers $K \quad \mathbb{Q}\ \sqrt{17}$. Hier haben wir die Invarianten

$$\Delta \quad 17 \quad \omega \quad \frac{17 \quad \sqrt{17}}{2} \quad \text{und} \quad \vartheta \quad \frac{1}{\omega \quad \omega} \quad \frac{2}{3 \quad \sqrt{17}} \quad \frac{3 \quad \sqrt{17}}{4}$$

Die Zahl ϑ ist als Kettenbruch $\overline{1\ 1\ 3}$. Damit berechnen sich die q_i als

$$q_{\ 1} \quad 0 \quad q_0 \quad 1 \quad q_1 \quad 1q_0 \quad 0 \quad 1 \quad q_2 \quad 3q_1 \quad 1 \quad 4$$

Nach dem Satz ist

$$\eta : \quad 4\vartheta \quad 1 \quad 4 \quad \sqrt{17}$$

die Fundamentaleinheit des Ringes der ganzen Zahlen von $\mathbb{Q}\ \sqrt{17}$.

Aufgabe 17.7 Bestimmen Sie die Fundamentaleinheit des Ringes ganzer Zahlen von dem Zahlkörper $\mathbb{Q}\ \sqrt{47}$.

Der Satz kann auch zum Auffinden der ganzzahligen Lösungen der *Pellschen Gleichung*

$$x^2 \quad dy^2 \quad 1 \qquad \text{für } d \qquad \text{quadratfrei}$$

benutzt werden. Falls N die Norm des quadratischen Zahlkörpers $K \quad \mathbb{Q}\ \sqrt{d}$ bezeichnet, ist diese Gleichung nämlich äquivalent zu

$$N\ x \quad y\sqrt{d} \quad 1 \qquad \text{mit } x\ y$$

Die Lösungen der Pellschen Gleichung entsprechen also den Einheiten in $\mathcal{O}_K$, deren Norm 1 ist und die in $\sqrt{d}$ liegen. Welche das genau sind, sagt der folgende Satz.

Satz 17.8 *Sei d quadratfrei und* η *die Fundamentaleinheit des Ringes ganzer Zahlen des reell–quadratischen Zahlkörpers K* $\mathbb{Q}\ \sqrt{d}$ *. Dann entsprechen die ganzzahligen Lösungen* $x\ y \quad ^2$ *der Pellschen Gleichung*

$$x^2 \quad dy^2 \quad 1$$

den Elementen

$$x \quad y\sqrt{d} \qquad \eta^n \qquad \textit{mit} \qquad \begin{matrix} 2\ n & \textit{falls } N\ \eta \quad 1 \\ 3\ n & \textit{falls } \eta \quad \sqrt{d} \end{matrix}$$

Beweis: Da — wie oben bemerkt — jede ganzzahlige Lösung $x\ y$ von $x^2 \quad dy^2 \quad 1$ zu einer Einheit $x \quad y\sqrt{d}$ korrespondiert und η eine Fundamentaleinheit ist, gibt es ein n mit

$$x \quad y\sqrt{d} \qquad \eta^n$$

Die Normbedingung $N\ x \quad y\sqrt{d} \qquad 1$ bedeutet daher

$$1 \quad N\ x \quad y\sqrt{d} \quad N \quad \eta^n \quad N\ \eta\ ^n$$

Somit ist diese Bedingung immer für $N\ \eta \qquad 1$ erfüllt und im Fall von $N\ \eta \qquad 1$ muss n gerade sein.

Betrachten wir nun die zweite Bedingung

$$x \quad y\sqrt{d} \qquad \eta^n \qquad \sqrt{d}$$

Dies ist natürlich trivialerweise im Fall von $\eta \quad \sqrt{d}$ erfüllt. Dies gilt zum Beispiel, wenn $\mathcal{O}_K \quad \sqrt{d}$, also $d \quad 1 \bmod 4$, ist. Sei daher nun $d \quad 1 \bmod 4$. Nehmen wir für das Folgende daher $\eta \quad \sqrt{d}$ an und schreiben

$$\eta \quad \frac{a \quad b\sqrt{d}}{2} \qquad \text{mit ungeraden } a \ b$$

Für η^2 ergibt sich

$$\eta^2 \quad \frac{a^2 \quad db^2 \quad 2ab\sqrt{d}}{4}$$

Wegen $4 \quad 2ab$ ist auch $\eta^2 \quad \sqrt{d}$. Nun ist jedoch $N \ \eta^2 \qquad 1$, und wir haben eine gebrochene Lösung der Pellschen Gleichung. Schreiben wir dies als

$$N \quad \frac{x \quad y\sqrt{d}}{2} \qquad 1 \qquad \text{mit ungeraden } x \ y$$

Dann folgt

$$x^2 \quad dy^2 \quad 4$$

Modulo 8 ist das Quadrat jeder ungeraden Zahl eins und somit ist $1 \quad d \quad 4 \bmod 8$, d.h. $d \quad 5 \bmod 8$.

Nun betrachten wir die dritte Potenz von η

$$\eta^3 \quad \frac{a^3 \quad 3dab^2 \qquad 3ba^2 \quad db^3 \ \sqrt{d}}{8}$$

Modulo 8 ist $a^2 \quad b^2 \quad 1$ und somit

$$a^3 \quad 3dab^2 \quad a \ 1 \quad 3d \qquad 0 \bmod 8 \qquad \text{und}$$
$$3ba^2 \quad db^3 \quad b \ 3 \quad d \qquad 0 \bmod 8$$

Wir können also den Bruch kürzen und sehen $\eta^3 \qquad \sqrt{d}$, folglich $\eta^{3n} \qquad \sqrt{d}$ für $n \qquad$. Tatsächlich gilt das für $n \qquad$, weil wir das Inverse einer solchen Potenz als $\eta \quad ^{3n}$ $N \ \eta^{3n} \ \sigma \ \eta^{3n}$ berechnen können. Nehmen wir nun an, dass $\eta^k \qquad \sqrt{d}$ für ein $k \qquad$ ist. Wir wollen $3 \ k$ zeigen. Wir wählen $n \qquad$ und $r \quad \{0 \ 1 \ 2 \quad$ mit $k \quad 3n \quad r$. Dann ist mit $\eta^k \qquad \sqrt{d}$ auch

$$\eta^k \ \ \eta \ \ ^{3n} \quad \eta^k \ \ ^{3n} \quad \eta^r \qquad \sqrt{d}$$

Da $\eta \ \ \eta^2 \qquad \sqrt{d}$, folgt $r \quad 0$, also $k \quad 3n$.

Wir wollen ein Zwischenergebnis des Beweises festhalten.

Bemerkung 17.9 *Die Fundamentaleinheit des Ringes ganzer Zahlen vom reell–quadratischen Zahlkörper* $\mathbb{Q} \ \sqrt{d}$ *liegt in* $\sqrt{d}$, *falls* $d \quad 5 \bmod 8$ *ist.*

Nun wollen wir umgekehrt die Lösungstechniken für die Pellsche Gleichung aus Abschnitt 10 dazu nutzen, um nochmal auf eine andere Weise die Fundamentaleinheit des Ringes ganzer Zahlen von $K \quad \mathbb{Q}\sqrt{d}$ zu bestimmen. Eine Einheit $x \quad y\sqrt{d}, x\ y \quad$, des Ringes $\mathcal{O}_K$ entspricht einer Lösung $x\ y \quad$ von

$$x^2 \quad dy^2 \quad 1$$

Sie kommt damit nach Satz 10.21 in der Form $x\ y$ als Näherungsbruch in der Kettenbruchentwicklung von $\sqrt{d}$ vor und ist wegen ggT $x\ y \quad 1$ daraus berechenbar. Im Fall von $d \quad 5 \bmod 8$ gibt es auch noch Einheiten von der Form

$$\varepsilon \quad \frac{x \quad y\sqrt{d}}{2} \quad 1 \qquad \text{mit } x\ y \qquad \text{und } x \quad y \quad 1 \bmod 2$$

Diese entsprechen den Lösungen $x\ y \quad ^2$ der Gleichung

$$1 \quad N\ \varepsilon \quad \frac{x^2 \quad dy^2}{4} \qquad x^2 \quad dy^2 \quad 4$$

Auch diese kommen nach Satz 10.21 für $d \quad 5 \quad 2\ 8 \quad 21$ in der Form $x\ y$ als Näherungsbruch in der Kettenbruchentwicklung von $\sqrt{d}$ vor. (Die beiden Fälle $d \quad 5\ 13$ werden wir später als Sonderfall betrachten.) Aus $x^2 \quad dy^2 \quad 4$ folgt ggT $x\ y \quad 2$, mit $x \quad y \quad 1 \bmod 2$ sogar ggT $x\ y \quad 1$. Daher können wir wieder x und y eindeutig aus $x\ y$ berechnen.

Das Auffinden der Lösungen von $x^2 \quad dy^2 \quad 4$ wird durch Satz 10.19 besonders einfach gemacht, weil dort für die Näherungsbrüche $p_n\ q_n$ von $\sqrt{d}$ die Gleichung

$$p_n^2 \quad dq_n^2 \quad 1^{\ n\ 1}c_n$$

zusammen mit einer Rekursionsformel für c_n bewiesen wurde. Es bleibt damit nur die Frage, wann die Fundamentaleinheit als Lösung auftritt. Der Leser wird schon vermuten, dass dies der Fall ist, wenn zum ersten Mal die Gleichung

$$p_n^2 \quad dq_n^2 \quad 1^{\ n\ 1}c_n \quad \{ \quad 1 \quad 4$$

erfüllt ist. Um dies zu zeigen, werden wir nutzen, dass nach Lemma 10.7

$$q_0 \quad q_1 \quad q_2 \quad q_3 \quad q_4$$

und auch $q_0 \quad q_1$ für $a_0 \quad 1$ gilt. Zeigen wir etwas Analoges für die Potenzen der Fundamentaleinheit:

Satz 17.10 *Sei η die Fundamentaleinheit des Ringes ganzer Zahlen eines reell–quadratischen Zahlkörpers $\mathbb{Q}\sqrt{d}$. Weiter seien $a_n\ b_n \quad \frac{1}{2}$ so gewählt, dass*

$$\eta^n \quad a_n \quad b_n\sqrt{d}$$

ist. Dann gilt

$$\eta^n \quad \eta^m \qquad n \quad m \qquad a_n \quad a_m \qquad b_n \quad b_m$$

mit Ausnahme von $d \quad 5$, $n \quad 1$ und $m \quad 2$, wo wegen

$$\eta \quad \frac{1 \quad \sqrt{5}}{2} \qquad \eta^2 \quad \frac{3 \quad \sqrt{5}}{2}$$

die letzte Äquivalenz nicht hält.

Beweis: Weil $\eta \quad 1$ ist, ist η^n eine streng monoton wachsende Folge, d.h. $\eta^n \quad \eta^m \quad n \quad m$. Dasselbe wollen wir nun von den Folgen a_n und b_n zeigen. Es reicht $a_n \quad a_{n\ 1}$ und $b_n \quad b_{n\ 1}$ zu zeigen. Wir rechnen

$$\eta^{n\ 1} \quad \eta^n \ \eta \quad a_n \quad b_n\sqrt{d} \ \ a_1 \quad b_1\sqrt{d} \quad a_n a_1 \quad b_n b_1 d \quad a_n b_1 \quad b_n a_1 \ \sqrt{d}$$

$$a_{n\ 1} \quad a_n a_1 \quad b_n b_1 d \quad \text{und} \quad b_{n\ 1} \quad a_n b_1 \quad b_n a_1$$

Somit folgt $a_n \quad a_{n\ 1}$ und $b_n \quad b_{n\ 1}$, falls $a_1 \quad 1$ ist, insbesondere also im Fall von $\eta \ \sqrt{d}$. Die möglichen Ausnahmen stellen die d dar, für die

$$\eta \quad \frac{1 \quad v\sqrt{d}}{2}$$

mit einem v ist. Da Einheiten die Norm $\quad 1$ haben, erhalten wir

$$1 \quad \frac{1 \quad dv^2}{4} \qquad 1 \quad dv^2 \quad 4$$

Es folgt $d \quad 5$ und $\eta \quad 1 \quad \sqrt{5} \quad 2$. Dafür müssen wir

$$a_{n\ 1} \quad \frac{a_n \quad 5b_n}{2} \quad a_n \quad \text{und} \quad b_{n\ 1} \quad \frac{a_n \quad b_n}{2} \quad b_n$$

nur für $n \quad 2$ beweisen. Diese beiden Aussagen sind äquivalent zu

$$5b_n \quad a_n \quad b_n$$

Nach den obigen Formeln ist das äquivalent zu

$$5\frac{a_{n\ 1} \quad b_{n\ 1}}{2} \quad \frac{a_{n\ 1} \quad 5b_{n\ 1}}{2} \quad \frac{a_{n\ 1} \quad b_{n\ 1}}{2}$$

was wegen $a_{n\ 1} \ b_{n\ 1}$ wahr ist.

Der Satz sagt, dass wir für $d \quad 5$ die Fundamentaleinheit $\eta \quad a \quad b\sqrt{d}$ als die Einheit mit minimalem b finden können. Im Fall $\eta \qquad \sqrt{d}$ liefert uns der Kettenbruchalgorithmus diese Einheiten als $p_n \quad q_n\sqrt{d}$ für gewisse n mit aufsteigenden q_n. Die Fundamentaleinheit ist somit die erste, die auftritt. Für $\eta \qquad \sqrt{d}$ haben wir das Problem, dass die Monotonie der q_n nicht ganz ausreicht, denn wir finden die Einheiten als

$$\frac{p_n \quad q_n\sqrt{d}}{\sqrt{c_n}}$$

für die n, wo

$$p_n^2 \quad dq_n^2 \qquad 1^{\ n\ 1}c_n \quad \{ \quad 1 \quad 4$$

gilt. Wir müssen dafür das Folgende zeigen:

Lemma 17.11 *Sei η die Fundamentaleinheit des Ringes ganzer Zahlen eines reell–quadratischen Zahlkörpers $\mathbb{Q}\ \sqrt{d}$, so dass $\eta \qquad \sqrt{d}$. Weiter seien $a_n \ b_n \qquad$ und $c_n \quad \{1 \ 2$ so gewählt, dass*

$$\eta^n \quad \frac{a_n \quad b_n\sqrt{d}}{c_n} \qquad \textit{mit} \ \ \text{ggT} \ a_n \ b_n \ c_n \qquad 1$$

ist. Dann gilt

$$\eta^n \quad \eta^m \qquad n \quad m \qquad a_n \quad a_m \qquad b_n \quad b_m$$

Für $d \quad 5$ ist die Aussage falsch, weil

n	1	2	3	4	5	6
η^n	$\frac{1 \quad \overline{5}}{2}$	$\frac{3 \quad \overline{5}}{2}$	$2 \quad \sqrt{5}$	$\frac{7 \quad 3 \quad \overline{5}}{2}$	$\frac{11 \quad 5 \quad \overline{5}}{2}$	$9 \quad 4\sqrt{5}$

n	7	8	9	10	11	12
η^n	$\frac{29 \quad 13 \quad \overline{5}}{2}$	$\frac{47 \quad 21 \quad \overline{5}}{2}$	$38 \quad 17\sqrt{5}$	$\frac{123 \quad 55 \quad \overline{5}}{2}$	$\frac{199 \quad 89 \quad \overline{5}}{2}$	$161 \quad 72\sqrt{5}$

ist.

Beweis: Das Vorgehen beim Beweis ist analog zum Beweis des vorangehenden Satzes. Mit $\eta \quad a_1 \quad b_1\sqrt{d} \quad 2$ berechnen wir

$$\eta^{n \ 1} \quad \eta^n \ \eta \quad \frac{a_n \quad b_n\sqrt{d}}{c_n} \ \frac{a_1 \quad b_1\sqrt{d}}{2} \quad \frac{a_n a_1 \quad b_n b_1 d}{2c_n} \quad \frac{a_n b_1 \quad b_n a_1}{2c_n}\sqrt{d}$$

$$\frac{a_{n \ 1}}{c_{n \ 1}} \quad \frac{a_n a_1 \quad b_n b_1 d}{2c_n} \quad \text{und} \quad \frac{b_{n \ 1}}{c_{n \ 1}} \quad \frac{a_n b_1 \quad b_n a_1}{2c_n}$$

Für die strenge Monotonie der a_n und b_n müssen wir

$$a_{n \ 1} \quad \frac{c_{n \ 1}}{c_n} \ \frac{a_n a_1 \quad b_n b_1 d}{2} \quad a_n \quad \text{und} \quad b_{n \ 1} \quad \frac{c_{n \ 1}}{c_n} \ \frac{a_n b_1 \quad b_n a_1}{2} \quad b_n$$

zeigen. Wegen $c_{n \ 1} \ c_n \quad 1 \ 2$ ist das für $a_1 \quad 5$ klar. Es bleibt, die Fälle $a_1 \quad 1$ und $a_1 \quad 3$ zu betrachten. Die Bedingung $a_1 \quad 1$ impliziert wie im Beweis des Satzes $d \quad 5$, was wir ausgeschlossen hatten. Für $a_1 \quad 3$ erhalten wir

$$1 \quad N \ \eta \quad \frac{9 \quad b_1^2 d}{4} \qquad b_1^2 d \quad 9 \quad 4$$

Neben $d \quad 5$ ist hier auch $d \quad 13$ mit $b_1 \quad 1$ möglich. Diesen Fall mit Fundamentaleinheit $\eta \quad 3 \quad \sqrt{13} \quad 2$ müssen wir genauer betrachten, zu zeigen ist

$$a_{n \ 1} \quad \frac{c_{n \ 1}}{c_n} \ \frac{3a_n \quad 13b_n}{2} \quad a_n \quad \text{und} \quad b_{n \ 1} \quad \frac{c_{n \ 1}}{c_n} \ \frac{a_n \quad 3b_n}{2} \quad b_n$$

Wegen $c_{n \ 1} \ c_n \quad 1 \ 2$ reicht es

$$3a_n \quad 13b_n \quad 4a_n \qquad \text{bzw.} \qquad a_n \quad 3b_n \quad 4b_n \qquad \text{also} \ 13b_n \quad a_n \quad b_n$$

zu beweisen. Für $n \quad 1$ ist das wegen $a_1 \quad 3$ und $b_1 \quad 1$ trivial. Für $n \quad 2$ ist das mit den obigen Formeln äquivalent zu

$$13\frac{c_n}{c_{n \ 1}} \ \frac{a_{n \ 1} \quad 3b_{n \ 1}}{2} \quad \frac{c_n}{c_{n \ 1}} \ \frac{3a_{n \ 1} \quad 13b_{n \ 1}}{2} \quad \frac{c_n}{c_{n \ 1}} \ \frac{a_{n \ 1} \quad 3b_{n \ 1}}{2}$$

$$13a_{n \ 1} \quad 13 \ 3b_{n \ 1} \quad 3a_{n \ 1} \quad 13b_{n \ 1} \quad a_{n \ 1} \quad 3b_{n \ 1}$$

Letzteres ist wegen $a_{n \ 1} \ b_{n \ 1}$ erfüllt.

Wir betrachten noch die Spezialfälle $d = 5$ und $d = 13$, bei denen wir nicht gezeigt haben, dass alle Einheiten größer als eins in der Kettenbruchentwicklung von $\sqrt{d}$ auftreten. Die Kettenbruchentwicklungen sind

$$\sqrt{5} = 2\,\overline{4} \qquad \text{und} \qquad \sqrt{13} = 3\,\overline{1\ 1\ 1\ 1\ 6}$$

Wir erhalten für $d = 5$ die Werte

$$\begin{array}{ll} p_0 & 2 \\ q_0 & 1 \\ c_0 & 1 \end{array} \quad \text{also} \quad 2^2 - 5 \cdot 1^2 = -1$$

Hier finden wir also $2 + \sqrt{5} = \eta^3$ als erste Einheit durch die Kettenbruchentwicklung. Man kann also in diesem Fall nicht alle Einheiten von $\mathcal{O}_K$, $K = \mathbb{Q}(\sqrt{5})$, durch die Kettenbruchentwicklung finden.

Für $d = 13$ haben wir die Werte

$$\begin{array}{ll} p_0 & 3 \\ q_0 & 1 \\ c_0 & 4 \end{array} \quad \text{also} \quad 3^2 - 13 \cdot 1^2 = -4$$

Hier erhalten wir bereits im ersten Schritt die Fundamentaleinheit $\eta = 3 + \sqrt{13} = 2$. Insgesamt ergibt sich der folgende

Algorithmus zur Bestimmung der Fundamentaleinheit

1. Für $d = 5$ ist $\eta = 1 + \sqrt{5} = 2$, fertig.
2. Entwickle $\sqrt{d}$ als Kettenbruch und berechne p_n, q_n, c_n (letzteres nach Satz 10.19), solange bis das erste n mit $c_n \in \{1, -4\}$ gefunden wird. Die Fundamentaleinheit ist dann
$$\eta = \frac{p_n + q_n\sqrt{d}}{\sqrt{c_n}}$$

Wir wollen noch ohne Beweis beschreiben, wie die Einheitengruppe $\mathcal{O}_K$ bei einem beliebigen Zahlkörper aussieht. Bei den quadratischen Zahlkörpern mussten wir zwischen den reell– und imaginär–quadratischen Zahlkörpern unterscheiden, allgemeiner führen wir die folgenden Invarianten ein:

$$r_1 : = \#\{\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C}) \mid \sigma(K) \subset \mathbb{R}\}$$
$$r_2 : = \#\{\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C}) \mid \sigma(K) \not\subset \mathbb{R}\}/2$$

Man beachte, dass auch r_2 eine natürliche Zahl ist, weil mit jedem $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ auch sein komplex konjugiertes $\overline{\sigma}$ in $\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ liegt. Wir hatten bereits bemerkt, dass aus der Galois–Theorie $\dim_{\mathbb{Q}} K = \#\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ folgt, hier also

$$\dim_{\mathbb{Q}} K = r_1 + 2r_2$$

Satz 17.12 (Einheitensatz von Dirichlet) *Ist K ein Zahlkörper und r r wie oben, dann gilt*

$$\mathcal{O}_K \quad H \quad {}^{r\ r\ 1}$$

wobei H eine endliche zyklische Gruppe gerader Ordnung ist.

Beweis: Siehe Satz D.25 in Anhang D.

Die Menge H entspricht unter dem Isomorphismus den Elementen endlicher Ordnung in $\mathcal{O}_K$. Dies sind genau die Einheitswurzeln in dem Körper K. Denn einerseits erfüllt jedes Element x endlicher Ordnung eine Gleichung x^d 1 und ist somit eine Einheitswurzel, andererseits liegt jede Einheitswurzel x K mit x^d 1 bereits in $\mathcal{O}_K$, weil sie die Ganzheitsgleichung x^d 1 0 erfüllt. Da H mit 1 ein Element der Ordnung 2 enthält, muss H eine gerade Anzahl von Elementen haben.

Zum Abschluss des Abschnittes wollen wir uns der Teilbarkeitstheorie von $\mathcal{O}_K$ zuwenden. Im Allgemeinen ist $\mathcal{O}_K$ kein faktorieller Ring, besitzt aber eine für faktorielle Ringe typische Eigenschaft.

Lemma 17.13 *Jedes Element x 0 des Ringes der ganzen Zahlen eines Zahlkörpers kann in ein Produkt von irreduziblen Elementen zerlegt werden.*

Beweis: Wir führen eine Induktion nach dem Betrag der Norm von x. Für $N\ x$ 1 ist x eine Einheit. Sei also $N\ x$ 2 und x nicht irreduzibel. Dann können wir x zerlegen in x yz, wobei $y\ z$ keine Einheiten sind, also $N\ y$ $N\ z$ 2. Folglich ist $N\ x$ $N\ y$ $N\ z$, und nach Induktionsvoraussetzung können y und z — und somit auch x — in ein Produkt von irreduziblen Elementen zerlegt werden.

In dem Ring $\mathcal{O}_K$ muss eine Primzahl p nicht mehr prim sein, zum Beispiel zerlegt sich 2 in i als

$$2 \quad 1 \quad i \quad 1 \quad i$$

Satz 17.14 *Sei $\mathcal{O}_K$ der Ring der ganzen Zahlen eines quadratischen Zahlkörpers K $\mathbb{Q}\ \sqrt{d}$. Sei p eine Primzahl in .*

1. *Falls $p\ d$, dann ist p nicht prim in $\mathcal{O}_K$.*
2. *Die Primzahl 2 ist genau dann prim in $\mathcal{O}_K$, wenn d 5 mod 8.*
3. *Sei p 2d. Dann ist p genau dann prim in $\mathcal{O}_K$, wenn $\frac{d}{p}$ 1.*

Beweis: Wenn $p\ d$, dann kann p nicht prim sein, weil

$$p\ d \quad \sqrt{d}\ \sqrt{d} \quad \text{aber } p \quad \sqrt{d}$$

Dies zeigt auch, dass 2 nicht prim für d 0 mod 2 ist. Für d 3 mod 4 ist 2 im Ring $\sqrt{d}$ nicht prim, weil

$$2\ 1 \quad d \quad 1 \quad \sqrt{d} \quad 1 \quad \sqrt{d} \quad \text{aber } 2 \quad 1 \quad \sqrt{d}$$

Es bleibt für $d \equiv 1 \bmod 4$ die Zahl 2 im Ring $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ zu betrachten. Im Fall $d \equiv 1 \bmod 8$ zeigt

$$2 \mid \frac{1-d}{4} = \frac{1-\sqrt{d}}{2}\cdot\frac{1+\sqrt{d}}{2} \quad \text{aber} \quad 2 \nmid \frac{1+\sqrt{d}}{2}$$

dass auch hier 2 nicht prim ist.

Sei schließlich $d \equiv 5 \bmod 8$. Wir wollen zeigen, dass 2 dann prim ist. Gegeben seien $x, y \in \mathcal{O}_K$ mit $2 \mid xy$. Dann gilt $4 \mid N(2) = N(x)N(y)$. Wir nehmen ohne Einschränkung $2 \mid N(x)$ an. Falls x von der Form

$$x = \frac{a+b\sqrt{d}}{2} \quad \text{mit } a, b \text{ ungerade}$$

ist, dann ist $2 \mid N(x)$ äquivalent zu $8 \mid a^2 - b^2 d$. Da aber das Quadrat einer ungeraden Zahl 1 modulo 8 ist, ist dies unmöglich. Also muss x von der Form $x = a + b\sqrt{d}$ mit a, b sein. Die Teilbarkeit von $N(x)$ durch 2 bedeutet nun $2 \mid a^2 - b^2 d$. Da d ungerade ist, müssen a und b entweder beide gerade oder ungerade sein. In beiden Fällen ist $x \cdot 2$ ein Element von $\mathcal{O}_K$ und x daher durch 2 teilbar.

Bei Punkt 3 setzen wir zuerst $\left(\frac{d}{p}\right) = 1$ voraus. Die Zahl d ist also ein quadratischer Rest modulo p, d.h. es gibt ein a mit $a^2 \equiv d \bmod p$. p kann dann nicht prim in $\mathcal{O}_K$ sein, weil

$$p \mid a^2 - d = (a + \sqrt{d})(a - \sqrt{d}) \quad \text{aber} \quad p \nmid a \pm \sqrt{d}$$

Sei nun $\left(\frac{d}{p}\right) = -1$. Wir wollen zeigen, dass p prim ist. Seien $x, y \in \mathcal{O}_K$ mit $p \mid xy$. Es folgt $p^2 \mid N(p) \mid N(x)N(y)$. Wir nehmen ohne Einschränkung $p \mid N(x)$ an. Schreiben wir x als

$$x = \frac{a+b\sqrt{d}}{2} \quad \text{mit } a, b$$

dann bedeutet dies

$$p \mid \frac{a^2 - b^2 d}{4}$$

Insbesondere $p \mid a^2 - b^2 d$ oder äquivalent dazu $a^2 \equiv b^2 d \bmod p$. Falls $b \not\equiv 0 \bmod p$ ist, gilt $(ab^{-2})^2 \equiv d \bmod p$, im Widerspruch dazu, dass d kein quadratischer Rest ist. Somit ist $b \equiv 0 \bmod p$ und damit auch $a \equiv 0 \bmod p$. Folglich ist $x \equiv p \equiv a + b\sqrt{d} \equiv 2 \bmod p$ ein Element in $\mathcal{O}_K$, und daher ist p ein Teiler von x.

Falls $\mathcal{O}_K$ faktoriell ist, kann man seine Primelemente gut charakterisieren, wie wir es bereits in Abschnitt 2 bei dem Ring $\mathbb{Z}[i]$ gemacht haben. Zum besseren Verständnis dieser Charakterisierung und zur späteren Verwendung erwähnen wir noch das folgende allgemeine Lemma.

Lemma 17.15 *Sei $\mathcal{O}_K$ der Ring der ganzen Zahlen eines quadratischen Zahlkörpers K. Eine Primzahl p ist genau dann reduzibel in $\mathcal{O}_K$, wenn ein $x \in \mathcal{O}_K$ existiert mit $N(x) = p$.*

Beweis: Ist $p = N(x) = x\sigma(x)$, so ist dies bereits eine Zerlegung von p, weil x und $\sigma(x)$ wegen $N(x) = N(\sigma(x)) = p$ keine Einheiten sind.

Nehmen wir nun an, dass die Zahl p reduzibel in $\mathcal{O}_K$ ist. Sie kann also als $p = xy$ mit $x, y \notin \mathcal{O}_K$ und $N(x), N(y) \neq 1$ zerlegt werden. Dann folgt aus der Zerlegung der Norm als

$$p^2 = N(p) = N(x)N(y)$$

dass $N(x) = N(y) = p$.

Satz 17.16 *Sei $\mathcal{O}_K$ der Ring der ganzen Zahlen eines quadratischen Zahlkörpers $K = \mathbb{Q}(\sqrt{d})$. Weiter sei $\mathcal{O}_K$ faktoriell. Dann gilt:*

Ein Element $x \in \mathcal{O}_K$ ist genau dann prim in $\mathcal{O}_K$, wenn $N(x)$ prim in $\mathbb{Z}$ ist oder x assoziiert zu einer Primzahl $p \in \mathbb{Z}$ ist, die auch prim in $\mathcal{O}_K$ ist.

Insbesondere ist jedes Primelement in $\mathcal{O}_K$ ein Teiler einer Primzahl in $\mathbb{Z}$.

Beweis: Ist $N(x)$ eine Primzahl in $\mathbb{Z}$, so ist x irreduzibel in $\mathcal{O}_K$, da jede nicht–triviale Zerlegung von x eine nicht–triviale Zerlegung von $N(x)$ impliziert. Nehmen wir jetzt an, dass x prim in $\mathcal{O}_K$ ist. x teilt seine Norm $N(x) = x\sigma(x)$. Zerlegen wir die Norm $N(x)$ in $\mathbb{Z}$ in ihre Primfaktoren, so muss x auf Grund seiner Primeigenschaft einen dieser Faktoren teilen. Nennen wir diesen p. Falls x assoziiert zu p ist, sind wir fertig. Sonst existiert eine Nicht–Einheit y mit $p = xy$. Anwenden der Normfunktion liefert

$$p^2 = N(p) = N(x)N(y)$$

Da x, y keine Einheiten sind, folgt $N(x) = N(y) = p$.

Weil jedes Element seine Norm teilt, ist der Zusatz in der Aussage des Satzes trivial.

Um zu beweisen, dass $\mathcal{O}_K$ ein faktorieller Ring ist, müssen wir zeigen, dass jedes irreduzible Element von $\mathcal{O}_K$ prim ist. Der folgende Satz reduziert diesen Nachweis bei quadratischen Zahlkörpern auf die irreduziblen Elemente aus $\mathbb{Z}$.

Satz 17.17 *Für den Ring der ganzen Zahlen $\mathcal{O}_K$ eines quadratischen Zahlkörpers sind äquivalent:*

1. *$\mathcal{O}_K$ ist faktoriell.*
2. *Jede Primzahl $p \in \mathbb{Z}$, die irreduzibel in $\mathcal{O}_K$ ist, ist auch prim in $\mathcal{O}_K$.*
3. *Jede Primzahl $p \in \mathbb{Z}$ ist entweder prim in $\mathcal{O}_K$ oder es existiert ein $x \in \mathcal{O}_K$ mit $N(x) = p$.*

Beweis: Der erste Punkt impliziert den zweiten nach Definition. Wir zeigen nun den dritten unter Annahme des zweiten. Sei $p \in \mathbb{Z}$ nicht prim in $\mathcal{O}_K$, dann ist p nach Voraussetzung sogar reduzibel. Lemma 17.15 impliziert die Existenz eines $x \in \mathcal{O}_K$ mit $N(x) = p$.

Setzen wir schließlich Punkt 3 voraus und zeigen 1. Nach Lemma 17.13 müssen wir nur zeigen, dass jedes irreduzible Element $y \in \mathcal{O}_K$ auch prim ist. Sei $p \in \mathbb{Z}$ ein Primteiler von $N(y)$ über $\mathbb{Z}$. Wenn p auch prim in $\mathcal{O}_K$ ist, dann folgt aus $p \mid N(y) = y\sigma(y)$, dass $p \mid y$ oder $p \mid \sigma(y)$. Letzteres impliziert $p \mid \sigma(p) = \sigma^2(y) = y$. Also ist auf jeden Fall p ein Teiler von y. Da y irreduzibel ist, ist es damit assoziiert zu dem Primelement p in $\mathcal{O}_K$.

Falls p nicht prim in $\mathcal{O}_K$ ist, wählen wir $x \in \mathcal{O}_K$ mit $N(x) = p$. Wir wollen zeigen, dass x und damit auch $\sigma(x)$ prim ist. Da $x\sigma(x) = p$ ist, haben wir echte Inklusionen $\mathcal{O}_K p \subset \mathcal{O}_K x \subset \mathcal{O}_K$ und $\mathcal{O}_K / \mathcal{O}_K x$ ist ein echter Quotientenring von $\mathcal{O}_K / \mathcal{O}_K p$. Da $\mathcal{O}_K = \mathbb{Z}[\omega]$, $\omega = \frac{\Delta + \sqrt{\Delta}}{2}$ ist, ist der Ring $\mathcal{O}_K / \mathcal{O}_K p$ isomorph zu $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Der einzige echte nicht–triviale Quotientenring davon ist $\mathbb{Z}/p\mathbb{Z}$, wie man schon durch Betrachtungen auf Gruppenniveau sieht. Also ist $\mathcal{O}_K / \mathcal{O}_K x$ isomorph zum Körper $\mathbb{Z}/p\mathbb{Z}$. Nehmen wir nun an, dass x das Produkt wz von Elementen aus $\mathcal{O}_K$ teilt. Modulo $\mathcal{O}_K x$ — also im Körper $\mathcal{O}_K / \mathcal{O}_K x$ — heißt das

$$w \cdot z \equiv 0 \pmod{\mathcal{O}_K x}$$

Wegen der Nullteilerfreiheit eines Körpers muss $w \equiv 0 \pmod{\mathcal{O}_K x}$ oder $z \equiv 0 \pmod{\mathcal{O}_K x}$ sein. Also gilt $w \in \mathcal{O}_K x$ oder $z \in \mathcal{O}_K x$. Dies entspricht $x \mid w$ oder $x \mid z$ und x ist somit prim.

Jetzt können wir den Beweis ähnlich wie im Fall p prim abschließen. Aus $x \mid N(x) = p$ und $p \mid N(y) = y\sigma(y)$ folgern wir $x \mid y\sigma(y)$. Aus der Primeigenschaft von x folgt $x \mid y$ oder $x \mid \sigma(y)$. Letzteres impliziert $\sigma(x) \mid \sigma^2(y) = y$. Da y irreduzibel ist, ist y also zu einem der Primelemente x oder $\sigma(x)$ assoziiert.

Korollar 17.18 *Der Ring $\mathcal{O}_K$ der ganzen Zahlen eines imaginär–quadratischen Zahlkörpers $K = \mathbb{Q}(\sqrt{d})$, d quadratfrei, kann höchstens dann ein faktorieller Ring sein, wenn d prim oder -1 ist.*

Beweis: Wir nehmen an, dass das $d \neq -1$ nicht prim ist und wählen einen Primfaktor $p \neq 3$ von d. Nach Satz 17.14.1 ist p nicht prim in $\mathcal{O}_K$. Wir behaupten, dass p auch nicht im Bild der Normabbildung liegt. Dann ist $\mathcal{O}_K$ nach dem Satz kein faktorieller Ring.

Angenommen, es gibt ein $x \in \mathcal{O}_K$ mit $N(x) = p$. Schreiben wir $x = a + b\sqrt{d}$ mit $a, b \in \frac{1}{2}\mathbb{Z}$, so bedeutet dies

$$a^2 - db^2 = 4p$$

Wegen $p \mid d$ folgt $p \mid a^2$, also $p \mid a$. Weiter muss $b \neq 0$ sein. Dann ist aber wegen $a^2 \equiv db^2 \pmod{p}$ und $p \neq 3$ und $d \not\equiv 2 \pmod{p}$

$$N(x) = p \cdot \frac{a^2 - db^2}{4} \equiv 0 \pmod{p}$$

im Widerspruch zu $N(x) = p$.

Aufgabe 17.19 Zeigen Sie, dass der Ring der ganzen Zahlen des quadratischen Zahlkörpers $\mathbb{Q}(\sqrt{-13})$ nicht faktoriell ist.

Zusatzaufgaben

Aufgabe 17.20 Bestimmen Sie zwei Elemente mit Norm -1 im Ring $\mathcal{O}_K$ der ganzen Zahlen im quadratischen Zahlkörper $K = \mathbb{Q}(\sqrt{29})$. Die Kettenbruchentwicklung von $\sqrt{29}$ ist $[5; \overline{2, 1, 1, 2, 10}]$.

Aufgabe 17.21 Sei K ein Zahlkörper und $x \quad K$. Gilt die Implikation

$$N_K\ x \qquad 1 \quad x \quad \mathcal{O}_K ?$$

Beweisen Sie die Aussage oder geben Sie ein Gegenbeispiel an.

Aufgabe 17.22 Sei $K \quad \mathbb{Q}\ \sqrt{d}$ ein quadratischer Zahlkörper. Die Einheiten von $\mathcal{O}_K$ mit Norm 1 bilden eine Untergruppe von $\mathcal{O}_K$, die wir mit $\mathcal{O}_{K\ 1}$ bezeichnen. Zeigen Sie: Falls es eine Primzahl p gibt mit $p\ d$ und $p \quad 3 \bmod 4$, dann gilt $\mathcal{O}_K \quad \mathcal{O}_{K\ 1}$.

Aufgabe 17.23 Sei $p \quad 3$ eine Primzahl, $K \quad \mathbb{Q}\ \sqrt{p}$ und η die Fundamentaleinheit von $\mathcal{O}_K$. Zeigen Sie, dass die folgenden Aussagen äquivalent sind:

1. $N\ \eta \qquad 1$.
2. Die Gleichung $x^2 \quad py^2 \qquad 1$ ist ganzzahlig lösbar.
3. Die Gleichung $x^2 \quad py^2 \qquad 4$ ist ganzzahlig lösbar.
4. $p \quad 1 \bmod 4$.

Aufgabe 17.24 Bestimmen Sie mit Hilfe des Einheitensatzes von Dirichlet die Struktur der Einheitengruppe von folgenden Körpern:

1. $\mathbb{Q}\ \sqrt[3]{5}$.
2. $\mathbb{Q}\ \zeta$, wobei ζ eine primitive elfte Einheitswurzel ist.
3. $\mathbb{Q}\ \alpha$, wobei $\alpha \qquad$ eine Nullstelle des Polynoms $X^3 \quad X^2 \quad 5X \quad 1 \qquad X$ ist.

Aufgabe 17.25 Bestimmen Sie, welche der folgenden Elemente in $\sqrt{3}$ irreduzibel sind:

$$1 \quad 2\sqrt{3} \quad 2 \quad 37 \quad 17$$

18 Die Idealklassengruppe

Wir haben bereits gesehen, dass nicht alle Ringe ganzer Zahlen faktoriell sind, d.h. ihre Elemente besitzen keine eindeutige Zerlegung in ein Produkt irreduzibler Elemente. Betrachten wir noch einmal zwei Beispiele:

$$\begin{array}{llll} 6 & 2\ 3 & \sqrt{6}\ \sqrt{6} & \text{in } \sqrt{6} \\ 6 & 2\ 3 & 6\ \sqrt{30}\ 6\ \sqrt{30} & \text{in } \sqrt{30} \end{array}$$

Die eindeutige Zerlegbarkeit eines Elementes hat sich jedoch als so nützlich erwiesen, dass man sie gerne irgendwie retten will. Kroneckers Idee war nun, die Elemente des Ringes der ganzen Zahlen $\mathcal{O}_K$ nicht in $\mathcal{O}_K$ zu zerlegen, sondern in einem etwas größeren Ring R, so dass sich dort die Elemente eindeutig zerlegen lassen. Da man nur diese eindeutige Zerlegbarkeit der Elemente aus $\mathcal{O}_K$ verlangt, muss R nicht notwendig faktoriell sein. Wir betrachten dies in unseren Beispielen nur für die Zahl 6. Im ersten Beispiel wählen wir den Ring $\sqrt{2}\ \sqrt{3}\ \sqrt{6}$. Dort haben wir die irreduzible Zerlegung

$$6 \quad \sqrt{2}\ \sqrt{2}\ \sqrt{3}\ \sqrt{3}$$

Wir erhalten die bisherigen Zerlegungen durch Zusammenfassen von jeweils zwei Faktoren. Ebenso gilt im zweiten Beispiel im Ring $\sqrt{2}\ \sqrt{3}\ \sqrt{5}\ \sqrt{30}$

$$6 \quad \sqrt{2}^2\ \sqrt{3}^2 \quad \sqrt{6} \quad \sqrt{5} \quad \sqrt{6} \quad \sqrt{5}$$

wobei die letzten beiden Faktoren Einheiten sind. Wieder finden wir durch zusammenfassen von Faktoren die beiden bisherigen Zerlegungen.

Obwohl dieser Ansatz von Kronecker prinzipiell zum Erfolg führt, ist die Beteiligung eines schwer zu bestimmenden größeren Ringes unangenehm. Dedekind hatte die Idee, statt den Ring zu vergrößern, besser den Begriff der Zahl zu verallgemeinern. Dazu definierte er die Ideale, die heute in allen Bereichen der Mathematik bekannt sind.

Wir erinnern uns, dass auf der Menge der Ideale eines Ringes R durch

$$I\ J \qquad \sum_{i\ 1}^{n} x_i y_i\ n \qquad x_i \quad I\ y_i \quad J$$

eine Multiplikation definiert ist. Offensichtlich ist das Ideal R ein neutrales Element bezüglich dieser Operation.

Aufgabe 18.1 Zeigen Sie: Für zwei Ideale $I\ J$ gilt $I\ J \quad I \quad J$.

S. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie,*
DOI 10.1007/978-3-8348-8263-9_18,

Als erstes motivierendes Beispiel bemerken wir, dass eine Zerlegung eines Elementes x in

$$x \quad y_1 \quad y_n$$

einer Zerlegung des Hauptideals x in das Produkt der Hauptideale y_i entspricht

$$x \qquad y_1 \qquad y_n$$

Ein sofort auffallender Vorteil der Sprache mit den Idealen ist, dass zwei Elemente x und x' genau dann assoziiert sind, wenn $x \qquad x'$. Der lästige Zusatz „bis auf Assoziiertheit“ wird also in den Sätzen entfallen.

Die Rolle der Primzahlen wird von den Primidealen übernommen. Diese lassen sich durch drei äquivalente Eigenschaften charakterisieren:

Satz 18.2 *Ein echtes Ideal R heißt Primideal, wenn es eine der folgenden drei äquivalenten Bedingungen erfüllt:*

1. *Für alle $x\ y \quad R$ mit $x\ y$ folgt x oder y .*
2. *Für alle Ideale $I\ J \quad R$ mit $I\ J$ folgt I oder J .*
3. *R ist ein Integritätsring.*

Beweis: Zunächst zeigen wir, dass aus der ersten Bedingung die zweite folgt. Sei $I\ J$, aber J . Wir wählen $y \quad J$. Dann gilt für jedes $x \quad I$, dass $xy \quad I\ J$. Nach Voraussetzung folgt x . Dies zeigt I .

Für die umgekehrte Schlussfolgerung seien $x\ y \quad R$ mit xy gegeben. Dann folgt aus $x\ y$ bereits x oder y , d.h. x oder y .

Um die Eigenschaft 3 aus 1 abzuleiten, sei für $x\ y \quad R$

$$0 \quad x \qquad y \qquad xy \qquad \text{in } R$$

Dies bedeutet xy . Nach Bedingung 1 folgt x oder y und entsprechend $x \qquad 0$ oder $y \qquad 0$. R ist also nullteilerfrei.

Setzen wir schließlich die Nullteilerfreiheit von R voraus und zeigen die Bedingung 1. Seien $x\ y \quad R$ mit xy gegeben, dann ist

$$x \qquad y \qquad xy \qquad 0$$

Aus der Nullteilerfreiheit folgt $x \qquad 0$ oder $y \qquad 0$, d.h. x oder y .

Dass die Beziehung zwischen Primidealen und Primelementen sehr eng ist, zeigt auch das folgende Lemma.

Lemma 18.3 *Sei R ein Integritätsring. Ein Hauptideal p ist genau dann ein Primideal, wenn p prim in R ist.*

Beweis: Sei p prim in R und $x\ y\quad R$ mit $xy\qquad p$, d.h. $p\ xy$. Da p prim ist, folgt $p\ x$ oder $p\ y$. Dies ist äquivalent zu $x\quad p\qquad$ oder $y\quad p\qquad$. Das Ideal ist also ein Primideal.

Setzen wir dies nun voraus. Seien $x\ y\quad R$ gegeben mit $p\ xy$. Dies können wir als $x\quad y$ $p\qquad$ sehen. Da ein Primideal ist, folgt $x\qquad p$ oder $y\qquad p$, d.h. $p\ x$ oder $p\ y$. Das Element p ist daher prim.

Unter den Primidealen sind die maximalen besonders wichtig. Für sie haben wir zwei Charakterisierungsmöglichkeiten.

Satz 18.4 *Ein Ideal R heißt maximales Ideal, wenn es eine der folgenden äquivalenten Bedingungen erfüllt:*

1. *Für jedes Ideal I mit I folgt I R.*
2. *R ist ein Körper.*

Beweis: Das Ideal besitze die erste Eigenschaft. Da R ein Ring ist, müssen wir nur zeigen, dass jedes $0\quad x\qquad R$ ein inverses Element besitzt. Das Ideal $x\qquad$ ist echt größer als und somit bereits ganz R. Es gibt also ein $y\quad R$ und $z\qquad$ mit $1\quad xy\quad z$. Dies heißt

$$1\quad x\qquad y$$

und $y\qquad$ ist invers zu $x\quad$.

Setzen wir nun voraus, dass R ein Körper ist. Sei I ein Ideal mit $I\qquad$. Wir wählen $x\quad I$ und dazu ein $y\quad R$ mit $1\quad x\qquad y\qquad$. Es gibt also ein $z\qquad$ mit $xy\quad z\quad 1$. Wegen $x\quad I$ und $z\qquad I$ folgt $1\quad I$ und somit $I\quad R$.

Aus den jeweils letzten Bedingungen der Sätze 18.2 und 18.4 folgt insbesondere, dass jedes maximale Ideal ein Primideal ist.

Unser Ziel ist es zu zeigen, dass in dem Ring ganzer Zahlen eines Zahlkörpers jedes Ideal in ein bis auf Reihenfolge eindeutiges Produkt von Primidealen zerlegt werden kann.

Betrachten wir unter diesen Gesichtspunkten unsere Eingangsbeispiele erneut. Im Ring $\sqrt{\ 6}$ hatten wir die folgenden zwei Zerlegungen der 6 in irreduzible Elemente:

$$6\quad 2\ 3\qquad \sqrt{\ 6}\ \sqrt{\ 6}$$

Nach Satz 17.14 sind 2 und 3 nicht prim, somit sind nach Lemma 18.3 die Hauptideale 2 und 3 keine Primideale. Die obige Zerlegung legt nahe, die Ideale $_1:\quad 2\ \sqrt{\ 6}$ und $_2:$ $3\ \sqrt{\ 6}$ zu betrachten. Diese sind tatsächlich (maximale) Primideale, da $\sqrt{\ 6}\quad _1$ 2 und $\sqrt{\ 6}\quad _2\qquad 3$ Körper sind. Es gilt

$$_1\quad _1\quad 2\ \sqrt{\ 6}\quad 2\ \sqrt{\ 6}\qquad 4\ 2\sqrt{\ 6}\quad 6\qquad 2\quad \text{und}$$

$$_2\quad _2\quad 3\ \sqrt{\ 6}\quad 3\ \sqrt{\ 6}\qquad 9\ 3\sqrt{\ 6}\quad 6\qquad 3$$

Daher ist

$$6\qquad _1{}^2\quad _2{}^2$$

die eindeutige Zerlegung des Hauptideals 6 als Produkt von Primidealen.

Die Zerlegung $6 \quad \sqrt{6} \ \sqrt{6}$ erhalten wir, wenn wir das Produkt als

$$6 \quad {}_1 \ {}_2 \quad {}_1 \ {}_2$$

zusammenfassen, da

$${}_1 \ {}_2 \quad 2 \ \sqrt{6} \quad 3 \ \sqrt{6} \quad 6 \ 2\sqrt{6} \ 3\sqrt{6} \quad 6 \quad \sqrt{6}$$

Beim zweiten Beispiel hatten wir im Ring $\sqrt{30}$ die Zerlegungen

$$6 \quad 2 \ 3 \quad 6 \quad \sqrt{30} \ \ 6 \quad \sqrt{30}$$

Hier ist die Zerlegung des Hauptideals 6 als Produkt von Primidealen

$$6 \quad {}_1^2 \ {}_2^2 \quad \text{mit} \quad \begin{matrix} {}_1 & 2 \ 6 & \sqrt{30} & 2 \ 6 & \sqrt{30} & 2 \ \sqrt{30} \\ {}_2 & 3 \ 6 & \sqrt{30} & 3 \ 6 & \sqrt{30} & 3 \ \sqrt{30} \end{matrix}$$

Es gilt

$${}_1^2 \quad 2 \qquad {}_2^2 \quad 3 \qquad {}_1 \ {}_2 \quad 6 \ 2\sqrt{30} \ 3\sqrt{30} \ 30 \quad 6 \ \sqrt{30} \quad 6 \quad \sqrt{30}$$

Die Zerlegung von allen Idealen in ein Produkt von Primidealen ist jedoch nicht in jedem Ring möglich, sondern nur in den sogenannten Dedekind–Ringen. (Für die Eigenschaft noethersch siehe Anhang B.6.)

Definition 18.5 *Ein* Dedekind–Ring *ist ein ganz–abgeschlossener, noetherscher Integritätsring, in dem jedes Primideal* 0 *schon maximal ist.*

Satz 18.6 *Der Ring der ganzen Zahlen* $\mathcal{O}_K$ *eines Zahlkörpers K ist ein Dedekind–Ring.*

Beweis: Wir erinnern uns, dass $\mathcal{O}_K$ nach Satz 16.10 ganz–abgeschlossen ist. Wir zeigen nun, dass $\mathcal{O}_K$ noethersch ist. Wir wissen, dass $\mathcal{O}_K$ als additive Gruppe isomorph zu ^{n} mit $n \quad \dim \ K$ ist. Jedes Ideal $I \quad \mathcal{O}_K$ ist nach Aufgabe 6.23 als additive Gruppe isomorph zu ^{k} mit $k \quad n$. Insbesondere ist es bereits als abelsche Gruppe von endlich vielen Elementen erzeugt.

Sei 0 ein Primideal. Wir wollen zeigen, dass maximal ist. Nach Korollar 16.18 enthält eine ganze Zahl $m \quad 0$. Der Ring $\mathcal{O}_K \ m\mathcal{O}_K$ ist auf Grund des Isomorphismus $\mathcal{O}_K \quad ^n$ als abelsche Gruppe isomorph zu $^n \ m \ ^n \quad m \ ^n$. Insbesondere ist $\mathcal{O}_K \ m\mathcal{O}_K$ endlich. Dies muss wegen $m\mathcal{O}_K$ auch für den Quotienten $\mathcal{O}_K$ gelten. Als endlicher Integritätsring ist $\mathcal{O}_K$ bereits ein Körper, und somit ist maximal.

Bevor wir zeigen, dass jedes Ideal ein Produkt von Primidealen ist, erweitern wir noch den Begriff des Ideals und zeigen, dass wir dadurch eine Gruppenstruktur auf dieser Menge erhalten.

Definition 18.7 *Sei K der Quotientenkörper eines Integritätsrings R. Ein* gebrochenes Ideal *I ist eine Teilmenge von K ungleich* $\{0$ *, für die ein* $0 \quad r \quad R$ *existiert, so dass* $rI \quad R$ *ein Ideal in R ist.*

Ein gebrochenes Ideal $x : Rx$ *mit* $x \quad K$ *heißt* gebrochenes Hauptideal.

Ein Ideal $I \quad 0$ *in R bezeichnet man als* ganzes Ideal.

$\mathrm{I}\ R$ *bezeichnet die Menge der gebrochenen Ideale,* $\mathrm{H}\ R$ *die Menge der gebrochenen Hauptideale.*

Beispiel Jedes gebrochene Hauptideal x ist ein gebrochenes Ideal, weil $x \ ^1 x \quad R$.

Auf den gebrochenen Idealen definieren wir ein Produkt durch die gleiche Formel wie bei den ganzen Idealen. Dass das Produkt zweier gebrochener Ideale $I \ J$ wieder ein gebrochenes Ideal ist, ist eine einfache Überlegung: Nach Definition existieren $0 \quad r \ s \quad R$, so dass $rI \ sJ \quad R$ Ideale sind. Dann ist auch $rI \quad sJ \quad rs \ IJ \quad R$ ein Ideal und somit IJ ein gebrochenes Ideal.

Offensichtlich wird durch dieses Produkt die Menge $\mathrm{H}\ R$ zu einer abelschen Gruppe, in der das Inverse zum gebrochenen Hauptideal x durch $x^{\ 1}$ gegeben ist. Um zu zeigen, dass auch $\mathrm{I}\ R$ mit diesem Produkt zu einer Gruppe wird, müssen wir das Inverse eines gebrochenen Ideals konstruieren. Der Kandidat ist der folgende

$$I^{\ 1} : \{x \quad K \quad xI \quad R$$

Per Definition gilt dann $I^{\ 1} \ I \quad R$. Die Menge $I^{\ 1}$ ist auch wirklich ein gebrochenes Ideal. Um dies zu sehen, wählen wir ein $0 \quad r \quad I \quad R$. Dann ist $rI^{\ 1} \quad I \ I^{\ 1} \quad R$. Die Abgeschlossenheit von $I^{\ 1}$ — und damit auch von $rI^{\ 1}$ — bezüglich der Addition und der Multiplikation mit Elementen aus R ist klar, somit ist $rI^{\ 1}$ ein Ideal und $I^{\ 1}$ ein gebrochenes Ideal.

Der Beweis, dass in einem Dedekind–Ring die Gleichung $I^{\ 1} \ I \quad R$ gilt, erfordert etwas Vorbereitung.

Aufgabe 18.8 Berechnen Sie im Ring der ganzen Zahlen des Zahlkörpers $\mathbb{Q}\ \sqrt{2}$ die Inversen der Ideale

$$I \quad 3\ 1 \quad 2\sqrt{2} \qquad \text{und} \qquad J \quad 7\ 1 \quad 2\sqrt{2}$$

Lemma 18.9 *Sei R ein Dedekind–Ring und I ein ganzes Ideal. Dann gibt es maximale Primideale* $_1 \quad _n$ *mit*

$$_1 \quad _2 \quad _n \quad I$$

Das leere Produkt (also $n \quad 0$) ist nach Konvention R.

Beweis: Sei M die Menge der Ideale, die das Lemma nicht erfüllen. Wir müssen zeigen, dass M leer ist. Angenommen, dies ist nicht der Fall. In M gibt es ein Ideal I, das maximal bezüglich der Inklusion ist; denn sollte es zu jedem Ideal in M immer ein größeres geben, dann erhalten wir eine echt aufsteigende Kette von Idealen, im Widerspruch zu R noethersch.

Das Ideal I kann kein Primideal sein, weil Primideale das Lemma trivialerweise erfüllen. Wir können daher $x \ y \quad R \quad I$ wählen mit $xy \quad I$. Seien

$$I_x : \quad I \quad x \qquad \text{und} \qquad I_y : \quad I \quad y$$

Beide Ideale liegen nicht in der Menge M, weil sie größer als I sind und I maximal in M ist. Sie enthalten daher beide ein Produkt von Primidealen, also

$$_1 \quad _n \quad I_x \qquad \text{und} \qquad _1 \quad _m \quad I_y$$

Nun gilt

$$I_x \; I_y \quad I \; I \quad I \quad y \quad x \; I \quad xy \quad I$$

$$_1 \quad _n \; _1 \quad _m \quad I$$

Folglich ist I nicht in M, im Widerspruch zu unserer Annahme.

Satz 18.10 *Sei R ein Dedekind–Ring. Dann ist die Menge aller gebrochenen Ideale* I R *eine multiplikative, abelsche Gruppe.*

Insbesondere ist I^{-1} das zu einem gebrochenen Ideal I inverse Ideal.

Beweis: Es reicht zu zeigen, dass I^{-1} das Inverse zu I ist. Sei zunächst I ein ganzes Primideal. Wegen $R \quad I^{-1}$ gilt

$$I \quad I \; R \quad I \; I^{-1} \quad R$$

Weil das Primideal I in einem Dedekind–Ring auch ein maximales Ideal ist, gilt $I \; I^{-1} \quad I$ oder $I \; I^{-1} \quad R$. Das zweite ist unsere Behauptung, also müssen wir zeigen, dass das erste unmöglich ist.

Nehmen wir an, es gelte $I \; I^{-1} \quad I$. Wir wählen $0 \quad x \quad I$ und $_1 \qquad _n$ nach dem Lemma, so dass

$$_1 \quad _n \quad x \quad I$$

und n minimal unter diesen Bedingungen ist. Nach Satz 18.2 ist eines der Primideale $_i$ in I enthalten. Sei dies ohne Einschränkung $_1$. Da I und $_1$ maximale Ideale sind, gilt sogar $_1 \quad I$. Weiter gilt

$$_2 \quad _n \quad x$$

wegen der Minimalität von n.

Sei nun $y \quad _2 \quad _n \quad x$ und $z : \quad y \; x$. Durch diese Wahl ist $yI \quad y \; _1 \quad x$, also $zI \quad R$ und folglich $z \quad I^{-1}$. Das Element z kann nicht in R liegen, weil sonst $y \quad xz \quad x$ wäre, im Widerspruch zu unserer Wahl von y. Nach unserer Annahme $I^{-1} \; I \quad I$ haben wir jetzt die folgende Situation

$$zI \quad I^{-1} \; I \quad I$$

Wir zeigen nun ähnlich wie im Beweis von Satz 16.5, dass z ganz über R ist. Sei $e_1 \qquad e_m$ ein Erzeugendensystem von I über R. Dann gibt es $\lambda_{ij} \quad R$ mit

$$ze_i \quad \sum_{j \; 1}^{m} \lambda_{ij} e_j \qquad \text{für } i \quad 1 \qquad m$$

$$0 \quad \sum_{j \; 1}^{m} \delta_{ij} z \quad \lambda_{ij} \; e_j \quad \text{für } i \quad 1 \qquad m$$

$$0 \quad \det \; \delta_{ij} z \quad \lambda_{ij}$$

Die Entwicklung der Determinante liefert eine Ganzheitsgleichung vom Grad m für z. Somit ist z ganz über R und folglich $z \in R$ wegen der Abgeschlossenheit von R in seinem Quotientenkörper. Dies widerspricht dem eben gezeigten $z \notin R$. Insgesamt erhalten wir $I \cdot I^{-1} = R$.

Wir wollen jetzt $I \cdot I^{-1} = R$ für ein beliebiges ganzes Ideal I zeigen. Sei wieder M die Menge der Ideale, für die das nicht gilt und I ein bezüglich der Inklusion maximales Ideal in M. Dies ist in einem Primideal $\mathfrak{p}$ enthalten, welches selbst nach dem eben Gezeigten invertierbar ist. Für das Ideal $\mathfrak{p}^{-1}I$ gilt daher wegen $R \subset \mathfrak{p}^{-1}$

$$I \subset R \cdot I \subset \mathfrak{p}^{-1} \cdot I \subset \mathfrak{p}^{-1} \cdot \mathfrak{p} = R$$

insbesondere ist $\mathfrak{p}^{-1}I$ ein ganzes Ideal.

Wir wollen die Gleichheit $I = \mathfrak{p}^{-1}I$ ausschließen. Sollte sie gelten, so hätten wir $zI \subset I$ für jedes $z \in \mathfrak{p}^{-1}$. Wie oben sieht man, dass z ganz über R ist, also in R liegt. Es würde $\mathfrak{p}^{-1} \subset R$ und somit $\mathfrak{p}^{-1} = \mathfrak{p}$ im Widerspruch zu $\mathfrak{p}^{-1} \neq R$ folgen.

Wir haben also $I \subsetneq \mathfrak{p}^{-1}I$. Da I maximal in M ist, liegt $J := \mathfrak{p}^{-1}I$ nicht in M, erfüllt also $J \cdot J^{-1} = R$. Es folgt die Invertierbarkeit von I:

$$I = \mathfrak{p}^{-1}J^{-1} = \mathfrak{p}^{-1}I \cdot J^{-1} = J \cdot J^{-1} = R$$

Wir müssen noch zeigen, dass das Inverse von I das oben definierte Ideal I^{-1} ist. Nach Definition von I^{-1} folgt aus der vorangehenden Gleichung $\mathfrak{p}^{-1} \subset J^{-1} = I^{-1}$ und daher

$$R \subset I \cdot \mathfrak{p}^{-1}J^{-1} = I \cdot I^{-1} = R$$

somit gilt auch die Gleichheit $I \cdot I^{-1} = R$.

Zum Abschluss sei I ein beliebiges gebrochenes Ideal. Nach Definition existiert ein $x \neq 0$ im Quotientenkörper, so dass $xI \subset R$. Aus dem eben Gezeigten folgt $xI \cdot xI^{-1} \subset R$ und somit

$$I \subset x \cdot xI^{-1} \subset R$$

Das gebrochene Ideal ist also invertierbar und wie oben schließen wir, dass I^{-1} sein Inverses ist.

Satz 18.11 *Sei R ein Dedekind–Ring. Jedes ganze Ideal in R kann in ein Produkt von Primidealen zerlegt werden. Diese Zerlegung ist bis auf Reihenfolge eindeutig.*

Jedes gebrochene Ideal I kann als endliches Produkt

$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}(I)}$$

von ganzzahligen Potenzen von Primidealen geschrieben werden.

Die eindeutigen Exponenten $\nu_{\mathfrak{p}}(I)$ heißen Bewertungen *von I.*

Beweis: Sei I ein ganzes Ideal. Wir beweisen zunächst die Existenz der Primidealzerlegung. Falls es Ideale gibt, für die das nicht möglich ist, wählen wir unter diesen ein bezüglich der Inklusion maximales Ideal I. Sei $\mathfrak{p}_1$ ein (maximales) Primideal, welches I enthält. Aus $I \subset \mathfrak{p}_1$

folgt $_1{}^1I \quad R$. Das gebrochene Ideal $_1{}^1I$ ist also ganz. Es gilt $I \quad _1{}^1I$, weil aus $I \quad _1{}^1I$ wegen der Gruppeneigenschaft von I R die Gleichheit $_1{}^1 \quad R$, also $_1 \quad R$ folgen würde.

Für das Ideal $_1{}^1I$ gibt es wegen $_1{}^1I \quad I$ nach Wahl von I eine Produktzerlegung

$$_1{}^1I \quad _2 \quad _n$$

somit besitzt I die Produktzerlegung

$$I \quad _1 \quad _n$$

im Widerspruch zur Wahl von I.

Um die Eindeutigkeit der Produktzerlegung bis auf Reihenfolge einzusehen, starten wir mit zwei Zerlegungen eines ganzen Ideals

$$I \quad _1 \quad _n \quad _1 \quad _m$$

Aus $_1 \quad I \quad _1 \quad _m$ folgt nach der Primidealeigenschaft von $_1$, dass es ein $_i$ gibt mit $_1 \quad _i$. Sei dies ohne Einschränkung $_1$. Da $_1$ und $_1$ maximale Ideale sind, gilt bereits $_1 \quad _1$. Nach Satz 18.10 können wir jetzt $_1$ aus der Produktzerlegung kürzen. Wir erhalten

$$_2 \quad _n \quad _2 \quad _m$$

Nach endlich vielen Wiederholungen sehen wir, dass die $_i$ und $_j$ bis auf Reihenfolge gleich sind.

Betrachten wir jetzt den Fall eines gebrochenen Ideals I. Dann existiert ein $r \quad R \quad \{0$, so dass $rI \quad R$ ein ganzes Ideal ist. Falls $_1 \quad _n$ und $_1 \quad _m$ die Produktzerlegungen von rI bzw. r sind, dann hat I die Zerlegung

$$I \quad r \quad ^1 \; rI \quad _1{}^1 \quad _m{}^1 \quad _1 \quad _n$$

Zusammenfassen von gleichen Idealen zu einer Potenz führt zur gewünschten Gestalt in der Aussage des Satzes.

Solche Darstellungen müssen auch eindeutig sein. Haben wir zwei Darstellungen eines gebrochenen Ideals, dann multiplizieren wir beide so mit Potenzen der Primideale, die mit negativen Exponenten in den Darstellungen vorkommen, dass wir zwei Darstellungen eines ganzen Ideals J bekommen. Die Eindeutigkeit der Darstellung von J als Produkt von Primidealen impliziert, dass die Primidealzerlegungen des gebrochenen Ideals I bis auf Reihenfolge gleich sind.

Die Eigenschaften der Dedekind–Ringe, die in den letzten beiden Sätzen gezeigt wurden, charakterisieren diese, d.h. ein Integritätsring, für den die Folgerung des Satzes 18.10 oder 18.11 gilt, ist ein Dedekind–Ring [R2, 7.1].

Aufgabe 18.12 Sei $K \quad \mathbb{Q} \sqrt{d}$ ein quadratischer Zahlkörper. Zerlegen Sie die Hauptideale p , p , in Primideale.

Um in der multiplikativen Sprache der Produktzerlegung bleiben zu können, definiert man die Teilbarkeit von Idealen. Wir werden aber unmittelbar im Anschluss an die Definition sehen, dass die Definition nur eine andere Schreibweise für die Inklusion ist.

Definition 18.13 *Seien $I\ J$ zwei ganze Ideale in einem Integritätsring. Dann teilt das Ideal I das Ideal J (geschrieben als $I\ J$) genau dann, wenn es ein ganzes Ideal L gibt mit $I\ L\quad J$.*

Lemma 18.14 *Für zwei ganze Ideale in einem Dedekind–Ring gilt:*

$$I\ J\qquad\qquad J\quad I$$

Beweis: Wenn I das Ideal J teilt, gibt es ein ganzes Ideal L mit $I\ L\quad J$. Wegen $L\quad R$ folgt $I\quad J$. Setzen wir andererseits $J\quad I$ voraus, so ist $I^{\ 1}\ J\quad I^{\ 1}\ I\quad R$ ein ganzes Ideal. Die triviale Gleichheit

$$I\quad I^{\ 1}\ J\quad\ J$$

impliziert nun, dass I das Ideal J teilt.

Für die ganzen Ideale eines Dedekind–Ringes kann man jetzt durch die gleichen Formeln wie bei einem faktoriellen Ring den größten gemeinsamer Teiler und das kleinste gemeinsame Vielfache definieren. Man erhält auch analoge Aussagen:

Lemma 18.15 *Sind $I\quad\prod\ ^{n_\mathfrak{p}}\ J\quad\prod\ ^{m_\mathfrak{p}}$ zwei ganze Ideale in einem Dedekind–Ring, so gilt*

$$I\quad J\quad \text{ggT}\ I\ J\quad\prod^{\min\ n_\mathfrak{p}\ m_\mathfrak{p}}\qquad \textit{und}$$

$$I\quad J\quad \text{kgV}\ I\ J\quad\prod^{\max\ n_\mathfrak{p}\ m_\mathfrak{p}}$$

Sind $I\ J$ teilerfremd, so gilt

$$I\quad J\quad I\ J\qquad \textit{und}\qquad I\quad J\quad R$$

Beweis: Die Formeln

$$\text{ggT}\ I\ J\quad\prod^{\min\ n_\mathfrak{p}\ m_\mathfrak{p}}\qquad\text{und}\qquad\text{kgV}\ I\ J\quad\prod^{\max\ n_\mathfrak{p}\ m_\mathfrak{p}}$$

folgen genau wie Fall der faktoriellen Ringe.

Die Formel $I\quad J\quad \text{ggT}\ I\ J\quad : L$ leiten wir wie folgt ab: Die Teilbarkeiten $L\ I$ und $L\ J$ bedeuten $I\quad L$ und $J\quad L$. Also haben wir notwendigerweise $I\quad J\quad L$. Das Ideal $I\quad J$ ist per Definition das kleinste Ideal, das I und J enthält, und damit der größte gemeinsame Teiler der Ideale I und J.

Die Formel $I\quad J\quad \text{kgV}\ I\ J$ wird analog bewiesen. Für teilerfremde I und J, also $n\ m\quad 0$ für alle , ist

$$I\quad J\quad\prod^{\max\ n_\mathfrak{p}\ m_\mathfrak{p}}\quad I\ J$$

$$I\quad J\quad\prod^{\min\ n_\mathfrak{p}\ m_\mathfrak{p}}\quad\prod^{0}\quad R$$

Durch Untersuchung der Gruppe der invertierbaren Ideale kann man entscheiden, ob ein Dedekind–Ring faktoriell ist. Dafür machen wir zunächst die folgende erstaunliche Beobachtung:

Satz 18.16 *Sei R ein Dedekind–Ring. Dann ist R genau dann ein faktorieller Ring, wenn er ein Hauptidealring ist.*

Beweis: Nach Satz 2.18 sind Hauptidealringe immer faktoriell. Nehmen wir daher an, dass R faktoriell ist. Es reicht zu zeigen, dass jedes Primideal ein Hauptideal ist, denn dann ist jedes ganze Ideal als Produkt von Primidealen auch ein Hauptideal. Sei also 0 ein Primideal. Wir wählen ein 0 x und zerlegen es im Ring R in Primfaktoren

$$x \quad p_1 \quad p_n$$

Auf Idealebene bedeutet dies

$$x \quad p_1 \quad p_2 \quad p_n$$

Da ein Primideal ist, folgt p_i für ein geeignetes i. Nun ist auch p_i nach Lemma 18.3 ein (maximales) Primideal, so dass bereits p_i gelten muss. Insbesondere ist ein Hauptideal.

Um die Abweichung eines Dedekind–Ringes von einem Hauptidealring zu messen, definieren wir:

Definition 18.17 *Sei R ein Dedekind–Ring. Die* Idealklassengruppe Cl R *von R ist die Quotientengruppe*

$$\mathrm{Cl}\ R \quad \mathrm{I}\ R \quad \mathrm{H}\ R$$

Es ist üblich, statt in der Idealklassengruppe in der Gruppe der gebrochenen Ideale mit der entsprechenden Äquivalenzrelation zu rechnen. Für zwei gebrochene Ideale setzt man daher

$$\begin{array}{lll} I \quad J & & I\ \mathrm{H}\ R \quad J\ \mathrm{H}\ R \\ & & x \quad K \ : I \quad x \quad J \\ & & x \quad K \ : I \quad xJ \end{array}$$

Korollar 18.18 *Für einen Dedekind–Ring R sind äquivalent:*

1. *R ist faktoriell.*
2. *R ist ein Hauptidealring.*
3. Cl R $\{1$.

Beweis: Es bleibt die fast triviale Äquivalenz von 2 und 3 zu zeigen. Sei R ein Hauptidealring und I ein beliebiges gebrochenes Ideal. Dann existiert ein r R $\{0$, so dass rI R ein ganzes Ideal ist. Hier ist rI sogar ein Hauptideal x für ein x R. Folglich ist I $r^{1}x$ ein gebrochenes Hauptideal.

Setzen wir jetzt voraus, dass Cl R trivial ist. Sei 0 I R ein beliebiges Ideal. Dann ist I ein gebrochenes Hauptideal, also I x mit x K . Wegen I R gilt x R, somit ist I ein Hauptideal. Schließlich ist daher R ein Hauptidealring.

Im nächsten Abschnitt werden wir die Idealklassengruppe des Ringes der ganzen Zahlen eines quadratischen Zahlkörpers berechnen. Wir können also insbesondere für diese Ringe entscheiden, ob sie faktoriell sind oder nicht. Wir werden auch sehen, dass für diese Zahlkörper die Idealklassengruppe immer endlich ist.

Mit Hilfe der Minkowski–Gittertheorie kann man die Endlichkeit ganz allgemein für die Ringe ganzer Zahlen von Zahlkörpern beweisen. Wir wollen dies hier ohne Beweis als Satz festhalten, da es mit anderen Techniken bewiesen wird, als den bisher in diesem Buch benutzten.

Satz 18.19 *Die Idealklassengruppe eines Zahlkörpers ist endlich.*

Beweis: Siehe Satz D.20 in Anhang D.

Definition 18.20 *Die* Klassenzahl *h eines Zahlkörpers ist die Ordnung seiner Idealklassengruppe.*

Eine Konsequenz der Endlichkeit der Idealklassengruppe ist zum Beispiel, dass für jedes ganze Ideal I die Potenz I^h ein Hauptideal ist.

Zusatzaufgaben

Aufgabe 18.21 In $\sqrt{41}$ gilt die Faktorisierung $42 \quad 2\ 3\ 7 \quad 1\ \sqrt{41}\ 1\ \sqrt{41}$.

1. Zeigen Sie, dass $42 \quad 2\ 1\ \sqrt{41} \quad : \ _1$ ist und dass $_1$ ein Primideal ist.
2. Bestätigen Sie, dass $1\ \sqrt{41} \quad _1$ und somit $42 \quad \frac{2}{1}$ ist.
3. Finden Sie nun Primideale $_2 \ \frac{\prime}{2} \ _3 \ \frac{\prime}{3}$, so dass $42 \quad _i \ \frac{\prime}{i}$ für $i \quad 2\ 3$ gilt.
4. Leiten Sie daraus her, dass $\frac{2}{1}\ _2 \ \frac{\prime}{2}\ _3 \ \frac{\prime}{3} \quad 42$, und folgern sie letztlich, dass beide Ideale sogar gleich sind.

Wie hängt dieses Ergebnis mit den beiden möglichen Faktorisierungen von 42 zusammen?

Aufgabe 18.22 Zeigen Sie, dass jedes Ideal in einem Dedekindring von zwei Elementen erzeugt wird. Zeigen Sie dazu zunächst : Sind $I\ J$ Ideale in einem Dedekindring R, so gibt es ein $x \quad I$ mit $xI^{\ 1} \quad J \quad R$, also ggT $xI^{\ 1}\ J \quad 1$.

Aufgabe 18.23 Sei h die Klassenzahl eines Zahlkörpers K und I ein ganzes Ideal in $\mathcal{O}_K$. Zeigen Sie: I^h ist ein Hauptideal.

Aufgabe 18.24 Sei h die Klassenzahl eines Zahlkörpers K und I ein ganzes Ideal in $\mathcal{O}_K$. Zeigen Sie: Es gibt eine ganz–algebraische Zahl α, so dass I in der Körpererweiterung L $K\ \alpha$ die Gleichung $\mathcal{O}_L\ I \quad \alpha$ erfüllt.

19 Die Klassenzahl quadratischer Zahlkörper

Ziel des Abschnittes ist es, einen Algorithmus zu entwickeln, mit dem wir ein Repräsentantensystem der Idealklassengruppe eines quadratischen Zahlkörpers bestimmen können. Dazu bringen wir zunächst die ganzen Ideale von $\mathcal{O}_K$ in eine Normalform.

Hilfssatz 19.1 *Sei K ein quadratischer Zahlkörper mit Diskriminante Δ. Sei ω Δ $\sqrt{\Delta}$ 2. Dann ist jedes ganze Ideal I seines Ringes ganzer Zahlen $\mathcal{O}_K$ ω von der Form*

$$I \quad a \qquad b \quad c\omega \qquad \text{mit } a\ b\ c \qquad \text{und } a\ c \quad 0$$

Beweis: Da I $\mathcal{O}_K$ ein Ideal ist, ist auch J : I ein Ideal in . Nach Korollar 16.18 ist J 0. Da ein Hauptidealring ist, ist das Ideal J von einem Element 0 a erzeugt.

Betrachten wir nun die Projektion

$$\pi : \mathcal{O}_K \qquad \omega \qquad n \quad m\omega \qquad m$$

Das Bild von I unter π ist eine Untergruppe von , also gleich c für ein c . Aus $a\omega$ I folgt π $a\omega$ a 0 und somit c 0. Nach Definition von c gibt es ein b mit b $c\omega$ I. Zusammenfassend haben wir bisher

$$a \qquad b \quad c\omega \qquad I$$

Sei nun x I. Dann gibt es ein m mit π x mc. Die Projektion des Elementes

$$y : \quad x \quad m\ b \quad c\omega \quad I$$

ergibt 0, also liegt y in I a. Folglich ist y na für ein n . Wir erhalten somit für x die Darstellung

$$x \quad na \quad m\ b \quad c\omega \quad a \qquad b \quad c\omega$$

Das Lemma zeigt insbesondere nochmal, dass jedes Ideal 0 I $\mathcal{O}_K$ als abelsche Gruppe isomorph zu ^{2} ist. Nicht jede Kombination der $a\ b\ c$ ist im obigen Hilfssatz möglich, genauer sehen die Ideale wie folgt aus:

S. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie,*
DOI 10.1007/978-3-8348-8263-9_19,

Satz 19.2 *Sei K ein quadratischer Zahlkörper mit Diskriminante Δ. Dann sind die ganzen Ideale des Ringes $\mathcal{O}_K$ ganzer Zahlen von K die Mengen der Form*

$$I \quad ka \quad k\frac{b \quad \sqrt{\Delta}}{2}$$

mit a b k , wobei

$$a\ k \quad 0 \qquad \textit{und} \qquad 4a\,\Delta \quad b^2$$

Durch die zusätzlichen Bedingungen a k 0 und a b a wird die Darstellung eindeutig.

Beweis: Nach dem Hilfssatz können wir jedes Ideal schreiben als

$$\alpha \qquad \frac{\beta \quad k\sqrt{\Delta}}{2}$$

mit α β k , wobei $\beta \quad k\Delta \bmod 2$ und $\alpha \ k \quad 0$. Da dies immer eine abelsche Gruppe ist, bleibt für die Idealeigenschaft von I nur die Abgeschlossenheit bezüglich der Multiplikation mit Elementen aus $\mathcal{O}_K$ zu überprüfen. Tatsächlich braucht man nur die Multiplikation mit dem Element ω zu testen, weil dann für ein beliebiges $n \quad m\omega \quad \mathcal{O}_K$ gilt:

$$n \quad m\omega\ I \quad nI \quad m\omega I \quad I \quad mI \quad I$$

Da α und $\beta \quad k\sqrt{\Delta}$ 2 das Ideal als –Modul erzeugen, reicht es sogar aus, nur $\alpha\omega \quad I$ und $\beta \quad k\sqrt{\Delta}\ \omega\ 2 \quad I$ zu überprüfen.

Die Bedingung $\alpha\omega \quad I$ ist äquivalent zur Existenz von n m mit

$$\begin{aligned}
&\alpha\omega \quad n\alpha \quad m\frac{\beta \quad k\sqrt{\Delta}}{2}\\
&\alpha\Delta \quad \alpha\sqrt{\Delta} \quad 2n\alpha \quad m\beta \quad mk\sqrt{\Delta}\\
&2n\alpha \quad m\beta \quad \Delta\alpha \quad mk \quad \alpha\ \sqrt{\Delta} \quad 0\\
&2n\alpha \quad m\beta \quad \Delta\alpha \quad 0 \quad \text{und} \quad \alpha \quad km\\
&\beta \quad k\ \Delta \quad 2n \quad \text{und} \quad \alpha \quad km
\end{aligned}$$

Setzen wir a : m und b : $\Delta \quad 2n$, dann schreibt sich die Menge I als

$$I \quad ka \quad k\frac{b \quad \sqrt{\Delta}}{2} \qquad \text{mit } kb \quad k\Delta \bmod 2$$

und für jede Menge dieser Form gilt $ka\ \omega \quad I$.

Die Bedingung $\omega k\ b \quad \sqrt{\Delta} \quad 2 \quad I$ ist wieder äquivalent zur Existenz zweier Zahlen $n\ m$ mit

$$\omega k\frac{b \quad \sqrt{\Delta}}{2} \quad nka \quad mk\frac{b \quad \sqrt{\Delta}}{2}$$

$$\frac{\Delta \quad \sqrt{\Delta}}{2}\ \frac{b \quad \sqrt{\Delta}}{2} \quad na \quad m\frac{b \quad \sqrt{\Delta}}{2}$$

$$\Delta\ b \quad 1 \quad 4na \quad 2mb \quad b \quad \Delta \quad 2m\ \sqrt{\Delta} \quad 0$$

$$\Delta\ b \quad 1 \quad 4na \quad 2mb \quad 0 \quad \text{und} \quad b \quad \Delta \quad 2m \quad 0$$

$$4na \quad \Delta \quad b^2 \quad \text{und} \quad 2m \quad b \quad \Delta$$

Weil $4\ \Delta \quad b^2$ bereits $b \quad \Delta \bmod 2$ impliziert, ist die Existenz von n und m äquivalent zu $4a\ \Delta \quad b^2$.

Zum Schluss zeigen wir, dass wir zusätzlich die Bedingungen $a\ k \quad 0$ und $a \quad b \quad a$ stellen können und die Darstellung dadurch eindeutig wird. Die Vorzeichen von a und k können wir offensichtlich wechseln, ohne dass sich das Ideal ändert. Ist $b \quad 2an \quad b'$ mit $n\ b' \quad$ und $a \quad b' \quad a$, dann gilt:

$$I \quad ka \quad k\frac{b \quad \sqrt{\Delta}}{2} \quad ka \quad k\frac{b' \quad \sqrt{\Delta}}{2}$$

wegen

$$k\frac{b \quad \sqrt{\Delta}}{2} \quad kan \quad k\frac{b' \quad \sqrt{\Delta}}{2}$$

Um die Eindeutigkeit von k zu zeigen, brauchen wir nur zu bemerken, dass k das kleinste positive Element im Bild von I unter der Projektion

$$\pi : \mathcal{O}_K \quad \omega \quad n \quad m\omega \quad m$$

ist. Da ka der eindeutige positive Erzeuger von I ist, ist auch a eindeutig. Das Urbild von k unter der Projektion π ist

$$\pi^{\ 1}\ k \quad k\frac{b \quad \sqrt{\Delta}}{2} \quad ka \quad k\frac{b \quad 2a \quad \sqrt{\Delta}}{2}$$

Durch die Bedingung $a \quad b \quad a$ ist b in der Menge $b \quad 2a$ eindeutig bestimmt.

Wir möchten nun den Idealen eine Zahl zuweisen, um durch das Zählen dieser Zahlen die Klassenzahl zu bestimmen. Für die Definition einer solchen Funktion bietet es sich an, die Zahlen $a\ b\ k$ aus dem vorangehenden Satz zu benutzen. Ideale, die sich höchstens in der Zahl k unterscheiden, sind offensichtlich äquivalent. Wir werden daher im Folgenden nur Ideale mit $k \quad 1$ berücksichtigen. Ein weiteres Problem ist, dass insbesondere b nur auf relativ künstliche Weise eindeutig gemacht wurde. Um nicht an diese Wahl gebunden zu sein und auch nicht mit mehrdeutigen Funktionen arbeiten zu müssen, benutzen wir statt der Menge der ganzen Ideale die Menge der Erzeugerpaare

$$\mathcal{E} : \quad a\ \frac{b \quad \sqrt{\Delta}}{2} \quad a\ b \quad a \quad 0 \quad 4a\ \Delta \quad b^2$$

Wir definieren nun die offensichtlich injektive Abbildung

$$\xi : \mathscr{E} \qquad K \quad \mathbb{Q}\sqrt{\Delta} \qquad\qquad a\ \frac{b \quad \sqrt{\Delta}}{2} \qquad\qquad \frac{b \quad \sqrt{\Delta}}{2a}$$

Wir wollen jetzt von dieser injektiven Abbildung ξ zu einer injektiven Abbildung Ξ kommen, die auf der Idealklassengruppe definiert ist. Wenn wir in $\mathscr{E}$ die Erzeugerpaare identifizieren, die äquivalente Ideale beschreiben, müssen wir auch die entsprechenden Zahlen in K identifizieren. Auf welche Weise dies geschieht, wollen wir nun klären.

Wir behaupten, dass die Abbildung

$$\text{GL } 2 \qquad K \quad \mathbb{Q} \qquad K \quad \mathbb{Q} \qquad\qquad \begin{matrix}\alpha & \beta\\ \gamma & \delta\end{matrix} \quad x \qquad \frac{\alpha x \quad \beta}{\gamma x \quad \delta}$$

eine Operation von GL 2 auf $K \quad \mathbb{Q}$ ist. Sei

$$A \qquad \begin{matrix}\alpha & \beta\\ \gamma & \delta\end{matrix}$$

Die Abbildung ist wohldefiniert. Wegen $\alpha\delta \quad \beta\gamma \quad \det A \quad 0$ gilt nämlich

$$Ax : \quad \frac{\alpha x \quad \beta}{\gamma x \quad \delta} \qquad \frac{\alpha x \quad \beta \quad \gamma\sigma\, x \quad \delta}{N\ \gamma x \quad \delta} \qquad \frac{\alpha\gamma N\, x \quad \beta\delta \quad \alpha\delta x \quad \beta\gamma\sigma\, x}{N\ \gamma x \quad \delta}$$

$$\frac{\alpha\gamma N\, x \quad \beta\delta \quad \beta\gamma\, x \quad \sigma\, x \qquad \alpha\delta \quad \beta\gamma\, x}{N\ \gamma x \quad \delta}$$

$$\frac{\alpha\gamma N\, x \quad \beta\delta \quad \beta\gamma \mathrm{Sp}\, x \qquad \det A\, x}{N\ \gamma x \quad \delta}$$

Da $N\, x \quad N\ \gamma x \quad \delta \quad \mathrm{Sp}\, x \quad \mathbb{Q}$, aber $x \quad \mathbb{Q}$ ist, liegt Ax in $K \quad \mathbb{Q}$.

Für E_2 und sogar E_2 gilt $x \quad E_2 x \qquad E_2\ x$. Für eine weitere Matrix

$$B \qquad \begin{matrix}\varepsilon & \zeta\\ \eta & \vartheta\end{matrix}$$

aus GL 2 ist

$$BA\ x \qquad \begin{matrix}\alpha\varepsilon & \gamma\zeta & \beta\varepsilon & \delta\zeta\\ \alpha\eta & \gamma\vartheta & \beta\eta & \delta\vartheta\end{matrix} \quad x \quad \frac{\alpha\varepsilon \quad \gamma\zeta\, x \quad \beta\varepsilon \quad \delta\zeta}{\alpha\eta \quad \gamma\vartheta\, x \quad \beta\eta \quad \delta\vartheta}$$

gleich

$$B\ Ax \qquad B\frac{\alpha x \quad \beta}{\gamma x \quad \delta} \qquad \frac{\varepsilon\frac{\alpha x \quad \beta}{\gamma x \quad \delta} \quad \zeta}{\eta\frac{\alpha x \quad \beta}{\gamma x \quad \delta} \quad \vartheta} \qquad \frac{\alpha\varepsilon x \quad \beta\varepsilon \quad \gamma\zeta x \quad \delta\zeta}{\alpha\eta x \quad \beta\eta \quad \gamma\vartheta x \quad \delta\vartheta}$$

Wie üblich bezeichnet GL 2 $K \quad \mathbb{Q}$ den Orbitraum dieser Operation.

Satz 19.3 *Sei K ein quadratischer Zahlkörper mit Diskriminante Δ. Sei $\mathscr{E}$ die Menge aller Erzeugerpaare der ganzen Ideale des Ringes ganzer Zahlen $\mathcal{O}_K$. Dann induziert die Funktion*

$$\xi : \mathscr{E} \quad K \quad a \ \frac{b \quad \sqrt{\Delta}}{2} \qquad \frac{b \quad \sqrt{\Delta}}{2a}$$

eine injektive Abbildung

$$\Xi : \mathrm{Cl}\ K \qquad \mathrm{GL}\ 2 \qquad K \quad \mathbb{Q}$$

Ist τ im Bild von ξ, dann liegt bereits ganz GL 2 τ *im Bild von ξ.*

Beweis: Wir starten mit zwei Erzeugerpaaren, die wir als

$$a \ a\tau \quad \text{mit} \ \tau \quad \frac{b \quad \sqrt{\Delta}}{2a} \qquad \text{und} \qquad u \ u\tau' \quad \text{mit} \ \tau' \quad \frac{v \quad \sqrt{\Delta}}{2u}$$

mit den entsprechenden Bedingungen an die Variablen $a\ b\ u\ v$ schreiben. Seien

$$I : \quad a \qquad a\tau \qquad \text{und} \qquad J : \quad u \qquad u\tau'$$

die davon erzeugten Ideale.

I und J liegen genau dann in der gleichen Idealklasse, wenn es $0 \quad s\ r \quad \mathcal{O}_K$ gibt mit

$$rI \quad sJ$$

rI bzw. sJ haben als freie abelsche Gruppen vom Rang 2 die Erzeuger $ra\ ra\tau$ bzw. $su\ su\tau'$. Diese –Moduln sind genau dann gleich, wenn es eine Matrix

$$A \qquad \begin{matrix} \alpha & \beta \\ \gamma & \delta \end{matrix} \qquad \mathrm{GL}\ 2$$

gibt mit

$$\begin{matrix} su\tau' & & \alpha & \beta & & ra\tau \\ su & & \gamma & \delta & & ra \end{matrix}$$

$$su\tau' \quad ra\ \alpha\tau \quad \beta \quad \text{und} \quad su \quad ra\ \gamma\tau \quad \delta$$

$$\tau' \quad \frac{\alpha\tau \quad \beta}{\gamma\tau \quad \delta} \quad \text{und} \quad su \quad ra\ \gamma\tau \quad \delta$$

Somit liegen die Bilder zweier Erzeugerpaare von äquivalenten Idealen in dem gleichen GL 2 –Orbit von $K \quad \mathbb{Q}$. Wenn wir uns daran erinnern, dass jede Idealklasse ein ganzes Ideal enthält, bekommen wir auf offensichtliche Weise eine wohldefinierte Abbildung Ξ.

Zeigen wir nun die Injektivität von Ξ, d.h., die zwei Ideale $I\ J$ wie oben mit GL 2 τ GL 2 τ' müssen äquivalent sein. Falls

$$\tau' \quad \frac{\alpha\tau \quad \beta}{\gamma\tau \quad \delta}$$

ist, setzen wir

$$r : \quad u \qquad \mathcal{O}_K \qquad \text{und} \qquad s : \quad a\ \gamma\tau \quad \delta \quad I \quad \mathcal{O}_K$$

Folglich können wir die obige Rechnung umkehren und erhalten $rI \quad sJ$. Somit liegen I und J in der gleichen Idealklasse.

Zum Abschluss seien I und τ wie oben und $\tau' \quad \mathrm{GL}\ 2 \quad \tau$, d.h.

$$\tau' \quad \frac{\alpha\tau \quad \beta}{\gamma\tau \quad \delta} \qquad \text{für } A \qquad \begin{matrix} \alpha & \beta \\ \gamma & \delta \end{matrix} \qquad \mathrm{GL}\ 2$$

Wir wollen zeigen, dass auch τ' im Bild von ξ liegt. Wir setzen $c: \quad b^2 \quad \Delta \quad 4a$ und berechnen

$$\tau' \quad \frac{\alpha\ b \quad \sqrt{\Delta} \quad 2a\beta}{\gamma\ b \quad \sqrt{\Delta} \quad 2a\delta} \quad \frac{\alpha b \quad 2a\beta \quad \alpha\sqrt{\Delta}}{\gamma b \quad 2a\delta \quad \gamma\sqrt{\Delta}}$$

$$\frac{\alpha b \quad 2a\beta \quad \alpha\sqrt{\Delta} \quad \gamma b \quad 2a\delta \quad \gamma\sqrt{\Delta}}{N\ \gamma b \quad 2a\delta \quad \gamma\sqrt{\Delta}}$$

$$\frac{\alpha b \quad 2a\beta \quad \gamma b \quad 2a\delta \quad \alpha\gamma\Delta \quad \alpha\ \gamma b \quad 2a\delta \quad \gamma\ \alpha b \quad 2a\beta \quad \sqrt{\Delta}}{\gamma b \quad 2a\delta^{\ 2} \quad \gamma^2\Delta}$$

$$\frac{\alpha\gamma\ b^2 \quad \Delta \quad 2ab\alpha\delta \quad 2ab\beta\gamma \quad 4a^2\beta\delta \quad 2a\ \det A\ \sqrt{\Delta}}{\gamma^2\ b^2 \quad \Delta \quad 4a\ b\gamma\delta \quad a\delta^2}$$

$$\frac{2a\ 2c\alpha\gamma \quad b\alpha\delta \quad b\beta\gamma \quad 2a\beta\delta \quad 2a\ \det A\ \sqrt{\Delta}}{4a\ c\gamma^2 \quad b\gamma\delta \quad a\delta^2}$$

$$\frac{v \quad \sqrt{\Delta}}{2u}$$

mit

$$v: \quad \det A \quad 2a\beta\delta \quad b\alpha\delta \quad b\beta\gamma \quad 2c\alpha\gamma \qquad u: \quad \det A \quad a\delta^2 \quad b\gamma\delta \quad c\gamma^2$$

wobei wir $\det A \quad 1$ ausgenutzt haben. Also wäre τ' das Bild des Paares

$$u \ \frac{v \quad \sqrt{\Delta}}{2}$$

falls dies in $\mathscr{E}$ liegt. Dafür müssen wir noch zeigen, dass $u \quad 0$ ist und $4u \quad \Delta \quad v^2$. Da τ' nach Konstruktion in $K \quad \mathbb{Q}$ liegt, ist es wohldefiniert und sein Nenner ungleich 0, d.h. $u \quad 0$. Weiterhin hat die Matrix

$$B: \qquad \begin{matrix} 2a & b \\ b & 2c \end{matrix}$$

die Determinante $4ac \quad b^2 \quad \Delta$. Wir betrachten B als symmetrische Bilinearform und führen einen Basiswechsel mit Hilfe der Matrix

$$C: \qquad \begin{matrix} \beta & \delta \\ \alpha & \gamma \end{matrix} \qquad \mathrm{GL}\ 2$$

durch, die wir aus A durch Vertauschen der Spalten und Transponieren gewinnen:

$$C^T BC \quad \begin{matrix} \beta & \delta \\ \alpha & \gamma \end{matrix}^T \quad \begin{matrix} 2a & b \\ b & 2c \end{matrix} \quad \begin{matrix} \beta & \delta \\ \alpha & \gamma \end{matrix}$$

$$\begin{matrix} \beta & \alpha \\ \delta & \gamma \end{matrix} \quad \begin{matrix} 2a\beta & b\alpha & 2a\delta & b\gamma \\ b\beta & 2c\alpha & b\delta & 2c\gamma \end{matrix}$$

$$\begin{matrix} 2\,a\beta^2 & b\alpha\beta & c\alpha^2 & 2a\beta\delta & b\alpha\delta & b\beta\gamma & 2c\alpha\gamma \\ 2a\beta\delta & b\alpha\delta & b\beta\gamma & 2c\alpha\gamma & 2\,a\delta^2 & b\gamma\delta & c\gamma^2 \end{matrix}$$

$$\det A \quad \begin{matrix} 2w & v \\ v & 2u \end{matrix}$$

für $w \quad \det A \quad a\beta^2 \quad b\alpha\beta \quad c\alpha^2$. Es gilt daher wegen $\det C \quad 1$

$$\Delta \quad \det B \quad \det C^T BC \quad 4uw \quad v^2$$

und damit $4u \quad \Delta \quad v^2$.

Nun geht es darum, die Bildpunkte von Ξ zu zählen. Hier unterscheiden sich der reell– und imaginär–quadratische Fall etwas. Wir starten mit der Betrachtung des imaginär–quadratischen Falles, der auf eine gut untersuchte Situation zurückgeführt werden kann. Sei also $\Delta \quad 0$. Wir beobachten, dass für $a \quad 0$ die Bildpunkte von ξ immer in der oberen Halbebene

$$\mathbb{H} : \quad \{z \qquad \mathrm{Im}\, z \quad 0$$

landen. Wir beschränken uns daher auf das Betrachten dieser *positiven Erzeugerpaare* und setzen

$$\mathscr{E} \quad : \qquad a \; \frac{b \quad \sqrt{\Delta}}{2} \qquad \mathscr{E} \; a \quad 0 \qquad \text{sowie} \quad \xi \quad : \mathscr{E} \qquad \mathbb{H}$$

als Einschränkung von ξ.

Wir müssen in dieser Situation die Wirkung von GL 2 klären:

Hilfssatz 19.4 *Sei* z *und* $A \quad \begin{matrix} \alpha & \beta \\ \gamma & \delta \end{matrix}$ GL 2 . *Für*

$$z' : \quad \frac{\alpha z \quad \beta}{\gamma z \quad \delta}$$

gilt

$$\mathrm{Im}\, z' \quad \det A \; \frac{\mathrm{Im}\, z}{\gamma z \quad \delta^{\,2}}$$

Beweis: Wegen z ist $\gamma z \quad \delta$, insbesondere also ungleich Null. Für z' gilt

$$z' \quad \frac{\alpha z \quad \beta}{\gamma z \quad \delta} \; \frac{\gamma \bar{z} \quad \delta}{\gamma \bar{z} \quad \delta} \quad \frac{\alpha\gamma\, z^{\,2} \quad \beta\delta \quad \alpha\delta z \quad \beta\gamma\bar{z}}{\gamma z \quad \delta^{\,2}}$$

und somit für seinen Imaginärteil

$$\mathrm{Im}\, z' \quad \alpha\delta \quad \beta\gamma \frac{\mathrm{Im}\, z}{\gamma z \quad \delta^2} \quad \det A \frac{\mathrm{Im}\, z}{\gamma z \quad \delta^2}$$

Insbesondere besagt der Hilfssatz, dass für ein $\tau \quad \mathbb{H}$ der Punkt $A\tau$ genau dann in $\mathbb{H}$ liegt, wenn $\det A \quad 1$ gilt. Definieren wir

$$\mathrm{SL}\ 2 \quad : \quad \{A \quad \mathrm{GL}\ 2 \quad \det A \quad 1$$

dann erhalten wir unmittelbar als Korollar zum Satz:

Korollar 19.5 *Sei K ein imaginär–quadratischer Zahlkörper mit Diskriminante* Δ. *Sei* $\mathscr{E}$ *die Menge aller positiven Erzeugerpaare der ganzen Ideale des Ringes ganzer Zahlen* $\mathcal{O}_K$. *Dann induziert die Funktion*

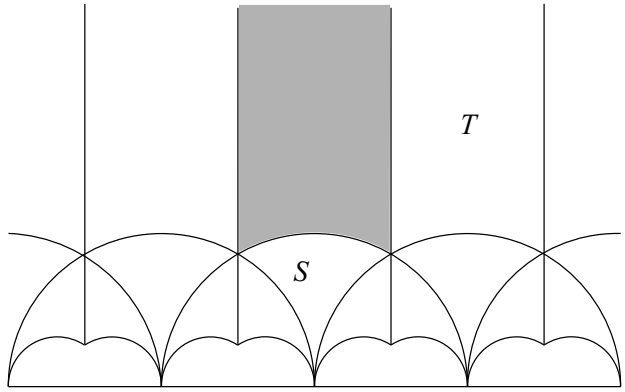
$$\xi \quad : \mathscr{E} \quad K \quad a \frac{b \quad \sqrt{\Delta}}{2} \quad \frac{b \quad \sqrt{\Delta}}{2a}$$

eine injektive Abbildung

$$\Xi \quad : \mathrm{Cl}\ K \quad \mathrm{SL}\ 2 \quad \mathbb{H}$$

Ist τ *im Bild von* ξ *, dann liegt bereits ganz* $\mathrm{SL}\ 2 \quad \tau$ *im Bild von* ξ .

Nun wollen wir den Orbitraum $\mathrm{SL}\ 2 \quad \mathbb{H}$ untersuchen. Dies macht man typischerweise, indem man einen *Fundamentalbereich* sucht. Dies ist eine abgeschlossene Menge $\mathbb{H}$, so dass jeder Orbit von $\mathrm{SL}\ 2 \quad \mathbb{H}$ einen Repräsentanten in hat, und falls ein Orbit mehr als einen Repräsentanten in hat, müssen alle Repräsentanten auf dem Rand von liegen. Das folgende Bild zeigt einige mögliche Fundamentalbereiche von $\mathrm{SL}\ 2 \quad \mathbb{H}$



Wir werden gleich zeigen, dass

$$: \quad z \quad \mathbb{H} \quad \mathrm{Re}\, z \quad \tfrac{1}{2} \quad z \quad 1$$

ein Fundamentalbereich ist. Die Eckpunkte von sind die Schnittpunkte der Geraden Rez 1 2 mit der oberen Hälfte des Einheitskreises, also ρ exp $2\pi i$ 3 und $\overline{\rho}$ exp πi 3 . Die anderen Fundamentalbereiche entstehen durch Anwenden der Elemente

$$T \quad \begin{matrix} 1 & 1 \\ 0 & 1 \end{matrix} \quad \text{und} \quad S \quad \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \quad \text{SL } 2$$

auf . Auf der oberen Halbebene ist

$$T : \mathbb{H} \quad \mathbb{H} \quad z \quad z \quad 1$$

die Translation um eins nach rechts und

$$S : \mathbb{H} \quad \mathbb{H} \quad z \quad 1 \; z$$

die Spiegelung am Einheitskreis gefolgt von einer Spiegelung an der imaginären Achse. Wir bemerken, dass S^2 E_2 trivial auf $\mathbb{H}$ operiert.

Wir werden es nicht weiter benutzen, aber es gilt:

Aufgabe 19.6 Zeigen Sie: Die Matrizen S und T erzeugen die Gruppe SL 2 .

Satz 19.7 *Die Menge ist ein Fundamentalbereich für* SL 2 $\mathbb{H}$ *Genauer gilt:*

1. *Jeder Orbit* SL 2 z, z $\mathbb{H}$, *hat einen Repräsentanten in* .
2. *Sind* z z' *zwei Repräsentanten eines Orbits, so gilt entweder*

$$\text{Re}z \quad \text{Re}z' \quad \tfrac{1}{2} \quad \textit{und} \quad z' \quad T\,z \quad \textit{oder} \quad z \quad T\,z'$$

oder

$$z \quad z' \quad 1 \quad \textit{und} \quad z' \quad S\,z$$

Beweis: Für Punkt 1 sei z $\mathbb{H}$ beliebig. Durch Anwenden von T und $T^{\,1}$ können wir den Realteil von z um eins erhöhen oder erniedrigen. Es gibt also ein n , so dass für z_1 : $T^n z$ gilt Rez_1 1 2. Ist z_1 1, so sind wir fertig. Wenn nicht, dann erfüllt die Zahl $S\,z_1$ die Bedingungen

$$S\,z_1 \quad 1 \quad \text{und} \quad \text{Im}S\,z_1 \quad \text{Im}z_1 \quad \text{Im}z$$

letztere nach Hilfssatz 19.4. Zu $S\,z_1$ suchen wir wie oben wieder ein n , so dass z_2 : $T^n S\,z_1$ einen Realteil vom Betrag kleiner gleich 1 2 hat. Falls jetzt z_2 1 gilt, sind wir fertig. Sonst ist

$$\text{Im}z_2 \quad \text{Im}S\,z_1 \quad \text{Im}z_1 \quad \text{Im}z$$

und wir wiederholen das Verfahren noch einige Male.

Es muss schließlich zum Erfolg führen, denn andernfalls erhalten wir eine unendliche Kette von z_i mit Re z_i 1 2 und

$$\text{Im}z \quad \text{Im}z_1 \quad \text{Im}z_2 \quad \text{Im}z_3$$

Die Imaginärteile dieser z_i berechnen sich aus z als

$$\mathrm{Im} z_i \quad \mathrm{Im} A_i\, z \quad \frac{\mathrm{Im} z}{\gamma_i z \quad \delta_i\ ^2} \qquad \text{für ein geeignetes } A_i \qquad \begin{matrix} \alpha_i & \beta_i \\ \gamma_i & \delta_i \end{matrix} \qquad \mathrm{SL}\ 2$$

Wegen $\mathrm{Im} z \quad \mathrm{Im} z_i$ muss

$$1 \quad \gamma_i z \quad \delta_i\ ^2 \quad \gamma_i^2\ \mathrm{Im} z\ ^2 \quad \gamma_i \mathrm{Re} z \quad \delta_i\ ^2$$

sein. Dies ist aber nur für endlich viele Wahlen von $\gamma_i\ \delta_i$ möglich. Folglich gibt es nur endlich viele Möglichkeiten für $\mathrm{Im} z_i$, im Widerspruch zur obigen unendlich langen Kette.

Bei Punkt 2 sei ohne Einschränkung $\mathrm{Im} z' \quad \mathrm{Im} z$. Sei weiter

$$A \qquad \begin{matrix} \alpha & \beta \\ \gamma & \delta \end{matrix} \qquad \mathrm{SL}\ 2 \qquad \text{so, dass} \quad z' \quad A\ z$$

Wieder mit dem Hilfssatz 19.4 erhalten wir

$$1 \quad \gamma z \quad \delta\ ^2 \quad \gamma^2\ \mathrm{Im} z\ ^2 \quad \gamma \mathrm{Re} z \quad \delta\ ^2$$

Nun ist $\mathrm{Im} z \quad \mathrm{Im} \rho \quad \sqrt{3}\ 2$, also $\mathrm{Im} z\ ^2 \quad 3\ 4$. Folglich ist $\gamma\ \delta \quad \{0 \quad 1$.

Ist $\gamma \quad 0$, so gilt wegen $1 \quad \det A \quad \alpha\delta \quad \beta\gamma \quad \alpha\delta$ bereits $\alpha \quad \delta \quad 1$. Weil E_2 trivial auf $\mathbb{H}$ operiert, können wir ohne Einschränkung $\alpha \quad \delta \quad 1$ annehmen. Dann ist

$$A \qquad \begin{matrix} 1 & \beta \\ 0 & 1 \end{matrix} \qquad T^\beta$$

eine Translation um β nach rechts. Es muss daher $\beta \qquad 1$ und $z' \quad z \quad 1$ gelten.

Ist $\delta \quad 0$, so können wir nach dem obigen Argument $\gamma \quad 1$ annehmen. Aus $\det A \quad 1$ folgt nun $\beta \qquad 1$, also

$$A \qquad \begin{matrix} \alpha & 1 \\ 1 & 0 \end{matrix} \qquad \text{und} \quad z' \quad \alpha \quad \frac{1}{z}$$

Insbesondere gilt

$$\mathrm{Im} z' \quad \mathrm{Im} \quad \frac{1}{z} \quad \frac{\mathrm{Im} \quad \overline{z}}{z\ ^2} \quad \frac{\mathrm{Im} z}{z\ ^2}$$

Nach Annahme war $\mathrm{Im} z' \quad \mathrm{Im} z$ und $z \quad 1$, so dass $z \quad 1$ und $\mathrm{Im} z' \quad \mathrm{Im} z$ folgt. Letztere Bedingung erlaubt, dieses Argument mit vertauschten Rollen von z und z' zu wiederholen. Folglich ist $z \quad 1 \quad z'$. Schließlich muss $\mathrm{Re} z' \qquad \mathrm{Re} z$ sein und daher

$$z' \qquad \overline{z} \qquad \frac{1}{z} \qquad S\ z$$

Der letzte Fall ist $\gamma \qquad \delta \quad 1$. Die Bedingung $1 \quad \gamma z \quad \delta\ ^2$ zusammen mit $\mathrm{Im} z\ ^2 \quad 3\ 4$ impliziert

$$1 \quad \mathrm{Im} z\ ^2 \quad \mathrm{Re} z \quad 1\ ^2 \quad \frac{3}{4} \quad \mathrm{Re} z \quad 1\ ^2$$

Wegen $\mathrm{Re} z \quad 1\ 2$ folgt $\mathrm{Re} z \quad 1\ 2$ und $\mathrm{Im} z\ ^2 \quad 3\ 4$. Somit ist $z \quad \rho$ und $z' \qquad \overline{\rho}$ oder umgekehrt. Auf dieses spezielle Paar treffen beide Möglichkeiten in der Aussage zu.

Nun sind wir in der Lage ein Repräsentantensystem für die Idealklassengruppe anzugeben.

Satz 19.8 *Sei K ein imaginär–quadratischer Zahlkörper mit Diskriminante Δ. Ein vollständiges Repräsentantensystem der Idealklassengruppe ist gegeben durch die Ideale*

$$I \quad a \quad \frac{b \quad \sqrt{\Delta}}{2} \qquad \text{für } a \qquad b$$

mit

$$4a \ \Delta \quad b^2 \quad b \quad a \quad \text{und} \quad 4a^2 \quad b^2 \quad \Delta$$

wobei im Falle der Gleichheit $b \quad a$ oder $4a^2 \quad b^2 \quad \Delta$ zusätzlich $b \quad 0$ gelten muss.

Beweis: Wir müssen überprüfen, welche positiven Idealerzeugerpaare unter der Abbildung ξ aus Korollar 19.5 in den Fundamentalbereich abgebildet werden. Das Idealerzeugerpaar

$$a \ \frac{b \quad \sqrt{\Delta}}{2}$$

wird auf

$$\tau : \quad \frac{b \quad \sqrt{\Delta}}{2a}$$

abgebildet. Diese Zahl liegt im Fundamentalbereich, falls

$$\mathrm{Re}\,\tau \qquad \frac{b}{2a} \qquad \frac{b}{2a} \quad \frac{1}{2} \qquad\qquad b \quad a$$

und

$$\tau \quad 1 \qquad\qquad \tau^{\,2} \quad \frac{b^2 \quad \Delta}{4a^2} \quad 1 \qquad\qquad 4a^2 \quad b^2 \quad \Delta$$

Im Falle der Gleichheit in einer der obigen Ungleichungen gibt es genau zwei Repräsentanten von $\mathrm{SL}\ 2 \quad \tau$ im Fundamentalbereich . Wir wählen davon denjenigen mit nicht–negativem Realteil.

Korollar 19.9 *Die Idealklassengruppe eines imaginär–quadratischen Zahlkörpers ist endlich.*

Beweis: Aus $b \quad a$ und $4a^2 \quad b^2 \quad \Delta$ folgt $4a^2 \quad a^2 \quad \Delta$ und $3a^2 \qquad \Delta \quad \Delta$. Daher sind nur endlich viele Werte für a möglich und wegen $b \quad a$ ebenso für b. Insgesamt erfüllen somit nur endlich viele Paare $a \ b$ die Bedingungen des Satzes, also es gibt nur endlich viele Idealklassen.

Beispiel Wir wollen die Klassenzahl des quadratischen Zahlkörpers $K \quad \mathbb{Q} \ \sqrt{\ 67}$ berechnen. Seine Diskriminante ist $\Delta \quad 67$. Wir müssen dafür die $a \quad , \ b$ bestimmen, die die Bedingungen des Satzes erfüllen. Aus

$$4a^2 \quad b^2 \quad \Delta \quad a^2 \quad \Delta$$

folgt $3a^2 \qquad \Delta \quad 67$, also $a \quad 4$. Wegen $b \quad a \quad 4$ und $4 \ \Delta \quad b^2$ muss $b \quad \{1 \ 3$ sein. Probieren wir diese beiden Möglichkeiten aus:

$$b \quad 1 : \quad 4a \ \Delta \quad 1^2 \qquad 68 \qquad\qquad a \ 17 \qquad\qquad a \quad 1$$

$$b \quad 3 : \quad 4a \ \Delta \quad 3^2 \qquad 76 \qquad\qquad a \ 19 \qquad\qquad a \quad 1$$

Also kommt wegen $b \quad a$ nur $a \quad 1$ und $b \quad 1$ in Frage. Weil dabei $a \quad b$ ist, ist nur $a \quad b \quad 1$ erlaubt. Das Repräsentantensystem von Cl K besteht daher nur aus dem Ideal

$$I \qquad \frac{1 \quad \sqrt{\quad 67}}{2} \qquad \mathcal{O}_K$$

$\mathcal{O}_K$ ist damit ein Hauptidealring.

Aufgabe 19.10 Bestimmen Sie die Klassenzahlen von $\mathbb{Q} \sqrt{\quad 74}$ und $\mathbb{Q} \sqrt{\quad 89}$.

Mit einem Computer ist es leicht, die Klassenzahlen der imaginär–quadratischen Zahlkörper durch diese Methode zu bestimmen. Die Klassenzahlen der kleinsten d sind:

d	1	2	3	5	6	7	10	11	13	14	15	17	19	21	22
h	1	1	1	2	2	1	2	1	2	4	2	4	1	4	2

d	23	26	29	30	31	33	34	35	37	38	39	41	42	43	46
h	3	6	6	4	3	4	4	2	2	6	4	8	4	1	4

d	47	51	53	55	57	58	59	61	62	65	66	67	69	70	71
h	5	2	6	4	4	2	3	6	8	8	8	1	8	4	7

Man erkennt, dass die Klassenzahl tendenziell mit d ansteigt. Schon Gauß vermutete, dass es zu jeder Klassenzahl nur endlich viele imaginär–quadratische Zahlkörper gibt. Dies wurde um 1930 bewiesen, jedoch zeigte der Beweis nicht, wie man zu einer gegebenen Klassenzahl diese imaginär–quadratischen Zahlkörper bestimmt. Für die Klassenzahl eins wurde dies durch Arbeiten von Heegner und Stark um 1969 getan. Sie bestimmten damit alle Hauptidealringe unter den Ringen ganzer Zahlen der imaginär–quadratischen Zahlkörper.

Satz 19.11 (Heegner–Stark) *Die imaginär–quadratischen Zahlkörper mit Klassenzahl* 1 *sind genau die mit Diskriminante*

$$3 \quad 4 \quad 7 \quad 8 \quad 11 \quad 19 \quad 43 \quad 67 \textit{ oder } 163$$

Bald darauf wurde der analoge Satz für die Klassenzahl 2 von Baker bewiesen. Goldfeld, Gross und Zagier entwickelten 1985 einen Algorithmus, mit dem das Problem auf eine endliche Rechnung zurückgeführt werden konnte [G]. Mittlerweile ist das Problem bis zur Klassenzahl 100 gelöst [W].

Aufgabe 19.12 Zeigen Sie, dass die imaginär–quadratischen Zahlkörper $K \quad \mathbb{Q} \sqrt{d}$ mit d $1 \quad 2 \quad 3 \quad 7 \quad 11$ euklidisch bezüglich der Norm $N \; a \quad b\sqrt{d} \quad a^2 \quad d\, b^2$ sind. Zeigen Sie weiter, dass kein imaginär–quadratischer Zahlkörper $\mathbb{Q} \sqrt{d}$ mit $d \quad 11$, insbesondere also $\Delta \quad 11$, euklidisch ist.

Kommen wir nun zu den reell–quadratischen Zahlkörpern. Hier schaffen wir es nicht, auf natürliche Weise in jeder Idealklasse ein bestimmtes Erzeugerpaar für ein bestimmtes Ideal auszuwählen. Wir werden hier in einem ersten Schritt eine endliche Menge $\mathscr{E}$ von Erzeugerpaaren auswählen, so dass jede Idealklasse zumindest eins der von ihnen erzeugten Ideale enthält. Im zweiten Schritt wollen wir dann entscheiden, welche der durch die Paare $\mathscr{E}$ erzeugten Ideale äquivalent sind.

Satz 19.13 *Sei K ein reell–quadratischer Zahlkörper mit Diskriminante Δ. In jeder Idealklasse gibt es ein Ideal, das ein Erzeugerpaar*

$$a \quad \frac{b \quad \sqrt{\Delta}}{2} \qquad a \qquad b \qquad \textit{und} \quad 4a \quad b^2 \quad \Delta$$

besitzt mit

$$a \quad b \quad a \quad c \qquad \textit{wobei} \quad c : \quad \frac{b^2 \quad \Delta}{4a}$$

Für dieses Paar gilt:

$$a \quad \frac{1}{2}\sqrt{\Delta} \qquad \textit{und} \qquad c \quad 0$$

Beweis: Sei ein beliebiges ganzes Ideal I gegeben. Nach Satz 19.2 besitzt es ein Erzeugerpaar

$$ka \quad k\frac{b \quad \sqrt{\Delta}}{2}$$

mit $k \quad a \quad 0$ und $\quad a \quad b \quad a$. Somit hat das äquivalente Ideal $\frac{1}{k}I$ das Erzeugerpaar

$$a \quad \frac{b \quad \sqrt{\Delta}}{2}$$

mit $\quad a \quad b \quad a$. Sei $c : \quad b^2 \quad \Delta \quad 4a$. Falls $a \quad c$ gilt, haben wir das gesuchte Erzeugerpaar gefunden. Für $a \quad c$ betrachten wir das äquivalente Ideal

$$\frac{b \quad \sqrt{\Delta}}{2a} I \qquad \frac{b \quad \sqrt{\Delta}}{2} \quad \frac{b^2 \quad \Delta}{4a} \qquad c \quad \frac{b \quad \sqrt{\Delta}}{2} \qquad a' \quad \frac{b' \quad \sqrt{\Delta}}{2}$$

$$\text{mit } a' : \quad c \quad b' \qquad b \bmod 2a' \text{ und } \quad a' \quad b' \quad a'$$

Nach Voraussetzung ist in diesem äquivalenten Ideal $a' \quad a$. Falls $a' \quad c'$ für $c' : \quad b'^2 \quad \Delta \quad 4a'$ gilt, haben wir jetzt das gesuchte Erzeugerpaar. Andernfalls wiederholen wir das Verfahren. Da bei jeder Wiederholung das a kleiner wird und wir a nur endlich oft verkleinern können, müssen wir nach endlich vielen Wiederholungen einen Punkt erreichen, wo $a \quad c$ gilt.

Dass c negativ ist, folgt aus

$$a \; c \quad b^2 \quad \Delta \quad 4ac \quad 4ac$$

Die Abschätzung $a \quad \sqrt{\Delta} \; 2$ ergibt sich jetzt durch

$$\Delta \quad \Delta \quad b^2 \qquad 4ac \quad 4a \; c \quad 4a^2$$

Korollar 19.14 *Die Idealklassengruppe eines reell–quadratischen Zahlkörpers ist endlich.*

Beweis: Es reicht zu bemerken, dass es nur endlich viele Ideale von dem im Satz beschriebenen Typ gibt. Das ist wegen

$$b \quad a \quad \frac{1}{2}\sqrt{\Delta}$$

unmittelbar klar.

Wir bezeichnen die Menge der durch Satz 19.13 beschriebenen Erzeugerpaare mit $\mathscr{E}$. Um die Klassenzahl zu bestimmen, reicht es nach Satz 19.3 herauszufinden, welche Elemente von $\xi \ \mathscr{E}$ im gleichen GL 2 –Orbit liegen. Um dies zu vereinfachen, werden wir zeigen, dass, wenn $\tau' \quad A\tau$ für $\tau \ \tau' \quad \xi \ \mathscr{E}$ und $A \quad$ GL 2 gilt, die Matrix A sehr speziell gewählt werden kann.

Zunächst beweisen wir, dass wir die unteren beiden Einträge als positiv annehmen dürfen.

Lemma 19.15 *Seien*

$$\tau \quad \frac{b \quad \sqrt{\Delta}}{2a} \quad \xi \ \mathscr{E} \qquad \textit{und} \qquad \tau' \quad \frac{v \quad \sqrt{\Delta}}{2u} \quad \xi \ \mathscr{E}$$

Es gelte

$$\tau' \quad \text{GL } 2 \quad \tau$$

Dann existiert eine Matrix

$$A \qquad \begin{matrix} \alpha & \beta \\ \gamma & \delta \end{matrix} \qquad \text{GL } 2$$

mit

$$\tau' \quad A\tau \qquad \textit{und} \qquad \gamma \ \delta \quad 0$$

Beweis: Sei

$$B \qquad \begin{matrix} \varepsilon & \zeta \\ \eta & \vartheta \end{matrix} \qquad \text{GL } 2$$

eine beliebige Matrix mit $\tau' \quad B\tau$. Die Idee ist nun eine Matrix $T \quad$ GL 2 zu suchen mit $\tau \quad T\tau$, so dass für ein k die unteren Einträge in BT^k positiv sind. Dann sind für $A \quad BT^k$ die Bedingungen im Satz erfüllt.

Falls $\eta \ \vartheta \quad 0$ sind, setzen wir $T \quad E_2$ und sind fertig. Für $\eta \ \vartheta \quad 0$ können wir $T \quad E_2$ benutzen. Es bleibt der Fall $\eta\vartheta \quad 0$, für den wir ein T und k suchen müssen, so dass das Produkt der unteren beiden Einträge in BT^k positiv ist.

Wir wählen eine Lösung $x \ y \quad ^2$ der Gleichung

$$x^2 \quad \Delta y^2 \quad 4 \quad \text{mit } x \quad y \quad 0 \bmod 2$$

zum Beispiel das Doppelte einer Lösung der Pellschen Gleichung (Satz 10.22). Wir setzen

$$T \qquad \begin{matrix} \frac{x \quad by}{2} & cy \\ ay & \frac{x \quad by}{2} \end{matrix} \qquad \text{wobei } c : \quad \frac{b^2 \quad \Delta}{4a}$$

Zeigen wir zuerst, dass $T\tau \quad \tau$ gilt:

$$T\tau \quad \frac{\frac{x \quad by}{2}\tau \quad cy}{ay\tau \quad \frac{x \quad by}{2}} \quad \frac{x \quad by \quad b \quad \sqrt{\Delta} \quad 4acy}{2a \; y \; b \quad \sqrt{\Delta} \quad x \quad by}$$

$$\frac{bx \quad b^2y \quad 4acy \quad x \quad by \; \sqrt{\Delta}}{2a \; x \quad y\sqrt{\Delta}}$$

$$\frac{bx \quad b^2y \quad 4acy \quad x \quad by \; \sqrt{\Delta} \; x \quad y\sqrt{\Delta}}{2aN \; x \quad y\sqrt{\Delta}}$$

$$\frac{bx^2 \quad by^2\Delta \quad b^2xy \quad 4acxy \quad xy\Delta \quad x^2 \quad y^2\Delta \; \sqrt{\Delta}}{2aN \; x \quad y\sqrt{\Delta}}$$

$$\frac{bx^2 \quad by^2\Delta \quad x^2 \quad y^2\Delta \; \sqrt{\Delta}}{2a \; x^2 \quad y^2\Delta} \quad \frac{b \quad \sqrt{\Delta}}{2a} \quad \tau$$

Sämtliche Einträge dieser Matrix T sind positiv. Für $ay \quad cy$ ist das klar. Wegen $x \; y \quad 0$ ist zumindest einer der Einträge $x \quad by \quad 2$ und $x \quad by \quad 2$ positiv. Aus

$$x \quad by \; x \quad by \quad x^2 \quad b^2y^2 \quad x^2 \quad \Delta y^2 \quad 4$$

folgt dann, dass auch der andere positiv sein muss.

Jetzt zeigen wir, dass das Produkt der unteren beiden Einträge in BT größer ist als in B. Das Produkt der unteren beiden Einträge in BT ist

$$P: \quad \frac{x \quad by}{2}\eta \quad ay\vartheta \qquad cy\eta \quad \frac{x \quad by}{2}\vartheta$$
$$cy\frac{x \quad by}{2}\eta^2 \qquad acy^2 \quad \frac{x^2 \quad b^2y^2}{4} \quad \eta\vartheta \quad ay\frac{x \quad by}{2}\vartheta^2$$

Den Koeffizienten von $\eta\vartheta$ formen wir wie folgt um:

$$acy^2 \quad \frac{x^2 \quad b^2y^2}{4} \qquad acy^2 \quad \frac{4 \quad \Delta y^2 \quad b^2y^2}{4}$$
$$1 \qquad ac \quad \frac{\Delta \quad b^2}{4} \quad y^2 \quad 1 \quad 2acy^2$$

und folglich

$$P \quad \eta\vartheta \quad \tfrac{1}{2} \quad cy \; x \quad by \; \eta^2 \quad 4acy^2\eta\vartheta \quad ay \; x \quad by \; \vartheta^2$$

$$\eta\vartheta \quad \tfrac{1}{2} \; \sqrt{\; cy \; x \quad by \; \eta^2} \quad \sqrt{ay \; x \quad by \; \vartheta^2}^{\;2}$$

$$\sqrt{\; acy^2 \; x^2 \quad b^2y^2 \; \eta^2\vartheta^2} \quad 2acy^2\eta\vartheta$$

$$\eta\vartheta \quad \sqrt{\; acy^2 \; 4 \quad 4acy^2 \; \eta^2\vartheta^2} \quad 2acy^2\eta\vartheta$$

$$\eta\vartheta \quad \sqrt{2acy^2\eta\vartheta^{\;2} \quad 4acy^2\eta^2\vartheta^2} \quad 2acy^2\eta\vartheta$$

$$\eta\vartheta$$

weil $4acy^2\eta^2\vartheta^2 \quad 0$ ist. Es gilt sogar $P \quad \eta\vartheta$, weil mindestens eine der beiden Ungleichungen echt ist. Für $\eta\vartheta \quad 0$ ist $4acy^2\eta^2\vartheta^2 \quad 0$ und damit die zweite Ungleichung echt. Im Fall $\eta\vartheta \quad 0$ ist entweder $\eta \quad 0$ oder $\vartheta \quad 0$, aber nicht beide zugleich, da B invertierbar ist. Damit ist offenbar die erste Ungleichung echt.

Wir haben gezeigt, dass das ganzzahlige Produkt der unteren beiden Einträge von B durch Rechtsmultiplikation mit T vergrößert wird, falls es nicht schon positiv ist. Analoges gilt damit für $BT \; BT^2 \quad$. Daher gibt es ein $k \quad$, so dass das Produkt in BT^k positiv wird.

Jetzt zeigen wir, dass wir die unteren beiden Einträge der Matrix A aus einer Kettenbruchentwicklung gewinnen können.

Satz 19.16 *Sei K ein reell–quadratischer Zahlkörper mit Diskriminante Δ. Seien*

$$\tau \quad \frac{b \quad \sqrt{\Delta}}{2a} \quad \xi \; \mathcal{O} \qquad \textit{und} \qquad \tau' \quad \frac{v \quad \sqrt{\Delta}}{2u} \quad \xi \; \mathcal{O}$$

Es gelte

$$a \quad u \qquad \textit{und} \qquad \tau' \quad \mathrm{GL}\ 2 \quad \tau$$

Dann existiert eine Matrix

$$A \qquad \begin{matrix} \alpha & \beta \\ \gamma & \delta \end{matrix} \qquad \mathrm{GL}\ 2 \qquad \textit{mit} \qquad \tau' \quad A\tau$$

so dass $\delta \;\; \gamma$ ein Näherungsbruch der Kettenbruchentwicklung von

$$\frac{b \quad \sqrt{\Delta}}{2a}$$

ist.

Beweis: Nach dem Lemma gibt es eine solche Matrix A mit der Bedingung $\gamma \; \delta \quad 0$ und $\tau' \quad A\tau$. Wir müssen also nur zeigen, dass $\delta \;\; \gamma$ für dieses A ein Näherungsbruch der Kettenbruchentwicklung ist. Nach der Rechnung am Ende des Beweises von Satz 19.3 gilt mit $c: \quad b^2 \quad \Delta \quad 4a$

$$u \quad \det A \quad c\gamma^2 \quad b\gamma\delta \quad a\delta^2$$

Wir betrachten zuerst den Fall $\det A \quad 1$. Dann gilt auf Grund der Voraussetzung $u \quad a$

$$\frac{1}{\gamma^2} \quad \frac{u}{a} \; \frac{1}{\gamma^2} \qquad \frac{\delta}{\gamma} \quad ^2 \quad \frac{b}{a} \; \frac{\delta}{\gamma} \qquad \frac{c}{a}$$

$$\frac{\delta}{\gamma} \quad \frac{b}{2a} \quad ^2 \quad \frac{4ac \quad b^2}{4a^2} \qquad \frac{\delta}{\gamma} \quad \frac{b}{2a} \quad ^2 \quad \frac{\Delta}{4a^2}$$

$$\frac{\delta}{\gamma} \quad \frac{b \quad \sqrt{\Delta}}{2a} \qquad \frac{\delta}{\gamma} \quad \frac{b \quad \sqrt{\Delta}}{2a}$$

Wegen $b \quad a \quad \sqrt{\Delta} \; 2$ ist der erste Faktor positiv. Weil das Produkt $u \quad a\gamma^2 \qquad 0$ ist, ist auch der zweite Faktor positiv. Dies nutzen wir, um den ersten Faktor abzuschätzen

$$\frac{\delta}{\gamma} \quad \frac{b \quad \sqrt{\Delta}}{2a} \qquad \frac{\delta}{\gamma} \quad \frac{b \quad \sqrt{\Delta}}{2a} \qquad \frac{\sqrt{\Delta}}{a} \quad \frac{\sqrt{\Delta}}{a} \quad 2$$

Daraus erhalten wir wiederum für den zweiten Faktor

$$0 \quad \frac{\delta}{\gamma} \quad \frac{b \quad \sqrt{\Delta}}{2a} \quad \frac{1}{2\gamma^2}$$

Nach Satz 10.20 ist somit $\delta \quad \gamma$ ein Näherungsbruch in der Kettenbruchentwicklung von b $\sqrt{\Delta} \quad 2a$.

Im Fall von $\det A \qquad 1$ führt man zunächst eine analoge Rechnung unter Ausnutzung von $0 \quad u \quad a \qquad c$ durch:

$$\frac{1}{\delta^2} \quad \frac{u}{c} \; \frac{1}{\delta^2} \qquad \frac{\gamma}{\delta}^{\,2} \quad \frac{b}{c} \; \frac{\gamma}{\delta} \qquad \frac{a}{c} \qquad \frac{\gamma}{\delta} \quad \frac{b \quad \sqrt{\Delta}}{2c} \qquad \frac{\gamma}{\delta} \quad \frac{b \quad \sqrt{\Delta}}{2c}$$

Die gleichen Argumente wie oben zeigen, dass $\gamma \; \delta$ ein Näherungsbruch von

$$\frac{b \quad \sqrt{\Delta}}{2c} \qquad \frac{2a \; b \quad \sqrt{\Delta}}{b^2 \quad \Delta} \qquad \frac{2a}{b \quad \sqrt{\Delta}} \qquad \frac{1}{\frac{b \quad \overline{\Delta}}{2a}}$$

ist. Bezeichen wir $b \quad \sqrt{\Delta} \quad 2a \quad 0$ mit x, dann ist $\gamma \; \delta \quad 0$ ein Näherungsbruch von $1 \; x$.

Zum Abschluss behaupten wir, dass die Näherungsbrüche von $1 \; x$ gerade die Inversen der Näherungsbrüche von x sind — mit der Ausnahme des bei x oder $1 \; x$ auftretenden Bruches 0. Dies beweist dann den Satz auch im Fall $\det A \qquad 1$.

Nach eventuellem Vertauschen von x und $1 \; x$ dürfen wir $x \quad 1$ annehmen. Die Zahl x hat dann eine Kettenbruchentwicklung

$$x \quad a_0 \; a_1 \; a_2 \qquad \text{mit } a_i$$

und folglich ist die Kettenbruchentwicklung von $1 \; x$

$$\frac{1}{x} \quad 0 \quad \frac{1}{x} \quad 0 \; x \quad 0 \; a_0 \; a_1 \; a_2$$

Die Näherungsbrüche $p_i \; q_i$ der Entwicklung von x sind bestimmt durch

$$\begin{matrix} p_i & p_{i\ 1} \\ q_i & q_{i\ 1} \end{matrix} \qquad \prod_{j\ 0}^{i} \begin{matrix} a_j & 1 \\ 1 & 0 \end{matrix}$$

und entsprechend die Näherungsbrüche $p'_i \; q'_i$ für $1 \; x$ durch

$$\begin{matrix} p'_i & p'_{i\ 1} \\ q'_i & q'_{i\ 1} \end{matrix} \qquad \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \prod_{j\ 1}^{i} \begin{matrix} a_{j\ 1} & 1 \\ 1 & 0 \end{matrix} \qquad \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \prod_{j\ 0}^{i\ 1} \begin{matrix} a_j & 1 \\ 1 & 0 \end{matrix}$$

$$\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \qquad \begin{matrix} p_{i\ 1} & p_{i\ 2} \\ q_{i\ 1} & q_{i\ 2} \end{matrix} \qquad \begin{matrix} q_{i\ 1} & q_{i\ 2} \\ p_{i\ 1} & p_{i\ 2} \end{matrix}$$

Es gilt also $p'_i \; q'_i \quad q_{i\ 1} \; p_{i\ 1}$, was wegen $p'_0 \; q'_0 \quad 0$ genau die Behauptung war.

Satz 19.17 *In der Situation des vorangegangenen Satzes sei die Kettenbruchentwicklung von*

$$\frac{b \quad \sqrt{\Delta}}{2a} \qquad a_0 \qquad a_n \overline{a_{n\ 1} \qquad a_{n\ h}}$$

Dann kann man sogar eine Matrix A finden, bei der $\delta \quad \gamma$ *einer der ersten* $n \quad h$ *Näherungsbrüche ist.*

Beweis: Seien p_i, q_i, ξ_i wie üblich durch die a_i definiert. Angenommen wir haben

$$A \qquad \begin{matrix} \alpha & \beta \\ q_m & p_m \end{matrix} \qquad \text{mit } m \quad n \quad h$$

Wir wollen A in ein Produkt zweier Matrizen aus GL 2 zerlegen,

$$A \quad BT \qquad \text{mit } B \qquad \begin{matrix} \alpha' & \beta' \\ q_{m\ h} & p_{m\ h} \end{matrix}$$

so dass $T\tau \quad \tau$ gilt. Denn dann ist

$$\tau' \quad A\tau \quad BT\tau \quad B\tau$$

Die Matrix B enthält jetzt in der unteren Zeile die p_i und q_i aus einem früheren Näherungsbruch. Nach einigen Wiederholungen erreichen wir p und q mit einem Index kleiner als $n \quad h$, wie gewünscht.

Wir wollen nun ein solches T mit

$$q_m \quad p_m \qquad q_{m\ h} \quad p_{m\ h} \quad T$$

konstruieren. Die Matrix B findet sich dann als $B \quad AT^{\ 1}$.

Aus der Periodizität des Kettenbruchs ergibt sich

$$x: \quad \frac{b \quad \sqrt{\Delta}}{2a} \qquad a_0 \qquad a_m \ \xi_m \qquad a_0 \qquad a_{m\ h} \ \xi_m$$

und damit

$$x \quad \frac{p_m\xi_m \quad p_{m\ 1}}{q_m\xi_m \quad q_{m\ 1}} \quad \frac{p_{m\ h}\xi_m \quad p_{m\ h\ 1}}{q_{m\ h}\xi_m \quad q_{m\ h\ 1}}$$

Nach Lemma 10.7 haben die Matrizen

$$\begin{matrix} p_m & p_{m\ 1} \\ q_m & q_{m\ 1} \end{matrix} \qquad \text{und} \qquad \begin{matrix} p_{m\ h} & p_{m\ h\ 1} \\ q_{m\ h} & q_{m\ h\ 1} \end{matrix}$$

beide Determinante 1, sind also invertierbar in GL 2 . Wir finden daher eine Matrix U GL 2 mit

$$\begin{matrix} p_m & p_{m\ 1} \\ q_m & q_{m\ 1} \end{matrix} \qquad U \qquad \begin{matrix} p_{m\ h} & p_{m\ h\ 1} \\ q_{m\ h} & q_{m\ h\ 1} \end{matrix}$$

Die Gleichung interpretieren wir jetzt so, dass 0 λ μ K existieren mit

$$\lambda \begin{matrix} x \\ 1 \end{matrix} \qquad \begin{matrix} p_m & p_{m\ 1} \\ q_m & q_{m\ 1} \end{matrix} \begin{matrix} \xi_m \\ 1 \end{matrix} \qquad \text{und}$$

$$\mu \begin{matrix} x \\ 1 \end{matrix} \qquad \begin{matrix} p_{m\ h} & p_{m\ h\ 1} \\ q_{m\ h} & q_{m\ h\ 1} \end{matrix} \begin{matrix} \xi_m \\ 1 \end{matrix}$$

Aus folgt

$$\lambda \begin{matrix} x \\ 1 \end{matrix} \qquad \mu U \begin{matrix} x \\ 1 \end{matrix}$$

Schreiben wir U als

$$U \qquad \begin{matrix} \varepsilon & \zeta \\ \eta & \vartheta \end{matrix}$$

so bedeutet dies

$$x \qquad \frac{\varepsilon x \quad \zeta}{\eta x \quad \vartheta}$$

Nun ist

$$\tau \qquad \frac{b \quad \sqrt{\Delta}}{2a} \qquad \sigma \qquad \frac{b \quad \sqrt{\Delta}}{2a} \qquad \sigma\ x$$

und daher

$$\tau \qquad \sigma\ x \qquad \frac{\varepsilon\sigma\ x \quad \zeta}{\eta\sigma\ x \quad \vartheta} \qquad \frac{\varepsilon \quad \sigma\ x \quad \zeta}{\eta \quad \sigma\ x \quad \vartheta} \qquad \frac{\varepsilon\tau \quad \zeta}{\eta\tau \quad \vartheta}$$

Dann gilt für die inverse Matrix

$$T^{\ 1} \qquad \frac{1}{\det T} \qquad \begin{matrix} \varepsilon & \zeta \\ \eta & \vartheta \end{matrix} \qquad \text{von } T \qquad \begin{matrix} \vartheta & \zeta \\ \eta & \varepsilon \end{matrix} \qquad \text{GL } 2$$

dass $T^{\ 1}\tau \quad \tau$ und somit $T\tau \quad \tau$.

Die Gleichung impliziert

$$p_m \quad \varepsilon p_{m\ h} \quad \zeta q_{m\ h}$$

$$q_m \quad \eta p_{m\ h} \quad \vartheta q_{m\ h}$$

also wie gefordert

$$q_m \quad p_m \qquad q_{m\ h} \quad p_{m\ h} \qquad \begin{matrix} \vartheta & \zeta \\ \eta & \varepsilon \end{matrix} \qquad q_{m\ h} \quad p_{m\ h} \quad T$$

Auf Grund der vorangehenden Sätze können wir uns bei der Suche nach einer Matrix A mit $\tau' \quad A\tau$ auf wenige mögliche γ δ beschränken. Nun legen diese beiden Einträge auch fast die restlichen Einträge von A fest. Nutzen wir zuerst $\det A \quad 1$.

Hilfssatz 19.18 *Seien* $\gamma\ \delta$ *mit* ggT $\gamma\ \delta$ 1 *sowie* e { 1 *gegeben. Man wähle ein* k *mit*

$$k\delta \quad e \bmod \gamma$$

und setze

$$l : \quad \frac{k\delta \quad e}{\gamma}$$

Dann sind die ganzzahligen Lösungen der Gleichung

$$\delta x \quad \gamma y \quad e$$

gegeben durch

$$x\ y \qquad k\ l \qquad \gamma\ \delta$$

Beweis: Ein $x\ y$ k $m\gamma\ l$ $m\delta$ mit m ist eine Lösung, weil

$$\delta\ k \quad m\gamma \quad \gamma\ l \quad m\delta \quad \delta k \quad \gamma l \quad \delta k \quad \delta k \quad e \quad e$$

Ist $x\ y$ eine beliebige Lösung, so gilt:

$$\delta x \quad \gamma y \quad e \quad \delta k \quad \gamma l \qquad \delta\ x \quad k \quad \gamma\ y \quad l$$

Wegen ggT $\gamma\ \delta$ 1 folgt

$$x \quad k \quad m\gamma \quad \text{und} \quad y \quad l \quad m\delta \qquad \text{für ein } m$$

Somit ist $x\ y$ von der behaupteten Gestalt.

Bezeichen wir den Näherungbruch, den wir im Augenblick für die Konstruktion von A verwenden wollen, mit $p\ q$, so gilt jetzt $\gamma \quad q$, $\delta \quad p$, $\alpha \quad k \quad mq$ und $\beta \quad l \quad mp$, also

$$A \qquad \begin{matrix} k & mq & l & mp \\ q & & p & \end{matrix}$$

Wir wollen ein solches A auf $\tau \quad b \quad \sqrt{\Delta} \quad 2a$ anwenden und setzen dafür $c : \quad b^2 \quad \Delta \quad 4a$. Dann erhalten wir ein $\tau' \quad v \quad \sqrt{\Delta} \quad 2u$ mit

$$u \quad \det A \quad cq^2 \quad bpq \quad ap^2$$

$$v \quad \det A \quad 2ckq \quad blq \quad 2alp \quad bkp \quad m \det A \quad 2cq^2 \quad 2bpq \quad 2ap^2$$

Durch die Einschränkungen $0 \quad u \quad a$ und $u \quad v \quad u$ werden hierbei die meisten noch möglichen Matrizen verworfen.

Beispiel Wir berechnen die Klassenzahl des Zahlkörpers $K \quad \mathbb{Q}\ \sqrt{15}$, indem wir dem von den Sätzen implizierten Algorithmus folgen. Die Diskriminante ist $\Delta \quad 60$. Wir bestimmen zuerst $\mathscr{E}$

$$\mathscr{E} \qquad a\ \frac{b \quad \sqrt{60}}{2} \qquad \begin{matrix} 1 \quad a \quad \sqrt{60}\ 2 \quad 3\ 9 \quad a \quad b \quad a \\ 4a\ 60 \quad b^2 \quad a \quad 60 \quad b^2 \quad 4a \quad : \quad c \end{matrix}$$

Aus $b \quad a \quad 3$ und $4\ 60 \quad b^2$ folgt $b \quad \{0\ 2$. Für $a \quad 1$ bleibt nur $b \quad 0$. Für $a \quad 2$ ist wegen $8\ 60 \quad b^2$ und $2 \quad b \quad 2$ nur $b \quad 2$ möglich. Im Fall $a \quad 3$ ist auch nur $b \quad 0$ möglich. Somit sieht $\mathscr{E}$ wie folgt aus:

$$\mathscr{E} \qquad 1 \ \frac{0 \quad \sqrt{60}}{2} \qquad 2 \ \frac{2 \quad \sqrt{60}}{2} \qquad 3 \ \frac{0 \quad \sqrt{60}}{2}$$

Nun müssen wir testen, welche der 3 Elemente von $\xi \ \mathscr{E}$ unter der Wirkung von GL 2 ineinander überführt werden. Wegen Satz 19.16 und 19.17 suchen wir nur nach Matrizen, die von großen a zu kleineren führen. Somit brauchen wir uns auch nur $a \ b \quad 2\ 2$ bzw. $a \ b \quad 3\ 0$ anschauen.

Betrachten wir zuerst $a \ b \quad 2\ 2$. Die Kettenbruchentwicklung von $2 \quad \sqrt{60} \quad 4$ ist $1\ \overline{2\ 3}$. Wir müssen also die ersten zwei Näherungsbrüche berücksichtigen. Diese sind:

$$\frac{1}{1} \quad \frac{3}{2}$$

Nun berechnen wir wie oben beschrieben alle Möglichkeiten für eine Matrix

$$A \qquad \begin{matrix} k & mq \\ q & p \end{matrix} \qquad \begin{matrix} l & mp \\ & p \end{matrix}$$

die eventuell die Elemente von $\xi \ \mathscr{E}$ aufeinander abbildet. Die folgende Tabelle fasst das zusammen:

p	q	$\det A$	k	l	u	v	v	$u\ u$
1	1	1	0	1	3			
1	1	1	0	1	3			
3	2	1	1	1	2	6 4		2
3	2	1	1	2	2			

Da fast überall u negativ ist oder $u \quad a \quad 2$ gilt, erhalten wir nur durch die dritte Zeile die Aussage, dass $2 \quad \sqrt{60} \quad 4$ im Orbit von $2 \quad \sqrt{60} \quad 4$ liegt. Dies ist natürlich trivial. Für $a \ b \quad 3\ 0$ sieht das anders aus: Die Kettenbruchentwicklung von $\sqrt{60} \quad 6$ ist $1\ \overline{3\ 2}$. Die ersten zwei Näherungsbrüche sind

$$\frac{1}{1} \quad \frac{4}{3}$$

und die Tabelle ist diesmal:

p	q	$\det A$	k	l	u	v	v	$u\ u$
1	1	1	0	1	2			
1	1	1	0	1	2	6 4		2
4	3	1	1	1	3	6 6		0
4	3	1	2	3	3			

Hier sehen wir aus der zweiten Zeile, dass $2 \quad \sqrt{60} \quad 4$ in dem gleichen GL 2 –Orbit liegt wie $\sqrt{60} \quad 6$. Die dritte Zeile liefert die triviale Bemerkung, dass $\sqrt{60} \quad 6$ im Orbit von $\sqrt{60} \quad 6$ ist. Somit ist die Klassenzahl von K gleich 2.

Aufgabe 19.19 Berechnen Sie die Klassenzahl von $\mathbb{Q} \ \sqrt{35}$.

Natürlich kann man jetzt mit einem Computer schnell die Klassenzahlen der reell–quadratischen Zahlkörper durch diese Methode bestimmen. Die Klassenzahlen der kleinsten d sind:

d	2	3	5	6	7	10	11	13	14	15	17	19	21	22	23
h	1	1	1	1	1	2	1	1	1	2	1	1	1	1	1

d	26	29	30	31	33	34	35	37	38	39	41	42	43	46	47
h	2	1	2	1	1	2	2	1	1	2	1	2	1	1	1

d	51	53	55	57	58	59	61	62	65	66	67	69	70	71	73
h	2	1	2	1	2	1	1	1	2	2	1	1	2	1	1

d	74	77	78	79	82	83	85	86	87	89	91	93	94	95	97
h	2	1	2	3	4	1	2	1	2	1	2	1	1	2	1

Wenn man diese Tabelle oder eine noch längere betrachtet, kann man vermuten, dass es unendlich viele reell–quadratische Zahlkörper mit Klassenzahl eins gibt. Dies ist jedoch noch nicht bewiesen, es ist sogar unbekannt, ob es überhaupt unendlich viele Zahlkörper mit Klassenzahl eins gibt.

Zusatzaufgaben

Aufgabe 19.20 Es seien τ $\frac{b \quad \overline{\Delta}}{2a}$ und τ' $\frac{v \quad \overline{\Delta}}{2u}$ mit Δ 0 und b a sowie c : $\frac{b^2 \quad \Delta}{4a}$. Nehmen Sie an, es existieren teilerfremde γ δ mit u $\gamma^2 c$ $\gamma\delta b$ $\delta^2 a$. Weiter seien

1. u quadratfrei und v 0 oder
2. ggT a u 1 und u prim.

Zeigen Sie nun, dass dann notwendigerweise τ' oder σ τ' im selben GL 2 –Orbit wie τ liegt.

Aufgabe 19.21 Seien a b c mit Δ b^2 $4ac$ 0 kein Quadrat. Zeigen Sie, dass die Zahlen

$$\frac{b \quad \sqrt{\Delta}}{2a} \qquad \frac{b \quad \sqrt{\Delta}}{2c} \qquad \frac{b \quad 2am \quad \sqrt{\Delta}}{2a} \quad \text{und} \quad \frac{b \quad 2cm \quad \sqrt{\Delta}}{4c \;\; a \quad bm \quad cm^2}$$

für m im gleichen GL 2 –Orbit liegen.

A Elementare Gruppentheorie

Definition A.1 *Eine Gruppe G ist eine Menge G zusammen mit einer Verknüpfung* : *G G G, so dass folgende Eigenschaften gelten:*

Die Verknüpfung ist assoziativ, d.h., für alle g h r G gilt g h r g h r.

Es gibt ein neutrales Element e G mit e g g e g für alle g G.

Für alle g G existiert ein inverses Element g ^{1} *G mit g g* ^{1} *g* ^{1} *g e.*

Die Gruppe G heißt abelsch (kommutativ), falls das folgende Axiom ebenfalls erfüllt ist:

Für alle g h G gilt g h h g.

Statt *g h* schreibt man oft *g h* (multiplikative Gruppe), kurz *gh*, oder *g h* (additive Gruppe). Die Schreibweise *g h* wird in der Regel nur bei abelschen Gruppen angewandt. Bei dieser Schreibweise wird das inverse Element wie üblich mit *g* statt *g* ^{1} bezeichnet. Für das neutrale Element schreibt man statt *e* in der Regel 0 bei additiven und 1 bei multiplikativen Gruppen.

Beispiel Die ganzen Zahlen bilden eine abelsche Gruppe mit der Addition.

Beispiel Die Restklassen von ganzen Zahlen modulo *n*, d.h. die Menge der Äquivalenzklassen unter der Relation *a b n a b* , bilden ebenfalls eine abelsche Gruppe, die mit *n* bezeichnet wird.

Beispiel Die bijektiven Abbildungen der Menge {1 2 3 *n* auf sich selbst bilden die sogenannte symmetrische Gruppe S_n, die *n*! Elemente besitzt. S_n ist nicht abelsch, falls *n* 3 ist.

Beispiel Die Menge der *m n*–Matrizen mit Koeffizienten in einer Gruppe *G* bildet eine additive, abelsche Gruppe unter der komponentenweisen Addition der Matrixeinträge. Diese Gruppe werden wir bei der Definition des Matrizenrings wiedersehen.

Beispiel Die Menge der invertierbaren *n n*–Matrizen mit Koeffizienten in den ganzen, rationalen oder reellen Zahlen bildet eine Gruppe unter Matrizenmultiplikation, die nicht abelsch ist für *n* 2. Sie wird mit GL *n* , GL *n* $\mathbb{Q}$ bzw. GL *n* bezeichnet. Haben die Matrizen Determinante 1, so werden die entsprechenden Gruppen mit SL 2 bezeichnet. Statt $\mathbb{Q}$ kann man auch Matrizen mit Koeffizienten in *n* oder einem beliebigen anderen Ring *R* betrachten. Ringe werden im nächsten Abschnitt behandelt.

Aus zwei (oder mehreren) Gruppen G_1 und G_2 kann man ein direktes Produkt G_1 G_2 konstruieren. Die zugrundeliegende Menge ist dabei das kartesische Produkt und die Verknüpfung durch *a b c d a c b d* gegeben.

S. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie,*
DOI 10.1007/978-3-8348-8263-9,

Definition A.2 *Sei G eine Gruppe. Eine Untergruppe H von G ist eine nicht–leere Teilmenge H G, so dass mit g h H auch gh 1 H liegt.*

Die Definition impliziert, dass H selbst eine Gruppe ist und insbesondere e in H liegt.

Definition A.3 *Ein Homomorphismus von Gruppen ist eine Abbildung* $\varphi : G_1 \quad G_2$ *mit* $\varphi\ e \quad e$ *und* $\varphi\ g \quad h \quad \varphi\ g \quad \varphi\ h$ *. Der Kern,* $\mathrm{Ker}\,\varphi$*, von* φ *ist die Menge aller* $g \quad G_1$ *mit* $\varphi\ g \quad e$*. Ein Isomorphismus* φ *ist ein bijektiver Homomorphismus.*

Der Kern von φ ist eine Untergruppe von G_1 — das Bild, $\mathrm{Im}\,\varphi$, eine Untergruppe von G_2.

Beispiel Ist $G \quad$, so bilden alle ganzen Zahlen, die Vielfache einer festen Zahl $n \quad$ sind, eine Untergruppe $H \quad n \quad$.

Beispiel Die Matrizen aus SL 2 , die im Kern der Abbildung

$$\mathrm{SL}\ 2 \qquad \mathrm{SL}\ 2 \quad n$$

liegen, bilden eine Untergruppe von SL 2 .

Ist eine beliebige Teilmenge S von G gegeben, so gibt es eine eindeutig bestimmte kleinste Untergruppe $S \quad G$, die alle Elemente aus S enthält. Sie ist eindeutig definiert als Durchschnitt aller Untergruppen H, die S enthalten. Ist G abelsch und S eine endliche Menge, so besteht S genau aus den endlichen Linearkombinationen $\{\sum_i^n{}_1 m_i s_i \quad s_i \quad S\ m_i \quad n$ von Elementen in S.

Eine wichtige Rolle bilden die Nebenklassen von G bzgl. einer Untergruppe H. Sie werden mit gH oder Hg bezeichnet und bestehen aus allen Vielfachen gh bzw. hg mit $h \quad H$. Nebenklassen g_1H und g_2H sind entweder disjunkt oder gleich, insbesondere ist $g_2 \quad g_1H$ äquivalent zu $g_2H \quad g_1H$. Die Nebenklassen bilden somit eine disjunkte Zerlegung von G.

Definition A.4 *Eine Untergruppe H einer Gruppe G heißt Normalteiler, falls gH Hg für alle Nebenklassen gilt.*

Man schreibt in diesem Fall $H \quad G$. Der Kern eines Homomorphismus ist immer ein Normalteiler. Ist G abelsch, so ist jede Untergruppe ein Normalteiler. Die wichtigste Eigenschaft eines Normalteilers ist die Möglichkeit Quotienten zu bilden.

Satz A.5 *Sei G eine Gruppe und H G ein Normalteiler. Dann existiert eine Gruppe G H und ein surjektiver Homomorphismus* $\varphi : G \quad G\ H$ *mit* $H \quad \mathrm{Ker}\,\varphi$.

Beweis: [Wü, Satz 1.38].

Die Elemente von $G\ H$ sind die Nebenklassen gH, und diese werden nach der Regel $gH \quad g'H \quad g\ Hg'\ H \quad g\ g'H\ H \quad gg'\ H$ unter Verwendung der Normalteilereigenschaft verknüpft.

Beispiel Ist $G \quad$ und $H \quad n \quad G$, so liefert diese Quotientenkonstruktion die Gruppe n .

Es gelten die folgenden sogenannten Isomorphiesätze:

Satz A.6 *Sei G eine (multiplikative) Gruppe.*

1. *Seien H K Normalteiler in G. Dann ist H Normalteiler in K, K H Normalteiler in G H, und es gilt G K G H K H .*

2. *Sei H G ein Normalteiler sowie K G eine Untergruppe. Dann ist K H ein Normalteiler in K, und es gilt K H K HK H.*

3. *Ist φ : G1 G2 ein Homomorphismus und H2 G2 ein Normalteiler, dann ist H1 φ 1 H2 G1 ein Normalteiler, und es gibt eine injektive induzierte Abbildung G1 H1 G2 H2. Sie ist ein Isomorphismus, falls φ surjektiv ist.*

Beweis: [Wü, Satz 1.40/1.41/1.42].

Der Index eines Normalteilers $H \quad G$ ist die Mächtigkeit der Quotientengruppe $G \quad H$, falls diese endlich ist.

Definition A.7 *Eine Operation einer Gruppe G auf einer Menge X ist eine Abbildung τ : G X X mit den Eigenschaften τ g τ h x τ gh x und τ e x x. Die Bahn (Der Orbit) eines Elementes x X ist die Menge aller τ g x mit g G.*

Die Menge der Bahnen bezeichnet man als Orbitraum $G \quad X$. Eine solche Operation wird auch Linksoperation genannt. Analog gibt es Rechtsoperationen mit einer Abbildung $\tau : X \quad G \quad X$, bei denen man die Menge der Bahnen mit $X \quad G$ bezeichnet. Häufig wird das τ in der Notation weggelassen, und man schreibt $gx : \quad \tau \; g \; x$ bei Linksoperationen und $xg : \quad \tau \; x \; g$ bei Rechtsoperationen.

Ist X eine endliche Menge mit n Elementen, so liefert eine solche Operation einen Homomorphismus $G \quad S_n$ von G in die symmetrische Gruppe, also die Bijektionen von X. Als Beispiel hat man die Operation von G auf sich selbst mit $\tau \; h \; g \quad hg$. Ist allgemeiner $H \quad G$ eine Untergruppe, so operiert H auf G ebenfalls durch $\tau \; h \; g \quad hg$, wobei $h \quad H$ und $g \quad G$ ist. Die Bahnen unter dieser Operation sind genau die Nebenklassen Hg. Operiert man von der rechten Seite, so ergeben sich die Nebenklassen gH.

Dies kann man anwenden, um nochmal den Index zu definieren. Der Index von H in G wird als Mächtigkeit einer Menge von Vertretern g für ein System von disjunkten Nebenklassen definiert. Die Notation für den Index ist $G : H$. Es gilt $G : \{e \quad \#G$ und $G : H \quad \#G \quad H$, falls H Normalteiler ist.

Satz A.8 *Sind G1 G2 G Untergruppen, so gilt*

$$G : G_1 \quad G : G_2 \quad G_2 : G_1$$

Beweis: [Wü, Satz 1.36].

Eine Gruppe G heißt zyklisch, wenn es ein $g \quad G$ gibt mit $g \quad G$. In diesem Fall ist die Abbildung $\varphi : \quad G \; m \quad g^m$ surjektiv, und G ist ein Quotient von . Der Kern von φ ist von der Form d , wobei d die Ordnung von g ist. Allgemeiner kann man die Ordnung ord$g$ eines Elements g einer Gruppe G als das kleinste d definieren mit $g^d \quad e$.

Satz A.9 (Lagrange) *In einer endlichen Gruppe G teilt die Ordnung eines jeden Elements g die Gruppenordnung #G.*

Beweis: [Wü, Satz 1.45].

Etwas allgemeiner gilt $G : H \quad \#G \ \#H$ für jede Untergruppe H von G. Durch einfache Überlegungen beweist man die folgenden Aussagen:

Satz A.10 *Sei G eine Gruppe und g G. Dann gilt:*

1. *Falls die Ordnung von g endlich ist, gilt: Die Ordnung von g ist genau dann d , wenn g^d e und $g^{d/p}$ e für alle Primteiler p von d ist.*
2. *Für jedes g G gilt*
$$\mathrm{ord}\, g^k \quad \frac{\mathrm{ord}\, g}{\mathrm{ggT}\ \mathrm{ord}\, g\ k}$$
3. *Ist G abelsch, dann gilt für alle a b G*
$$\mathrm{ord}\, ab \quad \mathrm{kgV}\ \mathrm{ord}\, a\ \mathrm{ord}\, b$$

Der Exponent einer endlichen Gruppe G ist die kleinste natürliche Zahl d mit $g^d \quad e$ für alle $g \quad G$. Der Exponent teilt immer die Gruppenordnung $\#G$.

B Elementare Ringtheorie

Definition B.1 *Ein Ring R ist eine Menge mit zwei assoziativen Verknüpfungen und , so dass folgende Gesetze gelten:*

R ist eine abelsche Gruppe mit neutralem Element 0.

R besitzt ein neutrales Element 1.

Für alle a b c R gelten die Distributivgesetze a b c ac bc sowie a b c ac bc.

Ist die Multiplikation abelsch, so nennt man R einen kommutativen Ring. Ein kommutativer Ring heißt Integritätsring, falls er keine Nullteiler hat, d.h. Elemente a b 0 mit ab 0. Ein Ring R ist ein Schiefkörper, falls jedes Element in R $\{0$ ein multiplikatives Inverses besitzt. Ein Körper ist ein kommutativer Schiefkörper. Eine Abbildung $\varphi : R_1$ R_2 zwischen Ringen ist ein Ringhomomorphismus, falls φ 1 1 gilt und φ mit und verträglich ist.

Jeder Ring R 0 enthält einen Unterring, der durch sukzessive Addition bzw. Subtraktion der 1 entsteht. Dieser ist entweder isomorph zu , falls die Summation niemals 0 ergibt, oder isomorph zu n , falls nach genau n Additionen 0 herauskommt. Man nennt n die Charakteristik von R und setzt sie 0, falls dieser Unterring ist. Ist R ein Integritätsring, so ist n eine Primzahl. Man schreibt n char R .

Beispiel Die ganzen Zahlen und die Restklassengruppen n bilden Ringe mit der üblichen Addition und Multiplikation.

Beispiel n n–Matrizen bilden einen Ring mit der komponentenweisen Addition und der Matrizenmultiplikation, der aber nicht kommutativ ist, falls n 2.

Beispiel Ist G eine abelsche Gruppe, so bilden die Endomorphismen von G einen Ring mit der durch φ ψ g : φ g ψ g gegebenen Addition und der Verknüpfung als Multiplikation. Der Gruppenring G ist ein weiterer Ring, der zu G assoziiert ist. Seine Elemente sind endliche Linearkombinationen $\sum_g a_g$ g mit a_g . Die Addition erfolgt formal, und die Multiplikation ist durch das Distributivgesetz motiviert:

$$\sum_g a_g \ g \qquad \sum_h b_h \ h \qquad \sum_r \ \sum_{gh \ r} a_g b_h \qquad r$$

Beispiel Der Polynomring $R\,X$ über einem Ring R ist wieder ein Ring und besteht aus den Elementen a_0 a_1X a_2X^2 a_nX^n für n $_0$ und a_i R. Die Addition erfolgt über die

S. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie,*
DOI 10.1007/978-3-8348-8263-9,

Addition der Vektoren $a_0 \quad a_n$, wobei verschieden lange Vektoren durch Nullen ergänzt werden. Die Multiplikation ist durch das Distributivgesetz gegeben:

$$\sum_{i \ 0}^{n} a_i X^i \qquad \sum_{j \ 0}^{m} a_j X^j \qquad \sum_{r \ 0}^{n \ m} \sum_{i \ j \ r} a_i b_j X^r$$

Der Grad eines Polynoms $f \quad a_0 \quad a_1 X \quad a_2 X^2 \quad a_n X^n \quad R\,X$ ist definiert als deg $f \quad n$, falls $a_n \quad 0$ ist. Ein besonderes Verfahren beim Betrachten von Polynomen ist das Abspalten von Nullstellen: Sei dazu $R \quad k$ ein Körper. Ist $f \quad k\,X$ und $\alpha \quad k$ mit $f\ \alpha \quad 0$, so kann man f schreiben als $f \quad X \quad \alpha\ g$ mit $g \quad k\,X$. Dies folgt durch Polynomdivision: Schreibe $f \quad X \quad \alpha\ g \quad h$ mit deg $h \quad$ deg $X \quad \alpha \quad 1$, also $h \quad k$ konstant. Wegen $f\ \alpha \quad 0$ folgt $h \quad 0$.

Beispiel Jeder endliche Integritätsring R ist ein Schiefkörper. Dies folgt, da die Multiplikation $R \quad R$ mit einem festen Element $\quad 0$ injektiv, also bijektiv sein muss.

Definition B.2 *Sei R ein Ring. Ein Links–Ideal I ist eine additive Untergruppe I von R, für die R I I gilt, d.h. r f I für alle r R und f I. Analog definiert man den Begriff des Rechtsideals durch I R R und ebenso zweiseitige Ideale.*

Insbesondere werden wir Ideale betrachten, die von mehreren Elementen $f_1 \quad f_m$ erzeugt werden und schreiben dafür

$$I \quad f_1 \quad f_m \qquad \sum_{i \ 1}^{m} r_i f_i \quad r_i \quad R$$

Ist $m \quad 1$, so nennen wir ein Ideal der Form $I \quad f$ ein Hauptideal.

Hat man ein zweiseitiges Ideal I gegeben, so kann man $R \ I$, die Nebenklassen unter der additiven Faktorgruppe, wieder als Ring auffassen. Auf Idealen kann man elementare Operationen bilden: Seien

$$IJ \qquad \sum_{i \ 1}^{n} a_i b_i \quad a_i \quad I \ b_i \quad J \ n$$

$$I \quad J \quad \{a \quad b \ \ a \quad I \ b \quad J$$

und $I \quad J$ der Durchschnitt. Dann gilt $I_1 \quad I_2 \ J \quad I_1 J \quad I_2 J$ sowie $IJ \quad I \quad J$.

Sei von nun an R ein kommutativer Ring. Dann ist jedes Links– oder Rechts–Ideal zweiseitig.

Definition B.3 *Ein echtes Ideal R ist ein Primideal, falls rs impliziert, dass r oder s . Mit anderen Worten: Das Komplement R ist eine multiplikativ abgeschlossene Menge von R. Ein Primideal heißt maximal, wenn für jedes Ideal I R mit I entweder I R oder I gilt.*

Satz B.4 *Ein Ideal I R ist ein Primideal genau dann, wenn R I ein Integritätsring ist. I ist maximal genau dann, wenn R I ein Körper ist. Jedes Ideal I R ist in einem maximalen Ideal enthalten.*

Beweis: Siehe Satz 18.2 und 18.4. Die letzte Aussage folgt, da jede total geordnete Menge von Idealen bezüglich eine kleinste obere Schranke, nämlich die Vereinigung, besitzt.

Definition B.5 *Ein R–(Links–)Modul M ist eine abelsche Gruppe M zusammen mit einer Abbildung : R M M (Skalarmultiplikation), die folgende Regeln erfüllt:*

1 *m* *m.*

r s m *rs m.*

ist bilinear, d.h. r s m r m s m und r m n r m r n.

Ein Untermodul N M ist eine additive Untergruppe, die abgeschlossen bezüglich der Skalarmultiplikation ist, d.h. R N N. Ein Morphismus von R–Moduln ist eine Abbildung f : M N, die mit Addition und Skalarmultiplikation in offensichtlicher Weise kommutiert.

Natürlich lässt man das meist weg.

Beispiel Jeder Ring *R* ist ein Modul über sich selbst. Die (Links)–Ideale in *R* sind genau die Untermoduln von *R*.

Ein Modul ist endlich erzeugt, falls es Elemente $m_1 \quad m_d$ gibt, so dass die Teilmenge $Rm_1 \quad Rm_d \quad M$, die alle Linearkombinationen der m_i enthält, bereits ganz *M* ist.

Definition B.6 *Ein R–Modul M ist noethersch, falls die aufsteigende Kettenbedingung für Untermoduln erfüllt ist: Jede aufsteigende Kette*

$$0 \quad M_0 \quad M_1 \quad M_2$$

von Untermoduln wird stationär, d.h. es gibt ein n, so dass $M_{n\ i}$ M_n für alle i 0. Da jeder Ring ein Modul über sich selbst ist, sind damit auch noethersche Ringe definiert.

Satz B.7 (Basissatz von Hilbert) *Ist R ein noetherscher Ring (z.B. ein Körper), so ist der Polynomring R k X1 Xn ebenfalls noethersch.*

Beweis: [Ku, Satz 2.3].

Satz B.8 *Ein R–Modul M ist noethersch genau dann, wenn jeder Untermodul N M endlich erzeugt ist oder wenn jede nicht–leere Menge von Untermoduln von M ein maximales Element besitzt.*

Beweis: [L, chap. VI, 1].

Sei $A \quad a_{ij}$ eine $n \quad n$–Matrix über einem kommutativen Ring *R*. Die Determinante von *A* über dem Ring *R* kann man mit Hilfe des Laplaceschen Entwicklungssatzes berechnen:

$$\det A \quad \sum_{j \ 1}^{n} \quad 1 \ ^{i \ j} a_{ij} \det A^{ij}$$

wobei A^{ij} die Streichungsmatrix ist, die entsteht, wenn man die i–te Zeile und j–te Spalte streicht. Definiert man die adjungierte (oder Cramersche) Matrix A mittels Transposition als

$$A_{ij} : \quad 1 \ ^{i \ j} \det A^{ji}$$

so folgt

$$AA \quad \det A \quad E_n$$

wobei E_n die $n \quad n$–Einheitsmatrix ist.

C Elementare Körpertheorie

Betrachten wir nun einen Körper K. Ist die Charakteristik von K gleich 0, so enthält K den Grundkörper $\mathbb{Q}$. Ist die Charakteristik $p \neq 0$, so enthält K den Grundkörper $\mathbb{F}_p$ p . In beiden Fällen ist K ein Vektorraum über dem Grundkörper $K_0 \cong \mathbb{Q}$ bzw. $K_0 \cong \mathbb{F}_p$. Die einfachsten Körper sind diejenigen, die endlich–dimensional über K_0 sind. Man spricht in diesem Fall von endlichen Körpererweiterungen. Im Fall $K_0 \cong \mathbb{Q}$ heißen solche Körpererweiterungen Zahlkörper, im Fall von $K_0 \cong \mathbb{F}_p$ endliche Körper. Die Zahlkörper können immer in die komplexen Zahlen eingebettet werden. Sind $K \subset L$ zwei Zahlkörper, so ist der Grad $L:K$ der Körpererweiterung die Dimension von L als K–Vektorraum. Für einen Körperturm $K \subset L \subset M$ gilt $M:K = M:L \cdot L:K$.

$K(\alpha) \subset L$ ist die kleinste Körpererweiterung von K, die α enthält. Ist $L = K(\alpha)$, so nennt man α ein primitives Element.

Satz C.1 (Satz vom primitiven Element) *Ist $K \subset L$ eine Erweiterung von Zahlkörpern, so gibt es ein $\alpha \in L$ mit $L = K(\alpha)$.*

Beweis: Eine solche Erweiterung ist nach Voraussetzung endlich und separabel, da K und L Erweiterungen von $\mathbb{Q}$ sind. Damit kann man [Wü, Satz 14.11] anwenden.

Sei $n = L:K$. Dann hat jedes $\beta \in L$ ein *Minimalpolynom* $m_\beta \in K[X]$ vom Grad n, das normierte (irreduzible) Polynom kleinsten Grades über K mit $m_\beta(\beta) = 0$. $K(\beta)$ ist isomorph zu $K[X]/(m_\beta)$. Das Minimalpolynom erzeugt das Ideal aller Polynome g mit $g(\beta) = 0$. Ist $L = K(\alpha)$, so hat das Minimalpolynom von α selbst den Grad $n = L:K$. Ist $K \subset K(\beta) \subset L$, so gilt $L:K = [K(\alpha):K(\beta)] \cdot [K(\beta):K]$, d.h. der Grad des Minimalpolynoms von β teilt $n = L:K$.

Betrachten wir nochmal eine Erweiterung $L = K(\alpha)$ von Zahlkörpern mit einem primitiven Element α. Das Minimalpolynom $f = m_\alpha$ von α hat n verschiedene Nullstellen α_i in , die Konjugierten von α. Jede Nullstelle α_i definiert einen eindeutigen Körpermonomorphismus σ_i von L nach mit $\sigma_i(\alpha) = \alpha_i$ und $\sigma_i|_K = \mathrm{id}_K$, nämlich

$$\sigma_i : K(\alpha) \to L \qquad \sum_{j=0}^{n-1} \lambda_j \alpha^j \mapsto \sum_{j=0}^{n-1} \lambda_j \alpha_i^j$$

Die Menge aller solchen K–linearen σ_i wird mit $\mathrm{Hom}_K(L)$ bezeichnet und hängt nicht von der Wahl von α ab.

Definition C.2 *Eine Erweiterung $K \subset L$ von Zahlkörpern heißt galoissch, wenn jedes $\sigma \in \mathrm{Hom}_K(L)$ bereits ein Automorphismus von L ist. Die* Galois–Gruppe $\mathrm{Gal}(L/K)$ *ist die Gruppe der Automorphismen* $\mathrm{Aut}_K(L)$ *von L, die K festlassen.*

S. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie,*
DOI 10.1007/978-3-8348-8263-9,

Nach Wahl eines primitiven Elements $\alpha \quad L$ kann man jede galoissche Erweiterung $K \quad L$ von Zahlkörpern als $L \quad K \ \alpha$ schreiben, so dass das Minimalpolynom $f \quad m_\alpha \quad K\,X$ von α den Grad $n \quad L : K$ besitzt. Alle anderen Nullstellen von f liegen dann auch in L, d.h. L ist ein Zerfällungskörper. Die Galoisgruppe Gal $L \ K$ ist in diesem Fall eine Untergruppe der Ordnung n in der symmetrischen Gruppe S_n, da Gal $L \ K$ die Nullstellen von f vertauscht.

Die Galois–Gruppe Gal $L \ K$ operiert auch auf den Wurzeln des Minimalpolynoms für jedes Element $\beta \quad L$. Das Minimalpolynom von β ist

$$m_\beta \quad \prod_{y \ S} X \quad y \quad K\,X \qquad \text{mit } S: \ \{\sigma\ \beta \quad \sigma \quad \text{Gal } L \ K$$

Satz C.3 (Hauptsatz der Galois–Theorie) *Sei $K \quad L$ galoissch. Ist $K \quad Z \quad L$ ein Zwischenkörper, so ist $Z \quad L$ wieder galoissch und* Gal $L \ Z$ *eine Untergruppe von* Gal $L \ K$. *Umgekehrt ist Z der Fixkörper unter* Gal $L \ Z$. *Die Erweiterung $K \quad Z$ ist galoissch genau dann, wenn die Untergruppe* Gal $L \ Z$ *ein Normalteiler ist. In diesem Fall gilt*

$$\text{Gal } Z \ K \quad \text{Gal } L \ K \quad \text{Gal } L \ Z$$

Beweis: Siehe [Wü, Satz 15.6 und Satz 15.13].

Als Korollar aus diesem Satz bekommt man:

Satz C.4 *Sei $\beta \quad L$ und $\beta_1 \quad \beta \ \beta_2 \quad \beta_r$ seine Konjugierten, also die Nullstellen des Minimalpolynoms von β über K in . Sei $g \ X_1 \quad X_r$ ein symmetrisches Polynom, d.h. g ist invariant unter Vertauschungen der X_i. Dann gilt*

$$g \ \beta_1 \ \beta_2 \quad \beta_r \quad K$$

Beweis: Man prüft leicht nach, dass $g \ \beta_1 \ \beta_2 \quad \beta_r$ invariant unter allen K–Automorphismen einer Galois–Erweiterung von K ist, die L enthält.

Betrachten wir nun den Fall endlicher Körper der Charakteristik $p \quad 0$.

Satz C.5 *Es gibt bis auf Isomorphie genau einen Körper $\mathbb{F}_q$ mit $q \quad p^m$ Elementen, falls p prim und $m \quad$ ist. $\mathbb{F}_q$ ist galoissch über $\mathbb{F}_p$. Die Galoisgruppe* Gal $\mathbb{F}_q \ \mathbb{F}_p$ *ist eine zyklische Gruppe, die vom Frobeniusautomorphismus $x \quad x^p$ erzeugt wird.*

Beweis: Siehe [Wü, Satz 14.10].

D Minkowskitheorie

In diesem Abschnitt beweisen wir die Endlichkeit der Klassenzahl (Satz 18.19) und den Dirichletschen Einheitensatz (Satz 17.12). Außerdem erklären wir die Klassenzahlformel, die beide in Verbindung bringt. Dazu benötigen wir einige Vorbereitungen.

Vorbemerkungen zu ganzen Idealen

Wir erinnern zunächst daran, dass in Definition 16.26 die Norm $N\ I$ eines Ideals $I \quad \mathcal{O}_K$ als Mächtigkeit des endlichen Quotienten $\mathcal{O}_K \ I$ eingeführt wurde.

Satz D.1 *Für je zwei ganze Ideale* $0 \quad I\ J \quad \mathcal{O}_K$ *gilt:* $N\ IJ \quad N\ I\ N\ J$.

Beweis: Der Ring $R \quad \mathcal{O}_K$ ist ein Dedekindring. Nach Satz 18.11 ist das Ideal J ein Produkt von Primidealen. Mittels Induktion kann man also annehmen, dass J ein Primideal ist. Es reicht dann zu zeigen, dass für alle Primideale gilt:

$$R\ I \quad R\ I\ I\ I$$

und

$$I\ I \quad R$$

Die erste Gleichung folgt aus

$$\text{Ker}\ R\ I \quad R\ I \quad I\ I$$

Für die zweite Gleichung überlegt man sich zuerst, dass wegen der eindeutigen Primfaktorzerlegung (Satz 18.11) gilt:

$$I \quad I$$

Zwischen diesen beiden Idealen kann kein weiteres Ideal liegen, denn sonst gäbe es ein ganzes Ideal mit

$$I^{\ 1} \quad R$$

im Widerspruch zur Maximalität von , denn in einem Dedekindring ist jedes Primideal 0 bereits maximal. Somit gilt für jedes $a \quad I \quad I$ schon

$$I \quad a \quad I$$

und folglich ist der R–Modul Homomorphismus

$$\varphi : R \quad I\ I \quad x \quad ax \quad I$$

S. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie,*
DOI 10.1007/978-3-8348-8263-9,

surjektiv. Es folgt, dass

$$\text{Ker } \varphi \quad R$$

gilt, denn $1 \quad \text{Ker } \varphi$. Wegen der Maximalität von folgt $\text{Ker } \varphi$ und damit die zweite Gleichung.

Mit Hilfe der Norm lassen sich einige nützliche Tatsachen in $\mathcal{O}_K$ beweisen:

Satz D.2 *Sei* $I \quad 0$ *ein Ideal in* $R \quad \mathcal{O}_K$.

1. *Ist* $N \; I$ *prim, so auch* I.
2. $N \; I$ *ist ein Element in* I, *d.h.* $I \quad N \; I$.
3. *Falls* I *ein Hauptideal ist, also* $I \quad x$ *für ein* $0 \quad x \quad \mathcal{O}_K$, *dann ist die Norm von* I *gleich dem Betrag der Körpernorm von* x, *d.h.* $N \; I \quad N \; x$.
4. *Ist* I *prim, so teilt es genau ein* $p \quad$ *und es gilt* $N \; I \quad p^m$ *mit* $m \quad n \quad K : \mathbb{Q}$.
5. *Jede natürliche Zahl* m *ist nur in endlich vielen Idealen enthalten.*
6. *Nur endlich viele Ideale haben Norm* $\quad N$ *für jede vorgegebene Schranke* N.

Beweis: 1) Folgt direkt aus Satz D.1.
2) Da $N \; I$ die Ordnung von $R \; I$ ist, gilt für das Element 1 auch $N \; I \quad 1 \quad 0$ in $R \; I$, d.h. $N \; I \quad I$.
3) Sei $I \quad x$ ein Hauptideal. Nach Aufgabe 16.47 ist $N \; x$ die Determinante der –linearen Abbildung $m_x : R \quad R$ gegeben durch Multiplikation mit x. Andererseits ist $N \; I$ die Ordnung des Kokerns dieser Abbildung zwischen freien –Moduln vom Rang n. Mit dem Diagonalisierungsalgorithmus aus Abschnitt 6 können wir annehmen, dass die darstellende Matrix M zu m_x in Diagonalgestalt ist, mit Einträgen $m_1 \quad m_n \quad \{0$ auf der Diagonalen. Mit Hilfssatz 6.12 folgt dann $N \; I \quad m_1 m_2 \quad m_n \quad \det M \quad N \; x$.
4) Wegen $I \quad N \; I \quad \prod p_i^{\alpha_i}$ gibt es mindestens eine Primzahl $p \quad$ mit $I \quad p$, also gibt es ein Ideal J mit $IJ \quad p$. Nach Satz D.1 und 3) folgt $N \; I \quad N \; p$ und aus $N \; p \quad p^n$ (siehe Aufgabe 16.45) folgt $N \; I \quad p^m$ mit $m \quad n$.
5) Sei I ein Ideal und $m \quad I$, d.h. $I \quad m$. Schreibe das Hauptideal m als endliches Produkt von Primidealen mittels Satz 18.11. Da I ein Teiler von m ist, ist I ein Produkt aus einer Teilmenge dieser Primideale. Damit gibt es nur endlich viele Möglichkeiten für I.
6) Es gilt $N \; I \quad I$ nach 2). Wende dann 5) auf $m \quad N \; I \quad N$ an.

Wir stellen nun noch eine weitere Definition und einige Resultate bereit, die die Norm benutzen, und die wir in Anwendungen der Minkowskitheorie benötigen. Sei dazu K ein Zahlkörper der Dimension $K : \mathbb{Q} \quad n$. Ist $p \quad$ eine Primzahl, so kann man das Hauptideal $p \quad \mathcal{O}_K$ eindeutig in ein Produkt von paarweise verschiedenen Primidealen zerlegen:

$$p \quad \begin{matrix} e_1 & & e_r \\ 1 & & r \end{matrix}$$

Die Restklassenkörper $\kappa_i : \quad \mathcal{O}_K \quad _i$ sind endliche Erweiterungskörper von $\mathbb{F}_p \quad p$, weil in κ_i wegen $p \quad _i$ die Primzahl p gleich 0 ist.

Definition D.3 *Die Zahlen e_i heißen* Verzweigungsindices*. Die Dimensionen f_i : dim $_p \mathcal{O}_K$ $_i$ heißen* Trägheitsindices*. Die Primzahl p heißt* verzweigt*, falls es einen Index i gibt mit e_i 2. Sie heißt* träge*, falls p prim bleibt in $\mathcal{O}_K$. Die Primzahl p heißt* voll zerlegt*, falls r n ist und alle e_i f_i 1 sind.*

Satz D.4 (Fundamentale Gleichung) *Die Trägheitsindices sind durch die Formel p^{f_i} N $_i$ festgelegt. Es gilt die Formel*

$$n \quad K:\mathbb{Q} \quad \sum_{i\ 1}^{r} e_i f_i$$

Ist K $\mathbb{Q}$ galoissch, so sind alle e_i und alle f_i gleich, und es gilt n efr.

Beweis: Die Formel p^{f_i} N $_i$ folgt, da f_i dim $_p \mathcal{O}_K$ $_i$ und N $_i$ $\#\mathcal{O}_K$ $_i$. Aus Satz D.1 schließt man, dass $\#\mathcal{O}_K$ $_i^{e_i}$ N $_i^{e_i}$ N $_i$ ^{e_i} $p^{e_i f_i}$. Aus N p p^n folgt n dim $_p \mathcal{O}_K$ $p\mathcal{O}_K$. Da alle $_i$ teilerfremd sind, gilt deshalb mit dem chinesischen Restsatz

$$n \quad \dim_{\ p} \mathcal{O}_K \ p\mathcal{O}_K \quad \dim_{\ p} \prod_{i\ 1}^{r} \mathcal{O}_K \ _i^{e_i} \quad \sum_{i\ 1}^{r} \dim_{\ p} \mathcal{O}_K \ _i^{e_i} \quad \sum_{i\ 1}^{r} e_i f_i$$

für die entsprechenden Hochzahlen der p–Potenzen.

Ist K $\mathbb{Q}$ galoissch, so ist Hom K gleich der Galoisgruppe G Aut K nach Anhang C. Alle σ G bilden somit Ringautomorphismen von $\mathcal{O}_K$. Man überlegt sich nun zuerst, dass die Galoisgruppe transitiv auf den Primidealen $_i$ operiert, die p teilen. Denn wenn es zwei solche Primideale $_1$ und $_2$ gäbe mit σ $_1$ $_2$ für alle σ G, so könnte man mit dem chinesischen Restsatz ein x $\mathcal{O}_K$ finden, so dass x 0 mod $_2$ und x 1 mod σ $_1$ für alle σ G. Aus x 0 mod $_2$ folgt, dass N x $\prod_\sigma \sigma$ x in $_2$ p liegt. Die andere Bedingung x 1 mod σ $_1$ für alle σ G impliziert dagegen, dass σ x $_1$ für alle σ G, und daher N x $_1$ p ist, ein Widerspruch.

Da G transitiv durch Automorphismen operiert, sind alle Restklassenkörper κ_i $\mathcal{O}_K$ $_i$ isomorph, sowie alle e_i und alle f_i gleich, und es folgt n efr.

Wir benötigen auch das folgende Resultat, das zeigt, wie man in einem wichtigen Spezialfall die Indices e_i und f_i berechnen kann. Quadratische Zahlkörper und Kreisteilungskörper erfüllen diese Voraussetzung.

Proposition D.5 *Sei K ein Zahlkörper, so dass $\mathcal{O}_K$ α mit α $\mathcal{O}_K$. Wir betrachten eine Primzahl p mit der eindeutigen Zerlegung*

$$p \quad _1^{e_1} \quad _r^{e_r}$$

Ist h das Minimalpolynom von α, so entspricht dieser Zerlegung von p eine Faktorisierung

$$\overline{h} \quad \prod_{i\ 1}^{r} \overline{h}_i^{e_i} \quad \mathbb{F}_p \ T$$

von h modulo p, in der man die Verzweigungsindices e_i als Multiplizität von $\overline{h}_i$ ablesen kann. Außerdem gilt für die Trägheitsindices f_i deg $\overline{h}_i$.

Wenn eine Primzahl p verzweigt ist, dann teilt p die Diskriminante Δ_K. Insbesondere gibt es nur endlich viele verzweigte Primzahlen.

Bemerkung D.6 *Der Zusatz über verzweigte Primzahlen gilt für beliebige Zahlkörper.*

Beweis: Es gilt $\mathcal{O}_K \quad \alpha \quad T \quad h$ und somit $\mathcal{O}_K \quad p \quad \mathbb{F}_p \; T \quad \overline{h}$. Aus der Zerlegung $\overline{h} \quad \prod_i^r {}_1 \overline{h}_i^{e_i}$ in irreduzible Faktoren folgt $\kappa_i \quad \mathbb{F}_p \; T \quad \overline{h}_i$, $f_i \quad \deg \overline{h}_i$ sowie $n \quad \sum_i e_i f_i$.

Für die Diskriminante Δ_K gilt nach dem Beweis von Lemma 16.23 die Formel $\Delta_K \quad \prod_{i \quad j} \alpha_i \quad \alpha_j \; ^2$, wobei $\alpha_1 \quad \alpha_n$ die paarweise verschiedenen Nullstellen von h sind. Somit ist p nur dann verzweigt, wenn Nullstellen modulo p zusammenfallen, d.h. wenn $\Delta_K \quad 0 \bmod p$.

Bemerkung D.7 *Ein quadratischer Zahlkörper* $K \quad \mathbb{Q} \sqrt{d}$ *mit quadratfreiem* d *hat nach dem Beweis von Satz 17.14 folgendes Verzweigungsverhalten bei einer Primzahl* p*:*

1. *Im Fall* $p \quad d$ *ist* p *verzweigt, d.h. es gilt* $p \quad ^2$ *für ein Primideal* $\quad$ *der Norm* p*.*

2. *Gilt* $p \quad 2d$ *und* $\frac{d}{p} \quad 1$*, so bleibt* p *prim mit Norm* p^2*, d.h.* p *ist träge.*

3. *Für* $p \quad 2d$ *und* $\frac{d}{p} \quad 1$ *ist* p *voll zerlegt, d.h.* $p \quad {}_1 \; {}_2$ *mit zwei verschiedenen Primidealen der Norm* p*. Es gilt* ${}_i \quad p \; a \quad \sqrt{d}$ *, wobei* $a^2 \quad d \bmod p$*.*

4. *Im Fall* $p \quad 2$ *kommt es auf die Restklasse von* $d \bmod 8$ *an:*

   Ist $d \quad 2 \bmod 4$*, so gilt* $2 \quad d$*, aber* $2 \quad \sqrt{d}$*, und daher ist* $2 \quad 2 \sqrt{d} \; ^2$ *verzweigt. Dies kann man auch mit Proposition D.5 testen, denn das Minimalpolynom von* $\sqrt{d}$ *ist* $h \quad T^2 \quad d \quad T^2 \bmod 2$*.*

   Gilt $d \quad 3 \bmod 4$*, so ist* 2 *ebenfalls verzweigt, denn es gilt* $2 \quad 2 \; 1 \quad \sqrt{d} \; ^2$*, da* $2 \; 1 \quad \sqrt{d} \quad 2 \; 1 \quad \sqrt{d}$ *. Das Minimalpolynom von* $\sqrt{d}$ *ist* $h \quad T^2 \quad d \quad T \quad 1 \; ^2 \bmod 2$*.*

   Im Fall $d \quad 1 \bmod 4$ *unterscheidet man* $d \quad 1 \bmod 8$ *und* $d \quad 5 \bmod 8$*. Im ersten Fall ist das Minimalpolynom von* $1 \quad \sqrt{d} \quad 2$ *gleich* $h \quad T^2 \quad T \quad \frac{1 \quad d}{4}$*, also* $\overline{h} \quad T^2 \quad T$ *modulo* 2*, daher ist* 2 *voll zerlegt. Im Fall* $d \quad 5 \bmod 8$ *ist* p *träge nach dem Beweis von Satz 17.14.*

Der Gitterpunktsatz von Minkowski

Definition D.8 *Ein* Gitter *vom Rang* m *im* ^{n} *ist eine additive Gruppe* $\Gamma \quad ^n$

$$\Gamma \quad \sum_{i \quad 1}^{m} a_i e_i \quad a_i$$

die von m *über* $\quad$ *linear unabhängigen Vektoren* $e_1 \quad e_m$ *erzeugt wird. Die Zahl* $m \quad n$ *wird der* Rang *von* Γ *genannt. Im Fall* $m \quad n$ *heißt das Gitter* vollständig.

Aus der Definition folgt unmittelbar, dass jedes Gitter $\Gamma \quad ^n$ eine *diskrete* additive Untergruppe bezüglich der Euklidischen Topologie auf ^{n} ist, d.h. jeder Punkt $x \quad \Gamma$ hat eine Umgebung U in der nur endlich viele Gitterpunkte von Γ liegen. Der Quotientenraum $^n \; \Gamma$ ist die Menge der Äquivalenzklassen unter Translation mit Γ. Wir bezeichnen mit $\Phi : \; ^n \quad ^n \; \Gamma$ die Quotientenabbildung.

Lemma D.9 *Sei eine Teilmenge* $\Gamma \quad ^n$ *gegeben.*

1. Γ *ist ein Gitter genau dann, wenn* Γ *eine diskrete additive Untergruppe von* ^{n} *ist.*
2. *Ist* Γ *ein Gitter, so ist* $^n \quad \Gamma$ *homöomorph zu einem Produkt* $S^1 \; ^m \quad ^n \; ^m$, *wobei* S^1 *der Einheitskreis ist.* $^n \quad \Gamma$ *ist somit genau dann kompakt, wenn* Γ *vollständig ist.*

Beweis: 1) Sei Γ ein Gitter. Bis auf eine invertierbare, lineare Selbstabbildung $^n \quad ^n$, die insbesondere ein Homöomorphismus ist, kann man annehmen, dass $e_1 \quad e_m$ in der Darstellung von Γ die ersten m Elemente der Standardbasis sind. Indem man Kugelumgebungen betrachtet, sieht man dann sofort, dass Γ diskret ist.

Sei nun umgekehrt Γ eine diskrete additive Untergruppe im ^{n} und $e_1 \quad e_m \quad \Gamma$ eine maximale, über linear unabhängige Menge von Elementen in Γ. Insbesondere ist jedes $x \quad \Gamma$ eine reelle Linearkombination der e_i. Wir zeigen mit Induktion über m, dass Γ ein Gitter ist. Der Induktionsanfang ist $m \quad 0$ und trivial zu beweisen, denn dann ist $\Gamma \quad 0$. Sei also $m \quad 1$. Betrachte den $m \quad 1$ –dimensionalen reellen Unterraum

$$V \quad \text{span } e_1 \quad e_{m \; 1}$$

Die additive Gruppe $\Gamma' : \quad V \quad \Gamma$ ist diskret in V, also ein Gitter nach Induktionsvoraussetzung. Seien $f_1 \quad f_{m \; 1} \quad \Gamma'$ über linear unabhängige Elemente, die Γ' als –Modul erzeugen. Setze $f_m : \quad e_m$. Betrachte nun die Menge

$$W : \quad \{a_1 f_1 \quad a_m f_m \quad \Gamma \quad 0 \quad a_m \quad 1 \text{ und } 0 \quad a_i \quad 1 \text{ für } i \quad 1 \quad m \quad 1$$

W ist beschränkt, also ist W endlich, da Γ diskret ist. Außerdem liegt der Punkt f_m in $W \quad \Gamma'$. Sei f_0 ein Punkt aus W mit minimalem reellen Koeffizienten $a_m \quad 0$ bei f_m. Dann gilt ebenfalls $f_0 \quad \Gamma'$. Wir können annehmen, dass $f_m \quad f_0$ ist, da beide die gleichen Eigenschaften haben. Jedes $x \quad \Gamma$ kann durch Subtraktion eines Vektors

$$v \quad b_1 f_1 \quad b_m f_m$$

mit ganzzahligen Koeffizienten b_i so abgeändert werden, dass $x \quad v \quad W$ ist und der letzte Koeffizient c_m in der reellen Basisdarstellung von x die Ungleichung $0 \quad c_m \quad 1$ erfüllt. Nach Konstruktion von $f_m \quad f_0$ folgt damit $c_m \quad 0$ und $x \quad v \quad \Gamma'$. Also ist x eine ganzzahlige Linearkombination der linear unabhängigen f_i und damit Γ ein Gitter.

2) Wie in 1) können wir annehmen, dass $e_1 \quad e_m$ in der Darstellung von Γ ein Teil der Standardbasis ist. Damit bekommt man einen Homöomorphismus

$$^n \quad \Gamma \quad ^m \quad ^n \; ^m$$

und die Aussage folgt, da vermöge der Exponentialabbildung $t \quad \exp 2\pi i t$ homöomorph zu $S^1 \quad \{z \quad z \quad 1$ ist.

Korollar D.10 *Ist* Γ *vollständig, so ist* $^n \quad \Gamma \quad S^1 \; ^n$ *ein kompakter Torus.*

Definition D.11 *Sei* Γ *ein vollständiges Gitter im* ^{n}. *Die Teilmenge* $F \quad ^n$ *der Form*

$$F : \quad \{a_1 e_1 \quad a_n e_n \quad \Gamma \quad 0 \quad a_i \quad 1 \textit{ für } i \quad 1 \quad n$$

heißt Fundamentalbereich *für* Γ.

Jeder Vektor im ^{n} hat dann einen eindeutigen Repräsentanten modulo Γ in F. Ein Fundamentalbereich F ist nicht eindeutig durch Γ bestimmt, da man die linear unabhängige Menge $e_1 \quad e_n$ wechseln kann. Eine Invariante von F ist jedoch das Lebesgue–Maß

$$\text{vol } \Gamma \ : \quad \text{vol } F \quad \int_F dx_1 \quad dx_n \quad \det e_1 \quad e_n$$

da F in ^{n} ein Lebesgue messbares Parallelotop ist, das invariant unter elementaren Transformationen ist.

Wir werden jetzt beschränkte, Lebesgue messbare Teilmengen $M \quad ^n$ betrachten und ihr Bild unter $\Phi : \ ^n \quad ^n \ \Gamma$ studieren. Das n–dimensionale Lebesgue–Maß von M bezeichnen wir immer mit vol M .

Lemma D.12 *Ist* vol $M \quad$ vol Γ *, so ist die Einschränkung* Φ_M *von* Φ *auf M nicht injektiv.*

Beweis: Wir bezeichnen mit $F \quad g$ das Translat von F unter $g \quad \Gamma$ und setzen $M_g : \ M \quad F \quad g$. Dann ist M die disjunkte Vereinigung der messbaren Mengen M_g. Durch Rücktranslation nach F erhalten wir aus den M_g messbare Teilmengen $M'_g : \ M_g \quad g \quad F$. Die Zuordnung $M_g \quad M'_g$ ist maßerhaltend, da das Lebesgue–Maß translationsinvariant ist. Die Vereinigung aller M'_g bezeichnen wir mit M'. Nun nehmen wir an, Φ_M sei injektiv. Dann sind alle M'_g disjunkt. Insbesondere ist M' als disjunkte, abzählbare Vereinigung messbarer Mengen M'_g selbst messbar und es gilt vol $M \quad$ vol M' . Wegen der Inklusion $M' \quad F$ erhalten wir vol $M \quad$ vol $M' \quad$ vol F , im Widerspruch zur Voraussetzung.

Definition D.13 *Eine Teilmenge* $M \quad ^n$ *heißt* (zentral-)symmetrisch*, falls mit jedem* $x \quad M$ *auch* $x \quad M$ *ist. M heißt* konvex*, falls mit je zwei Punkten* $x \quad y$ *in M auch die Verbindungslinie*

$$\lambda x \quad 1 \quad \lambda \ y \quad \lambda \quad 0 \ 1$$

ganz in M liegt.

Satz D.14 (Gitterpunktsatz von Minkowski) *Sei* Γ *ein vollständiges Gitter in* ^{n} *mit Fundamentalbereich F. Weiter sei M eine beschränkte, messbare, konvexe und symmetrische Teilmenge im* ^{n}*. Falls*

$$\text{vol } M \quad 2^n \text{vol } F$$

so enthält M einen Punkt aus $\Gamma \quad \{0$ *. Die gleiche Aussage gilt auch, falls M kompakt, konvex und symmetrisch ist und*

$$\text{vol } M \quad 2^n \text{vol } F$$

Beweis: Wir betrachten das *verdoppelte* Gitter 2Γ. Sein Fundamentalbereich ist $2F$ und hat Volumen 2^nvol F . Die Quotientenabbildung werde wieder mit

$$\Phi : \ ^n \quad ^n \ 2\Gamma$$

bezeichnet. Wegen vol $M \quad 2^n$vol $F \quad$ vol $2F$ kann Φ nach Lemma D.12 auf M nicht injektiv sein. Also gibt es $x \ y \quad M$ mit $x \quad y$ und $x \quad y \quad 2\Gamma$. Wegen der Symmetrie von M ist $y \quad M$. Aufgrund der Konvexität von M ist also auch

$$0 \quad \omega : \ \frac{1}{2} \ x \quad y \quad M$$

Das Element ω ist aber auch in Γ, da $x \quad y \quad 2\Gamma$ und hat daher die gewünschten Eigenschaften.

Ist M kompakt und vol $M \quad 2^n$vol F , so betrachte $1 \quad \varepsilon \ M$ für $\varepsilon \quad 0$.

Die Endlichkeit der Klassenzahl

Sei nun K ein Zahlkörper vom Grad n über $\mathbb{Q}$. Es gibt n Körpermonomorphismen

$$\sigma_i : K$$

die $\mathbb{Q}$ festlassen. Für jedes σ ist auch

$$\overline{\sigma} : K \qquad \overline{\sigma}\ \alpha\ :\ \overline{\sigma\ \alpha}$$

ein Monomorphismus, und es gilt genau dann $\overline{\sigma}$ σ, wenn σ reell ist, d.h. in landet. Jedes nicht–reelle σ kommt also als Paar σ $\overline{\sigma}$. Wir können daher die Monomorphismen so nummerieren, dass die ersten r_1 Stück reell sind und die restlichen $2r_2$ n r_1 Stück echt komplex sind:

$$\sigma_1 \qquad \sigma_{r_1}\ \sigma_{r_1\ 1}\ \overline{\sigma}_{r_1\ 1} \qquad \sigma_{r_1\ r_2}\ \overline{\sigma}_{r_1\ r_2}$$

Im Gegensatz zum restlichen Buch schreiben wir hier r_1 für r und r_2 für r .

Definition D.15 *Wir definieren den* Minkowskiraum

$$V_K : \qquad {}^{r_1} \qquad {}^{r_2}$$

und die Abbildung

$$\sigma : K \qquad V_K$$

durch

$$\alpha \qquad \sigma_1\ \alpha \qquad \sigma_{r_1}\ \alpha\ \ \sigma_{r_1\ 1}\ \alpha \qquad \sigma_{r_1\ r_2}\ \alpha$$

V_K ist eine n–dimensionale –Algebra mit komponentenweiser Multiplikation, und damit wird σ ein Ringhomomorphismus, sogar ein Morphismus von $\mathbb{Q}$–Algebren. V_K versehen wir auch noch mit einer Banachraumstruktur, die von ^{n} ^{r_1} ^{2r_2} induziert wird:

$$x_1 \qquad x_{r_1}\ z_1 \qquad z_{r_2} \qquad \overline{x_1^2 \qquad x_{r_1}^2 \quad z_1\ {}^2 \qquad z_{r_2}\ {}^2}$$

Offensichtlich ist σ injektiv, da alle Komponenten injektiv sind.

Wir wollen im Folgenden den Satz von Minkowski anwenden, indem wir das Bild von ganzen Idealen unter der Abbildung σ betrachten. Wir wissen aus Korollar 16.25, dass jedes ganze Ideal I 0 genau n über $\mathbb{Q}$ linear unabhängige Erzeuger b_1 b_n besitzt. Deren Bilder $\sigma\ b_1$ $\sigma\ b_n$ sind wieder linear unabhängig über $\mathbb{Q}$, da σ injektiv ist. Wir benötigen diese Aussage auch über :

Lemma D.16 *Ist b_1 b_n eine $\mathbb{Q}$–Basis von K, so sind $\sigma\ b_1$ $\sigma\ b_n$ V_K linear unabhängig über .*

Beweis: Wir betrachten die n n –Matrizen

$$D : \begin{array}{ccccccc} \sigma_1\ b_1 & \sigma_{r_1}\ b_1 & \sigma_{r_1\ 1}\ b_1 & \overline{\sigma}_{r_1\ 1}\ b_1 & \sigma_{r_1\ r_2}\ b_1 & \overline{\sigma}_{r_1\ r_2}\ b_1 \\ \vdots & & \vdots & \vdots & & \vdots \\ \sigma_1\ b_n & \sigma_{r_1}\ b_n & \sigma_{r_1\ 1}\ b_n & \overline{\sigma}_{r_1\ 1}\ b_n & \sigma_{r_1\ r_2}\ b_n & \overline{\sigma}_{r_1\ r_2}\ b_n \end{array}$$

und

$$A: \quad \begin{matrix} \sigma_1\ b_1 & \sigma_{r_1}\ b_1 & \mathrm{Re}\ \sigma_{r_1\ 1}\ b_1 & \mathrm{Im}\ \sigma_{r_1\ 1}\ b_1 & \mathrm{Im}\ \sigma_{r_1\ r_2}\ b_1 \\ \vdots & & \vdots & \vdots & \vdots \\ \sigma_1\ b_n & \sigma_{r_1}\ b_n & \mathrm{Re}\ \sigma_{r_1\ 1}\ b_n & \mathrm{Im}\ \sigma_{r_1\ 1}\ b_n & \mathrm{Im}\ \sigma_{r_1\ r_2}\ b_n \end{matrix}$$

Es gilt $\det A \quad 2i \quad^{r_2} \det D$, wie man durch elementare Umformungen leicht sieht. Es gilt weiterhin

$$\det D\ ^2 \quad \Delta\ b_1 \quad b_n$$

nach Definition der Diskriminante. Nach Lemma 16.23 gilt $\Delta\ b_1 \quad b_n \quad 0$, also folgt damit $\det A \quad 0$. Hieraus folgt die Behauptung, denn die Zeilen von A sind, unter dem Isomorphismus $V_K \quad^{r_1 \quad 2r_2}$, durch $\sigma\ b_1 \quad \sigma\ b_n$ gegeben.

Korollar D.17 *Sei $I \quad 0$ ein ganzes Ideal in $\mathcal{O}_K$. Dann ist $\sigma\ I \quad V_K$ ein vollständiges Gitter und das Volumen des Fundamentalbereichs F von $\sigma\ I$ ist gegeben durch*

$$\mathrm{vol}\ F \quad 2\ ^{r_2} N\ I\ \sqrt{\Delta_K}$$

Beweis: Sei $b_1 \quad b_n$ eine –Basis von I. Wir haben in Satz 16.32 gezeigt:

$$N\ I \quad \frac{\sqrt{\Delta\ b_1 \quad b_n}}{\Delta_K}$$

Wegen $I \quad 0$ und Korollar 16.25 bilden $b_1 \quad b_n$ eine $\mathbb{Q}$–Basis von K, so dass wir das vorangegangene Lemma anwenden können. Die Zeilen der Matrix A bilden eine –Basis von $\sigma\ I$. Die Determinante von D ist $\sqrt{\Delta\ b_1 \quad b_n}$. Also folgt:

$$\mathrm{vol}\ F \quad \det A \quad 2\ ^{r_2} \det D \quad 2\ ^{r_2} \sqrt{\Delta\ b_1 \quad b_n} \quad 2\ ^{r_2} N\ I\ \sqrt{\Delta_K}$$

und somit die Behauptung.

Satz D.18 *Jedes ganze Ideal $I \quad 0$ in $\mathcal{O}_K$ enthält ein Element $\alpha \quad 0$ mit*

$$N\ \alpha \quad \frac{4}{\pi}\ ^{r_2} \frac{n!}{n^n} \sqrt{\Delta_K}\, N\ I$$

Beweis: $N\ \alpha$ ist nach Definition genau das Produkt

$$\sigma_1\ \alpha \quad \sigma_{r_1}\ \alpha\ \sigma_{r_1\ 1}\ \alpha\ ^2 \quad \sigma_{r_1\ r_2}\ \alpha\ ^2$$

Sei $M\ c$ die Menge aller $x \quad V_K$ mit

$$x_1 \quad x_{r_1} \quad 2\ z_1 \quad 2\ z_{r_2} \quad c$$

Für reelles $c \quad 0$ ist die Menge $M\ c$ kompakt, konvex und symmetrisch. Man berechnet mit Induktion über $n \quad r_1 \quad 2r_2$

$$\mathrm{vol}\ M\ c \quad 2^{r_1}\ \frac{\pi}{2}\ ^{r_2} \frac{c^n}{n!}$$

Der Satz von Minkowski besagt, dass $M\ c$ einen Punkt $\sigma\ \alpha \quad 0$ von $\Gamma \quad \sigma\ I$ enthält, falls

$$\text{vol}\ M\ c \qquad 2^n \text{vol}\ F$$

wobei F der Fundamentalbereich ist. Da

$$\text{vol}\ F \quad 2^{\ r_2} N\ I\ \sqrt{\Delta_K}$$

bedeutet das:

$$2^{r_1}\ \ \frac{\pi}{2}\ \ ^{r_2}\ \frac{c^n}{n!} \quad 2^n\ \ ^{r_2} N\ I\ \sqrt{\Delta_K}$$

Wir können also

$$c^n \qquad \frac{4}{\pi}\ \ ^{r_2}\ n! N\ I\ \sqrt{\Delta_K}$$

wählen und erhalten ein $\alpha \quad I \quad \{0$ mit $\sigma\ \alpha \qquad M\ c$. Die Ungleichung

$$a_1 \quad a_n\ ^{1/n} \quad \frac{1}{n}\ a_1 \qquad\qquad a_n$$

zwischen dem *arithmetischen und geometrischen Mittel* impliziert dann

$$N\ \alpha \qquad \sigma_1\ \alpha \qquad \sigma_{r_1}\ \alpha\ \sigma_{r_1\ \ 1}\ \alpha^{\ 2} \qquad \sigma_{r_1\ \ r_2}\ \alpha^{\ 2} \qquad \frac{c}{n}^{\ n} \qquad \frac{4}{\pi}\ \ ^{r_2}\ \frac{n!}{n^n}\sqrt{\Delta_K} N\ I$$

wie gewünscht.

Korollar D.19 *Jedes ganze Ideal I ist äquivalent zu einem ganzen Ideal J mit*

$$N\ J \qquad \frac{4}{\pi}\ \ ^{r_2}\ \frac{n!}{n^n}\sqrt{\Delta_K}$$

Beweis: Betrachte das Ideal $I\ \ ^{1}$. Indem man mit dem Hauptnenner durchmultipliziert, erhält man ein ganzes Ideal in der selben Klasse wie $I\ \ ^{1}$, d.h. es gilt $I \qquad 1$. Also gibt es nach dem Satz ein Element $\alpha \qquad$ mit

$$N\ \alpha \qquad \frac{4}{\pi}\ \ ^{r_2}\ \frac{n!}{n^n}\sqrt{\Delta_K} N$$

Es gilt

$$\alpha \qquad J$$

für ein ganzes Ideal J mit $J \qquad I$, da $\qquad I\ \ ^{1}$. Also gilt nach Satz D.2 und Satz D.1

$$N \quad N\ J \quad N \quad \alpha \qquad N\ \alpha$$

und daher

$$N \quad N\ J \qquad N\ \alpha \qquad \frac{4}{\pi}\ \ ^{r_2}\ \frac{n!}{n^n}\sqrt{\Delta_K} N$$

Nun folgt die Behauptung durch Kürzen von $N \quad$.

Satz D.20 (Endlichkeit der Klassengruppe) *Die Klassengruppe* $\text{Cl}\ \mathcal{O}_K$ *ist endlich.*

Beweis: Die Menge aller Äquivalenzklassen von gebrochenen Idealen modulo Hauptidealen kann nach dem bisher Bewiesenen in den ganzen Idealen mit beschränkter Norm gesucht werden. Dies sind nur endlich viele nach Satz D.2.

Definition D.21 *Die Ordnung von* Cl $\mathcal{O}_K$ *ist die* Klassenzahl *und wird oft mit h bezeichnet. Die universelle Konstante*

$$C \quad C\ r_1\ r_2 \qquad \frac{4}{\pi}^{r_2}\ \frac{n!}{n^n}$$

für $n \quad r_1 \quad 2r_2$ *heißt* Minkowskikonstante.

In der Tabelle sind alle Werte für $n \quad 5$ mit auf 3 Dezimalstellen aufgerundeten Werten aufgelistet.

n	r_1	r_2	C
2	0	1	0.637
2	2	0	0.500
3	1	1	0.283
3	3	0	0.223
4	0	2	0.152
4	2	1	0.120
4	4	0	0.094
5	1	2	0.063
5	3	1	0.049
5	5	0	0.039

Beispiele Sei $K \quad \mathbb{Q}\ \sqrt{\ 5\ }$. Dann ist $C \quad 0\ 637$ und $\Delta_K \qquad 20$. Also haben alle Erzeuger der Klassengruppe eine Norm, die durch $C\sqrt{20} \quad 2\ 85$ beschränkt ist und man muss daher als Erzeuger nur Ideale der Norm 2 suchen. Es gibt aber nur ein Ideal der Norm 2, da

$$2\ 1 \quad \sqrt{\ 5\ }^{\ 2} \qquad 2$$

Es folgt sofort, dass die Klassengruppe $\quad 2 \quad$ ist, mit Erzeuger $\ 2\ 1 \quad \sqrt{\ 5\ }$.

Ist $K \quad \mathbb{Q}\ \zeta_5$ der Kreisteilungskörper der fünften Einheitswurzeln, so ist $n \quad 4$, $r_1 \quad 0$, $r_2 \quad 2$ und $\Delta_K \quad 125$ nach Aufgabe 16.43. Somit muss man nur Ideale der Norm kleiner gleich $0\ 152\sqrt{125} \quad 1\ 699$ untersuchen, die es nicht gibt. Es folgt $h \quad 1$ in diesem Fall. Bereits Kummer konnte viele Klassenzahlen von Kreisteilungskörpern $\mathbb{Q}\ \zeta_p$ berechnen. So erhielt er $h\ \mathbb{Q}\ \zeta_{23} \qquad 3$ und $h\ \mathbb{Q}\ \zeta_{37} \qquad 37$. Damit widerlegte er falsche Beweise für die Fermatsche Vermutung [ST].

Der Dirichletsche Einheitensatz

Definition D.22 *Definiere*

$$_{1 \qquad r_1\ r_2} : V_K : \qquad \{0\ ^{r_1} \qquad \{0\ ^{r_2} \qquad L_K : \qquad ^{r_1\ r_2}$$

durch

$$x_1 \qquad x_{r_1}\ z_1 \qquad z_{r_2} \ : \quad \log x_1 \qquad \log x_{r_1}\ \log z_1\ ^2 \qquad \log z_{r_2}\ ^2$$

L_K ist der sogenannte logarithmische Minkowskiraum. *Dann gilt*

$$xy \qquad x \qquad y$$

Die Komposition mit σ aus Definition D.15

$$: K \quad ^{\sigma} \; V_K \qquad L_K$$

wird ebenfalls mit bezeichnet.

Lemma D.23 (Lemma von Kummer) *Sei f X ein normiertes Polynom, dessen Nullstellen α_1 α_n alle den Betrag* 1 *haben. Dann sind alle Nullstellen von f Einheitswurzeln.*

Beweis: Man kann annehmen, dass f $\prod_{i \; 1}^{n} X \quad \alpha_i$ über irreduzibel ist. Für jedes k setze

$$f_k : \prod_{i \; 1}^{n} X \quad \alpha_i^k \qquad X^n \quad a_1 X^{n \; 1} \qquad a_n$$

Dieses Polynom f_k hat Koeffizienten a_j, die selbst symmetrische Polynome P_j vom Grad j in den ganz–algebraischen Wurzeln α_i^k sind. Aus der Galois–Theorie folgt dann f_k X . Da P_j aus $\binom{n}{j}$ Summanden besteht, gilt darüber hinaus

$$a_j \qquad \binom{n}{j}$$

da α_i^k 1 ist und alle Koeffizienten von P_j gleich 1 sind. Also gibt es insgesamt nur endlich viele solcher Polynome und daher Indizes k m mit

$$f_k \quad f_m$$

Also gibt es eine Permutation τ der Menge $\{1 \; 2 \qquad n$ mit

$$\alpha_i^k \quad \alpha_{\tau \; i}^m$$

Nach $n!$–maliger Anwendung erreicht man somit

$$\alpha_i^{\; k^{n!} \quad m^{n!}} \qquad 1$$

für alle i. Es folgt, dass alle α_i Einheitswurzeln sind.

Lemma D.24 *Der Kern von $: \mathcal{O}_K$ L_K sind genau die Einheitswurzeln in $\mathcal{O}_K$. Dies ist eine endliche, zyklische Gruppe gerader Ordnung w und wird mit $\mathcal{O}_{K\,\mathrm{tors}}$ bezeichnet.*

Beweis: α ist Null, falls $\sigma_i \; \alpha \qquad 1$ für alle Monomorphismen $\sigma_i : K \qquad$. Also hat in diesem Fall das Polynom

$$\prod_i T \quad \sigma_i \; \alpha \qquad T$$

nach dem Lemma von Kummer nur Einheitswurzeln als Nullstellen. Insbesondere ist die Nullstelle α selbst auch eine Einheitswurzel. Da der Einheitskreis kompakt ist und $\mathcal{O}_K$ diskret ist, sind alle solchen α von endlicher Anzahl. Daher ist $\mathcal{O}_{K\,\mathrm{tors}}$ eine endliche Gruppe. Ihre Ordnung w ist gerade, da sie das Element 1 der Ordnung 2 enthält. $\mathcal{O}_{K\,\mathrm{tors}}$ ist als endliche Untergruppe von K eine zyklische Gruppe nach Satz 7.2.

Satz D.25 (Dirichletscher Einheitensatz) *Das Bild* $E \quad \sigma\ \mathcal{O}_K$ *von* $\mathcal{O}_K$ *unter* $\quad$ *ist ein Gitter vom Rang* $r_1 \quad r_2 \quad 1$ *in* L_K.

Beweis: Ist $\alpha \quad \mathcal{O}_K$, so ist $N\ \alpha \qquad 1$, also gilt $\log N\ \alpha \qquad 0$ und damit

$$\sum_i {}_i\ \alpha \qquad 0$$

Daher ist E in der reellen Ebene $H \quad L_K$ mit der Gleichung

$$x_1 \qquad x_{r_1\ r_2} \quad 0$$

enthalten. Es reicht also zu zeigen, dass E ein vollständiges Gitter in H ist. Dies ist wegen Lemma D.9 äquivalent dazu, dass E diskret in H ist und $H \ E$ kompakt ist.

Um zu zeigen, dass E diskret ist, wähle ein $R \quad 0$. Die Menge aller $\alpha \quad \mathcal{O}_K$ mit $\quad \alpha \qquad R$ ist enthalten im Bild unter $\quad$ der Menge aller α mit

$$\sigma_i\ \alpha^{\ \varepsilon_i} \quad \exp R$$

wobei $\varepsilon_i \quad 1$ oder 2. Da $\sigma\ \mathcal{O}_K$ als Gitter diskret in V_K ist, folgt die Endlichkeit dieser Menge. Hieraus folgt, dass $0 \quad E$ eine Umgebung besitzt, die nur endlich viele Punkte von E enthält. Da E eine Gruppe ist, folgt daraus die Diskretheit von E.

Wir zeigen nun, dass $H \ E$ kompakt ist. Dazu wählt man Konstanten $c_j \quad 0$ mit

$$c_1 c_2 \quad c_{r_1\ r_2} \quad C: \quad \frac{4}{\pi}^{\ r_2} \text{vol}\ \sigma\ \mathcal{O}_K$$

und definiert damit die kompakte Produktmenge

$$U: \quad \{x \quad V_K: x_i^{\ \varepsilon_i} \quad c_i \text{ für } i \quad 1 \qquad r_1 \quad r_2$$

mit Lebesgue–Maß vol $U \qquad 2^{r_1}\pi^{r_2}c_1c_2 \quad c_{r_1\ r_2}$.

Sei ferner S die Menge

$$S: \quad \{x \quad V_K: N\ x \qquad \prod x_i^{\ \varepsilon_i} \quad 1 \qquad V_K$$

Damit gilt $\quad S \qquad H$. Bis auf assoziierte Elemente gibt es nach Satz D.2 nur endlich viele von Null verschiedene $\alpha \quad \mathcal{O}_K$ mit $N\ \alpha \qquad c_1c_2 \quad c_{r_1\ r_2}$. Seien diese $\alpha_1 \qquad \alpha_N$. Wir benutzen nun die punktweise Multiplikation, die auf V_K definiert ist, und setzen

$$U_S: \quad S \qquad \sigma\ \alpha_i \quad {}^1U \qquad \overset{N}{\underset{i\ 1}{}}$$

Die Menge U_S ist kompakt, da U kompakt ist. Wir behaupten, dass folgende Identität von Mengen gilt:

$$S \qquad \sigma\ e\ U_S \qquad \overset{}{\underset{e \quad K}{}}$$

Hieraus folgt

$$H\ E \qquad S \quad E \qquad U_S \quad E$$

und damit die Kompaktheit von $H\ E$, da U_S kompakt ist.

Beweis der Identität: Sei $y\ S$. Wir wissen bereits, dass $\sigma\ \mathcal{O}_K\ V_K$ ein vollständiges Gitter mit Volumen vol $\sigma\ \mathcal{O}_K$ ist. Multipliziert man dieses Gitter mit y, so erhält man ein vollständiges Gitter $y\sigma\ \mathcal{O}_K\ V_K$ mit Volumen

$$\text{vol}\ y\sigma\ \mathcal{O}_K\ \ \text{vol}\ \sigma\ \mathcal{O}_K$$

denn die Multiplikationsabbildung mit y hat die Determinante $N\ y$ nach Aufgabe 16.47 und in diesem Fall ist $N\ y\ \ 1$, da $y\ S$. Nach Wahl der c_j gilt

$$\text{vol}\ U\ \ 2^{r_1}\pi^{r_2}c_1c_2\ \ c_{r_1\ r_2}\ \ 2^{r_1}\pi^{r_2}\ \ \frac{4}{\pi}^{r_2}\ \text{vol}\ \sigma\ \mathcal{O}_K\ \ 2^n\text{vol}\ y\sigma\ \mathcal{O}_K$$

Nach dem Gitterpunktsatz von Minkowski gibt es also ein

$$0\ \ x\ \ U\ \ y\sigma\ \mathcal{O}_K$$

Ein solches x lässt sich schreiben als $x\ \ y\sigma\ \alpha$ mit $0\ \ \alpha\ \ \mathcal{O}_K$. Da $x\ \ U$ ist, erfüllt α die Gleichung $N\ \alpha\ \ N\ y\sigma\ \alpha\ \ N\ x\ \ c_1c_2\ \ c_{r_1\ r_2}$. Nach Wahl der α_i gibt es daher einen Index i und eine Einheit $e\ \ \mathcal{O}_K$, so dass $\alpha\ e\ \ \alpha_i$ ist, und daher

$$y\ \ \sigma\ \alpha\ \ ^1x\ \ \sigma\ e\ \sigma\ \alpha_i\ ^1\ x$$

Also gilt $y\ \ \sigma\ e\ U_S$. Da y beliebig war, folgt die behauptete Darstellung von S als Vereinigungsmenge.

Korollar D.26 *Die Gruppe $\mathcal{O}_K$ ist isomorph zu*

$$\mathcal{O}_{K\ \text{tors}}\ \ ^{r_1\ r_2\ 1}$$

Definition D.27 *Ein System von* Fundamentaleinheiten *ist eine –Basis*

$$e_1\ \ e_{r_1\ r_2\ 1}$$

des freien Anteils von $\mathcal{O}_K$. Den Regulator R_K *von K definiert man als den Betrag der Determinante eines beliebigen maximalen Minors der Matrix*

$$\begin{matrix} {}_1\ e_1 & & {}_1\ e_{r_1\ r_2\ 1} \\ \vdots & & \vdots \\ {}_{r_1\ r_2}\ e_1 & & {}_{r_1\ r_2}\ e_{r_1\ r_2\ 1} \end{matrix}$$

Der Regulator R_K hängt nicht von der Wahl der –Basis von Fundamentaleinheiten oder des Minors ab, wie wir gleich sehen werden.

Beispiel $K\ \ \mathbb{Q}\ \sqrt{2}$. Dann ist $\mathcal{O}_K\ \ 2\ \ $. Eine Fundamentaleinheit ist $u\ \ 1\ \ \sqrt{2}$. Der Regulator ist somit $R_K\ \ \log\ 1\ \ \sqrt{2}$.

Was bedeutet der Regulator? Die erste Antwort ist:

Satz D.28 *Das Volumen des Fundamentalbereichs des Einheitengitters in H ist*

$$\text{vol} \quad \mathcal{O}_K \qquad \sqrt{r_1 \quad r_2}\, R_K$$

Insbesondere ist $R_K \quad 0$ *und hängt nicht von den Fundamentaleinheiten oder der Wahl des Minors ab.*

Beweis: Seien $e_1 \qquad e_{r_1 \quad r_2 \quad 1}$ Fundamentaleinheiten. Setze

$$e \quad e_{r_1 \quad r_2} \quad \frac{1}{\sqrt{r_1 \quad r_2}} \; 1 \; 1 \qquad 1$$

e ist ein Vektor der Norm 1 und orthogonal zu H. Somit berechnet die Determinante

$$\det \begin{matrix} {}_{1}\, e_1 & & {}_{1}\, e_{r_1 \quad r_2} \\ \vdots & & \vdots \\ {}_{r_1 \quad r_2}\, e_1 & & {}_{r_1 \quad r_2}\, e_{r_1 \quad r_2} \end{matrix}$$

bis auf Vorzeichen das Volumen des aus dem Fundamentalbereich durch e erweiterten $r_1 \quad r_2$–dimensionalen Parallelotops. Addiert man die ersten $r_1 \quad r_2 \quad 1$ Zeilen zur letzten Zeile, so ergibt sich in der letzten Zeile der Vektor

$$0 \qquad 0 \; \sqrt{r_1 \quad r_2}$$

Somit folgt durch Entwicklung nach der letzten Zeile:

$$\text{vol} \quad \mathcal{O}_K \qquad \sqrt{r_1 \quad r_2}\, R_K$$

Betrachtet man statt der letzten Zeile eine andere, so ändert sich das Ergebnis nicht, d.h. R_K hängt nicht von der Wahl des Minors ab. Betrachtet man eine andere Basis von Fundamentaleinheiten, so wechselt die Determinante des betrachteten Minors höchstens das Vorzeichen, da ein Basiswechsel von –Basen der Multiplikation mit einer invertierbaren Matrix mit – Koeffizienten entspricht.

Die Klassenzahlformel

Nun kommen wir zu einer tiefer liegenden Antwort auf die Frage, was der Regulator bedeutet:

Definition D.29 *Man definiert die* Dedekindsche ζ–Funktion *eines Zahlkörpers K durch*

$$\zeta_K \; s \; : \quad {}_{0} \sum_{I \quad K} N \; I \quad {}^{s} \qquad \prod_{0} \; 1 \quad N \qquad {}^{s \quad 1}$$

wobei I alle ganzen Ideale und alle Primideale durchläuft. Diese Darstellungen konvergieren absolut für Re $s \quad 1$ *und definieren dort eine holomorphe Funktion [Z].*

Beispiel Die *Riemannsche* ζ–Funktion

$$\zeta \; s \quad \sum_{n \quad 1}^{\infty} \frac{1}{n^s} \qquad \prod_{p} \; 1 \quad p \quad {}^{s \quad 1}$$

ist der Spezialfall $K \quad \mathbb{Q}$.

Proposition D.30 *Im Fall quadratischer Zahlkörper $K = \mathbb{Q}(\sqrt{d})$ mit d quadratfrei hat man*

$$\zeta_K(s) = \zeta(s) \prod_p \left(1 - \frac{\Delta_K}{p} p^{-s}\right)^{-1}$$

Dabei ist das sogenannte Kronecker–Symbol $\frac{a}{2}$ für alle $a \equiv 0, 1 \bmod 4$ definiert durch

$$\frac{a}{2} = \begin{cases} 1 & \text{falls } a \equiv 1 \bmod 8 \\ -1 & \text{falls } a \equiv 5 \bmod 8 \\ 0 & \text{falls } a \equiv 0 \bmod 4 \end{cases}$$

Beweis: Die Diskriminante Δ_K ist entweder d oder $4d$, und es gilt immer $\Delta_K \equiv 0, 1 \bmod 4$. Außerdem ist $\frac{\Delta_K}{p} = \frac{d}{p}$ für alle ungeraden Primzahlen p, da 4 ein Quadrat ist. Um die Formel für $\zeta_K(s)$ mit Hilfe von Satz 17.14 und Bemerkung D.7 zu beweisen, machen wir eine Fallunterscheidung:

1. Ist p eine ungerade Primzahl und $p \mid d$, so ist p verzweigt, d.h. es gilt $p = \mathfrak{p}^2$ für ein Primideal $\mathfrak{p}$ der Norm p. Der Faktor $(1 - p^{-s})^{-1}$ im Produkt $\zeta_K(s)$ kommt daher nur einmal vor, was $\frac{d}{p} = \frac{\Delta_K}{p} = 0$ entspricht.

2. Gilt $p \nmid 2d$ und $\frac{d}{p} = \frac{\Delta_K}{p} = 1$, so bleibt p träge mit Norm p^2. Dies entspricht dem Produkt der Faktoren $(1 - p^{-s})^{-1}(1 - \frac{\Delta_K}{p} p^{-s})^{-1} = (1 - p^{2-s})^{-1}$.

3. Gilt $p \nmid 2d$ und $\frac{d}{p} = \frac{\Delta_K}{p} = -1$, so ist p voll zerlegt, d.h. $p = \mathfrak{p}_1\mathfrak{p}_2$ mit zwei verschiedenen Primidealen der Norm p. Der entsprechende Beitrag im Produkt ist $(1 - p^{-s})^{-1}(1 - \frac{\Delta_K}{p} p^{-s})^{-1} = (1 - p^{-s})^{-2}$.

4. Ist schließlich $p = 2$, so haben wir das Symbol $\frac{\Delta}{2}$ so definiert, dass die Produktdarstellung mit dem Verzweigungsverhalten aus Bemerkung D.7 kompatibel ist.

Die folgende *Klassenzahlformel*, die 1917 von E. Hecke in voller Allgemeinheit bewiesen wurde, beinhaltet die bisher eingeführten Größen h, w und Δ_K und zeigt insbesondere die Bedeutung des Regulators R_K:

Satz D.31 (Klassenzahlformel) *Sei K ein beliebiger Zahlkörper. $\zeta_K(s)$ hat eine analytische Fortsetzung auf $\mathbb{C}$ mit einem einfachen Pol bei $s = 1$ mit dem Residuum*

$$\operatorname{Res}_{s=1} \zeta_K(s) = \frac{2^{r_1} (2\pi)^{r_2} h}{w\sqrt{\Delta_K}} R_K$$

Beweis: Siehe [N, Kap. VII, Korollar (5.11)]. Einen Beweis im Fall quadratischer Zahlkörper findet man in [Z].

Es gibt eine *Funktionalgleichung*, die $\zeta_K(s)$ und $\zeta_K(1 - s)$ verbindet:

$$\zeta_K(1 - s) = \Delta_K^{s - \frac{1}{2}} \left(\cos\frac{\pi s}{2}\right)^{r_1 + r_2} \left(\sin\frac{\pi s}{2}\right)^{r_2} 2^n (2\pi)^{-sn} \Gamma(s)^n \zeta_K(s)$$

Für $K = \mathbb{Q}$ lautet sie in symmetrischer Schreibweise:

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-\frac{1-s}{2}}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s)$$

Benutzt man die Funktionalgleichung, so bekommt man eine *Variante der Klassenzahlformel*:

Korollar D.32 *Die Funktion $\zeta_K(s)$ hat eine Nullstelle der Ordnung $r_1 + r_2 - 1$ bei $s = 0$ und der erste nicht–triviale Taylorkoeffizient in der Entwicklung bei $s = 0$ ist*

$$\zeta_K(0) = \frac{h}{w} R_K$$

Die Klassenzahlformel kann man im Fall abelscher Zahlkörper, also zum Beispiel bei quadratischen Zahlkörpern oder Kreisteilungskörpern, weiter verfeinern und erhält so analytische Reihen, die die konkrete Berechnung der Klassenzahl h erlauben [H].

E Einführung in PARI/GP

PARI/GP ist ein freies Computeralgebra System, das für alle gängigen Computerplattformen verfügbar ist. Es gehört zu den besten Programmen zur Berechnung zahlentheoretischer Probleme und schlägt dabei meist die allseits bekannten, großen kommerziellen Systeme. Viele der Algorithmen aus diesem Buch sind in PARI/GP implementiert. Wir wollen hier kurz demonstrieren, wie man das System benutzt und in einigen Beispielen konkrete Probleme löst. Wir setzen voraus, dass eine Version von der Homepage p //p r . .u b rd u . r installiert und gestartet wurde. Man kann das Programm wie einen Taschenrechner benutzen, der entweder symbolisch exakt oder auf etwa 28 Stellen numerisch genau rechnet. Das Kommando

```
%
```

berechnet den Rest von 23 mod 5. Ausführlicher kann man den Quotient und Rest mit d r ausrechnen. Ebenso kann man Brüche in $\mathbb{Q}$ addieren und multiplizieren, transzendente Funktionen wie sin π 2 berechnen oder einen ggT berechnen:

```
/  /

s  P /

 d          0
```

Primzahltests führt man mit dem Kommando

```
spr    0000
```

durch. Dies liefert hier das Ergebnis 1, also ist 700001 eine Primzahl. Durch

```
? spr
```

wird eine Hilfe aufgerufen, die erklärt, welcher Primzahltest verwendet wird und welche Optionen möglich sind. Ein einfaches ? ruft eine allgemeine Hilfe auf. Mit

```
r  ^
```

faktorisiert man die Fermat Zahl 2^{128} 1. Das Kommando

```
r    s r
```

liefert das bekannte periodische Ergebnis 2 2 2 2 2 . In den Ringen n kann man rechnen, indem man Elemente durch

```
d    0
```

in diesem Fall also 23 mod 103 definiert. Potenzen von a berechnet man einfach mit

```
^ 0
```

S. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie,*
DOI 10.1007/978-3-8348-8263-9,

um z.B. den kleinen Satz von Fermat zu testen. Wenden wir uns jetzt einer Berechnung in Zahlkörpern zu. Sei K der Kreisteilungskörper $K \quad \mathbb{Q}\ \zeta$, wobei ζ eine Nullstelle des Polynoms $P \quad X^4 \quad X^3 \quad X^2 \quad X \quad 1$ ist, siehe Aufgabe 16.43. In der folgenden Sitzung wird K definiert und dann einige Invarianten berechnet:

```
K b          ^    ^    ^          (definiert K)
K.p                                (definierendes Polynom)
K.s                                (r    0, r    2)
K.                                 (Basis von O_K)
K.d s                              (Diskriminante Δ    125)
K.r    s                           (alle Nullstellen von P)
K. u                               (Fundamentaleinheiten in O_K)
K. u                               (Torsionseinheiten)
K. u u                             (alle Einheiten)
K.    p                            (Klassengruppe)
K.r                                (Regulator)
```

Natürlich hat PARI/GP viele weitere Möglichkeiten, und wir regen an, diese selbst auszuprobieren.

F Lösungshinweise zu den Aufgaben

Aufgabe 1.2: Im Fall $p \quad 4k \quad 1$ betrachtet man die ungerade Zahl $P \quad 4\prod p_i \quad 1$, wobei p_i alle ungeraden Primzahlen der Form $4k \quad 1$ durchläuft. P ist von der selben Form, aber nicht durch ein p_i teilbar. Man beachte, dass P nicht Produkt von Primfaktoren der Form $4k \quad 1$ sein kann, da ein solches wieder von der Form $4k \quad 1$ wäre. Somit muss es einen Teiler der Form $4k \quad 1$ geben und man kann wie im Satz von Euklid schließen. Im Fall $p \quad 4k \quad 1$ betrachte man $P \quad 4\prod p_i^2 \quad 1$, wobei p_i alle ungeraden Primzahlen der Form $4k \quad 1$ durchläuft.
Aufgabe 1.6: Sei $f \; T \quad a_0 \quad a_1 T \quad a_d T^d$ ein Polynom mit Primzahlwerten auf $_0$. Es gelte oBdA $a_d \quad 0$. Damit ist $f \; x \quad \infty$ für $x \quad \infty$. $p \quad f \; 0 \quad a_0$ ist eine Primzahl und damit ist $f \; m \; a_0$ durch p teilbar und damit nicht mehr prim für $m \gg 0$.
Aufgabe 1.7: Faktorisieren Sie $n^2 \quad 1$ und $n^4 \quad 1$ mit der binomischen Formel.
Aufgabe 1.8: Benutzen Sie das Sieb des Eratosthenes.
Aufgabe 1.9: Zeigen Sie, dass diese Zahlen der Reihe nach durch $2 \; 3 \quad$ teilbar sind.
Aufgabe 1.10: Jeweils eine der Zahlen ist durch 3 teilbar.
Aufgabe 1.11: Falls $n \; p$ zwei weitere Primfaktoren hat, so gilt $n \quad p^3$.
Aufgabe 1.12: Zu 1.: Die Zahl $p_1 p_2 \quad p_k \quad 1$ ist teilerfremd zu $p_k \; _1$ und ist daher entweder prim oder durch eine Primzahl p_m mit $m \quad k$ teilbar. Es folgt $p_k \; _1 \quad p_1 p_2 \quad p_k \quad 1$. Zu 2.: Wir zeigen sogar $p_n \quad 2^{2^n}$ mit Induktion über n. Es gilt $p_n \; _1 \quad p_1 p_2 \quad p_n \quad 1 \quad 2^{2^1} 2^{2^2} \quad 2^{2^n} \quad 1 \quad 2^{2^n \; 1 \; 2} \quad 1 \quad 2^{2^n \; 1}$. Zu 3.: Aus 2. folgt $\pi \; 2^{2^n} \quad n$. Zu $x \quad 2$ wähle n mit $e^{e^n \; 1} \quad x \quad e^{e^n}$. Dann folgt $e^n \; 1 \quad 2^n$, falls $n \quad 2$ und daher $\pi \; x \quad \pi \; e^{e^n \; 1} \quad \pi \; e^{2^n} \quad \pi \; 2^{2^n} \quad n \quad \log\log x$.
Aufgabe 2.4: Die Eindeutigkeit ist einfach. Für die Existenz betrachte $q \quad \frac{a}{b}$.
Aufgabe 2.6: Benutzen Sie $\quad 2 \quad 7i \quad 1 \quad i \quad \frac{5}{2} \quad \frac{9}{2} i$.
Aufgabe 2.7: Der Fall $\sqrt{2}$ geht wie i. Versuchen Sie, in $\sqrt{\;5}$ die Zahl $1 \quad \sqrt{\;5}$ durch 2 zu teilen.
Aufgabe 2.13: Für die Irreduzibilität mache man einen Ansatz zur Zerlegung von $2 \quad \sqrt{\;5}$. Um zu zeigen, dass $2 \quad \sqrt{\;5}$ nicht prim ist, kann man $2 \quad \sqrt{\;5} \; 2 \quad \sqrt{\;5} \quad 9 \quad 3 \; 3$ nutzen.
Aufgabe 2.20: $47355 \quad 3 \; 5 \; 7 \; 11 \; 41$.
Aufgabe 2.21: Betrachten Sie das Ideal, das von X und 3 erzeugt wird, und zeigen Sie, dass es kein Hauptideal ist.
Aufgabe 2.22: Betrachten Sie die Nullstellen von f : .
Aufgabe 2.23: $8 \; 14 \; 36 \quad 2$ und $2X^3 \quad X^2 \quad 2X \quad 1 \; 6X^2 \quad 13X \quad 5 \quad 2X \quad 1$.
Aufgabe 2.24: I_1 ist kein Hauptideal, siehe Aufgabe 2.21. I_2 enthält das Element 1, ist also ein Hauptideal.
Aufgabe 2.25: Benutzen Sie Polynomdivision mit Rest für 1. und 2. Es gilt $X^4 \quad 8X^3$

S. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie,*
DOI 10.1007/978-3-8348-8263-9,

$14X^2 \quad 8X \quad 15 \quad X \quad 1 \; X \quad 5 \; X \quad 3 \; X \quad 1$.

Aufgabe 2.26: Für $\sqrt{2}$ betrachten Sie die Funktion $N\ a \quad b\sqrt{2} \quad a^2 \quad 2b^2$ und argumentieren wie bei i . Bei $\sqrt{3}$ betrachtet man $N\ a \quad b\sqrt{3} \quad a^2 \quad 3b^2$.

Aufgabe 2.27: Betrachten Sie die euklidische Funktion $N\ a \quad b\sqrt{7} \quad a^2 \quad 7b^2$ für $1 \quad \sqrt{7} \quad 2$. Bei $\sqrt{7}$ studieren Sie $1 \quad \sqrt{7} \quad 1 \quad \sqrt{7} \quad 2^3$.

Aufgabe 2.28: Ist $b \quad 0$ und $N' \; b \quad N \; b$, so gibt es kein Problem bei der Division mit Rest. Ist dagegen $N' \; b \quad N \; b$, so gilt $N' \; b \quad N \; bc$ für ein $c \quad R$. Zeigen Sie zuerst, dass $N' \; bc \quad N \; bc$. Teilen Sie dann mit Rest durch bc statt durch b, indem Sie die Division mit Rest für N verwenden.

Aufgabe 2.29: Berechnen Sie jeweils die Norm in i und suchen Sie nach gemeinsamen Primteilern der Normen.

Aufgabe 2.30: Faktorisieren Sie die Zahlen zuerst. Ist eine Primzahl p teilbar durch $a \quad ib$ in i , so wird sie bereits von $a^2 \quad b^2$ geteilt. Somit ist $p \quad 2$ oder $p \quad 1 \bmod 4$.

Aufgabe 3.4: ggT 3080 7956 4.

Aufgabe 3.6: $x \quad 3k \quad 1$ und $y \quad 1 \quad 2k$ für k .

Aufgabe 3.8: ggT 3080 7956 4.

Aufgabe 3.10: ggT 3080 7956 4 979 3080 379 7956.

Aufgabe 3.11: Die meisten Programmiersprachen haben Kommandos wie `d` und `d` zum Teilen oder Restbilden bereits implementiert.

Aufgabe 3.14: ggT 681 361 1 44 681 83 361 und ggT 12345 54321 3 3617 12345 822 54321.

Aufgabe 3.15: ggT $x^3 \quad 4x^2 \quad x \quad 6 \; x^4 \quad 14x^3 \quad 59x^2 \quad 46x \quad 120 \quad x \quad 1$.

Aufgabe 3.16: Benutzen Sie Polynomdivision mit der „Variablen“ 2.

Aufgabe 3.17: Benutzen Sie die Diskussion von i aus Abschnitt 2.

Aufgabe 3.18: Euklidischer Algorithmus.

Aufgabe 3.19: Benutzen Sie die binomische Formel $a^2 \quad b^2 \quad a \quad b \; a \quad b$.

Aufgabe 3.20: Euklidischer Algorithmus.

Aufgabe 4.3: Fertigen Sie Tabellen für die $10^i \bmod n$ an.

Aufgabe 4.4: Rechnen Sie modulo 7 und berücksichtigen Sie alle tatsächlich vorkommenden Schaltjahre. Auf Unix–Rechnern kann man mit dem Kommando `0` das Ergebnis (Mittwoch) ablesen.

Aufgabe 4.9: $x \quad 64 \bmod 101$.

Aufgabe 4.13: Zuerst ein Spezialfall: Wir wollen die simultanen Kongruenzen $x \quad a_i \bmod m_i$ für $1 \quad i \quad n$ lösen, wobei alle m_i paarweise teilerfremd sind. Dazu betrachte $M : \; \prod_i m_i$ und $M_i : \; M \; m_i$. Dann sind M_i und m_i teilerfremd, und wir können die Gleichungen $M_i \; c_i \quad 1 \bmod m_i$ lösen. Die Zahlen $e_i : \; M_i \; c_i$ bilden dann eine Teilung der Eins, d.h. $e_i \quad 0 \bmod m_j$ für $i \quad j$ und $e_i \quad 1 \bmod m_i$. Eine Lösung ist damit offensichtlich $\sum_i e_i \; a_i$, und diese ist eindeutig modulo M. Im allgemeinen Fall betrachte man $M : \; \mathrm{kgV} \; m_1 \quad m_n$ anstelle des Produktes und argumentiere analog weiter.

Aufgabe 4.14: $3^{100} \quad 1 \bmod 16$, also ist das Ergebnis 3.

Aufgabe 4.15: $7^{67839} \quad 3 \bmod 10$ und $2^{67839} \quad 8 \bmod 10$.

Aufgabe 4.16: Zu 1.: $x \quad 4 \bmod 13$. Zu 2.: $x \quad 9 \bmod 20$ und $x \quad 19 \bmod 20$. Zu 3.: $x \quad 77 \bmod 630$. Zu 4.: $x \quad 101 \bmod 221$.

Aufgabe 4.17: Berechnen Sie ggT 12 30 6 und untersuchen Sie, ob Sie damit die Schulden ausgleichen können.

Aufgabe 4.18: Lösen Sie die simultanen Kongruenzen $x \quad 1 \bmod 7$ und $x \quad 3 \bmod 5$. Das Ergebnis ist $x \quad 218$.

Aufgabe 4.19: Lösen Sie die simultanen Kongruenzen $x \equiv 2 \bmod 13$ und $x \equiv 11 \bmod 17$. Das Ergebnis ist $x \equiv 470$.

Aufgabe 4.20: Wegen $2^n \equiv 1 \bmod p$ gilt $d \mid n$. Angenommen, es gilt $n = dd'$ und $2^d - 1 = kp^2$. Dann folgt $2^n - 2^{dd'} - 1 = kp^{2d'} - 1^{d'} \equiv 1 \bmod p^2$, ein Widerspruch.

Aufgabe 4.21: Zuerst zeigt man die folgende Aussage: Sind x, y teilerfremd, dann haben $x + y$ und $\frac{x^p + y^p}{x + y}$ höchstens den gemeinsamen Primfaktor p. Ist nämlich p' irgendein gemeinsamer Faktor, so folgt $0 \equiv \frac{x^p + y^p}{x + y} \equiv x^{p-1} - x^{p-2}y + \cdots + y^{p-1} \equiv px^{p-1} \bmod p'$ wegen $y \equiv x \bmod p'$ und damit $p = p'$. Benutzt man diese Aussage, so bekommt man ganze Zahlen a und c mit $x + y = a^p$ und $\frac{x^p + y^p}{x + y} = c^p$. Ebenso $y + z = b^p$ und $x + z = d^p$. Sei $q = 2p + 1$. Der Fall $q \mid xyz$ kann nicht auftreten, denn $1 + 1 + 1 \not\equiv 0 \bmod q$. Also $q \nmid xyz$. Angenommen $q \nmid x$ sowie $q \nmid yz$. Dann folgt $2x + y + z \equiv b^p - a^p - d^p \bmod q$, also muss b durch q teilbar sein, und es gilt $y + z \equiv 0 \bmod q$. Wegen $\frac{y^p + z^p}{y + z} = t^p$ mit $t \in \mathbb{Z}$ bekommen wir $t^p \equiv py^{p-1} \bmod q$. Da q die Zahl t nicht teilt, folgt $py^{p-1} \not\equiv 1 \bmod q$. $x + y \equiv a^p \bmod q$ impliziert dann $y \equiv a^p \bmod q$ und damit $p \equiv 1 \bmod q$, ein Widerspruch!

Aufgabe 5.6: Benutzen Sie die Linearkombination $1 = 4 \cdot 13 - 3 \cdot 17$.

Aufgabe 5.7: Der Kern der natürlichen Abbildung $\mathbb{Z} \to \mathbb{Z}_m \times \mathbb{Z}_n$ ist immer durch alle Vielfachen von kgV (m, n) gegeben. Ist Φ ein Isomorphismus, so ist der Kern aber gerade $\{0\}$.

Aufgabe 5.11: $U_2 = \{1\}$, $U_3 = \{1, 2\}$, $U_4 = \{1, 3\}$, $U_5 = \{1, 2, 3, 4\}$, $U_6 = \{1, 5\}$, $U_7 = \{1, 2, 3, 4, 5, 6\}$, $U_8 = \{1, 3, 5, 7\}$, $U_9 = \{1, 2, 4, 5, 7, 8\}$, $U_{10} = \{1, 3, 7, 9\}$, $U_{11} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, $U_{12} = \{1, 5, 7, 11\}$, $U_{13} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$, $U_{14} = \{1, 3, 5, 9, 11, 13\}$, $U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$.

Aufgabe 5.16: Ist $n = p^\alpha$, so ist $\sum_{d \mid p^\alpha} \varphi(d) = 1 + \sum_{1 \le \beta \le \alpha} p^{\beta-1}(p-1) = 1 + (p-1)\frac{1 - p^\alpha}{1 - p} = p^\alpha$. Nutzen Sie nun die Multiplikativität von φ.

Aufgabe 5.20: $3^4 = 0 \bmod 7$, $3^4 = 1 \bmod 7$, $3^{4+4} = 6 \bmod 7$ und $3^{4+4+1} = 3^2 = 6 \bmod 7$.

Aufgabe 5.22: Ist $n = p^\alpha$, so ist $\varphi(n) = p^{\alpha-1}(p-1) = n - n/p$. Also ist n in diesem Fall prim genau dann, wenn $\alpha = 1$ ist. Ist n beliebig und p ein Primfaktor von n, so ist ebenfalls $\varphi(n) = n - n/p$, also zeigt das gleiche Argument, dass $n = p$ ist.

Aufgabe 5.23: Ist p ungerade, so ist $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$ gerade für $\alpha \ge 1$. $\varphi(2^\alpha)$ ist gerade für $\alpha \ge 2$.

Aufgabe 5.24: Betrachten Sie die Struktur Fermatscher Primzahlen sowie die Formel für $\varphi(n)$ genauer.

Aufgabe 5.25: Benutzen Sie $0 = a^3 - 1 = (a-1)(a^2 + a + 1)$ und die Binomialformel.

Aufgabe 5.26: $\varphi(143) = 120$, $e = 11$, $d = 11$ und $17^{11} \equiv 127 \bmod 143$.

Aufgabe 5.27: Benutzen Sie die gleiche Methode wie im Beweis des Satzes von Wilson: Sei p eine Primzahl mit $p \equiv 1 \bmod 4$ und $p \mid a^2 + b^2$. Setzen Sie $c := ab^{-1} \bmod p$ und zeigen Sie, dass $c^2 \equiv -1 \bmod p$. Lösungen für $p = 5, 13, 17, 29$ sind 2, 5, 13, 12.

Aufgabe 5.28: $\ker\varphi = \{a \mid a \equiv 0 \bmod n, a \equiv 0 \bmod m\} = \{a \mid a \equiv 0 \bmod \text{kgV}(m, n)\} = \{a \mid a \equiv 0 \bmod mn\}$. Die linke Abbildung ist die Inklusion $\ker\varphi = \{0\}$ und die rechte Abbildung ist gegeben durch $a \mapsto b \equiv a \bmod d$. Dann folgt $n = m \cdot \text{Im}\varphi = \text{ggT}(m, n)$.

Aufgabe 5.29: Die Anzahl τ und Summe σ von Teilern einer Zahl sind nach dem Distributivgesetz offensichtlich multiplikativ für teilerfremde m, n.

Aufgabe 5.30:

$$f \quad g \quad mn \qquad \sum_{d \; mn} f \; d \; g \; \frac{mn}{d} \qquad \sum_{\substack{d_1 \; m \; d_2 \; n \\ \text{ggT} \; d_1 \; d_2 \quad 1}} f \; d_1 d_2 \; g \; \frac{mn}{d_1 d_2}$$

$$\sum_{d_1 \; m} \sum_{d_2 \; n} f \; d_1 \; f \; d_2 \; g \; \frac{m}{d_1} \; g \; \frac{n}{d_2} \qquad f \quad g \quad m \quad f \quad g \quad n$$

Aufgabe 5.31: Ist $\mu \; n \qquad 1 \; ^{k}$ für quadratfreies n, so gibt k die Anzahl der Primfaktoren an und ist bei teilerfremden $m \; n$ offenbar additiv modulo 2.
Aufgabe 5.32: Man zeigt genauer: Die Abbildungen $f \quad f \quad 1$ und $g \quad \mu \quad g$ auf dem Raum der zahlentheoretischen Funktionen sind invers zueinander. Dies impliziert, dass $g \quad \mu \quad g \; 1 \quad g \quad \mu \quad 1$, da die Faltung offensichtlich kommutativ ist. Also reicht es zu zeigen, dass $\mu \quad 1 \quad 1 \quad \mu \quad e$ gilt, wobei e die Funktion mit $e \; 1 \qquad 1$ und $e \; n \qquad 0$ für $n \quad 2$ ist, das neutrale Element bei der Faltung. Dazu betrachtet man das Polynom $F \quad \prod_{p \; n} 1 \quad X_p$, wobei X_p eine Variable für jede Primzahl p ist. F hat im Fall $n \quad 2$ den Koeffizienten $\mu \; p_1 \quad p_l$ bei $X_{p_1} \quad X_{p_l}$. Also gilt: $\mu \quad 1 \quad n \quad \sum_{d \; n} \mu \; d \quad F \; 1 \qquad 1 \quad 0$.
Aufgabe 6.2: Die Definition impliziert sofort, dass $1 \quad g \quad g, m \quad n \; g \qquad mn \quad g, \; m \quad n \quad g$ $m \; g \quad n \; g$ und $m \quad g \quad g' \qquad m \; g \quad m \; g'$.
Aufgabe 6.4: Beide Seiten sind jeweils die kleinste Untergruppe, die g enthält.
Aufgabe 6.9: Zeigen Sie zuerst, dass die Determinante eine Einheit in ist.
Aufgabe 6.10: Suchen Sie eine Matrix in GL $k \; \mathbb{Q} \quad \text{Mat} \; k \qquad$ mit Determinante $\qquad 1$.
Aufgabe 6.14: Wenn man dem Diagonalisierungsalgorithmus folgt, ist die zugehörige Diagonalmatrix genau $1 \; 4 \; 2 \; 0$.
Aufgabe 6.18: Die Gruppe ist jeweils $\qquad 4 \qquad 2$.
Aufgabe 6.19: Faktorisieren Sie alle $n \quad 30$ und wenden Sie Satz 6.13 an.
Aufgabe 6.20: Die zugehörige Diagonalmatrix ist $2 \; 6 \; 30 \; 210 \; 0$ mit dem Diagonalisierungsalgorithmus folgt. Also ist $G \qquad 2 \qquad 6 \qquad 30 \qquad 210$. Nun sortiere.
Aufgabe 6.21: Die zugehörige Diagonalmatrix ist $2 \quad 3$, wenn man zuerst dem Diagonalisierungsalgorithmus folgt.
Aufgabe 6.22: Der Isomorphismus ist gegeben durch $z \quad z \; p^{l}$.
Aufgabe 6.23: Gruppen der Form $\quad m \quad$ sind niemals Untergruppen von $\; ^{k}$, da $\; ^{k}$ keine Elemente a mit $ma \quad 0$ enthält.
Aufgabe 6.24: Betrachten Sie eine Primzahl $p \quad n_l$ und den $\quad p \;$ –Vektorraum $G \; pG$.
Aufgabe 6.25: Zu 1: Angenommen $\mathbb{Q} \qquad$ ist ein Produkt von zyklischen Gruppen der Form $\prod_I \qquad \prod_J \quad n_j$. Betrachte dann das Element 1 in diesem Produkt. Auf welche Elemente in diesem Produkt wird dann $1 \quad n$ abgebildet? Zu 2: Ist $\mathbb{Q} \quad$ durch $q_1 \qquad q_m$ erzeugt, so wähle eine Primzahl, die in keinem der Nenner der q_i auftaucht. Dann ist $p \quad ^{1} \quad \mathbb{Q}$, Widerspruch!
Aufgabe 6.26: Man kann nach dem Diagonalisierungsalgorithmus annehmen, dass R $d_1 \qquad d_n$ diagonal ist. Dann ist $\det R \qquad d_1 d_2 \quad d_n \quad \text{ord} \; G$.
Aufgabe 6.27: Sei $\; ^{k} \qquad ^{k}$ die Abbildung, die durch Multiplikation mit einer Matrix A gegeben wird. Der Diagonalisierungsalgorithmus über liefert die Diagonalmatrix $1 \; 1 \qquad 1$ und die Transformationsmatrix A als Kombination von Elementarmatrizen.
Aufgabe 7.6: Mit $x \quad 3$ gilt $3^2 \quad 9 \quad 1 \mod 2^3$, aber $3 \quad 1 \mod 2^2$ für $r \quad 3$. Das Problem beim Hilfssatz ist der Induktionsschritt von 2 nach 3. Das Problem wird aber im Fall $x \quad 1 \mod 4$ eliminiert.
Aufgabe 7.8: Das kann passieren: $p \quad 3, r \quad 2, \zeta \quad 2$ und $\zeta \quad p \quad 5$.

Aufgabe 7.10: Folgt aus Lemma 5.13, Satz 7.7 und Satz 7.9.
Aufgabe 7.11: Genau die angegebenen Elemente erzeugen U_n, denn jede andere Potenz von ζ ist nicht primitiv und ζ lässt sich durch diese Elemente wieder darstellen.
Aufgabe 7.13: Lösungen sind $13^3 \quad 4 \bmod 17$, $2^3 \quad 5^3 \quad 6^3 \quad 8 \bmod 13$ und $1^2 \quad 8^2 \quad 13^2 \quad 20^2 \quad 1 \bmod 21$. Beachten Sie, dass U_{21} nicht zyklisch ist und benutzen Sie zuerst Lemma 5.13, um zu einer ähnlichen Situation wie im Beispiel im Text zu kommen.
Aufgabe 7.15: Die kleinste Primitivwurzel zu $p \quad 17$ ist 3. Ihre Potenzen 3^i mit ggT $i \; \varphi \; 17 \quad 1$ sind 3 10 5 11 14 7 12 6. Für $p \quad 31$ bekommt man die Primitivwurzeln 3 17 13 24 22 12 11 21 3 und für $p \quad 43$ die Liste 3 28 30 12 26 19 34 5 18 33 20 29 jeweils als aufeinanderfolgende Potenzen der 3.
Aufgabe 7.16: $\log_2 11 \quad 30 \bmod 37$ und $\log_5 65 \quad 27 \bmod 547$.
Aufgabe 7.17: $x \quad 20 \; 32 \; 34 \bmod 43$ bzw. $x \quad 3 \; 4 \; 11 \; 17 \; 18 \; 24 \; 31 \; 32 \bmod 35$.
Aufgabe 7.18: $\quad 14 \quad 2 \quad 7$. Es gibt aber kein n mit $\#U_n \quad 7$.
Aufgabe 7.19: $m \quad 29, 43$ und 49 erfüllen $7 \quad \varphi \; m$. Daher ist $\quad 7 \quad ^3$ eine Untergruppe von U_n mit $n \quad 29 \; 43 \; 49$.
Aufgabe 7.20: Ist $p \quad 3$, so ist $U_{p^k \; 1}$ zyklisch mit Erzeuger ζ. Dann wird der Kern durch alle Potenzen von ζ^{p^k} erzeugt und ist isomorph zu $\quad p$.
Aufgabe 7.21: U_{10} ist isomorph zu $\quad 4$ mit Erzeuger $\zeta \quad 7$. U_{27} ist isomorph zu $\quad 18$ mit Erzeuger $\zeta \quad 2$. U_{80} ist isomorph zu $\quad 2 \quad 4 \quad 4$ mit Erzeugern $\zeta \quad 31 \; 21 \; 17$. U_{100} ist isomorph zu $\quad 2 \quad 20$ mit Erzeugern $\zeta \quad 51 \; 77$. U_{300} ist isomorph zu $\quad 2 \quad 2 \quad 20$ mit Erzeugern $\zeta \quad 151 \; 101 \; 277$.
Aufgabe 7.22: Ausprobieren.
Aufgabe 7.23: 1) Die möglichen Ordnungen von 2 modulo p sind 1 2 4 a $2a$ und $4a$. Es gilt $2^4 \quad 16 \quad 1 \bmod p$, da $p \quad 3 \; 5$, also sind die Ordnungen 1 2 4 unmöglich. Falls die Ordnung a oder $2a$ ist, so ist 2 ein quadratischer Rest modulo p. Dies widerspricht aber $p \quad 4a \quad 1 \quad 5 \bmod 8$. 2) Die Ordnung von $\quad 2$ ist ein Teiler von $2q$ wegen dem kleinen Fermat. Dann argumentiert man wie in 1).
Aufgabe 7.24: Benutzen Sie Satz 7.9 und rechnen Sie in der additiven Gruppe $\quad 2 \quad 32$.
Aufgabe 7.25: Direkte Anwendung des Algorithmus.
Aufgabe 7.26: Benutzen Sie Satz 7.7 und den chinesischen Restsatz.
Aufgabe 7.27: Benutzen Sie Satz 7.9 und den chinesischen Restsatz.
Aufgabe 8.1: $p \quad 3$: $4a \; ay^2 \quad by \quad c \quad 2ay^{\;2} \quad 4aby \quad 4ac \quad 2ay^{\;2} \quad 2 \quad 2ay \; b \quad 4ac \quad 2ay \quad b^{\;2} \quad 4ac \quad b^2$. Setze also $x \quad 2ay \quad b$ und $d \quad b^2 \quad 4ac$. Im Fall $p \quad 2$ gibt es die Gleichungen $y^2 \quad y \quad 1 \quad 0, y^2 \quad 1 \quad 0, y^2 \quad y \quad 0$ sowie $y^2 \quad 0$. Die erste davon besitzt keine Lösung, die anderen haben die Lösungen $y \quad 1, y \quad 0 \; 1$ sowie $y \quad 0$.
Aufgabe 8.4: Ist p ungerade und ζ Primitivwurzel, so hat ζ keine Quadratwurzel modulo p mehr, sonst wäre ζ eine gerade Potenz einer anderen Primitivwurzel. Ein Gegenbeispiel für die Umkehrung ist $p \quad 3 \bmod 4$ und $\zeta \quad 1 \bmod p$. Dann ist $\quad \frac{1}{p} \quad 1 \quad ^{\frac{p \; 1}{2}} \quad 1$, aber ζ ist keine Primitivwurzel für $p \quad 7$, da $\zeta^2 \quad 1 \bmod p$.
Aufgabe 8.11: Suchen Sie Primzahlen $p \quad q$ und ein a mit $\quad \frac{a}{p} \quad \frac{a}{q} \quad 1$ und setzen Sie $n \quad pq$.
Aufgabe 8.13: $\quad \frac{37}{859} \quad 1$ und $\quad \frac{10270}{25511} \quad 1$.
Aufgabe 8.14: $51 \quad 3 \quad 17$ und $\quad \frac{41}{3} \quad \frac{41}{17} \quad 1$.
Aufgabe 8.16: $x^2 \quad 56 \bmod 113$ hat Lösungen $x \quad 13 \bmod 113$.
Aufgabe 8.17: Siehe Hinweis in Aufgabenstellung.

Aufgabe 8.18: $x^2 \equiv 6 \bmod 43$ bzw. $x^2 \equiv 881 \bmod 4073$ haben jeweils die Lösungen $x \equiv 7 \bmod 43$ bzw. $x \equiv 257 \bmod 4073$.

Aufgabe 8.19: Wenn die Diskriminante ein Quadrat ist, gibt es zwei Lösungen (mit Vielfachheit), sonst keine.

Aufgabe 8.20: $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}\frac{3-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right) = 1 \Leftrightarrow p \equiv 1 \bmod 6$, da p ungerade ist.

Aufgabe 8.21: $\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) = 1 \Leftrightarrow p \equiv 1 \bmod 12$.

Aufgabe 8.22: $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{p^2-1}{8}} = 1 \Leftrightarrow p \equiv 1 \bmod 8$.

Aufgabe 8.23: Berechnen Sie $\left(\frac{75}{p}\right)$ mit dem Reziprozitätsgesetz.

Aufgabe 8.24: Es reicht zu zeigen, dass 2 ein quadratischer Rest ist.

Aufgabe 8.25: Reziprozitätsgesetz für das Jacobisymbol.

Aufgabe 8.26: $10403 = 101 \cdot 103$ und man berechnet die Legendresymbole. Eines davon ist -1, daher gibt es keine Lösung.

Aufgabe 8.27: Für jede Lösung a, b betrachten Sie weitere Lösungen, z.B. $a^2 - b^2$, die Sie daraus konstruieren können.

Aufgabe 9.3: $178 = 3^2 + 13^2$, $373 = 7^2 + 18^2$ und $4797 = 6^2 + 69^2$.

Aufgabe 9.7: Die Darstellung ist nicht eindeutig, denn man kann ein Produkt $(a^2 + b^2)(c^2 + d^2)$ $= (ac - bd)(ac - bd)(cd + cd)$ als $N = (ac - bd)(cd + cd)$ oder als $N = (ac - bd)(cd + cd)$ schreiben, ähnlich bei mehr Faktoren. Minimale Beispiele sind $50 = 7^2 + 1 = 5^2 + 5^2$, $325 = 1^2 + 18^2 = 6^2 + 17^2 = 10^2 + 15^2$ und $1105 = 4^2 + 33^2 = 9^2 + 32^2 = 12^2 + 31^2 = 23^2 + 24^2$.

Aufgabe 9.8: Verwenden Sie Satz 9.2.

Aufgabe 9.9: Imitieren Sie den Beweis von Satz 9.6.

Aufgabe 9.10: Wir beweisen zuerst den Zwei–Quadrate Satz für eine Primzahl p mit $p \equiv 1 \bmod 4$. Sei also $u \equiv \zeta^{\frac{p-1}{4}} \bmod p$, wobei ζ eine Primitivwurzel ist. Betrachte das Gitter $\Gamma \subset \mathbb{Z}^2$ aller Paare x, y mit $y \equiv ux \bmod p$. Das Volumen des Fundamentalbereichs F ist p, da $[\mathbb{Z}^2 : \Gamma] = p$. Die Kreisscheibe M um den Ursprung in $\mathbb{R}^2$ mit Radius $r = \sqrt{3p - 2}$ hat vol $M = \pi r^2 > 4p$. Nach dem Gitterpunktsatz von Minkowski gibt es ein $x, y \in \Gamma$ mit $0 < x^2 + y^2 = r^2 < 3p - 2$. Es ist also $0 < x^2 + y^2 < 2p$. Andererseits gilt $x^2 + y^2 = x^2 + u^2x^2 \equiv 0 \bmod p$. Also ist $x^2 + y^2 = p$.

Zum Vier–Quadrate Satz: Sei $p > 3$ prim. Es gibt Zahlen $u, v < p$ mit $u^2 + v^2 + 1 \equiv 0 \bmod p$ nach dem Schubfachprinzip, denn sowohl u^2 als auch $-1 - v^2$ nehmen $\frac{p-1}{2}$ verschiedene Werte an. Wären diese alle verschieden, so gäbe es $p - 1$ verschiedene Zahlen in $\mathbb{Z}_p$, ein Widerspruch. Betrachte nun das Gitter $\Gamma = \{(a, b, c, d) \in \mathbb{Z}^4 : c \equiv ua + vb, d \equiv ub - va \bmod p\}$. Γ hat p^2 Elemente, also hat der Fundamentalbereich das Volumen p^2. Sei jetzt M eine Kugel mit Radius r und $r^2 = 1 + 9p$. Dann gilt vol $M = \frac{\pi^2 r^4}{2} > 16p^2$. Es gibt also einen Punkt $(0, a, b, c, d) \neq (0, 0, 0, 0, 0) \in \Gamma$ mit $2p > a^2 + b^2 + c^2 + d^2 \equiv 0 \bmod p$. Wie eben folgt $a^2 + b^2 + c^2 + d^2 = p$.

Aufgabe 9.11: Siehe Hinweise in der Aufgabenstellung.

Aufgabe 10.1: $17 \cdot 99 = 0 \cdot 5 + 1 \cdot 4 + 1 \cdot 2$.

Aufgabe 10.2: $y = 2 + \frac{2}{\ldots}$ bedeutet $y = 2 + \frac{1}{y}$, also $y = 1 + \sqrt{2}$. Damit ist $x = y - 1 = \sqrt{2}$.

Aufgabe 10.3: Berechnen Sie zuerst $a_m - a_n$ und machen Sie Induktion nach $n - m$.

Aufgabe 10.5: Mit Induktion folgt, dass $a_0 < b_0 < a_{n-1} < b_{n-1}$ sowie $a_{n-1} < \xi < b_{n-1} < \zeta$, also $a_n < b_n$ und $\xi < \zeta$.

Aufgabe 10.10: Zeigen Sie erst die stärkere Ungleichung $|p_n - \alpha q_n| < |p - \alpha q|$ für jeden Bruch p/q mit $1 \leq q < q_n$. Um dies zu zeigen, zeige man zunächst die Ungleichung

$p_{n-1} - \alpha q_{n-1}$ $p_n - \alpha q_n$ mittels der rekursiven Definition der Näherungsbrüche. Dies beweist, dass man die Behauptung durch Induktion über n zeigen kann, wenn man sich auf $q_{n-1} < q < q_n$ beschränkt.

Aufgabe 10.14: Die Eigenschaft Körperautomorphismus ist leicht zu zeigen. Wendet man den Automorphismus auf die Gleichung an, so ergibt sich, dass $\overline{x}$ ebenfalls eine Lösung x ist, da $x \in \mathbb{Q}$. Da die Gleichung genau zwei Lösungen hat, folgt die Behauptung.

Aufgabe 10.18: $x = \sqrt{m^2 - 1}$ bedeutet $x^2 = m^2 - 1$, also $x = m - x = m - 1$ oder $x = m - \frac{1}{m - x} = m\,\overline{2m}$.

Aufgabe 10.23: $1 + \sqrt{5} = 2\,\overline{1\ 3}$ und $\sqrt{3} + 2 = 0\,\overline{1\ 6\ 2}$.

Aufgabe 10.24: $x = \sqrt{m^2 - 1}$ bedeutet $x^2 = m^2 - x = m - x = m - 1$, also $x = m - \frac{1}{m - x}$.

Aufgabe 10.25: Der Kettenbruch zu $\sqrt{3}$ ist $1\,\overline{1\ 2}$, also sind die ersten Näherungsbrüche $\frac{2}{1}$, $\frac{5}{3}$, $\frac{7}{4}$ und man bekommt die ersten beiden Lösungen $2^2 - 3 \cdot 1^2 = 1$ und $7^2 - 3 \cdot 4^2 = 1$. Der Kettenbruch zu $\sqrt{13}$ ist $3\,\overline{1\ 1\ 1\ 1\ 6}$, und man muss eine Weile suchen, um die erste Lösung $649^2 - 13 \cdot 180^2 = 1$ zu finden.

Aufgabe 10.26: $\begin{matrix} x & dy \\ y & x \end{matrix} \cdot \begin{matrix} x' & dy' \\ y' & x' \end{matrix} = \begin{matrix} X & dY \\ Y & Y \end{matrix}$, wobei $X = xx' + dyy'$ und $Y = xy' + x'y$.

Aufgabe 10.27: $x = \overline{10}$.

Aufgabe 10.28: Es gilt $z = n + \frac{1}{z}$, also $z = \overline{n}$. Für $n = 3$ bekommt man $z = \frac{3 + \sqrt{13}}{2}$ und die Lösung $x = y = 3 + 1$ der Pellschen Gleichung.

Aufgabe 10.29: Die Näherungsbrüche konvergieren abwechselnd von oben und unten, daher erfüllen von zwei aufeinanderfolgenden wenigstens einer eine doppelt so gute Abschätzung wie in Satz 10.9. Bei drei aufeinanderfolgenden Näherungsbrüchen ist der Beweis schwerer, wir verweisen auf [K].

Aufgabe 10.30: Es git $x = \overline{2\ 1}$.

Aufgabe 11.2: $S_1 = 4$, $S_2 = 14$, $S_3 = 194 = 67 \bmod 127$, $S_4 = 42 \bmod 127$, $S_5 = 111 \bmod 127$ und $S_6 = 111^2 - 2 = 0 \bmod 127$.

Aufgabe 11.4: $7^{70} = 1 \bmod 71$, aber $7^{n/q} \neq 1$ für $q = 2, 5, 7$.

Aufgabe 11.7: Tatsächlich ist $3^{128} \equiv 1 \bmod 257$.

Aufgabe 11.11: Zeigen Sie, dass $n - 1$ durch $36k$ kgV $(6k, 12k, 18k)$ teilbar ist.

Aufgabe 11.13: Wir testen $a = 5, 7, 11$ und finden jeweils $a^{36} \equiv 1 \pmod{\frac{a}{71}} \bmod 73$. 91 ist nicht prim, da $11^{45} = 8 \equiv 1 \pmod{\frac{11}{91}} \bmod 91$.

Aufgabe 11.15: Siehe [Ko, S. 131].

Aufgabe 11.16: Für $n = 73$ gilt $n - 1 = 72 = 2^3 \cdot 9$, d.h. $m = 9$ und $t = 3$. Wir testen $a = 2, 3, 5$ und erhalten $2^9 = 1 \bmod 73$, $3^{18} \equiv 1 \bmod 73$ und $5^{36} \equiv 1 \bmod 73$. Für $n = 91$ gilt $n - 1 = 90 = 2 \cdot 45$, also $t = 1$ und $m = 45$. Es gilt $2^{45} = 57 \bmod 91$, also ist 91 nicht prim.

Aufgabe 11.19: Die Aussage folgt aus $f^k \circ^m = f^{km}$ und $X^k \cdot^m = X^{km}$.

Aufgabe 11.20: Wie Lösung von Aufgabe 11.4.

Aufgabe 11.21: Man bekommt in diesem Fall $F_k = 2^{2^k} + 1 = 4^{2^{k-1}} + 1 = (-1)^{2^{k-1}} + 1 = 2 \bmod 5$ und damit $5^{\frac{F_k - 1}{2}} \equiv \frac{5}{F_k} \equiv \frac{F_k}{5} \equiv \frac{2}{5} \equiv -1$.

Aufgabe 11.22: Wenden Sie den Pocklington Test an.

Aufgabe 11.23: Beide sind prim.

Aufgabe 11.24: $n = 2^{11} - 1 = 2047 = 23 \cdot 89$ ist nicht prim.

Aufgabe 12.2: Angenommen $n = pq$ mit echten Teilern p, q. Wenn $x = \frac{p+q}{2}$ gilt, ist $x^2 - n = y^2$ ein Quadrat mit $y = \frac{p-q}{2}$, und man findet die echten Teiler p, q darin.

Aufgabe 12.4: 7729 59 131. Benutzen Sie $\sqrt{7729}$ 87 1 10 1 2 1 2 21 .
Aufgabe 12.5: U_{2^r} 2 2^{r-2} für r 3. Benutzen Sie die explizite Beschreibung des Isomorphismus.
Aufgabe 12.6: Es reicht B { 1 2 3 5 7 . Man berechnet z_0 88^2 7729 3 5, z_1 89^2 7729 2^6 3, z_2 90^2 7729 7 53, z_3 91^2 7729 2^3 3 23 und z_4 92^2 7729 3 5 7^2. Hieraus folgt z_0 z_4 3^2 5^2 7^2 105^2 und wir bekommen 95^2 88 92 ^{2} mod 7729. Also erhalten wir die Teiler von 7729 als ggT 7729 x y , wobei x 88 92 8096 und y 105.
Aufgabe 12.7: 23205 3 5 7 13 17.
Aufgabe 12.8: Man beginnt mit x_1 115^2 13199 26 und findet ein Quadrat bei 132^2 13199 5^2 13^2. Also berechnet man die Teiler von 13199 als ggT 13199 132 65 67 und 197.
Aufgabe 12.9: Sei p 3 der kleinste Primfaktor von n. Es gilt n x y n für 0 x y n, also ggT x y n. Angenommen mehr als die Hälfte der x y erfüllt ggT x y n 1. Dann erfüllen mehr als die Hälfte der 0 x y n die Beziehung ggT x y n n. Andererseits ist die Rate der x y, die durch p teilbar sind 1 p 1 3. Widerspruch.
Aufgabe 12.10: Es gilt 87^2 7429 2^2 5 7 und 88^2 7429 3^2 5 7, also bekommt man die Teiler ggT 7429 87 88 210 17 und 437 19 23.
Aufgabe 12.11: X^{4a-2} X^{2a-2} $2X^{2a-1}$ 1 X^{2a-1} X^{a-1} 1 X^{2a-1} X^{a-1} 1 .
Aufgabe 12.12: Ist p q und p q klein, so findet man x_i p und z_i p^2 n für i p q.
Aufgabe 13.3: 1 2 3 2 5 2 5^2 2 5^3 , 7 4 3 5 5^2 5^3 .
Aufgabe 13.4: $\frac{17}{5003}$ 1, also hat die mittlere Gleichung keine Lösung. Die letzte Gleichung hat keine Lösung mod 2^2, also auch nicht in $_2$. Die erste Gleichung hat die Lösungen x 1 in 3 und kann — wie am Anfang des Abschnittes — explizit zu den Lösungen x 1 3 3^2 $_3$ geliftet werden.
Aufgabe 13.13: Die erste Gleichung hat immer zwei Lösungen mod 5^k, k 1: x 1 3 5^2 2 5^3 3 5^4 . Die zweite Gleichung hat die Lösung x 2 mod 5, die 5 Lösungen x 2 7 12 17 22 mod 25, die 10 Lösungen x 2 12 27 37 52 62 77 87 102 112 mod 125, die 10 Lösungen x 2 87 127 212 252 337 377 462 502 587 mod 625 und die 10 Lösungen x 2 87 627 712 1252 1337 1877 1962 2502 2587 mod 5^5.
Aufgabe 13.17: Gleichung 1 hat 4 Lösungen x 127 58 mod 851. Gleichung 2 hat die Lösungen x 793 9 13 4 13^2 und x 820 12 13 8 13^2 mod 13^3.
Aufgabe 13.18: Einzige Lösung ist x 317 5 3 7 6 7^3 mod 7^4.
Aufgabe 13.19: Liften Sie die Aussage des chinesischen Restsatzes.
Aufgabe 13.20: Verwenden Sie zunächst Satz 13.15, um die Anzahl der Nullstellen x_i in $_5$ zu bestimmen, und berechnen Sie die Bewertungen v_5 f' x_i . Arbeiten Sie dann mit Hilfssatz 13.14, um die Anzahl der Nullstellen in 5^k für k zu ermitteln.
Aufgabe 13.21: Da x_i Nullfolge ist, konvergiert die p–adische Bewertung der x_i gegen 0, d.h. sie enthalten Faktoren p^{m_i} mit m_i ∞. Die Reihe konvergiert also in $\mathbb{Q}_p$, da die ersten Koeffizienten in der p–adischen Darstellung sich nicht mehr verändern.
Aufgabe 13.22: Wie in zeigt man, dass m kein Quadrat in einem angeordneten Körper sein kann. Andererseits gibt es in allen $\mathbb{Q}_p$ negative Quadrate, da dies schon in $\mathbb{F}_p$ und U_8 gilt und man danach liften kann.
Aufgabe 13.23: Benutzen Sie Legendre–Symbole für die Lösbarkeit der drei quadratischen Faktoren.
Aufgabe 13.24: Lösen Sie $2x$ 1 bzw. $3x$ 5 in $_p$ mit Satz 13.15.
Aufgabe 13.25: p^7 p^5 p^3 p^3 u für eine Einheit u.

Aufgabe 13.26: Benutzen Sie die p–adische Bewertung und Satz 13.15.
Aufgabe 13.27: Lösen Sie $x^2 \quad m$ in $\mathbb{Q}_p$ mit Satz 13.15.
Aufgabe 13.28: Mit Induktion über n.
Aufgabe 13.29: Untersuchen Sie zuerst, ob 75 quadratischer Rest modulo p ist.
Aufgabe 13.30: Benutzen Sie die Definition von $\quad_p$ und den Satz von Tychonoff. Dann schreibe man $\mathbb{Q}_p$ als Vereinigung von Kopien von $\quad_p$.
Aufgabe 14.6: Wir betrachten das Polynom $f \quad 2X^2 \quad X \quad \frac{u \quad 1}{8} \quad \quad _2 X$. Es gilt $f \ \frac{u \quad 1}{8}$ $0 \bmod 2$ und $f' \ \frac{u \quad 1}{8} \quad 1 \bmod 2$. Daher finden wir nach dem Henselschen Lemma eine Lösung $w \quad _2$ von f mit $w \quad \frac{u \quad 1}{8} \bmod 2$. Nun ist $4w \quad 1$ eine Quadratwurzel von u, weil $4w \quad 1 \ ^2 \quad u \quad 16w^2 \quad 8w \quad 1 \quad u \quad 8 \ 2w^2 \quad w \quad \frac{u \quad 1}{8} \quad 8f \ w \quad 0$. Insgesamt können wir das Element des Kerns $u2^n$ als Quadrat von $4w \quad 1 \ 2^{n/2}$ schreiben, d.h. $\operatorname{Ker}\tilde{\Phi}_2 \quad \mathbb{Q}_2 \ ^2$.
Aufgabe 14.19: Sei $r \quad \frac{c}{a}$ und — nach Betrachten von Spezialfällen — $p \quad 3$ teilerfremd zu a im Fall $a \quad 5$. Man muss zunächst eine Gleichung der Form $ax^2 \quad c \bmod p$ lösen. Dies geht für alle p, für die ac ein Quadrat modulo p ist.
Aufgabe 14.20: Betrachten Sie die Diskriminante $b^2 \quad 4c$ in $\mathbb{Q}$ und allen $\mathbb{Q}_p$ sowie $\quad .$
Aufgabe 14.21: Benutzen Sie das Hilbert–Symbol modulo 3 5 7 jeweils. Die mittlere Gleichung besitzt die nicht–triviale Lösung $x \quad y \quad 1, z \quad 2$.
Aufgabe 14.22: Untersuchen Sie Zahlen aus $\mathbb{Q} \quad \mathbb{Q}_p \ \mathbb{Q}_q$ darauf, ob sie Quadrate sind.
Aufgabe 14.23: Zeigen Sie zunächst, dass jeder Automorphismus von $\mathbb{Q}_p$ den Unterring $\quad_p$ auf sich abbildet.
Aufgabe 14.24: Untersuchen Sie die Lösung der Gleichung $nz^2 \quad b^2 \quad a^2$ mit dem Hilbert–Symbol $\frac{n \quad 1}{p}$ und benutzen Sie $\frac{1}{p} \quad 1 \ ^{\frac{p \quad 1}{2}}$.
Aufgabe 14.25: Seien $x_0 \ y_0$ und $x \ y$ zwei verschiedene Lösungen. Entwickeln der Gleichung $1 \quad ax^2 \quad by^2 \quad a \ x \quad x_0 \quad x_0 \ ^2 \quad b \ y \quad y_0 \quad y_0 \ ^2$ ergibt dann $a \ x \quad x_0 \ ^2 \quad b \ y \quad y_0 \ ^2 \quad 2ax_0 \ x \quad x_0 \quad 2by_0 \ y \quad y_0 \quad 0$. Setzt man $t \quad x \quad x_0 \quad y \quad y_0$, so ergibt sich gerade die behauptete Gleichung, außer im Fall $y \quad y_0$, d.h. $t \quad \infty$, bei dem dann $x \quad x_0$ folgt.
Aufgabe 14.26: Untersuchen Sie die Gleichungen erst modulo p und wenden Sie dann Satz 13.15 an.
Aufgabe 14.27: Wenden Sie Satz 13.15 an.
Aufgabe 15.10: Eine Lösung in $\quad$ findet man durch Auflösen der Gleichung nach X, Y oder Z. Lösungen in $\mathbb{Q}_p$ findet man direkt für $p \quad 2 \ 3 \ 5$ und mit Hilfe des Henselschen Lemmas für andere p, indem man zuerst die Gleichung in $\mathbb{F}_p$ elementar löst. Über $\mathbb{Q}$ gibt es keine nicht–triviale Lösung, siehe [S] oder [C, 4].
Aufgabe 15.14: Eine Lösung der Gleichung $2x^2 \quad 5y^2 \quad c$ mit $x \ y \quad \mathbb{Q}$ ist gleichbedeutend zu einer Lösung der Gleichung $2x^2 \quad 5y^2 \quad cz^2 \quad 0$ oder nach Multiplikation mit c zu einer Gleichung der Form $2c \ x^2 \quad 5c \ y^2 \quad z^2$, die auf die Hilbert–Symbole $\frac{2c \quad 5c}{p}$ für alle p führt.
Aufgabe 15.15: Jede nicht–triviale Lösung von $aX^2 \quad bY^2 \quad cZ^2 \quad 0$ in $\quad ^3$ liefert eine Lösung $aX^2 \quad bY^2 \quad 0 \bmod c$, d.h. von $abX^2 \quad b^2Y^2 \quad 0 \bmod c$. Das Element $w \quad bY \ X \bmod c$ existiert damit (oBdA $X \quad 0 \bmod c$) und löst damit die Gleichung $w^2 \quad ab \bmod c$. Ebenso erhält man $u \quad cZ \ Y$ und $v \quad aX \ Z$ mit $u^2 \quad bc \bmod a$ und $v^2 \quad ac \bmod b$. Ist umgekehrt $u \ v \ w$ gegeben mit $u^2 \quad bc \bmod a$, $v^2 \quad ac \bmod b$ und $w^2 \quad ab \bmod c$, so betrachte $w^2 \quad ab \bmod c$ und das Inverse $a \ ^1$ von $a \bmod c$. Dann gilt für alle $x \ y \ z$, dass $ax^2 \quad by^2 \quad cz^2 \quad ax^2 \quad by^2 \quad x \quad a \ ^1wy \quad ax \quad wy \bmod c$. Durch die anderen beiden Bedingungen sieht man, dass man $ax^2 \quad by^2 \quad cz^2$ auch modulo a und b als Produkt linearer

Faktoren schreiben kann. Der Chinesische Restsatz liefert damit eine nicht–triviale Faktorisierung $ax^2 \quad by^2 \quad cz^2 \quad a_1x \quad a_2y \quad a_3z \quad a_4x \quad a_5y \quad a_6z \mod abc$. Jeder der beiden Linearfaktoren hat Lösungen $\mod abc$, wie man durch Abzählen der Restklassen sieht. Außerdem erfüllen diese $x \quad \sqrt{bc}$, $y \quad \sqrt{ac}$ und $z \quad \sqrt{ab}$. Daraus folgt $ax^2 \quad by^2 \quad cz^2 \quad 0$ oder $ax^2 \quad by^2 \quad cz^2 \quad abc$. Im ersten Fall sind wir fertig, im zweiten Fall betrachte $X \quad xz \quad by$, $Y \quad yz \quad ax$ und $Z \quad z^2 \quad ab$.

Aufgabe 15.16: Sei $n : \quad \#\{i \quad v_p \quad a_i \quad 1$. Ist $n \quad 2$, so zeige man zuerst, dass ein $0 \quad x \quad \mathbb{Q}_p^4$ existiert mit $f \quad x \quad 0$. Ist $n \quad 2$, dann sei oBdA $v_p \quad a_1 \quad v_p \quad a_2 \quad 0$ und $v_p \quad a_3 \quad v_p \quad a_4 \quad 1$. In diesem Fall zeige man, dass ein nichttriviales $x \quad \mathbb{Q}_p^4$ mit $f \quad x \quad 0$ genau dann existiert, wenn eines der Elemente $a_2 \quad a_1 \quad a_4 \quad a_3$ ein Quadrat in $\quad_p$ ist.

Aufgabe 16.2: Ein Zahlkörper der Dimension 2 besitzt ein Element $x \quad \mathbb{Q}$ und wird als Vektorraum von $1 \quad x$ erzeugt. Das Element x^2 erfüllt eine Relation $x^2 \quad bx \quad c \quad 0$, und damit gilt $K \quad \mathbb{Q} \quad \sqrt{d}$, wobei $d \quad b^2 \quad 4c$ ist.

Aufgabe 16.6: $x \quad \sqrt{3}$ und $y \quad \sqrt[3]{2}$ erfüllen $x^2 \quad 3$ und $y^3 \quad 2$. $z \quad x \quad y$ erfüllt die Ganzheitsgleichung $z^6 \quad 9z^4 \quad 4z^3 \quad 27z^2 \quad 36z \quad 23 \quad 0$.

Aufgabe 16.12: Da $\mathbb{Q}\,X$ ein euklidischer Ring mit der Gradfunktion ist, ist $\mathbb{Q}\,X$ ein Hauptidealring, also existiert f und ist das Element kleinsten Grades mit der Eigenschaft $f \quad x \quad 0$.

Aufgabe 16.14: Man überlege sich zuerst, dass die Einschränkung der Einbettung auf $\mathbb{Q}$ die Inklusion $\mathbb{Q} \quad$ sein muss. Danach betrachte man die möglichen Bilder von $\sqrt{d}$ unter Berücksichtigung von $\sqrt{d} \quad \sqrt{d} \quad d \quad \mathbb{Q}$.

Aufgabe 16.16: $\mathrm{Sp}_{K/} \quad \sqrt{3} \quad 0$, $N_{K/} \quad \sqrt{3} \quad 9$ und das Minimalpolynom von $\sqrt{3}$ ist $T^2 \quad 3$. $\mathrm{Sp}_{K/} \quad 3\sqrt[4]{3} \quad 2\sqrt{27} \quad 0$, $N_{K/} \quad 3\sqrt[4]{3} \quad 2\sqrt{27} \quad 11421$ und das Minimalpolynom ist $T^4 \quad 216T^2 \quad 648T \quad 11421$.

Aufgabe 16.19: Starten Sie mit dem Minimalpolynom des Elementes. An welcher Stelle des Minimalpolynoms treten die Spur und die Norm des Elementes auf?

Aufgabe 16.34: Da $\Delta_K \quad d$ oder $4d$ ist, muss man nur $p \quad 2$ im Fall $q \quad 1 \mod 4$ betrachten.

Aufgabe 16.35: Zeigen Sie zuerst, dass z Liouvillesch ist, d.h. zu jedem $n \quad$ ein Bruch $\frac{p}{q} \quad \mathbb{Q}$ existiert mit $q \quad 2$ und $z \quad \frac{p}{q} \quad \frac{1}{q^n}$. Zeigen Sie andererseits, dass jede algebraische Zahl, die Nullstelle eines Polynoms vom Grad n ist, eine Ungleichung der Form $z \quad \frac{p}{q} \quad \frac{1}{M \cdot q^n}$ erfüllt, indem Sie den Mittelwertsatz der Differentialrechnung anwenden. Folgern Sie aus beiden Ungleichungen, dass z nicht algebraisch sein kann.

Aufgabe 16.36: $23 \quad 5$ ist algebraisch mit Minimalpolynom $5X \quad 23$, aber nicht ganz. $1 \quad \sqrt[3]{5} \quad 3$ ist algebraisch, aber nicht ganz, denn der Ganzheitsring von $\mathbb{Q}\ \sqrt[3]{5}$ ist $\sqrt[3]{5}$, siehe Aufgabe 16.38. $1 \quad \sqrt{7} \quad \sqrt{5}$ ist ebenso algebraisch, aber nicht ganz, weil sein Minimalpolynom $X^4 \quad 16 \quad 5X^2 \quad 36 \quad 25$ ist. Schließlich ist $\exp \quad 2\pi i \quad 13$ eine 13–te Einheitswurzel, also ganz über $\quad$.

Aufgabe 16.37: Folgt direkt aus Korollar 16.33.

Aufgabe 16.38: Sei $\vartheta^3 \quad 5$. Die Menge $1 \quad \vartheta \quad \vartheta^2$ hat $\Delta \quad 1 \quad \vartheta \quad \vartheta^2 \quad 3^3 \quad 5^2$. Ganze Elemente sind also von der Form $\frac{1}{3} \quad a_1 \quad a_2\vartheta \quad a_3\vartheta^2$ oder $\frac{1}{5} \quad a_1 \quad a_2\vartheta \quad a_3\vartheta^2$. Berechnet man in beiden Fällen Spur und Norm, so sieht man, dass dadurch keine neuen Elemente entstehen. Also ist $1 \quad \vartheta \quad \vartheta^2$ eine Ganzheitsbasis.

Aufgabe 16.39: α hat das Minimalpolynom $T^3 \quad 2$ und somit Spur 0. Dagegen gilt $\alpha^{2\ 3} \quad \alpha^{3\ 2} \quad 2^2 \quad 4$ und damit hat α^2 das Minimalpolynom $T^3 \quad 4$ und damit ebenfalls Spur 0.

Aufgabe 16.40: Die Diskriminanten der Körper $\mathbb{Q}\ \sqrt{p}$ und $\mathbb{Q}\ \sqrt{q}$ sind p bzw. $4q$ und damit teilerfremd. Daher ist der Ring ganzer Zahlen erzeugt von den Produkten $\omega_i \quad \omega'_j$, wobei $\omega_1 \quad \omega_2$ und $\omega'_1 \quad \omega'_2$ jeweils Ganzheitsbasen von $\mathbb{Q}\ \sqrt{p}$ und $\mathbb{Q}\ \sqrt{q}$ sind. Siehe [N, Satz 2.11]

für einen Beweis der letzten Aussage, die man auch in diesem Fall direkt zeigen kann.

Aufgabe 16.41: Will man a durch b mit Rest teilen, so betrachte $x \quad a \; b \quad K$ und nehme ein $y \quad \mathcal{O}_K$ mit $N\, x \quad y \quad 1$. Hieraus folgt $a \quad bx \quad yb \quad r$ mit $N\, r \quad N\, bx \quad by \quad N\, b\, N\, x \quad y \quad N\, b$. Also ist $\mathcal{O}_K$ euklidisch.

Aufgabe 16.42: Ziehen Sie die Wurzel aus Satz 16.32.

Aufgabe 16.43: Sei $\alpha \quad a_0 \quad a_1\zeta_p \qquad a_p \; {}_2\zeta_p^{\,p\;2} \quad \mathbb{Q}\,\zeta_p$ eine ganze Zahl. Es ist zu zeigen, dass $a_k \qquad$. Das Element $\alpha\zeta_p{}^k \quad \alpha\zeta_p$ hat Spur Sp $\alpha\zeta_p{}^k \quad \alpha\zeta_p \qquad pa_k$, also ist $b_k : \quad pa_k \qquad$. Setze nun $\lambda : \quad 1 \quad \zeta_p$. Es gilt $N\, \lambda \qquad p$. Wir schreiben $p\alpha \quad b_0 \quad b_1\zeta_p \qquad b_p \; {}_2\zeta_p^{\,p\;2} \quad c_0 \quad c_1\lambda \qquad c_p \; {}_2\lambda^{p\;2}$ mit geeigneten Koeffizienten c_k. Wir müssen zeigen, dass c_k durch p teilbar ist. Dies beweist man durch Induktion: Der Induktionsanfang ist $c_0 \quad b_0 \qquad b_p \; {}_2 \quad 0 \bmod p$. Im Induktionsschritt zeigt man $c_k \quad \mu_k\lambda$ für ein μ_k und damit $c_k^{p\;1} \quad pN\; \mu_k$, also $p \quad c_k$. Die Diskriminante berechnet sich mit dieser Basis zu $\Delta \qquad 1 \;{}^{p\;1}/_2 p^{p\;2}$.

Aufgabe 16.44: Norm und Spur lassen sich sofort aus dem Minimalpolynom ablesen. Ist $f \quad X^3 \quad pX \quad q \quad X \quad \alpha_1 \; X \quad \alpha_2 \; X \quad \alpha_3$, so gilt $\prod_{i \;\; j} \alpha_i \quad \alpha_j{}^2 \qquad 4p^3 \quad 27q^2$. Die Diskriminante der $\mathbb{Q}$–Basis $1 \;\; \alpha \;\; \alpha^2$ hat nur 2 als quadratischen Primfaktor. Somit muss man nur $\frac{1}{2}$, $\frac{\alpha}{2}$, $\frac{\alpha^2}{2}$, $\frac{1 \quad \alpha}{2}$, $\frac{\alpha \quad \alpha^2}{2}$ und $\frac{1 \quad \alpha^2}{2}$ auf Ganzheit testen mit Norm und Spur. Beachte, dass die Norm multiplikativ ist. Eine Ganzheitsbasis ist dann $1 \;\; \frac{1 \quad \alpha}{2} \;\; \alpha^2$.

Aufgabe 16.45: Alle Konjugierten von a sind gleich, da $a \quad \mathbb{Q}$ ist.

Aufgabe 16.46: Folgt aus der folgenden exakten Sequenz von abelschen Gruppen:

$$0 \qquad \mathrm{Hom}_K\, L \qquad \mathrm{Hom} \quad L \qquad \mathrm{Hom} \quad K \qquad 0$$

wobei der zweite Pfeil durch Restriktion auf K gegeben ist.

Aufgabe 16.47: Zunächst hängen det und Spur einer darstellenden Matrix einer linearen Abbildung nicht von der Wahl der Basis ab. Die Elemente $1 \;\; \alpha \;\; \alpha^2 \qquad \alpha^{n\;1}$ spannen einen Unterkörper K' von K auf. Wegen Aufgabe 16.45 und den Formeln aus Aufgabe 16.46 dürfen wir annehmen, dass $K' \quad K$ ist, also dass $1 \;\; \alpha \;\; \alpha^2 \qquad \alpha^{n\;1}$ eine Basis von K ist. In dieser Basis sieht man aber sofort, dass die darstellende Matrix M das Minimalpolynom f von α als charakteristisches Polynom hat.

Aufgabe 17.7: $48 \quad 7\sqrt{47}$ aus Kettenbruchentwicklung.

Aufgabe 17.19: $14 \quad 2 \;\; 7 \quad 1 \quad \sqrt{\;13\;} \quad 1 \quad \sqrt{\;13\;}$.

Aufgabe 17.20: Zwei Elemente sind $\frac{5 \quad \sqrt{29}}{2}$ und $70 \quad 13\sqrt{29}$, die man aus der Kettenbruchentwicklung erhält.

Aufgabe 17.21: Gegenbeispiel: $x \qquad 3 \quad 4i \quad 5 \quad \mathbb{Q}\, i$.

Aufgabe 17.22: $\quad 1$ ist kein Quadrat mod p, falls $p \quad 3 \bmod 4$.

Aufgabe 17.23: Schwierig ist nur, von Punkt 4. nach 2. zu kommen. Betrachten Sie dazu eine Fundamentallösung $x'\; y'$ von $x^2 \quad py^2 \quad 1$ für ein solches p. Welche Paritäten müssen $x'\; y'$ haben? Betrachten Sie nun $x' \quad 1$ und $x' \quad 1$. Man zeige $2 \quad \mathrm{ggT}\; x' \quad 1 \;\; x' \quad 1$ und betrachte die Gleichung $x' \quad 1 \;\; x' \quad 1 \qquad py^2$. Was bedeutet das für $x' \quad 1$ und $x' \quad 1$? Welche Möglichkeiten gibt es unter der Bedingung, dass $x'\; y'$ eine Fundamentallösung von $x^2 \quad py^2 \quad 1$ sein soll? Kann man daraus eine Lösung für $x^2 \quad py^2 \qquad 1$ gewinnen?

Aufgabe 17.24: In $\mathbb{Q}\; \sqrt[3]{5}$ gilt $r \qquad r \qquad 1$ und $H \qquad 2$ mit dem Erzeuger $\quad 1$. Die Fundamentaleinheit von $\mathbb{Q}\; \sqrt[3]{5}$ ist $2\alpha^2 \quad 4\alpha \quad 1$. Für jeden Kreisteilungskörper $\mathbb{Q}\,\zeta_p$ mit p prim gilt $r \qquad 0$ und $r \qquad p \quad 1 \quad 2$ (warum?). Also hat der freie Anteil den Rang $r \qquad 1 \quad 5 \quad 1 \quad 4$ für $p \quad 11$. In diesem Fall ist $H \qquad 22$ mit dem Erzeuger $\quad 1 \;\; \zeta \qquad \zeta^{10}$. Der freie Anteil der Einheitengruppe von $\mathbb{Q}\;\zeta$ wird erzeugt durch $\zeta^5 \quad 1 \;\; \zeta^8 \quad \zeta^7, \zeta^8 \quad \zeta^5 \quad \zeta$

und $\zeta^5 \quad \zeta^2$. In $\mathbb{Q} \ \alpha$ ist $r \quad 3, r \quad 0$ und der freie Anteil der Einheitengruppe ist durch α und $\alpha^2 \quad \alpha \quad 1$ erzeugt. Es gilt hier $H \quad 2$ erzeugt durch $\quad 1$.

Aufgabe 17.25: Verwenden Sie Satz 17.14 und Satz 17.16. $N \ 1 \quad 2\sqrt{3} \quad 11$, also ist $1 \quad 2\sqrt{3}$ irreduzibel. 2 ist nicht irreduzibel, da $3 \quad 5 \mod 8$. 37 ist nicht prim nach Satz 17.14, da $\frac{3}{37} \quad 1$, 17 dagegen schon, da $\frac{3}{17} \quad 1$.

Aufgabe 18.1: Alle Produkte $x_i y_i$ aus $I \ J$ sind in $I \quad J$, da I und J Ideale sind.

Aufgabe 18.8: $\sqrt{2}$ ist ein Hauptidealring, und es gilt $3 \ 1 \quad 2\sqrt{2} \quad 1$, da $N \ 1 \quad 2\sqrt{2} \quad 7$, mit inversem Ideal ebenfalls 1. Das Ideal $7 \ 1 \quad 2\sqrt{2} \quad 1 \quad 2\sqrt{2}$ hat inverses Ideal $\frac{1}{7} \ 1 \quad 2\sqrt{2}$.

Aufgabe 18.12: Benutzen Sie die Idee im Beweis von Satz 17.17.

Aufgabe 18.21: $_1 \quad 2 \ 1 \quad \sqrt{41}$ ist ein Primideal, denn seine Norm $N \ _1 \quad \#\mathcal{O} \ _1$ ist 2. Es gilt $2 \quad 1 \quad \sqrt{41} \quad 1 \quad \sqrt{41}$, also ist auch $1 \quad \sqrt{41} \quad _1$. Damit ist $42 \quad 1 \quad \sqrt{41} \ 1 \quad \sqrt{41} \quad \frac{2}{1}$. Die anderen vier Ideale $_2$, $'_2$, $_3$ und $'_3$ sind $3 \ 1 \quad \sqrt{41}$ und $7 \ 1 \quad \sqrt{41}$ und haben Norm 3 bzw. 7. Hieraus folgt auch $42 \quad \frac{2}{1} \ _2 \ '_2 \ _3 \ '_3$, da 42^2 das Produkt der Normen ist. Die verschiedenen Faktorisierungen ergeben sich aus Kombinationen der Primideale.

Aufgabe 18.22: Zum Beweis des Hinweises: Sei $J \quad \prod_i \ _i^{c_i}$ die Primzerlegung von J, so muss man zeigen, dass $\alpha I \ ^1 \quad _i \quad R$ für alle i. Es gibt nun $\alpha_i \quad I \prod \ _i \quad I \prod$ für alle i (warum?). Zeigen Sie nun durch Widerspruch, dass $\alpha : \ \sum_i \alpha_i \quad I$, aber nicht $\alpha \quad I \ _i$ gilt. Danach zeigt man: Jedes (gebrochene) Ideal I in einem Dedekindring R wird durch 2 Elemente erzeugt. Ein Erzeuger kann beliebig in $I \quad \{0$ gewählt werden. Hinweis dazu: Man wähle $\beta \quad 0$ in I und $J \quad \beta I \ ^1$ und verwende die vorherige Aussage.

Aufgabe 18.23: Da h die Ordnung der Klassengruppe ist, ist I^h trivial in der Klassengruppe.

Aufgabe 18.24: Verwenden Sie Aufgabe 18.23, um $I^h \quad \beta$ zu erhalten. Dann sei α die ganz–algebraische Zahl, die man durch Ziehen einer h–ten Wurzel aus β bekommt.

Aufgabe 19.6: Betrachten Sie die Untergruppe Γ, die von $S \ T$ erzeugt wird. Man zeigt zuerst, dass jedes Element in der oberen Halbebene einen Repräsentanten im Fundamentalbereich modulo Γ besitzt, und dass Elemente an den Rändern von Γ nur in offensichtlicher Weise aufeinander abgebildet werden unter SL 2 . Nimmt man nun $A \quad$ SL 2 und einen Punkt z im Inneren von , so gibt es ein $A' \quad \Gamma$ mit $A'Az \quad D$. Da z nicht am Rand liegt, gilt $A'Az \quad z$ und damit $A'A \quad 1$ und damit $A \quad \Gamma$, da $1 \quad S^2 \quad \Gamma$.

Aufgabe 19.10: $\mathbb{Q} \ \sqrt{74}$ hat $h \quad 10$, $\mathbb{Q} \ \sqrt{89}$ hat $h \quad 12$.

Aufgabe 19.12: Benutzen Sie Aufgabe 16.41, um die Fälle $d \quad 1 \quad 2 \quad 3 \quad 7 \quad 11$ zu untersuchen. Gehen Sie dabei wie im Fall $d \quad 1$ in der Vorlesung vor. Ist $d \quad 11$ und Φ eine beliebige euklidische Funktion, so wählt man zuerst ein $a \quad 0$ in $\mathcal{O}_K$ mit $\Phi \ a$ minimal, das keine Einheit, also nicht 1 ist. Durch Division durch a mit Rest sieht man, dass $\#\mathcal{O}_K \quad a \quad 3$ ist, da nur die Reste $0 \quad 1$ auftreten, weil ein Rest $\quad 0$ eine Einheit sein muss wegen der Minimalität von a. Die Gleichung $u^2 \quad d \ v^2 \quad 3$ besitzt aber für $d \quad 11$ nur die triviale Lösung $u \quad 1, v \quad 0$. Widerspruch!

Aufgabe 19.19: $\mathbb{Q} \ \sqrt{35}$ hat $h \quad 2$.

Aufgabe 19.20: Die Gleichungen $y\delta \quad x\gamma \quad 1$ und $2a\delta \quad b\gamma \ x \quad b\delta \quad 2c\gamma \ y \quad v$ haben die Lösungen $x \quad v\delta \quad b\delta \quad 2c\gamma \quad 2u$ und $y \quad 2a\delta \quad b\gamma \quad b\gamma \quad 2u$. Daraus folgt $ax^2 \quad bxy \quad cy^2 \quad w \quad v^2 \quad \Delta \quad 4u$. Es gilt $4au \quad 2a\delta \quad b\gamma \ ^2 \quad \Delta\gamma^2$ und damit $4u \quad 2a\delta \quad b\gamma \quad v\gamma \ 2a\delta \quad b\gamma \quad v\gamma$. Unter Ausnutzung der Voraussetzungen und $b \quad v \mod 2$ folgt die Behauptung.

Aufgabe 19.21: Benutzen Sie die Matrizen $\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}$, $\begin{matrix} 1 & 0 \\ m & 1 \end{matrix}$ und $\begin{matrix} 1 & m \\ 0 & 1 \end{matrix}$.

Literaturverzeichnis

[AKS] Agrawal, M., N. Kayal und N. Saxena: *PRIMES is in P*, Ann. of Math. **160** (2004), 781–793.

[AGP] Alford, W., A. Granville und C. Pomerance: *There are infinitely many Carmichael numbers*, Ann. Math. **139** (1994), 703–722.

[B] Bornemann, F.: *Primes is in P: a breakthrough for "everyman"*, Notices of the AMS **50** (2003), 545–552.

[C] Cassels, J.: *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. **41** (1966), 193–291.

[Ch] Cohn, H.: *A short proof of the simple continued fraction expansion of e*, Amer. Math. Monthly **113** (2006), 57–62.

[CP] Crandall, R. und C. Pomerance: *Prime numbers: a computational perspective*, Springer Verlag 2001.

[E] Euler, L.: *De fractionibus continuis dissertatio*, Commentarii academiae scientiarum Petropolitanae **9**, 98–137 (1744); einsehbar in Eulers Opera Omnia, Band **14**, Seite 187–215, Teubner Verlag 1925.

[F] Frey, G.: *Elementare Zahlentheorie*, Vieweg Verlag 1984.

[G] Goldfeld, D.: *Gauß's class number problem for imaginary quadratic fields*, Bull. Amer. Math. Soc. (N.S.) **13** (1985), 23–37.

[H] Hasse, H.: *Über die Klassenzahl abelscher Zahlkörper*, Akademie Verlag 1952.

[K] Khintchine, A.: *Kettenbrüche*, Teubner Verlag 1956.

[Ko] Koblitz, N.: *A course in number theory and cryptography*, Graduate Text **114**, 2te Auflage, Springer Verlag 1994.

[Ku] Kunz, E.: *Einführung in die kommutative Algebra und algebraische Geometrie*, Vieweg Verlag 1980.

[L] Lang, S.: *Algebra*, Addison–Wesley Verlag 1984.

[N] Neukirch, J.: *Algebraische Zahlentheorie*, Springer Verlag 1992.

S. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie,*
DOI 10.1007/978-3-8348-8263-9,

[MS] Mignotte, M. und D. Ştefănescu: *Polynomials: an algorithmic approach*, Springer Verlag 1999.

[P] Pomerance, C.: *Primality testing: variations on a theme of Lucas*, Congr. Numerantium **201** (2010), 301–312.

[R1] Ribenboim, P.: *The new book of prime number records*, Springer Verlag 1996.

[R2] Ribenboim, P.: *Classical theory of algebraic numbers*, Springer Verlag 2001.

[S] Selmer, E.: *The diophantine equation* $ax^3 \quad by^3 \quad cz^3 \quad 0$, Acta Math. **85** (1951), 203–262 und **92** (1954), 191–197.

[Sh] Shor, P.: *Algorithms for quantum computation: discrete logarithms and factoring*, Proc. of 35th Annual Symposion on Foundations of Computer Science, IEEE Computer Society Press (1994), 124–134.

[ST] Stewart, I. und D. Tall: *Algebraic number theory and Fermat's last theorem*, Third Edition, A. K. Peters Verlag 2002.

[W] Watkins, M.: *Class numbers of imaginary quadratic fields*, Math. Comp. **73** (2004), 907–938.

[Wü] Wüstholz, G.: *Algebra*, Vieweg Verlag 2004.

[Z] Zagier, D.: *Zetafunktionen und quadratische Körper*, Springer Verlag 1981.

Sachwortverzeichnis

S. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie,*
DOI 10.1007/978-3-8348-8263-9,