

Elementare Zahlentheorie

(Notizen zu einer Vorlesung im WS 2004-05)

Benjamin Klopsch

Eine kleine Auswahl von Mathematikern, deren Namen eng mit der elementaren Zahlentheorie verbunden sind.

- EUKLIDES** (um -300). Griechischer Geometer, der in Alexandria lehrte. Schrieb unter anderem die „Elemente“, ein dreizehnbändiges Werk, in dem die Mathematik in der Gestalt einer axiomatisch-deduktiven Theorie erscheint. Buch VII der „Elemente“ enthält eine Einführung in die Zahlentheorie.
- DIOPHANTOS** (um 250). Griechischer Mathematiker in Alexandria, der sich um die Weiterentwicklung der Arithmetik verdient gemacht hat und erste Ansätze zu einem algebraischen Symbolismus entwickelte. Sein Hauptwerk „Arithmetica“ besteht aus einer Sammlung von zahlentheoretischen Problemen und deren Lösungen.
- LEONARDO DI PISA (FIBONACCI)** (circa 1180–1228). Weitgereister Kaufmann und Kenner der islamischen Welt, aufgewachsen in Nordafrika. Mit seinem Buch „Liber abaci“ führte er in Europa das Rechnen mit arabischen Ziffern im Dezimalsystem ein. Erlaubte negative Zahlen und Null als Lösungen von Gleichungen.
- PIERRE DE FERMAT** (1601–1665). Französischer Jurist und Parlamentsrat in Toulouse. Hobby-Mathematiker mit wenig Liebe fürs Detail. Lieferte wichtige Beiträge zur Zahlentheorie, analytischen Geometrie und Infinitesimalrechnung. Mitbegründer der Wahrscheinlichkeitstheorie.
- LEONHARD EULER** (1707–1783). Mathematiker, Physiker und Philosoph, geboren in Basel. Vater von dreizehn Kindern. Wirkte an den Akademien in St. Petersburg und Berlin. Bedeutende Ergebnisse in fast allen Bereichen der Mathematik und Verfasser zahlreicher einflußreicher Lehrbücher.
- JOSEPH LOUIS LAGRANGE** (1736–1813). Mathematiker und Physiker. Arbeitete in Turin, Berlin und Paris. Ähnlich wie Euler sehr vielseitig und produktiv; schrieb wichtige Lehrbücher.
- ADRIEN-MARIE LEGENDRE** (1752–1833). Französischer Mathematiker. Wirkte in Paris. Beschäftigte sich mit den Grundlagen der Geometrie (Parallelenaxiom), mit Zahlen- und Funktionentheorie.
- CARL FRIEDRICH GAUSS** (1777–1855). Astronom, Mathematiker und Physiker, geboren in Braunschweig. Professor und Direktor der Sternwarte in Göttingen. Leistete auf vielen Gebieten der Mathematik ausgefeilte Beiträge, unter anderem zur Zahlentheorie („Disquisitiones Arithmeticae“, 1801). Entwickelte sehr weitreichende Ideen, die aber teilweise unveröffentlicht blieben.
- PETER GUSTAV LEJEUNE DIRICHLET** (1805–1859). Professor für Mathematik in Breslau, Berlin und Göttingen. Lieferte wichtige Beiträge zur Analysis und Zahlentheorie und war ein erfolgreicher akademischer Lehrer.
- JULIUS WILHELM RICHARD DEDEKIND** (1831–1916). Professor für Mathematik in Zürich und Braunschweig. Arbeitete vor allem auf den Gebieten Algebra und Zahlentheorie. Bedeutend als Herausgeber der gesammelten Werke von Dirichlet, Gauß und Riemann. Einer der ersten Vertreter der Mengenlehre.

Inhaltsverzeichnis

Eine kleine Auswahl von Mathematikern	i
Inhaltsverzeichnis	iii
Kapitel 1. Primfaktorzerlegung	1
1. Der Ring \mathbb{Z} der ganzen Zahlen	1
2. Teilbarkeit in Integritätsbereichen	4
3. Eindeutige Primfaktorzerlegung in \mathbb{Z}	6
4. Ideale und Kongruenzen – ein Zwischenstück	8
5. DEDEKINDSche Ringe – ein Streifzug	10
Kapitel 2. Quadratische Zahlkörper	15
1. Ganzheitsringe in quadratischen Zahlkörpern	15
2. Einheiten in Ganzheitsringen quadratischer Zahlkörper	19
3. Primfaktorzerlegung in Ganzheitsringen quadratischer Zahlkörper	22
4. Quadratisches Reziprozitätsgesetz	27
Anhang A. Sammlung der Arbeitsblätter	31
Literaturverzeichnis	41

KAPITEL 1

Primfaktorzerlegung

Eine wichtige Grundlage der Zahlentheorie bildet der Satz von der eindeutigen Primfaktorzerlegung der natürlichen Zahlen. Wir geben zunächst einen direkten Beweis dieser Tatsache an. Anschließend erläutern wir in einem Ausblick, wie sich das Phänomen der eindeutigen Primfaktorzerlegung allgemeiner in den Idealgruppen algebraischer Zahlringe fortsetzt.

1. Der Ring \mathbb{Z} der ganzen Zahlen

Die elementare Zahlentheorie beschäftigt sich in erster Linie mit den Eigenschaften der natürlichen Zahlen $1, 2, 3, \dots$ bezüglich der Addition und Multiplikation. Die Methoden sind „elementar“, in dem Sinne, daß z.B. keine komplizierteren Hilfsmittel der Analysis oder Algebra benutzt werden.

Wir müssen uns zunächst einige Gedanken über die Natur der Zahlen selbst machen, egal wie vertraut sie uns erscheinen mögen. Oft zitiert findet sich der Ausspruch KRONECKERS, die ganzen Zahlen habe der liebe Gott gemacht, alles andere sei Menschenwerk. Egal, ob man dem zustimmen mag oder nicht, ausgehend von den Ideen CANTORS und DEDEKINDS hat sich die Mathematik im Laufe des zwanzigsten Jahrhunderts immer stärker zu einer mengentheoretischen Beschreibung ihrer Ergebnisse hinentwickelt. Gemäß dieser Sichtweise bauen alle mathematischen Objekte, insbesondere auch die Zahlen, auf dem (undefinierten) Grundbegriff der *Menge* auf.

Tatsächlich haben die natürlichen Zahlen ihren Ursprung in der Tätigkeit des Zählens, und dies setzt unbestreitbar die Existenz gewisser zu zählender und damit unterscheidbarer Objekte voraus. In [3] heißt es:

„Wenn man also mit einem einzigen Satz beschreiben wollte, womit die Mathematik befaßt ist, könnte man sagen, daß sie aus der Vielfalt der uns umgebenden Wirklichkeit einen einzigen Aspekt – und nur diesen – aufgreift und ausarbeitet, nämlich den folgenden: Es sind überall einzelne Objekte erkennbar, die man deutlich voneinander unterscheiden und nach Belieben gedanklich zu Ansammlungen zusammenfassen kann.“

Diese Auffassung spiegelt deutlich den naiven Mengenbegriff CANTORS aus dem Jahre 1895 wider: „Eine Menge ist eine Zusammenfassung bestimmter wohlunterschiedener Objekte unserer Anschauung oder unseres Denkens, welche Elemente der Menge genannt werden, zu einem Ganzen.“

Beispiele von Mengen liefern die vertrauten Zahlbereiche:

$\mathbb{N} = \{1, 2, 3, \dots\}$	Menge der natürlichen Zahlen,
$\mathbb{N}_0 := \{0\} \cup \mathbb{N}$	Menge der natürlichen Zahlen einschließlich Null,
$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$	Menge der ganzen Zahlen.

Streng genommen müßten diese Mengen erst einmal aus den Axiomen der Mengentheorie konstruiert werden. Die entsprechenden Überlegungen hierzu gehen zurück auf DEDEKIND. Wir begnügen uns an dieser Stelle mit einer knappen Skizze, um zumindest die allgemeine Vorgehensweise ersichtlich zu machen. Ausführlicher und sehr lesenswert ist in diesem Zusammenhang [2, Kapitel 1].

Den Ausgangspunkt für unsere Konstruktion bilden eine Menge N mit ausgezeichnetem Element e und eine Abbildung $\varphi : N \rightarrow N$ (die sogenannte Nachfolgerfunktion), so daß die folgenden Bedingungen erfüllt sind:

- (1) φ ist injektiv,
- (2) $e \notin \text{Bild}(\varphi)$,
- (3) jede Teilmenge $T \subseteq N$ mit $e \in T$ und $T\varphi \subseteq T$ ist schon gleich N .

Die Existenz eines solchen Tripels (N, e, φ) ist gleichbedeutend mit der Existenz überhaupt irgendeiner unendlichen Menge. Letzteres wird innerhalb des ZERMELO-FRAENKELschen Systems axiomatisch gefordert. Die namhaften PEANOSchen Axiome sind äquivalent zu (1)–(3), sofern sie nur mengentheoretisch interpretiert werden.

Das Tripel (N, e, φ) liefert ein (nicht kanonisches) Modell für die *natürlichen Zahlen*: Man schreibt $\mathbb{N} := N$ und etwas suggestiver $1 := e$, $2 := 1^\varphi$, $3 := 2^\varphi$, etc. In den Axiomen (1) und (2) wird die naive Vorstellung des Zählens begrifflich präzisiert: Man beginnt bei Eins und zählt immer weiter, ohne jemals erneut auf eine schon genannte Zahl zu stoßen. Das Axiom (3) besagt anschaulich, daß man durch beharrliches Fortzählen schließlich jede Zahl erreicht, und ist gleichbedeutend mit dem Prinzip der vollständigen Induktion.

MEMO. Eine *teilweise geordnete Menge* ist ein Paar (M, \leq) , bestehend aus einer Menge M und einer zweistelligen Relation \leq auf M , so daß für alle $a, b, c \in M$ die folgenden Bedingungen erfüllt sind:

- (1) $a \leq a$ (Reflexivität),
- (2) $(a \leq b \wedge b \leq a) \implies a = b$ (Antisymmetrie),
- (3) $(a \leq b \wedge b \leq c) \implies a \leq c$ (Transitivität).

Eine *total geordnete Menge* (auch *Kette* genannt) ist eine teilweise geordnete Menge (M, \leq) , in der je zwei Elemente vergleichbar sind, d.h. für alle $a, b \in M$ gilt $a \leq b$ oder $b \leq a$ (Linearität).

Der sogenannte DEDEKINDsche Rekursionsatz liefert die Eindeutigkeit der natürlichen Zahlen und erlaubt zugleich die Definition von Addition und Multiplikation. Alle vertrauten Rechenregeln lassen sich nun nachweisen: Es gelten die bekannten Assoziativ-, Kommutativ- und Distributivgesetze. Die Relation $<$ wird wie folgt auf \mathbb{N} definiert: Es gilt $m < n$ genau dann, wenn es ein $k \in \mathbb{N}$ gibt mit $m + k = n$. Man schreibt $m \leq n$, falls $m = n$ oder $m < n$ ist. Die Kleinergleich-Relation \leq ist dann wie gewünscht reflexiv, transitiv, antisymmetrisch und linear.

MEMO. Ein Paar $H = (H, \circ)$, bestehend aus einer Menge H und einer assoziativen Verknüpfung \circ auf H , heißt eine *Halbgruppe*. Ist $H = (H, \circ)$ eine Halbgruppe und $e \in H$, so heißt e *neutrales Element* in H , falls für alle $h \in H$ gilt: $e \circ h = h \circ e = h$. Existiert in einer Halbgruppe ein neutrales Element, so ist dieses schon eindeutig bestimmt. Eine Halbgruppe (H, \circ) heißt *kommutativ* (auch *abelsch*), falls die Verknüpfung \circ kommutativ ist.

MEMO. Ein Paar $G = (G, \circ)$, bestehend aus einer Menge G und einer Verknüpfung \circ auf G , heißt eine *Gruppe*, wenn die folgenden Bedingungen erfüllt sind:

- (1) G ist eine Halbgruppe mit neutralem Element e .
- (2) Zu jedem $a \in G$ existiert $b \in G$, so daß $b \circ a = a \circ b = e$.

Das Element b , dessen Existenz in Axiom (2) zu vorgegebenem a eingefordert wird, ist (durch a) eindeutig bestimmt und heißt *Inverses* von a .

Die Gruppenverknüpfung wird meist multiplikativ geschrieben (neutrales Element: 1, das zu a Inverse: a^{-1}), für abelsche Gruppen benutzt man auch die additive Schreibweise (neutrales Element: 0, das zu a Inverse: $-a$).

Das Bedürfnis, uneingeschränkt Rechnungen immer komplexer werdender Natur auszuführen, motiviert schrittweise die nunmehr algebraische Konstruktion der vertrauten Zahlbereiche

\mathbb{Z}	Ring der ganzen Zahlen,
\mathbb{Q}	Körper der rationalen Zahlen,
\mathbb{R}	Körper der reellen Zahlen,
\mathbb{C}	Körper der komplexen Zahlen.

MEMO. Ein Tripel $R = (R, +, \cdot)$, bestehend aus einer Menge R und zwei Verknüpfungen $+$ und \cdot auf R , heißt ein *Ring*, wenn die folgenden Bedingungen erfüllt sind:

- (1) $(R, +)$ ist eine abelsche Gruppe (das neutrale Element heißt Nullelement und wird mit 0 bezeichnet).
- (2) (R, \cdot) ist eine Halbgruppe.
- (3) Für alle $a, b, c \in R$ gilt $a(b + c) = ab + ac$ und $(a + b)c = ac + bc$ (Distributivgesetze).

Ein Ring R heißt *kommutativ*, wenn (R, \cdot) kommutativ ist. Ein Ring R heißt *nullteilerfrei*, wenn für alle $a, b \in R \setminus \{0\}$ gilt $ab \neq 0$. Ein Ring R heißt *Ring mit Eins*, wenn die Halbgruppe (R, \cdot) ein neutrales Element (Einselement) besitzt, welches von 0 verschieden ist; ein solches Einselement wird mit 1 bezeichnet. Ein *Integritätsbereich* ist ein kommutativer, nullteilerfreier Ring mit Eins.

Sei R ein Ring mit Eins. Ein Element $a \in R$ heißt *Einheit* in R , falls es ein $b \in R$ gibt mit $ab = ba = 1$. Die Einheiten in R bilden bezüglich \cdot eine Gruppe, die mit R^* bezeichnet wird.

Ein *Körper* ist ein kommutativer Ring mit Eins, in dem jedes von Null verschiedene Element eine Einheit ist. Insbesondere ist jeder Körper nullteilerfrei.

Jeder Integritätsbereich R besitzt einen sogenannten *Quotientenkörper*; dieser ist bis auf Isomorphie eindeutig bestimmt dadurch, daß er R als Teilring enthält und minimal mit dieser Eigenschaft ist.

Die systematische Einführung der *ganzen Zahlen* beruht auf der Beobachtung, daß jede ganze Zahl sich als Differenz zweier natürlicher Zahlen darstellen läßt. Ähnlich wird die Definition von \mathbb{Q} als Quotientenkörper von \mathbb{Z} dadurch motiviert, daß jede rationale Zahl ein Bruch zweier geeigneter ganzer Zahlen ist. Die Konstruktion von \mathbb{R} aus \mathbb{Q} ist vergleichsweise komplizierter, da hier auch topologische Gesichtspunkte eine Rolle spielen.

MEMO. Es sei R ein Ring und \leq eine (beliebige) zweistellige Relation auf R . Dann heißt \leq eine *Anordnung* von R und das Paar $R = (R, \leq)$ ein *geordneter Ring*, wenn (R, \leq) eine total geordnete Menge ist und für alle $a, b, c \in R$ gilt:

- (1) $a \leq b \implies a + c \leq b + c$ (Monotonie bezüglich $+$),
 (2) $(a \leq b \wedge 0 \leq c) \implies ac \leq bc$ (Monotonie bezüglich \cdot).

Die Verknüpfungen $+$, \cdot sowie die Anordnung \leq lassen sich von \mathbb{N} auf \mathbb{Z} sinnvoll fortsetzen, letztere durch die Definition: $a \leq b$ genau dann, wenn $b - a \in \mathbb{N}_0$. Es gilt der entscheidende

Hauptsatz 1.1 (Kennzeichnung der ganzen Zahlen). *Die ganzen Zahlen \mathbb{Z} bilden unter der bekannten Addition und Multiplikation einen Integritätsbereich. Mit der gewöhnlichen Kleinerleich-Relation wird \mathbb{Z} zu einem geordneten Ring, in dem jede nach unten beschränkte nicht-leere Teilmenge ein kleinstes Element besitzt.*

Es läßt sich zeigen, daß die genannten Eigenschaften \mathbb{Z} als geordneten Ring bis auf Isomorphie eindeutig charakterisieren; vgl. [4]. Wir beenden diesen Abschnitt mit einem ausführlichen Beweis der folgenden Eindeutigkeitsaussage.

Satz 1.2. *Auf dem Ring \mathbb{Z} gibt es genau eine Anordnung, nämlich die gewöhnliche Kleinerleich-Relation \leq .*

Beweis. Sei \preccurlyeq eine beliebige Anordnung von \mathbb{Z} . Zu zeigen ist eigentlich: Für alle $a, b \in \mathbb{Z}$ gilt: $a \leq b \iff a \preccurlyeq b$. Aufgrund von Reflexivität, Antisymmetrie und Vergleichbarkeit genügt jedoch bereits eine Richtung, z.B.: Für alle $a, b \in \mathbb{Z}$ mit $a \leq b$ ist auch $a \preccurlyeq b$.

Wir zeigen zunächst: $0 \preccurlyeq 1$. Angenommen, dies gilt nicht. Das Prinzip der Vergleichbarkeit liefert dann $1 \preccurlyeq 0$, und die Monotonie der Addition zeigt: $0 = 1 + (-1) \preccurlyeq 0 + (-1) = -1$. Die Monotonie der Multiplikation liefert daher $0 = 0 \cdot (-1) \preccurlyeq (-1) \cdot (-1) = 1$, also $0 \preccurlyeq 1$. Aus der Antisymmetrie folgt nun $0 = 1$, ein Widerspruch. Damit ist $0 \preccurlyeq 1$ wie gewünscht.

Als nächstes beweisen wir per Induktion, daß für alle $n \in \mathbb{N}_0$ gilt: $0 \preccurlyeq n$. Die Reflexivität sichert den Induktionsanfang: $0 \preccurlyeq 0$. Sei nun $n > 0$. Nach Induktionsvoraussetzung ist $0 \preccurlyeq n - 1$. Aus $0 \preccurlyeq 1$ folgt dann gemäß der Monotonie der Addition: $0 \preccurlyeq 1 = 0 + 1 \preccurlyeq (n - 1) + 1 = n$, also in der Tat $0 \preccurlyeq n$.

Seien nun $a, b \in \mathbb{Z}$ mit $a \leq b$. Zu zeigen ist: $a \preccurlyeq b$. Fürwahr, aus $a \leq b$ folgt definitionsgemäß $k := b - a \in \mathbb{N}_0$, und somit gilt $0 \preccurlyeq k$. Die Monotonie der Addition liefert daher $a = a + 0 \preccurlyeq a + k = b$, also $a \preccurlyeq b$ wie gewünscht. \square

Die Anordnung \leq besitzt eine eindeutige Fortsetzung von \mathbb{Z} auf \mathbb{Q} , so daß \mathbb{Q} die Struktur eines geordneten Körpers erhält; für alle $x, y \in \mathbb{Q}$ gilt: $x \leq y$ genau dann, wenn es $n \in \mathbb{N}$ mit $n(y - x) \in \mathbb{N}_0$ gibt.

Aufgabe 1.3. Besitzt der Körper \mathbb{C} der komplexen Zahlen eine Anordnung? Zeige, daß der Ring $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ genau zwei Anordnungen erlaubt. Läßt der Polynomring $\mathbb{Q}[X]$ eine Anordnung zu?

2. Teilbarkeit in Integritätsbereichen

Wir betrachten in diesem Abschnitt etwas allgemeiner einen Integritätsbereich R , d.h. einen kommutativen, nullteilerfreien Ring mit Einselement $1 \neq 0$. (Zahlentheorie läßt sich nicht nur auf \mathbb{Z} , sondern z.B. auch auf Polynomringen über endlichen Körpern betreiben!)

Definition 2.1. Seien $a, b \in R$. Man sagt, a teilt b , wenn es ein $c \in R$ gibt mit $ac = b$, und schreibt dann $a \mid b$. Die Elemente a und b heißen zueinander *assoziiert*, in Zeichen $a \sim b$, falls $a \mid b$ und $b \mid a$.

Lemma 2.2. Seien $a, b_1, b_2 \in R$.

- (1) Die Teilbarkeitsrelation \mid ist reflexiv und transitiv (aber nicht symmetrisch!).
- (2) Jedes Element aus R teilt 0; die Null teilt nur sich selbst.
- (3) Ein Teiler von 1 teilt jedes Element von R .
- (4) Es gilt $a \mid 1$ genau dann, wenn a eine Einheit ist (d.h. $a \in R^*$).
- (5) Die Elemente b_1 und b_2 sind zueinander assoziiert genau dann, wenn gilt $b_1 = b_2 e$ für eine geeignete Einheit $e \in R^*$.
- (6) Aus $a \mid b_1$ und $a \mid b_2$ folgt für alle $c_1, c_2 \in R$: $a \mid (c_1 b_1 + c_2 b_2)$.

Diese Rechenregeln sind leicht nachzuweisen. Die Aussagen (1) und (5) des Lemmas besagen, daß \sim eine Äquivalenzrelation auf R definiert, deren Äquivalenzklassen gerade aus den Mengen $aR^* = \{ae \mid e \in R^*\}$, $a \in R$, bestehen. Aus (5) sieht man zudem, daß assoziierte Elemente dasselbe Teilverhalten haben.

Definition 2.3. (a) Seien $a, b \in R$ mit $a \mid b$. Dann heißt a *trivialer Teiler* von b , falls gilt: $a \sim 1$ oder $a \sim b$; andernfalls heißt a *echter Teiler* von b .

(b) Sei $a \in R \setminus (\{0\} \cup R^*)$. Dann heißt a *unzerlegbar* (auch *irreduzibel*), falls a keine echten Teiler besitzt; a heißt *prim*, falls für alle $b, c \in R$ aus $a \mid bc$ schon $a \mid b$ oder $a \mid c$ folgt.

(c) Zwei Elemente $a, b \in R$ heißen zueinander *teilerfremd*, falls für jedes $t \in R$ aus $t \mid a$ und $t \mid b$ schon $t \in R^*$ folgt.

Lemma 2.4. Sei $p \in R$ prim. Dann ist p unzerlegbar.

Beweis. Sei $a \in R$ ein Teiler von p . Wir finden $b \in R$, so daß gilt: $p \mid p = ab$. Da p prim ist, folgt $p \mid a$ oder $p \mid b$. Gilt $p \mid a$, so ist a assoziiert zu p und somit kein echter Teiler von p .

Sei nun $p \mid b$. Wir finden $c \in R$, so daß gilt: $p = ab = acp$. Da R nullteilerfrei ist, folgt $1 = ac$. Also ist $a \in R^*$ kein echter Teiler von p . \square

MEMO. Sind $G = (G, \circ)$ und $U = (U, *)$ Gruppen, so heißt U *Untergruppe* von G , in Zeichen $U \leq G$, falls $U \subseteq G$ und $* = \circ|_{U \times U}$. Sei G eine Gruppe und $U \subseteq G$. Dann ist U (die Trägermenge einer) Untergruppe von G genau dann, wenn U nicht leer ist und für alle $a, b \in U$ gilt $a^{-1}b \in U$.

Aufgabe 2.5. In dem Ring $R := \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ ist $2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Insbesondere gilt $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$.

Zeige: (a) $R^* = \{-1, 1\}$, (b) 2 ist unzerlegbar (in R), (c) 2 ist nicht prim (in R).

MEMO. Sei R ein kommutativer Ring. Eine Teilmenge I von R heißt *Ideal* von R , in Zeichen $I \trianglelefteq R$, falls gilt:

- (1) I ist eine additive Untergruppe von R .
- (2) Für alle $a \in R$ und $b \in I$ gilt $ab \in I$.

Für jedes $a \in R$ ist $aR = \{ab \mid b \in R\}$ ein Ideal von R ; Ideale dieser Gestalt heißen *Hauptideale*. Ein *Hauptidealring* ist ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist.

Lemma 2.6. Sei R ein Hauptidealring und $p \in R$ unzerlegbar. Dann ist p prim.

Beweis. Seien $a, b \in R$ mit $p \mid ab$. Zu zeigen ist: $p \mid a$ oder $p \mid b$. Offensichtlich ist $I := \{x \in R \mid p \mid ax\}$ ein Ideal von R . Also finden wir $m \in R$ mit $I = mR$. Wegen $p \in I$ gilt $m \mid p$. Da p unzerlegbar ist, folgt $m \in R^*$ oder $m \sim p$. Ist $m \in R^*$, so ist $I = R$, also $1 \in I$, und daraus folgt $p \mid a$. Sei nun $m \sim p$. Wegen $b \in I$ erhalten wir $p \mid m \mid b$, also $p \mid b$. \square

3. Eindeutige Primfaktorzerlegung in \mathbb{Z}

Im Ring \mathbb{Z} der ganzen Zahlen gibt es einen grundlegenden Zusammenhang zwischen Teilbarkeit und Anordnung.

MEMO. Die (archimedische) *Betragsfunktion* ist auf \mathbb{Q} wie folgt definiert:

$$|x| := \begin{cases} x & \text{falls } 0 \leq x, \\ -x & \text{falls } x < 0. \end{cases}$$

Für alle $x, y \in \mathbb{Q}$ gilt:

- (1) $|x| \geq 0$, und $|x| = 0 \iff x = 0$;
- (2) $|xy| = |x| \cdot |y|$;
- (3) $|x + y| \leq |x| + |y|$ (Dreiecksungleichung).

Lemma 3.1. Es ist $\mathbb{Z}^* = \{-1, 1\}$, und für alle $a, b \in \mathbb{Z}$ gilt:

- (1) $a \mid b \implies |a| \leq |b|$,
- (2) $a \sim b \iff |a| = |b|$.

Diese Beobachtungen ergeben sich leicht mit Hilfe der Monotonie-Eigenschaften der Kleinerleich-Relation. Aufgrund von Aussage (2) beschränkt man sich bei Teilbarkeitsbetrachtungen in \mathbb{Z} oft auf den Bereich der natürlichen Zahlen: Die Menge \mathbb{N}_0 bildet ein Repräsentantensystem für die Äquivalenzklassen bezüglich \sim in \mathbb{Z} .

Definition 3.2. Für $a \in \mathbb{Z}$ bezeichne $T^+(a) := \{t \in \mathbb{N} \mid t \mid a\}$ die Menge der positiven Teiler von a .

Eine natürliche Zahl p heißt *Primzahl*, falls $p \neq 1$ und $T^+(p) = \{1, p\}$ ist. Die Menge aller Primzahlen wird mit \mathbb{P} bezeichnet.

Bemerkung 3.3. Es gilt: $\mathbb{P} = \{p \in \mathbb{N}_0 \mid p \text{ ist unzerlegbar in } \mathbb{Z}\}$.

Die Zahlen 2, 3, 5, 7, 11, 13, 17, 19, 23, ... sind bekanntlich Primzahlen. Bereits in den Elementen von EUKLID findet sich die Aussage, daß „es mehr Primzahlen gibt als jede vorgelegte Anzahl von Primzahlen“; siehe Satz 3.6.

Zugleich sollte man sich jedoch vor Augen halten: Es ist kein „effektives“ Verfahren bekannt, das zu gegebenem $n \in \mathbb{N}$ eine Primzahl p liefert, die größer als n ausfällt. Glaubt man <http://primes.utm.edu/bios/home.php>, so ist $2^{24036583} - 1$ mit insgesamt 7235733 Dezimalstellen die bislang (Stichtag 13. Oktober, 2004) größte natürliche Zahl, die in einem rechentechnischen Sinne nachweislich prim ist. Hierbei handelt es sich – nicht ganz zufällig – um eine sogenannte MERSENNEsche Primzahl.

Definition 3.4. Für jedes $a \in \mathbb{Z} \setminus \{1, -1\}$ ist die Teilmengens $T^+(a) \setminus \{1\}$ nicht leer und besitzt daher ein kleinstes Element, das wir mit $\text{kpT}(a)$ bezeichnen.

Lemma 3.5. Sei $a \in \mathbb{Z} \setminus \{1, -1\}$. Dann gilt $p := \text{kpT}(a) \in \mathbb{P}$.

Beweis. Sei $t \in T^+(p) \setminus \{1\}$. Zu zeigen ist: $t = p$. Aus $t \mid p$ und $p \mid a$ folgt $t \mid a$, und somit $t \in T^+(a) \setminus \{1\}$. Dies impliziert $p = \text{kpT}(a) \leq t$. Wegen $t \mid p$ gilt auch $t \leq p$, insgesamt also $t = p$. \square

Satz 3.6 (Euklid). *Es gibt unendlich viele Primzahlen.*

Beweis. Seien $r \in \mathbb{N}$ und $a_1, a_2, \dots, a_r \in \mathbb{N}$. Offenbar reicht es, eine Primzahl p zu bestimmen, die nicht unter den Zahlen a_1, a_2, \dots, a_r vorkommt. Setze $n := a_1 \cdots a_r + 1 \geq 2$. Nach Lemma 3.5 ist $p := \text{kpT}(n) \in \mathbb{P}$.

Angenommen, $p \in \{a_1, \dots, a_r\}$. Aus $p \mid n$ und $p \mid a_1 \cdots a_r$ folgt $p \mid (n - a_1 \cdots a_r) = 1$. Somit ist $p \in \{1, -1\}$. Dies widerspricht der Tatsache $p \in \mathbb{P}$. \square

Lemma 3.7 (Division mit Rest). *Seien $a, b \in \mathbb{Z}$ mit $b \neq 0$. Dann gibt es eindeutig bestimmte $q, r \in \mathbb{Z}$ mit den Eigenschaften: $a = bq + r$ und $0 \leq r < |b|$.*

Beweis. Die Menge $M := \{m \in \mathbb{Z} \mid bm \leq a\}$ ist nach oben bzw. nach unten beschränkt, je nach dem, ob $b > 0$ oder $b < 0$ ist. Setze

$$q := \begin{cases} \max M & \text{falls } b > 0, \\ \min M & \text{falls } b < 0 \end{cases}$$

und $r := a - bq$. Dann haben q, r die gewünschten Eigenschaften.

Seien nun $\tilde{q}, \tilde{r} \in \mathbb{Z}$ mit $a = b\tilde{q} + \tilde{r}$ und $0 \leq \tilde{r} < |b|$. Dann gilt $b(q - \tilde{q}) = \tilde{r} - r$, also $b \mid (\tilde{r} - r)$. Aus $|\tilde{r} - r| < |b|$ folgt daher $\tilde{r} - r = 0$ und somit $\tilde{r} = r$, $\tilde{q} = q$. \square

Satz 3.8 (Untergruppen von \mathbb{Z}). *Die Untergruppen von $(\mathbb{Z}, +)$ sind genau die Mengen $U = m\mathbb{Z}$, $m \in \mathbb{N}_0$, versehen mit der induzierten Verknüpfung. Insbesondere bildet jede additive Untergruppe von \mathbb{Z} ein Ideal von \mathbb{Z} .*

Beweis. Offenbar sind die Mengen $m\mathbb{Z}$, $m \in \mathbb{N}_0$, paarweise verschieden, und jede von diesen bildet eine Untergruppe bezüglich der induzierten Verknüpfung. Sei nun U eine beliebige Untergruppe von \mathbb{Z} . Ist $U = \{0\}$, so gilt $U = 0\mathbb{Z}$. Sei nun $U \neq \{0\}$. Dann ist $U^+ := \{u \in U \mid u > 0\} \neq \emptyset$. Setze $m := \min U^+$.

Offenbar gilt dann $m\mathbb{Z} \subseteq U$. Sei nun $u \in U$. Division mit Rest liefert dann $u = mq + r$ für geeignete $q, r \in \mathbb{Z}$ mit $0 \leq r < m$. Es folgt $r = u - mq \in U$ und, aufgrund der Wahl von m , schließlich $r = 0$. Also ist $u = mq \in m\mathbb{Z}$. Daraus folgt $U = m\mathbb{Z}$. \square

Korollar 3.9. *Der Ring \mathbb{Z} der ganzen Zahlen ist ein Hauptidealring.*

Insbesondere besteht in \mathbb{Z} gemäß Lemmata 2.4 und 2.6 kein Unterschied zwischen den Eigenschaften „unzerlegbar“ und „prim“. Wir kommen nun zu dem grundlegenden Satz über die eindeutige Primfaktorzerlegung.

Hauptsatz 3.10 (Eindeutige Primfaktorzerlegung). *Zu jeder natürlichen Zahl $a \in \mathbb{N}$ gibt es ein $m \in \mathbb{N}_0$ und Primzahlen $p_1, \dots, p_m \in \mathbb{P}$ mit $a = p_1 \cdots p_m$.*

Eine solche Darstellung von a als Produkt von Primzahlen ist – bis auf die Reihenfolge der Faktoren – eindeutig durch a bestimmt.

Beweis. Sei $a \in \mathbb{N}$. Unter einer *aufsteigenden Primfaktorzerlegung* (kurz: aPFZ) von a verstehen wir ein Tupel (p_1, \dots, p_m) , wobei $m \in \mathbb{N}_0$, $p_1, \dots, p_m \in \mathbb{P}$ mit $p_1 \leq \dots \leq p_m$ und $a = p_1 \cdots p_m$. Zu zeigen ist: a besitzt genau eine aPFZ.

Die Existenz einer aPFZ beweisen wir durch Induktion nach a . Der Induktionsanfang $a = 1$ ist klar: Das leere Tupel $()$ ist eine aPFZ von 1. Sei nun $a > 1$. Nach

Lemma 3.5 ist $p_0 := \text{kpT}(a) \in \mathbb{P} \cap T^+(a)$ der kleinste Primteiler von a . Wir finden $b \in \mathbb{Z}$ mit $a = p_0 b$, und offenbar gilt $b \in \{1, \dots, a-1\}$. Nach Induktionsvoraussetzung besitzt b eine aPFZ (p_1, \dots, p_m) . Wegen $\{p_1, \dots, p_m\} \subseteq \mathbb{P} \cap T^+(b) \subseteq \mathbb{P} \cap T^+(a)$ ist $p_0 \leq p_1, \dots, p_m$. Somit ist (p_0, p_1, \dots, p_m) eine aPFZ von a .

Wir kommen nun zum Beweis der Eindeutigkeit. Sei sowohl (p_1, \dots, p_m) als auch (q_1, \dots, q_n) eine aPFZ von a . Ohne Einschränkung gelte $m \leq n$. Zu zeigen ist: $(p_1, \dots, p_m) = (q_1, \dots, q_n)$. Wir benutzen Induktion nach m . Der Induktionsanfang ist trivial: Aus $m = 0$ folgt $a = 1$, und offenbar ist $()$ die einzige aPFZ von 1. Sei nun $m \geq 1$. Es gilt: $p_1 \mid a = q_1 \cdots q_n$ und $q_1 \mid a = p_1 \cdots p_m$. Aufgrund der Primeigenschaft von p_1 bzw. q_1 finden wir deshalb $i \in \{1, \dots, n\}$ und $j \in \{1, \dots, m\}$ mit $p_1 \mid q_i$ und $q_1 \mid p_j$. Da q_i und p_j unzerlegbar sind, folgt nun $p_1 = q_i$ und $q_1 = p_j$. Das ergibt $q_1 \leq q_i = p_1$ und $p_1 \leq p_j = q_1$, also $p_1 = q_1$. Die Induktionsvoraussetzung angewandt auf $a' := p_2 \cdots p_m = q_2 \cdots q_n$ liefert $(p_2, \dots, p_m) = (q_2, \dots, q_n)$. \square

Aufgabe 3.11 (HILBERTSche Halbgruppe). Betrachte $H := \{4k + 1 \mid k \in \mathbb{N}_0\} = \{1, 5, 9, 13, 17, 21, \dots\}$. Überprüfe, daß H bezüglich der gewöhnlichen Multiplikation eine Halbgruppe mit Einselement bildet. Ein Element $h \in H$ heie *unzerlegbar*, wenn für alle $a, b \in H$ mit $h = ab$ gilt: $a = 1$ oder $b = 1$. Beweise, daß jedes Element $h \in H$ sich als Produkt unzerlegbarer Elemente schreiben lät. Ist eine solche Darstellung (bis auf die Reihenfolge der Faktoren) stets eindeutig durch h bestimmt?

4. Ideale und Kongruenzen – ein Zwischenstück

Die eindeutige Primfaktorzerlegung in \mathbb{Z} kann als Spezialfall eines viel allgemeineren Phänomens angesehen werden. Letzteres lät sich sehr überzeugend in der Sprache der Ideale formulieren. In diesem Abschnitt vergegenwärtigen wir uns vorbereitend grundlegende Eigenschaften von Idealen.

MEMO. Sei R ein kommutativer Ring, und sei $I \triangleleft R$. Zwei Elemente $a, b \in R$ heißen *kongruent modulo I* , in Zeichen $a \equiv_I b$, falls gilt $a - b \in I$. Die so definierte Kongruenzrelation \equiv_I auf R besitzt die Eigenschaften einer Äquivalenzrelation. Ist $I = mR$ ein Hauptideal, so schreibt man für $a \equiv_{mR} b$ auch kurz $a \equiv_m b$ und sagt, a ist kongruent zu b modulo m .
 Auf der Restklassenmenge $R/I = \{a+I \mid a \in R\}$ lät sich mittels Repräsentanten eine natürliche Ringstruktur definieren: Für $a+I, b+I \in R/I$ ist $(a+I) + (b+I) = (a+b) + I$ und $(a+I)(b+I) = ab + I$. Die Abbildung $R \rightarrow R/I, a \mapsto a+I$ ist ein surjektiver Ringhomomorphismus.
 Sei $\varphi : R \rightarrow S$ ein Ringhomomorphismus. Der *Kern* von φ ist definiert als $\text{Kern}(\varphi) := \{a \in R \mid a^\varphi = 0\}$ und bildet ein Ideal von R . Das *Bild* von φ ist definiert als $\text{Bild}(\varphi) := \{a^\varphi \mid a \in R\}$ und bildet einen Unterring von S . Das Bild von φ ist kanonisch isomorph zu dem Restklassenring $R/\text{Kern}(\varphi)$.

Nach Satz 3.8 ist jedes Ideal von \mathbb{Z} ein Hauptideal, d.h. von der Form $m\mathbb{Z}$, $m \in \mathbb{N}_0$. Das Rechnen mit ganzen Zahlen modulo einer festen Zahl $m \in \mathbb{N}_0$ entspricht gerade dem Rechnen im Restklassenring $\mathbb{Z}/m\mathbb{Z}$.

Beispiel 4.1 (Elementare Teilbarkeitstests). Sei $N = [a_n, a_{n-1}, \dots, a_0]_{\text{dez}}$ eine im Dezimalsystem geschriebene natürliche Zahl. Es gelten also $n \in \mathbb{N}_0$, $a_0, \dots, a_n \in \{0, 1, \dots, 9\}$ und $N = a_0 + 10^1 a_1 + \dots + 10^n a_n$.

Dann gilt:

$$\begin{aligned} 2 \mid N &\iff 2 \mid a_0, & \text{denn } 10 &\equiv_2 0; \\ 4 \mid N &\iff 4 \mid (a_0 + 10a_1), & \text{denn } 100 &\equiv_4 0; \\ 8 \mid N &\iff 8 \mid (a_0 + 10a_1 + 100a_2), & \text{denn } 1000 &\equiv_8 0; \\ 5 \mid N &\iff 5 \mid a_0 \iff a_0 \in \{0, 5\}, & \text{denn } 10 &\equiv_5 0. \end{aligned}$$

Um die Teilbarkeit bezüglich 3, 9, 7, 11, 13 zu entscheiden, betrachte die folgenden „Quersummen“:

$$\begin{aligned} S &:= a_0 + a_1 + \dots + a_n, & S^* &:= a_0 - a_1 + a_2 - a_3 + \dots + (-1)^n a_n, \\ T &:= (a_0 + 10a_1 + 100a_2) - (a_3 + 10a_4 + 100a_5) + (a_6 + 10a_7 + 100a_8) - \dots \\ &= [a_2, a_1, a_0]_{\text{dez}} - [a_5, a_4, a_3]_{\text{dez}} + [a_8, a_7, a_6]_{\text{dez}} - \dots \end{aligned}$$

Dann gilt:

$$\begin{aligned} 3 \mid N &\iff 3 \mid S, & \text{denn } 10 &\equiv_3 1; \\ 9 \mid N &\iff 9 \mid S, & \text{denn } 10 &\equiv_9 1; \\ 7 \mid N &\iff 7 \mid T, & \text{denn } 1000 &\equiv_7 -1; \\ 11 \mid N &\iff 11 \mid S^*, & \text{denn } 10 &\equiv_{11} -1; \\ 13 \mid N &\iff 13 \mid T, & \text{denn } 1000 &\equiv_{13} -1. \end{aligned}$$

MEMO. Sei R ein kommutativer Ring mit 1.
 Sei $I \trianglelefteq R$. Dann heißt I *maximales Ideal* von R , falls $I \neq R$ und aus $I \subsetneq J \trianglelefteq R$ stets $J = R$ folgt. Das Ideal I heißt *Primideal* von R , falls $I \neq R$ und für alle $a, b \in R$ mit $ab \in I$ gilt: $a \in I$ oder $b \in I$.
 Man überlegt sich leicht:
 (1) I ist ein maximales Ideal von $R \iff R/I$ ist ein Körper.
 (2) I ist ein Primideal von $R \iff R/I$ ist ein Integritätsbereich.
 Insbesondere ist jedes maximale Ideal ein Primideal.
 Ein *maximales Hauptideal* von R ist ein maximales Element in der durch \subseteq teilweise geordneten Menge $\{I \mid I \neq R \text{ ein Hauptideal von } R\}$.

Die folgenden einfachen Beobachtungen legen schon nahe, daß sich gewisse Teilbarkeitseigenschaften zweckreich mit Hilfe des Idealbegriffs formulieren lassen.

Lemma 4.2. *Sei R ein Integritätsbereich. Dann gilt für alle $a, b \in R$:*

- (1) $a \mid b$ genau dann, wenn $aR \supseteq bR$;
- (2) $a \sim b$ genau dann, wenn $aR = bR$;
- (3) $a \in R^*$ genau dann, wenn $aR = R$;
- (4) a ist unzerlegbar in R genau dann, wenn $aR \neq \{0\}$ ein maximales Hauptideal von R ist;
- (5) a ist prim in R genau dann, wenn $aR \neq \{0\}$ ein Primideal von R ist.

Korollar 4.3. *Sei $m \in \mathbb{Z}$. Dann ist der Restklassenring $\mathbb{Z}/m\mathbb{Z}$ genau dann ein Körper, wenn $|m|$ eine Primzahl ist.*

Der englische Fachbegriff für Körper ist „field“. Mittlerweile ist es üblich, den endlichen Körper $\mathbb{Z}/p\mathbb{Z}$, $p \in \mathbb{P}$, mit dem Symbol \mathbb{F}_p zu bezeichnen. Man kann sich

überlegen, daß es allgemeiner zu jeder Primzahlpotenz p^k bis auf Isomorphie genau einen Körper der Mächtigkeit p^k gibt; dieser wird dann entsprechend mit \mathbb{F}_{p^k} bezeichnet.

5. Dedekindsche Ringe – ein Streifzug

Eine wichtige Rolle in der Zahlentheorie spielen die sogenannten Ganzheitsringe algebraischer Zahlkörper. Jeder von diesen stellt in gewisser Weise eine Verallgemeinerung der gewöhnlichen ganzen Zahlen dar. Einfache Beispiele sind $\mathbb{Z}[\sqrt{2}]$ und $\mathbb{Z}[\sqrt{-5}]$; vgl. Aufgaben 1.3 und 2.5. Ringe dieser Art – sie heißen Ganzheitsringe quadratischer Zahlkörper – werden ausführlicher im nächsten Kapitel behandelt.

Auch in Ganzheitsringen algebraischer Zahlkörper gibt es eine eindeutige Primfaktorzerlegung, im allgemeinen jedoch nicht mehr auf der Ebene der Zahlen selbst, sondern auf der Ebene der Ideale. Die entsprechenden Überlegungen gehen zurück auf DEDEKIND und KUMMER; letzterer spricht noch von „idealen Zahlen“. Eine systematische Untersuchung der Ganzheitsringe findet in der algebraischen Zahlentheorie statt.

MEMO. Sei R ein kommutativer Ring mit 1.
 Ein Ideal A von R heißt *endlich erzeugt*, falls es $m \in \mathbb{N}$ und $a_1, \dots, a_m \in R$ gibt mit $A = a_1R + \dots + a_mR$.
 Der Ring R heißt *noethersch*, falls jede nicht-leere Menge von Idealen von R ein maximales Element bezüglich \subseteq enthält.

Ein wichtiges algebraisches Werkzeug, welches in einem allgemeinen Rahmen gewisserweise das Prinzip der vollständigen Induktion ersetzt, ist das sogenannte ZORNSche Lemma. Man kann sich überlegen, daß dieses äquivalent zum sogenannten Auswahlaxiom ist; siehe [2, Kapitel 14].

Zornsches Lemma. *Sei (\mathcal{M}, \subseteq) eine teilweise geordnete Menge, welche die folgenden Bedingungen erfüllt: $\mathcal{M} \neq \emptyset$ und jede nicht-leere Teilkette von (\mathcal{M}, \subseteq) hat eine obere Schranke in \mathcal{M} . Dann besitzt \mathcal{M} ein maximales Element.*

Lemma 5.1. *Sei R ein kommutativer Ring mit 1, und sei $A \trianglelefteq R$ mit $A \neq R$. Dann existiert ein maximales Ideal M von R mit $A \subseteq M$.*

Beweis. Sei \mathcal{M} die Menge aller Ideale I von R mit $A \subseteq I \subsetneq R$. Wegen $A \in \mathcal{M}$ ist \mathcal{M} nicht leer. Ist \mathcal{J} eine nicht-leere Teilkette von (\mathcal{M}, \subseteq) , so ist $\bigcup \mathcal{J}$ eine obere Schranke von \mathcal{J} in \mathcal{M} ; beachte hierbei, daß R ein Einselement besitzt. Damit sind die Voraussetzungen für das ZORNSche Lemma erfüllt: \mathcal{M} besitzt ein maximales Element M . Offensichtlich ist M ein maximales Ideal von R mit $A \subseteq M$. \square

Lemma 5.2. *Sei R ein kommutativer Ring. Dann ist R noethersch genau dann, wenn jedes Ideal von R endlich erzeugt ist.*

Beweis. Sei zunächst R noethersch, und sei $A \trianglelefteq R$. Bezeichne mit \mathcal{M} die Menge aller endlich erzeugten Ideale I von R mit $I \subseteq A$. Wegen $\{0\} \in \mathcal{M}$ ist \mathcal{M} nicht leer. Wähle ein maximales Element J von \mathcal{M} bezüglich \subseteq . Es genügt, zu zeigen: $J = A$. Dazu machen wir die Widerspruchsannahme: $J \subsetneq A$. Wähle $a \in A \setminus J$. Dann ist $I := J + aR$ ein endlich erzeugtes Ideal von R mit $J \subsetneq I \subseteq A$. Dies widerspricht der Wahl von J . Also ist $A = J$ endlich erzeugt.

Sei nun vorausgesetzt, daß jedes Ideal von R endlich erzeugt ist, und sei \mathcal{M} eine nicht-leere Menge von Idealen von R . Wir überprüfen die noch ausstehende

Voraussetzung, um das ZORNSche Lemma anwenden zu können. Sei \mathcal{T} eine nicht-leere Teilkette von (\mathcal{M}, \subseteq) . Dann ist $\bigcup \mathcal{T}$ ein Ideal von R , also endlich erzeugt und damit schon gleich einem (zwangsläufig maximalen) Element von \mathcal{T} . Somit bildet $\bigcup \mathcal{T} \in \mathcal{T}$ eine obere Schranke für \mathcal{T} in \mathcal{M} . \square

Im folgenden bezeichne R stets einen Integritätsbereich und K dessen Quotientenkörper. Wir definieren

$$\begin{aligned} \mathcal{J}(R) &:= \{I \mid I \neq 0 \text{ ein Ideal von } R\}, \\ \mathcal{P}(R) &:= \{P \mid P \neq 0 \text{ ein Primideal von } R\}. \end{aligned}$$

Als nächstes wollen wir ein Produkt auf der Menge $\mathcal{J}(R)$ der von Null verschiedenen Ideale erklären.

Definition 5.3. Für Teilmengen $A, B \subseteq K$ definieren wir das Produkt

$$A \circ B := \{a_1 b_1 + \dots + a_m b_m \mid m \in \mathbb{N}, a_i \in A, b_i \in B\}.$$

Ist $A = \{a\}$ einelementig und B additiv abgeschlossen, so schreiben wir in Übereinstimmung mit unserer bisherigen Praxis auch aB statt $\{a\} \circ B$.

Die Menge $\mathcal{J}(R)$ ist bezüglich \circ eine kommutative Halbgruppe mit R als Einselement. Für alle $A, B \in \mathcal{J}(R)$ gilt $A \circ B \subseteq A \cap B \in \mathcal{J}(R)$.

Definition 5.4. Seien $A, B \in \mathcal{J}(R)$. Man sagt, A teilt B , falls es ein $C \in \mathcal{J}(R)$ gibt mit $A \circ C = B$, und schreibt dann $A \mid B$.

Lemma 5.5. Seien $A, B \in \mathcal{J}(R)$ und $P \in \mathcal{P}(R)$. Dann gilt:

- (1) $A \mid B$ impliziert $A \supseteq B$.
- (2) $P \supseteq A \circ B$ impliziert $P \supseteq A$ oder $P \supseteq B$.

Definition 5.6. (1) Für $A \in \mathcal{J}(R)$ definiere $A^* := \{x \in K \mid xA \subseteq R\}$. Ein Ideal $A \in \mathcal{J}(R)$ heißt *invertierbar*, falls $A \circ A^* = R$ ist.

(2) Wir sagen, R erfüllt die *Teilerregel für Ideale*, falls für alle $A, B \in \mathcal{J}(R)$ gilt: $A \mid B$ genau dann, wenn $A \supseteq B$.

(3) Wir sagen, R erfüllt die *Kürzungsregel für Ideale*, falls für alle $A, B, C \in \mathcal{J}(R)$ gilt: $B \circ A = C \circ A$ impliziert $B = C$.

Offenbar gilt $A \subseteq A \circ A^* \in \mathcal{J}(R)$ für alle $A \in \mathcal{J}(R)$. Wegen $1 \in R$ ist $R^* = R$.

Lemma 5.7 (Schwache Kürzungsregel). Sei R noethersch, und seien $A, B \in \mathcal{J}(R)$ mit $B \circ A = A$. Dann folgt $B = R$.

Beweis. Da R noethersch ist, finden wir nach Lemma 5.2 ein $m \in \mathbb{N}$ und $a_1, \dots, a_m \in A \setminus \{0\}$ mit $A = a_1 R + \dots + a_m R$. Wegen $A = B \circ A$ finden wir $b_{11}, \dots, b_{mm} \in B$, so daß gilt:

$$\begin{aligned} a_1 &= b_{11}a_1 + b_{12}a_2 + \dots + b_{1m}a_m, \\ &\vdots \\ a_m &= b_{m1}a_1 + b_{m2}a_2 + \dots + b_{mm}a_m. \end{aligned}$$

Daraus folgt

$$\begin{pmatrix} 1 - b_{11} & -b_{12} & \cdots & -b_{1m} \\ -b_{21} & 1 - b_{22} & \cdots & -b_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ -b_{m1} & -b_{m2} & \cdots & 1 - b_{mm} \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Die Determinante der Matrix auf der linken Seite ist von der Gestalt $1 - b$ mit $b \in B$. Da R ein Integritätsbereich ist, gilt $1 - b = 0$, also $1 = b \in B$. Es folgt $B = R$. \square

Definition 5.8. Ein Ring R heißt *Dedekindring*, wenn die folgenden Bedingungen erfüllt sind:

- (1) R ist ein Integritätsbereich.
- (2) Zu jedem $A \in \mathcal{J}(R)$ gibt es ein $m \in \mathbb{N}_0$ und Primideale $P_1, \dots, P_m \in \mathcal{P}(R)$ mit $A = P_1 \circ \dots \circ P_m$. Eine solche Darstellung von A als Produkt von Primidealen ist – bis auf die Reihenfolge der Faktoren – eindeutig durch A bestimmt.

Dedekindringe lassen sich auf vielfältige Weise charakterisieren. Zum Beispiel ist R ein Dedekindring genau dann, wenn in ihm die Teilerregel für Ideale gilt. Uns genügt das folgende hinreichende Kriterium, welches sich vergleichsweise einfach herleiten läßt.

Hauptsatz 5.9. *Sei R ein noetherscher Integritätsbereich, in dem jedes von Null verschiedene Primideal invertierbar ist. Dann folgt: R ist ein Dedekindring, und R erfüllt sowohl die Teiler- als auch die Kürzungsregel für Ideale.*

Beweis. Wir beweisen der Reihe nach die folgenden Aussagen:

- (1) Zu jedem $A \in \mathcal{J}(R)$ gibt es ein $m \in \mathbb{N}_0$ und Primideale $P_1, \dots, P_m \in \mathcal{P}(R)$ mit $A = P_1 \circ \dots \circ P_m$.
- (2) Eine solche Darstellung von A als Produkt von Primidealen ist in dem gewünschten Sinne eindeutig.
- (3) Jedes $A \in \mathcal{J}(R)$ ist invertierbar; insbesondere gilt in R die Kürzungsregel für Ideale.
- (4) In R gilt die Teilerregel für Ideale.

ad (1). Sei $\mathcal{M} := \{A \in \mathcal{J}(R) \mid \forall m \in \mathbb{N}_0 \forall P_1, \dots, P_m \in \mathcal{P}(R) : P_1 \circ \dots \circ P_m \neq A\}$. Zu zeigen ist: $\mathcal{M} = \emptyset$. Angenommen, \mathcal{M} ist nicht leer. Da R noethersch ist, besitzt \mathcal{M} ein bezüglich \subseteq maximales Element A . Offenbar gilt $A \neq R$. Also finden wir aufgrund von Lemma 5.1 ein maximales Ideal P_0 von R mit $A \subseteq P_0$. Dann ist $B := P_0^* \circ A \in \mathcal{J}(R)$ und $A \subseteq B$. Wir behaupten $A \neq B$. Tatsächlich ergäbe sich aus $A = B$ durch Multiplikation mit P_0 die Gleichung $P_0 \circ A = P_0 \circ P_0^* \circ A = A$ im Widerspruch zu Lemma 5.7. Also gilt $A \subsetneq B$ und damit $B \notin \mathcal{M}$. Wir finden $m \in \mathbb{N}_0$ und $P_1, \dots, P_m \in \mathcal{P}(R)$ mit $B = P_1 \circ \dots \circ P_m$. Daraus folgt $A = P_0 \circ B = P_0 \circ P_1 \circ \dots \circ P_m$ im Widerspruch zu $A \in \mathcal{M}$.

ad (2). Seien $m, n \in \mathbb{N}_0$ mit $m \leq n$ und $P_1, \dots, P_m, Q_1, \dots, Q_n \in \mathcal{P}(R)$ mit

$$(5.1) \quad P_1 \circ \dots \circ P_m = Q_1 \circ \dots \circ Q_n.$$

Wir argumentieren mittels Induktion nach m . Ist $m = 0$, so ist die linke Seite von (5.1) gleich R , und es folgt $n = 0$. Damit ist der Induktionsanfang gesichert. Sei nun $m \geq 1$. Ohne Beschränkung der Allgemeinheit dürfen wir annehmen, daß P_1 minimal bezüglich \subseteq unter den Idealen P_1, \dots, P_m ist. Da P_1 ein Primideal ist,

folgt aus $P_1 \supseteq Q_1 \circ \dots \circ Q_n$ nach Lemma 5.5 etwa $P_1 \supseteq Q_1$. Ähnlich erhalten wir $Q_1 \supseteq P_i$ für ein geeignetes $i \in \{1, \dots, m\}$. Also gilt $P_1 \supseteq Q_1 \supseteq P_i$. Aufgrund der Minimalität von P_1 folgt dann $P_1 = Q_1 = P_i$. Multipliziert man beide Seiten der Ausgangsgleichung (5.1) mit $P_1^* = Q_1^*$, so ergibt sich $P_2 \circ \dots \circ P_m = Q_2 \circ \dots \circ Q_n$. Nun greift die Induktionsvoraussetzung.

ad (3). Sei $A \in \mathcal{J}(R)$. Wir finden $m \in \mathbb{N}_0$ und $P_1, \dots, P_m \in \mathcal{P}(R)$ mit $A = P_1 \circ \dots \circ P_m$. Dann ist $P_1^* \circ \dots \circ P_m^* \subseteq A^*$, also $A \circ A^* = R$.

ad (4). Seien $A, B \in \mathcal{J}(R)$ mit $A \supseteq B$. Zu zeigen ist: $A \mid B$. Setze $C := A^* \circ B \in \mathcal{J}(R)$. Dann gilt $A \circ C = B$ wie gewünscht. \square

Korollar 5.10. *Jeder Hauptidealring ist ein Dedekindring.*

Beweis. Sei R ein Hauptidealring. Nach Lemma 5.2 ist R noethersch. Sei $P \in \mathcal{P}(R)$. Dann finden wir $p \in R \setminus \{0\}$ mit $P = pR$. Also gilt $p^{-1}R \subseteq P^*$ und somit $P \circ P^* = R$, d.h. P ist invertierbar. \square

Gleichbedeutend zu Korollar 5.10 ist die Aussage: Jedes Element eines Hauptidealringes läßt sich als Produkt von unzerlegbaren Elementen schreiben, wobei die Faktoren in einem solchen Produkt bis auf Assoziation und Reihenfolge eindeutig bestimmt sind.

Wichtige Beispiele für Hauptidealringe sind die sogenannten EUKLIDISCHEN RINGE. Unter diesen befindet sich etwa der Ring der ganzen GAUSSSchen Zahlen $\mathbb{Z}[i]$; siehe [5].

Aufgabe 5.11 (Fortsetzung von Aufgabe 2.5). Sei $R := \mathbb{Z}[\sqrt{-5}]$. Wir zeigen im nächsten Kapitel, daß R ein Dedekindring ist. Wie läßt sich die Gleichung $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ mit Hilfe der Idealtheorie deuten? Setze

$$P := 2R + (1 + \sqrt{-5})R, \quad Q_1 := 3R + (1 + \sqrt{-5})R, \quad Q_2 := 3R + (1 - \sqrt{-5})R$$

und zeige:

- (a) $P, Q_1, Q_2 \in \mathcal{P}(R)$,
- (b) $2R = P \circ P$ und $3R = Q_1 \circ Q_2$,
- (c) $(1 + \sqrt{-5})R = P \circ Q_1$ und $(1 - \sqrt{-5})R = P \circ Q_2$.

Also besitzt das Hauptideal $6R$ die Primfaktorzerlegung $6R = P \circ P \circ Q_1 \circ Q_2$. Unterschiedliches Zusammenfassen der Primfaktoren liefert nun tatsächlich

$$2R \circ 3R = (P \circ P) \circ (Q_1 \circ Q_2) = (P \circ Q_1) \circ (P \circ Q_2) = (1 + \sqrt{-5})R \circ (1 - \sqrt{-5})R.$$

KAPITEL 2

Quadratische Zahlkörper

Welche natürlichen Zahlen lassen sich als Summe von zwei Quadraten darstellen? Die Antwort zu diesem klassischen Problem kannte schon FERMAT: Eine natürliche Zahl n läßt sich genau dann als Summe von zwei Quadraten (ganzer Zahlen) schreiben, wenn der quadratfreie Rest von n keinen Primteiler p der Form $p \equiv_4 3$ besitzt.

Der entscheidende Schritt in dem Beweis dieses schönen Satzes besteht darin, zu zeigen, daß jede Primzahl p mit $p \equiv_4 1$ tatsächlich die Summe zweier Quadrate ist. Zu einer Erklärung dieses Sachverhalts kommt man auf die folgende natürliche Weise. Die Gleichung $p = x^2 + y^2$, über deren Lösbarkeit mittels ganzer Zahlen x, y zu befinden ist, vereinfacht sich, wenn wir vom Ring der ganzen Zahlen \mathbb{Z} zum Ring der sogenannten ganzen GAUSSSchen Zahlen $\mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i$ übergehen. Hier gilt nämlich $i^2 = -1$, und die ursprüngliche Gleichung ist äquivalent zu $p = (x + yi)(x - yi)$. Es ist dann zu überlegen, unter welchen Voraussetzungen und auf welche Art sich p in dem größeren Ring $\mathbb{Z}[i]$ faktorisieren läßt.

Zu einem ganz ähnlichen Ansatz führt das Studium der inzwischen weithin bekannten Schar von Gleichungen $x^n + y^n = z^n$, $n \in \mathbb{N}$. In den Fällen $n \in \{1, 2\}$ lassen sich viele ganzzahlige Lösungen direkt angeben; vgl. Arbeitsblatt 1. FERMAT vermutete, daß im Gegensatz dazu die Gleichung $x^n + y^n = z^n$ für $n \geq 3$ keine Lösungen $x, y, z \in \mathbb{Z} \setminus \{0\}$ zuläßt. Ein nicht elementarer Nachweis dieser Vermutung gelang vor etwa zehn Jahren dem Mathematiker WILES, der damit weltweit für Aufsehen sorgte. An dieser Stelle soll nur die folgende einfache Beobachtung festgehalten werden. Bezeichnet man mit $\mathbb{Z}[\zeta]$ den kleinsten Unterring von \mathbb{C} , der neben den ganzen Zahlen auch die primitive n -te Einheitswurzel $\zeta = \exp(2\pi i/n) \in \mathbb{C}$ enthält, so läßt sich die ursprüngliche Gleichung etwas zweckmäßiger in der Form $(z - x)(z - \zeta x) \cdots (z - \zeta^{n-1}x) = y^n$ schreiben. Es ist also zu überlegen, unter welchen Umständen sich die n -te Potenz einer ganzen Zahl y in dem Ring $\mathbb{Z}[\zeta]$ auf die angegebene Weise faktorisieren läßt. Insbesondere ist zu klären, ob in einem geeigneten Sinne eine eindeutige Primfaktorzerlegung in dem Ring $\mathbb{Z}[\zeta]$ möglich ist.

Die angeführten Ringe $\mathbb{Z}[i]$ und $\mathbb{Z}[\zeta]$ sind wichtige Beispiele für Ganzheitsringe algebraischer Zahlkörper. In diesem Kapitel beschränken wir uns auf die Untersuchung von Ganzheitsringen in quadratischen Zahlkörpern. Letztere stellen ein Verbindungsglied von der elementaren zur algebraischen Zahlentheorie dar.

1. Ganzheitsringe in quadratischen Zahlkörpern

Es sei \mathbb{C} der Körper der komplexen Zahlen. Bekanntlich gilt $\mathbb{C} = \mathbb{R}(i)$, wobei i eine Wurzel der Gleichung $X^2 + 1$ bezeichnet. Als \mathbb{R} -Vektorraum besitzt \mathbb{C} die Dimension zwei; es ist $\mathbb{C} = \mathbb{R} + \mathbb{R}i$. Der Betrag einer komplexen Zahl $z = x + yi$ (mit $x, y \in \mathbb{R}$) ist gegeben durch $|z| = \sqrt{x^2 + y^2}$.

MEMO. Sei R ein Unterring eines kommutativen Ringes K , und sei $a \in K$. Dann bezeichnet $R[a]$ den kleinsten Unterring von K , der sowohl R als auch a enthält. Ist K sogar ein Körper, so bezeichnet $R(a)$ den kleinsten Unterkörper von K , der sowohl R als auch a enthält.

Merke: Bekannterweise schreibt man $R[X]$ für den Polynomring über R . Der Ring $R[a]$ ist gerade das Bild des natürlichen Homomorphismus $\eta_a : R[X] \rightarrow K$, $f(X) \mapsto f(a)$, der durch Einsetzen von a gegeben ist. Ebenso erhält man den Körper $R(a)$ als Bild von $R(X)$, dem Ring der rationalen Funktionen über R .

Ist K ein Körper mit $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$, so können wir K als Vektorraum über \mathbb{Q} auffassen. Die Dimension des \mathbb{Q} -Vektorraums K heißt *Grad* von K über \mathbb{Q} und wird mit $[K : \mathbb{Q}]$ bezeichnet. Körper von endlichem Grad über \mathbb{Q} heißen *algebraische Zahlkörper*. Wir studieren im folgenden diejenigen Zahlkörper, die gewissermaßen am wenigsten von \mathbb{Q} abweichen.

Definition 1.1. Ein Körper K mit $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ und $[K : \mathbb{Q}] = 2$ heißt *quadratischer Zahlkörper*. Ist hierbei $K \subseteq \mathbb{R}$, so wird K genauer *reell-quadratisch*, andernfalls *imaginär-quadratisch* genannt.

Sei $x \in \mathbb{R}$. Für $x \geq 0$ ist \sqrt{x} üblicherweise definiert als die nicht-negative Quadratwurzel von x in \mathbb{R} . Für $x < 0$ setzen wir nun fest: $\sqrt{x} := i\sqrt{-x}$. Somit gilt in jedem Fall $(\sqrt{x})^2 = x$ und $\sqrt{x^2} = |x|$.

Eine ganze Zahl $d \in \mathbb{Z}$ heißt *quadratfrei*, falls d durch kein Quadrat n^2 einer ganzen Zahl $n \in \mathbb{Z} \setminus \{1, -1\}$ teilbar ist, d.h. falls $|d|$ Produkt von paarweise verschiedenen Primzahlen ist.

Lemma 1.2 (Quadratfreier Rest). *Zu jedem $a \in \mathbb{Q}^*$ gibt es genau eine quadratfreie Zahl $d \in \mathbb{Z}$ mit $a(\mathbb{Q}^*)^2 = d(\mathbb{Q}^*)^2$.*

Beweis. Sei $a \in \mathbb{Q}^*$. Wegen der eindeutigen Primfaktorzerlegung für ganze Zahlen, läßt sich a im wesentlichen eindeutig als Produkt von Primzahlpotenzen schreiben: Wir finden $v \in \{0, 1\}$, $m \in \mathbb{N}_0$, paarweise verschiedene $p_1, \dots, p_m \in \mathbb{P}$ und *ganzzahlige* Exponenten $e_1, \dots, e_m \in \mathbb{Z} \setminus \{0\}$, so daß $a = (-1)^v \cdot p_1^{e_1} \cdots p_m^{e_m}$. Offenbar ist $a \in (\mathbb{Q}^*)^2$ genau dann, wenn $v = 0$ und alle Exponenten e_1, \dots, e_m gerade sind.

Setze $d := (-1)^v \cdot p_1^{\bar{e}_1} \cdots p_m^{\bar{e}_m}$, wobei $\bar{e}_i \in \{0, 1\}$ für $i \in \{1, \dots, m\}$ jeweils durch die Kongruenzbedingung $e_i \equiv_2 \bar{e}_i$ festgelegt ist. Dann ist $d \in \mathbb{Z}$ offensichtlich quadratfrei und bestimmt dieselbe $(\mathbb{Q}^*)^2$ -Nebenklasse wie a . Zudem ist d als quadratfreier Vertreter eindeutig durch a bestimmt. \square

Satz 1.3 (Klassifikation der quadratischen Zahlkörper). *Die quadratischen Zahlkörper sind genau die Körper $\mathbb{Q}(\sqrt{d})$ mit $d \in \mathbb{Z} \setminus \{1\}$ quadratfrei.*

Beweis. Sei zunächst eine quadratfreie Zahl $d \in \mathbb{Z} \setminus \{1\}$ vorgegeben. Dann ist $\sqrt{d} \notin \mathbb{Q}$, und man rechnet nach, daß die Menge $\mathbb{Q} + \mathbb{Q}\sqrt{d}$ abgeschlossen bzgl. den Grundrechenarten ist. Also ist $\mathbb{Q}(\sqrt{d}) = \mathbb{Q} + \mathbb{Q}\sqrt{d}$ ein quadratischer Zahlkörper. Offenbar ist $\{x^2 \mid x \in \mathbb{Q}(\sqrt{d})^*\} \cap \mathbb{Q} = (\mathbb{Q}^*)^2 \cup d(\mathbb{Q}^*)^2$. Daher ist d nach Lemma 1.2 eindeutig durch $\mathbb{Q}(\sqrt{d})$ bestimmt.

Sei nun umgekehrt K ein quadratischer Zahlkörper. Wir finden $x \in K \setminus \mathbb{Q}$. Dann ist $K = \mathbb{Q} + \mathbb{Q}x$ und insbesondere $x^2 = b + 2ax$ mit $a, b \in \mathbb{Q}$. Setze $y := x - a \in K \setminus \mathbb{Q}$. Dann ist $y^2 = a^2 + b \in \mathbb{Q}^*$. Nach Lemma 1.2 finden wir $d \in \mathbb{Z}$ quadratfrei mit $(a^2 + b)(\mathbb{Q}^*)^2 = d(\mathbb{Q}^*)^2$. Dann ist $K = \mathbb{Q}(x) = \mathbb{Q}(y) = \mathbb{Q}(\sqrt{a^2 + b}) = \mathbb{Q}(\sqrt{d})$, und insbesondere gilt dabei $d \neq 1$. \square

Im folgenden bezeichne $d \in \mathbb{Z} \setminus \{1\}$ eine quadratfreie Zahl und $K = \mathbb{Q}(\sqrt{d}) = \mathbb{Q} + \mathbb{Q}\sqrt{d}$ den zugehörigen quadratischen Zahlkörper. Zudem stehe σ stets für den nicht-identischen Automorphismus von K , der durch den nachstehenden Satz ausgezeichnet wird.

Satz 1.4. *Die Abbildung $\sigma : K \rightarrow K, a + b\sqrt{d} \mapsto a - b\sqrt{d}$ liefert einen nicht-identischen Automorphismus des Körpers K . Außer der Identität und σ besitzt K keine weiteren Automorphismen: $\text{Aut}(K) = \{\text{id}_K, \sigma\}$.*

Beweis. Es gilt $K = \mathbb{Q}(\sqrt{d}) \cong \mathbb{Q}[X]/(X^2 - d)\mathbb{Q}[X]$. Offenbar bildet der Ringautomorphismus $\mathbb{Q}[X] \rightarrow \mathbb{Q}[X], f(X) \mapsto f(-X)$ das Ideal $(X^2 - d)\mathbb{Q}[X]$ in sich ab und induziert somit einen nicht-identischen Automorphismus σ von K .

Ist nun $\tau \in \text{Aut}(K)$ vorgegeben, so bildet τ notwendigerweise jede rationale Zahl auf sich selbst ab, und daher gilt $d = d^\sigma = ((\sqrt{d})^\sigma)^\sigma = ((\sqrt{d})^\sigma)^2$, also $(\sqrt{d})^\sigma \in \{\sqrt{d}, -\sqrt{d}\}$. Wegen $K = \mathbb{Q}(\sqrt{d})$ folgt $\tau \in \{\text{id}_K, \sigma\}$. \square

Definition 1.5. Sei $x = a + b\sqrt{d} \in K$ (mit $a, b \in \mathbb{Q}$). Die Größen $\text{Sp}(x) := \text{Sp}_{K|\mathbb{Q}}(x) := x + x^\sigma = 2a$ und $\text{N}(x) := \text{N}_{K|\mathbb{Q}} := xx^\sigma = a^2 - b^2d$ heißen *Spur* bzw. *Norm* von x (bezüglich der Körpererweiterung $K|\mathbb{Q}$).

Lemma 1.6. *Die Spur ist eine lineare Abbildung des \mathbb{Q} -Vektorraums K auf den ein-dimensionalen \mathbb{Q} -Vektorraum \mathbb{Q} .*

Die Norm induziert einen Gruppenhomomorphismus von K^ nach \mathbb{Q}^* .*

Beweis. Seien $x, y \in K$ und $a \in \mathbb{Q}$. Dann gilt

$$\begin{aligned} \text{Sp}(ax + y) &= (ax + y) + (ax + y)^\sigma = ax + a^\sigma x^\sigma + y + y^\sigma \\ &= a(x + x^\sigma) + (y + y^\sigma) = a \text{Sp}(x) + \text{Sp}(y). \end{aligned}$$

Damit ist die Spur eine \mathbb{Q} -lineare Abbildung, die wegen $\text{Sp}(a/2) = a$ nicht die Nullabbildung ist. Des weiteren gilt

$$\text{N}(xy) = (xy)(xy)^\sigma = xyx^\sigma y^\sigma = (xx^\sigma)(yy^\sigma) = \text{N}(x)\text{N}(y),$$

womit schon alles gezeigt ist. \square

Lemma 1.7. *Sei $x \in K$. Dann ist die Abbildung $\mu_x : K \rightarrow K, y \mapsto yx$ ein Endomorphismus des \mathbb{Q} -Vektorraumes K . Die Spur und die Determinante von μ_x sind gerade $\text{Sp}(x)$ und $\text{N}(x)$. Es gilt $x^2 - \text{Sp}(x)x + \text{N}(x) = 0$.*

Beweis. Offenbar ist die Rechtsmultiplikation μ_x mit x eine \mathbb{Q} -lineare Abbildung. Wegen $K = \mathbb{Q} + \mathbb{Q}\sqrt{d}$ finden wir $a, b \in \mathbb{Q}$ mit $x = a + b\sqrt{d}$. Die Matrix von $\mu_x : K \rightarrow K$ bzgl. der \mathbb{Q} -Basis $(1, \sqrt{d})$ ist dann

$$M_x := \begin{pmatrix} a & b \\ bd & a \end{pmatrix},$$

und sie hat tatsächlich die Spur $2a = \text{Sp}(x)$ und die Determinante $a^2 - b^2d = \text{N}(x)$.

Die angegebene quadratische Gleichung für x folgt aus dem bekannten Satz von Cayley-Hamilton durch Übergang von μ_x zu x . Oder man rechnet sie direkt nach: $x^2 - \text{Sp}(x)x + \text{N}(x) = x^2 - (x + x^\sigma)x + (xx^\sigma) = 0$. \square

Definition 1.8. Ein Element $x \in K$ heißt *ganz*, falls $\text{Sp}(x) \in \mathbb{Z}$ und $\text{N}(x) \in \mathbb{Z}$. Die Menge aller ganzen Zahlen in K wird mit $\mathcal{O} := \mathcal{O}_K$ bezeichnet.

Man überlegt sich leicht, daß $\mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$ ist. In diesem Sinne stellt \mathcal{O} eine Verallgemeinerung der gewöhnlichen ganzen Zahlen dar. Als nächstes geht es darum, zu zeigen, daß \mathcal{O} ein Unterring von K mit interessanten arithmetischen Eigenschaften ist. – Schließlich wollen wir Zahlentheorie betreiben!

Wir setzen

$$\omega := \begin{cases} (1 + \sqrt{d})/2 & \text{falls } d \equiv_4 1, \\ \sqrt{d} & \text{falls } d \not\equiv_4 1. \end{cases}$$

Lemma 1.9. *Es gilt $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\omega = \{a + b\omega \mid a, b \in \mathbb{Z}\}$.*

Beweis. Sei $x = a + b\sqrt{d} \in K$ (wobei $a, b \in \mathbb{Q}$). Nach Definition ist $x \in \mathcal{O}$ gleichbedeutend mit

$$2a = \text{Sp}(x) \in \mathbb{Z} \quad \text{und} \quad a^2 - b^2d = \text{N}(x) \in \mathbb{Z}.$$

Dies motiviert uns dazu, $a = \tilde{a}/2$ und $b = \tilde{b}/2$ zu schreiben. Dann ist $x \in \mathcal{O}$ äquivalent zu

$$\tilde{a} \in \mathbb{Z} \quad \text{und} \quad (\tilde{a}^2 - \tilde{b}^2d)/4 \in \mathbb{Z},$$

also äquivalent zu

$$\tilde{a}, \tilde{b} \in \mathbb{Z} \text{ mit } \tilde{a}^2 - \tilde{b}^2d \equiv_4 0.$$

Merke, daß das Quadrat einer ganzen Zahl stets kongruent zu 0 oder 1 modulo 4 ist, und zwar je nachdem, ob diese Zahl gerade oder ungerade ist. Für $d \equiv_4 1$ gilt daher $x \in \mathcal{O}$ genau dann, wenn $\tilde{a}, \tilde{b} \in \mathbb{Z}$ entweder beide gerade oder beide ungerade sind. Für $d \not\equiv_4 1$ ist $x \in \mathcal{O}$ gleichbedeutend mit $\tilde{a}, \tilde{b} \in 2\mathbb{Z}$. Daraus ergibt sich die Behauptung. \square

Satz 1.10 (Struktur des Ganzheitsringes). *Es gilt $\mathcal{O} = \mathbb{Z}[\omega] = \mathbb{Z} + \mathbb{Z}\omega$. Somit bildet \mathcal{O} einen Integritätsbereich, dessen Quotientenkörper (innerhalb von K) gleich K ist. Jedes Ideal von \mathcal{O} läßt sich von zwei Elementen erzeugen; insbesondere ist \mathcal{O} noethersch. Die Einschränkung $\sigma|_{\mathcal{O}}$ des nicht-identischen Automorphismus von K auf \mathcal{O} liefert einen Ringautomorphismus.*

Beweis. Zunächst rechnen wir nach, daß $\mathcal{O} = \mathbb{Z}[\omega]$ ist. Nach Lemma 1.9 genügt es, nachzuweisen, daß die Menge $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\omega$ einen Unterring von K bildet. Nicht offensichtlich ist dabei nur die Abgeschlossenheit unter Multiplikation. Konkret ist zu zeigen: $\omega^2 \in \mathcal{O}$.

Ist $d \not\equiv_4 1$, so folgt unmittelbar $\omega^2 = d \in \mathcal{O}$. Ist $d \equiv_4 1$, so gilt $(2\omega - 1)^2 = d$, also $4\omega^2 - 4\omega + 1 = d$, also $\omega^2 = \omega + (d - 1)/4 \in \mathcal{O}$. Damit ist $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\omega = \mathbb{Z}[\omega]$ ein Unterring von K .

Als Unterring eines Körpers, der die 1 enthält, ist \mathcal{O} selbstverständlich ein Integritätsbereich. Offenbar ist $K = \mathbb{Q}(\omega)$ der Quotientenkörper von $\mathcal{O} = \mathbb{Z}[\omega]$. Für alle $x \in K$ gilt per Definition $x \in \mathcal{O}$ genau dann, wenn $x^\sigma \in \mathcal{O}$. Damit ist klar, daß σ einen Ringautomorphismus von \mathcal{O} induziert.

Zu zeigen bleibt nur noch: Jedes Ideal von \mathcal{O} läßt sich von zwei Elementen erzeugen. Es gilt sogar: Jede additive Untergruppe von $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\omega$ läßt sich von zwei Elementen erzeugen. Sei nämlich U eine additive Untergruppe von $\mathbb{Z} + \mathbb{Z}\omega$. Dann sind $A := \{a \in \mathbb{Z} \mid \exists b \in \mathbb{Z} : a + b\omega \in U\}$ und $B := \{b \in \mathbb{Z} \mid b\omega \in U\}$ additive Untergruppen von \mathbb{Z} , nach Satz 3.8 also von der Gestalt $A = a\mathbb{Z}$ und $B = b\mathbb{Z}$. Wähle $c \in \mathbb{Z}$ mit $a + c\omega \in U$. Eine einfache Rechnung zeigt: $U = (a + c\omega)\mathbb{Z} + b\omega\mathbb{Z}$. \square

Der Ring \mathcal{O} heißt *Ganzheitsring* (auch *Hauptordnung* – daher der Buchstabe \mathcal{O}) des quadratischen Zahlkörpers K . Allgemeinere Ordnungen werden auf Arbeitsblatt 5 studiert.

2. Einheiten in Ganzheitsringen quadratischer Zahlkörper

Im folgenden bezeichne wieder $d \in \mathbb{Z} \setminus \{1\}$ eine quadratfreie Zahl, $K = \mathbb{Q}(\sqrt{d})$ den zugehörigen quadratischen Zahlkörper und \mathcal{O} den Ganzheitsring von K .

Die Einheitengruppe $\mathbb{Z}^* = \{1, -1\}$ des Ringes \mathbb{Z} der ganzen Zahlen ist zyklisch der Ordnung zwei und damit denkbar klein. Die Beschreibung der Einheitengruppe \mathcal{O}^* des Ganzheitsringes \mathcal{O} hängt stark davon ab, ob K imaginär- oder reell-quadratisch ist.

MEMO. Sei G eine Gruppe und $S \subseteq G$ eine beliebige Teilmenge von G . Der Durchschnitt $\langle S \rangle := \bigcap \{U \leq S \subseteq U\}$ aller Untergruppen von G , die S enthalten, ist selbst eine Untergruppe von G und heißt die *von S erzeugte Untergruppe*. Ist $S = \{s_1, \dots, s_m\}$, so schreibt man auch $\langle s_1, \dots, s_m \rangle := \langle S \rangle$. Läßt sich G von einem einzigen Element erzeugen, so heißt G *zyklisch*.

Man überlegt leicht, daß jede zyklische Gruppe homomorphes Bild der unendlichen zyklischen Gruppe $\mathbb{Z} = (\mathbb{Z}, +)$ ist: Die zyklischen Gruppen sind bis auf Isomorphie genau die Gruppen $\mathbb{Z}/n\mathbb{Z} = (\mathbb{Z}/n\mathbb{Z}, +)$ mit $n \in \mathbb{N}_0$. Insbesondere ist nicht nur jeder Quotient sondern auch jede Untergruppe einer zyklischen Gruppe wiederum zyklisch; siehe Satz 3.8 in Kapitel 1.

Lemma 2.1. Sei $x \in \mathcal{O}$. Dann gilt $x \in \mathcal{O}^*$ genau dann, wenn $N(x) \in \{1, -1\}$ ist.

Beweis. Sei zuerst $x \in \mathcal{O}^*$. Dann ist $y := x^{-1} \in \mathcal{O}$ und $1 = N(1) = N(xy) = N(x)N(y)$. Daraus folgt $N(x) \in \mathbb{Z}^* = \{1, -1\}$.

Sei nun $N(x) \in \{1, -1\}$ vorausgesetzt. Dann ist $y := N(x)x^\sigma \in \mathcal{O}$ und $xy = N(x)xx^\sigma = N(x)^2 = 1$. Somit gilt $x \in \mathcal{O}^*$. \square

Satz 2.2 (Einheitengruppe \mathcal{O}^* für imaginär-quadratische Zahlkörper). Sei $d < 0$. Dann gilt:

$$\mathcal{O}^* = \begin{cases} \{1, i, -1, -i\} \cong \mathbb{Z}/4\mathbb{Z} & \text{falls } d = -1, \\ \{1, \frac{1+\sqrt{-3}}{2}, \frac{-1+\sqrt{-3}}{2}, -1, \frac{-1-\sqrt{-3}}{2}, \frac{1-\sqrt{-3}}{2}\} \cong \mathbb{Z}/6\mathbb{Z} & \text{falls } d = -3, \\ \{1, -1\} \cong \mathbb{Z}/2\mathbb{Z} & \text{sonst.} \end{cases}$$

Beweis. Sei $x \in \mathcal{O}$. Nach Lemma 2.1 ist $x \in \mathcal{O}^*$ gleichbedeutend mit $|N(x)| = 1$.

Wir betrachten zunächst den Fall $d \equiv_4 1$. Dann ist $x = (a + b\sqrt{d})/2 \in \mathcal{O}$, wobei $a, b \in \mathbb{Z}$ der Bedingung $a \equiv_2 b$ genügen. Es gilt $N(x) = (a^2 - b^2d)/4$. Wegen $d < 0$ ist der letzte Ausdruck nicht-negativ und nur in endlich vielen Fällen gleich 1, nämlich für $(a, b) \in \{(2, 0), (-2, 0)\}$ und, falls $d = -3$, zusätzlich für $(a, b) \in \{(1, 1), (-1, 1), (-1, -1), (1, -1)\}$. Diese Werte liefern die angegebenen Einheiten.

Sei nun $d \not\equiv_4 1$. Dann ist $x = a + b\sqrt{d}$ mit $a, b \in \mathbb{Z}$, und es gilt $N(x) = a^2 - b^2d$. Wegen $d < 0$ ist der letzte Ausdruck wieder nicht-negativ und nur in endlich vielen Fällen gleich 1, nämlich für $(a, b) \in \{(1, 0), (-1, 0)\}$ und, falls $d = -1$, zusätzlich für $(a, b) \in \{(0, 1), (0, -1)\}$. Wieder erhalten wir die angegebenen Einheiten. \square

Die Beschreibung der Einheitengruppe eines reell-quadratischen Zahlkörpers ist etwas aufwendiger. Bemerkenswert ist, daß dabei mehrfach das einfache Schubfachprinzip eine entscheidende Rolle spielt.

Dirichletsches Schubfachprinzip. Sind M, N Mengen mit $\#M > \#N$, so gibt es keine injektive Abbildung $M \rightarrow N$.

Anschaulich bedeutet dies zum Beispiel: In jeder Millionenstadt gibt es mindestens zwei Personen, die exakt die gleiche Anzahl von Haaren auf dem Kopf tragen. Denn typischerweise hat jeder Mensch weniger als eine Million Haare.

Lemma 2.3. Sei $c \in \mathbb{R}_{>0}$, und bezeichne mit σ den nicht-identischen Automorphismus von K . Dann ist $\{x \in \mathcal{O} \mid |x| < c \text{ und } |x^\sigma| < c\}$ endlich.

Beweis. Setze $\tilde{c} := \max\{2c, c^2\}$. Dann sind $\mathcal{F} := \{f_0 + f_1X + X^2 \in \mathbb{Z}[X] \mid |f_0| \leq \tilde{c} \text{ und } |f_1| \leq \tilde{c}\}$ und folglich $\mathcal{W} := \{w \in \mathbb{C} \mid \exists f \in \mathcal{F} : f(w) = 0\}$ endlich. Ist $x \in \mathcal{O}$ mit $|x| < c$ und $|x^\sigma| < c$, so folgt $f := N(x) - \text{Sp}(x)X + X^2 \in \mathcal{F}$. Nach Lemma 1.7 haben wir $f(x) = 0$, also $x \in \mathcal{W}$. \square

Lemma 2.4. Sei $x \in \mathbb{R}_{>0}$ irrational und $m \in \mathbb{N}$. Dann gibt es ganze Zahlen a, b mit $(a, b) \neq (0, 0)$, $|a| \leq m$, $|b| \leq m$ und $|a + bx| \leq (1 + x)/m$.

Beweis. Setze $M := \{a + bx \mid a, b \in \mathbb{Z} \text{ mit } 0 \leq a, b \leq m\}$. Da x irrational ist, sind 1 und x linear unabhängig über \mathbb{Q} , also enthält M wirklich $(m+1)^2$ verschiedene Elemente. Weiterhin gilt für alle $y \in M$ die Abschätzung $0 \leq y \leq m(1+x)$. Wir denken uns das reelle Intervall $[0, m(1+x)]$ als Vereinigung von m^2 Intervallen der Länge $L := (1+x)/m$:

$$[0, m(1+x)] = [0, L] \cup [L, 2L] \cup \dots \cup [(m^2-1)L, m^2L].$$

Nach dem Schubfachprinzip finden wir $a_1 + b_1x, a_2 + b_2x \in M$ und $j \in \{0, \dots, m^2-1\}$, so daß

$$jL \leq a_1 + b_1x < a_2 + b_2x \leq (j+1)L.$$

Setze nun $a := a_2 - a_1$ und $b := b_2 - b_1$. Dann gelten $(a, b) \neq (0, 0)$, $|a| \leq m$, $|b| \leq m$ und $0 \leq a + bx \leq (1+x)/m$, wie gewünscht. \square

MEMO. Die *Ordnung* einer Gruppe G ist die Anzahl $|G|$ der Elemente von G . Die *Ordnung eines Elements* $g \in G$ ist definiert als $\text{ord}(g) := |\langle g \rangle|$. Elemente endlicher Ordnung heißen *Torsionselemente*. Ist G abelsch, so sieht man leicht, daß die Torsionselemente eine Untergruppe, die sogenannte *Torsionsuntergruppe* von G , bilden.

Hauptsatz 2.5 (Einheitengruppe \mathcal{O}^* für reell-quadratische Zahlkörper). Es sei $d > 0$. Dann ist $\mathcal{O}^* = \{1, -1\} \times Z$, wobei Z eine unendliche zyklische Gruppe ist.

Beweis. Wegen $\mathcal{O}^* \subseteq \mathbb{R}^*$ sind die Torsionselemente von \mathcal{O}^* , d.h. die Elemente endlicher Ordnung in \mathcal{O} , genau 1 und -1 .

Da $\sqrt{d} \in \mathbb{R}$ irrational ist, zeigt Lemma 2.4, daß die endliche Menge $\mathcal{S}_m := \{a + b\sqrt{d} \in \mathbb{Z} + \mathbb{Z}\sqrt{d} \mid (a, b) \neq (0, 0), |a| \leq m, |b| \leq m, |a + b\sqrt{d}| \leq (1 + \sqrt{d})/m\}$ für kein $m \in \mathbb{N}$ leer ist. Als nächstes beweisen wir, daß die Menge

$$\mathcal{S} := \bigcup \{\mathcal{S}_m \mid m \in \mathbb{N}\}$$

unendlich ist. Wegen $0 \notin \mathcal{S}$ genügt es, zu zeigen, daß \mathcal{S} dem Betrage nach beliebig kleine Elemente enthält. Ist $\varepsilon \in \mathbb{R}_{>0}$ vorgegeben, wähle $m \in \mathbb{N}$ mit $(1 + \sqrt{d})/m < \varepsilon$. Dann finden wir in der Tat $a + b\sqrt{d} \in \mathcal{S}_m \subseteq \mathcal{S}$ mit $|a + b\sqrt{d}| \leq (1 + \sqrt{d})/m < \varepsilon$. Also ist die Menge \mathcal{S} unendlich.

Für $m \in \mathbb{N}$ definieren wir

$$\begin{aligned}\mathcal{S}_m^+ &:= \{a + b\sqrt{d} \in \mathcal{S}_m \mid a > 0\} \\ \mathcal{S}_m^0 &:= \{a + b\sqrt{d} \in \mathcal{S}_m \mid a = 0\}.\end{aligned}$$

Wegen $\sqrt{d} > 1$ sind $\mathcal{S}_1^0 = \{\sqrt{d}, -\sqrt{d}\}$ und $\mathcal{S}_m^0 = \emptyset$ für $m \geq 2$. Weiterhin ist für alle $m \in \mathbb{N}$ und $a + b\sqrt{d} \in \mathcal{S}_m$ auch $-a - b\sqrt{d} \in \mathcal{S}_m$. Somit ist mit \mathcal{S} auch die Menge

$$\mathcal{S}^+ := \bigcup \{\mathcal{S}_m^+ \mid m \in \mathbb{N}\} = \{a + b\sqrt{d} \in \mathcal{S} \mid a > 0\}$$

unendlich. Als nächstes zeigen wir, daß für alle $x \in \mathcal{S}^+$ gilt

$$0 < |N(x)| \leq (1 + \sqrt{d})^2.$$

Seien dazu $m \in \mathbb{N}$ und $x = a + b\sqrt{d} \in \mathcal{S}_m^+$ vorgegeben. Dann gelten die Abschätzungen $|a + b\sqrt{d}| \leq (1 + \sqrt{d})/m$ und $|a|, |b| \leq m$, also $|a - b\sqrt{d}| \leq m(1 + \sqrt{d})$. Daraus folgt tatsächlich $0 < |N(x)| = |(a + b\sqrt{d})(a - b\sqrt{d})| \leq (1 + \sqrt{d})^2$.

Per Definition ist $N(x)$ für alle $x \in \mathcal{S}^+$ ganzzahlig. Es folgt, daß $\{N(x) \mid x \in \mathcal{S}^+\}$ endlich ist. Nach dem Schubfachprinzip finden wir $n \in \mathbb{Z} \setminus \{0\}$ mit $|n| \leq (1 + \sqrt{d})^2$, so daß die Menge

$$\mathcal{S}^* := \{x \in \mathcal{S}^+ \mid N(x) = n\}$$

unendlich ist. Wir definieren auf \mathcal{S}^* eine Äquivalenzrelation, indem wir für $a_1 + b_1\sqrt{d}, a_2 + b_2\sqrt{d} \in \mathcal{S}^*$ festlegen:

$$a_1 + b_1\sqrt{d} \sim a_2 + b_2\sqrt{d}, \quad \text{falls } a_1 \equiv_n a_2 \text{ und } b_1 \equiv_n b_2.$$

Auf diese Weise zerfällt die unendliche Menge \mathcal{S}^* in höchstens n^2 Äquivalenzklassen. Daher finden wir $x_1 = a_1 + b_1\sqrt{d}, x_2 = a_2 + b_2\sqrt{d} \in \mathcal{S}^*$ mit $x_1 \neq x_2$, aber $x_1 \sim x_2$. Für $y := x_1/x_2 \in K$ ist dann $N(y) = N(x_1)/N(x_2) = 1$. Wegen $x_1 \neq x_2$ ist $y \neq 1$; wegen $a_1, a_2 > 0$ ist $x_1 \neq -x_2$, also $y \neq -1$. Entscheidend ist nun, daß $y \in \mathcal{O}$ liegt. Bezeichne mit σ den nicht-identischen Automorphismus von K . Dann gilt in der Tat

$$\begin{aligned}y &= \frac{x_1}{x_2} = 1 + \frac{x_1 - x_2}{x_2} = 1 + \frac{(x_1 - x_2)x_2^\sigma}{N(x_2)} = 1 + \frac{x_1 - x_2}{n} x_2^\sigma \\ &= 1 + \left(\frac{a_1 - a_2}{n} + \frac{b_1 - b_2}{n} \sqrt{d} \right) x_2^\sigma \in \mathbb{Z} + \mathbb{Z}\sqrt{d} \subseteq \mathcal{O}.\end{aligned}$$

Somit haben wir in $y \in \mathcal{O}^* \setminus \{1, -1\}$ eine Einheit unendlicher Ordnung gefunden.

Wegen $y \in \mathbb{R}^* \setminus \{1, -1\}$ gilt $\max\{y, -y, y^{-1}, -y^{-1}\} > 1$. Somit ist $Z_0 := \{u \in \mathcal{O}^* \mid u > 1\} \neq \emptyset$. Als nächstes zeigen wir, daß Z_0 ein kleinstes Element besitzt. Wähle $w \in Z_0$ und setze $U := \{u \in Z_0 \mid u < w\}$. Für $u \in U$ folgt aus $|uu^\sigma| = N(u) = 1$ dann $|u^\sigma| = u^{-1} < 1 < w$. Nach Lemma 2.3 ist daher U endlich, und somit ist $z := \min U$ zugleich das kleinste Element von Z_0 .

Setze $Z := \langle z \rangle$. Dann ist Z eine unendliche zyklische Gruppe, insbesondere $\{1, -1\} \cap Z = \{1\}$. Es bleibt zu zeigen, daß das direkte Produkt $\{1, -1\} \times Z$ ganz \mathcal{O}^* ausmacht. Sei also $u \in \mathcal{O}^*$. Nach Multiplikation mit -1 , falls erforderlich, dürfen wir annehmen, daß $u > 0$ ist. Dann finden wir $m \in \mathbb{Z}$ mit $z^m \leq u < z^{m+1}$. Daraus folgt $1 \leq u/z^m < z$, und mit der Definition von z dann $u = z^m \in Z$. \square

Der Beweis des vorstehenden Satzes zeigt: $\mathcal{O}^* = \{1, -1\} \times \langle z \rangle$ mit $z := \min\{u \in \mathcal{O}^* \mid u > 1\}$. Das erzeugende Element z heißt *Grundeinheit*. Im allgemeinen ist es nicht ganz einfach, die Grundeinheit zu einem vorgegebenen quadratischen Zahlkörper

zu bestimmen. Überlegungen in dieser Richtung führen zu der sogenannten Kettenbruchentwicklung einer reellen Zahl und finden sich häufig unter dem Stichwort „PELLEsche Gleichung“; siehe [5].

Beispiel 2.6. (a) Die Grundeinheit zu $K = \mathbb{Q}(\sqrt{2})$ ist $1 + \sqrt{2}$. Denn für $y = a + b\sqrt{2} \in \mathcal{O}^* \setminus \{1, -1\}$ ist genau ein Element der Menge $\{y, -y, y^{-1}, -y^{-1}\} = \{y, -y, y^\sigma, -y^\sigma\} = \{a + b\sqrt{2}, a - b\sqrt{2}, -a + b\sqrt{2}, -a - b\sqrt{2}\}$ größer als 1. Also befindet sich die Grundeinheit in der Menge $\mathbb{N}_0 + \mathbb{N}_0\sqrt{2}$, und es folgt $\min\{u \in \mathcal{O}^* \mid u > 1\} = 1 + \sqrt{2}$.

(b) Ähnlich sieht man, daß die Grundeinheit für $K = \mathbb{Q}(\sqrt{5})$ durch die *goldene Schnitzzahl* $\frac{1+\sqrt{5}}{2}$ gegeben ist; vgl. Arbeitsblatt 8.

3. Primfaktorzerlegung in Ganzheitsringen quadratischer Zahlkörper

Im folgenden bezeichne wieder $d \in \mathbb{Z} \setminus \{1\}$ eine quadratfreie Zahl, $K = \mathbb{Q}(\sqrt{d})$ den zugehörigen quadratischen Zahlkörper und \mathcal{O} den Ganzheitsring in K . Es bezeichne σ den nicht-identischen Automorphismus des Körpers K .

Als erstes zeigen wir, daß \mathcal{O} ein Dedekindring ist, d.h. daß es in \mathcal{O} eine eindeutige Primfaktorzerlegung für Ideale gibt; vgl. Abschnitt 5 in Kapitel 1.

Wir erinnern an die Notation

$$\mathcal{J}(\mathcal{O}) = \{I \mid I \neq 0 \text{ ein Ideal von } \mathcal{O}\}, \quad \mathcal{P}(\mathcal{O}) = \{P \mid P \neq 0 \text{ ein Primideal von } \mathcal{O}\}.$$

MEMO. Sei $r \in \mathbb{N}$, und seien $a_1, \dots, a_r \in \mathbb{Z}$. Da \mathbb{Z} ein Hauptidealring ist, existiert $b \in \mathbb{N}_0$ mit $a_1\mathbb{Z} + \dots + a_r\mathbb{Z} = b\mathbb{Z}$. Die Zahl b ist wohlbestimmt und heißt *größter gemeinsamer Teiler* von a_1, \dots, a_r , in Zeichen $b = \text{ggT}(a_1, \dots, a_r)$. Ein effektives Verfahren zur Bestimmung des größten gemeinsamen Teilers zweier ganzer Zahlen liefert der bekannte EUKLIDISCHE Algorithmus.

Das *kleinste gemeinsame Vielfache* $\text{kgV}(a_1, \dots, a_r)$ von a_1, \dots, a_r ist diejenige Zahl $c \in \mathbb{N}_0$, für die gilt: $a_1\mathbb{Z} \cap \dots \cap a_r\mathbb{Z} = c\mathbb{Z}$.

Lemma 3.1. Sei $A \in \mathcal{J}(\mathcal{O})$. Dann ist $A^\sigma = \{\alpha^\sigma \mid \alpha \in A\} \in \mathcal{J}(\mathcal{O})$, und es existiert ein $a \in \mathbb{N}$ mit $A \circ A^\sigma = a\mathcal{O}$.

Beweis. Nach Satz 1.10 ist $\sigma|_{\mathcal{O}}$ ein Ringautomorphismus. Also ist $A^\sigma \in \mathcal{J}(\mathcal{O})$. Des weiteren finden wir nach Satz 1.10 Erzeuger $\alpha, \beta \in \mathcal{O}$ für das Ideal A . Offenbar folgt aus $A = \alpha\mathcal{O} + \beta\mathcal{O}$ unmittelbar $A^\sigma = \alpha^\sigma\mathcal{O} + \beta^\sigma\mathcal{O}$. Daher gilt

$$A \circ A^\sigma = \alpha\alpha^\sigma\mathcal{O} + \alpha\beta^\sigma\mathcal{O} + \alpha^\sigma\beta\mathcal{O} + \beta\beta^\sigma\mathcal{O}.$$

Hierbei sind $\alpha\alpha^\sigma = N(\alpha), \beta\beta^\sigma = N(\beta) \in \mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$, und ebenso ist $\alpha\beta^\sigma + \alpha^\sigma\beta = \text{Sp}(\alpha\beta^\sigma) \in \mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$. Setze $a := \text{ggT}(\alpha\alpha^\sigma, \beta\beta^\sigma, \alpha\beta^\sigma + \alpha^\sigma\beta) \in \mathbb{N}$.

Wir behaupten $A \circ A^\sigma = a\mathcal{O}$. Die Inklusion „ \supseteq “ ist klar, denn a ist per Definition Linearkombination von $\alpha\alpha^\sigma, \beta\beta^\sigma, \alpha\beta^\sigma + \alpha^\sigma\beta \in A \circ A^\sigma$ mit Koeffizienten in \mathbb{Z} . Nun steht nur noch der Nachweis der entgegengesetzten Inklusion „ \subseteq “ aus. Offenbar sind $\alpha\alpha^\sigma, \beta\beta^\sigma \in a\mathcal{O}$. Zu zeigen bleibt: $\alpha\beta^\sigma, \alpha^\sigma\beta \in a\mathcal{O}$, äquivalent dazu: $x := \alpha\beta^\sigma/a$ und $x^\sigma = \alpha^\sigma\beta/a$ liegen in \mathcal{O} . Dazu berechnen wir die Spur und die Norm:

$$\text{Sp}(x) = \text{Sp}(x^\sigma) = x + x^\sigma = (\alpha\beta^\sigma + \alpha^\sigma\beta)/a \in \mathbb{Z},$$

$$N(x) = N(x^\sigma) = xx^\sigma = (\alpha\alpha^\sigma)/a \cdot (\beta\beta^\sigma)/a \in \mathbb{Z}.$$

Also sind $x, x^\sigma \in \mathcal{O}$ wie gewünscht. □

Für $A \in \mathcal{J}(\mathcal{O})$ ist $A^* = \{x \in K \mid xA \subseteq \mathcal{O}\}$ gemäß Definition 5.6.

Lemma 3.2. *Jedes von Null verschiedene Ideal von \mathcal{O} ist invertierbar, d.h. für jedes $A \in \mathcal{J}(\mathcal{O})$ gilt: $A \circ A^* = \mathcal{O}$.*

Beweis. Sei $A \in \mathcal{J}(\mathcal{O})$. Nach Lemma 3.1 ist $A \circ A^\sigma = a\mathcal{O}$ mit $a \in \mathbb{N}$, also $A^* = a^{-1}A^\sigma$ und $A \circ A^* = \mathcal{O}$. \square

Hauptsatz 3.3. *Der Ganzheitsring \mathcal{O} eines quadratischen Zahlkörpers ist ein Dedekindring und erfüllt die Teilerregel für Ideale:*

Jedes Ideal $A \in \mathcal{J}(\mathcal{O})$ läßt sich im wesentlichen eindeutig als Produkt von Primidealen schreiben, und für alle $A, B \in \mathcal{J}(\mathcal{O})$ gilt $A \mid B$ genau dann, wenn $A \supseteq B$.

Beweis. Dies folgt aus Hauptsatz 5.9 in Kapitel 1, Satz 1.10 und Lemma 3.2. \square

Nachdem wir nun wissen, daß sich die Ideale von \mathcal{O} eindeutig in Primfaktoren zerlegen lassen, liegt es nahe, die Menge der Primideale $\mathcal{P}(\mathcal{O})$ näher zu bestimmen. Das folgende Lemma zeigt, daß es dazu zweckmäßig ist, das Zerlegungsverhalten von Idealen der Form $p\mathcal{O}$, $p \in \mathbb{P}$, zu untersuchen.

Lemma 3.4. *Sei $P \in \mathcal{P}(\mathcal{O})$. Dann gibt es genau eine Primzahl $p \in \mathbb{P}$ mit $p \in P$; diese Primzahl ist dadurch ausgezeichnet, daß $P \cap \mathbb{Z} = p\mathbb{Z}$ ist.*

Beweis. Mit $x \in P \setminus \{0\}$ ist $N(x) = xx^\sigma \in (P \cap \mathbb{Z}) \setminus \{0\}$. Damit ist $P \cap \mathbb{Z}$ ein von Null verschiedenes Primideal von \mathbb{Z} , also von der angegebenen Gestalt. \square

MEMO. Sei R ein kommutativer Ring mit 1, und sei $I \trianglelefteq R$. Dann induziert die kanonische Projektion $R \rightarrow R/I$ eine inklusionserhaltende bijektive Abbildung $\Psi : \{A \mid I \subseteq A \trianglelefteq R\} \rightarrow \{J \mid J \trianglelefteq R/I\}$, $A \mapsto \{a + I \mid a \in A\}$. Mittels Ψ sind Primideale zu Primidealen und maximale Ideale zu maximalen Idealen assoziiert.

Satz 3.5. *Jeder endliche Integritätsbereich ist ein Körper.*

Beweis. Sei R ein endlicher Integritätsbereich, und sei $x \in R \setminus \{0\}$. Gesucht ist ein multiplikativ inverses Element zu x . Betrachte dazu die Folge $(x^n)_{n \in \mathbb{N}}$ in R . Da R endlich ist, finden wir $m, n \in \mathbb{N}$ mit $m < n$ und $x^m = x^n$. Dann gilt $x^m(1 - x^{n-m}) = x^m - x^n = 0$, und da R nullteilerfrei ist, folgt $x \cdot x^{n-m-1} = x^{n-m} = 1$. \square

MEMO. Sei R ein kommutativer Ring mit 1. Zwei Ideale $A, B \trianglelefteq R$ heißen *relativ prim* zueinander, falls $A + B = R$. Der sogenannte *Chinesische Restsatz* besagt folgendes (vgl. Aufgabenblatt 4):

Sei $m \in \mathbb{N}$, und seien A_1, \dots, A_m paarweise relativ prime Ideale von R . Dann ist $A_1 \circ \dots \circ A_m = A_1 \cap \dots \cap A_m$, und es gilt

$$R/(A_1 \circ \dots \circ A_m) \cong R/A_1 \times \dots \times R/A_m.$$

Satz und Definition 3.6. *Sei $p \in \mathbb{P}$. Dann liegt genau einer der folgenden drei Fälle vor.*

I. *Es existieren $P, Q \in \mathcal{P}(\mathcal{O})$ mit $P \neq Q$ und $p\mathcal{O} = P \circ Q$. In diesem Fall heißt p zerlegt in K , und es gelten*

$$\mathcal{O}/P \cong \mathcal{O}/Q \cong \mathbb{F}_p, \quad \mathcal{O}/p\mathcal{O} \cong \mathbb{F}_p \times \mathbb{F}_p.$$

II. Es existiert $P \in \mathcal{P}(\mathcal{O})$ mit $p\mathcal{O} = P \circ P$. In diesem Fall heißt p verzweigt in K , und es gelten

$$\mathcal{O}/P \cong \mathbb{F}_p, \quad \mathcal{O}/p\mathcal{O} \cong \mathbb{F}_p[X]/X^2\mathbb{F}_p[X].$$

III. Es gilt $p\mathcal{O} \in \mathcal{P}(\mathcal{O})$. In diesem Fall heißt p träge in K , und $\mathcal{O}/p\mathcal{O} \cong \mathbb{F}_{p^2}$ ist ein Körper mit p^2 Elementen.

Beweis. Der natürliche Epimorphismus $\mathbb{Z}[X] \rightarrow \mathbb{Z}[\omega] = \mathcal{O}$, $g(X) \mapsto g(\omega)$, der durch Einsetzen von ω gegeben ist, hat den Kern $f\mathbb{Z}[X]$, wobei

$$f = (X - \omega)(X - \omega^\sigma) = \begin{cases} X^2 - d & \text{falls } d \not\equiv_4 1 \\ X^2 - X + (1 - d)/4 & \text{falls } d \equiv_4 1. \end{cases}$$

das Minimalpolynom von ω über \mathbb{Q} bezeichnet. Die Restklassenabbildung $\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, $a \mapsto a + p\mathbb{Z} = \bar{a}$ setzt sich durch koeffizientenweise Anwendung fort zu einem Epimorphismus $\mathbb{Z}[X] \rightarrow \mathbb{F}_p[X]$, $g \mapsto \bar{g}$, dessen Kern gerade $p\mathbb{Z}[X]$ ist.

Von zentraler Bedeutung ist nun die folgende Isomorphiekette

$$\frac{\mathcal{O}}{p\mathcal{O}} \cong \frac{\mathbb{Z}[X]}{p\mathbb{Z}[X] + f\mathbb{Z}[X]} \cong \frac{\mathbb{F}_p[X]}{f\mathbb{F}_p[X]},$$

die sich durch Vertauschen der Reihenfolge des Faktorisierens ergibt. Dadurch rückt das Zerlegungsverhalten von $\bar{f} \in \mathbb{F}_p[X]$ in den Vordergrund. Es gibt drei Fälle.

Fall I. Das Polynom \bar{f} hat zwei verschiedene Nullstellen \bar{a}_1, \bar{a}_2 in \mathbb{F}_p . Dann gilt $\bar{f} = \bar{g}_1\bar{g}_2$, wobei $g_1 := X - a_1, g_2 := X - a_2 \in \mathbb{Z}[X]$ gewählt sind, so daß $\bar{g}_1 = X - \bar{a}_1$ und $\bar{g}_2 = X - \bar{a}_2$. Setze $P := p\mathcal{O} + g_1(\omega)\mathcal{O}$ und $Q := p\mathcal{O} + g_2(\omega)\mathcal{O}$. Mit dem Chinesischen Restsatz folgt die Behauptung.

Fall II. Das Polynom \bar{f} hat eine doppelte Nullstelle \bar{a} in \mathbb{F}_p . Dann gilt $\bar{f} = \bar{g}^2$, wobei $g := X - a \in \mathbb{Z}[X]$ gewählt ist, so daß $\bar{g} = X - \bar{a}$. Setze $P := p\mathcal{O} + g(\omega)\mathcal{O}$. Es folgt die Behauptung.

Fall III. Das Polynom \bar{f} hat keine Nullstellen in \mathbb{F}_p . Dann ist \bar{f} irreduzibel über \mathbb{F}_p , und mit Satz 3.5 folgt die Behauptung. \square

Beispiel 3.7. In $K = \mathbb{Q}(\sqrt{7})$ ist 57 zerlegt, denn $8^2 = 64 \equiv_{57} 7$. Somit gilt $57\mathcal{O} = P \circ Q$ mit $P = 57\mathcal{O} + (\sqrt{7} - 8)\mathcal{O}$ und $Q = P^\sigma = 57\mathcal{O} + (\sqrt{7} + 8)\mathcal{O}$. Zu weiteren konkreten Rechnungen regt das Arbeitsblatt 9 an.

MEMO. Sei G eine endliche Gruppe und $H \leq G$ eine Untergruppe. Der bekannte Satz von LAGRANGE besagt, daß die Untergruppenordnung $|H|$ die Gruppenordnung $|G|$ teilt; siehe Aufgabenblatt 6. Der Quotient $|G : H| := |G|/|H|$ heißt *Index* von H in G . Insbesondere teilt die Ordnung $\text{ord}(g)$ jedes Elementes $g \in G$ die Gruppenordnung $|G|$.

Der Exponent einer endlichen Gruppe G ist das kleinste gemeinsame Vielfache aller Elementordnungen: $\exp(G) := \text{kgV}\{\text{ord}(g) \mid g \in G\}$. Stets teilt der Exponent $\exp(G)$ die Ordnung $|G|$ einer endlichen Gruppe G , insbesondere ist $\exp(G) \leq |G|$.

Satz 3.8. Jede endliche Untergruppe der multiplikativen Gruppe eines Körpers ist zyklisch.

Beweis. Seien K ein Körper, G eine endliche Untergruppe von K^* und $e := \exp(G)$. Dann gilt $g^e = 1$ für jedes $g \in G$. Also ist G in der Nullstellenmenge des

Polynoms $X^e - 1$ enthalten. Da ein Polynom e -ten Grades in K höchstens $e \leq |G|$ Nullstellen besitzt, schöpft G die gesamte Nullstellenmenge aus, und es gilt $e = |G|$.

Wir überlegen nun, daß eine endliche abelsche Gruppe A mit $\exp(A) = |A|$ stets zyklisch ist. Seien dazu $a, b \in A$ und $m := \text{ord}(a), n := \text{ord}(b)$. Es genügt offenbar, ein Element in A anzugeben, das die Ordnung $\text{kgV}(m, n)$ hat. Indem wir b durch $b^{\text{ggT}(m, n)}$ ersetzen, dürfen wir ohne Einschränkung annehmen, daß $\text{ggT}(m, n) = 1$ ist. Dann sind m und n teilerfremd, und daher gilt $\langle a \rangle \cap \langle b \rangle = \{1\}$. Der Chinesische Restsatz zeigt: $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}$. Entsprechend haben wir $\langle a, b \rangle = \langle a \rangle \times \langle b \rangle = \langle ab \rangle$, wobei ab tatsächlich die Ordnung $mn = \text{kgV}(m, n)$ besitzt. \square

Korollar 3.9. *Die multiplikative Gruppe eines endlichen Körpers K ist zyklisch. Die von Null verschiedenen Quadrate bilden eine Untergruppe $Q := \{x^2 \mid x \in K^*\}$ vom Index zwei in K^* . Die Gruppe Q ist zyklisch der Ordnung $(|K| - 1)/2$, und es gilt $Q = \{x \in K^* \mid \text{ord}(x) \mid (|K| - 1)/2\}$.*

Beispiel 3.10. Die multiplikative Gruppe $\mathbb{F}_7^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ eines Primkörpers mit sieben Elementen wird erzeugt von $\bar{3}$. Es gilt nämlich: $\bar{3}^2 = \bar{2}$, $\bar{3}^3 = \bar{6}$, $\bar{3}^4 = \bar{4}$, $\bar{3}^5 = \bar{5}$, $\bar{3}^6 = \bar{1}$. Die von Null verschiedenen Quadrate sind gerade $\bar{2}$, $\bar{4}$ und $\bar{1}$.

Definition 3.11. Sei $a \in \mathbb{Z}$. Für $p \in \mathbb{P} \setminus \{2\}$ setzen wir $\bar{a} = a + p\mathbb{Z} \in \mathbb{F}_p$ und definieren das (erweiterte) **LEGENDRE-Symbol** gemäß

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & \text{falls } \bar{a} = 0, \\ 1 & \text{falls } \bar{a} \in \{x^2 \mid x \in \mathbb{F}_p^*\}, \\ -1 & \text{falls } \bar{a} \in \mathbb{F}_p^* \setminus \{x^2 \mid x \in \mathbb{F}_p^*\}. \end{cases}$$

Für die Primzahl 2 definieren wir das (erweiterte) **LEGENDRE-Symbol** gemäß

$$\left(\frac{a}{2}\right) := \begin{cases} 0 & \text{falls } a \equiv_2 0, \\ 1 & \text{falls } a \equiv_8 1 \text{ oder } a \equiv_8 7, \\ -1 & \text{falls } a \equiv_8 3 \text{ oder } a \equiv_8 5. \end{cases}$$

Eine grundlegende Eigenschaft des **LEGENDRE-Symbols** ist seine Multiplikativität.

Lemma 3.12. *Sei $p \in \mathbb{P}$. Dann gilt für alle $a, b \in \mathbb{Z}$:*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right).$$

Beweis. Dies ist eine leichte Rechnung. Sei zunächst $p > 2$. Nach Korollar 3.9 bilden die von Null verschiedenen Quadrate $Q = \{x^2 \mid x \in \mathbb{F}_p^*\}$ eine Untergruppe vom Index zwei in \mathbb{F}_p^* . Der kanonische Homomorphismus $\mathbb{F}_p^* \rightarrow \mathbb{F}_p^*/Q \cong \{1, -1\}$ ist gegeben durch $\bar{a} \mapsto \left(\frac{a}{p}\right)$. Die Multiplikativität des **LEGENDRE-Symbols** ist im wesentlichen die Homomorphieeigenschaft dieser Abbildung.

Sei nun $p = 2$. Die Einheitengruppe des Restklassenrings $\mathbb{Z}/8\mathbb{Z}$ ist eine **KLEINSche Vierergruppe**: $(\mathbb{Z}/8\mathbb{Z})^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Die Abbildung $(\mathbb{Z}/8\mathbb{Z})^* \rightarrow \{1, -1\}$, $\bar{a} \mapsto \left(\frac{a}{2}\right)$ ist diesmal einer von drei möglichen nicht-trivialen Homomorphismen. \square

Mit etwas Aufwand läßt sich jedem algebraischen Zahlkörper eine strukturelle Invariante, die sogenannte Diskriminante, zuordnen. Wir begnügen uns hier mit einer ad-hoc-Definition.

Definition 3.13. Die *Diskriminante* des quadratischen Zahlkörpers $K = \mathbb{Q}(\sqrt{d})$ ist die Zahl

$$\delta_K := \begin{cases} d & \text{falls } d \equiv_4 1, \\ 4d & \text{falls } d \not\equiv_4 1. \end{cases}$$

Damit erhalten wir eine übersichtliche Beschreibung des Zerlegungsverhaltens der Primzahlen in einem quadratischen Zahlkörper.

Hauptsatz 3.14 (Zerlegungsgesetz). *Sei $p \in \mathbb{P}$. Dann läßt sich das Zerlegungsverhalten von $p\mathcal{O}$ in \mathcal{O} anhand der Diskriminante $\delta := \delta_K$ wie folgt ablesen:*

- (1) p ist zerlegt in K genau dann, wenn $\left(\frac{\delta}{p}\right) = 1$;
- (2) p ist verzweigt in K genau dann, wenn $\left(\frac{\delta}{p}\right) = 0$;
- (3) p ist träge in K genau dann, wenn $\left(\frac{\delta}{p}\right) = -1$.

Beweis. Aus dem Beweis von Satz 3.6 ist uns bereits bekannt, daß das Zerlegungsverhalten von $p\mathcal{O}$ maßgeblich durch die Nullstellenmenge des Polynoms

$$f = \begin{cases} X^2 - d & \text{falls } d \not\equiv_4 1 \\ X^2 - X + (1-d)/4 & \text{falls } d \equiv_4 1. \end{cases}$$

modulo p bestimmt wird. Sei $\bar{f} \in \mathbb{F}_p[X]$ das Bild von f unter der natürlichen Restklassenabbildung. Dann kommt es darauf an, wie viele Elemente die Nullstellenmenge $\text{Nullst}(f, p) := \{\bar{a} \in \mathbb{F}_p \mid \bar{f}(\bar{a}) = 0\}$ hat:

$$\begin{aligned} p \text{ ist zerlegt} &\iff \#\text{Nullst}(f, p) = 2, \\ p \text{ ist verzweigt} &\iff \#\text{Nullst}(f, p) = 1, \\ p \text{ ist träge} &\iff \#\text{Nullst}(f, p) = 0. \end{aligned}$$

Sei zunächst $d \not\equiv_4 1$. Dann sind $\bar{f} = X^2 - \bar{d}$ und $\delta = 4d$. Ist $p \neq 2$, so gilt offenbar $\left(\frac{\delta}{p}\right) = \left(\frac{4}{p}\right)\left(\frac{d}{p}\right) = \left(\frac{d}{p}\right)$, und tatsächlich erhalten wir

$$\begin{aligned} \#\text{Nullst}(f, p) = 2 &\iff \bar{d} \neq 0 \text{ ist Quadrat in } \mathbb{F}_p &\iff \left(\frac{\delta}{p}\right) = 1, \\ \#\text{Nullst}(f, p) = 1 &\iff \bar{d} = 0 &\iff \left(\frac{\delta}{p}\right) = 0, \\ \#\text{Nullst}(f, p) = 0 &\iff \bar{d} \neq 0 \text{ ist kein Quadrat in } \mathbb{F}_p &\iff \left(\frac{\delta}{p}\right) = -1. \end{aligned}$$

Ist $p = 2$, so gilt $\left(\frac{\delta}{p}\right) = 0$; und tatsächlich ist $\text{Nullst}(f, p) = 1$, denn entweder haben wir $\bar{f} = X^2$ oder $\bar{f} = X^2 + 1$.

Sei nun $d \equiv_4 1$. Dann sind $\bar{f} = X^2 - X + \overline{(1-d)/4}$ und $\delta = d$. Ist $p \neq 2$, so gilt $\bar{f} = (X - 1/2)^2 - \bar{d}/4$, und wegen $\left(\frac{4}{p}\right) = 1$ erhalten wir tatsächlich

$$\begin{aligned} \#\text{Nullst}(f, p) = 2 &\iff \bar{d}/4 \neq 0 \text{ ist Quadrat in } \mathbb{F}_p &\iff \left(\frac{\delta}{p}\right) = 1, \\ \#\text{Nullst}(f, p) = 1 &\iff \bar{d}/4 = 0 &\iff \left(\frac{\delta}{p}\right) = 0, \\ \#\text{Nullst}(f, p) = 0 &\iff \bar{d}/4 \neq 0 \text{ ist kein Quadrat in } \mathbb{F}_p &\iff \left(\frac{\delta}{p}\right) = -1. \end{aligned}$$

Sei nun $p = 2$. Dann nimmt $\left(\frac{\delta}{p}\right)$ den Wert 1 oder -1 an, je nachdem, ob $d \equiv_8 1$ oder $d \equiv_8 5$ ist. Entsprechend gilt entweder $\bar{f} = X^2 + X$, also $\text{Nullst}(f, p) = 2$, oder $\bar{f} = X^2 + X + 1$, also $\text{Nullst}(f, p) = 0$. \square

4. Quadratisches Reziprozitätsgesetz

Um den Hauptsatz 3.14 in der Praxis anwenden zu können, bedarf es einer Methode, mittels derer sich LEGENDRE-Symbole effektiv auswerten lassen. Ein solches Rechenverfahren wird durch das sogenannte Quadratische Reziprozitätsgesetz bereitgestellt.

Lemma 4.1. Für $p \in \mathbb{P} \setminus \{2\}$ gilt $\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = 0$.

Beweis. Der zu untersuchende Ausdruck ist gleich der Anzahl der Quadrate in \mathbb{F}_p^* abzüglich der Anzahl der Nicht-Quadrate in \mathbb{F}_p^* . Die Quadrate in \mathbb{F}_p^* bilden nach Korollar 3.9 eine Untergruppe vom Index zwei in \mathbb{F}_p^* . Somit kommt auf jedes Quadrat genau ein Nicht-Quadrat, und der Ausdruck ist null. \square

Satz 4.2 (EULERSches Kriterium). Sei $p \in \mathbb{P} \setminus \{2\}$, und sei $a \in \mathbb{Z}$. Dann gilt

$$\left(\frac{a}{p}\right) \equiv_p a^{(p-1)/2}.$$

Beweis. Nach Korollar 3.9 ist die Menge $Q := \{x^2 \mid x \in \mathbb{F}_p^*\}$ der von Null verschiedenen Quadrate gekennzeichnet durch $Q = \{x \in \mathbb{F}_p^* \mid x^{(p-1)/2} = 1\}$.

Ist $\bar{a} = 0$, so gilt $\left(\frac{\bar{a}}{p}\right) = 0 \equiv_p a^{(p-1)/2}$. Ist $\bar{a} \in Q$, so gilt $\text{ord}(\bar{a}) \mid (p-1)/2$, also $\left(\frac{\bar{a}}{p}\right) = 1 \equiv_p a^{(p-1)/2}$. Ist schließlich $\bar{a} \in \mathbb{F}_p^* \setminus Q$, so gilt $\text{ord}(\bar{a}^{(p-1)/2}) = 2$, also $\left(\frac{\bar{a}}{p}\right) = -1 \equiv_p a^{(p-1)/2}$. \square

Korollar 4.3. Sei $p \in \mathbb{P} \setminus \{2\}$. Dann gilt

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

Lemma 4.4. Sei $n \in \mathbb{N}$ mit $n \geq 2$, und sei $\zeta \in \mathbb{C}$ eine n -te Einheitswurzel. Dann ist $\sum_{j=0}^{n-1} \zeta^j = 0$.

Beweis. Aus $\zeta \neq 1$ und $(\zeta - 1) \sum_{j=0}^{n-1} \zeta^j = \zeta^n - 1 = 0$ folgt $\sum_{j=0}^{n-1} \zeta^j = 0$. \square

Definition 4.5. Für $p \in \mathbb{P}$ setze

$$\hat{p} := \begin{cases} 2 & \text{falls } p = 2, \\ (-1)^{(p-1)/2} p & \text{falls } p > 2. \end{cases}$$

Wir bemerken im Vorübergehen, daß für jede Primzahl $p > 2$ gilt: $\hat{p} \equiv_4 1$, und kommen nun zu dem berühmten Quadratischen Reziprozitätsgesetz. Dieses ist ein wahres Schmuckstück der elementaren Zahlentheorie und zugleich Ausgangspunkt für weitreichende Verallgemeinerungen in der algebraischen Zahlentheorie. Das Quadratische Reziprozitätsgesetz wurde scheinbar unabhängig von EULER, LEGENDRE und GAUSS entdeckt und erstmals 1796 von GAUSS ordentlich bewiesen. Der Beweis, den wir angeben, beruht implizit auf dem Zerlegungsverhalten von Primzahlen, allerdings nicht nur in quadratischen Zahlkörpern sondern auch in den sogenannten Kreisteilungskörpern, die wir nicht im Detail behandelt haben.

Hauptsatz 4.6 (Quadratisches Reziprozitätsgesetz).

Für Primzahlen p, q gilt:

$$\left(\frac{p}{q}\right) = \left(\frac{\hat{q}}{p}\right).$$

Beweis. Für $p = q$ sind beide Ausdrücke gleich null. Sei jetzt $p \neq q$.

Wir betrachten zunächst den Fall $2 \in \{p, q\}$. Ist $p = 2$, so ist die Behauptung wegen

$$\left(\frac{\hat{q}}{2}\right) = \left(\frac{(-1)^{(q-1)/2}}{2}\right) \left(\frac{q}{2}\right) = \left(\frac{q}{2}\right)$$

gleichbedeutend mit $\left(\frac{2}{q}\right) = \left(\frac{q}{2}\right)$. Ist $q = 2$, so ergibt sich die entsprechende Behauptung $\left(\frac{2}{p}\right) = \left(\frac{p}{2}\right)$ für p anstelle von q . Wir beweisen letztere.

Der Wert des LEGENDRE-Symbols $\left(\frac{2}{p}\right)$ hängt per Definition nur von p modulo 8 ab. Es genügt daher, zu zeigen:

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{falls } p \equiv_8 1 \text{ oder } p \equiv_8 7, \\ -1 & \text{falls } p \equiv_8 3 \text{ oder } p \equiv_8 5. \end{cases}$$

Sei $\zeta := \exp(2\pi i/8)$ eine primitive achte Einheitswurzel in \mathbb{C} . Im folgenden werden wir in dem Faktorring $\mathbb{Z}[\zeta]/p\mathbb{Z}[\zeta]$ rechnen. Entscheidend ist hierbei, daß $\mathbb{Z} \cap p\mathbb{Z}[\zeta] = p\mathbb{Z}$ ist. Somit ist für ganze Zahlen a, b die Kongruenz $a \equiv b$ modulo $p\mathbb{Z}[\zeta]$ gleichbedeutend mit $a \equiv b$ modulo $p\mathbb{Z}$. Wir dürfen daher etwas unverbindlich von Kongruenzen modulo p reden.

Setze

$$G := \zeta - \zeta^3 - \zeta^5 + \zeta^7 = 2(\zeta - \zeta^3) \in \mathbb{Z}[\zeta].$$

(Merke: G ist eine sogenannte GAUSSsche Summe. Die Vorzeichen der einzelnen Summanden sind gegeben durch $\left(\frac{1}{2}\right), \left(\frac{3}{2}\right), \left(\frac{5}{2}\right), \left(\frac{7}{2}\right)$.) Dann gilt $G^2 = 4(\zeta^2 - 2\zeta^4 + \zeta^6) = 4(i + 2 - i) = 8$. Insbesondere ist G modulo p invertierbar.

Wir berechnen G^p modulo p auf zweierlei Weise:

$$\begin{aligned} G^p &= (G^2)^{(p-1)/2} G \\ &= 8^{(p-1)/2} G && \text{denn } G^2 = 8 \\ &\equiv_p \left(\frac{8}{p}\right) G && \text{nach Satz 4.2} \\ &= \left(\frac{2}{p}\right) G, \\ G^p &\equiv_p \zeta^p - \zeta^{3p} - \zeta^{5p} + \zeta^{7p} && \text{wegen } (x+y)^p \equiv x^p + y^p \text{ modulo } p \\ &= \begin{cases} G & \text{falls } p \equiv_8 1 \text{ oder } p \equiv_8 7, \\ -G & \text{falls } p \equiv_8 3 \text{ oder } p \equiv_8 5. \end{cases} && \text{wegen } \zeta^8 = 1 \end{aligned}$$

Setzt man beide Ausdrücke gleich, so ergibt sich

$$\left(\frac{2}{p}\right) G \equiv_p \begin{cases} G & \text{falls } p \equiv_8 1 \text{ oder } p \equiv_8 7, \\ -G & \text{falls } p \equiv_8 3 \text{ oder } p \equiv_8 5. \end{cases}$$

Da G modulo p invertierbar ist, folgt die Behauptung.

Es bleibt somit der Fall $p, q > 2$. Sei $\zeta := \exp(2\pi i/q)$ eine primitive q -te Einheitswurzel in \mathbb{C} . Im folgenden werden wir in dem Faktorring $\mathbb{Z}[\zeta]/p\mathbb{Z}[\zeta]$ rechnen. Wie zuvor ist entscheidend, daß $\mathbb{Z} \cap p\mathbb{Z}[\zeta] = p\mathbb{Z}$ ist. Wir dürfen daher wiederum etwas unverbindlich von Kongruenzen modulo p reden.

Setze

$$G := \sum_{j=1}^{q-1} \binom{j}{q} \zeta^j \in \mathbb{Z}[\zeta].$$

(Wir erkennen hier besser als zuvor die Struktur der GAUSSSche Summe G .) Dann gilt

$$\begin{aligned} G^2 &= \left(\sum_{j=1}^{q-1} \binom{j}{q} \zeta^j \right) \cdot \left(\sum_{k=1}^{q-1} \binom{k}{q} \zeta^k \right) \\ &= \sum_{j=1}^{q-1} \left(\binom{j}{q} \zeta^j \sum_{k=1}^{q-1} \binom{-jk}{q} \zeta^{-jk} \right) && k \mapsto -jk \text{ liefert Umordnung} \\ &= \sum_{j=1}^{q-1} \sum_{k=1}^{q-1} \binom{-j^2k}{q} \zeta^{j(1-k)} + \underbrace{\sum_{k=1}^{q-1} \binom{-k}{q} \zeta^0}_{=0} && \text{nach Lemma 4.1} \\ &= \left(\frac{-1}{q} \right) \sum_{j=0}^{q-1} \sum_{k=1}^{q-1} \binom{k}{q} \zeta^{j(1-k)} && \text{wegen } \binom{-j^2k}{q} = \binom{-k}{q} = \left(\frac{-1}{q} \right) \binom{k}{q} \\ &= \left(\frac{-1}{q} \right) q + \left(\frac{-1}{q} \right) \sum_{k=2}^{q-1} \binom{k}{q} \underbrace{\sum_{j=0}^{q-1} \zeta^{j(1-k)}}_{=0} && \text{nach Lemma 4.4} \\ &= \hat{q} && \text{nach Korollar 4.3.} \end{aligned}$$

Insbesondere ist G modulo p invertierbar.

Wir berechnen G^p modulo p auf zweierlei Weise:

$$\begin{aligned} G^p &= (G^2)^{(p-1)/2} G \\ &= (\hat{q})^{(p-1)/2} G && \text{denn } G^2 = \hat{q} \\ &\equiv_p \left(\frac{\hat{q}}{p} \right) G && \text{nach Satz 4.2,} \\ G^p &\equiv_p \sum_{j=1}^{q-1} \binom{j}{q} \zeta^{jp} && \text{wegen } (x+y)^p \equiv x^p + y^p \text{ modulo } p \\ &= \left(\frac{p}{q} \right) \sum_{j=1}^{q-1} \binom{jp}{q} \zeta^{jp} && \text{wegen } \binom{j}{q} = \binom{p}{q} \binom{jp}{q} \\ &= \left(\frac{p}{q} \right) G. \end{aligned}$$

Setzt man beide Ausdrücke gleich, so ergibt sich

$$\left(\frac{\hat{q}}{p} \right) G \equiv_p \left(\frac{p}{q} \right) G.$$

Da G modulo p invertierbar ist, folgt die Behauptung. \square

Beispiel 4.7. Durch die Berechnung von $\left(\frac{33}{103}\right)$ weisen wir nach, daß die Primzahl 103 in $K = \mathbb{Q}(\sqrt{33})$ zerlegt ist. In der Tat ergibt sich durch wiederholte Anwendung des Quadratischen Reziprozitätsgesetzes:

$$\begin{aligned} \left(\frac{33}{103}\right) &= \left(\frac{3}{103}\right) \left(\frac{11}{103}\right) = \left(\frac{-103}{3}\right) \left(\frac{-103}{11}\right) = \left(\frac{2}{3}\right) \left(\frac{7}{11}\right) = (-1) \left(\frac{-11}{7}\right) \\ &= (-1) \left(\frac{3}{7}\right) = (-1) \left(\frac{-7}{3}\right) = (-1) \left(\frac{2}{3}\right) = (-1)^2 = 1. \end{aligned}$$

Beispiel 4.8. Sei $K = \mathbb{Q}(\sqrt{-5})$ mit Ganzheitsring $\mathcal{O} = \mathbb{Z}[\sqrt{-5}]$. Die von Null verschiedenen Quadrate modulo 5 sind gerade 1 und 4. Mit Hilfe des Quadratischen Reziprozitätsgesetzes können wir daher ein einfaches Kriterium dafür angeben, welchen Wert das LEGENDRE-Symbol $\left(\frac{-5}{p}\right)$ für vorgegebenes $p \in \mathbb{P} \setminus \{2\}$ annimmt:

$$\begin{aligned} \left(\frac{-5}{p}\right) &= \left(\frac{-1}{p}\right) \left(\frac{5}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{p}{5}\right) \\ &= \begin{cases} 0 & \text{falls } p = 5, \\ 1 & \text{falls } (p \equiv_4 1 \text{ und } p \equiv_5 1, 4) \text{ oder } (p \equiv_4 3 \text{ und } p \equiv_5 2, 3), \\ -1 & \text{falls } (p \equiv_4 1 \text{ und } p \equiv_5 2, 3) \text{ oder } (p \equiv_4 3 \text{ und } p \equiv_5 1, 4) \end{cases} \\ &= \begin{cases} 0 & \text{falls } p = 5, \\ 1 & \text{falls } p \equiv_{20} 1, 3, 7, 9. \\ -1 & \text{falls } p \equiv_{20} 11, 13, 17, 19. \end{cases} \end{aligned}$$

Daraus folgt für $p \in \mathbb{P}$ nach Hauptsatz 3.14:

$$\begin{aligned} p \text{ ist zerlegt in } \mathbb{Q}(\sqrt{-5}) &\iff p \equiv_{20} 1, 3, 7, 9 \\ p \text{ ist verzweigt in } \mathbb{Q}(\sqrt{-5}) &\iff p \in \{2, 5\}, \\ p \text{ ist träge in } \mathbb{Q}(\sqrt{-5}) &\iff p \equiv_{20} 11, 13, 17, 19. \end{aligned}$$

ANHANG A

Sammlung der Arbeitsblätter

Auf den nachfolgenden Seiten finden sich die verschiedenen Arbeitsblätter, die wöchentlich in den Übungen zu der Vorlesung besprochen wurden.

Arbeitsblatt zur Elementaren Zahlentheorie

Sei $\mathcal{P}_{\mathbb{Z}} := \{(a, b, c) \in \mathbb{Z}^3 \mid a^2 + b^2 = c^2\}$. Die Elemente dieser Menge wurden schon in der Antike erfolgreich untersucht und heißen gemeinhin *pythagoreische Tripel*. Bekannte Beispiele von pythagoreischen Tripeln sind $(3, 4, 5)$ und $(5, 12, 13)$. Wir wollen zusätzlich auch $\mathcal{P}_{\mathbb{Q}} := \{(x, y, z) \in \mathbb{Q}^3 \mid x^2 + y^2 = z^2\}$ betrachten.

- (1) Für alle $s, t \in \mathbb{Z}$ ist $(s^2 - t^2, 2st, s^2 + t^2) \in \mathcal{P}_{\mathbb{Z}}$.
- (2) Ist $(a, b, c) \in \mathcal{P}_{\mathbb{Z}}$, so ist wenigstens eine der Zahlen a, b gerade.
- (3) Das pythagoreische Tripel $(a, b, c) \in \mathcal{P}_{\mathbb{Z}}$ erfülle die Zusatzbedingungen:

(i) $a, b, c \in \mathbb{N}_0$ sind paarweise teilerfremd, (ii) b ist gerade.

Dann existieren $s, t \in \mathbb{N}_0$ mit $(a, b, c) = (s^2 - t^2, 2st, s^2 + t^2)$. Sind diese eindeutig durch (a, b, c) bestimmt?

Hinweis: Schreibe $b = 2\tilde{b}$. Dann gilt $\tilde{b}^2 = (c+a)/2 \cdot (c-a)/2$. Zeige (unter Verwendung der eindeutigen Primfaktorzerlegung für \mathbb{Z}), daß hier beide Faktoren Quadrate ganzer Zahlen sind, und schreibe sodann $(c+a)/2 = s^2$, $(c-a)/2 = t^2$.

- (4) Es gilt $\mathcal{P}_{\mathbb{Q}} = \{((s^2 - t^2)q, 2stq, (s^2 + t^2)q) \mid s, t \in \mathbb{Z} \text{ und } q \in \mathbb{Q}\}$.
- (5) Für welche $n, k \in \mathbb{N}$ ist $(n, n+k, n+2k) \in \mathcal{P}_{\mathbb{Z}}$?

BEMERKUNG. Man kann sich auch geometrisch einen Überblick über die pythagoreischen Tripel verschaffen. Dazu bemerkt man, daß ein offensichtlicher Zusammenhang zwischen ganzzahligen Lösungen der Gleichung $A^2 + B^2 = C^2$ und rationalen Lösungen der Gleichung $X^2 + Y^2 = 1$ besteht. Letztere beschreibt den Einheitskreis und hat unter anderem die triviale Lösung $P_0 := (1, 0)$. Ist $Q = (x, y) \in \mathbb{Q}^2 \setminus \{P_0\}$ ein weiterer Punkt auf dem Einheitskreis, so beschreibt die Gleichung $Y = qX - q$ mit $q = y/(x-1) \in \mathbb{Q}$ die Verbindungsgerade von P_0 und Q .

Umgekehrt besitzt jede Gerade $Y = qX - q$, $q \in \mathbb{Q}$, zusätzlich zu P_0 einen weiteren Schnittpunkt mit dem Einheitskreis. Dieser hat die rationalen Koordinaten $x = (q^2 - 1)/(q^2 + 1)$ und $y = -2q/(q^2 + 1)$. Schreibt man $q = s/t$ mit $s, t \in \mathbb{Z}$, $t \neq 0$, so ergibt sich $x = (s^2 - t^2)/(s^2 + t^2)$ und $y = -2st/(s^2 + t^2)$. Dies liefert z.B. das pythagoreische Tripel $(s^2 - t^2, 2st, s^2 + t^2)$.

Anders als bei der oben vorgeschlagenen Rechnung kommt man mit diesem Ansatz *ohne* die Verwendung der eindeutigen Primfaktorzerlegung für \mathbb{Z} aus.

Arbeitsblatt zur Elementaren Zahlentheorie

Für $n \in \mathbb{N}$ bezeichnet $T^+(n) := \{t \in \mathbb{N} \mid t \mid n\}$ die Menge der positiven Teiler von n . Zwei natürliche Zahlen m, n heißen *teilerfremd*, falls $T^+(m) \cap T^+(n) = \{1\}$ ist. Die *Teilersumme* einer natürlichen Zahl $n \in \mathbb{N}$ ist definiert als $\sigma(n) := \sum_{t \in T^+(n)} t$.

- (1) Sind $m, n \in \mathbb{N}$ teilerfremd, so gilt $\sigma(mn) = \sigma(m)\sigma(n)$.
- (2) Für $p \in \mathbb{P}$ und $k \in \mathbb{N}_0$ gilt: $\sigma(p^k) = (p^{k+1} - 1)/(p - 1)$.
(Diese Formel findet sich schon bei DESCARTES.)
- (3) Berechne $\sigma(28)$ und $\sigma(180)$.
- (4) Eine natürliche Zahl $n \in \mathbb{N}$ heißt *vollkommen*, falls gilt: $\sigma(n) = 2n$. Leite die folgende Beschreibung gerader vollkommener Zahlen her, deren einfache Richtung „ \Leftarrow “ von EUKLID und schwierigere Richtung „ \Rightarrow “ von EULER stammt.

Sei $s \in \mathbb{N}$ mit $s \geq 2$, und sei $b \in \mathbb{N}$ mit $2 \nmid b$. Sei $a := 2^{s-1}b$. Dann ist a vollkommen genau dann, wenn $b = 2^s - 1 \in \mathbb{P}$.

Hinweis für „ \Rightarrow “: Zeige $2^s b = \sigma(a) = (2^s - 1)\sigma(b)$, also $(2^s - 1)(\sigma(b) - b) = b$. Insbesondere teilt $\sigma(b) - b$ die Zahl b , und es gilt $1 \leq \sigma(b) - b < b$. Führe die Annahme $\sigma(b) - b \neq 1$ zu einem Widerspruch.

- (5) Ist $s \in \mathbb{N}$ mit $2^s - 1 \in \mathbb{P}$, so gilt $s \in \mathbb{P}$.

Der Begriff einer vollkommenen Zahl findet sich bereits bei EUKLID. Im Altertum zählte n selbst nicht zu den Teilern von n ; gemäß dieser „überholten“ Auffassung sind die vollkommenen Zahlen also genau die Zahlen, die gleich ihrer Teilersumme sind. Die ersten vier vollkommenen Zahlen sind 6, 28, 496, 8128; dies wußten schon die Griechen. Das Problem, alle vollkommenen Zahlen zu bestimmen, ist bis heute ungelöst. Insbesondere ist nicht bekannt, ob es ungerade vollkommene Zahlen gibt. (Man weiß: Es gibt keine ungerade vollkommene Zahl kleiner als 10^{50} .)

Primzahlen der Gestalt $2^s - 1$, $s \in \mathbb{N}$, heißen MERSENNEsche Primzahlen. Es ist ein offenes Problem, ob es unendlich viele MERSENNEsche Primzahlen gibt.

Arbeitsblatt zur Elementaren Zahlentheorie

Zur Abwechslung eine Reihe von zahlentheoretischen Knobelaufgaben:

- (1) Seien $a, m \in \mathbb{N} \setminus \{1\}$, so daß $a^m + 1$ eine Primzahl ist.
Zeige: a ist gerade und m eine Potenz von 2.
- (2) Sei $k \in \mathbb{N}$. Sei $M := \{1, 2, \dots, 2k\}$, und sei $T \subseteq M$ mit $|T| > k$.
Zeige: Dann existieren $a, b \in T$ mit $a \neq b$ und $a \mid b$.
- (3) Seien $a, b \in \mathbb{Z}$, so daß $u := a^2 + b^2$ ungerade ist. Zeige: $u \equiv_4 1$.
- (4) Zeige: Es gibt unendlich viele Primzahlen p mit $p \equiv_4 3$.
- (5) Welche natürlichen Zahlen sind „multiplikativ vollkommen“, d.h. gleich dem Produkt ihrer (positiven) echten Teiler?
- (6) Zeige: Für jedes $n \in \mathbb{N}$ haben die Zahlen n^5 und n , als Dezimalzahlen geschrieben, dieselbe Endziffer.
- (7) Welche $m, n \in \mathbb{N}$ haben die Eigenschaft $(m + n) \mid mn$.
- (8) Zeige: $2^{20} - 1$ ist durch 41 teilbar.
- (9) Bestimme die letzten beiden Ziffern in der Dezimaldarstellung der natürlichen Zahlen 2^{1000} und $9^{(9^9)}$.

Arbeitsblatt zur Elementaren Zahlentheorie

I. Der Satz von EUKLID, daß es unendlich viele Primzahlen gibt, läßt sich auch so formulieren: Der Ring \mathbb{Z} besitzt unendlich viele maximale Ideale. Im folgenden geht es um eine Verallgemeinerung dieser Aussage, die dem Mathematiker KAPLANSKY zugeschrieben wird.

- (1) Zeige: Jeder endliche Integritätsbereich ist ein Körper.

Hinweis: Betrachte die Potenzen eines von Null verschiedenen Elementes, um auf dessen Inverses zu stoßen.

- (2) Sei R ein kommutativer Ring mit 1, und bezeichne mit $\mathcal{M}(R)$ die Menge aller maximalen Ideale von R . Zeige: $R = R^* \cup (\bigcup \mathcal{M}(R))$.

- (3) Sei R ein Integritätsbereich, der nur endlich viele Einheiten und nur endlich viele maximale Ideale besitzt; d.h. R^* und $\mathcal{M}(R)$ seien endlich.

Zeige: Dann ist R ein endlicher Körper.

Hinweis: Nach (1) genügt es, nachzuweisen, daß R endlich ist. Betrachte zunächst den einfachen Fall $\{0\} \in \mathcal{M}(R)$.

Setze dann $\{0\} \notin \mathcal{M}(R)$ voraus. Seien M_1, \dots, M_r die maximalen Ideale von R . Wähle für jedes $i \in \{1, \dots, r\}$ ein $m_i \in M_i \setminus \{0\}$, und definiere die Abbildungen $\varphi_i : M_i \rightarrow R, x \mapsto 1 + m_1 \cdots m_{i-1} x m_{i+1} \cdots m_r$. Zeige, daß für jedes $i \in \{1, \dots, r\}$ die Abbildung φ_i das Ideal M_i injektiv nach R^* überführt. Wende schließlich (2) an.

II. Weitere Knobelaufgaben:

- (1) Finde ein Teilbarkeitskriterium für die Zahl 37.

- (2) Beweise den sogenannten *Chinesischen Restsatz* für den Ring \mathbb{Z} : Sind $a, b \in \mathbb{N}$ zueinander teilerfremd, so besteht der Ringisomorphismus

$$\mathbb{Z}/(ab)\mathbb{Z} \rightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}, \quad x + (ab)\mathbb{Z} \mapsto (x + a\mathbb{Z}, x + b\mathbb{Z}).$$

Hinweis: Überlege zunächst, warum die Abbildung wie angegeben über Repräsentanten definiert werden darf. Benutze dann die Gleichungen $(ab)\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$ und $\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$.

- (3) Bestimme die letzten drei Ziffern in der Dezimaldarstellung der natürlichen Zahl 7^{9999} .

Hinweis: Es gilt $1001 = 7 \cdot 11 \cdot 13$. Überlege, daß $7^{20} \equiv_{125} 1$ ist, und wende den Chinesischen Restsatz an.

Arbeitsblatt zur Elementaren Zahlentheorie

I. Beweise das folgende Lemma (aus der Vorlesung): Zu jedem $a \in \mathbb{Q}^*$ gibt es genau eine quadratfreie Zahl $d \in \mathbb{Z}$ mit $a(\mathbb{Q}^*)^2 = d(\mathbb{Q}^*)^2$.

Berechne konkret für die Restklasse $(25725/2255)(\mathbb{Q}^*)^2$ den zugehörigen quadratfreien Vertreter $d \in \mathbb{Z}$. Bestimme den Isomorphietyp der Quotientengruppe $G := \mathbb{Q}^*/(\mathbb{Q}^*)^2$ und gib ein minimales Erzeugendensystem für G an.

II. Sei $f(z) = az^2 + bz + c \in \mathbb{Z}[z]$ mit $a \neq 0$ irreduzibel über \mathbb{Q} . Bezeichne mit $\alpha, \bar{\alpha} \in \mathbb{C}$ die Nullstellen von f .

Für vorgegebenes $m \in \mathbb{Z}$ interessieren uns die ganzzahligen Lösungen $x, y \in \mathbb{Z}$ der DIOPHANTischen Gleichung

$$(0.1) \quad m = ax^2 + bxy + cy^2.$$

Zeige, daß die Menge aller Teilkörper von \mathbb{C} , die α enthalten, ein eindeutig bestimmtes kleinstes Element besitzt; bezeichne diesen Körper mit $K := \mathbb{Q}(\alpha)$. Weise nach, daß K den Grad 2 über \mathbb{Q} hat, also ein quadratischer Zahlkörper ist.

Die Gleichung (0.1) läßt sich über K auch so schreiben:

$$\frac{m}{a} = (x - \alpha y)(x - \bar{\alpha} y) \quad (x, y \in \mathbb{Z});$$

die Größe auf der rechten Seite ist die sogenannte *Norm* von $x - \alpha y \in K$. Die Menge $M := \mathbb{Z} + \alpha\mathbb{Z} = \{x + \alpha y \mid x, y \in \mathbb{Z}\}$ heißt *vollständiger \mathbb{Z} -Modul* in K ; der Definition nach ist dies tatsächlich ein \mathbb{Z} -Modul. Die Menge $\mathfrak{D}(M) := \{\xi \in K \mid \xi M \subseteq M\}$ wird *Ordnung* zu M in K genannt.

Zeige, daß $\mathfrak{D}(M)$ ein Unterring von K ist, der die 1 enthält, und daß der Quotientenkörper von $\mathfrak{D}(M)$ innerhalb von K gleich K ist.

Betrachte nun konkret $f(z) = z^2 + z + 1$, und berechne $\alpha, \bar{\alpha}$ und $\mathfrak{D}(M)$. Bestimme alle ganzzahligen Lösungen der Gleichung $19 = x^2 + xy + y^2$.

Arbeitsblatt zur Elementaren Zahlentheorie

Auf diesem Arbeitsblatt geht es um grundlegende Begriffe und Sachverhalte aus der Gruppentheorie. Im folgenden sei $G = (G, \cdot)$ stets eine Gruppe.

Sei $H \leq G$ eine Untergruppe von G . Für $g \in G$ bezeichnet $gH = \{gh \mid h \in H\}$ die (Links-)Nebenklasse von H mit Repräsentanten g . Die Menge aller Nebenklassen gH , $g \in G$, wird mit G/H bezeichnet.

- (a) Zeige: G/H bildet eine *Partition* von G , d.h. G ist die disjunkte Vereinigung aller H -Nebenklassen.
- (b) Zeige: Je zwei H -Nebenklassen sind gleich mächtig.
- (c) Unter welcher Bedingung an H läßt sich auf G/H repräsentantenweise eine Gruppenmultiplikation erklären?

Die Anzahl der H -Nebenklassen wird der *Index* von H in G genannt und mit $|G : H|$ bezeichnet.

- (d) Zeige: $|G| = |G : H| \cdot |H|$. Insbesondere gilt der Satz von LAGRANGE: Ist G eine endliche Gruppe und $H \leq G$, so ist $|H|$ ein Teiler von $|G|$.

Sei $S \subseteq G$ eine beliebige Teilmenge von G . Zeige, daß der Durchschnitt aller Untergruppen von G , die S enthalten, wieder eine Untergruppe von G ist; diese Untergruppe wird mit $\langle S \rangle$ bezeichnet und heißt die *von S erzeugte Untergruppe* von G . Ist $S = \{s_1, \dots, s_m\}$, so schreibt man auch $\langle s_1, \dots, s_m \rangle := \langle S \rangle$. Läßt sich G von einem einzigen Element erzeugen, so heißt G *zyklisch*.

- (e) Zeige: Die zyklischen Gruppen sind bis auf Isomorphie genau die Gruppen $\mathbb{Z}/n\mathbb{Z} = (\mathbb{Z}/n\mathbb{Z}, +)$, $n \in \mathbb{N}_0$.
- (f) Ist die Gruppe $(\mathbb{Q}, +)$ endlich erzeugt?
- (g) Sei $n \in \mathbb{N}$. Zeige: Jede Untergruppe von $\mathbb{Z}^n = (\mathbb{Z}^n, +)$ läßt sich von n Elementen erzeugen.

Die *Ordnung* einer Gruppe G ist die Anzahl $|G|$ der Elemente von G . Die *Ordnung* eines Elementes g ist definiert als $\text{ord}(g) := |\langle g \rangle|$.

- (h) Sei $n := |G|$ endlich. Zeige, daß für alle $g \in G$ gilt $g^n = 1$. Insbesondere gilt der kleine Satz von FERMAT: Ist $p \in \mathbb{P}$ und $a \in \mathbb{Z}$ nicht durch p teilbar, so folgt $a^{p-1} \equiv_p 1$.

Arbeitsblatt zur Elementaren Zahlentheorie Weihnachtsedition

Aus einem mathematischen Seminar des hohen Nordens (Kiel) ist folgendes Weihnachtsträtsel überliefert.

Hier ist ein Weihnachtsträtsel, mit dem sich die ganze Familie beschäftigen kann, wenn über die Feiertage 'mal Langeweile aufkommen sollte.

Es geht darum, herauszufinden, in welchem Stall das Christkind geboren wurde. Fünf Ställe liegen in einer Reihe entlang der Straße. Jeder von diesen trägt eine andere Farbe. In jedem Stall wohnt ein anderer Hirte aus einer anderen Landschaft Palästinas. Jeder Stallhirte bevorzugt ein bestimmtes Getränk, benutzt ein bestimmtes Gewürz und hält ein bestimmtes Haustier. Keiner der Hirten trinkt das gleiche Getränk, würzt mit demselben Gewürz oder hält das gleiche Tier wie ein anderer Hirte. Himmlische Botschafter haben die folgenden Hinweise vergeben:

- (1) Das Christkind ist in dem Stall geboren, in dem ein Esel gehalten wird.
- (2) Der galiläische Hirte lebt in einem roten Stall.
- (3) Der smaritanische Hirte hält einen Hund.
- (4) Der judäische Hirte trinkt gerne Tee.
- (5) Der grüne Stall liegt, von der Straße gesehen, links neben dem weißen Stall.
- (6) Der Hirte des grünen Stalles trinkt Fruchtnektar.
- (7) Der Hirte, der mit Nelken würzt, hält einen Vogel.
- (8) Der Hirte, der im mittleren Stall wohnt, trinkt Milch.
- (9) Der Hirte des gelben Stalles würzt mit Pfeffer.
- (10) Der ituräische Hirte wohnt im ersten Stall von links.
- (11) Der Hirte, der mit Koriander würzt, wohnt neben dem, der eine Katze hält.
- (12) Der Hirte, der ein Kamel hält, wohnt neben dem, der mit Pfeffer würzt.
- (13) Der mit Zimt würzt trinkt gerne Wein.
- (14) Der ituräische Hirte wohnt neben dem blauen Stall.
- (15) Der peräische Hirte würzt mit Safran.
- (16) Der mit Koriander würzt hat einen Nachbarn, der Wasser trinkt.

Also, in welchem Stall wurde das Christkind geboren?

Arbeitsblatt zur Elementaren Zahlentheorie

I. Sei $K := \mathbb{Q}(\sqrt{2})$ mit Ganzheitsring $\mathcal{O} = \mathbb{Z}[\sqrt{2}]$. Zeige: Zu jedem $r \in \mathbb{R}$ und $\varepsilon \in \mathbb{R}_{>0}$ gibt es ein $x \in \mathcal{O}$ mit $|r - x| < \varepsilon$. Dies bedeutet anschaulich, daß sich \mathcal{O} schlecht auf der reellen Zahlengeraden einzeichnen läßt.

Betrachte nun die Abbildung $\psi : K \rightarrow \mathbb{R} \times \mathbb{R}$, $a + b\sqrt{2} \mapsto (a + b\sqrt{2}, a - b\sqrt{2})$. Skizziere das Bild von \mathcal{O} unter ψ . Wo liegen in dieser Skizze die Bider der Einheiten $x \in \mathcal{O}^*$?

II. Seien A, B zwei verschiedene Punkte der EUKLIDischen Ebene \mathbb{E} . Sei $S \in \mathbb{E}$ ein dritter Punkt, der auf der Strecke \overline{AB} liege und diese also in zwei Teile, \overline{AS} und \overline{SB} , zerschneide. Bezeichne mit a die Länge von \overline{AS} und mit b die Länge von \overline{SB} . Es gelte $a \geq b$.

Gilt nun $(a + b)/a = a/b$, verhält sich also die Länge der Gesamtstrecke \overline{AB} zur Länge der größeren Teilstrecke \overline{AS} wie die Länge der größeren Teilstrecke \overline{AS} zur Länge der kleineren Teilstrecke \overline{SB} , so nennt man (A, S, B) eine *Konfiguration des goldenen Schnittes*; das Verhältnis $\varphi := a/b$ heißt *goldene Schnittzahl*.

- (1) Zeige, daß $\varphi = (1 + \sqrt{5})/2$ gerade die Grundeinheit zu $\mathbb{Q}(\sqrt{5})$ ist.
- (2) Prüfe nach, daß die folgende Konstruktion mit Zirkel und Lineal eine Konfiguration (A, S, B) des goldenen Schnittes liefert.

Gegeben seien $A, S \in \mathbb{E}$ im Abstand $a > 0$ von einander. Bezeichne mit g die Gerade durch A und S . Errichte in S eine Senkrechte h zu g und bestimme auf dieser einen Punkt $C \in \mathbb{E}$ im Abstand a von S . Konstruiere den Mittelpunkt M von \overline{AS} , und schlage einen Kreis c um M , der durch C führt. Erhalte in demjenigen Schnittpunkt von g und c , der S näher liegt, den gewünschten Punkt B .

- (3) Sei $\mathcal{F} := \overline{P_1P_2P_3P_4P_5}$ ein gleichseitiges Fünfeck mit der Kantenlänge $a > 0$. Bezeichne mit Q den Schnittpunkt der Diagonalen $\overline{P_1P_3}$ und $\overline{P_2P_5}$. Zeige, daß $\overline{QP_3P_4P_5}$ eine Raute ist. (Hinweis: Nutze die Symmetrieachsen von \mathcal{F} , die durch P_1 und P_4 verlaufen.) Wende den Strahlensatz (mit Zentrum Q) an, um zu zeigen, daß (P_5, Q, P_2) eine Konfiguration des goldenen Schnittes bildet. D.h.: „Je zwei Diagonalen in \mathcal{F} treffen sich im goldenen Schnitt.“
- (4) Gebe ein Konstruktionsverfahren mit Zirkel und Lineal für das gleichseitige Fünfeck an.

GAUSS hat diejenigen $n \in \mathbb{N}$, für die das regelmäßige n -Eck mit Zirkel und Lineal konstruierbar ist, genau gekennzeichnet. Dabei treten die FERMATSchen Primzahlen, d.h. Primzahlen der Gestalt $1 + 2^{2^k}$, $k \in \mathbb{N}$ auf. Es ist unbekannt, ob es neben 3, 5, 17, 257 und 65537 noch weitere FERMATSche Primzahlen gibt.

Arbeitsblatt zur Elementaren Zahlentheorie

I (a) Sei $K := \mathbb{Q}(\sqrt{7})$ mit Ganzheitsring $\mathcal{O} = \mathbb{Z}[\sqrt{7}]$. Schreibe $p\mathcal{O}$ als Produkt von Primidealen und bestimme den Faktoring $\mathcal{O}/p\mathcal{O}$ für $p \in \{2, 3, 5, 7, 11\}$. Benutze das Quadratische Reziprozitätsgesetz, um ein allgemeines Kriterium dafür aufzustellen, welche Primzahlen in K zerlegt sind.

(b) Berechne das LEGENDRE-Symbol $\left(\frac{91}{257}\right)$. Was läßt sich also über den Faktoring $\mathbb{Z}[\sqrt{91}]/257\mathbb{Z}[\sqrt{91}]$ sagen?

II Ein kleiner Fragenkatalog als Denkanstoß zur Vorbereitung auf die mündliche Abschlußprüfung:

- (1) Wie lauten die PEANOSchen Axiome für die natürlichen Zahlen? Beweise die Gleichung $\sum_{k=1}^n k^2 = n(n+1)(2n+1)/6$.
- (2) Der Ring der ganzen Zahlen ist ein geordneter Ring. Was bedeutet das? Gib ein Beispiel für einen Ring an, der keine Anordnung besitzt.
- (3) Wie unterscheiden sich prime und unzerlegbare Elemente eines Integritätsbereiches? Wieso ist jedes prime Element unzerlegbar?
- (4) Inwiefern verallgemeinert sich der Satz von der eindeutigen Primfaktorzerlegung in \mathbb{Z} auf andere Ringe, wie z.B. $\mathbb{Z}[\sqrt{-1}]$ oder $\mathbb{Z}[\sqrt{5}]$?
- (5) Nenne ein elementares Teilbarkeitskriterium für das Problem „ $7 \mid N$ “.
- (6) Wieso ist $\mathbb{Z}/m\mathbb{Z}$ ein Körper genau dann, wenn $m \in \mathbb{P}$ ist? Gibt es einen endlichen Körper mit genau 10 Elementen?
- (7) Was ist ein Dedekindring? Gibt verschiedene Beispiele an.
- (8) Was besagt das ZORNSche Lemma und wozu taugt es?
- (9) Wie ist der Ganzheitsring eines quadratischen Zahlkörpers definiert? Bestimme den Ganzheitsring von $\mathbb{Q}(\sqrt{13})$.
- (10) Was läßt sich über die Einheiten und über die Primideale in dem Ganzheitsring von $\mathbb{Q}(\sqrt{13})$ sagen?
- (11) Welches Zerlegungsverhalten hat 101 in $\mathbb{Z}[\sqrt{11}]$?
- (12) Wie heißt das Quadratische Reziprozitätsgesetz und in welchem Zusammenhang steht es mit der Faktorisierung von Idealen in einem quadratischen Zahlkörper? Erläutere dies anhand des Beispiels $\left(\frac{-89}{137}\right)$.

Literaturverzeichnis

- [1] A. BAKER, *A Concise Introduction to the Theory of Numbers* (Cambridge University Press, Cambridge, 1984).
- [2] EBBINGHAUS ET AL., *Zahlen* (Springer-Verlag, Berlin, 1992).
- [3] O. VON GRUDZINSKI UND R. SCHNABEL, *Mathematische Grundlagen* (Mathematisches Seminar der Universität Kiel, Wintersemester 2002/2003).
- [4] F. ISCHEBECK, *Einladung zur Zahlentheorie* (Wissenschaftsverlag, Leipzig, 1992).
- [5] H. KOCH UND H. PIEPER, *Zahlentheorie* (Deutscher Verlag der Wissenschaften, Berlin, 1976).

(Es handelt sich hier um eine kleine Auswahl von Büchern, die mir bei der Vorbereitung der Vorlesung hilfreich waren und die überdies ergänzende Informationen enthalten.)