Zahlentheorie

Prof. Dr. Holger Brenner
Universität Osnabrück
Fachbereich Mathematik/Informatik

Sommersemester 2008

1. Vorlesung

In der Zahlentheorie wollen wir Eigenschaften der ganzen Zahlen verstehen. Dazu ist es sinnvoll, nicht nur $\mathbb{Z}$ selbst zu betrachten, sondern auch davon abgeleitete Objekte, wie Restklassenringe (Modulare Arithmetik), Ringe der ganzen Zahlen in Körpererweiterungen von $\mathbb{Q}$, wie etwa den Ring der Gaussschen Zahlen, Lokalisierungen und Komplettierungen wie die p-adischen Zahlen. Die grundlegende Gemeinsamkeit dieser Objekte ist, dass es sich um kommutative Ringe handelt. Deshalb werden wir von Anfang an die benötigten Begriffe auf der Ringebene entwickeln.

Beispiel 1.1. Betrachten wir die Frage, welche natürlichen Zahlen die Summe von zwei Quadratzahlen sind. Anders formuliert, für welche n hat die Gleichung

$$n = x^2 + y^2$$

Lösungen mit ganzen Zahlen x, y? Es ist

$$\begin{array}{llll} 0 = 0 + 0, & 1 = 1 + 0, & 2 = 1 + 1, & 3, \\ 4 = 4 + 0, & 5 = 4 + 1, & 6, & 7, \\ 8 = 4 + 4, & 9 = 9 + 0, & 10 = 9 + 1, & 11, \\ 12, & 13 = 9 + 4, & 14, & 15, \\ 16, & 17 = 16 + 1, & 18 = 9 + 9, & 19, \\ 20 = 16 + 4. & & & \end{array}$$

Erkennt man hier schon eine Struktur? Es ist in der Zahlentheorie üblich, solche Fragen erstmal für Primzahlen zu verstehen, und die Ergebnisse dann auf zusammengesetzte Zahlen zu übertragen. Von den Primzahlen ≤ 20 sind $3, 7, 11, 19$ keine Summe von zwei Quadraten, während $2, 5, 13$ und 17 es sind. Es fällt auf, dass die erste Reihe alle den Rest 3 bei Division durch 4 haben, und die zweite Reihe (von 2 abgesehen) den Rest 1. Hier zeigt sich bereits, dass es sinnvoll ist, zu anderen Ringen überzugehen, um Fragen über natürliche Zahlen zu beantworten. Die „Division mit Rest“ durch 4 ist ein Ringhomomorphismus

$$\mathbb{Z} \longrightarrow \mathbb{Z}/(4) = \{0, 1, 2, 3\}, n \longmapsto n \mod 4 .$$

Dabei ist in $\mathbb{Z}/(4)$ die Addition und die Multiplikation modulo 4 erklärt, also etwa $3 \cdot 3 = 9 = 1$. Die Abbildung respektiert also die Addition und die Multiplikation. Wenn nun die Gleichung

$$n = x^2 + y^2$$

in $\mathbb{Z}$ eine Lösung besitzt, so liefert das sofort auch eine Lösung modulo 4, nämlich

$$n = x^2 + y^2 \mod 4$$

bzw.

$$(n \mod 4) = (x \mod 4)^2 + (y \mod 4)^2$$

oder

$$\bar{n} = \bar{x}^2 + \bar{y}^2 .$$

Nun sind aber in $\mathbb{Z}/(4)$ die Quadrate einfach $0^2 = 2^2 = 0$ und $1^2 = 3^2 = 1$ und damit sind $0, 1$ und 2 Summe von Quadraten in $\mathbb{Z}/(4)$, aber nicht 3. Es bestätigt sich also bereits die obige Beobachtung, dass natürliche Zahlen (nicht nur Primzahlen), die den Rest 3 modulo 4 haben, nicht die Summe von zwei Quadraten sein können.

Für Primzahlen mit dem Rest 1 modulo 4 liefert die Betrachtung im Restklassenring $\mathbb{Z}/(4)$ natürlich nur, dass eine notwendige Bedingung erfüllt ist, woraus sich natürlich noch lange nicht auf eine Darstellung als Summe von zwei Quadraten schließen lässt. Die Zahl 21 zeigt auch, dass eine Zahl, die modulo 4 den Rest 1 besitzt, nicht selbst die Summe von zwei Quadraten ist. Wir werden aber im Verlauf der Vorlesung sehen, dass es für Primzahlen mit dieser Restbedingung gilt. Dafür werden wir in einem weiteren Ring arbeiten, nämlich im Ring der Gaußschen Zahlen

$$\mathbb{Z}[i] = \mathbb{Z} \oplus \mathbb{Z}i$$

(einem Unterring der komplexen Zahlen). Dort können wir schreiben

$$n = x^2 + y^2 = (x + iy)(x - iy)\,,$$

wodurch die Frage, ob eine Zahl Summe von zwei Quadraten ist, mit der Frage der multiplikativen Zerlegung von natürlichen Zahlen in einem neuen Ring in Zusammenhang gebracht wird.

Wir erinnern kurz an die Definition eines Ringes und eines kommutativen Ringes.

Definition 1.2. Ein *Ring* R ist eine Menge mit zwei Verknüpfungen $+$ und $\cdot$ und mit zwei ausgezeichneten Elementen 0 und 1 derart, dass folgende Bedingungen erfüllt sind:

(1) $(R, +, 0)$ ist eine abelsche Gruppe.
(2) $(R, \cdot, 1)$ ist ein Monoid.
(3) Es gelten die *Distributivgesetze*, also $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ und $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ für alle $a, b, c \in R$.

Definition 1.3. Ein Ring R heißt *kommutativ*, wenn die Multiplikation kommutativ ist.

Das wichtigste Beispiel für uns ist der (kommutative) Ring der ganzen Zahlen $\mathbb{Z}$. Wir werden aber noch viele weitere Ringe kennenlernen, die zahlentheoretisch relevant sind. Wir verwenden wie üblich die Konvention, dass die Multiplikation stärker bindet als die Addition und schreiben in der Regel ab anstatt $a \cdot b$.

Teilbarkeitsbegriffe

Definition 1.4. Sei R ein kommutativer Ring, und a, b Elemente in R. Man sagt, dass a das Element b *teilt* (oder dass b von a geteilt wird, oder dass b ein *Vielfaches* von a ist), wenn es ein $c \in R$ gibt derart, dass $b = c \cdot a$ ist. Man schreibt dafür auch $a|b$.

Lemma 1.5. *(Teilbarkeitsregeln) In einem kommutativen Ring R gelten folgende Teilbarkeitsbeziehungen.*

(1) *Für jedes Element a gilt $1 \mid a$ und $a \mid a$.*
(2) *Für jedes Element a gilt $a \mid 0$.*
(3) *Gilt $a \mid b$ und $b \mid c$, so gilt auch $a \mid c$.*
(4) *Gilt $a \mid b$ und $c \mid d$, so gilt auch $ac \mid bd$.*
(5) *Gilt $a \mid b$, so gilt auch $ac \mid bc$ für jedes $c \in R$.*
(6) *Gilt $a \mid b$ und $a \mid c$, so gilt auch $a \mid rb + sc$ für beliebige Elemente $r, s \in R$.*

Beweis. Siehe Aufgabe 1.2. □

Definition 1.6. Ein Element u in einem kommutativen Ring R heißt *Einheit*, wenn es ein Element $v \in R$ gibt derart, dass $uv = 1$ ist.

Bemerkung 1.7. Eine Einheit ist also ein Element, das die 1 teilt. Das Element v mit der Eigenschaft $uv = 1$ ist dabei eindeutig bestimmt. Hat nämlich auch w die Eigenschaft $uw = 1$, so ist

$$v = v1 = v(uw) = (vu)w = 1w = w.$$

Das im Falle der Existenz eindeutig bestimmte v mit $uv = 1$ nennt man das (multiplikativ) *Inverse* zu u und bezeichnet es mit u^{-1}. Die Menge aller Einheiten in einem kommutativen Ring bilden eine kommutative Gruppe (bzgl. der Multiplikation mit 1 als neutralem Element), die man die *Einheitengruppe* von R nennt. Sie wird mit $R^\times$ bezeichnet.

In den Ringen, die uns bisher begegnet sind, sind die Einheitengruppen einfach zu betimmen. Es ist $\mathbb{Z}^\times = \{1, -1\}$ und $(\mathbb{Z}/(4))^\times = \{1, 3\}$. Im Ring der Gaußschen Zahlen gibt es vier Einheiten: $1, -1, i, -i$, siehe die nächste Vorlesung.

Definition 1.8. Zwei Elemente a und b eines kommutativen Ringes R heißen *assoziiert*, wenn es eine Einheit $u \in R$ gibt derart, dass $a = ub$ ist.

Bemerkung 1.9. Die Assoziiertheit ist eine Äquivalenzrelation. Siehe Aufgabe 1.1.

Das folgende Lemma besagt, dass es für die Teilbarkeitsrelation nicht auf Einheiten und Assoziiertheit ankommt.

Lemma 1.10. *(Einheiten und Teilbarkeit) In einem kommutativen Ring R gelten folgende Teilbarkeitsbeziehungen.*

(1) -1 *ist eine Einheit, die zu sich selbst invers ist.*
(2) *Jede Einheit teilt jedes Element.*
(3) *Sind a und b assoziiert, so gilt $a|c$ genau dann, wenn $b|c$.*
(4) *Teilt a eine Einheit, so ist a selbst eine Einheit.*

Beweis. Siehe Aufgabe 1.3. □

Für Teilbarkeitsuntersuchungen sind die beiden folgenden Begriffe fundamental. Unter bestimmten Voraussetzungen, etwa wenn ein Hauptidealbereich vorliegt, sind sie äquivalent.

Definition 1.11. Eine Nichteinheit p in einem kommutativen Ring heißt *irreduzibel* (oder *unzerlegbar*), wenn eine Faktorisierung $p = ab$ nur dann möglich ist, wenn einer der Faktoren eine Einheit ist.

Definition 1.12. Eine Nichteinheit $p \neq 0$ in einem kommutativen Ring heißt *prim* (oder ein *Primelement*), wenn folgendes gilt: Teilt p ein Produkt ab mit $a, b \in R$, so teilt es einen der Faktoren.

Eine Einheit ist also nach Definition nie ein Primelement. Dies ist eine Verallgemeinerung des Standpunktes, dass 1 keine Primzahl ist. Dabei ist die 1 nicht deshalb keine Primzahl, weil sie „zu schlecht“ ist, sondern weil sie „zu gut“ ist. Vor dem nächsten Lemma erinnern wir an den Begriff des Integritätsbereiches. Häufig wird die Teilbarkeitstheorie nur für Integritätsbereiche entwickelt.

Definition 1.13. Ein kommutativer, nullteilerfreier, von null verschiedener Ring heißt *Integritätsbereich*.

Ein *Nullteiler* ist ein Element x mit der Eigenschaft, dass es ein von null verschiedenes Element y mit $xy = 0$ gibt. Die Null ist in einem von null verschieden Ring stets ein Nullteiler. *Nullteilerfrei* bedeutet, dass die Null der einzige Nullteiler ist bzw. dass alle von null verschiedenen Elemente keine Nullteiler oder *Nichtnullteiler* sind. Nullteilerfrei kann man auch so formulieren, dass aus einer Gleichung $xy = 0$ folgt, dass $x = 0$ oder $y = 0$ ist.

Definition 1.14. Ein kommutativer Ring R heißt *Körper*, wenn $R \neq 0$ ist und wenn jedes von 0 verschiedene Element ein multiplikatives Inverses besitzt.

In einem Körper sind also alle von null verschiedenen Elemente Einheiten (und insbesondere Nichnullteiler). Körper sind also insbesondere Integritätsbereiche. In einem Körper ist die Teilbarkeitsbeziehung uninteressant, da jedes von null verschiedene Element jedes andere Element teilt.

Lemma 1.15. *In einem Integritätsbereich ist ein Primelement stets irreduzibel.*

Beweis. Angenommen, wir haben eine Zerlegung $p = ab$. Wegen der Primeigenschaft teilt p einen Faktor, sagen wir $a = ps$. Dann ist $p = psb$ bzw. $p(1-sb) = 0$. Da p kein Nullteiler ist, folgt $1 = sb$, so dass also b eine Einheit ist. □

2. Vorlesung

Definition 2.1. Eine nichtleere Teilmenge $\mathfrak{a}$ eines kommutativen Ringes R heißt *Ideal*, wenn die beiden folgenden Bedingungen erfüllt sind:

(1) Für alle $a, b \in \mathfrak{a}$ ist auch $a + b \in \mathfrak{a}$.
(2) Für alle $a \in \mathfrak{a}$ und $r \in R$ ist auch $ra \in \mathfrak{a}$.

Bemerkung 2.2. Ein Ideal ist eine Untergruppe der additiven Gruppe von R, die zusätzlich die zweite oben angeführte Eigenschaft erfüllt. Ein Ideal ist das Gleiche wie ein R- Untermodul von R.

Definition 2.3. Zu einer Familie von Elementen $a_j \in R$, $j \in J$, in einem kommutativen Ring R bezeichnet $(a_j : j \in J)$ das von den a_j *erzeugte Ideal*. Es besteht aus allen (endlichen) *Linearkombinationen*

$$\sum_{j \in J_0} r_j a_j \,,$$

wobei $J_0 \subseteq J$ eine endliche Teilmenge und $r_j \in R$ ist.

Definition 2.4. Ein Ideal $\mathfrak{a}$ in einem kommutativen Ring R der Form

$$\mathfrak{a} = (a) = Ra = \{ra : \, r \in R\}.$$

heißt *Hauptideal*.

Mit dem Idealbegriff lassen sich Teilbarkeitsbeziehungen ausdrücken.

Lemma 2.5. *Sei R ein kommutativer Ring und $a, b \in R$. Dann gelten folgende Aussagen.*

(1) *Das Element a ist ein Teiler von b (also $a|b$), genau dann, wenn $(b) \subseteq (a)$.*
(2) *a ist eine Einheit genau dann, wenn $(a) = R = (1)$.*
(3) *Ist R ein Integritätsbereich, so gilt $(a) = (b)$ genau dann, wenn a und b assoziiert sind.*

Beweis. Siehe Aufgabe 2.4. □

Definition 2.6. Ein kommutativer Ring, in dem jedes Ideal ein Hauptideal ist, heißt *Hauptidealring*. Ein integrer Hauptidealring heißt *Hauptidealbereich*.

Größter gemeinsamer Teiler

Definition 2.7. Sei R ein kommutativer Ring und $a_1, \ldots, a_k \in R$. Dann heißt ein Element $t \in R$ *gemeinsamer Teiler* der $a_1, \ldots, a_k$, wenn t jedes a_i teilt ($i = 1, \ldots, k$). Ein Element $g \in R$ heißt *größter gemeinsamer Teiler* der $a_1, \ldots, a_k$, wenn g ein gemeinsamer Teiler ist und wenn jeder gemeinsame Teiler t dieses g teilt.

Die Elemente $a_1, \ldots, a_k$ heißen *teilerfremd*, wenn 1 ihr größter gemeinsamer Teiler ist.

Bemerkung 2.8. Eine Einheit ist immer ein gemeinsamer Teiler für jede Auswahl von Elementen. Ein größter gemeinsamer Teiler muss nicht existieren im Allgemeinen. Ist t ein gemeinsamer Teiler der $a_1, \ldots, a_k$ und u eine Einheit, so ist auch ut ein gemeinsamer Teiler der $a_1, \ldots, a_k$. Die Elemente $a_1, \ldots, a_k$ sind *teilerfremd* genau dann, wenn jeder gemeinsame Teiler davon eine Einheit ist (es gibt noch andere Definitionen von teilerfremd, die nicht immer inhaltlich mit dieser übereinstimmen).

Lemma 2.9. *Sei R ein kommutativer Ring, $a_1, \ldots, a_k \in R$ und $\mathfrak{a} = (a_1, \ldots, a_k)$ das davon erzeugte Ideal. Ein Element $t \in R$ ist ein gemeinsamer Teiler von $a_1, \ldots, a_k \in R$ genau dann, wenn $\mathfrak{a} \subseteq (t)$ ist, und t ist ein größter gemeinsamer Teiler genau dann, wenn für jedes $s \in R$ mit $\mathfrak{a} \subseteq (s)$ folgt, dass $(t) \subseteq (s)$ ist. Ein größter gemeinsamer Teiler erzeugt also ein minimales Hauptoberideal von $\mathfrak{a}$.*

Beweis. Aus $\mathfrak{a} = (a_1, \ldots, a_k) \subseteq (t)$ folgt sofort $(a_i) \subseteq (t)$ für $i = 1, \ldots, k$, was gerade bedeutet, dass t diese Elemente teilt, also ein gemeinsamer Teiler ist. Sei umgekehrt t ein gemeinsamer Teiler. Dann ist $a_i \in (t)$ und da $\mathfrak{a} = (a_1, \ldots, a_k)$ das kleinste Ideal ist, das alle a_i enthält, muss $\mathfrak{a} \subseteq (t)$ gelten. Der zweite Teil folgt sofort aus dem ersten. □

Bevor wir mit der Teilbarkeitstheorie für Hauptidealbereiche fortfahren, wollen wir zunächst zeigen, dass die ganzen Zahlen einen Hauptidealbereich bilden. Dies geschieht über den Begriff des Euklidischen Bereiches, der an die Division mit Rest anknüpft. Im Ring der ganzen Zahlen gilt die Division mit Rest. Ihre Bedeutung liegt grob gesprochen darin, dass sie ein Maß dafür liefert, wie weit eine Zahl davon entfernt ist, eine andere zu teilen.

Division mit Rest

Für ganze Zahlen a, b, $b \neq 0$, gibt es (eindeutig bestimmte) ganze Zahlen q, r mit

$$a = qb + r \text{ und } 0 \leq r < |b| .$$

Dabei bezeichnet $|\ |$ den Betrag einer ganzen Zahl. Das Symbol q soll dabei an Quotient erinnern und r an Rest. Teilt man die Gleichung durch b, so erhält man in $\mathbb{Q}$ die Beziehung

$$\frac{a}{b} = q + \frac{r}{b} \text{ mit } q \in \mathbb{Z} \text{ und } 0 \leq \frac{r}{b} < 1\,.$$

Definition 2.10. Ein *euklidischer Bereich* (oder *euklidischer Ring*) ist ein Integritätsbereich R, für den eine Abbildung $\delta : R - \{0\} \to \mathbb{N}$ existiert, die die folgende Eigenschaft erfüllt:

Für Elemente a, b mit $b \neq 0$ gibt es $q, r \in R$ mit

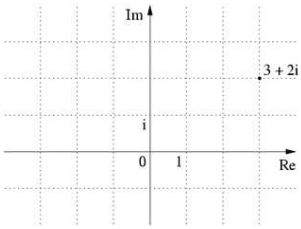
$$a = qb + r \text{ und } r = 0 \text{ oder } \delta(r) < \delta(b)\,.$$

Die in der Definition auftauchende Abbildung δ nennt man auch *euklidische Funktion*. Die ganzen Zahlen $\mathbb{Z}$ bilden also einen euklidischen Ring mit dem Betrag als euklidischer Funktion.

Beispiel 2.11. Für einen Körper K ist der Polynomring $K[X]$ in einer Variablen ein euklidischer Bereich, wobei die euklidische Funktion δ durch die Gradfunktion gegeben ist. Viele Parallelen zwischen dem Polynomring $K[X]$ und $\mathbb{Z}$ beruhen auf dieser Eigenschaft. Die Gradfunktion hat die Eigenschaft

$$\delta(fg) = \delta(f) + \delta(g)\,.$$

Beispiel 2.12.



Gaußsche Zahlen als Gitterpunkte in der komplexen Zahlenebene

Eine Gaußsche Zahl z ist durch $z = a + b\mathrm{i}$ gegeben, wobei a und b ganze Zahlen sind. Die Menge dieser Zahlen wird mit $\mathbb{Z}[\mathrm{i}]$ bezeichnet. Die Gaußschen Zahlen sind die Gitterpunkte, d.h. die Punkte mit ganzzahligen Koordinaten, in der komplexen Ebene. Sie bilden mit komponentenweiser Addition und mit der induzierten komplexen Multiplikation einen kommutativen Ring.

Eine euklidische Funktion ist durch die Norm N gegeben, die durch $N(a + b\mathrm{i}) := a^2 + b^2$ definiert ist. Man kann auch schreiben $N(z) = z \cdot \bar{z}$, wobei $\bar{z}$ die komplexe Multiplikation bezeichnet. Die Norm ist das Quadrat des komplexen Absolutbetrages und wie dieser multiplikativ, also $N(zw) = N(z)N(w)$.

Mit der Norm lassen sich auch leicht die Einheiten von $\mathbb{Z}[\mathrm{i}]$ bestimmen: ist $wz = 1$, so ist auch $N(zw) = N(z)N(w) = 1$, also $N(z) = +/-1$. Damit sind genau die Elemente $\{1, -1, \mathrm{i}, -\mathrm{i}\}$ diejenigen Gaußschen Zahlen, die Einheiten sind.

Lemma 2.13. *Der Ring der Gaußschen Zahlen ist mit der Normfunktion ein euklidischer Bereich.*

Beweis. Seien $w, z \in \mathbb{Z}[i]$, $z \neq 0$. Wir betrachten den Quotienten

$$\frac{w}{z} = \frac{w\bar{z}}{z\bar{z}} = q_1 + q_2 i\,.$$

Dies ist eine komplexe Zahl mit rationalen Koeffizienten, also $q_1, q_2 \in \mathbb{Q}$. Es gibt ganze Zahlen a_1, a_2 mit $|q_1 - a_1|, |q_2 - a_2| \leq 1/2$. Damit ist

$$q_1 + q_2 i = a_1 + a_2 i + (q_1 - a_1) + (q_2 - a_2)i$$

mit $a_1 + a_2 i \in \mathbb{Z}[i]$. Ferner ist

$$N((q_1 - a_1) + (q_2 - a_2)i) \leq (\frac{1}{2})^2 + (\frac{1}{2})^2 < 1\,.$$

Multiplikation mit z ergibt

$$w = z(a_1 + a_2 i) + z((q_1 - a_1) + (q_2 - a_2)i)$$

und aus der Multiplikativität der Norm folgt

$$N(z((q_1 - a_1) + (q_2 - a_2)i)) = N(z)N((q_1 - a_1) + (q_2 - a_2)i) < N(z)\,.$$

□

Folgendes Lemma hilft bei der Bestimmung der Primelemente der Gaußschen Zahlen und in ähnlichen Ringen.

Lemma 2.14. *Sei R ein euklidischer Bereich mit einer multiplikativen euklidischen Funktion $N : R - \{0\} \longrightarrow \mathbb{N}_+$ (es werden also nur positive Werte angenommen). Ist dann für $f \in R$ die Zahl $N(f)$ prim, so ist f irreduzibel in R.*

Beweis. Sei $f = gh$ eine Faktorzerlegung. Dann ist $N(f) = N(g)N(h)$ und da nach Voraussetzung $N(f)$ eine Primzahl ist, folgt, dass einer der Faktoren, sagen wir $N(h)$, eine Einheit ist, also $N(h) = 1$. Wir wenden auf 1 und h die Division mit Rest an und erhalten

$$1 = qh + r\,,$$

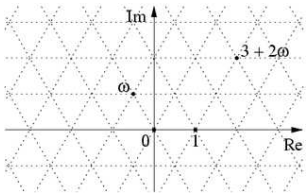
wobei $r = 0$ ist oder $N(r) < N(h) = 1$. Letzteres ist aber ausgeschlossen, so dass $r = 0$ sein muss und damit ist h eine Einheit. Also ist f irreduzibel. □

Wir werden später sehen, dass in euklidischen Bereichen irreduzible Elemente bereits prim sind. Das vorstehende Lemma ist also ein Kriterium für Primelemente. Die Umkehrung gilt übrigens nicht. Z. B. ist 3 ein Primelement in $\mathbb{Z}[i]$, aber $N(3) = 9$ ist keine Primzahl.

Nach den Gaußschen Zahlen sind die sogenannten Eisenstein-Zahlen ein wichtiges Beispiel für quadratische Zahlbereiche.

Gotthold Eisenstein (1823 Berlin - 1852 Berlin)

Beispiel 2.15.



Eisenstein-Zahlen als Punkte eines Dreiecksgitters in der komplexen Zahleneben

Die Eisenstein-Zahlen sind komplexe Zahlen der Form

$$z = a + b(\frac{1}{2} + \frac{\mathrm{i}}{2}\sqrt{3})$$

mit ganzen Zahlen a und b. Insbesondere ist

$$\omega = -\frac{1}{2} + \frac{\mathrm{i}}{2}\sqrt{3} = e^{2\pi \mathrm{i}/3}$$

eine Eisenstein-Zahl. Diese Zahl ist zugleich eine (primitive) dritte Einheitswurzel (also $\omega^3 = 1$), so dass der Ring der Eisenstein-Zahlen zugleich der dritte Kreisteilungsring ist. Wegen $\omega^3 - 1 = (\omega - 1)(\omega^2 + \omega + 1)$ und $\omega \neq 1$ gilt die Gleichung

$$\omega^2 + \omega + 1 = 0\,.$$

Die Eisenstein-Zahlen enthalten den Ring $\mathbb{Z}[\sqrt{-3}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{-3}$. Im obigen Bild besteht dieser Ring aus jeder zweiten horizontalen Zeile des Gitters und ist damit ein rechtwinkliges Gitter. Es gilt der folgende Satz.

Satz 2.16. *Für den Ring $\mathbb{Z}[\sqrt{-3}]$ ist die Norm (das Quadrat des komplexen Betrages) keine euklidische Funktion, aber für den Ring der Eisenstein-Zahlen $\mathbb{Z}[\omega]$ mit $\omega = \frac{-1+\sqrt{3}i}{2}$ ist die Norm eine euklidische Funktion.*

Beweis. Wie dem Beweis zur Euklidizität der Gaußschen Zahlen zu entnehmen ist, ist für einen Unterring der komplexen Zahlen der Form $\Gamma = \mathbb{Z} \oplus \mathbb{Z}x$

(mit $x \notin \mathbb{R}$) die Norm eine euklidische Funktion genau dann, wenn sich zu jedem Element $z \in \mathbb{Q}(\Gamma) = \mathbb{Q} \oplus \mathbb{Q}x$ ein Element $u \in \Gamma$ findet, das zu z einen Abstand kleiner als 1 besitzt. Sei zunächst $\Gamma = \mathbb{Z} \oplus \mathbb{Z}\sqrt{-3}$. Das Element $\omega = \frac{-1+\sqrt{-3}}{2} \in \mathbb{Q}(\Gamma)$ hat den minimalen Abstand zu den vier Gitterpunkten $(0,0), (-1,0), (0,\sqrt{3}), (-1,\sqrt{3})$, und dieser ist stets

$$|\frac{-1+\sqrt{-3}}{2}| = \sqrt{\frac{1}{4}+\frac{3}{4}} = 1\,.$$

Für den Ring der Eisenstein-Zahlen $\mathbb{Z}[\omega]$ sind die Gittermaschen gleichmäßige Dreiecke mit Seitenlänge eins, und jede komplexe Zahl hat zu mindestens einem Gitterpunkt einen Abstand < 1. □

Es lässt sich zeigen, dass der Ring $\mathbb{Z}[\sqrt{-3}]$ auch keine andere euklidische Funktion besitzt (er ist auch kein Hauptidealbereich, noch nicht mal, wie wir später sehen und erklären werden, normal).

Eine wichtige Konsequenz aus der Existenz einer euklidischen Funktion ist, dass ein Hauptidealbereich vorliegt.

Satz 2.17. *Ein euklidischer Bereich ist ein Hauptidealbereich.*

Beweis. Sei I ein von null verschiedenes Ideal. Betrachte die nicht-leere Menge

$$\{\delta(a) : a \in I, a \neq 0\}\,.$$

Diese Menge hat ein Minimum m, das von einem Element $b \in I, b \neq 0$ herrührt, sagen wir $m = \delta(b)$. Wir behaupten, dass $I = (b)$ ist. Sei hierzu $a \in I$ gegeben. Aufgrund der Definition eines euklidischen Bereiches gilt $a = qb + r$ mit $r = 0$ oder $\delta(r) < \delta(b)$. Wegen $r \in I$ und der Minimalität von $\delta(b)$ kann der zweite Fall nicht eintreten. Also ist $r = 0$ und a ist ein Vielfaches von b. □

3. Vorlesung

Der euklidische Algorithmus

Euklid (4. Jahrhundert v. C.)

Definition 3.1. Seien zwei Elemente a, b (mit $b \neq 0$) eines euklidischen Bereichs R mit euklidischer Funktion δ gegeben. Dann nennt man die durch die Anfangsbedingungen $r_0 = a$ und $r_1 = b$ und die mittels der Division mit Rest

$$r_i = q_i r_{i+1} + r_{i+2}$$

rekursiv bestimmte Folge r_i die *Folge der euklidischen Reste.*

Satz 3.2. *Seien zwei Elemente $r_0 = a, r_1 = b \neq 0$ eines euklidischen Bereichs R mit euklidischer Funktion δ gegeben. Dann besitzt die Folge r_i, $i = 0, 1, 2, \ldots$, der euklidischen Reste folgende Eigenschaften.*

(1) *Es ist $r_{i+2} = 0$ oder $\delta(r_{i+2}) < \delta(r_{i+1})$.*
(2) *Es gibt ein (minimales) $k \geq 2$ mit $r_k = 0$.*
(3) *Es ist* $\mathrm{ggT}(r_{i+1}, r_i) = \mathrm{ggT}(r_i, r_{i-1})$.
(4) *Sei $k \geq 2$ der erste Index derart, dass $r_k = 0$ ist. Dann ist*

$$\mathrm{ggT}(a, b) = r_{k-1}\,.$$

Beweis. (1) Dies folgt unmittelbar aus der Definition der Division mit Rest.
(2) Solange $r_i \neq 0$ ist, wird die Folge der natürlichen Zahlen $\delta(r_i)$ immer kleiner, so dass irgendwann der Fall $r_i = 0$ eintreten muss.
(3) Wenn t ein gemeinsamer Teiler von r_{i+1} und von r_{i+2} ist, so zeigt die Beziehung

$$r_i = q_i r_{i+1} + r_{i+2}\,,$$

dass t auch ein Teiler von r_i und damit ein gemeinsamer Teiler von r_{i+1} und von r_i ist. Die Umkehrung folgt genauso.
(4) Dies folgt aus (3) mit der Gleichungskette

$$\begin{aligned}\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r_2) = \mathrm{ggT}(r_2, r_3) = \ldots = \mathrm{ggT}(r_{k-2}, r_{k-1}) \\ = \mathrm{ggT}(r_{k-1}, r_k) = \mathrm{ggT}(r_{k-1}, 0) = r_{k-1}.\end{aligned}$$

□

Als Beispiel zum euklidischen Algorithmus lösen wir die folgende Aufgabe.

Aufgabe: Bestimme in $\mathbb{Z}$ mit Hilfe des euklidischen Algorithmus den größten gemeinsamen Teiler von 1071 und 1029.

Lösung:

Der größte gemeinsame Teiler von 1071 und 1029 wird mit dem euklidischen Algorithmus wie folgt berechnet:

$$1071 = 1 \cdot 1029 + 42$$

$$1029 = 24 \cdot 42 + 21$$

$$42 = 2 \cdot 21 + 0$$

Der größte gemeinsame Teiler von 1071 und 1029 ist somit 21.

Aufgabe: Bestimme in $\mathbb{Z}[\mathrm{i}]$ mit Hilfe des euklidischen Algorithmus den größten gemeinsamen Teiler von $7+4\mathrm{i}$ und $5+3\mathrm{i}$.

Lösung:

Wir setzen $a = 7+4\mathrm{i}$ und $b = 5+3\mathrm{i}$ und führen die Division mit Rest a/b durch. Es ist (in $\mathbb{C}$)

$$\frac{a}{b} = \frac{7+4\mathrm{i}}{5+3\mathrm{i}} = \frac{(7+4\mathrm{i})(5-3\mathrm{i})}{(5+3\mathrm{i})(5-3\mathrm{i})} = \frac{47-\mathrm{i}}{34} = \frac{47}{34} - \frac{1}{34}\mathrm{i}\,.$$

Die beste Approximation für diese komplexe Zahl mit einer ganzen Gaußschen Zahl ist 1, so dass die Division mit Rest ergibt:

$$a = 1 \cdot b + r \text{ mit } r = a - b = 2 + \mathrm{i}\,.$$

Die nächste durchzuführende Division ist somit

$$\frac{b}{r} = \frac{5+3\mathrm{i}}{2+\mathrm{i}} = \frac{(5+3\mathrm{i})(2-\mathrm{i})}{(2+\mathrm{i})(2-\mathrm{i})} = \frac{13+\mathrm{i}}{5} = \frac{13}{5} + \frac{1}{5}\mathrm{i}\,.$$

Die beste Approximation für diese komplexe Zahl mit einer ganzen Gaußschen Zahl ist 3, so dass die Division mit Rest ergibt:

$$b = 3 \cdot r + s \text{ mit } s = b - 3r = 5 + 3\mathrm{i} - 3(2+\mathrm{i}) = -1\,.$$

Da dies eine Einheit ist, sind $a = 7+4\mathrm{i}$ und $b = 5+3\mathrm{i}$ teilerfremd.

Satz 3.3. *(Lemma von Bezout) Sei R ein Hauptidealring. Dann gilt:*

Elemente $a_1, \ldots, a_n$ besitzen stets einen größten gemeinsamen Teiler d, und dieser lässt sich als Linearkombination der $a_1, \ldots, a_n$ darstellen, d.h. es gibt Elemente $r_1, \ldots, r_n \in R$ mit $r_1a_1 + r_2a_2 + \ldots + r_na_n = d$.

Insbesondere besitzen teilerfremde Elemente $a_1, \ldots, a_n$ eine Darstellung der 1.

Beweis. Sei $I = (a_1, \ldots, a_n)$ das von den Elementen erzeugte Ideal. Da wir in einem Hauptidealring sind, handelt es sich um ein Hauptideal; es gibt also ein Element d mit $I = (d)$. Wir behaupten, dass d ein größter gemeinsamer Teiler der $a_1, \ldots, a_n$ ist. Die Inklusionen $(a_i) \subseteq I = (d)$ zeigen, dass es sich um einen gemeinsamen Teiler handelt. Sei e ein weiterer gemeinsamer Teiler der $a_1, \ldots, a_n$. Dann ist wieder $(d) = I \subseteq (e)$, was wiederum $e|d$ bedeutet. Die Darstellungsaussage folgt unmittelbar aus $d \in I = (a_1, \ldots, a_n)$.

Im teilerfremden Fall ist $I = (a_1, \ldots, a_n) = R$. □

Lemma 3.4. *(von Euklid) Sei R ein Hauptidealbereich und $a, b, c \in R$. Es seien a und b teilerfremd und a teile das Produkt bc. Dann teilt a den Faktor c.*

Beweis. Da a und b teilerfremd sind, gibt es nach Lemma von Bezout (Lemma 3.3) Elemente $r, s \in R$ mit $ra+sb = 1$. Die Voraussetzung, dass a das Produkt

bc teilt, schreiben wir als $bc = da$. Damit gilt

$$c = c1 = c(ra + sb) = cra + csb = a(cr + ds),$$

was zeigt, dass c ein Vielfaches von a ist. □

Satz 3.5. *Sei R ein Hauptidealbereich. Dann ist ein Element genau dann prim, wenn es irreduzibel ist.*

Beweis. Ein Primelement in einem Integritätsbereich ist nach Lemma 1.15 stets irreduzibel. Sei also umgekehrt p irreduzibel, und nehmen wir an, dass p das Produkt ab teilt, sagen wir $pc = ab$. Nehmen wir an, dass a kein Vielfaches von p ist. Dann sind aber a und p teilerfremd, da eine echte Inklusionskette $(p) \subset (p, a) = (d) \subset R$ der Irreduzibilität von p widerspricht. Damit teilt p nach Lemma 3.4 den anderen Faktor b. □

Lemma 3.6. *In einem Hauptidealbereich lässt sich jede Nichteinheit $a \neq 0$ darstellen als Produkt von irreduziblen Elementen.*

Beweis. Angenommen, jede Zerlegung $a = p_1 \cdots p_k$ enthalte nicht irreduzible Elemente. Dann gibt es in jedem solchen Produkt einen Faktor, der ebenfalls keine Zerlegung in irreduzible Faktoren besitzt. Wir erhalten also eine unendliche Kette $a_1 = a, a_2, a_3, \ldots$, wobei a_{n+1} ein nicht-trivialer Teiler von a_n ist. Somit haben wir eine echt aufsteigende Idealkette

$$(a_1) \subset (a_2) \subset (a_3) \subset \ldots .$$

Die Vereinigung dieser Ideale ist aber ebenfalls ein Ideal und nach Voraussetzung ein Hauptideal. Dies ist ein Widerspruch. □

Satz 3.7. *In einem Hauptidealbereich lässt sich jede Nichteinheit $a \neq 0$ darstellen als Produkt von Primelementen. Diese Darstellung ist eindeutig bis auf Reihenfolge und Assoziiertheit. Wählt man aus jeder Assoziiertheitsklasse von Primelementen einen festen Repräsentanten p, so gibt es eine bis auf die Reihenfolge eindeutige Darstellung $a = u \cdot p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$, wobei u eine Einheit ist und die p_i Repräsentanten sind.*

Beweis. Die erste Aussage folgt direkt aus Lemma 3.6 und Satz 3.5.

Die behauptete Eindeutigkeit bis auf Umordnung bedeutet, dass wenn

$$a = u \cdot p_1 \cdots p_k = v \cdot q_1 \cdots q_m \qquad (*)$$

zwei Primfaktorzerlegungen sind, dass dann $k = m$ ist und es eine Permutation τ auf $\{1, \ldots, k\}$ gibt derart, dass p_i und $q_{\tau(i)}$ assoziiert sind für alle $i \in \{1, \ldots, k\}$. Wir beweisen diese Aussage durch Induktion über k. Sei zuerst $k = 0$ (das sei zugelassen). Dann steht links eine Einheit, also muss auch rechts eine Einheit stehen, was $m = 0$ bedeutet.

Sei also $k > 0$ und die Aussage sei für alle kleineren k bewiesen. Die Gleichung $(*)$ bedeutet insbesondere, dass p_k das Produkt rechts teilt. Da p_k prim ist, muss p_k einen der Faktoren rechts teilen. Nach Umordnung kann

man annehmen, dass q_m von p_k geteilt wird. Da q_m ebenfalls prim ist, sind q_m und p_k assoziiert. Also ist $q_m = wp_k$ mit einer Einheit w und man kann die Gleichung $(*)$ nach p_k kürzen und erhält

$$u \cdot p_1 \cdots p_{k-1} = (vw) \cdot q_1 \cdots q_{m-1} .$$

Die Induktionsvoraussetzung liefert dann $k - 1 = m - 1$. □

Diesen Satz kann man auch so ausdrücken, dass Hauptidealbereiche faktoriell sind im Sinne der folgenden Definition. Für solche Bereiche gilt ganz allgemein, dass die Primfaktorzerlegung eindeutig ist.

Definition 3.8. Ein Integritätsbereich heißt *faktorieller Bereich*, wenn folgende beiden Eigenschaften erfüllt sind.

(1) Jedes irreduzible Element in R ist prim.
(2) Jedes Element $a \in R$, $a \neq 0$, ist ein Produkt aus irreduziblen Elementen.

Korollar 3.9. *Jede positive natürliche Zahl lässt sich eindeutig als Produkt von Primzahlen darstellen.*

Beweis. Dies folgt sofort aus Satz 3.7. □

Korollar 3.10. *Sei R ein Hauptidealbereich und seien a und b zwei Elemente $\neq 0$ mit Primfaktorzerlegungen*

$$a = u \cdot p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k} \text{ und } b = v \cdot p_1^{s_1} \cdot p_2^{s_2} \cdots p_k^{s_k}$$

(wobei die Exponenten auch null sein können). Dann gilt $a|b$ genau dann, wenn $r_i \leq s_i$ ist für alle Exponenten $i = 1, \ldots, k$.

Beweis. Wenn die Exponentbedingung erfüllt ist, so ist $s_i - r_i \geq 0$ und man kann schreiben

$$b = vu^{-1} p_1^{s_1 - r_1} \cdots p_k^{s_k - r_k} ,$$

was die Teilbarkeit bedeutet. Die Umkehrung folgt aus der Eindeutigkeit der Primfaktorzerlegung in Hauptidealbereichen (siehe Satz 3.7). □

Satz 3.11. *Sei R ein Hauptidealbereich und $p \neq 0$ ein Element. Dann sind folgende Bedingungen äquivalent.*

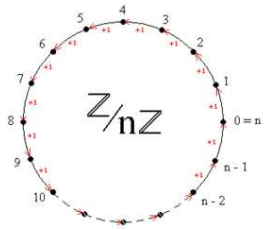
(1) *p ist ein Primelement.*
(2) *$R/(p)$ ist ein Integritätsbereich.*
(3) *$R/(p)$ ist ein Körper.*

Beweis. Die Äquivalenz (1) $\Leftrightarrow$ (2) gilt in jedem kommutativen Ring (auch für $p = 0$), und (3) impliziert natürlich (2). Sei also (1) erfüllt und sei $a \in R/(p)$ von null verschieden. Wir bezeichnen einen Repräsentanten davon in R ebenfalls mit a. Es ist dann $a \notin (p)$ und es ergibt sich eine echte Idealinklusion

$(p) \subset (a,p)$. Ferner können wir schreiben $(a,p) = (b)$, da wir in einem Hauptidealring sind. Es folgt $p = cb$. Da c keine Einheit ist und p prim (also irreduzibel) ist, muss b eine Einheit sein. Es ist also $(a,p) = (1)$, und das bedeutet modulo p, also in $R/(p)$, dass a eine Einheit ist. Also ist $R/(p)$ ein Körper. □

4. Vorlesung

Die Restklassenringe $\mathbb{Z}/(n)$



Satz 4.1. *(Einheiten modulo n) Genau dann ist $a \in \mathbb{Z}$ eine Einheit modulo n (d.h. a repräsentiert eine Einheit in $\mathbb{Z}/(n)$) wenn a und n teilerfremd sind.*

Beweis. Sind a und n teilerfremd, so gibt es nach Lemma von Bezout (Lemma 3.3) eine Darstellung der 1, es gibt also natürliche Zahlen r, s mit $ra+sn = 1$. Betrachtet man diese Gleichung modulo n, so ergibt sich $ra = 1$ in $\mathbb{Z}/(n)$. Damit ist a eine Einheit mit Inversem $a^{-1} = r$.

Ist umgekehrt a eine Einheit in $\mathbb{Z}/(n)$, so gibt es ein $r \in \mathbb{Z}/(n)$ mit $ar = 1$ in $\mathbb{Z}/(n)$. Das bedeutet aber, dass $ar - 1$ ein Vielfaches von n ist, so dass also $ar - 1 = sn$ gilt. Dann ist aber wieder $ar - sn = 1$ und a und n sind teilerfremd. □

Korollar 4.2. *Der Restklassenring $\mathbb{Z}/(n)$ ist genau dann ein Körper, wenn n eine Primzahl ist.*

Beweis. Die Zahl n ist genau dann prim, wenn sie teilerfremd zu jeder Zahl a, $0 < a < n$, ist. Dies ist nach Lemma zu modularen Einheiten (Satz 4.1) genau dann der Fall, wenn in $\mathbb{Z}/(n)$ jedes von null verschiedene Element eine Einheit ist. □

Leonhard Euler (1707-1783)

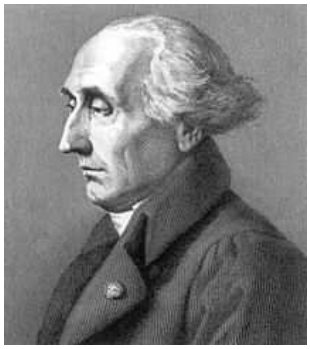
Definition 4.3. Zu einer natürlichen Zahl n bezeichnet $\varphi(n)$ die Anzahl der Elemente von $(\mathbb{Z}/(n))^\times$. Man nennt $\varphi(n)$ die *Eulersche Funktion.*

Bemerkung 4.4. Die Eulersche Funktion $\varphi(n)$ gibt also (nach Lemma zu modularen Einheiten (Satz 4.1)) an, wie viele Zahlen r, $0 < r < n$, zu n teilerfremd sind.

Satz 4.5. *(Euler) Sei n eine natürliche Zahl. Dann gilt für jede zu n teilerfremde Zahl a die Beziehung*

$$a^{\varphi(n)} = 1 \mod n\,.$$

Beweis. Das Element a gehört zur Einheitengruppe $(\mathbb{Z}/(n))^\times$, die $\varphi(n)$ Elemente besitzt. Nach Satz von Lagrange ist aber die Gruppenordnung ein Vielfaches der Ordnung des Elementes. □



Joseph-Louis Lagrange (1736 Turin - 1813 Paris)

Als Spezialfall erhalten wir den sogenannten kleinen Fermatschen Satz:

Lemma 4.6. *(Kleiner Fermat) Für eine Primzahl p und eine beliebige ganze Zahl a gilt*

$$a^p \equiv a \mod p\,.$$

Anders ausgedrückt: $a^p - a$ ist durch p teilbar.

Beweis. Ist a nicht durch p teilbar, so definiert a ein Element $\bar{a}$ in der Einheitengruppe $(\mathbb{Z}/p)^\times$; diese Gruppe hat die Ordnung $\varphi(p) = p-1$, und nach

Satz von Lagrange gilt $\bar{a}^{p-1} = 1$. Durch Multiplikation mit a ergibt sich die Behauptung. Für Vielfache von p gilt die Aussage ebenso, da dann beidseitig null steht. □

Pierre de Fermat (1607/08-1665)

Beispiel 4.7. Sei beispielsweise $p = 5$. Dann ist für

$$\begin{aligned} a = 1 &: 1^5 = 1 \mod 5 \\ a = 2 &: 2^5 = 32 = 2 \mod 5 \\ a = 3 &: 3^5 = 243 = 3 \mod 5 \\ a = 4 &: 4^5 = 1024 = 4 \mod 5\,. \end{aligned}$$

Definition 4.8. Ein Körper heißt *endlich*, wenn er nur endlich viele Elemente besitzt.

Satz 4.9. *Sei K ein endlicher Körper. Dann ist das Produkt aller von 0 verschiedener Elemente aus K gleich -1.*

Beweis. Die Gleichung $x^2 = 1$ hat in einem Körper nur die Lösungen 1 und -1, die allerdings gleich sein können. Das bedeutet, dass für $x \neq 1, -1$ immer $x \neq x^{-1}$ ist. Damit kann man das Produkt aller Einheiten schreiben als

$$1(-1)x_1x_1^{-1}\cdots x_kx_k^{-1}\,.$$

Ist $-1 \neq 1$, so ist das Produkt -1. Ist hingegen $-1 = 1$, so fehlt in dem Produkt der zweite Faktor und das Produkt ist $1 = -1$. □

Korollar 4.10. *(Wilson) Sei p eine Primzahl. Dann ist*

$$(p-1)! = -1 \mod p\,.$$

Beweis. Dies folgt unmittelbar aus Satz 4.9, da ja die Fakultät durch alle Zahlen zwischen 1 und $p-1$ läuft, also durch alle Einheiten im Restklassenkörper $\mathbb{Z}/(p)$. □

Wir wollen im folgenden die Struktur der Restklassenringe $\mathbb{Z}/(n)$ verstehen, insbesondere, wenn die Primfaktorzerlegung von n bekannt ist.

Lemma 4.11. *Seien n und k positive natürliche Zahlen, und k teile n. Dann gibt es einen kanonischen Ringhomomorphismus*

$$\mathbb{Z}/(n) \longrightarrow \mathbb{Z}/(k),\ (a \mod n) \longmapsto (a \mod k).$$

Beweis. Wir betrachten die Ringhomomorphismen

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\varphi} & \mathbb{Z}/(k) \\ \phi\downarrow & & \\ \mathbb{Z}/(n) & & \end{array}$$

Aufgrund der Teilerbeziehung haben wir die Beziehung

$$\text{kern } \phi = (n) \subseteq (k) = \text{kern } \varphi\,.$$

Aufgrund des Homomorphisatzes hat man daher eine kanonische Abbildung von links unten nach rechts oben. □

Zur Formulierung des Chinesischen Restsatzes erinnern wir an den Begriff des Produktringes.

Definition 4.12. Seien $R_1, \ldots, R_n$ kommutative Ringe. Dann heißt das Produkt

$$R_1 \times \cdots \times R_n\,,$$

versehen mit komponentenweiser Addition und Multiplikation, der *Produktring* der R_i, $i = 1, \ldots, n$.

Satz 4.13. *(Chinesischer Restsatz) Sei n eine positive natürliche Zahl mit kanonischer Primfaktorzerlegung $n = p_1^{r_1} \cdot p_2^{r_2} \cdot \cdots \cdot p_k^{r_k}$ (die p_i seien also verschieden und $r_i \geq 1$). Dann induzieren die kanonischen Ringhomomorphismen $\mathbb{Z}/(n) \to \mathbb{Z}/(p_i^{r_i})$ einen Isomorphismus*

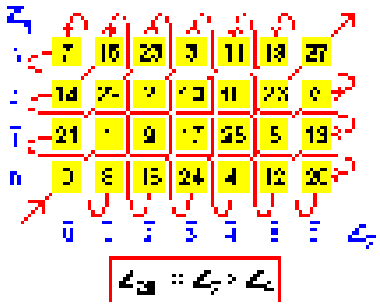
$$\mathbb{Z}/(n) \cong \mathbb{Z}/(p_1^{r_1}) \times \mathbb{Z}/(p_2^{r_2}) \times \cdots \times \mathbb{Z}/(p_k^{r_k})\,.$$

Zu einer gegebenen ganzen Zahl $(a_1, a_2, \ldots, a_k)$ gibt es also genau eine natürliche Zahl $a < n$, die die simultanen Kongruenzen

$$a = a_1 \mod p_1^{r_1},\ a = a_2 \mod p_2^{r_2},\ \ldots,\ a = a_k \mod p_k^{r_k}$$

löst.

Beweis. Da die Ringe links und rechts beide endlich sind und die gleiche Anzahl von Elementen haben, nämlich n, genügt es, die Injektivität zu zeigen. Sei x eine natürliche Zahl, die im Produktring (rechts) zu null wird, also modulo $p_i^{r_i}$ den Rest null hat für alle $i = 1, 2, \ldots, k$. Dann ist x ein Vielfaches von $p_i^{r_i}$ für alle $i = 1, 2, \ldots, k$, d.h., in der Primfaktorzerlegung von x muss p_i zumindest mit Exponent r_i vorkommen. Also muss x nach Satz 3.10 ein Vielfaches des Produktes sein muss, also ein Vielfaches von n. Damit ist $x = 0$ in $\mathbb{Z}/(n)$ und die Abbildung ist injektiv. □



Aufgabe:

(a) Bestimme für die Zahlen 3, 5 und 7 modulare Basislösungen, finde also die kleinsten positiven Zahlen, die in

$$\mathbb{Z}/(3) \times \mathbb{Z}/(5) \times \mathbb{Z}/(7)$$

die Restetupel $(1,0,0)$, $(0,1,0)$ und $(0,0,1)$ repräsentieren.

(b) Finde mit den Basislösungen die kleinste positive Lösung x der simultanen Kongruenzen

$$x = 2 \mod 3, x = 4 \mod 5 \text{ und } x = 3 \mod 7$$

Lösung:

(a) $(1,0,0)$: alle Vielfachen von $5 \cdot 7 = 35$ haben modulo 5 und modulo 7 den Rest 0. Unter diesen Vielfachen muss also die Lösung liegen. 35 hat modulo 3 den Rest 2, somit hat 70 modulo 3 den Rest 1. Also repräsentiert 70 das Restetupel $(1,0,0)$.

$(0,1,0)$: hier schaut man die Vielfachen von 21 an, und 21 hat modulo 5 den Rest 1. Also repräsentiert 21 das Restetupel $(0,1,0)$.

$(0,0,1)$: hier schaut man die Vielfachen von 15 an, und 15 hat modulo 7 den Rest 1. Also repräsentiert 15 das Restetupel $(0,0,1)$.

(b) Man schreibt (in $\mathbb{Z}/(3) \times \mathbb{Z}/(5) \times \mathbb{Z}/(7)$)

$$(2,4,3) = 2(1,0,0) + 4(0,1,0) + 3(0,0,1)\,.$$

Die Lösung ist dann

$$2 \cdot 70 + 4 \cdot 21 + 3 \cdot 15 = 140 + 84 + 45 = 269\,.$$

Die minimale Lösung ist dann $269 - 2 \cdot 105 = 59$.

Die Einheiten im Restklassenring

Wir wollen zeigen, dass die Einheitengruppe $(\mathbb{Z}/(p))^\times$, wenn p eine Primzahl ist, eine zyklische Gruppe ist, also von einem Element erzeugt wird. Der Restklassenring $\mathbb{Z}/(p)$ ist ein Körper, und wir werden hier nach einigen Vorbereitungen allgemeiner zeigen, dass jede endliche Untergruppe der

multiplikativen Gruppe eines Körpers zyklisch ist. Dazu benötigen wir einige Resultate über kommutative Gruppen und zu Polynomringen über Körpern. Wir beginnen mit zwei gruppentheoretischen Lemmata. Wir verwenden multiplikative Schreibweise.

Lemma 4.14. *Sei G eine kommutative Gruppe und $x, y \in G$ Elemente der endlichen Ordnungen $n = \operatorname{ord}(x)$ und $m = \operatorname{ord}(y)$, wobei n und m teilerfremd seien. Dann hat xy die Ordnung nm.*

Beweis. Sei $(xy)^k = 1$. Wir haben zu zeigen, dass k ein Vielfaches von nm ist. Es ist

$$1 = (x^k y^k)^n = x^{kn} y^{kn} = y^{kn} \,,$$

da ja n die Ordnung von x ist. Aus dieser Gleichung erhält man, dass kn ein Vielfaches der Ordnung von y, also von m sein muss. Da n und m teilerfremd sind, folgt aus Lemma von Euklid (Lemma 3.4), dass k ein Vielfaches von m ist. Ebenso ergibt sich, dass k ein Vielfaches von n ist, so dass k, wieder aufgrund der Teilerfremdheit, ein Vielfaches von nm sein muss. □

Definition 4.15. Der *Exponent* $\exp(G)$ einer endlichen Gruppe G ist die kleinste positive Zahl n mit der Eigenschaft, dass $x^n = 1$ ist für alle $x \in G$.

Lemma 4.16. *Sei G eine endliche kommutative Gruppe und sei $\exp(G) = \operatorname{ord}(G)$, wobei $\exp(G)$ den Exponenten der Gruppe bezeichnet. Dann ist G zyklisch.*

Beweis. Sei $n = \operatorname{ord}(G) = p_1^{r_1} \cdots p_k^{r_k}$ die Primfaktorzerlegung der Gruppenordnung. Der Exponent der Gruppe ist

$$\exp(G) = \operatorname{kgV}(\operatorname{ord}(x) : x \in G) \,.$$

Sei p_i ein Primteiler von n. Wegen $\exp(G) = \operatorname{ord}(G)$ gibt es ein Element $x \in G$, dessen Ordnung ein Vielfaches von $p_i^{r_i}$ ist. Dann gibt es auch (in der von x erzeugten zyklischen Untergruppe) ein Element x_i der Ordnung $p_i^{r_i}$. Dann hat das Produkt $x_1 \cdots x_k \in G$ nach Lemma 4.14 die Ordnung n. □

5. Vorlesung

In diesem Abschnitt beschäftigen wir uns mit der Einheitengruppe der Restklassenringe $\mathbb{Z}/(n)$, also mit $(\mathbb{Z}/(n))^\times$. Ihre Anzahl wird durch die Eulersche Funktion φ ausgedrückt. Wir brauchen noch kurz einige Vorbereitungen über Polynomringe.

Satz 5.1. *Sei K ein Körper und sei $K[X]$ der Polynomring über K. Sei $P \in K[X]$ ein Polynom und $a \in K$. Dann ist a genau dann eine Nullstelle von P, wenn P ein Vielfaches des linearen Polynoms $X - a$ ist.*

Beweis. Wenn P ein Vielfaches von $X - a$ ist so kann man

$$P = (X - a)Q$$

mit einem weiteren Polynom Q schreiben. Einsetzen ergibt

$$P(a) = (a-a)Q(a) = 0\,.$$

Im Allgemeinen gibt es aufgrund Fakt eine Darstellung

$$P = (X-a)Q + R\,,$$

wobei $R = 0$ oder aber den Grad null besitzt, also eine Konstante ist. Einsetzen ergibt

$$P(a) = R\,.$$

Wenn also $P(a) = 0$ ist, so muss der Rest $R = 0$ sein, und das bedeutet, dass $P = (X-a)Q$ ist. Also ist $X - a$ ein Linearfaktor von P. □

Korollar 5.2. *Sei K ein Körper und $K[X]$ der Polynomring über K. Sei $P \in K[X]$ ein Polynom (ungleich null) vom Grad d. Dann besitzt P maximal d Nullstellen.*

Beweis. Wir beweisen die Aussage durch Induktion über d. Für $d = 0, 1$ ist die Aussage offensichtlich richtig. Sei also $d \geq 2$ und die Aussage sei für kleinere Grade bereits bewiesen. Sei a eine Nullstelle von P. Dann ist $P = Q(X-a)$ nach Satz 5.1 und Q hat den Grad $d-1$, so dass wir auf Q die Induktionsvoraussetzung anwenden können. Das Polynom Q hat also maximal $d-1$ Nullstellen. Für $b \in K$ gilt $P(b) = Q(b)(b-a)$. Dies kann nur dann null sein, wenn einer der Faktoren null ist, so dass eine Nullstelle von P gleich a ist oder aber eine Nullstelle von Q ist. Es gibt also maximal d Nullstellen von P. □

Satz 5.3. *Sei $U \subseteq K^\times$ eine endliche Untergruppe der multiplikativen Gruppe eines Körpers K. Dann ist U zyklisch.*

Beweis. Sei $n = \operatorname{ord}(U)$ und $e = \exp(U)$ der Exponent dieser Gruppe. Dies bedeutet, dass alle Elemente $x \in U$ eine Nullstelle des Polynoms $X^e - 1$ sind. Nach Korollar 5.2 ist die Anzahl der Nullstellen aber maximal gleich dem Grad, so dass $n = e$ folgt. Nach Lemma 4.14 ist dann U zyklisch. □

Wir können damit im Fall einer Primzahl die Struktur der Einheitengruppe des Restklassenringes verstehen.

Satz 5.4. *Sei p eine Primzahl. Dann ist die Einheitengruppe $(\mathbb{Z}/(p))^\times$ zyklisch der Ordnung $p-1$. Es gibt also (sogenannte primitive) Elemente g mit der Eigenschaft, dass die Potenzen g^i, $i = 0, 1, \ldots, p-2$, alle Einheiten durchlaufen.*

Beweis. Dies folgt unmittelbar aus Satz 5.3, da $\mathbb{Z}/(p)$ ein endlicher Körper ist. □

Definition 5.5. Eine Einheit $u \in (\mathbb{Z}/(n))^\times$ heißt *primitiv* (oder eine *primitive Einheit*), wenn sie die Einheitengruppe erzeugt.

Bemerkung 5.6. Der Satz 5.4 sagt insbesondere, dass es für eine Primzahl p primitive Elemente im Restklassenkörper $\mathbb{Z}/(p)$ gibt. Er ist lediglich ein Existenzsatz und gibt keinen Hinweis, wie primitive Elemente zu konstruieren oder zu finden sind. Für eine beliebige natürliche Zahl n ist die Einheitengruppe der Restklassenringe $\mathbb{Z}/(n)$ im Allgemeinen nicht zyklisch. Wir werden später diejenigen Zahlen charakterisieren, die diese Eigenschaft besitzen. Für eine Primzahl p und eine Einheit $g \in (\mathbb{Z}/(p))^\times$ bedeutet die Eigenschaft, primitiv zu sein, dass ein Gruppenisomorphismus

$$(\mathbb{Z}/(p-1),+) \longrightarrow ((\mathbb{Z}/(p))^\times,\cdot),\ i \longmapsto g^i\,,$$

vorliegt.

Korollar 5.7. *(Anzahl von primitiven Elementen) Sei p eine Primzahl. Dann gibt es in $\mathbb{Z}/(p)$ genau $\varphi(p-1)$ primitive Elemente.*

Beweis. Aufgrund der Existenz von primitiven Elementen gibt es eine Isomorphie $\mathbb{Z}/(p-1) \cong (\mathbb{Z}/(p))^\times$. Daher geht es um die Anzahl der Erzeuger der additiven Gruppe $\mathbb{Z}/(p-1)$. Ein Element aus $\mathbb{Z}/(p-1)$ ist ein Gruppen-Erzeuger genau dann, wenn es in $\mathbb{Z}/(p-1)$ (als Ring betrachtet) eine Einheit ist. Deshalb ist die Anzahl gerade $\varphi(p-1)$. □

Wir kehren nun zum allgemeinen Fall zurück, wo n eine beliebige positive ganze Zahl ist.

Satz 5.8. *Sei n eine positive natürliche Zahl mit kanonischer Primfaktorzerlegung $n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$. Dann induziert der Isomorphismus (des Chinesischen Restsatzes) $\mathbb{Z}_n/(n) \cong \mathbb{Z}/(p_1^{r_1}) \times \mathbb{Z}/(p_2^{r_2}) \times \cdots \times \mathbb{Z}/(p_k^{r_k})$ einen Isomorphismus der Einheitengruppen*

$$(\mathbb{Z}/(n))^\times \cong (\mathbb{Z}/(p_1^{r_1}))^\times \times (\mathbb{Z}/(p_2^{r_2}))^\times \times \cdots \times (\mathbb{Z}/(p_k^{r_k}))^\times\,.$$

Insbesondere ist die Einheitengruppe von $\mathbb{Z}/(n)$ höchstens dann zyklisch, wenn die Einheitengruppen von $\mathbb{Z}/(p_i^{r_i})$ zyklisch sind für alle $i = 1,\ldots,k$.

Beweis. Ein Ringisomorphismus induziert natürlich einen Isomorphismus der Einheitengruppen, und die Einheitengruppe eines Produktringes ist die Produktgruppe der beteiligten Einheitengruppen. Ist eine Produktgruppe zyklisch, so muss auch jede Komponentengruppe zyklisch sein, da diese auch Restklassengruppen der Produktgruppe sind (unter der Projektion auf die Komponente). □

Aus obiger Einheitenversion des Chinesischen Restsatzes folgt für die Eulersche Funktion, wenn $n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$ die Primfaktorzerlegung ist, die Identität

$$\varphi(n) = \varphi(p_1^{r_1}) \cdot \varphi(p_2^{r_2}) \cdots \varphi(p_k^{r_k})\,.$$

Man muss also nur noch $\varphi(p^r)$ für eine Primzahl p berechnen, wobei natürlich $\varphi(p) = p-1$ ist. Für p^r mit $r \geq 2$ ist eine Zahl $0 < a < p^r$ genau dann teilerfremd zu p^r, wenn sie teilerfremd zu p ist, und das ist genau dann der

Fall, wenn sie kein Vielfaches von p ist. Die Vielfachen von p im beschriebenen Intervall sind genau die Zahlen bp mit $0 \leq b < p^{r-1}$. Dies sind p^{r-1} Stück, so dass es also $p^r - p^{r-1} = p^{r-1}(p-1)$ Einheiten gibt. Wir erhalten demnach

$$\varphi(p^r) = p^{r-1}(p-1)$$

und insgesamt

$$\varphi(n) = p_1^{r_1-1}(p_1-1) \cdot p_2^{r_2-1}(p_2-1) \cdots p_k^{r_k-1}(p_k-1)\,.$$

Lemma 5.9. *Sei p eine Primzahl und $r \geq 1$. Dann ist der durch die kanonische Projektion $\mathbb{Z}/(p^r) \longrightarrow \mathbb{Z}/(p)$ induzierte Homomorphismus*

$$(\mathbb{Z}/(p^r))^\times \longrightarrow (\mathbb{Z}/(p))^\times$$

der Einheitengruppen surjektiv.

Beweis. Sei $a \in (\mathbb{Z}/(p))^\times$ eine Einheit. Dann ist a teilerfremd zu p und damit kein Vielfaches von p. Wir fassen a als Element in $\mathbb{Z}/(p^r)$ auf. Da a nach wie vor kein Vielfaches von p ist, ist es auch in $\mathbb{Z}/(p^r)$ eine Einheit, und zugleich ein Urbild von $a \in (\mathbb{Z}/(p))^\times$. □

Lemma 5.10. *Sei $p \geq 3$ eine Primzahl und $r \geq 1$. Dann ist der Kern des Einheiten -Homomorphismus*

$$\varphi : (\mathbb{Z}/(p^r))^\times \longrightarrow (\mathbb{Z}/(p))^\times$$

zyklisch der Ordnung p^{r-1}.

Beweis. Wir zeigen, dass das Element $a = 1+p$, das offensichtlich zum Kern von $\varphi : (\mathbb{Z}/(p^r))^\times \longrightarrow (\mathbb{Z}/(p))^\times$ gehört, in der Einheitengruppe $(\mathbb{Z}/(p^r))^\times$ die Ordnung p^{r-1} besitzt. Da diese Kerngruppe die Ordnung p^{r-1} hat, muss die (multiplikative) Ordnung von a ein Teiler davon sein, also von der Gestalt p^s mit $s \leq r-1$ sein. Wir zeigen, dass $a^{p^{r-2}} \neq 1$ in $(\mathbb{Z}/(p^r))^\times$ ist, so dass also nur noch die Ordnung p^{r-1} möglich bleibt.

Nehmen wir also $a^{p^{r-2}} = 1 \mod p^r$ an, das bedeutet

$$a^{p^{r-2}} - 1 = (1+p)^{p^{r-2}} - 1 = 0 \mod p^r\,.$$

Ausmultiplizieren ergibt den Ausdruck

$$\binom{p^{r-2}}{1}p + \binom{p^{r-2}}{2}p^2 + \binom{p^{r-2}}{3}p^3 + \ldots = 0 \mod p^r\,.$$

Der erste Summand ist dabei $\binom{p^{r-2}}{1}p = p^{r-1}$ und wir betrachten die weiteren Summanden

$$\binom{p^{r-2}}{k}p^k\,.$$

mit $k \geq 2$. Wir schreiben

$$\begin{aligned}\binom{p^{r-2}}{k} &= \frac{p^{r-2}!}{k!(p^{r-2}-k)!} \\ &= \frac{p^{r-2}\cdot(p^{r-2}-1)\cdots(p^{r-2}-k+1)}{k\cdot(k-1)\cdots 1} \\ &= \frac{p^{r-2}\cdot(p^{r-2}-1)\cdots(p^{r-2}-k+1)}{k\cdot 1\cdots(k-1)}\,.\end{aligned}$$

So geordnet steht vorne $\frac{p^{r-2}}{k}$ und dann folgen Ausdrücke der Form $\frac{p^{r-2}-j}{j}$, $j = 1,\ldots,k-1$. Der Exponent der Primzahl p in diesen letztgenannten Brüchen ist oben und unten gleich. Daher hängt der p-Exponent des Binomialkoeffizienten $\binom{p^{r-2}}{k}$ nur von $\frac{p^{r-2}}{k}$ ab. Sei i der p-Exponent von k. Der p-Exponent von $\frac{p^{r-2}}{k}$ ist dann $r-2-i$ und damit ist der p-Exponent von $\binom{p^{r-2}}{k}p^k$ gleich

$$r-2-i+k\,.$$

Wir behaupten, dass dies $\geq r$ ist, was für $i=0$ klar ist (wegen $k \geq 2$). Sei also $i \geq 1$. Dann gilt aber, wegen $p \geq 3$, die Abschätzung

$$i \leq p^i - 2 \leq k-2\,,$$

was genau die Aussage ergibt. Damit ist insgesamt in der obigen Summation der erste Summand, also p^{r-1}, kein Vielfaches von p^r, aber alle weiteren Summanden sind Vielfache von p^r, was einen Widerspruch bedeutet. □

Satz 5.11. *Sei $p \geq 3$ eine Primzahl und $r \geq 1$. Dann ist die Einheitengruppe*

$$(\mathbb{Z}/(p^r))^\times$$

des Restklassenrings $\mathbb{Z}/(p^r)$ zyklisch.

Beweis. Nach Lemma 5.9 ist die Abbildung

$$\varphi : (\mathbb{Z}/(p^r))^\times \longrightarrow (\mathbb{Z}/(p))^\times$$

surjektiv. Die Einheitengruppe $(\mathbb{Z}/(p))^\times$ ist zyklisch aufgrund der Aussage (Satz 5.4). Sei $v \in (\mathbb{Z}/(p))^\times$ ein erzeugendes (also primitives) Element dieser Gruppe (der Ordnung $p-1$) und sei $u \in (\mathbb{Z}/(p^r))^\times$ ein Element, das auf v abgebildet wird. Die Ordnung von u ist dann ein positives Vielfaches von $p-1$. Es gibt daher auch ein $w \in (\mathbb{Z}/(p))^\times$ (nämlich eine gewissse Potenz von u), das genau die Ordnung $p-1$ besitzt.

Auf der anderen Seite gibt es nach Lemma 5.10 ein Element $a \in (\mathbb{Z}/(p))^\times$, das den Kern von φ erzeugt und die Ordnung p^{r-1} besitzt. Die Ordnung von ¡aw ist somit das kleinste gemeinsame Vielfache von p^{r-1} und $p-1$, also $p^{r-1}(p-1)$. Da dies die Gruppenordnung ist, muss die Gruppe zyklisch sein und awist ein Erzeuger. □

Bemerkung 5.12. Für $p = 2$ ist die Einheitengruppe von $\mathbb{Z}/(2^r)$ im Allgemeinen nicht zyklisch. Für $r = 1$ ist sie zyklisch (sogar trivial) und für $r = 2$ ist $(\mathbb{Z}/(2^2))^\times = (\mathbb{Z}/(4))^\times$ ebenfalls zyklisch der Ordnung zwei, und zwar ist 3 primitiv. Für $r = 3$ hingegen ist $(\mathbb{Z}/(2^3))^\times = (\mathbb{Z}/(8))^\times$ nicht zyklisch. Es gilt nämlich

$$1^2 = 1 \mod 8,\ 3^2 = 9 = 1 \mod 8,\ 5^2 = 25 = 1 \mod 8 \text{ und}$$
$$7^2 = 49 = 1 \mod 8,$$

so dass alle Einheiten die Ordnung zwei haben und es keinen Erzeuger gibt. Die Einheitengruppe ist isomorph zu

$$(\mathbb{Z}/(8))^\times \cong \mathbb{Z}/(2) \times \mathbb{Z}/(2)\,.$$

Ähnliche Überlegungen wie in Lemma 5.10 zeigen, dass die Einheitengruppe von $\mathbb{Z}/(2^r)$ für $r \geq 3$ isomorph zu $\mathbb{Z}/(2^{r-2}) \times \mathbb{Z}/(2)$ ist, und zwar ist 5 ein Element der Ordnung 2^{r-2}. Jede Einheit in $\mathbb{Z}/(2^r)$ hat somit eine Darstellung der Form $\pm 5^i$.

6. Vorlesung

Wir beenden zunächst unsere Überlegungen, wann die Einheitengruppe eines Restklassenringes von $\mathbb{Z}$ zyklisch ist.

Lemma 6.1. *Die Einheitengruppe von $\mathbb{Z}/(2^r)$ ist nicht zyklisch für $r \geq 3$.*

Beweis. Die Abbildung

$$(\mathbb{Z}/(2^r))^\times \longrightarrow (\mathbb{Z}/(2^{r-1}))^\times$$

ist surjektiv (da genau die ungeraden Elemente die Einheiten sind) und hat als Kern eine Gruppe, die isomorph zu $\mathbb{Z}/(2)$ ist. Der Kern besteht also neben 1 aus einem weiteren Element $a \in (\mathbb{Z}/(2^r))^\times$, das die Ordnung zwei besitzt. Das Element -1 wird unter der Abbildung auf -1 geschickt, und in $(\mathbb{Z}/(2^{r-1}))^\times$ gilt $-1 \neq 1$, da $r - 1 \geq 2$ ist. Deshalb gehört -1 nicht zum Kern und somit ist $a \neq -1$ in $(\mathbb{Z}/(2^r))^\times$. Also besitzt diese Gruppe zwei verschiedene Elemente der Ordnung zwei. Damit kann die Gruppe nicht zyklisch sein. □

Unser abschließendes Resultat ist nun der folgende Satz.

Satz 6.2. *Die Einheitengruppe $(\mathbb{Z}/(n))^\times$ ist genau dann zyklisch, wenn*

$$n = 1, 2, 4, p^s, 2p^s$$

ist, wobei p eine ungerade Primzahl und $s \geq 1$ ist.

Beweis. In den beschriebenen Fällen ist die Einheitengruppe $(\mathbb{Z}/(n))^\times$ zyklisch aufgrund von Satz 5.4, Bemerkung 5.12 und der Isomorphie

$$(\mathbb{Z}/(2p^r))^\times \cong (\mathbb{Z}/(2))^\times \times (\mathbb{Z}/(p^r))^\times \cong (\mathbb{Z}/(p^r))^\times\,.$$

Sei also umgekehrt n gegeben mit der Eigenschaft, dass $(\mathbb{Z}/(n))^\times$ zyklisch sei. Es sei $n = 2^r \cdot p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$ die kanonische Primfaktorzerlegung mit ungeraden Primzahlen $p_1, \ldots, p_k$ und $r_i \geq 1$, die nach dem Chinesischen Restsatz zur Isomorphie

$$(\mathbb{Z}/(n))^\times \cong (\mathbb{Z}/(2^r))^\times \times (\mathbb{Z}/(p_1^{r_1}))^\times \times (\mathbb{Z}/(p_2^{r_2}))^\times \times \cdots \times (\mathbb{Z}/(p_k^{r_k}))^\times .$$

führt. Da Restklassengruppen von zyklischen Gruppen wieder zyklisch sind, folgt, dass $r = 0, 1$ oder 2 ist. Ein Produkt von zyklischen Gruppen ist nur dann zyklisch, wenn die beteiligten Ordnungen paarweise teilerfremd sind. Die Ordnungen von $(\mathbb{Z}/(p_i^{r_i}))^\times$ sind aber gerade für p_i ungerade und $r_i \geq 1$, und die Ordnung von $(\mathbb{Z}/(2^r))^\times$ ist gerade für $r \geq 2$. Also ist $k \leq 1$. Bei $k = 1$ ist $r = 2$ nicht möglich. Bei $k = 0$ verbleiben die angeführten Fälle $n = 1, 2, 4$. □

Quadratische Reste

Wir wollen nun wissen, welche Zahlen k modulo einer fixierten Zahl n (häufig einer Primzahl) ein Quadrat sind, also eine Quadratwurzel besitzen. Man spricht von quadratischen Resten und quadratischen Nichtresten (besser ist es, von nichtquadratischen Resten zu sprechen).

Definition 6.3. Eine ganze Zahl k heißt *quadratischer Rest* modulo n, wenn es eine Zahl x gibt mit

$$x^2 = k \mod n .$$

Im anderen Fall heißt k ein *quadratischer Nichtrest* modulo n.

Eine Quadratzahl ist natürlich auch ein quadratischer Rest modulo jeder Zahl n. Umgekehrt ist eine Zahl, die selbst keine Quadratzahl ist, modulo gewisser Zahlen ein quadratischer Rest und modulo gewisser Zahlen ein quadratischer Nichtrest. Grundsätzlich kann man zu gegebenen k und n naiv testen, ob k ein quadratischer Rest ist oder nicht, indem man alle Reste quadriert und schaut, ob der durch k definierte Rest dabei ist. Die Frage nach den Quadratresten weist aber eine Reihe von Gesetzmäßigkeiten auf, die wir im folgenden kennen lernen werden und mit deren Hilfe man effektiver entscheiden kann, ob ein Quadratrest vorliegt oder nicht.

Satz 6.4. *(Quadratreste und Chinesischer Restsatz) Sei n eine positive natürliche Zahl mit kanonischer Primfaktorzerlegung $n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_s^{r_s}$ (die p_i seien also verschieden). Dann ist k genau dann Quadratrest modulo n, wenn k Quadratrest modulo $p_i^{r_i}$ ist für alle $i = 1, \ldots, s$.*

Beweis. Dies folgt unmittelbar aus dem Chinesischen Restsatz (Satz 4.13). □

Satz 6.5. *(Quadratreste unter Reduktion I) Sei p eine ungerade Primzahl und sei $k \in \mathbb{Z}/(p^r)$.*

(1) *Ist k teilerfremd zu p (also kein Vielfaches von p), dann ist k genau dann ein Quadratrest modulo p^r, wenn k ein Quadratrest modulo p ist.*
(2) *Ist $k = p^s u$ mit u teilerfremd zu p und $s < r$, so ist k genau dann ein Quadratrest modulo p^r, wenn s gerade und wenn u ein Quadratrest modulo p ist.*

Beweis. Die natürliche Abbildung $\mathbb{Z}/(p^r) \longrightarrow \mathbb{Z}/(p)$ liefert sofort, dass ein Quadratrest modulo p^r auch ein Quadratrest modulo p ist. Wir zeigen zunächst die Umkehrung für Einheiten. Nach Lemma 5.9 ist die Abbildung

$$(\mathbb{Z}/(p^r))^\times \longrightarrow (\mathbb{Z}/(p))^\times$$

surjektiv und nach Satz 5.11 sind die beteiligten Gruppen zyklisch. D.h. ein Erzeuger wird auf einen Erzeuger abgebildet. Insbesondere kann man diese Gruppen so mit additiven zyklischen Gruppen identifizieren, dass der Homomorphismus die 1 auf die 1 schickt. Dies erreicht man, indem man im folgenden kommutativen Diagramm die Identifikation links mit einem primitiven Element $g \in \mathbb{Z}/(p^r)$ und rechts ebenfalls mit g (jetzt aufgefasst in $\mathbb{Z}/(p)$ stiftet.

$$\begin{array}{ccc} (\mathbb{Z}/(p^r))^\times & \longrightarrow & (\mathbb{Z}/(p))^\times \\ \cong \uparrow & & \uparrow \cong \\ \mathbb{Z}/(p^{r-1}(p-1)) & \longrightarrow & \mathbb{Z}/(p-1) \end{array} .$$

Wir schreiben die untere horizontale Abbildung, unter Verwendung des Chinesischen Restsatzes (Satz 4.13), als

$$\mathbb{Z}/(p^{r-1}) \times \mathbb{Z}/(p-1) \cong \mathbb{Z}/(p^{r-1}(p-1)) \longrightarrow \mathbb{Z}/(p-1) \text{ mit } 1 = (1,1) \longmapsto 1\,.$$

Da überdies p und $p-1$ teilerfremd sind, liegt hier insgesamt einfach die Projektion $(b_1, b_2) \mapsto b_2$ vor.

Die Voraussetzung, dass k modulo p ein Quadratrest ist, übersetzt sich dahingehend, dass das k entsprechende Element (sagen wir $b = (b_1, b_2)$) in $\mathbb{Z}/(p-1)$ ein Vielfaches von 2 ist. D.h. die zweite Komponente, also b_2, ist ein Vielfaches der 2. Da modulo der ungeraden Zahl p^{r-1} jede Zahl ein Vielfaches von 2 ist (da 2 eine Einheit in $\mathbb{Z}/(p^{r-1})$, ist auch die erste Komponente, also b_1, ein Vielfaches von 2 und so muss b insgesamt ein Vielfaches der 2 sein.

Sei nun $k = p^s u$, $1 \leq s \leq r-1$, und zunächst angenommen, dass k ein Quadrat ist. D.h wir können k schreiben als $k = x^2$ mit $x = p^t v$, wobei v eine Einheit sei. Es ist also $p^s u = p^{2t} v^2$ in $\mathbb{Z}/(p^r)$ und es ist $2t < r$ (sonst steht hier 0). Durch Betrachten modulo p^s und modulo p^{2t} sieht man, dass $s = 2t$ sein muss. Insbesondere ist s gerade. Es gilt also $p^s u = p^s v^2 \mod p^r$ und somit können wir $p^s(u - v^2) = cp^r$ schreiben. Kürzen in $\mathbb{Z}$ ergibt $u - v^2 = cp^{r-s}$, also $u = v^2 \mod p$. Also ist u ein quadratischer Rest modulo p und nach dem ersten Teil auch modulo p^r.

Die Umkehrung von (2) ist nach der unter (1) bewiesenen Aussage klar. □

Satz 6.6. *(Quadratreste unter Reduktion II) Sei $p = 2$ und sei $k \in \mathbb{Z}/(2^r)$.*

(1) *Für $r = 2$ ist k genau dann quadratischer Rest, wenn $k = 0, 1 \mod 4$ ist.*
(2) *Für $r \geq 3$ und k ungerade ist k genau dann quadratischer Rest modulo 2^r, wenn $k = 1 \mod 8$ ist.*

Beweis. (1) ist trivial.

(2). In $\mathbb{Z}/(8)$ ist von den ungeraden Zahlen lediglich die 1 ein Quadrat, so dass der Ringhomomorphismus

$$\mathbb{Z}/(2^r) \to \mathbb{Z}/(8)$$

für $r \geq 3$ zeigt, dass die numerische Bedingung notwendig ist. Sei diese umgekehrt nun erfüllt, also $a \in (\mathbb{Z}/(2^r))^\times$ mit $a = 1 \mod 8$. Dann kann man nach Bemerkung 5.12 schreiben $a = \pm 5^i$. Dies gilt aber auch modulo 8, woraus sofort folgt, dass i gerade und dass das Vorzeichen positiv ist. Dann ist $5^{i/2}$ eine Quadratwurzel von a in $\mathbb{Z}/(2^r)$. □

Wir werden uns im folgenden weitgehend darauf beschränken, welche Zahlen modulo einer Primzahl Quadratreste sind. Da allerdings die Primfaktorzerlegung einer größeren Zahl nicht völlig unproblematisch ist, müssen wir später auch Techniken entwickeln, die ohne Kenntnis der Primfaktorzerlegung auskommen. Direkt beantworten lässt sich die Frage, wann -1 ein Quadratrest modulo einer Primzahl ist.

Satz 6.7. *(Wann ist -1 ein Quadratrest) Sei p eine Primzahl. Dann gelten folgende Aussagen.*

Für $p = 2$ ist $-1 = 1$ ein Quadrat in $\mathbb{Z}/(2)$.

Für $p = 1 \mod 4$ ist -1 ein Quadrat in $\mathbb{Z}/(p)$.

Für $p = 3 \mod 4$ ist -1 kein Quadrat in $\mathbb{Z}/(p)$.

Beweis. Die erste Aussage ist klar, sei also p ungerade. Nach Satz 5.4 ist die Einheitengruppe zyklisch der geraden Ordnung $\mathrm{l}\, p - 1$. Identifiziert man $((\mathbb{Z}/(p))^\times, \cdot)$ mit $(\mathbb{Z}/(p-1), +)$, so entspricht -1 dem Element $(p-1)/2$, und -1 besitzt genau dann eine Quadratwurzel, wenn $(p-1)/2$ in $\mathbb{Z}/(p-1)$ ein Vielfaches von 2 ist. Dies ist aber genau dann der Fall, wenn $(p-1)/2$ selbst gerade ist, was zu $p = 1 \mod 4$ äquivalent ist. □

7. Vorlesung

Für ungerade Primzahlen kann man sofort eine Aussage über die Anzahl der Quadratreste machen.

Satz 7.1. *(Anzahl von Quadratresten) Sei p eine ungerade Primzahl. Dann gibt es $\frac{p+1}{2}$ quadratische Reste modulo p und $\frac{p-1}{2}$ nichtquadratische Reste modulo p.*

Beweis. Zunächst ist 0 ein quadratischer Rest. Wir betrachten im folgenden nur noch die Einheiten in $\mathbb{Z}/(p)$ (also die von 0 verschiedenen Reste) und zeigen, dass es darunter gleich viele quadratische und nichtquadratische Reste gibt. Die Abbildung

$$(\mathbb{Z}/(p))^\times \longrightarrow (\mathbb{Z}/(p))^\times,\, x \longmapsto x^2\,,$$

ist offenbar ein Gruppenhomomorphismus der Einheitengruppe in sich selbst. Ein Element $k \in (\mathbb{Z}/(p))^\times$ ist genau dann ein Quadratrest, wenn es im Bild dieses Homomorphismus liegt. Nach dem Isomorphiesatz ist „Bild = Urbild modulo Kern“, so dass wir den Kern bestimmen müssen. Der Kern besteht aus allen Elementen x mit $x^2 = 1$. Dazu gehören 1 und -1, und diese beiden Elemente sind verschieden, da p ungerade ist. Aus der polynomialen Identität $x^2 - 1 = (x+1)(x-1)$ folgt, dass es keine weiteren Lösungen geben kann. Der Kern besteht also genau aus 2 Elementen und damit besteht das Bild aus $(p-1)/2$ Elementen. □

Definition 7.2. Für eine ungerade Primzahl p und eine zu p teilerfremde Zahl $k \in \mathbb{Z}$ definiert man das *Legendre-Symbol*, geschrieben $\left(\frac{k}{p}\right)$ (sprich „k nach p“), durch

$$\left(\frac{k}{p}\right) := \begin{cases} 1, \text{ falls } k \text{ quadratischer Rest modulo } p \text{ ist,} \\ -1, \text{ falls } k \text{ kein quadratischer Rest modulo } p \text{ ist.} \end{cases}$$

Insbesondere ist $\left(\frac{k}{p}\right) = \left(\frac{k \mod p}{p}\right)$. Die Werte des Legendre-Symbols, also 1 und -1, kann man dabei in $\mathbb{Z}$, in $\mathbb{Z}^\times$ oder in $(\mathbb{Z}/(p))^\times$ auffassen.

Lemma 7.3. *(Multiplikativität des Legendre-Symbols) Sei p eine ungerade Primzahl. Dann ist die Abbildung*

$$(\mathbb{Z}/(p))^\times \longrightarrow \{\pm 1\},\, k \longmapsto \left(\frac{k}{p}\right)\,,$$

ein Gruppenhomomorphismus.

Beweis. Die Quadrate bilden offenbar eine Untergruppe in der Einheitengruppe $(\mathbb{Z}/(p))^\times$, die nach Satz 7.1 den Index 2 besitzt. Daher ist

$$(\mathbb{Z}/(p))^\times/(\text{Quadrate}) \cong \mathbb{Z}/(2) \cong \{\pm 1\}\,.$$

und die Restklassenabbildung ist gerade die Abbildung auf das Legendre-Symbol. □

Satz 7.4. *(Euler-Kriterium) Sei p eine ungerade Primzahl. Dann gilt für eine zu p teilerfremde Zahl k die Gleichheit*

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

Beweis. Es ist $(k^{\frac{p-1}{2}})^2 = k^{p-1} = 1$ nach Fermat (Satz 4.6). Daher ist $k^{\frac{p-1}{2}} = \pm 1$. Die Abbildung

$$(\mathbb{Z}/(p))^\times \longrightarrow \{\pm 1\},\ k \longmapsto k^{\frac{p-1}{2}}\ ,$$

ist (wie jedes Potenzieren) ein Gruppenhomomorphismus. Die Quadrate werden darunter auf 1 abgebildet, da für $k = x^2$ die Gleichheit

$$k^{\frac{p-1}{2}} = (x^2)^{\frac{p-1}{2}} = x^{p-1} = 1$$

gilt. Da nach dem Satz 5.11 die Einheitengruppe $(\mathbb{Z}/(p))^\times$ zyklisch ist, muss diese Abbildung surjektiv sein (sonst hätte jedes Element eine kleinere Ordnung). Damit muss diese Abbildung mit der durch das Legendre-Symbol gegebenen übereinstimmen. □

Seien p und q zwei ungerade Primzahlen. Dann kann p ein quadratischer Rest modulo q sein (oder nicht) und q kann ein quadratischer Rest modulo p sein, oder nicht. Das Quadratische Reziprozitätsgesetz, das von Euler entdeckt und von Gauss erstmals bewiesen wurde, behauptet nun, dass es einen direkten Zusammenhang zwischen diesen beiden Eigenschaften gibt. Es erlaubt weiterhin mit den beiden unten genannten Ergänzungssätzen algorithmisch zu entscheiden, ob eine Zahl ein quadratischer Rest oder ein quadratischer Nichtrest ist.

Carl Friedrich Gauss (1777-1855)

Satz 7.5. *(Quadratisches Reziprozitätsgesetz) Seien p und q zwei verschiedene ungerade Primzahlen. Dann gilt:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} -1 & \textit{wenn} \quad p = q = 3 \mod 4 \\ 1 & \textit{sonst.} \end{cases}$$

Beweis. Dies wird weiter unten nach einigen Vorbereitungen bewiesen. Die zweite Gleichung ist elementar. □

Die beiden folgenden Sätze werden die Ergänzungssätze zum quadratischen Reziprozitätsgesetz genannt.

Satz 7.6. *(1. Ergänzungssatz zum quadratischen Reziprozitätsgesetz) Für eine ungerade Primzahl p gilt:*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \textit{falls} \quad p = 1 \mod 4 \\ -1 & \textit{sonst} \quad (\textit{also } p = -1 \mod 4) \end{cases} .$$

Beweis. Die Gleichung von links und rechts wurde bereits im Satz 6.7 bewiesen. Die erste Gleichung ist auch ein Spezialfall des Eulerschen Kriteriums (Satz 7.4) und die zweite Gleichung ist elementar. □

Satz 7.7. *(2. Ergänzungssatz zum quadratischen Reziprozitätsgesetz) Für eine ungerade Primzahl p gilt:*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \textit{falls} \quad p = \pm 1 \mod 8 \\ -1 & \textit{sonst} \quad (\textit{also } p = \pm 3 \mod 8) \end{cases} .$$

Beweis. Dies wird weiter unten bewiesen. □

Die Elemente im Restklassenkörper $\mathbb{Z}/(p)$ werden meist durch die Zahlen von null bis $p-1$ repräsentiert. Für das folgende Vorzeichenlemma von Gauß ist es sinnvoll, ein anderes Repräsentantensystem (für die von null verschiedenen Elemente) zu fixieren. Wir setzen $t = \frac{p-1}{2}$ und

$$S = S_- \cup S_+ \text{ mit } S_- = \{-t, -t+1, \ldots, -2, -1\} \text{ und } S_+ = \{1, 2, \ldots, t-1, t\} .$$

Wir unterteilen also die Einheitengruppe in eine positive und eine negative Hälfte. Dieses Repräsentantensystem ist dadurch ausgezeichnet, dass jedes Element durch das betragmäßig kleinste Element repräsentiert wird. Im folgenden Lemma betrachtet man zu einer zu p teilerfremden Zahl k die Menge der Vielfachen

$$ik,\ i = 1, \ldots, t ,$$

in $\mathbb{Z}/(p)$ und schaut, ob sie in der negativen oder der positiven Hälfte liegen. Man definiert die sogenannten Gaußschen Vorzeichen

$$\epsilon_i = \epsilon_i(k) = \begin{cases} 1, \text{ falls } ik \in S_+ \\ -1, \text{ falls } ik \in S_- . \end{cases}$$

Lemma 7.8. *(Gaußsches Vorzeichenlemma) Für eine ungerade Primzahl p und eine zu p teilerfremde Zahl k gilt mit den soeben eingeführten Bezeichnungen*

$$\left(\frac{k}{p}\right) = \epsilon_1 \cdot \epsilon_2 \cdots \epsilon_t .$$

Beweis. Es sei $s_i \in S_+$ durch die Bedingung

$$ik = \epsilon_i s_i \mod p$$

festgelegt. Wir betrachten alle Vielfachen jk, $j \in S = (\mathbb{Z}/(p))^\times$. Die Menge all dieser Vielfachen ist selbst ganz S, da ja k eine Einheit und daher die Multiplikation mit k eine Bijektion ist. Es ist $(-i)k = -ik = -\epsilon_i s_i$ für

$i \in S_+ = \{1, \ldots, t\}$. Daher ist $S_+ = \{1, \ldots, t\} = \{s_1, \ldots, s_t\}$. Deshalb gilt $t! = \prod_{i=1}^{t} s_i$ und somit

$$t!k^t = (\prod_{i=1}^{t} i)(\prod_{i=1}^{t} k) = \prod_{i=1}^{t} ik = \prod_{i=1}^{t} \epsilon_i s_i = (\prod_{i=1}^{t} \epsilon_i)(\prod_{i=1}^{t} s_i) = (\prod_{i=1}^{t} \epsilon_i)t! \mod p\,.$$

Durch kürzen mit $t!$ (das ist eine Einheit) ergibt sich $k^t = \prod_{i=1}^{t} \epsilon_i \mod p$, und das Eulersche Kriterium (Satz 7.4), nämlich $k^t = k^{\frac{p-1}{2}} = \left(\frac{k}{p}\right) \mod p$, liefert das Ergebnis. □

Mit dem Gaußschen Vorzeichenlemma beweisen wir zunächst den zweiten Ergänzungssatz zum quadratischen Reziprozitätsgesetz, der beschreibt, wann 2 ein quadratischer Rest ist.

Satz 7.9. *(2. Ergänzungssatz zum quadratischen Reziprozitätsgesetz) Für eine ungerade Primzahl p gilt:*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \textit{falls} \quad p = \pm 1 \mod 8 \\ -1 & \textit{sonst} \quad (\textit{also } p = \pm 3 \mod 8) \end{cases}.$$

Beweis. Wir benutzen das Gaußsche Vorzeichenlemma (Lemma 7.8) und haben zu bestimmen, wie viele der Zahlen $2i$, $i = 1, \ldots, t = (p-1)/2$, in S_- liegen. Nun ist $2i \in S_-$ genau dann, wenn $2i > (p-1)/2$ ist (alle zu betrachtenden Vielfachen von 2 sind kleiner als p). Dies ist äquivalent zu $i > (p-1)/4$ und wir haben das kleinste i mit dieser Eigenschaft zu finden. Ist $p-1$ ein Vielfaches von 4, so ist $(p-1)/4 + 1$ das kleinste i und insgesamt gibt es in diesem Fall

$$\frac{p-1}{2} - (\frac{p-1}{4} + 1) + 1 = \frac{p-1}{4}$$

solcher i. Diese Anzahl ist bei $p = 1 \mod 8$ gerade und bei $p = 5 \mod 8$ ungerade, was das Ergebnis in diesen Fällen ergibt.

Sei also nun $p = 3, 7 \mod 8$ bzw. $p = 3 \mod 4$. Dann ist das kleinste i derart, dass $2i > (p-1)/2$ ist, gleich $(p-1)/4 + 1/2$, und es gibt insgesamt

$$\frac{p-1}{2} - (\frac{p-1}{4} + \frac{1}{2}) + 1 = \frac{p-1}{4} + \frac{1}{2} = \frac{p+1}{4}$$

solche i. Diese Anzahl ist bei $p = 3 \mod 8$ ungerade und bei $p = 7 \mod 8$ gerade, was die Behauptung in diesen Fällen ergibt. □

8. Vorlesung

Im nächsten Lemma verwenden wir folgende Notation:

Zu einer ungeraden Primzahl p und einer Zahl $k \in \mathbb{Z}$ sei

$$S(k,p) = \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ki}{p} \right\rfloor .$$

Lemma 8.1. *Sei p eine ungerade Primzahl und $k \in \mathbb{Z}$ kein Vielfaches von p. Dann gelten folgende Aussagen.*

(1) *Es ist $\epsilon_i = (-1)^{\lfloor \frac{2ki}{p} \rfloor}$, wobei ϵ_i wie im Gaußschen Vorzeichenlemma (Lemma 7.8) definiert ist.*
(2) $\left(\frac{k}{p}\right) = (-1)^{S(2k,p)}$.
(3) *Ist k ungerade, so ist $\left(\frac{k}{p}\right) = (-1)^{S(k,p)}$.*

Beweis. (1). Wir schreiben

$$\left\lfloor \frac{2ki}{p} \right\rfloor = \left\lfloor 2 \left\lfloor \frac{ki}{p} \right\rfloor + 2(\frac{ki}{p} - \left\lfloor \frac{ki}{p} \right\rfloor) \right\rfloor = 2 \left\lfloor \frac{ki}{p} \right\rfloor + \left\lfloor 2(\frac{ki}{p} - \left\lfloor \frac{ki}{p} \right\rfloor) \right\rfloor .$$

Damit ist $\left\lfloor \frac{2ki}{p} \right\rfloor$ gerade genau dann, wenn $\left\lfloor 2(\frac{ki}{p} - \left\lfloor \frac{ki}{p} \right\rfloor) \right\rfloor = 0$ ist. Dies bedeutet $\frac{ki}{p} - \left\lfloor \frac{ki}{p} \right\rfloor < \frac{1}{2}$, was wiederum zu $ki - p \left\lfloor \frac{ki}{p} \right\rfloor < p/2$ äquivalent ist. Der Term $ki - p \left\lfloor \frac{ki}{p} \right\rfloor$ ist der Rest von ki bei Division durch p. Nach Definition ist ϵ_i genau dann 1, wenn dieser Rest $< p/2$ ist.

(2). Aus Teil (1) und dem Gaußschen Vorzeichenlemma (Lemma 7.8) folgt wegen (mit $t = \frac{p-1}{2}$)

$$\left(\frac{k}{p}\right) = \prod_{i=1}^{t} \epsilon_i = \prod_{i=1}^{t} (-1)^{\lfloor \frac{2ki}{p} \rfloor} = (-1)^{S(2k,p)}$$

die Behauptung.

(3). Sei nun k ungerade. Dann ist $(p+k)/2$ eine ganze Zahl. Unter Verwendung von Teil (2) erhält man

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

Für den Exponenten rechts gilt

$$S(p+k,p) = \sum_{i=1}^{t} \left\lfloor \frac{i(p+k)}{p} \right\rfloor = \sum_{i=1}^{t} \left\lfloor \frac{ik}{p} \right\rfloor + \sum_{i=1}^{t} i = S(k,p) + \frac{(t+1)t}{2} .$$

Wegen $\frac{p^2-1}{8} = \frac{(p+1)}{2}\frac{(p-1)}{2}\frac{1}{2} = \frac{(t+1)t}{2}$ folgt nach dem zweitem Ergänzungssatz (Satz 7.9) die Identität $\left(\frac{2}{p}\right) = (-1)^{\frac{(t+1)t}{2}}$. Man kann daher in der Gesamtgleichungskette

$$\begin{aligned} \left(\frac{2}{p}\right)\left(\frac{k}{p}\right) &= (-1)^{S(p+k,p)} = (-1)^{S(k,p)+\frac{(t+1)t}{2}} \\ &= (-1)^{S(k,p)}(-1)^{\frac{(t+1)t}{2}} = (-1)^{S(k,p)} \left(\frac{2}{p}\right) \end{aligned}$$

kürzen und erhält die Aussage. □

Satz 8.2. *(Quadratisches Reziprozitätsgesetz) Seien p und q zwei verschiedene ungerade Primzahlen. Dann gilt:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} -1 & \textit{wenn} \quad p = q = 3 \mod 4 \\ 1 & \textit{sonst.} \end{cases}$$

Beweis. Sei $t = \frac{p-1}{2}$ und $u = \frac{q-1}{2}$. Nach Teil (3) des Lemmas 8.1 gilt $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{S(p,q)+S(q,p)}$, so dass also $tu = S(p,q) + S(q,p)$ zu zeigen ist. Betrachte

$$M = \{qi - pj : 1 \le i \le t,\, 1 \le j \le u\}\,.$$

Diese Menge besitzt tu Elemente, und $0 \notin M$, da ja p und q teilerfremd sind. Es seien M_- die negativen Elemente aus M und M_+ die positiven Elemente aus M. Es ist $qi - pj > 0$ genau dann, wenn $\frac{qi}{p} > j$ ist, was genau für $1 \le j \le \lfloor \frac{qi}{p} \rfloor$ der Fall ist. Zu jedem i, $1 \le i \le t$, gibt es also genau $\lfloor \frac{qi}{p} \rfloor$ Elemente in M_+. Damit hat M_+ genau $\sum_{i=1}^{t} \lfloor \frac{qi}{p} \rfloor = S(q,p)$ Elemente. Die entsprechende Überlegung liefert, dass M_- genau $S(p,q)$ Elemente besitzt, woraus

$$tu = |M| = |M_+| + |M_-| = S(q,p) + S(p,q)$$

folgt. □

Das quadratische Reziprozitätsgesetz kann man auch so formulieren: Sind p und q zwei verschiedene ungerade Primzahlen, so gilt:

$$\left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{q}{p}\right) & \text{wenn } p \equiv q \equiv 3 \pmod 4 \\ \left(\frac{q}{p}\right) & \text{sonst.} \end{cases}$$

Damit kann man die Berechnung von $\left(\frac{p}{q}\right)$ auf die Berechnung von $\left(\frac{q}{p}\right)$ zurückführen. Darauf beruht der folgende Algorithmus.

Bemerkung 8.3. Seien p und q ungerade verschiedene Primzahlen, und man möchte $\left(\frac{p}{q}\right)$ berechnen, also herausfinden, ob p ein quadratischer Rest modulo q ist oder nicht. Ist $p > q$, so berechnet man zuerst den Rest p mod q, und ersetzt p durch den kleineren Rest, der natürlich keine Primzahl sein muss. Ist hingegen $p < q$, so berechnet man die Reste von p und q modulo 4 und kann dann mittels dem quadratischen Reziprozitätsgesetz $\left(\frac{p}{q}\right)$ auf $\left(\frac{q}{p}\right)$ zurückführen. In beiden Fällen kommt man also auf eine Situation, wo $\left(\frac{k}{q}\right)$ zu berechnen ist, wo q eine ungerade Primzahl ist und $k < q$ beliebig. Sei $k = 2^\alpha \cdot p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ die Primfaktorzerlegung von k. Dann ist nach der Multiplikativität des Legendre-Symbols (Lemma 7.3)

$$\left(\frac{k}{q}\right) = \left(\frac{2^\alpha}{q}\right) \cdot \left(\frac{p_1^{\alpha_1}}{q}\right) \cdots \left(\frac{p_r^{\alpha_r}}{q}\right) = \left(\frac{2}{q}\right)^\alpha \cdot \left(\frac{p_1}{q}\right)^{\alpha_1} \cdots \left(\frac{p_r}{q}\right)^{\alpha_r}.$$

Jetzt kann $\left(\frac{2}{q}\right)$ nach dem 2. Ergänzungsgesetz (Satz 7.9) berechnet und die $\left(\frac{p_i}{q}\right)$ können für $i = 1, \ldots, r$ nach dem gleichen Verfahren auf die Berechnung von $\left(\frac{q}{p_i}\right)$ zurückgeführt werden (von den Exponenten α, α_i kommt es nur auf die Parität an). Bei diesem Verfahren werden natürlich die Nenner (und damit auch die Zähler) in den Legendre-Symbolen kleiner, so dass man schließlich das Resultat erhält.

Beispiel 8.4. Man möchte entscheiden, ob die Gleichung

$$x^2 = 10 \mod 13$$

eine Lösung besitzt. Dazu berechnet man

$$\left(\frac{10}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{5}{13}\right) .$$

Der erste Faktor

$$\left(\frac{2}{13}\right)$$

lässt sich mit Hilfe des zweiten Ergänzungssatzes zu -1 bestimmen, weil $13 \mod 8 = 5$ und $p = 5 \mod 8$ ergibt das Vorzeichen -1.

Um den zweiten Faktor zu berechnen, wendet man das Reziprozitätsgesetz an:

$$\left(\frac{5}{13}\right) = + \left(\frac{13}{5}\right) ,$$

weil $5 \mod 4 = 1$ gilt. $13 \mod 4$ braucht gar nicht mehr berechnet zu werden, da es ausreicht, dass hier 5 oder 13 modulo 4 den Rest 1 lässt, damit das Vorzeichen + ist. Jetzt nutzt man, dass $13 = 3 \mod 5$ ist. Man schreibt:

$$\left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) .$$

Wiederum wendet man hier das Quadratische Reziprozitätsgesetz an: Es ist

$$\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1 ,$$

da $5 \mod 4 = 1$ ist und da $2 = -1$ kein Quadrat modulo 3 ist.

Setzt man nun beide Faktoren zusammen, so ergibt sich folgendes Resultat:

$$\left(\frac{10}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{5}{13}\right) = (-1) \cdot (-1) = 1 .$$

Und damit weiß man, dass die obige Gleichung eine Lösung besitzt. (Die beiden Lösungen lauten 6 und 7. Auf dieses Ergebnis kommt man leider nur durch Probieren. Hat man aber eine Lösung, z.B. die 6, so berechnet man die zweite Lösung, indem man das additive Inverse im Körper $Z \mod 13$ bestimmt $(13 - 6 = 7)$.

Beispiel 8.5. Man möchte entscheiden, ob die Gleichung

$$x^2 = 57 \mod 127$$

eine Lösung besitzt. Dazu berechnet man

$$\left(\frac{57}{127}\right) = \left(\frac{3}{127}\right)\left(\frac{19}{127}\right)$$

und kann wie oben die beiden Faktoren mit dem Reziprozitätsgesetz weiter vereinfachen:

$$\left(\frac{3}{127}\right) = -\left(\frac{127}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

und

$$\left(\frac{19}{127}\right) = -\left(\frac{127}{19}\right) = -\left(\frac{13}{19}\right) = -\left(\frac{19}{13}\right) = -\left(\frac{6}{13}\right)$$

$$= (-1)\left(\frac{2}{13}\right)\left(\frac{3}{13}\right) = (-1)(-1)\left(\frac{13}{3}\right) = (-1)(-1)\left(\frac{1}{3}\right) = (-1)(-1)1 = 1$$

Setzt man alles zusammen, so ergibt sich

$$\left(\frac{57}{127}\right) = -1$$

und damit die Erkenntnis, dass die obige Gleichung keine Lösung besitzt.

Zur Berechnung des Legendre-Symbols muss man die Primfaktorzerlegung der beteiligten Zahlen kennen, was für große Zahlen ein erheblicher Rechenaufwand darstellen kann. Die Einführung des Jacobi-Symbols erlaubt es, zu entscheiden, ob eine Zahl quadratischer Rest ist oder nicht, ohne Primfaktorzerlegungen zu kennen.

Definition 8.6. Für eine ungerade Zahl n und eine ganze Zahl k definiert man das *Jacobi-Symbol*, geschrieben $\left(\frac{k}{n}\right)$ (k *nach* n), wie folgt. Es sei $n = p_1 \cdots p_r$ die Primfaktorzerlegung von n. Dann setzt man

$$\left(\frac{k}{n}\right) := \left(\frac{k}{p_1}\right) \cdots \left(\frac{k}{p_r}\right) .$$

Carl Gustav Jacob Jacobi (1804-1851)

Im Fall $n = p$ eine ungerade Primzahl ist das Jacobi-Symbol nichts anderes als das Legendre-Symbol. Das Jacobi-Symbol ist also eine Verallgemeinerung des Legendre-Symbols. Es ist aber zu beachten, dass die inhaltliche Definition des Legendre-Symbols sich im allgemeinen nicht auf das Jacobi-Symbol überträgt. Das Jacobi-Symbol ist *nicht* genau dann 1, wenn k ein Quadrat modulo n ist.

Lemma 8.7. *(Eigenschaften des Jacobi-Symbols) Seien k, k_1, k_2 ganze Zahlen und seien n, n_1, n_2 ungerade positive Zahlen. Dann gelten folgende Aussagen.*

(1) *Das Jacobi-Symbol $\left(\frac{k}{n}\right)$ hängt nur vom Rest $k \mod n$ ab.*
(2) *Es ist $\left(\frac{k_1 k_2}{n}\right) = \left(\frac{k_1}{n}\right)\left(\frac{k_2}{n}\right)$.*
(3) *Es ist $\left(\frac{k}{n_1 n_2}\right) = \left(\frac{k}{n_1}\right)\left(\frac{k}{n_2}\right)$.*

Beweis. Diese Aussagen folgen sofort aus der Definition des Jacobi-Symbols bzw. aus der Multiplikativität des Legendre-Symbols im Zähler. □

Für das Jacobi-Symbol gilt das quadratische Reziprozitäts mitsamt den Ergänzungssätzen.

Satz 8.8. *(Quadratisches Reziprozitätsgesetz mit Jacobi-Symbol) Seien n und m positive ungerade Zahlen. Dann gelten folgende Aussagen.*

(1) $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}}$.
(2) $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$.
(3) $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$.

Beweis. Diese Aussagen werden in den Übungen bewiesen. □

Bemerkung 8.9. Seien n und m ungerade verschiedene Zahlen, und man möchte das Jacobi-Symbol $\left(\frac{n}{m}\right)$ berechnen (man berechnet im Allgemeinen nicht, ob n ein quadratischer Rest modulo m ist, dies ist nur dann der Fall, wenn m eine Primzahl ist). Durch die Restberechnung $n \mod m$ können wir sofort annehmen, dass $n < m$ ist. Wir schreiben

$$n = 2^\alpha k\,,$$

wobei k ungerade sei. Dann gilt nach Lemma 8.7

$$\left(\frac{n}{m}\right) = \left(\frac{2^\alpha}{m}\right) \cdot \left(\frac{k}{m}\right) = \left(\frac{2}{m}\right)^\alpha \cdot \left(\frac{k}{m}\right)\,.$$

Hier kann, nach dem quadratischen Reziprozitätsgesetz für das Jacobi-Symbol (Satz 8.8) (und der Ergänzungssätze), $\left(\frac{2}{m}\right)$ berechnet werden und $\left(\frac{k}{m}\right)$ kann auf $\left(\frac{m}{k}\right)$ zurückgeführt werden. Bei diesem Verfahren werden natürlich die Nenner (und damit auch die Zähler) in den Jacobi-Symbolen kleiner, so dass man schließlich das Resultat erhält.

9. Vorlesung

In diesem Abschnitt werden wir die Frage beantworten, welche ganze Zahlen sich also Summe von zwei Quadraten darstellen lassen, oder, anders formuliert, wann die diophantische Gleichung

$$n = x^2 + y^2$$

eine Lösung mit ganzen Zahlen x, y besitzt. Wir werden dabei wesentlich den Ring der Gaußschen Zahlen $\mathbb{Z}[\mathrm{i}]$ verwenden und schließen dabei an Vorlesung 2 an. Zunächst betrachten wir den Fall, wo $n = p$ eine ungerade Primzahl ist. Es gilt folgende Charakterisierung.

Satz 9.1. *Sei p ein ungerade Primzahl. Dann sind folgende Aussagen äquivalent.*

(1) *p ist die Summe von zwei Quadraten, $p = x^2 + y^2$ mit $x, y \in \mathbb{Z}$.*
(2) *p ist die Norm eines Elementes aus $\mathbb{Z}[\mathrm{i}]$.*
(3) *p ist zerlegbar (nicht prim) in $\mathbb{Z}[\mathrm{i}]$.*
(4) *-1 ist ein Quadrat in $\mathbb{Z}/(p)$.*
(5) $p = 1 \mod 4$

Beweis. (1) $\Leftrightarrow$ (2). Dies folgt sofort aus $x^2+y^2 = (x+y\mathrm{i})(x-y\mathrm{i}) = N(x+y\mathrm{i})$ (diese Äquivalenz gilt für alle ganze Zahlen).

(2) $\Rightarrow$ (3). Die Normdarstellung

$$p = N(x + y\mathrm{i}) = (x + y\mathrm{i})(x - y\mathrm{i})$$

ist eine Faktorzerlegung in $\mathbb{Z}[\mathrm{i}]$. Da x und y beide von null verschieden sind, ist $N(x + iy) \geq 2$ und $x + y\mathrm{i}$ ist keine Einheit, also ist die Zerlegung nicht trivial. Da der Ring der Gaußschen Zahlen euklidisch ist, sind prim und unzerlegbar äquivalent.

(3) $\Rightarrow$ (2). Sei p zerlegbar, sagen wir $p = wz$ mit Nichteinheiten $w, z \in \mathbb{Z}[\mathrm{i}]$. Dann ist $p^2 = N(p) = N(w)N(z)$. Dann muss $N(w) = p$ sein.

(3) $\Leftrightarrow$ (4). Es gilt

$$\mathbb{Z}[\mathrm{i}]/(p) \cong (\mathbb{Z}[X]/(X^2+1))/(p) \cong \mathbb{Z}[X]/(X^2+1, p) \cong (\mathbb{Z}/(p)[X])/(X^2+1)\,.$$

Dieser (endliche) Restklassenring ist ein Körper genau dann, wenn p prim in $\mathbb{Z}[\mathrm{i}]$ ist (wegen Satz 3.11). Andererseits zeigt die Darstellung rechts, dass ein Körper genau dann vorliegt, wenn das Polynom $X^2 + 1$ ein irreduzibles Polynom in $(\mathbb{Z}/(p))[X]$ ist, und dies ist genau dann der Fall, wenn das Polynom keine Nullstelle in $\mathbb{Z}/(p)$ besitzen, was bedeutet, dass -1 kein Quadrat in $\mathbb{Z}/(p)$ ist.

Die Äquivalenz (4) $\Leftrightarrow$ (5) wurde schon im Satz 6.7 gezeigt. □

Bemerkung 9.2. Sei p eine Primzahl, die modulo 4 den Rest 1 besitzt, so dass es nach Satz 9.1 eine Darstellung als Summe von zwei Quadraten geben

muss. Wie findet man eine solche Darstellung explizit? Einerseits durch probieren, andererseits kann man aber entlang dem Beweis des Satzes vorgehen. Dazu muss man folgende Schritte gehen:

(1) Finde in $\mathbb{Z}/(p)$ ein Element a mit $a^2 = -1$. Um dies zu finden braucht man in der Regel ein primitives Element in diesem Restklassenkörper (ist b ein primitives Element, so kann man $a = b^{(p-1)/4}$ nehmen; siehe auch Aufgabe 11.9).
(2) Die Abbildung $\mathbb{Z}[\mathrm{i}] \to \mathbb{Z}/(p)$, die ganze Zahlen modulo p nimmt und i auf a schickt, ist ein surjektiver Ringhomomorphismus auf einen Körper. Der Kern ist ein Hauptideal, das von p und von $a - \mathrm{i}$ erzeugt wird.
(3) Finde mit dem euklidischen Algorithmus einen Erzeuger z für das Hauptideal $(p, a - \mathrm{i})$. Ein solcher Erzeuger hat die Norm $N(z) = p$.

Beispiel 9.3. Sei $p = 13$ (man sieht natürlich sofort eine Darstellung). Mit dem oben beschriebenen Verfahren müsste man wie folgt vorgehen:

In $\mathbb{Z}/(13)$ ist $5^2 = 25 = -1$, also kann man $a = 5$ nehmen. Dies führt zum Ideal $(13, 5 - \mathrm{i})$.

Die Division mit Rest liefert

$$\frac{13}{5 - \mathrm{i}} = \frac{13(5 + \mathrm{i})}{(5 - \mathrm{i})(5 + \mathrm{i})} = \frac{65 + 13\mathrm{i}}{26}\,.$$

und 2 ist eine beste Approximation. Damit ist:

$$13 = 2 \cdot (5 - \mathrm{i}) + r \text{ mit } r = 3 + 2\mathrm{i}\,.$$

Die nächste durchzuführende Division liefert

$$\frac{5 - \mathrm{i}}{3 + 2\mathrm{i}} = \frac{(5 - \mathrm{i})(3 - 2\mathrm{i})}{13} = \frac{13 - 13\mathrm{i}}{13} = 1 - \mathrm{i}\,.$$

Damit ist also $5 - \mathrm{i} = (1 - \mathrm{i})(3 + 2\mathrm{i})$ und somit ist $3 + 2\mathrm{i}$ ein Erzeuger des Ideals.

Aus dem Hauptsatz können wir problemlos ableiten, wie sich die Primzahlen in $\mathbb{Z}[\mathrm{i}]$ verhalten:

Korollar 9.4. *(Primzahlen in $\mathbb{Z}[\mathrm{i}]$) Die Primzahlen haben in $\mathbb{Z}[\mathrm{i}]$ folgendes Zerlegungsverhalten:*

- *Es ist $2 = -\mathrm{i}(1 + i)^2$, und $1 + \mathrm{i}$ ist prim in $\mathbb{Z}[\mathrm{i}]$.*
- *Für $p = 1 \mod 4$ ist $p = (x + y\mathrm{i})(x - y\mathrm{i})$, wobei beide Faktoren prim sind.*
- *Für $p = 3 \mod 4$ ist p prim in $\mathbb{Z}[\mathrm{i}]$.*

Beweis. Aufgrund von Satz 9.1 ist im zweiten Fall lediglich noch zu zeigen, dass die beiden Faktoren prim sind. Wegen

$$p^2 = N(p) = N(x + y\mathrm{i})N(x - y\mathrm{i})$$

haben die beiden Faktoren die Norm p und sind deshalb nach Lemma 2.14 prim. □

Bemerkung 9.5. Für eine Gaußsche Zahl $z \in \mathbb{Z}[i]$ kann man folgendermaßen entscheiden, ob sie prim ist bzw. wie ihre Primfaktorzerlegung aussieht:

(1) Berechne die Norm $N(z)$. Ist diese eine Primzahl, so ist nach Lemma 2.14 das Element z selbst prim.
(2) Bestimme die (ganzzahligen) Primfaktoren von $N(z)$. Schreibe
$$N(z) = z\bar{z} = 2^r p_1 \cdots p_s q_1 \cdots q_t \,,$$
wobei die p_i ungerade mit Rest 1 modulo 4 und die q_j ungerade mit Rest 3 modulo 4 seien.
(3) Schreibe $p_i = N(u_i) = u_i\overline{u_i}$ für die Primfaktoren p_i mit Rest 1 modulo 4, und $2^r = (-i)^r(1+i)^{2r}$. Damit ist
$$z\bar{z} = (-i)^r(1+i)^{2r} u_1\overline{u_1} \cdots u_s\overline{u_s} q_1 \cdots q_t \,.$$
(4) Liste die möglichen Primfaktoren von z (und zugleich von $\overline{z}$) auf: das sind $1+i$ (falls 2 mit positivem Exponenten vorkommt), die u_i und $\overline{u_i}$ sowie die q_j (da $\mathbb{Z}[i]$ ein Hauptidealbereich ist und somit die eindeutige Primfaktorzerlegung gilt, setzt sich die Primfaktorzerlegung von z und von $\bar{z}$ aus Primfaktoren der rechten Seite zusammen).
(5) Durch 2^r und die q_j kann man sofort durchdividieren.
(6) Für die möglichen Primfaktoren u_i und $\overline{u_i}$ muss man überprüfen (durch Division mit Rest), ob sie Primfaktoren von z sind oder nicht (wenn nicht, so teilen sie $\bar{z}$). Statt Division kann man auch die möglichen Kombinationen ausmultiplizieren.

Wie kommen nun zur Bestimmung aller ganzen Zahlen, die Summe von zwei Quadraten sind.

Lemma 9.6. $2 = 1 + 1$ *ist eine Summe von Quadraten.*

Sind die natürlichen Zahlen m und n jeweils eine Summe von Quadratzahlen, so ist auch das Produkt mn eine Summe von Quadratzahlen.

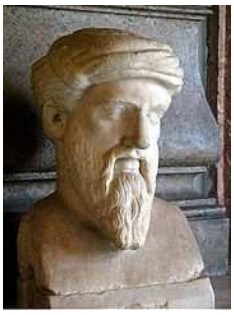
Ist $n = r^2 m$, und ist m eine Summe von Quadratzahlen, so auch n.

Beweis. Die erste Aussage ist klar, für die zweite hat man die Charakterisierung mit der Norm und die Multiplikativität der Norm auszunutzen. Ist $m = x^2 + y^2$, so kann man einfach mit r^2 multiplizieren. □

Satz 9.7. *(Charakterisierung von Quadratsummen) Sei n eine positive natürliche Zahl. Schreibe $n = r^2 m$, wobei jeder Primfaktor von m nur einfach vorkomme. Dann ist n die Summe von zwei Quadraten genau dann, wenn in der Primfaktorzerlegung von m nur 2 und Primzahlen vorkommen, die modulo 4 den Rest 1 haben.*

Beweis. Erfüllt n die angegebene Bedingung an die Primfaktorzerlegung, so ist n nach dem vorangehenden Lemma und dem Hauptsatz die Summe zweier Quadrate. Sei umgekehrt angenommen, dass n die Summe zweier Quadrate ist, so dass also eine Zerlegung $n = (x + \mathrm{i}y)(x - \mathrm{i}y)$ vorliegt. Sei p ein Primfaktor von n, der modulo 4 den Rest 3 besitze. Dann ist nach Satz 9.1 p prim in $\mathbb{Z}[\mathrm{i}]$ und teilt einen und damit (betrachte die Konjugation) beide Faktoren in der Zerlegung, jeweils mit dem gleichen Exponenten. Damit ist der Exponent von p in der Primfaktorzerlegung von n gerade und p kommt in der Primfaktorzerlegung von m nicht vor. □

10. Vorlesung

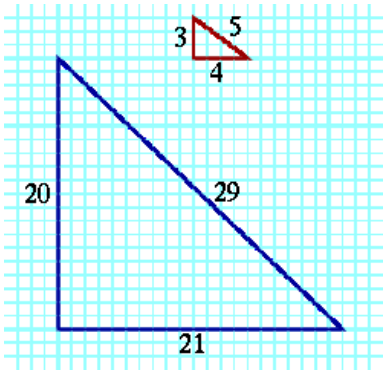


Büste des Pythagoras von Samos (6. Jh v. Chr.)

Definition 10.1. Ein *pythagoreisches Tripel* ist eine ganzzahlige Lösung $(x, y, z) \in \mathbb{Z}^3$ der diophantischen Gleichung

$$x^2 + y^2 = z^2 \,.$$

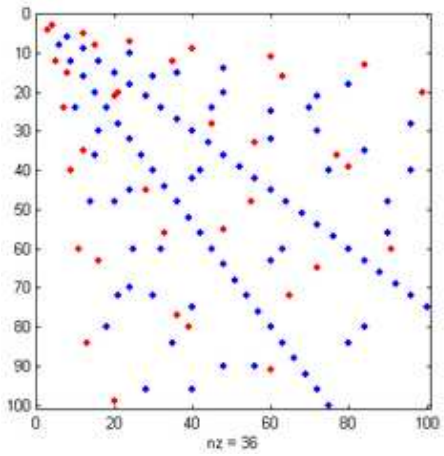
Es heißt *primitiv*, wenn x, y, z keinen gemeinsamen Teiler besitzen.



Bemerkung 10.2. Lösungstripel, bei denen (mindestens) ein Eintrag null ist, heißen trivial. Nach der Umkehrung des Satzes des Pythagoras bildet ein solches Tripel die Seitenlängen eines rechtwinkligen Dreieckes. Es geht also um rechtwinklige Dreiecke mit der Eigenschaft, dass alle drei Seiten eine ganzzahlige Länge haben (dabei sind x, y die Seitenlängen der Katheden und z ist die Seitenlänge der Hypothenuse). Das bekannteste pythagoreische

Tripel ist zweifellos $(3, 4, 5)$. Wenn zwei Zahlen davon einen gemeinsamen Teiler haben, so hat natürlich auch die dritte diesen Teiler, und das Tripel ist nicht primitiv.

Ferner sind x und y nicht zugleich ungerade, siehe Aufgabe 10.1.



Die roten Punkte sind primitive pythagoreische Tripel, die blauen nicht-primitive

Wir wollen alle (primitiven) pythagoreischen Tripel finden. Man kann das Problem umformulieren, indem man durch z^2 teilt. Dann ist das Problem äquivalent zu:

Bestimme alle rationalen Lösungen für die Gleichung

$$r^2 + s^2 = 1 \ (r, s \in \mathbb{Q}) \, .$$

Es geht also um alle Punkte auf dem Einheitskreis (in der Ebene mit Mittelpunkt $(0, 0)$ und Radius 1, deren beide Koordinaten rationale Zahlen sind. Die trivialen Lösungen sind die komplexen Zahlen $1, \mathrm{i}, -1, -\mathrm{i}$.

Bemerkung 10.3. Der (Einheits-)Kreis ist ein eindimensionales Objekt und es gibt verschiedene (Teil-)Parametrisierungen für ihn, etwa durch

$$x \longmapsto (x, \sqrt{1 - x^2}) \, ,$$

oder die trigonometrische Parametrisierung

$$t \longmapsto (\cos(t), \sin(t)) \, ,$$

Hier brauchen wir aber eine Parametrisierung, die rationale Zahlen in solche Punkte überführt, deren beide Koordinaten rational sind.

Wir betrachten hierzu die Abbildung, die einen Punkt t auf der y-Achse auf den Durchstoßungspunkt (x, y) abbildet, den der Einheitskreis mit der durch $(0, t)$ und $(-1, 0)$ definierten Geraden bildet. Aufgrund des Strahlensatzes haben wir die Bedingung

$$\frac{t}{1} = \frac{y}{1 + x}$$

bzw. $y = t(1+x)$. Setzt man diese Gleichung in die Gleichung des Einheitskreises ein, so erhält man

$$1 = x^2 + y^2 = x^2 + t^2(x+1)^2$$

und damit

$$0 = (x^2-1) + t^2(x+1)^2 = (x+1)\left((x-1) + t^2(x+1)\right) .$$

Da uns die erste Lösung $x = -1$ nicht interessiert, betrachten wir den zweiten Faktor

$$0 = (x-1) + t^2(x+1) = x(1+t^2) + t^2 - 1 ,$$

die zu

$$x = \frac{1-t^2}{1+t^2} \quad \text{und} \quad y = t \cdot (x+1) = t \cdot \left(\frac{1-t^2}{1+t^2} + 1\right) = \frac{2t}{1+t^2}$$

führt. Die Abbildung

$$t \longmapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) = (x,y)$$

ist also eine rationale Parametrisierung des Einheitskreises.

Wir fassen zusammen:

Satz 10.4. *Die Abbildung*

$$\mathbb{Q} \longrightarrow S^1_{\mathbb{Q}},\ t \longmapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) = (x,y) ,$$

von der Menge der rationalen Zahlen in die Menge der Punkte auf dem Einheitskreis mit rationalen Koordinaten ist injektiv, und mit der Ausnahme von $(-1,0)$ *liegt jeder Punkt im Bild.*

Beweis. Dies wurde bereits oben bewiesen, die Injektivität ist klar von der geometrischen Interpretation her und ist als eine Übung zu beweisen. □

Korollar 10.5. *Die Menge der Punkte auf dem Einheitskreis mit rationalen Koordinaten bilden eine dichte Teilmenge.*

Beweis. Die Parametrisierung

$$\varphi : \mathbb{R} \longrightarrow S^1,\ t \longmapsto \varphi(t) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) ,$$

ist stetig, da sie komponentenweise durch rationale Funktionen gegeben ist. Sei $s \in S^1$ ein Punkt des Einheitskreises. Der Punkt $s = (-1,0)$ (der Punkt, der von der Parametrisierung nicht erfasst wird), ist selbst rational. Sei also $s \neq (-1,0)$, und sei $t \in \mathbb{R}$ eine reelle Zahl mit $\varphi(t) = s$. Sei $\epsilon > 0$ vorgegeben. Aufgrund der Stetigkeit gibt es dann auch ein $\delta > 0$ derart, dass die Ballumgebung $B(t,\delta)$ nach $B(s,\epsilon)$ hinein abgebildet wird, also $\varphi(B(t,\delta)) \subseteq B(s,\epsilon)$.

Da die rationalen Zahlen innerhalb der reellen Zahlen dicht liegen, gibt es eine rationale Zahl $q \in B(t, \delta)$. Dann ist $\varphi(q)$ ein Punkt auf dem Einheitskreis mit rationalen Koordinaten, der in der ϵ-Umgebung von s liegt. □

u	v	$x = u^2 - v^2$	$y = 2uv$	$z = u^2 + v^2$	$x^2 + y^2 = z^2$
2	1	3	4	5	$9 + 16 = 25$
3	2	5	12	13	$25 + 144 = 169$
4	1	15	8	17	$225 + 64 = 289$
4	3	7	24	25	$49 + 576 = 625$
5	2	21	20	29	$441 + 400 = 841$
6	1	35	12	37	$1225 + 144 = 1369$
5	4	9	40	41	$81 + 1600 = 1681$
7	2	45	28	53	$2025 + 784 = 2809$
6	5	11	60	61	$121 + 3600 = 3721$
7	4	33	56	65	$1089 + 3136 = 4225$
8	1	63	16	65	$3969 + 256 = 4225$
8	3	55	48	73	$3025 + 2304 = 5329$
7	6	13	84	85	$169 + 7056 = 7225$
9	2	77	36	85	$5929 + 1296 = 7225$
8	5	39	80	89	$1521 + 6400 = 7921$
9	4	65	72	97	$4225 + 5184 = 9409$

Satz 10.6. *(Charakterisierung pythagoreischer Tripel) Sei (x, y, z) ein pythagoreisches Tripel mit y gerade und $z \neq -x$. Dann gibt es eindeutig bestimmte ganze teilerfremde Zahlen (u, v) mit $u > 0$ und $a \in \mathbb{Z}$ und mit*

$$x = a(u^2 - v^2),\ y = a(2uv),\ z = a(u^2 + v^2)\,.$$

Das pythagoreische Tripel ist primitiv genau dann, wenn a eine Einheit ist und u und v nicht beide ungerade sind.

Beweis. Sei (x, y, z) ein pythagoreisches Tripel. Der Fall $z = 0$ ist ausgeschlossen. Dann ist $(\frac{x}{z}, \frac{y}{z})$ ein Punkt auf dem Einheitskreis mit rationalen Koordinaten. Nach Satz 10.4 gibt es, da $z \neq -x$ vorausgesetzt wurde, eine eindeutig bestimmte rationale Zahl t mit

$$\left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right) = (\frac{x}{z}, \frac{y}{z})\,.$$

Dann gibt es eine rationale Zahl $q \neq 0$ mit

$$x = q(1 - t^2),\ y = q2t,\ z = q(1 + t^2)\,.$$

Sei $t = \frac{v}{u}$ mit ganzen teilerfremden Zahlen u, v, $u > 0$. Wir ersetzen q durch $\tilde{q} = \frac{q}{u^2}$ und haben dann

$$x = \tilde{q}(u^2 - v^2),\ y = \tilde{q}2uv,\ z = \tilde{q}(u^2 + v^2)\,.$$

Da u und v teilerfremd sind, sind auch $u, v, u^2 - v^2$ paarweise teilerfremd. Ein Primteiler des Nenners von $\tilde{q}$ teilt $2uv$ und $u^2 - v^2$. Daher kommt nur 2 in Frage. In diesem Fall wären aber $u^2 - v^2$ und $u^2 + v^2$ gerade, und u und v wären beide ungerade. Dann wäre aber $y = \tilde{q}2uv$ ungerade im Widerspruch zur Voraussetzung. Also ist $\tilde{q}$ eine ganze Zahl.

Wenn das pythagoreische Tripel primitiv ist, so muss in dieser Darstellung $\tilde{q} = 1$ oder -1 sein. Außerdem können dann u und v nicht beide ungerade sein, sonst wäre 2 ein gemeinsamer Teiler des Tripels. Wenn umgekehrt diese Bedingungen erfüllt sind, so ist das Tripel primitiv. □

Satz 10.7. *(Satz von Euler) Die diophantische Gleichung*

$$x^4 + y^4 = z^2$$

hat keine ganzzahlige nichttriviale Lösung.

Beweis. Sei (x, y, z) eine nichttriviale Lösung, d.h. alle Einträge sind $\neq 0$. Wir können annehmen, dass alle Einträge sogar positiv sind. Wenn es eine solche Lösung gibt, dann gibt es auch eine nichttriviale Lösung mit minimalem positivem z (unter allen nichttrivialen Lösungen). Wir zeigen, dass es dann eine Lösung mit kleinerem positiven z_1 gibt, was einen Widerspruch bedeutet.

Wegen der Minimalität ist (x, y, z) primitiv, die Einträge sind also (sogar paarweise) teilerfremd. Wir können x als ungerade annehmen. Es ist dann

$$(x^2, y^2, z)$$

ein primitives pythagoreisches Tripel. Daher gibt es nach Satz 10.6 teilerfremde natürliche Zahlen (u, v) mit

$$x^2 = u^2 - v^2,\ y^2 = 2uv,\ z = u^2 + v^2$$

und mit $u + v$ ungerade. Betrachtung der ersten Gleichung modulo 4 zeigt, dass u ungerade sein muss (und v gerade). Die erste Gleichung

$$u^2 = x^2 + v^2$$

ist selbst ein primitives pythagoreisches Tripel. Es gibt als erneut teilerfremde natürliche Zahlen (r, s) mit

$$x = r^2 - s^2,\ v = 2rs,\ u = r^2 + s^2$$

(x ist ungerade, v gerade) mit $r + s$ ist ungerade. Somit sind $r, s, r^2 + s^2 = u$ paarweise teilerfremd. Aus

$$y^2 = 2uv = 4(r^2 + s^2)rs$$

folgt

$$\left(\frac{y}{2}\right)^2 = (r^2 + s^2)rs$$

und aus der Teilerfremdheit der Faktoren folgt, dass die einzelnen Faktoren hier selbst Quadrate sind, also

$$r = x_1^2,\ s = y_1^2,\ r^2 + s^2 = z_1^2\,.$$

Damit ist

$$z_1^2 = r^2 + s^2 = x_1^4 + y_1^4$$

eine neue nichttriviale Lösung der ursprünglichen Gleichung. Wegen

$$z_1 \leq z_1^2 = r^2 + s^2 = u < u^2 + v^2 = z$$

widerspricht dies der Minimalität von z. □

Korollar 10.8. *(Großer Fermat für Exponenten vier) Die Fermat-Quartik*

$$x^4 + y^4 = z^4$$

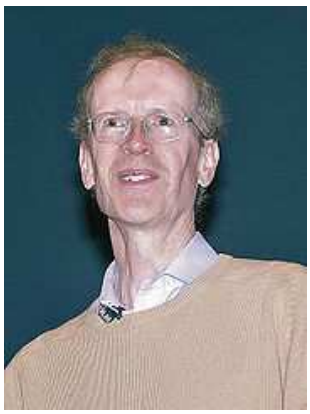
hat keine ganzzahlige nichttriviale Lösung.

Beweis. Dies folgt sofort aus dem Satz von Euler (Satz 10.7). □

Generell nennt man Gleichungen der Form

$$x^n + y^n = z^n$$

Fermat-Gleichungen. Die berühmte Vermutung von Fermat, der sogenannte „Große Fermat“, besagt, dass es für $n \geq 3$ keine nicht-trivialen Lösungen gibt. Dies haben wir soeben für $n = 4$ bewiesen. Der Fall $n = 3$ (Fermat-Kubiken) lässt sich ebenfalls noch einigermaßen elementar bestätigen (Euler) und hat mit den Eisenstein-Zahlen zu tun. Nach rund 350 Jahren wurde der Große Fermat schließlich 1995 von Andrew Wiles bewiesen.



Andrew Wiles (*1953)

Satz 10.9. *(von Wiles (Großer Fermat)) Die diophantischen Gleichungen*

$$x^n + y^n = z^n$$

besitzen für $n \geq 3$ keine ganzzahligen nichttriviale Lösungen.

Beweis. Der Beweis für diese Aussage geht bei Weitem über den Inhalt einer Vorlesung über elementare Zahlentheorie hinaus. □

11. Vorlesung

Satz 11.1. *(von Euklid) Es gibt unendlich viele Primzahlen.*

Beweis. Angenommen, die Menge aller Primzahlen sei endlich, sagen wir $\{p_1, p_2, \ldots, p_r\}$. Man betrachtet die Zahl

$$N = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_r \ + 1 \, .$$

Diese Zahl ist durch keine der Primzahlen p_i teilbar, da immer ein Rest 1 verbleibt. Damit sind die Primfaktoren von N nicht in der Ausgangsmenge enthalten - Widerspruch. □

Kann man weitere Aussagen darüber machen, wieviele Primzahlen es gibt? Wir werden zunächst die Frage betrachten, was man über die Reihe

$$\sum_{p \in \mathbb{P}} \frac{1}{p}$$

sagen kann. Dies ist also die Summe aller Kehrwerte von Primzahlen,

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \ldots \, .$$

Bekanntlich divergiert die harmonische Reihe, also die Summe über aller Kehrwerte von positiven ganzen Zahlen. Dagegen konvergiert die Summe über alle Kehrwerte von Quadraten, es gibt also im gewissen Sinn wenig Quadrate. Für jede unendliche Teilmenge $M \subseteq \mathbb{N}$ ist es eine interessante und meistens schwierige Frage, ob $\sum_{n \in M} \frac{1}{n}$ konvergiert oder divergiert. Für die Primzahlen werden wir das hier in Kürze beantworten. Die Beantwortung hängt eng mit der Riemannschen ζ-Funktion zusammen. Die hier benutzten Methoden gehören zur analytischen Zahlentheorie.

Georg Friedrich Bernhard Riemann (1826-1866)

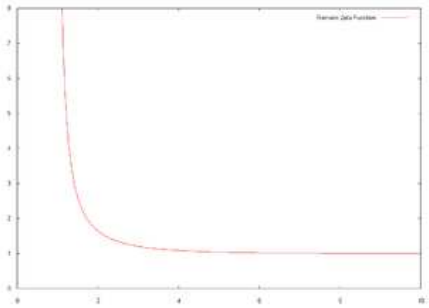
Definition 11.2. Die *Riemannsche ζ-Funktion* ist für $s \in \mathbb{C}$ mit Realteil 1 definiert durch

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Satz 11.3. *(Geometrische Reihe) Für alle komplexen Zahlen z mit $|z| < 1$ konvergiert die Reihe $\sum_{k=0}^{\infty} z^k$ und es gilt*

$$\sum_{k=0}^{\infty} z^k = \frac{1}{1-z}.$$

Beweis. Dies wird in der Grundvorlesung Analysis bewiesen. □



Lemma 11.4. *Sei T eine endliche Menge von Primzahlen und sei s eine komplexe Zahl mit $\Re(s) > 0$. Es sei $M(T)$ die Menge aller natürlichen Zahlen, die sich als Produkt von Primzahlen aus T darstellen lassen. Dann ist*

$$\prod_{p \in T} \frac{1}{1-p^{-s}} = \sum_{n \in M(T)} \frac{1}{n^s}.$$

Beweis. Sei $T = \{p_1, \ldots, p_k\}$. Es ist $|p^{-s}| < 1$ nach Voraussetzung über den Realteil. Unter Verwendung der geometrischen Reihe ergibt sich

$$\begin{aligned}
\prod_{p \in T} \frac{1}{1-p^{-s}} &= \frac{1}{1-p_1^{-s}} \cdots \frac{1}{1-p_k^{-s}} \\
&= \left(\sum_{i=0}^{\infty} (p_1^{-s})^i \right) \cdots \left(\sum_{i=0}^{\infty} (p_k^{-s})^i \right) \\
&= \sum_{0 \le i_1, \ldots, i_k < \infty} (p_1^{-s})^{i_1} \cdots (p_k^{-s})^{i_k} \\
&= \sum_{n \in M(T)} n^{-s}.
\end{aligned}$$

□

Aus dieser Aussage ergibt sich sofort ein neuer Beweis dafür, dass es unendlich viele Primzahlen gibt. Wenn es nämlich nur endlich viele Primzahlen gäbe, so könnte man T als die endliche Menge aller Primzahlen ansetzen. Für $s = 1$ stünde dann links eine reelle Zahl, und rechts würde die Summe

über alle natürlichen Kehrwerte stehen. Dies ist aber die harmonische Reihe, und diese divergiert!

Satz 11.5. *(Produktdarstellung der Riemannschen ζ-Funktion) Sei s eine komplexe Zahl mit $\Re(s) > 1$. Dann gilt für die Riemannsche ζ-Funktion die Produktdarstellung*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} \frac{1}{1 - p^{-s}} \,.$$

Beweis. Dies folgt aus Lemma 11.4, wenn man für T die ersten k Primzahlen überhaupt ansetzt und dann k gegen unendlich laufen lässt. Die Konvergenz der linken Seite, also die Wohldefiniertheit der ζ-Funktion, sichert dabei auch die Konvergenz der rechten Seite. □

Korollar 11.6. *Das unendliche Produkt*

$$\prod_{p \in \mathbb{P}} \frac{1}{1 - p^{-1}}$$

divergiert.

Beweis. Dies folgt aus der endlichen Produktdarstellung (Satz 11.5) für $s = 1$. Man hat die Gleichheit

$$\prod_{p \in T_k} \frac{1}{1 - p^{-1}} = \sum_{n \in M(T_k)} \frac{1}{n} \,,$$

wobei T_k die ersten k Primzahlen umfasse. Für $k \to \infty$ ergibt sich rechts die harmonische Reihe, die bekanntlich divergiert. Also divergiert auch das Produkt links. □

Wir können nun die oben formulierte Frage beantworten.

Satz 11.7. *(Euler) Die Reihe der Kehrwerte der Primzahlen, also*

$$\sum_{p \in \mathbb{P}} \frac{1}{p}$$

divergiert.

Beweis. Das Produkt $\prod_{i=1}^{k} \frac{1}{1-p_i^{-1}}$ divergiert für $k \to \infty$ aufgrund von Korollar 11.6 und ist insbesondere unbeschränkt. Daher ist auch der natürliche Logarithmus davon unbeschränkt. Dieser ist

$$\ln\left(\prod_{i=1}^{k} \frac{1}{1 - p_i^{-1}}\right) = \sum_{i=1}^{k} \ln\left(\frac{1}{1 - p_i^{-1}}\right) = -\sum_{i=1}^{k} \ln(1 - p_i^{-1}) \,.$$

Die Potenreihenentwicklung des natürlichen Logarithmus ist

$$\ln(1 - x) = -\sum_{j=1}^{\infty} \frac{x^j}{j}$$

für $|x| < 1$. Angewendet auf die vorstehende Situation ergibt das

$$= \sum_{i=1}^{k} (\sum_{j=1}^{\infty} \frac{(p_i^{-1})^j}{j}) = \sum_{i=1}^{k} \frac{1}{p_i} + \sum_{i=1}^{k} \left(\sum_{j=2}^{\infty} \frac{(p_i^{-1})^j}{j} \right) .$$

Für die hinteren Summanden hat man die Abschätzungen

$$\sum_{j=2}^{\infty} \frac{(p_i^{-1})^j}{j} \leq \sum_{j=2}^{\infty} \left(\frac{1}{p_i} \right)^j = \left(\frac{1}{p_i} \right)^2 \left(\sum_{j=0}^{\infty} \left(\frac{1}{p_i} \right)^j \right) = \left(\frac{1}{p_i} \right)^2 \frac{1}{1 - p_i^{-1}} \leq \frac{2}{p_i^2} ,$$

wobei hinten wieder die geometrische Reihe benutzt wurde. Damit ist insgesamt

$$\sum_{i=1}^{k} \left(\sum_{j=2}^{\infty} \frac{(p_i^{-1})^j}{j} \right) \leq \sum_{i=1}^{k} \frac{2}{p_i^2} \leq 2 \sum \frac{1}{n^2} .$$

Da die Summe der reziproken Quadrate konvergiert, ist diese Gesamtsumme beschränkt. Daher ist die Summe $\sum_{i=1}^{k} \frac{1}{p_i}$ unbeschränkt, was die Behauptung ist. □

Bemerkung 11.8. Ein Primzahlzwilling ist ein Paar bestehend aus p und $p + 2$, wobei diese beiden Zahlen Primzahlen sind. Die ersten Beispiele sind

$$(3, 5),\ (5, 7),\ (11, 13),\ (17, 19),\ (29, 31), \ldots .$$

Es ist ein offenes Problem der Zahlentheorie, ob es unendlich viele Primzahlzwillinge gibt (was aber stark vermutet wird). Dagegen ist bekannt, dass die zugehörige Reihe, also

$$\sum_{p, p+2 \in \mathbb{P}} \frac{1}{p}$$

konvergiert. In diesem Sinne gibt es also, verglichen mit der Gesamtzahl der Primzahlen, wenige Primzahlzwillinge.

Die Funktion $\pi(x)$

Es gehört zu den schwierigsten Fragen der Zahlentheorie und der Mathematik überhaupt, die Verteilung der Primzahlen zu verstehen. Viele offene Fragen und Vermutungen beziehen sich auf Teilaspekte dieses Problems.

Einfachere Fragestellungen, die bereits die Schwierigkeit im Allgemeinen erahnen lassen, sind etwa: gibt es mehr Primzahlen unterhalb von n als zwischen n und n^2? Gibt es stets eine Primzahl zwischen n und $2n$? Gibt es stets eine Primzahl zwischen n^2 und $(n + 1)^2$?

Es ist hilfreich, folgende Funktion einzuführen, die Primzahlfunktion genannt wird.

Definition 11.9. Die für $x \in \mathbb{R}$ definierte Funktion

$$x \longmapsto \pi(x) := \#\{p \leq x, p \text{ Primzahl}\}$$

heißt *Primzahlfunktion*.

Bemerkung 11.10. Die Primzahlfunktion zählt also, wieviele Primzahlen es unterhalb einer gewissen Schranke gibt. Sie nimmt offenbar nur natürliche Zahlen als Werte an und sie ist eine monton wachsende Treppenfunktion. Sie hat genau an den Primzahlen eine Sprungstelle. Die Frage nach der Verteilung von Primzahlen ist gleichbedeutend dazu, gute Approximationen bzw. Abschätzungen für sie durch andere, besser verstandene (analytische) Funktionen zu finden.

Jacques Salomon Hadamard (1865 Versailles - 1963 Paris)

Charles-Jean de La Vallée Poussin (1866 Löwen - 1962 Brüssel)

Ein Hauptresultat der analytischen Zahlentheorie ist der sogenannte Primzahlsatz von Hadamard und de la Vallée Pousin von 1896. Es besagt grob gesprochen, dass sich die Primzahlfunktion $\pi(x)$ in etwa so verhält wie $x/\ln(x)$, also dass der Quotient der beiden Funktionen gegen 1 konvergiert. Hier tritt der natürliche Logarithmus (zur Basis e) auf.

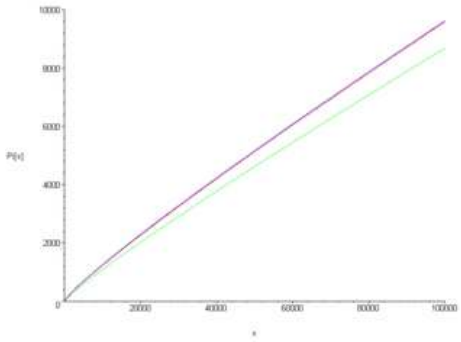
Satz 11.11. *Es gilt die asymptotische Abschätzung*

$$\pi(x) \sim \frac{x}{\ln(x)}\,.$$

Das heißt, dass

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln(x)}} = \lim_{x\to\infty} \frac{\pi(x)\ln(x)}{x} = 1\,.$$

Beweis. Dies ist ein Satz der analytischen Zahlentheorie, den wir hier nicht beweisen. □



Wir erwähnen abschließend ohne Beweis noch den Satz von Dirichlet. Einzelne Spezialfälle werden in den Aufgaben besprochen.

Peter Gustav Lejeune Dirichlet (1805-1859)

Satz 11.12. *(von Dirichlet) Sei n eine natürliche Zahl und a eine zu n teilerfremde Zahl. Dann gibt es unendlich viele Primzahlen, die modulo n den Rest a haben.*

Beweis. Dies ist ein Satz der analytischen Zahlentheorie, den wir im Rahmen dieser Vorlesung nicht beweisen können. □

12. Vorlesung

Die Abschätzungen von Tschebyschow

Pafnuti Lwowitsch Tschebyschow (1821-1894 Petersburg)

Wir wollen in diesem Abschnitt die Abschätzungen von Tschebyschow beweisen, die die Anzahl der Primzahlen unterhalb einer gewissen Zahl sowohl nach oben als auch nach unten abschätzen. Sie stellen eine Vorstufe zum Primzahlsatz von Hadamard und de la Vallée Pousin dar. Ihr Beweis benötigt einige Vorbereitungen.

Definition 12.1. Die *erste Tschebyschow-Funktion* $\vartheta(x)$ ist gegeben durch

$$\vartheta(x) = \sum_{p \leq x, p \text{ prim}} \ln(p)\,.$$

Lemma 12.2. *Die Tschebyschow-Funktion* $\vartheta(x) = \sum_{p\in\mathbb{P},\, p\leq x} \ln(p)$ *genügt der Abschätzung*

$$\vartheta(x) < (4\ln(2))x\,.$$

Beweis. Der Binomialkoeffizient

$$\binom{2n}{n} = \frac{(2n)\cdot(2n-1)\cdots(n+2)\cdot(n+1)}{n\cdot(n-1)\cdots 2\cdot 1}$$

wird von allen Primzahlen p mit $n < p \leq 2n$ geteilt, da diese den Zähler, aber nicht den Nenner teilen. Aus der Binomischen Formel ergibt sich die Abschätzung

$$2^{2n} = (1+1)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} > \binom{2n}{n}\,.$$

Diese zwei Beobachtungen zusammen ergeben die Abschätzung

$$2^{2n} > \prod_{n<p\leq 2n,\, p\in\mathbb{P}} p\,.$$

Wir wenden auf diese Abschätzung den natürlichen Logarithmus an und erhalten

$$2n\ln(2) > \sum_{n<p\leq 2n,\, p\in\mathbb{P}} \ln(p) = \vartheta(2n) - \vartheta(n)\,.$$

Geschicktes Aufsummieren ergibt dann

$$\begin{aligned}
\vartheta(2^r) &= \vartheta(2^r) - \vartheta(1) \\
&= (\vartheta(2) - \vartheta(1)) + (\vartheta(4) - \vartheta(2)) + \ldots + (\vartheta(2^r) - \vartheta(2^{r-1})) \\
&< 2\ln(2) + \ldots + 2\cdot 2^{r-1}\ln(2) \\
&= \sum_{i=0}^{r-1} 2\cdot 2^i \cdot \ln(2) \\
&= 2\ln(2)(1+2+4+\ldots+2^{r-1}) \\
&= 2\ln(2)(2^r-1) \\
&= \ln(2)(2^{r+1}-2)\,.
\end{aligned}$$

Insbesondere erhält man für Zahlen x mit $2^{r-1} < x \leq 2^r$ die Abschätzung

$$\vartheta(x) \leq \vartheta(2^r) < (2^{r+1}-2)\ln(2) < 2^{r+1}\ln(2) = (4\ln(2))\cdot 2^{r-1} < (4\ln(2))\cdot x\,.$$

□

Lemma 12.3. *(Identität von Legendre) Für eine Primzahl p und eine natürliche Zahl n ist*

$$\nu_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots\,.$$

Beweis. Hierzu muss man einfach zählen, wie viele der Zahlen zwischen 1 und n Vielfache von p, wie viele Vielfache von p^2 etc. sind. Das ergibt genau die Summe rechts. □

Satz 12.4. *(Abschätzungen von Tschebyschow) Es gibt Konstanten $C > c > 0$ derart, dass die Primzahlfunktion $\pi(x)$ für alle x den Abschätzungen*

$$c\frac{x}{\ln(x)} \leq \pi(x) \leq C\frac{x}{\ln(x)}$$

genügt.

Beweis. Wir betrachten zuerst die Abschätzung nach oben. Für $\sqrt{x} < p$ gilt $\ln(x)/2 < \ln(p)$ und somit $2\ln(p)/\ln(x) > 1$. Ferner gilt für $x \geq 2$ die Abschätzung $2\sqrt{x} > \ln(x)$ und somit

$$\sqrt{x} = x/\sqrt{x} < 2x/\ln(x).$$

Aus diesen zwei Vorüberlegungen und aus Lemma 12.2 folgt dann die Abschätzung

$$\pi(x) \;=\; \pi(\sqrt{x}) + (\pi(x) - \pi(\sqrt{x}))$$

$$\begin{aligned}
&\leq \sqrt{x} + \sum_{\sqrt{x}<p\leq x,\, p\in\mathbb{P}} 1 \\
&< \sqrt{x} + \frac{2}{\ln(x)} \left(\sum_{\sqrt{x}<p\leq x,\, p\in\mathbb{P}} \ln(p) \right) \\
&< \sqrt{x} + \frac{2}{\ln(x)} \vartheta(x) \\
&< \sqrt{x} + \frac{2}{\ln(x)} (4\ln(2)) x \\
&\leq (2 + 8\ln(2)) \frac{x}{\ln(x)}.
\end{aligned}$$

Die Abschätzung ist also mit $C = 2 + 8\ln(2)$ erfüllt.

Wir betrachten nun die Abschätzung nach unten. Nach Legendres Identität (Lemma 12.3) ist

$$\begin{aligned}
\nu_p\left(\binom{2n}{n}\right) &= \nu_p\left(\frac{(2n)!}{n!n!}\right) \\
&= \left\lfloor \frac{2n}{p} \right\rfloor + \ldots + \left\lfloor \frac{2n}{p^k} \right\rfloor - 2\left(\left\lfloor \frac{n}{p} \right\rfloor + \ldots + \left\lfloor \frac{n}{p^k} \right\rfloor \right).
\end{aligned}$$

Die Summe läuft hierbei bis zum maximalen k mit $p^k \leq 2n$, also bis $k = \lfloor \log_p(2n) \rfloor = \left\lfloor \frac{\ln(2n)}{\ln(p)} \right\rfloor$. Da die einzelnen Summanden der Summe links nur 0 oder 1 sein können, folgt,

$$\nu_p\left(\binom{2n}{n}\right) \leq \left\lfloor \frac{\ln(2n)}{\ln(p)} \right\rfloor.$$

Durch betrachten aller Primzahlen ergibt sich daraus die Abschätzung

$$\binom{2n}{n} \leq \prod_{p<2n,p \text{ prim}} p^{\left\lfloor \frac{\ln(2n)}{\ln(p)} \right\rfloor}.$$

Andererseits ist

$$2^n \leq \frac{2n}{n}\frac{2n-1}{n-1}\cdots\frac{n+1}{1} = \binom{2n}{n}.$$

Wir wenden den Logarithmus auf die zusammengesetzte Abschätzung an und erhalten

$$n\ln(2) \leq \sum_{p<2n} \left\lfloor \frac{\ln(2n)}{\ln(p)} \right\rfloor \ln(p).$$

Für $p > \sqrt{2n}$ ist $\ln(p) > \frac{\ln(2n)}{2}$ und damit $\left\lfloor \frac{\ln(2n)}{\ln(p)} \right\rfloor = 1$. Wir verwenden dies in der folgenden Aufspaltung und erhalten

$$\begin{aligned}
n\ln(2) &\leq \sum_{p<\sqrt{2n}} \left\lfloor \frac{\ln(2n)}{\ln(p)} \right\rfloor \ln(p) + \sum_{\sqrt{2n}\leq p<2n} \left\lfloor \frac{\ln(2n)}{\ln(p)} \right\rfloor \ln(p) \\
&\leq \sum_{p<\sqrt{2n}} \ln(2n) + \sum_{\sqrt{2n}\leq p<2n} \ln(p)
\end{aligned}$$

$$\leq \quad \sqrt{2n}\ln(2n) + \vartheta(2n).$$

Dies ergibt die Abschätzung

$$\vartheta(2n) \geq n\left(\ln(2) - \frac{\sqrt{2n}\ln(2n)}{n}\right).$$

Der Bruch rechts ist beschränkt (und konvergiert gegen null). Man erhält also eine positive Konstante M mit $\vartheta(2n) \geq Mn$ für n hinreichend groß. Für x zwischen $2n$ und $2n+2$ hat man

$$\vartheta(x) \geq \vartheta(2n) \geq Mn \geq M\frac{x-2}{2},$$

und dies ist wiederum $\geq Nx$ für eine geeignete positive Schranke N (und für x hinreichend groß). Dann gibt es aber auch eine positive Schranke c mit $\vartheta(x) \geq cx$ für alle $x \geq 2$. Aus

$$cx \leq \vartheta(x) = \sum_{p \leq x} \ln(p) \leq \pi(x)\ln(x)$$

folgt nun $c\frac{x}{\ln(x)} \leq \pi(x)$ wie behauptet. □

Korollar 12.5. *Es ist*

$$\lim_{x\to\infty} \frac{\pi(x)}{x} = 0\,.$$

Beweis. Nach der Abschätzung von Tschebyschow (Satz 12.4) nach oben gilt

$$\frac{\pi(x)}{x} \leq C\frac{1}{\ln(x)}\,.$$

Da der Logarithmus gegen unendlich strebt, geht der Kehrwert gegen 0, was die Behauptung impliziert. □

Die Aussage dieses Korollars bedeutet, dass die Wahrscheinlichkeit, dass eine zufällig aus dem Intervall [1,x] gewählte natürliche Zahl prim ist, bei x hinreichend groß beliebig klein ist.

Satz 12.6. *Es gibt eine reelle Zahl $D > 1$ derart, dass es für jede natürliche Zahl $n \geq 1$ zwischen $n+1$ und Dn stets eine Primzahl gibt.*

Beweis. In Lemma 12.2 und im Beweis zur Abschätzung von Tschebyschow nach unten haben wir gesehen, dass es reelle positive Konstanten b und B gibt mit

$$bx < \vartheta(x) < Bx\,.$$

Mit $D = B/b$ gilt dann

$$\vartheta(Dx) > bDx = Bx > \vartheta(x)\,.$$

Daher liegt zwischen x und Dx mindestens eine Primzahl. □

In diesem Satz kann man sogar $D = 2$ erreichen. Dies war von Joseph Bertrand vermutet worden und wurde von Tschebyschow bewiesen.

Joseph Bertrand (1822-1900 Paris)

Satz 12.7. *(Bertrandsches Postulat) Für jede natürliche Zahl n gibt es eine Primzahl zwischen $n+1$ und $2n$.*

Beweis. Dies werden wir hier nicht beweisen. Die Ausage ist aber prinzipiell mit den in diesem Abschnitt verwendeten Methoden beweisbar. □

Ein offenes Problem ist hingegen die Vermutung von Legendre, die besagt, dass es zwischen zwei aufeinanderfolgenden Quadratzahlen, also zwischen n^2 und $(n+1)^2$ stets eine Primzahl gibt.

13. Vorlesung

Mersenne-Primzahlen

Marin Mersenne (1588-1648)

Definition 13.1. Eine Primzahl der Form 2^n-1 heißt *Mersennesche Primzahl.*

Generell nennt man die Zahl $M_n = 2^n - 1$ die n-te *Mersenne-Zahl.* Mit dieser Bezeichnung sind die Mersenne-Primzahlen genau diejenigen Mersenne-Zahlen, die Primzahlen sind.

Lemma 13.2. *Ist 2^n-1 eine Primzahl, so ist auch n eine Primzahl.*

Beweis. Sei eine Darstellung $n = ab$ mit natürlichen Zahlen a, b gegeben. Wir setzen in der polynomialen Identität

$$X^k - 1 = (X - 1)(X^{k-1} + X^{k-2} + \ldots + X + 1)$$

$X = 2^a$ und $k = b$ ein und erhalten, dass $2^a - 1 | 2^n - 1$. Da $2^n - 1$ als prim vorausgesetzt wurde, folgt $2^a - 1 = 1$ oder $2^a - 1 = 2^n - 1$, also $a = 1$ oder $a = n$. □

Bemerkung 13.3. Die Mersennezahl $M_n = 2^n - 1$ hat im Dualsystem eine Entwicklung, die aus genau n Einsen besteht. Die ersten Mersenne-Primzahlen sind

$$2^2 - 1 = 3, 2^3 - 1 = 7, 2^5 - 1 = 31, 2^7 - 1 = 127\,.$$

Die Zahl $2^{11} - 1 = 2047 = 23 \cdot 89$ ist die erste Mersene-Zahl, wo der Exponent zwar prim ist, die aber selbst keine Mersenne-Primzahl ist. Dies wurde 1536 von Hudalrichus Regius (Walter Hermann Ryff) gezeigt. Der nächste Kandidat, nämlich $2^{13} - 1 = 8191$, ist wieder prim. Bis ca. 1950 war bekannt, dass für die Exponenten

$$2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107 \text{ und } 127$$

Mersenne-Primzahlen vorliegen, und keine weiteren unterhalb dem Exponenten 258. Von verschiedenen Leuten, unter anderem von Cataldi und Mersenne selbst, wurden falsche Behauptungen aufgestellt. Ab ca. 1950 kamen Computer zum Bestimmen von Mersenne-Primzahlen zum Einsatz, und es wurden bisher insgesamt 44 Mersenne-Primzahlen gefunden. Es ist aber unbekannt, ob es unendlich viele Mersenne-Primzahlen gibt.

Alle größten bekannten Primzahlen sind Mersenne-Zahlen. Das liegt daran, dass es für diese Zahlen einen vergleichsweise einfachen Primzahltest gibt, nämlich den *Lucas-Lehmer-Test*. Mit diesem Test wird etwa alle zwei Jahre eine neue größte Primzahl gefunden.

Mersenne-Zahlen stehen in direktem Verhältnis zu den vollkommenen Zahlen.

Vollkommene Zahlen

Definition 13.4. Eine natürliche Zahl n heißt *vollkommen*, wenn sie mit der Summe aller ihrer von n verschiedenen Teiler übereinstimmt.

Bereits Euklid stellte fest, dass die ersten vier vollkommenen Zahlen sich als

$$2^{k-1}(2^k - 1)$$

darstellen lassen:

- Für $k = 2$: $2^1(2^2 - 1) = 6 = 1 + 2 + 3$
- Für $k = 3$: $2^2(2^3 - 1) = 28 = 1 + 2 + 4 + 7 + 14$

• Für $k = 5$: $2^4(2^5 - 1) = 496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248$

• Für $k = 7$: $2^6(2^7 - 1) = 8128 = 1 + 2 + 4 + 8 + 16 + 32 + 64 + 127 + 254 + 508 + 1016 + 2032 + 4064$.

Euklid bewies, dass $2^{k-1}(2^k-1)$ immer dann eine vollkommene Zahl ist, wenn $2^k - 1$ eine Primzahl ist, also eine Mersenne-Primzahl ist. Euler bewies, dass auf diese Weise alle geraden vollkommenen Zahlen erzeugt werden können. Bevor wird diesen Satz von Euklid-Euler beweisen, brauchen wir eine kleine Vorüberlegung.

Definition 13.5. Zu einer natürlichen Zahl n bezeichnet man die Summe aller natürlichen Teiler davon als $\sigma(n)$, also

$$\sigma(n) = \sum_{t|n} t\,.$$

Eine vollkommene Zahl kann man also dadurch charakterisieren, dass $\sigma(n) = 2n$ ist.

Lemma 13.6. *(zur Teilersumme) Zu zwei natürlichen teilerfremden Zahlen n und m gilt*

$$\sigma(nm) = \sigma(n)\sigma(m)\,.$$

Beweis. Bei zwei teilerfremden Zahlen n und m hat jeder positive Teiler t des Produkts nm die eindeutige Form $t = ab$, wobei a ein Teiler von n und b ein Teiler von m ist. Also gilt

$$\sigma(nm) = \sum_{t|mn} t = \sum_{a|m \text{ und } b|n} ab = (\sum_{a|n} a)(\sum_{b|m} b) = \sigma(n)\sigma(m)\,.$$

□

Damit können wir beweisen.

Satz 13.7. *(Charakterisierung von geraden vollkommenen Zahlen mit Mersenne-Zahlen) Eine gerade Zahl n ist genau dann vollkommen, wenn $n = 2^{k-1}(2^k - 1)$ ist mit $2^k - 1$ prim.*

Beweis. Sei zunächst $n = 2^{k-1}(2^k - 1)$ mit $2^k - 1$ prim. Dann sind die von n verschiedenen Teiler von n gegeben durch

$$2^i,\ i = 0, \ldots, k-1, \text{ und } (2^k - 1)2^i,\ i = 0, \ldots, k-2\,.$$

Daher ist ihre Summe gleich

$$\sum_{i=0}^{k-1} 2^i + (2^k - 1)\sum_{i=0}^{k-2} 2^i = 2^k - 1 + (2^k - 1)(2^{k-1} - 1) = (2^k - 1)2^{k-1} = n\,,$$

also ist n vollkommen. Sei umgekehrt n vollkommen. Wir setzen (in Anlehnung an das Ziel) an

$$n = 2^{k-1}u$$

mit u ungerade und $k \geq 2$, da ja n gerade ist. Für teilerfremde Zahlen ist die Teilersumme gleich dem Produkt der beiden Teilersummen. Daher ist einerseits

$$\sigma(n) = \sigma(2^{k-1}u) = \sigma(2^{k-1})\sigma(u) = (2^k - 1)\sigma(u)$$

und andererseits wegen der Vollkommenheit

$$\sigma(n) = 2n = 2^k u\,.$$

Insgesamt ergibt sich also $(2^k - 1)\sigma(u) = 2^k u$. Da $2^k - 1$ ungerade ist, gilt

$$\sigma(u) = x2^k \text{ und } u = x(2^k - 1)\,.$$

Die Annahme $x > 1$ führt schnell zum Widerspruch, da es dann zumindest die drei verschiedenen Teiler $1, x, x(2^k - 1)$ von u gibt, was zu

$$\sigma(u) \geq (2^k - 1)x + 1 + x > 2^k x$$

führt. Also ist $x = 1$ und somit $\sigma(u) = 2^k = u + 1$. Die Teilersumme einer Zahl u ist aber gleich $u + 1$ nur dann, wenn eine Primzahl vorliegt. □

Es ist unbekannt, ob es unendlich viele vollkommene Zahlen gibt, da es ja auch unbekannt ist, ob es unendlich viele Mersenne-Primzahlen gibt. Es ist unbekannt, ob es überhaupt auch ungerade vollkommene Zahlen gibt.

Befreundete Zahlen

Definition 13.8. Zwei verschiedene natürliche Zahlen m und n heißen *befreundet*, wenn m gleich der Summe der echten Teiler von n ist und umgekehrt.

Das klassische Beispiel für ein befreundetes Zahlenpaar ist 220 und 284. Zwei verschiedene Zahlen sind befreundet genau dann, wenn

$$\sigma(m) = m + n = \sigma(n)$$

ist. Der folgende Satz erlaubt es, einige weitere befreundete Zahlenpaare zu finden, aber keineswegs alle.

Thabit Ibn Qurra (826 (?)-901)

Satz 13.9. *(Regel von Thabit) Sei $k \geq 2$ eine natürliche Zahl und seien $a = 3 \cdot 2^{k-1} - 1$, $b = 3 \cdot 2^k - 1$ und $c = 9 \cdot 2^{2k-1} - 1$ allesamt Primzahlen. Dann sind*

$$m = 2^k ab \text{ und } n = 2^k c$$

befreundet.

Beweis. Wir berechnen $\sigma(m)$, $\sigma(n)$ und $m + n$. Es ist

$$\begin{aligned}\sigma(m) &= \sigma(2^k ab) \\ &= \sigma(2^k)\sigma(a)\sigma(b) \\ &= (2^{k+1} - 1)(3 \cdot 2^{k-1})(3 \cdot 2^k) \\ &= (2^{k+1} - 1) \cdot 9 \cdot 2^{2k-1}\,.\end{aligned}$$

Weiter ist

$$\begin{aligned}\sigma(n) &= \sigma(2^k c) \\ &= \sigma(2^k)\sigma(c) \\ &= (2^{k+1} - 1)(1 + c) \\ &= (2^{k+1} - 1) \cdot 9 \cdot 2^{2k-1}\,.\end{aligned}$$

Schließlich ist

$$\begin{aligned}m + n &= 2^k(ab + c) \\ &= 2^k((3 \cdot 2^{k-1} - 1)(3 \cdot 2^k - 1) + 9 \cdot 2^{2k-1} - 1) \\ &= 2^k(9 \cdot 2^{2k-1} - 3 \cdot 2^{k-1} - 3 \cdot 2^k + 9 \cdot 2^{2k-1}) \\ &= 2^k(9 \cdot 2^{2k} - 9 \cdot 2^{k-1}) \\ &= 2^k 2^{k-1} \cdot 9(2^{k+1} - 1)\,.\end{aligned}$$

□

k	$a = 3 \cdot 2^{k-1} - 1$	$b = 3 \cdot 2^k - 1$	$c = 9 \cdot 2^{2k-1} - 1$	$m = 2^k ab$	$n = 2^k c$
2	5	11	71	220	284
3	11	23	$287 = 7 \cdot 41$		
4	23	47	1151 (prim)	17296	18416
5	47	95	$4607 = 17 \cdot 271$		
6	$95 = 5 \cdot 19$	191	$18431 = 7 \cdot 2633$		
7	191	383	73727	9363584	9437056

Das Paar 1184 und 1210 ist befreundet, aber nicht erhältlich über die Regel von Thabit.

14. Vorlesung

Fermatsche Primzahlen

Definition 14.1. Eine Primzahl der Form $2^s + 1$, wobei s eine positive natürliche Zahl ist, heißt *Fermatsche Primzahl*.

Lemma 14.2. *Bei einer Fermatschen Primzahl $2^s + 1$ hat der Exponent die Form $s = 2^r$ mit einem $r \in \mathbb{N}$.*

Beweis. Wir schreiben $s = 2^k u$ mit u ungerade. Damit ist

$$2^{2^k u} + 1 = (2^{2^k})^u + 1 \, .$$

Für ungerades u gilt generell die polynomiale Identität (da -1 eine Nullstelle ist)

$$X^u + 1 = (X+1)(X^{u-1} - X^{u-2} + X^{u-3} - \ldots + X^2 - X + 1) \, .$$

Also ist $2^{2^k} + 1 \geq 3$ ein Teiler von $2^{2^k u} + 1$. Da diese Zahl nach Voraussetzung prim ist, müssen beide Zahlen gleich sein, und dies bedeutet $u = 1$. □

Eine Fermatsche Primzahl ist nach diesem Lemma also insbesondere eine Fermat-Zahl im Sinne der folgenden Definition.

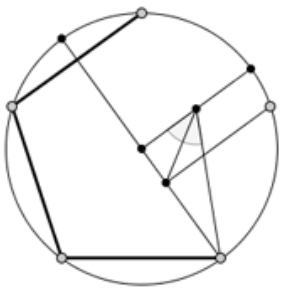
Definition 14.3. Eine Zahl der Form $2^{2^r} + 1$, wobei r eine natürliche Zahl ist, heißt *Fermat-Zahl*.

Satz 14.4. *Ein reguläres n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn die Primfaktorzerlegung von n die Gestalt hat*

$$n = 2^\alpha p_1 \cdots p_k \, ,$$

wobei die p_i verschiedene Fermatsche Primzahlen sind.

Beweis. Dieser Satz wird in einer Vorlesung über Körpertheorie bzw. Galoistheorie bewiesen. □



Konstruktion eines regulären Fünfecks mit Zirkel und Lineal

Es ist unbekannt, ob es unendlich viele Fermatsche Primzahlen gibt. Es ist noch nicht mal bekannt, ob es außer den ersten fünf Fermat-Zahlen

$$3, 5, 17, 257, 65537$$

überhaupt weitere Fermat-Zahlen gibt, die prim sind. Der folgende Satz hilft bei der Auffindung von Primteilern, da er die Suche wesentlich einschränkt.

Satz 14.5. *Sei $F_r = 2^{2^r} + 1$ eine Fermat-Zahl mit $r \geq 2$. Dann erfüllt jeder Primfaktor p von F_r die Bedingung*

$$p = 2^{r+2}a + 1$$

mit einem $a \in \mathbb{N}_+$.

Beweis. Sei also p ein Primteiler von $F_r = 2^{2^r} + 1$. Dies bedeutet, dass in $\mathbb{Z}/(p)$ die Gleichung

$$2^{2^r} = -1$$

vorliegt. Nach quadrieren ist $2^{2^{r+1}} = 1$ und die Ordnung von 2 ist 2^{r+1} (eine kleinere Ordnung ist nicht möglich, da diese ein Teiler von 2^{r+1} sein muss, aber $2^{2^r} \neq 1$ ist). Diese Ordnung ist ein Teiler von $p - 1$, woraus folgt, dass $p = 1 \mod 8$ ist. Dies bedeutet nach dem zweiten Ergänzungssatz (Satz 7.9) zum quadratischen Reziprozitätsgesetz, dass 2 ein Quadratrest modulo p ist. Sei $x^2 = 2 \mod p$. Dann ist aber die Ordnung von x genau 2^{r+2}. Nach dem Schluss von eben ist 2^{r+2} ein Teiler von $p-1$, was $p = 2^{r+2}a+1$ bedeutet. □

Satz 14.6. *Zwei verschiedene Fermatsche Zahlen F_m und F_n sind teilerfremd.*

Beweis. Sei $m > n$. Dann ist

$$F_m - 2 = 2^{2^m} - 1 = (2^{2^n})^{2^{m-n}} - 1\,.$$

Hierbei ist 2^{m-n} gerade, und daher ist $F_n = 2^{2^n} + 1$ ein Teiler von dieser Zahl. Das bedeutet, dass ein gemeinsamer Teiler von F_m und von F_n auch ein Teiler von $F_m - 2$ ist, also ein Teiler von 2. Da alle Fermat-Zahlen ungerade sind, bleibt nur 1 als gemeinsamer Teiler übrig. □

Bemerkung 14.7. Aus Satz 14.6 folgt erneut, dass es unendlich viele Primzahlen gibt. Jede Fermatzahl $F_r = 2^{2^r} + 1$ hat mindestens einen Primfaktor p_r, und diese sind alle verschieden.

Sophie Germain Primzahlen

Definition 14.8. Eine Primzahl p mit der Eigenschaft, dass auch $2p+1$ eine Primzahl ist, heißt *Sophie Germain Primzahl*.

Beispiele sind $(2,5)$, $(3,7)$, $(5,11)$, $(11,23)$, $(\ 23,47)$, $(\ 29,59)$, etc. Es ist unbekannt, ob es unendlich viele Sophie Germain Zahlen gibt.

Wir kommen nochmal zurück zu Mersenne-Zahlen und besprechen einige Situation, wo man Aussagen über mögliche Primteiler machen kann.

Satz 14.9. *(Mersenne-Zahlen zu Sophie Germain Primzahlen) Sei p eine Sophie Germain Primzahl, $q = 2p+1$ und M_p die zugehörige Mersenne Zahl. Dann ist q ein Teiler von M_p genau dann, wenn $q = \pm 1 \mod 8$ ist.*

Beweis. Es ist $q = 2p+1$ ein Teiler von $M_p = 2^p - 1$ genau dann, wenn $2^p = 1$ in $\mathbb{Z}/(q)$ ist. Wegen $p = \frac{q-1}{2}$ ist dies nach dem Euler-Kriterium genau dann der Fall, wenn 2 ein Quadratrest modulo q ist. Dies ist nach dem zweiten Ergänzungssatz (Satz 7.9) genau bei $q = \pm 1 \mod 8$ der Fall. □

Bemerkung 14.10. Ist p eine Sophie-Germain Primzahl, die modulo 4 den Rest 3 hat, so ist $q = 2p+1 = -1 \mod 8$ und nach Satz 14.9 ist q ein Teiler von M_p. Bei $p > 3$ ist dies ein echter Teiler und M_p ist nicht prim.

Für $p = 3$ ist $M_3 = 2^3 - 1 = 7 = 2p+1$. Für $p = 11$ ist $q = 23$ prim und es ist $23 | M_{11} = 2047$. Für $p = 23$ ist $q = 47$ wieder prim und es folgt, dass M_{23} ein Vielfaches von 47 ist.

Andere notwendige Bedingungen für Primteiler von Mersenne-Zahlen werden im folgenden Satz ausgedrückt.

Satz 14.11. *Sei p eine ungerade Primzahl und $M_p = 2^p - 1$ die zugehörige Mersenne-Zahl. Ist q ein Primfaktor von M_p, so ist*

$$q = 1 \mod 2p \text{ und } q = \pm 1 \mod 8\,.$$

Beweis. Es sei q ein Teiler von $M_p = 2^p - 1$. Dies bedeutet

$$2^p = 1 \mod q\,.$$

Dann ist p die Ordnung von 2 und nach Lagrange/Fermat (Satz 4.6) ist p ein Teiler von $q-1$. Dies bedeutet wiederum

$$q = 1 \mod p\,.$$

Da p und q ungerade sind, folgt sogar $q = 1 \mod 2p$. Wenn x ein primitives Element von $\mathbb{Z}/(q)$ ist, so ist $2 = x^{\frac{q-1}{p}j}$, da alle Elemente der Ordnung p sich so schreiben lassen. Da dieser Exponent gerade ist, muss 2 ein Quadratrest sein, und der zweite Ergänzungssatz (Satz 7.9) liefert die Kongruenzbedingung modulo 8. □

Pseudo-Primzahlen

Als Pseudo-Primzahlen bezeichnet man grob gesprochen solche Zahlen, die zwar nicht prim sind, aber wesentliche Eigenschaften mit Primzahlen gemeinsam haben.

Definition 14.12. Eine natürliche Zahl n heißt *quasiprim* zur Basis a, wenn $a^{n-1} = 1$ modulo n gilt.

Definition 14.13. Eine natürliche Zahl n, die nicht prim ist, mit der Eigenschaft, dass für jede zu n teilerfremde ganze Zahl a gilt

$$a^{n-1} = 1 \mod n\,,$$

heißt *Carmichael-Zahl*.

Eine Carmichael-Zahl hat also die Eigenschaft, dass sie quasiprim zu jeder zu n teilerfremden Basis a ist.

Satz 14.14. *Eine natürliche nicht-prime Zahl $n \geq 2$ ist genau dann eine Carmichael-Zahl, wenn für jeden Primteiler p von n gilt, dass $p-1$ die Zahl $n-1$ teilt und dass er einfach vorkommt.*

Beweis. Sei $n = p_1^{r_1} \cdots p_k^{r_k}$ die kanonische Primfaktorzerlegung. Nach dem chinesischen Restsatz (Satz 4.13) ist

$$(\mathbb{Z}/(n))^\times \cong (\mathbb{Z}/(p_1^{r_1}))^\times \times \cdots \times (\mathbb{Z}/(p_k^{r_k}))^\times\,.$$

Sei $a = (a_1, \ldots, a_k)$ eine zu n teilerfremde Zahl und sei vorausgesetzt, dass n eine Carmichael-Zahl ist. Dann ist insbesondere

$$(a_i)^{n-1} = 1 \mod p_i^{r_i}$$

für jeden Index i. Wählt man für a_i ein primitives Element (was nach Satz 5.11 möglich ist; für $p_i = 2$ ist nichts zu zeigen), so hat dies die Ordnung $(p_i - 1)p_i^{r_i-1}$. Da $n-1$ ein Vielfaches der Ordnung ist und da p und $n-1$ teilerfremd sind, folgt, dass $n-1$ ein Vielfaches von $p-1$ ist. Bei $r_i \geq 2$ gibt es Elemente der Ordnung p in $(\mathbb{Z}/(p^{r_i}))^\times$ (auch bei $p = 2$), und es ergibt sich der Widerspruch $p|(n-1)$. Also sind alle Exponenten einfach.

Für die Umkehrung ist nach Voraussetzung $r_i = 1$. Sei wieder $a = (a_1, \ldots, a_k)$ eine Einheit. Dann ist

$$a^{n-1} = (a_1^{n-1}, \ldots, a_k^{n-1}) = ((a_1^{p_1-1})^{\frac{n-1}{p_1-1}}, \ldots, (a_k^{p_k-1})^{\frac{n-1}{p_k-1}}) = (1, \ldots, 1) = 1\,.$$

Also ist n eine Carmichael-Zahl. □

Beispiel 14.15. Die kleinste Carmichael-Zahl ist

$$561 = 3 \cdot 11 \cdot 17\,.$$

Dies folgt aus der Charakterisierung (Satz 14.14), da 2, 10 und 16 Teiler von 560 sind.

Es ist inzwischen bekannt, dass es unendlich viele Carmichael-Zahlen gibt.

15. Vorlesung

Bevor wir uns mit algebraischer Zahlentheorie, insbesondere mit quadratischen Zahlbereichen, genauer beschäftigen können, brauchen wir einige neue algebraische Begriffe. Zur Motivation betrachten wir das folgende kommutative Diagramm.

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}[i] \\ \downarrow & & \downarrow \\ \mathbb{Q} & \longrightarrow & \mathbb{Q}[i] \end{array}$$

In der unteren Zeile stehen Körper, und zwar ist $\mathbb{Q} \subset \mathbb{Q}[i]$ eine endliche Körpererweiterung vom Grad zwei. Ferner ist $\mathbb{Q}$ der kleinste Körper, der die ganzen Zahlen $\mathbb{Z}$ enthält, und ebenso ist $\mathbb{Q}[i]$ der kleinste Körper, der die Gaußschen Zahlen $\mathbb{Z}[i]$ enthält. Die Gaußschen Zahlen sind, in einem zu präzisierenden Sinne, die ganzen Zahlen im Körper $\mathbb{Q}[i]$.

Dies ist nicht selbstverständlich. Betrachten wir stattdessen die Körpererweiterung $\mathbb{Q} \subset \mathbb{Q}[\sqrt{-3}]$ (ebenfalls vom Grad zwei), was ist dann der Ring der ganzen Zahlen?

$$\begin{array}{ccccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}[\sqrt{-3}] & \longrightarrow & \mathbb{Z}[\omega] \\ \downarrow & & \downarrow & & \downarrow \\ \mathbb{Q} & \longrightarrow & \mathbb{Q}[\sqrt{-3}] & = & \mathbb{Q}[\sqrt{-3}] \end{array}$$

Hier ist $\omega = \frac{-1+\sqrt{3}i}{2}$ und $\mathbb{Z}[\omega]$ ist der Ring der Eisenstein-Zahlen, den wir in der zweiten Vorlesung kennengelernt haben. Für die beiden Ringe $\mathbb{Z}[\sqrt{-3}]$ und $\mathbb{Z}[\omega]$ ist $\mathbb{Q}[\sqrt{-3}]$ der kleinste sie enthaltende Körper. Auf den ersten Blick wirkt vermutlich $\mathbb{Z}[\sqrt{-3}]$ natürlicher. Andererseits ist der Ring der Eisenstein-Zahlen euklidisch und damit faktoriell, hat also deutlich bessere Eigenschaften.

Im Folgenden werden wir bestimmen, was für eine beliebige endliche Körpererweiterung $\mathbb{Q} \subseteq L$ der richtige Ganzheitsring in L ist. Zuerst präzisieren wir, was wir eben dadurch beschrieben haben, dass $\mathbb{Q}$ der kleinste Körper ist, der $\mathbb{Z}$ enthält.

Definition 15.1. Zu einem Integritätsbereich R ist der *Quotientenkörper* $Q(R)$ definiert als die Menge der formalen Brüche

$$Q(R) = \{\frac{r}{s} : r, s \in R,\ s \neq 0\}$$

mit natürlichen Identifizierungen und Operationen.

Mit natürlichen Identifikationen meinen wir die (Erweiterungs- bzw. Kürzungs-)Regel

$$\frac{r}{s} = \frac{tr}{ts} (t \neq 0)\,.$$

Für die Operationen gelten

$$\frac{r}{s} + \frac{t}{u} = \frac{ru + ts}{su}$$

(auf Hauptnenner bringen) und

$$\frac{r}{s} \cdot \frac{t}{u} = \frac{rt}{su} .$$

Mit diesen Operationen liegt in der Tat, wie man schnell überprüft, ein Ring vor. Und zwar handelt es sich um einen Körper, denn für jedes Element $\frac{r}{s} \neq 0$ ist $\frac{s}{r}$ das Inverse.

Der Integritätsbereich R findet sich in $Q(R)$ wieder durch die Elemente $\frac{r}{1}$. Diese natürliche Inklusion

$$R \subseteq Q(R)$$

ist ein Ringhomomorphismus. Das Element $r = \frac{r}{1}$ hat bei $r \neq 0$ das Inverse $\frac{1}{r}$. Zwischen R und $Q(R)$ gibt es keinen weiteren Körper. Ein solcher muss nämlich zu $r \neq 0$ das (eindeutig bestimmte) Inverse $\frac{1}{r}$ enthalten und dann aber auch alle Produkte $s\frac{1}{r} = \frac{s}{r}$.

Definition 15.2. Seien R und A kommutative Ringe und sei $R \to A$ ein fixierter Ringhomomorphismus. Dann nennt man A eine *R-Algebra*.

Wenn eine R-Algebra vorliegt so nennt man den zugehörigen Ringhomomorphismus auch den *Strukturhomomorphismus*. Das vielleicht wichtigste Beispiel einer R-Algebra ist der Polynomring $R[X]$. Ein R-Algebra-Homomorphismus von $R[X]$ in eine weitere R-Algebra B ist gegeben durch die Zuordnung $X \mapsto f$, wobei $f \in B$ ein Element ist. Diese Abbildung nennt man den *Einsetzungshomomorphismus*. Er schickt ein Polynom $\sum_{i=0} r_i X^i$, $r_i \in R$, auf $\sum_{i=0} r_i f^i \in B$, wobei die r_i via dem Strukturhomomorphismus als Elemente in B aufgefasst werden.

Definition 15.3. Sei K ein Körper und A eine kommutative K-Algebra. Es sei $f \in A$ ein Element. Dann heißt f *algebraisch* über K, wenn es ein von null verschiedenes Polynom $P \in K[X]$ gibt mit $P(f) = 0$.

Wenn ein Polynom $P \neq 0$ das algebraische Element $f \in A$ annulliert (also $P(f) = 0$ ist), so kann man durch den Leitkoeffizienten dividieren und erhält dann auch ein normiertes annullierendes Polynom. Über einem Körper sind also die Begriffe ganz (später) und algebraisch äquivalent.

Definition 15.4. Sei K ein Körper und A eine kommutative K-Algebra. Es sei $f \in A$ ein über K algebraisches Element. Dann heißt das normierte Polynom $P \in K[X]$ mit $P(f) = 0$ und vom minimalen Grad mit dieser Eigenschaft, das *Minimalpolynom* von f.

Die über den rationalen Zahlen $\mathbb{Q}$ algebraischen komplexen Zahlen erhalten einen speziellen Namen.

Definition 15.5. Eine komplexe Zahl z heißt *algebraisch* oder *algebraische Zahl*, wenn sie algebraisch über den rationalen Zahlen $\mathbb{Q}$ ist. Andernfalls heißt sie *transzendent*.

Ferdinand von Lindemann (1852-1939)

Bemerkung 15.6. Eine komplexe Zahl $z \in \mathbb{C}$ ist genau dann algebraisch, wenn es ein von null verschiedenes Polynom P mit rationalen Koeffizienten gibt mit $P(z) = 0$. Durch Multiplikation mit einem Hauptnenner kann man für eine algebraische Zahl auch ein annullierendes Polynom mit ganzzahligen Koeffizienten finden (das allerdings nicht mehr normiert ist). Eine rationale Zahl q ist trivialerweise algebraisch, da sie Nullstelle des linearen rationalen Polynoms $X - q$ ist. Weiterhin sind die reellen Zahlen $\sqrt{q}$ und $q^{1/n}$ für $q \in \mathbb{Q}$ algebraisch. Dagegen sind die Zahlen e und π nicht algebraisch. Diese Aussagen sind keineswegs selbstverständlich, die Transzendenz von π wurde beispielsweise von Lindemann 1882 gezeigt

Definition 15.7. Sei L ein Körper und $K \subseteq L$ ein Unterkörper von L. Dann heißt L ein *Erweiterungskörper* (oder *Oberkörper*) von K und die Inklusion $K \subseteq L$ heißt eine *Körpererweiterung*.

Eine K-Algebra A kann man stets in natürlicher Weise als Vektorraum über dem Körper K auffassen (ist K kein Körper, so ist eine K-Algebra ein K-Modul. Die Skalarmultiplikation wird dabei einfach über den Strukturhomomorphismus erklärt. Durch den Vektorraumbegriff hat man sofort die folgenden Begriffe zur Verfügung.

Definition 15.8. Eine Körpererweiterung $K \subseteq L$ heißt *endlich*, wenn L ein endlich-dimensionaler Vektorraum über K ist.

Definition 15.9. Sei $K \subseteq L$ eine endliche Körpererweiterung. Dann nennt man die K-(Vektorraum-)Dimension von L den *Grad* der Körpererweiterung.

Ein Element $f \in L$ einer Körpererweiterung $K \subseteq L$ definiert durch Multiplikation eine K-lineare Abbildung

$$\varphi_f : L \longrightarrow L,\, y \longmapsto fy\,.$$

Über diese Konstruktion werden Norm und Spur von f erklärt.

Bemerkung 15.10. Zu einer linearen Abbildung

$$\varphi : V \longrightarrow V$$

eines endlich-dimensionalen K-Vektorraumes V in sich wird die Determinante $\det(\varphi)$ und die Spur $S(\varphi)$ wie folgt berechnet. Man wählt eine K-Basis $v_1, \ldots, v_n \in V$ und repräsentiert die lineare Abbildung bezüglich dieser Basis durch eine quadratische $n \times n$-Matrix

$$\begin{pmatrix} \lambda_{1,1} & \cdots & \lambda_{1,n} \\ \vdots & \ddots & \vdots \\ \lambda_{n,1} & \cdots & \lambda_{n,n} \end{pmatrix}$$

mit $\lambda_{ij} \in K$ und rechnet dann die Determinante aus. Es folgt aus dem Determinantenmultiplikationssatz, dass dies unabhängig von der Wahl der Basis ist. Die Spur ist gegeben durch

$$S(\varphi) = \lambda_{1,1} + \lambda_{2,2} + \ldots + \lambda_{n,n} \, ,$$

und dies ist ebenfalls unabhängig von der Wahl der Basis. Norm und Spur sind Elemente aus K.

Definition 15.11. Sei $K \subseteq L$ eine endliche Körpererweiterung. Zu einem Element $f \in L$ nennt man die Determinante der K-linearen Abbildung

$$\varphi_f : L \longrightarrow L, \, y \longmapsto fy \, ,$$

die *Norm* von f. Sie wird mit $N(f)$ bezeichnet.

Definition 15.12. Sei $K \subseteq L$ eine endliche Körpererweiterung. Zu einem Element $f \in L$ nennt man die Spur der K-linearen Abbildung

$$\varphi_f : L \longrightarrow L, \, y \longmapsto fy,$$

die *Spur* von f. Sie wird mit $S(f)$ bezeichnet.

Lemma 15.13. *Sei $K \subseteq L$ eine endliche Körpererweiterung. Dann hat die Norm*

$$N : L \longrightarrow K, \, f \longmapsto N(f),$$

folgende Eigenschaften:

(1) *Es ist $N(fg) = N(f)N(g)$.*
(2) *Für $f \in K$ ist $N(f) = f^n$, wobei n den Grad der Körpererweiterung bezeichne.*
(3) *Es ist $N(f) = 0$ genau dann, wenn $f = 0$ ist.*

Beweis. (1) Folgt aus dem Determinantenmultiplikationssatz.

(2) Zu einer beliebigen Basis von L wird die Multiplikation mit einen Element aus K durch die Diagonalmatrix beschrieben, bei der jeder Diagonaleintrag f ist. Die Determinante ist dann f^n.

(3) Die eine Richtung ist klar, sei also $f \neq 0$. Dann ist f eine Einheit und daher ist die Multiplikation mit x eine bijektive lineare Abbildung, und deren Determinante ist $\neq 0$. $\square$

Lemma 15.14. *Sei $K \subseteq L$ eine endliche Körpererweiterung vom Grad n. Dann hat die Spur*

$$S : L \longrightarrow K,\, f \longmapsto S(f)\,,$$

folgende Eigenschaften:

(1) *Die Spur ist additiv und K-linear, also $S(f+g) = S(f) + S(g)$ und $S(\lambda f) = \lambda S(f)$ für $\lambda \in K$.*
(2) *Für $f \in K$ ist $S(f) = nf$.*

Beweis. Dies folgt aus den Definitionen. □

Eine Körpererweiterung $K \subseteq L$ heißt *einfach*, wenn sie von einem Element f erzeugt wird. Das bedeutet, dass es außer L keinen Körper zwischen K und L gibt, der f enthält. Das Element f nennt man dann auch ein *primitives Element* der Körpererweiterung. Ist L endlich und einfach, so ist

$$L = K[f] \cong K[X]/(P)\,,$$

wobei P das Minimalpolynom von f ist.

Satz 15.15. *Sei $K \subseteq L = K[f]$ eine einfache endliche Körpererweiterung vom Grad n. Dann hat das Minimalpolynom P von f die Gestalt*

$$P = X^n - S(f)X^{n-1} + \ldots + (-1)^n N(f)\,.$$

Beweis. Das Minimalpolynom und das charakteristische Polynom der durch f definierten K-linearen Abbildung

$$\varphi_f : L \longrightarrow L,\, y \longmapsto fy,$$

haben beide den Grad n, so dass sie übereinstimmen. Sei bezüglich einer Basis $v_1, \ldots, v_n$ von L diese lineare Abbildung durch die Matrix $(\lambda_{ij})_{ij}$ gegeben. Dann ist das charakteristische Polynom gleich

$$\chi_f = \det \begin{pmatrix} X - \lambda_{1,1} & \cdots & -\lambda_{1,n} \\ \vdots & \ddots & \vdots \\ -\lambda_{n,1} & \cdots & X - \lambda_{n,n} \end{pmatrix} = X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0\,.$$

Zum Koeffizienten a_{n-1} leisten nur diejenigen Permutationen einen Beitrag, bei denen $(n-1)$-mal die Variable X vorkommt, und das ist nur bei der identischen Permutation (also der Diagonalen) der Fall. Multipliziert man die Diagonale distributiv aus, so ergibt sich $X^n - \sum_{i=1}^n \lambda_{ii} X^{n-1} + \ldots$, so dass also $a_{n-1} = -S(f)$ gilt. Setzt man in der obigen Gleichung $X = 0$, so ergibt sich, dass a_0 die Determinante der negierten Matrix ist, woraus $a_0 = (-1)^n N(f)$ folgt. □

Definition 15.16. Sei $K \subseteq L$ eine endliche Körpererweiterung. Sie heißt *separabel*, wenn für jedes Element $x \in L$ das Minimalpolynom separabel ist, also in keinem Erweiterungskörper eine mehrfache Nullstelle besitzt.

In unserem Zusammenhang, wo wir uns für Körpererweiterungen von $\mathbb{Q}$ interessieren, also in Charakteristik null sind, ist eine Körpererweiterung stets separabel (siehe Aufgabe 15.8), und wir haben den folgenden Satz zur Verfügung.

Satz 15.17. *(vom primitiven Element) Sei $K \subseteq L$ eine separable endliche Körpererweiterung. Dann wird L von einem Element erzeugt, d.h. es gibt $f \in L$ mit*

$$L = K(f) \cong K[X]/(P)$$

mit einem irreduziblen (Minimal-)Polynom $P \in K[X]$.

Beweis. Dies ist ein wichtiges Standardresultat aus der Theorie der Körpererweiterungen. □

16. Vorlesung

Diskriminanten

Definition 16.1. Sei $K \subseteq L$ eine endliche Körpererweiterung vom Grad n und seien $b_1, \ldots, b_n$ Elemente in L. Dann wird die *Diskriminante* von $b_1, \ldots, b_n$ definiert durch

$$\triangle(b_1, \ldots, b_n) = \det(S(b_i b_j)_{i,j}) \, .$$

Die $n \times n$ Produkte $b_i b_j$, $1 \leq i, j \leq n$, sind dabei Elemente in L, von denen man die Spur nimmt, die in K liegt. Man erhält also eine quadratische $n \times n$-Matrix über K. Deren Determinante ist nach Definition die Diskriminante. Im folgenden werden wir vor allem an der Diskriminante von speziellen Basen interessiert sein, so dass sich die Diskriminante als Invariante eines Zahlkörpers erweist.

Bei einem Basiswechsel verhält sich die Diskriminante wie folgt.

Lemma 16.2. *Sei $K \subseteq L$ eine endliche Körpererweiterung vom Grad n und seien $b_1, \ldots, b_n$ und $c_1, \ldots, c_n$ zwei K-Basen von L. Der Basiswechsel werde durch $c = Tb$ mit der Übergangsmatrix $T = (t_{ij})_{ij}$ beschrieben. Dann gilt für die Diskriminanten die Beziehung*

$$\triangle(c_1, \ldots, c_n) = (\det(T))^2 \triangle(b_1, \ldots, b_n) \, .$$

Beweis. Ausgeschrieben haben wir die Beziehungen $c_i = \sum_{j=1}^n t_{ij} b_j$. Damit gilt

$$c_i c_k = (\sum_{j=1}^n t_{ij} b_j)(\sum_{m=1}^n t_{km} b_m) = \sum_{j,m} t_{ij} t_{km} b_j b_m \, .$$

Wir schreiben $c_{ik} := S(c_i c_k)$ und $b_{jm} := S(b_j b_m)$. Wegen der K-Linearität der Spur gilt

$$c_{ik} = S(c_i c_k) = S(\sum_{j,m} t_{ij} t_{km} b_j b_m) = \sum_{j,m} t_{ij} t_{km} S(b_j b_m) = \sum_{j,m} t_{ij} t_{km} b_{jm} \, .$$

Wir schreiben diese Gleichung mit den Matrizen $C = (c_{ik})$, $B = (b_{jm})$ und $T = (t_{ij})$ als

$$C = T^{\text{transp}} B T \, ,$$

und die Behauptung folgt dann aus dem Determinantenmultiplikationssatz. □

Lemma 16.3. *Sei $K \subseteq L$ eine separable endliche Körpererweiterung vom Grad n und sei $b_1, \ldots, b_n$ eine K-Basis von L. Dann ist*

$$\triangle(b_1, \ldots, b_n) \neq 0 \, .$$

Beweis. Wir beweisen diese Aussage nur in Charakteristik null.

Sei angenommen, dass die Diskriminante null ist. Das bedeutet, dass das durch die Matrix $S(b_i b_j)_{ij}$ definierte lineare Gleichungssystem eine nichttriviale Lösung $(\lambda_1, \ldots, \lambda_n)$ besitzt. Es ist also

$$\sum_{i=1}^{n} \lambda_i S(b_i b_j) = 0$$

für alle j. Sei $x = \sum_{i=1}^{n} \lambda_i b_i$. Dann ist für jedes j

$$S(x b_j) = S((\sum_{i=1}^{n} \lambda_i b_i) b_j) = S(\sum_{i=1}^{n} \lambda_i b_i b_j) = \sum_{i=1}^{n} \lambda_i S(b_i b_j) = 0 \, .$$

Da x eine Einheit in L ist, ist auch $x b_j$,$j = 1, \ldots, n$ eine Basis und es folgt, dass die Spur überall den Wert null hat. Dies ist aber bei einer separablen Erweiterung nicht möglich: in Charakteristik null folgt dies sofort aus 15.14. □

Beschreibung von Spur und Norm mit Einbettungen

Satz 16.4. *Sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n. Dann gibt es genau n Einbettungen von L in die komplexen Zahlen $\mathbb{C}$.*

Beweis. Nach dem Satz vom primitiven Element (Satz 15.17) wird L durch ein Element erzeugt, es ist also

$$L = \mathbb{Q}(x) \cong \mathbb{Q}[X]/(F)$$

mit einen irreduziblen Polynom $F \in \mathbb{Q}[X]$ vom Grad n. Da F irreduzibel ist und da die Ableitung $F' \neq 0$ ist folgt, dass F und F' teilerfremd sind. Nach dem Satz 2.17 ergibt sich, dass F und F' das Einheitsideal erzeugen, also $AF + BF' = 1$ ist. Wir betrachten diese Polynome nun als Polynome in $\mathbb{C}[X]$, wobei die polynomialen Identitäten erhalten bleiben. Über den

komplexen Zahlen zerfallen F und F' in Linearfaktoren, und wegen der Teilerfremdheit bzw. der daraus resultierenden Identität haben F und F' keine gemeinsame Nullstelle. Daraus folgt wiederum, dass F keine mehrfache Nullstelle besitzt, sondern genau n verschiedene komplexe Zahlen $z_1, \ldots, z_n$ als Nullstellen besitzt. Jedes z_i definiert nun einen Ringhomomorphismus

$$\rho_i : L \cong \mathbb{Q}[X]/(F) \longrightarrow \mathbb{C},\ X \longmapsto z_i\,.$$

Da L ein Körper ist, ist diese Abbildung injektiv. Da dabei X auf verschiedene Elemente abgebildet wird, liegen n verschiedene Abbildungen vor. Es kann auch keine weiteren Ringhomomorphismen $L \to \mathbb{C}$ geben, da jeder solche durch $X \mapsto z$ gegeben ist und $F(z) = 0$ sein muss. □

Man beachte im vorstehenden Satz, dass das Bild von verschiedenenen Einbettungen $\rho_i : L \to \mathbb{C}$ der gleiche Unterkörper sein kann. Dies gilt bereits für quadratische Erweiterungen wie $\mathbb{Q}[i]$. Man hat die beiden Einbettung $\rho_1, \rho_2 : \mathbb{Q}[i] \to \mathbb{C}$, wobei die eine i auf i und die andere i auf $-i$ schickt. Das Bild ist aber beidesmal gleich.

Wenn das Bild einer Einbettung ganz in den reellen Zahlen liegt, so spricht man auch von einer reellen Einbettung. Allgemein spricht man von konjugierten Einbettungen. Zu einem Element $z \in L$ nennt man die verschiedenen komplexen Zahlen

$$z_1 = \rho_1(z), \ldots, z_n = \rho_n(z)$$

zueinander konjugiert. Diese sind allesamt Nullstellen eines irreduziblen Polynoms F mit rationalen Koeffizienten vom Grad n.

Lemma 16.5. *Sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung und $z \in L$ ein Element. Es seien $\rho_1, \ldots, \rho_n : L \to \mathbb{C}$ die verschiedenen komplexen Einbettungen und es sei $M = \{z_1, \ldots, z_k\}$ die Menge der verschiedenen Werte $\rho_i(z)$. Dann gilt für das Minimalpolynom G von z die Gleichung*

$$G = (X - z_1)(X - z_2) \cdots (X - z_k)\,.$$

Beweis. Sei $K \subseteq L$ der von z erzeugte Unterkörper von L. Es ist dann $K \cong \mathbb{Q}[X]/(G)$, und K (bzw. G) haben den Grad k über $\mathbb{Q}$. Die Einbettungen $\sigma : K \to \mathbb{C}$ entsprechen den komplexen Nullstellen M' von G, und daher ist

$$G = \prod_{\sigma} (X - \sigma(z))\,.$$

Die Einbettungen $\rho_i : L \to \mathbb{C}$ induzieren eine Einbettung $\sigma_i = \rho_i$ und somit ist $\rho_i(z) = \sigma_i(z)$, also $M \subseteq M'$. Andererseits lässt sich eine Einbettung $\sigma : K \to \mathbb{C}$ zu einer Einbettung $L \to \mathbb{C}$ fortsetzen, da L über K separabel ist und von einem Element erzeugt wird und das zugehörige Minimalpolynom über $\mathbb{C}$ zerfällt. Daher ist auch $M' \subseteq M$. □

Wir erwähnen ohne Beweis die folgende Beschreibung von Norm und Spur, die wir aber in der Vorlesung nicht intensiv verwenden werden.

Lemma 16.6. *Sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n und seien $\rho_i : L \to \mathbb{C}$ die n verschiedenen komplexen Einbettungen. Es sei $z \in L$ und $z_i = \rho_i(z)$, $i = 1, \ldots, n$. Dann ist*

$$N(z) = z_1 \cdots z_n \text{ und } S(z) = z_1 + \ldots + z_n \, .$$

Beweis. Wir verzichten auf einen Beweis. □

Moduln und Ideale

Für den Begriff des Ganzheitsringes in einem Erweiterungskörper $\mathbb{Q} \subseteq L$ benötigen wir den Begriff des Moduls, der den eines Vektorraums in dem Sinne verallgemeinert, dass der Skalarenbereich kein Körper mehr sein muss, sondern ein beliebiger kommutativer Ring sein darf.

Definition 16.7. Sei R ein kommutativer Ring und $M = (M, +, 0)$ eine kommutative Gruppe. Man nennt M einen *R- Modul*, wenn es eine Operation

$$R \times M \longrightarrow M, \, (r, v) \longmapsto rv = r \cdot v \, ,$$

gibt, die folgende Axiome erfüllt (dabei seien $r, s \in R$ und $u, v \in M$ beliebig):

(1) $r(su) = (rs)u$,
(2) $r(u + v) = (ru) + (rv)$,
(3) $(r + s)u = (ru) + (su)$,
(4) $1u = u$.

Definition 16.8. Sei R ein kommutativer Ring und M ein R-Modul. Eine Teilmenge $U \subseteq M$ heißt *Untermodul*, wenn sie eine Untergruppe von M ist und wenn für jedes $u \in U$ und $r \in R$ gilt, dass auch $ru \in U$ ist.

Definition 16.9. Sei R ein kommutativer Ring und M ein R-Modul. Eine Teilmenge $v_i \in M$, $i \in I$, heißt *Erzeugendensystem* für M, wenn es für jedes Element $v \in M$ eine Darstellung

$$v = \sum_{i \in J} r_i v_i$$

gibt, wobei $J \subseteq I$ endlich ist und $r_i \in R$.

Definition 16.10. Sei R ein kommutativer Ring und M ein R-Modul. Der Modul M heißt *endlich erzeugt* oder *endlich*, wenn es ein endliches Erzeugendensystem v_i, $i \in I$, für ihn gibt (also mit einer endlichen Indexmenge).

Ein kommutativer Ring R selbst ist in natürlicher Weise ein R-Modul, wenn man die Ringmultiplikation als Skalarmultiplikation interpretiert. Die Ideale sind dann genau die R-Untermoduln von R. Die Begriffe Ideal-Erzeugendensystem und Modul-Erzeugendensystem stimmen für Ideale überein.

Unter den Idealen sind besonders die Primideale und die maximalen Ideale relevant.

Definition 16.11. Ein Ideal $\mathfrak{p}$ in einem kommutativen Ring R heißt *Primideal*, wenn $\mathfrak{p} \neq R$ ist und wenn für $r, s \in R$ mit $r \cdot s \in \mathfrak{p}$ folgt: $r \in \mathfrak{p}$ oder $s \in \mathfrak{p}$.

Lemma 16.12. *(Charakterisierung von Primhauptideal) Sei R ein Integritätsbereich und $p \in R$, $p \neq 0$. Dann ist p genau dann ein Primelement, wenn das von p erzeugte Hauptideal (p) ein Primideal ist.*

Beweis. Das ist trivial. □

Lemma 16.13. *(Charakterisierung von Primideal) Sei R ein kommutativer Ring und $\mathfrak{p}$ ein Ideal in R. Dann ist $\mathfrak{p}$ ein Primideal genau dann, wenn der Restklassenring $R/\mathfrak{p}$ ein Integritätsbereich ist.*

Beweis. Sei zunächst $\mathfrak{p}$ ein Primideal. Dann ist insbesondere $\mathfrak{p} \subset R$ und somit ist der Restklassenring $R/\mathfrak{p}$ nicht der Nullring. Sei $fg = 0$ in $R/\mathfrak{p}$ wobei f, g durch Elemente in R repräsentiert seien. Dann ist $fg \in \mathfrak{p}$ und damit $f \in \mathfrak{p}$ oder $g \in \mathfrak{p}$, was in $R/\mathfrak{p}$ gerade $f = 0$ oder $g = 0$ bedeutet.

Ist umgekehrt $R/\mathfrak{p}$ ein Integritätsring, so handelt es sich nicht um den Nullring und daher ist $\mathfrak{p} \neq R$. Sei $f, g \notin \mathfrak{p}$. Dann ist $f, g \neq 0$ in $R/\mathfrak{p}$ und daher $fg \neq 0$ in $R/\mathfrak{p}$, also ist $fg \notin \mathfrak{p}$. □

Definition 16.14. Ein Ideal $\mathfrak{m}$ in einem kommutativen Ring R heißt *maximales Ideal*, wenn $\mathfrak{m} \neq R$ ist und wenn es zwischen $\mathfrak{m}$ und R keine weiteren Ideale gibt.

Lemma 16.15. *(Charakterisierung von maximalen Idealen) Sei R ein kommutativer Ring und $\mathfrak{m}$ ein Ideal in R. Dann ist $\mathfrak{m}$ ein maximales Ideal genau dann, wenn der Restklassenring $R/\mathfrak{m}$ ein Körper ist.*

Beweis. Nach Aufgabe 16.10 entsprechen die Ideale im Restklassenring $R/\mathfrak{m}$ eindeutig den Idealen in R zwischen $\mathfrak{m}$ und R. Nun ist $R/\mathfrak{m}$ ein Körper genau dann, wenn es genau nur zwei Ideale gibt, und dies ist genau dann der Fall, wenn $\mathfrak{m} \neq R$ ist und es dazwischen kein weiteres Ideal gibt. Dies bedeutet, dass $\mathfrak{m}$ maximal ist. □

Korollar 16.16. *(Maximale Ideale sind prim) Sei R ein kommutativer Ring und $\mathfrak{m}$ ein maximales Ideal. Dann ist $\mathfrak{m}$ ein Primideal.*

Beweis. Dies folgt sofort aus den Charakterisierungen für Primideale und für maximale Ideale mit den Restklassenringen. □

17. Vorlesung

Definition 17.1. Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Für ein Element $x \in S$ heißt eine Gleichung der Form

$$x^n + r_{n-1}x^{n-1} + r_{n-2}x^{n-2} + \ldots + r_1 x + r_0 = 0\,,$$

wobei die Koeffizienten r_i, $i = 0, \ldots, n-1$, zu R gehören, eine *Ganzheitsgleichung* für x.

Definition 17.2. Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Ein Element $x \in S$ heißt *ganz*, wenn x eine Ganzheitsgleichung mit Koeffizienten aus R erfüllt.

Wenn $R = K$ ein Körper und S eine K-Algebra ist, so ist $x \in S$ algebraisch über K genau dann, wenn es ganz über K ist. Dies stimmt aber im Allgemeinen nicht, siehe Aufgabe.

Definition 17.3. Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Dann nennt man die Menge der Elemente $x \in S$, die ganz über R sind, den *ganzen Abschluss* von R in S.

Definition 17.4. Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Dann heißt S *ganz* über R, wenn jedes Element $x \in S$ ganz über R ist.

S ist genau dann ganz über R, wenn der ganze Abschluss von R in S gleich S ist.

Lemma 17.5. *Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Für ein Element $x \in S$ sind folgende Aussagen äquivalent.*

(1) *x ist ganz über R.*
(2) *Es gibt eine R-Unteralgebra T von S mit $x \in T$ und die ein endlicher R-Modul ist.*
(3) *Es gibt einen endlichen R-Untermodul M von S, der einen Nichtnullteiler aus S enthält, mit $xM \subseteq M$.*

Beweis. (1) $\Rightarrow$ (2). Wir betrachten die von den Potenzen von x erzeugte R-Unteralgebra $R[x]$ von S, die aus allen polynomialen Ausdrücken in x mit Koeffizienten aus R besteht. Aus einer Ganzheitsgleichung

$$x^n + r_{n-1}x^{n-1} + r_{n-2}x^{n-2} + \ldots + r_1 x + r_0 = 0$$

ergibt sich

$$x^n = -r_{n-1}x^{n-1} - r_{n-2}x^{n-2} - \ldots - r_1 x - r_0 \,.$$

Man kann also x^n durch einen polynomialen Ausdruck von einem kleineren Grad ausdrücken. Durch Multiplikation dieser letzten Gleichung mit x^i kann man jede Potenz von x mit einem Exponenten $\geq n$ durch einen polynomialen Ausdruck von einem kleineren Grad ersetzen. Insgesamt kann man dann aber all diese Potenzen durch polynomiale Ausdrücke vom Grad $\leq n-1$ ersetzen. Damit ist

$$R[x] = R + Rx + Rx^2 + \ldots + Rx^{n-2} + Rx^{n-1}$$

und die Potenzen $x^0 = 1, x^1, x^2, \ldots, x^{n-1}$ bilden ein endliches Erzeugendensystem von $T = R[x]$.

(2) $\Rightarrow$ (3). Sei $x \in T \subseteq S$, T eine R-Unteralgebra, die als R-Modul endlich erzeugt sei. Dann ist $xT \subseteq T$, und T enthält den Nichtnullteiler 1.

(3) $\Rightarrow$ (1). Sei $M \subseteq S$ ein endlich erzeugter R-Untermodul mit $xM \subseteq M$. Seien $y_1, \ldots, y_n$ erzeugende Elemente von M. Dann ist insbesondere xy_i für jedes i eine R-Linearkombination der y_j, $j = 1, \ldots, n$. Dies bedeutet

$$xy_i = \sum_{j=1}^{n} r_{ij} y_j$$

mit $r_{ij} \in R$ oder als Matrix geschrieben

$$x \begin{pmatrix} y_1 \\ y_2 \\ . \\ . \\ y_n \end{pmatrix} = \begin{pmatrix} r_{1,1} & r_{1,2} & . & . & r_{1,n} \\ r_{2,1} & r_{2,2} & . & . & r_{2,n} \\ . & . & . & . & . \\ . & . & . & . & . \\ r_{n,1} & r_{n,2} & . & . & r_{n,n} \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \\ . \\ . \\ y_n \end{pmatrix} .$$

Dies schreiben wir als

$$0 = \begin{pmatrix} x - r_{1,1} & -r_{1,2} & . & . & -r_{1,n} \\ -r_{2,1} & x - r_{2,2} & . & . & -r_{2,n} \\ . & . & . & . & . \\ . & . & . & . & . \\ -r_{n,1} & -r_{n,2} & . & . & x - r_{n,n} \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \\ . \\ . \\ y_n \end{pmatrix} .$$

Nennen wir diese Matrix A (die Einträge sind aus S), und sei A^{adj} die adjungierte Matrix. Dann gilt $A^{adj}Ay = 0$ (y bezeichne den Vektor $(y_1, \ldots, y_n)$) und nach der Cramerschen Regel ist $A^{adj}A = (\det A)E_n$, also gilt $((\det A)E_n)y = 0$. Es ist also $(\det A)y_j$ für alle j und damit $(\det A)z$ für alle z. Da M nach Voraussetzung einen Nichtnullteiler enthält, muss $\det A = 0$ sein. Die Determinante ist aber ein normierter polynomialer Ausdruck in x vom Grad n, so dass eine Ganzheitsgleichung vorliegt. □

Korollar 17.6. *Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Dann ist der ganze Abschluss von R in S eine R-Unteralgebra von S.*

Beweis. Die Ganzheitsgleichungen $X - r$, $r \in R$, zeigen, dass jedes Element aus R ganz über R ist. Seien $x_1 \in S$ und $x_2 \in S$ ganz über R. Nach der Charakterisierung der Ganzheit(Lemma 17.5) gibt es endliche R-Unteralgebren $T_1, T_2 \subseteq S$ mit $x_1 \in T_1$ und $x_2 \in T_2$. Sei $y_1, \ldots, y_n$ ein R-Erzeugendensystem von T_1 und $z_1, \ldots, z_m$ ein R-Erzeugendensystem von T_2. Wir können annehmen, dass $y_1 = z_1 = 1$ ist. Betrachte den endlich erzeugten R-Modul

$$T = T_1 \cdot T_2 = \langle y_i z_j,\, i = 1, \ldots, n,\, j = 1, \ldots, m \rangle ,$$

der offensichtlich $x_1 + x_2$ und $x_1 x_2$ (und 1) enthält. Dieser R-Modul T ist auch wieder eine R-Algebra, da für zwei beliebige Elemente gilt

$$(\sum r_{ij} y_i z_j)(\sum s_{kl} y_k z_l) = \sum r_{ij} s_{kl} y_i y_k z_j z_l ,$$

und für die Produkte gilt $y_i y_k \in T_1$ und $z_j z_l \in T_2$ so dass diese Linearkombination zu T gehört. Dies zeigt, dass die Summe und das Produkt von zwei ganzen Elementen wieder ganz ist. Deshalb ist der ganze Abschluss ein Unterring von S, der R enthält. Also liegt eine R-Unteralgebra vor. □

Definition 17.7. Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Man nennt R *ganz-abgeschlossen* in S, wenn der ganze Abschluss von R in S gleich R ist.

Definition 17.8. Ein Integritätsbereich heißt *normal*, wenn er ganz-abgeschlossen in seinem Quotientenkörper ist.

Definition 17.9. Sei R ein Integritätsbereich und $Q(R)$ sein Quotientenkörper. Dann nennt man den ganzen Abschluss von R in $Q(R)$ die *Normalisierung* von R.

Satz 17.10. *(Normalität faktorieller Bereiche) Sei R ein faktorieller Integritätsbereich. Dann ist R normal.*

Beweis. Sei $K = Q(R)$ der Quotientenkörper von R und $q \in K$ ein Element, das die Ganzheitsgleichung

$$q^n + r_{n-1}q^{n-1} + r_{n-2}q^{n-2} + \ldots + r_1 q + r_0 = 0$$

mit $r_i \in R$ erfüllt. Wir schreiben $q = a/b$ mit $a, b \in R$, wobei wir annehmen können, dass die Darstellung gekürzt ist, dass also a und $b \in R$ keinen gemeinsamen Primteiler besitzen. Wir haben zu zeigen, dass b eine Einheit in R ist, da dann $q = ab^{-1}$ zu R gehört.

Wir multiplizieren obige Ganzheitsgleichung mit b^n und erhalten in R

$$a^n + (r_{n-1}b)a^{n-1} + (r_{n-2}b^2)a^{n-2} + \ldots + (r_1 b^{n-1})a + (r_0 b^n) = 0\,.$$

Wenn b keine Einheit ist, dann gibt es auch einen Primteiler p von b. Dieser teilt alle Summanden $(r_{n-i}b^i)a^{n-i}$ für $i \geq 1$ und daher auch den ersten, also a^n. Das bedeutet aber, dass a selbst ein Vielfaches von p ist im Widerspruch zur vorausgesetzten Teilerfremdheit. □

Korollar 17.11. *(Wurzeln aus Elementen) Sei R ein faktorieller (oder normaler) Integritätsbereich und $a \in R$. Wenn es ein Element $x \in Q(R)$ gibt mit $x^k = a$, so ist bereits $x \in R$.*

Beweis. Die Voraussetzung bedeutet, dass $x \in Q(R)$ ganz über R ist, da es die Ganzheitsgleichung

$$X^k - a = 0$$

erfüllt. Also ist $x \in R$ wegen der Normalität. □

Korollar 17.12. *(Irrationalität von Wurzeln) Sei $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ die kanonische Primfaktorzerlegung der natürlichen Zahl n. Sei k eine positive natürliche Zahl und sei vorausgesetzt, dass nicht alle Exponenten α_i ein Vielfaches von k sind. Dann ist die reelle Zahl*

$$n^{\frac{1}{k}}$$

irrational.

Beweis. Die Zahl $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ kann nach Voraussetzung keine k-te Wurzel in $\mathbb{Z}$ besitzen, da in einer k-ten Potenz alle Exponenten zu Primzahlen Vielfache von k sind. Wegen der Faktorialität von $\mathbb{Z}$ und der Fakt Normalität kann es auch kein $x \in Q(\mathbb{Z}) = \mathbb{Q}$ geben mit $x^k = n$. Daher ist die reelle Zahl $n^{\frac{1}{k}}$ irrational. □

Lemma 17.13. *(Quotientenkörper und Ganzheit) Sei R ein Integritätsbereich mit Quotientenkörper $K = Q(R)$ und sei $K \subseteq L$ eine endliche Körpererweiterung. Der ganze Abschluss von R in L sei mit S bezeichnet. Dann ist L der Quotientenkörper von S.*

Beweis. Sei $f \in L$. Nach Voraussetzung ist L endlich über K. Daher erfüllt f eine Ganzheitsgleichung der Form

$$f^n + q_{n-1}f^{n-1} + \ldots + q_1 f + q_0 = 0$$

mit $q_i \in K$. Sei $r \in R$ ein gemeinsames Vielfaches der Nenner aller q_i, $i = 1, \ldots, n-1$. Multiplikation mit r^n ergibt dann

$$(rf)^n + q_{n-1}r(rf)^{n-1} + \ldots + q_1 r^{n-1}(rf) + q_0 r^n = 0\,.$$

Dies ist eine Ganzheitsgleichung für rf, da die Koeffizienten $q_{n-i}r^i$ nach Wahl von r alle zu R gehören. Damit ist $rf \in S$, da S der ganze Abschluss ist. Somit zeigt $f = \frac{rf}{r}$, dass f als ein Bruch mit einem Zähler aus S und einem Nenner aus $R \subseteq S$ darstellbar ist, also im Quotientenkörper $Q(S)$ liegt. □

18. Vorlesung

Wir werden uns in dieser Vorlesung hauptsächlich für den ganzen Abschluss von $\mathbb{Z}$ in einem endlichen Erweiterungskörper der rationalen Zahlen $\mathbb{Q}$ interessieren.

Definition 18.1. Sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung. Dann nennt man den ganzen Abschluss von $\mathbb{Z}$ in L den *Ring der ganzen Zahlen* in L. Solche Ringe nennt man auch *Zahlbereiche*.

Den endlichen Erweiterungskörper L von $\mathbb{Q}$ nennt man übrigens einen *Zahlkörper*.

Satz 18.2. *Sei R ein Zahlbereich. Dann ist R ein normaler Integritätsbereich.*

Beweis. Nach Satz 17.13 ist L der Quotientenkörper des Ganzheitsrings R. Ist $q \in Q(R) = L$ ganz über R, so ist q nach Aufgabe 17.3 auch ganz über $\mathbb{Z}$ und gehört selbst zu R. □

Lemma 18.3. *Sei R ein Zahlbereich. Dann enthält jedes von null verschiedene Ideal $\mathfrak{a}$ in R eine Zahl $m \in \mathbb{Z}$ mit $m \neq 0$.*

Beweis. Sei $0 \neq f \in \mathfrak{a}$. Dieses Element ist nach der Definition eines Zahlbereiches ganz über $\mathbb{Z}$ und erfüllt demnach eine Ganzheitsgleichung

$$f^n + k_{n-1}f^{n-1} + k_{n-2}f^{n-2} + \ldots + k_1 f + k_0 = 0$$

mit ganzen Zahlen k_i. Bei $k_0 = 0$ kann man die Gleichung mit f kürzen, da $f \neq 0$ ein Nichtnullteiler ist. So kann man sukzessive fortfahren und erhält schließlich eine Ganzheitsgleichung, bei der der konstante Term nicht 0 ist. Sei also in obiger Gleichung $k_0 \neq 0$. Dann ist

$$f(f^{n-1} + k_{n-1}f^{n-2} + k_{n-2}f^{n-3} + \ldots + k_1) = -k_0$$

und somit ist $k_0 \in (f) \cap \mathbb{Z}$. □

Satz 18.4. *Sei R ein Zahlbereich und sei $f \in Q(R) = L$. Dann ist f genau dann ganz über $\mathbb{Z}$, wenn die Koeffizienten des Minimalpolynoms von f über $\mathbb{Q}$ alle ganzzahlig sind.*

Beweis. Das Minimalpolynom P von f über $\mathbb{Q}$ ist ein normiertes irreduzibles Polynom mit Koeffizienten aus $\mathbb{Q}$. Wenn die Koeffizienten sogar ganzzahlig sind, so liegt direkt eine Ganzheitsgleichung für f über $\mathbb{Z}$ vor.

Sei umgekehrt f ganz über $\mathbb{Z}$, und sei $S \in \mathbb{Z}[X]$ ein normiertes ganzzahliges Polynom mit $S(f) = 0$, das wir als irreduzibel in $\mathbb{Z}[X]$ annehmen dürfen. Wir betrachten $S \in \mathbb{Q}[X]$. Dort gilt

$$S = PT\,.$$

Da nach dem Lemma von Gauß (siehe Aufgabe 18.2) ein irreduzibles Polynom von $\mathbb{Z}[X]$ auch in $\mathbb{Q}[X]$ irreduzibel ist, folgt $S = P$ und daher sind alle Koeffizienten von P ganzzahlig. □

Es ergibt sich insbesondere, dass die Norm und die Spur von Elementen aus einem Zahlbereich zu $\mathbb{Z}$ gehören.

Lemma 18.5. *Sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n und R der zugehörige Zahlbereich. Sei $\mathfrak{a}$ ein von null verschiedenes Ideal in R. Dann enthält $\mathfrak{a}$ Elemente $b_1, \ldots, b_n$, die eine $\mathbb{Q}$-Basis von L sind.*

Beweis. Es sei $v_1, \ldots, v_n$ eine $\mathbb{Q}$-Basis von L. Das Ideal $\mathfrak{a}$ enthält nach Lemma 18.3 ein Element $0 \neq m \in \mathfrak{a} \cap \mathbb{Z}$. Nach (dem Beweis von) Satz 17.13 kann man schreiben $v_i = \frac{r_i}{n_i}$ mit $r_i \in R$ und $n_i \in \mathbb{Z} - \{0\}$. Dann sind die $m(n_i v_i) \in \mathfrak{a}$ und bilden ebenfalls eine $\mathbb{Q}$-Basis von L. □

Satz 18.6. *Sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n und R der zugehörige Zahlbereich. Sei $\mathfrak{a}$ ein von null verschiedenes Ideal in R. Seien $b_1, \ldots, b_n \in \mathfrak{a}$ Elemente, die eine $\mathbb{Q}$-Basis von L bilden und für die der Betrag der Diskriminante*

$$|\triangle(b_1, \ldots, b_n)|$$

unter all diesen Basen aus $\mathfrak{a}$ minimal sei. Dann ist

$$\mathfrak{a} = \mathbb{Z}b_1 + \ldots + \mathbb{Z}b_n\,.$$

Beweis. Sei $f \in \mathfrak{a}$ ein beliebiges Element. Wir haben zu zeigen, dass sich f als eine $\mathbb{Z}$-Linearkombination $f = k_1 b_1 + \ldots + k_n b_n$ mit $k_i \in \mathbb{Z}$ schreiben lässt, wenn die $b_1, \ldots, b_n \in \mathfrak{a}$ eine $\mathbb{Q}$-Basis von L mit minimalem Diskriminantenbetrag bilden. Es gibt eine eindeutige Darstellung

$$f = q_1 b_1 + \ldots + q_n b_n$$

mit rationalen Zahlen $q_i \in \mathbb{Q}$. Sei angenommen, dass ein q_i nicht ganzzahlig ist, wobei wir $i = 1$ annehmen dürfen. Wir schreiben dann $q_1 = k + \delta$ mit $k \in \mathbb{Z}$ und einer rationalen Zahl δ zwischen 0 und 1. Dann ist auch

$$c_1 = f - k b_1 = \delta b_1 + \sum_{i=2}^{n} q_i b_i,\, b_2, \ldots, b_n$$

eine $\mathbb{Q}$-Basis von L, die in $\mathfrak{a}$ liegt. Die Übergangsmatrix der beiden Basen ist

$$T = \begin{pmatrix} \delta & q_2 & q_3 & \cdots & q_n \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} .$$

Nach Lemma 16.2 gilt für die beiden Diskriminanten die Beziehung

$$\triangle(c_1, b_2, \ldots, b_n) = (\det(T))^2 \triangle(b_1, b_2, \ldots, b_n) .$$

Wegen $= (\det(T))^2 = \delta^2 < 1$ und da die Diskriminanten nach Lemma 16.3 nicht null sind, ist dies ein Widerspruch zur Minimalität der Diskriminanten. □

Korollar 18.7. *(Struktur von Idealen) Sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n und R der zugehörige Zahlbereich. Sei $\mathfrak{a}$ ein von null verschiedenes Ideal in R. Dann ist $\mathfrak{a}$ eine freie Gruppe vom Rang n, d.h. es gibt Elemente $b_1, \ldots, b_n \in \mathfrak{a}$ mit*

$$\mathfrak{a} = \mathbb{Z} b_1 + \ldots + \mathbb{Z} b_n .$$

Beweis. Nach Lemma 18.5 gibt es überhaupt Elemente $b_1, \ldots, b_n \in \mathfrak{a}$, die eine $\mathbb{Q}$-Basis von L bilden. Daher gibt es auch solche Basen, wo der Betrag der Diskriminante minimal ist. Für diese gilt nach Satz 18.6, dass sie ein $\mathbb{Z}$-Erzeugendensystem von $\mathfrak{a}$ bilden. □

Korollar 18.8. *(Additive Struktur der Zahlbereiche) Sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n und R der zugehörige Zahlbereich. Dann ist R eine freie Gruppe vom Rang n, d.h. es gibt Elemente $b_1, \ldots, b_n \in R$ mit*

$$R = \mathbb{Z} b_1 + \ldots + \mathbb{Z} b_n .$$

Beweis. Dies folgt direkt aus Korollar 18.7, angewendet auf das Ideal $\mathfrak{a} = R$. □

Ein solches System von Erzeugern $b_1, \ldots, b_n$ nennt man auch eine *Ganzheitsbasis*.

Korollar 18.9. *Sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n und R der zugehörige Zahlbereich. Es sei $m \in \mathbb{Z}$. Dann gibt es einen Gruppenisomorphismus*

$$R/(m) \cong (\mathbb{Z}/(m))^n .$$

Für eine Primzahl $m = p$ ist $R/(m)$ eine Algebra der Dimension n über dem Körper $\mathbb{Z}/(p)$. Zu jeder Primzahl p gibt es Primideale $\mathfrak{p}$ in R mit $\mathfrak{p} \cap \mathbb{Z} = (p)$.

Beweis. Nach Korollar 18.8 ist $R \cong \mathbb{Z}^n$ (als abelsche Gruppen). Das von m in R erzeugte Ideal besteht (unter dieser Identifizierung) aus allen Elementen der Form

$$m(a_1, \ldots, a_n) = (ma_1, \ldots, ma_n) ,$$

d.h. in jeder Komponente steht ein Vielfaches von m. Die Restklassengruppe $R/(m)$ ist demnach gleich $(\mathbb{Z}/(m))^n$ und besitzt m^n Elemente. Aufgrund der Ganzheit ist $mR \cap \mathbb{Z} = m\mathbb{Z}$ (siehe Aufgabe 18.4) und aufgrund des Isomorphiesatzes hat man einen injektiven Ringhomomorphismus

$$\mathbb{Z}/(m) \longrightarrow R/(m) ,$$

so dass $R/(m)$ eine von null verschiedene $\mathbb{Z}/(m)$-Algebra ist.

Für eine Primzahl p ist $R/(p)$ ein Vektorraum über $\mathbb{Z}/(p)$ der Dimension n. Deshalb gibt es darin (mindestens) ein maximales Ideal, und dieses entspricht einem maximalen Ideal $\mathfrak{m}$ in R mit $p \in \mathfrak{m}$. Daher ist $(p) = (p)R \cap \mathbb{Z} \subseteq \mathfrak{m} \cap \mathbb{Z}$, und dieser Durchschnitt ist ein Primideal, also gleich (p). □

Emmy Noether (1882-1935)

Definition 18.10. Ein kommutativer Ring R heißt *noethersch*, wenn jedes Ideal darin endlich erzeugt ist.

Korollar 18.11. *(Zahlbereiche sind noethersch) Jeder Zahlbereich ist ein noetherscher Ring.*

Beweis. Nach Satz 18.6 ist jedes von null verschiedene Ideal als additive Gruppe isomorph zu $\mathbb{Z}^n$, also ist insbesondere jedes Ideal als abelsche Gruppe endlich erzeugt. Insbesondere sind die Ideale dann als Ideale (also als R-Moduln) endlich erzeugt. □

Satz 18.12. *Sei R ein Zahlbereich. Dann ist jeder echte Restklassenring von R endlich.*

Beweis. Nach 18.3 gibt es ein $m \in \mathbb{Z} \cap \mathfrak{a}$, $m \neq 0$. Damit ist $mR \subseteq \mathfrak{a}$ und damit hat man eine surjektive Abbildung

$$R/(m) \longrightarrow R/\mathfrak{a}\,.$$

Der Ring links ist nach 18.9 endlich (mit m^n Elementen), also besitzt der Ring rechts auch nur endlich viele Elemente. □

Satz 18.13. *Sei R ein Zahlbereich. Dann ist jedes von null verschiedene Primideal von R bereits ein maximales Ideal.*

Beweis. Sei $\mathfrak{p}$ ein Primideal $\neq 0$ in R. Dann ist der Restklassenring $R/\mathfrak{p}$ nach Lemma 16.13 ein Integritätsbereich und nach Satz 18.12 endlich. Ein endlicher Integritätsbereich ist aber bereits ein Körper, so dass nach Satz 18.12 ein maximales Ideal vorliegt. □

Richard Dedekind (1831-1916)

Die bisher etablierten Eigenschaften von Zahlbereichen lassen sich im folgenden Begriff zusammenfassen.

Definition 18.14. Einen Integritätsbereich R nennt man einen *Dedekindbereich*, wenn er noethersch und normal ist und wenn jedes von null verschiedene Primideal darin maximal ist.

Korollar 18.15. *(Zahlbereiche sind Dedekindbereiche) Jeder Zahlbereich ist ein Dedekindbereich.*

Beweis. Dies folgt aus Satz 18.2, aus Korollar 18.11 und aus Satz 18.13. □

19. Vorlesung

Wir haben zuletzt gesehen, dass ein Zahlbereich, d.h. der Ring der ganzen Zahlen in einer endlichen Körpererweiterung L von $\mathbb{Q}$, stets ein sogenannter Dedekindbereich ist. Darüber hinaus gilt auch:

Satz 19.1. *Hauptidealbereiche sind Dedekindbereiche.*

Beweis. Die Normalität folgt aus Satz 3.7 und Satz 17.10. Die Eigenschaft noethersch folgt, da in einem Hauptidealbereich jedes Ideal sogar von einem Element erzeugt wird. Die Maximalität der von null verschiedenen Primideale folgt aus Satz 3.11. □

Definition 19.2. Sei R der Zahlbereich zur endlichen Körpererweiterung $\mathbb{Q} \subseteq L$. Dann nennt man die Diskriminante einer Ganzheitsbasis von R die *Diskriminante* von R (und die *Diskriminante* von L).

Die Diskriminante eines Zahlbereichs (oder eines Zahlkörpers) ist eine wohldefinierte ganze Zahl. Nach Definition ist die Diskriminante so gewählt, dass sie betragsmäßig minimal unter allen Diskriminanten zu (Ganzheits-)Basen aus R ist. Zwei solche Diskriminanten unterscheiden sich um ein Quadrat einer Einheit aus $\mathbb{Z}$, so dass auch das Vorzeichen wohldefiniert ist.

Wir wollen uns im weiteren Verlauf der Vorlesung mit Ringerweiterungen $\mathbb{Z} \subseteq R$, wo R der Ring der ganzen Zahlen in einem Erweiterungskörper von $\mathbb{Q}$ ist, beschäftigen, insbesondere mit quadratischen Erweiterungen. Was bei einer solchen Erweiterung mit einer (gewöhnlichen) Primzahl p passiert, also ob sie in R ein Primelement bleibt oder nicht und welche Primideale aus $\mathfrak{p}$ über p liegen, kann man weitgehend „modulo“ p bestimmen.

Ist z. B. R durch ein in $\mathbb{Z}[X]$ irreduzibles Polynom F gegeben, also $R \cong \mathbb{Z}[X]/(F)$, so wird die „Faser“ (diese Terminologie lässt sich genauer begründen) über p durch den Restklassenring $(\mathbb{Z}/(p))[X]/(\bar{F})$ beschrieben (den wir auch den Faserring über p nennen), wobei $\bar{F}$ bedeutet, dass man jeden Koeffizient von F (der ja eine ganze Zahl ist) durch seine Restklasse in $\mathbb{Z}/(p)$ ersetzt. Dabei kann natürlich die Irreduzibilität des Polynoms verloren gehen, und dies beschreibt wichtige Eigenschaften von p in R. Man beachte hierbei die Isomorphie

$$R/pR \cong (\mathbb{Z}/(p))[X]/(\bar{F}) \,,$$

die auf allgemeinen Gesetzen für Ideale beruht. Sie besagt insbesondere, dass p ein Primelement in R ist genau dann, wenn $\bar{F}$ irreduzibel in $(\mathbb{Z}/(p))[X]$ ist. Insgesamt liegt eine endliche Erweiterung

$$\mathbb{Z}/(p) \subseteq (\mathbb{Z}/(p))[X]/(\bar{F})$$

vor. Dabei sind beide Ringe endlich (besitzen also nur endlich viele Elemente), und links steht ein endlicher Körper, so dass die Erweiterung also sofort ein Vektorraum ist (der selbst ein Körper sein kann, aber nicht muss) und

eine gewisse Dimension besitzt (nämlich den Grad von $\bar{F}$). In diesem Abschnitt beschäftigen wir uns allgemein mit endlichen Ringen und vor allem mit endlichen Körpern.

Endliche Körper

Wir erinnern kurz an die Charakteristik eines Ringes. Zu jedem kommutativen Ring gibt es den kanonischen Ringhomomorphismus $\varphi : \mathbb{Z} \to R$, und der Kern davon ist ein Ideal $\mathfrak{a}$ in $\mathbb{Z}$ und hat daher die Form $\mathfrak{a} = (n)$ mit einem eindeutig bestimmten $n \geq 0$. Diese Zahl nennt man die Charakteristik von R. Ist R ein Körper, so ist dieser Kern ein Primideal, also $\mathfrak{a} = 0$ oder $\mathfrak{a} = (p)$ mit einer Primzahl p. Man spricht von Charakteristik null oder von positiver Charakteristik $p > 0$.

Wir erinnern ferner an den Begriff des Frobenius-Homomorphismus (siehe Aufgabe 4.7): für einen Ring R der Charakteristik p (p Primzahl) ist die Abbildung $R \to R$, $f \mapsto f^p$, ein Ringhomomorphismus.

Wir haben bereits die endlichen Primkörper $\mathbb{Z}/(p)$ zu einer Primzahl p kennengelernt. Sie besitzen p Elemente, und ein Körper besitzt genau dann die Charakteristik p, wenn er diesen Primkörper enthält.

Lemma 19.3. *Sei K ein endlicher Körper. Dann besitzt K genau p^n Elemente, wobei p eine Primzahl ist und $n \geq 1$.*

Beweis. Der endliche Körper kann nicht Charakteristik null besitzen, und als Charakteristik eines Körpers kommt ansonsten nach der Vorüberlegung nur eine Primzahl in Frage. Diese sei mit p bezeichnet. Das bedeutet, dass K den Körper $\mathbb{Z}/(p)$ enthält. Damit ist aber K ein Vektorraum über $\mathbb{Z}/(p)$, und zwar, da K endlich ist, von endlicher Dimension. Sei n die Dimension, $n \geq 1$. Dann hat man eine $\mathbb{Z}/(p)$-Vektorraum-Isomorphie $K \cong (\mathbb{Z}/(p))^n$ und somit besitzt K gerade p^n Elemente. □

Die vorstehende Aussage gilt allgemeiner für endliche Ringe, die einen Körper enthalten.

Endliche Körper der Anzahl p^n konstruiert man, indem man in $(\mathbb{Z}/(p))[X]$ ein irreduzibles Polynom vom Grad n findet. Ob ein gegebenes Polynom irreduzibel ist lässt sich dabei grundsätzlich in endlich vielen Schritten entscheiden, da es ja zu jedem kleineren Grad überhaupt nur endlich viele Polynome gibt, die als Teiler in Frage kommen können. Zur Konstruktion von einigen kleinen endlichen Körpern siehe die Aufgabe 19.6.

Lemma 19.4. *Sei K ein Körper der Charakteristik p, sei $q = p^e$, $e \geq 1$. Es sei*

$$M = \{x \in K : x^q = x\}.$$

Dann ist M ein Unterkörper von K.

Beweis. Zunächst gilt für jedes Element $x \in \mathbb{Z}/(p) \subseteq K$, dass

$$x^{p^e} = (x^p)^{p^{e-1}} = x^{p^{e-1}} = \ldots = x$$

ist, wobei wir wiederholt den kleinen Fermat (Korollar 4.6) benutzt haben. Insbesondere ist also $0, 1, -1 \in M$. Es ist $z^q = F^e(z)$ und der Frobenius

$$F : K \longrightarrow K,\ x \longmapsto x^p,$$

ist ein Ringhomomorphismus. Daher ist für $x, y \in M$ einerseits

$$(x+y)^q = F^e(x+y) = F^e(x) + F^e(y) = x^q + y^q = x + y$$

und andererseits

$$(xy)^q = x^q y^q = xy\,.$$

Ferner gilt für $x \in M$, $x \neq 0$, die Gleichheit

$$(x^{-1})^q = (x^q)^{-1} = x^{-1}\,,$$

so dass auch das Inverse zu M gehört und in der Tat ein Körper vorliegt. □

Lemma 19.5. *Sei K ein Körper der Charakteristik p, sei $q = p^e$, $e \geq 1$. Das Polynom $X^q - X$ zerfalle über K in Linearfaktoren. Dann ist*

$$M = \{x \in K : x^q = x\}$$

ein Unterkörper von K mit q Elementen.

Beweis. Nach Lemma 19.4 ist M ein Unterkörper von K, und nach Satz 5.2 besitzt er höchstens q Elemente. Es ist also zu zeigen, dass $F = X^q - X$ keine mehrfache Nullstellen hat. Dies folgt aber aus $F' = -1$ und einer kleinen Zusatzüberlegung (Aufgabe!). □

Wenn es also einen Erweiterungskörper $\mathbb{Z}/(p) \subseteq K$ gibt, über den das Polynom $X^q - X$ in Linearfaktoren zerfällt, so hat man bereits einen Körper mit q Elementen gefunden. Es gibt aber generell zu jedem Körper und jedem Polynom einen Erweiterungskörper, über dem das Polynom in Linearfaktoren zerfällt.

Lemma 19.6. *Sei K ein Körper und F ein Polynom aus $K[X]$. Dann gibt es einen Erweiterungskörper $K \subseteq L$ derart, dass F über L in Linearfaktoren zerfällt.*

Beweis. Sei $F = P_1 \cdots P_r$ die Zerlegung in Primpolynome in $K[X]$, und sei P_1 nicht linear. Dann ist

$$K \longrightarrow K[Y]/(P_1) =: K'$$

eine Körpererweiterung von K nach Satz 3.11. Wegen $P_1(Y) = 0$ in K' ist die Restklasse y von Y in K' eine Nullstelle von P_1. Daher gilt in $K'[X]$ die Faktorisierung

$$P_1 = (X - y)\tilde{P}\,,$$

wobei $\tilde{P}$ einen kleineren Grad als P_1 hat. Das Polynom F hat also über K' mindestens einen Linearfaktor mehr als über K. Induktive Anwendung von dieser Konstruktion liefert eine Kette von Erweiterungen $K \subset K' \subset K'' \ldots$, die stationär wird, sobald F in Linearfaktoren zerfällt. □

Satz 19.7. *Sei p eine Primzahl und $e \in \mathbb{N}_+$. Dann gibt es bis auf Isomorphie genau einen Körper mit $q = p^e$ Elementen.*

Beweis. Existenz. Wir wenden das Lemma 19.6 auf den Grundkörper $\mathbb{Z}/(p)$ und das Polynom $X^q - X$ an und erhalten einen Körper L der Charakteristik p, über dem $X^q - X$ in Linearfaktoren zerfällt. Nach Lemma 19.5 gibt es dann einen Unterkörper M von L, der aus genau q Elementen besteht.

Eindeutigkeit. Seien K und L zwei Körper mit q Elementen. Es sei $x \in K^\times$ ein primitives Element, das nach Satz 5.3 existiert. Daher ist $K \cong \mathbb{Z}/(p)[X]/(F)$, wobei $F \in \mathbb{Z}/(p)[X]$ das Minimalpolynom von $x \in K$ ist. Da $K^\times$ die Ordnung $q-1$ besitzt, gilt für jede Einheit $z^{q-1} = 1$ und damit überhaupt $z^q = z$ für alle $z \in K$. D.h., dass jedes Element von K eine Nullstelle von $X^q - X$ ist und dass daher $X^q - X$ über K in Linearfaktoren zerfällt. Da insbesondere $x^q - x = 0$ ist, muss das Minimalpolynom F ein Teiler von $X^q - X$ sein, also

$$X^q - X = F \cdot G\,.$$

Nun zerfällt (aus den gleichen Gründen) das Polynom $X^q - X$ auch über L und insbesondere hat F eine Nullstelle $\lambda \in L$. Der Einsetzungshomomorphismus liefert einen Ringhomomorphismus

$$K \cong \mathbb{Z}/(p)[X]/(F) \longrightarrow L\,.$$

Da beides Körper sind, muss dieser injektiv sein. Da links und rechts jeweils q-elementige Mengen stehen, muss er auch surjektiv sein. □

Notation 19.8. Sei p eine Primzahl und $e \in \mathbb{N}_+$. Der aufgrund von Satz 19.7 bis auf Isomorphie eindeutig bestimmte endliche Körper mit $q = p^e$ Elementen wird mit

$$\mathbb{F}_q$$

bezeichnet.

Quadratische Ringerweiterungen über einem Körper

Die quadratischen Erweiterungen eines Körpers kann man wie folgt charakterisieren.

Lemma 19.9. *Sei K ein Körper und $K \subset L$ eine Ringerweiterung vom Grad zwei. Dann gibt es die folgenden drei Möglichkeiten:*

(1) *L ist ein Körper.*
(2) *L ist von der Form $L = K[\epsilon]/\epsilon^2$.*

(3) *L ist der Produktring $L \cong K \times K$.*

Beweis. Nach Voraussetzung ist L ein zweidimensionaler K-Vektorraum. Wir können das Element $1 \in K \subset L$ zu einer K-Basis $1, u$ von L ergänzen ($u \notin K$). Wegen $u^2 \in L$ hat man eine Darstellung

$$u^2 = au + b$$

mit eindeutig bestimmten Elementen $a, b \in K$. Damit ist L isomorph zum Restklassenring $L \cong K[U]/(U^2 - aU - b)$. Ist das Polynom $P = U^2 - aU - b$ irreduzibel über K, so ist L ein Körper und wir sind im ersten Fall. Andernfalls gibt es eine Zerlegung $P = (U - c)(U - d)$ mit $c, d \in K$. Bei $c = d$ kann man die Restklasse von $U - c$ (also $u - c$) als ϵ bezeichnen und ist im zweiten Fall, da ja $\epsilon^2 = 0$ gilt. Sei also $c \neq d$ vorausgesetzt. Dann induzieren die beiden K-Algebra Homomorphismen $\varphi_1 : L \to K$, $u \mapsto c$, und $\varphi_2 : L \to K$, $u \mapsto d$, einen Homomorphismus

$$\varphi = \varphi_1 \times \varphi_2 : L \longrightarrow K \times K\,.$$

Dieser ist surjektiv, da $\varphi(1) = (1, 1)$ und $\varphi(u) = (c, d)$ ist und diese Bildvektoren linear unabhängig sind, also eine Basis von $K \times K$ bilden. Damit ist φ aber auch injektiv und es liegt eine Isomorphie wie im dritten Fall behauptet vor. □

20. Vorlesung

Definition 20.1. Ein *quadratischer Zahlbereich* ist der Ring der ganzen Zahlen in einem Erweiterungskörper von $\mathbb{Q}$ vom Grad 2.

Quadratische Zahlbereiche sind zwar die einfachsten Zahlbereiche, sind aber keinwegs einfach, sondern zeigen bereits die Reichhaltigkeit der algebraischen Zahlentheorie.

Wir interessieren uns in der algebraischen Zahlentheorie insbesondere für folgende Fragen.

(1) Wann ist ein Zahlbereich R ein Hauptidealbereich und wann ist er faktoriell?
(2) Wenn R kein Hauptidealbereich ist, gibt es dann andere Versionen, die die eindeutige Primfaktorzerlegung ersetzen (ja: lokal und auf Idealebene).
(3) Wenn R kein Hauptidealbereich ist, kann man dann die Abweichung von der Eigenschaft, ein Hauptidealbereich zu sein, in irgendeiner Form messen? (ja: durch die sogenannte Klassengruppe).

Definition 20.2. Eine ganze Zahl heißt *quadratfrei*, wenn jeder Primfaktor von ihr nur mit einfachem Exponent vorkommt.

Notation 20.3. Zu einer quadratfreien Zahl $D \neq 0, 1$ bezeichnet man den zugehörigen quadratischen Zahlbereich, also den Ring der ganzen Zahlen in $\mathbb{Q}[\sqrt{D}]$, mit

$$A_D \, .$$

Eine quadratischen Körpererweiterungen der rationalen Zahlen wird beschrieben durch ein normiertes irreduzibles Polynom, das man durch quadratisches Ergänzen auf die Form $X^2 - q$ bringen kann. Durch Multiplikation mit einem Quadrat (siehe Aufgabe 12.8) kann man q durch eine quadratfreie ganze Zahl ersetzen. Ein großer Unterschied besteht je nachdem, ob D positiv oder negativ ist. Im positiven Fall ist $\sqrt{D}$ eine reelle irrationale Zahl, im negativen Fall handelt es sich um eine imaginäre Zahl. Man definiert:

Definition 20.4. Sei $D \neq 0, 1$ quadratfrei und A_D der zugehörige quadratische Zahlbereich. Dann heißt A_D *reell-quadratisch*, wenn D positiv ist, und *imaginär-quadratisch*, wenn D negativ ist.

Definition 20.5. Sei D eine quadratfreie Zahl und sei $\mathbb{Q}[\sqrt{D}]$ die zugehörige quadratische Körpererweiterung und A_D der zugehörige quadratische Zahlbereich. Dann wird der Automorphismus (auf $\mathbb{Q}[\sqrt{D}]$, auf $\mathbb{Z}[\sqrt{D}]$ und auf A_D)

$$a + b\sqrt{D} \longmapsto a - b\sqrt{D}$$

als *Konjugation* bezeichnet.

Wir bezeichnen die Konjugation von z mit $\bar{z}$.

Bemerkung 20.6. Im imaginär-quadratischen Fall, wenn also $D < 0$ ist, so ist $\sqrt{D} = i\sqrt{-D}$ mit $\sqrt{-D}$ reell. Die Konjugation schickt dies dann auf $-\sqrt{D} = -i\sqrt{-D}$, so dass diese Konjugation mit der komplexen Konjugation übereinstimmt. Im reell-quadratischen Fall allerdings hat die Konjugation $\sqrt{D} \mapsto -\sqrt{D}$ nichts mit der komplexen Konjugation zu tun.

Bemerkung 20.7. Bei einer endlichen Körpererweiterung $K \subseteq L$ werden Norm und Spur eines Elementes $z \in L$ über die Determinante und die Spur der Multiplikationsabbildung $f : L \to L$ definiert. Im Fall einer quadratischen Erweiterung $\mathbb{Q} \subset \mathbb{Q}[\sqrt{D}]$ sind diese beiden Invarianten einfach zu berechnen: Da 1 und $\sqrt{D}$ eine $\mathbb{Q}$-Basis bilden, ist $z = a + b\sqrt{D}$ und damit ist die Multiplikationsmatrix gegeben durch

$$\begin{pmatrix} a & bD \\ b & a \end{pmatrix} .$$

Somit ist

$$N(z) = a^2 - b^2 D = (a + b\sqrt{D})(a - b\sqrt{D})$$

und

$$S(z) = 2a = (a + b\sqrt{D}) + (a - b\sqrt{D}) \, .$$

Lemma 20.8. *Sei $\mathbb{Q} \subset L$ eine quadratische Körpererweiterung und $f \in L$. Dann ist f genau dann ganz über $\mathbb{Z}$, wenn sowohl die Norm als auch die Spur von f zu $\mathbb{Z}$ gehören.*

Beweis. Dies folgt aus Satz 18.4, aus Satz 15.15, und aus der Gestalt des Minimalpolynoms im quadratischen Fall. □

Satz 20.9. *(Beschreibung quadratischer Zahlbereiche) Sei D eine quadratfreie Zahl und A_D der zugehörige quadratische Zahlbereich. Dann gilt*

$$A_D = \mathbb{Z}[\sqrt{D}], \text{ wenn } D = 2, 3 \mod 4$$

und

$$A_D = \mathbb{Z}[\frac{1+\sqrt{D}}{2}], \text{ wenn } D = 1 \mod 4\,.$$

Beweis. Sei $x \in A_D$ gegeben, $x = a + b\sqrt{D}$, $a, b \in \mathbb{Q}$. Aus Lemma 20.8 folgt

$$N(x) = a^2 - Db^2 \in \mathbb{Z} \text{ und } S(x) = 2a \in \mathbb{Z}\,.$$

Aus der zweiten Gleichung folgt, dass $a = n/2$ ist mit $n \in \mathbb{Z}$. Sei $b = r/s$ mit r, s teilerfremd, $s \geq 1$. Die erste Gleichung wird dann zu

$$\left(\frac{n}{2}\right)^2 - D\left(\frac{r}{s}\right)^2 = k \in \mathbb{Z}$$

bzw.

$$n^2 - 4D\left(\frac{r}{s}\right)^2 = 4k\,.$$

Dies bedeutet, da r und s teilerfremd sind, dass $4D$ von s^2 geteilt wird. Da ferner D quadratfrei ist, folgt, dass $s = 1$ oder $s = 2$ ist. Im ersten Fall ist n ein Vielfaches von 2 (da n^2 ein Vielfaches von 4 ist), so dass $x \in \mathbb{Z}[\sqrt{D}]$ ist. Sei also $s = 2$, was zur Bedingung

$$n^2 - Dr^2 = 4k$$

führt. Wir betrachten diese Gleichung modulo 4. Bei n und r gerade ist $x \in \mathbb{Z}[\sqrt{D}]$. Die einzigen Quadrate in $\mathbb{Z}/(4)$ sind 0 und 1, so dass für $D = 2, 3 \mod 4$ keine weitere Lösung existiert. Für $D = 1 \mod 4$ hingegen gibt es auch noch die Lösung $n = 1 \mod 2$ und $r = 1 \mod 2$, also n und r beide ungerade. Diese Lösungen gehören alle zu $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$.

Die umgekehrte Inklusion $\mathbb{Z}[\sqrt{D}] \subseteq A_D$ ist klar, sei also $D = 1 \mod 4$. Dann ist aber

$$\left(\frac{1+\sqrt{D}}{2}\right)^2 - \frac{1+\sqrt{D}}{2} = \frac{1 + D + 2\sqrt{D} - 2 - 2\sqrt{D}}{4} = \frac{D-1}{4} \in \mathbb{Z}\,,$$

und dabei ist $\frac{D-1}{4}$ eine ganze Zahl, so dass dies sofort eine Ganzheitsgleichung über $\mathbb{Z}$ ergibt. □

In den im vorstehenden Satz beschriebenen Fällen kann man jeweils den Ring der ganzen Zahlen durch eine Gleichung beschreiben. Für $D = 2, 3 \mod 4$ ist

$$A_D \cong \mathbb{Z}[X]/(X^2 - D)\,.$$

Für $D = 1 \mod 4$ setzt man häufig $\omega = \frac{1+\sqrt{D}}{2}$ für den Algebra-Erzeuger. Dieser Erzeuger erfüllt $\omega^2 - \omega - \frac{D-1}{4}$. Wir haben also

$$A_D \cong \mathbb{Z}[\omega]/(\omega^2 - \omega - \frac{D-1}{4})\,.$$

Wie werden häufiger in beiden Fällen diese Ganzheitsbasis $1, \omega$ nennen, mit $\omega = \sqrt{D}$ im ersten Fall und $\omega = \frac{1+\sqrt{D}}{2}$ im zweiten Fall.

Lemma 20.10. *(Diskriminante von quadratischen Zahlbereichen) Sei D eine quadratfreie Zahl und A_D der zugehörige quadratische Zahlbereich Dann ist die Diskriminante von A_D gleich*

$$\triangle = 4D, \text{ wenn } D = 2, 3 \mod 4$$

und

$$\triangle = D, \text{ wenn } D = 1 \mod 4\,.$$

Beweis. Im Fall $D = 2, 3 \mod 4$ ist $A_D = \mathbb{Z}[X]/(X^2 - D)$ und daher bilden 1 und X eine Ganzheitsbasis. Die möglichen Produkte zu dieser Basis sind in Matrixschreibweise

$$\begin{pmatrix} 1 & X \\ X & D \end{pmatrix}.$$

Wendet man darauf die Spur an so erhält man

$$\begin{pmatrix} 2 & 0 \\ 0 & 2D \end{pmatrix}$$

und die Determinante davon ist 4D.

Im Fall $D = 1 \mod 4$ ist hingegen $A_D = \mathbb{Z}[\omega]/(\omega^2 - \omega - \frac{D-1}{4})$ und eine Ganzheitsbasis ist 1 und ω. Die Matrix der Basisprodukte ist dann

$$\begin{pmatrix} 1 & \omega \\ \omega & \omega + \frac{D-1}{4} \end{pmatrix}.$$

Wendet man darauf die Spur an (die Spur von ω ist 1), so erhält man

$$\begin{pmatrix} 2 & 1 \\ 1 & 1 + \frac{D-1}{2} \end{pmatrix}$$

und die Determinante davon ist $2(1 + \frac{D-1}{2}) - 1 = 2 + D - 1 - 1 = D$. □

Bemerkung 20.11. Das Verhalten von Primzahlen in einer quadratischen Erweiterung lässt sich aus der oben erzielten Beschreibung mit Gleichungen erhalten.

Bei $D = 2, 3 \mod 4$ hat man einfach

$$R/(p) = \mathbb{Z}/(p)[X]/(X^2 - D)\,,$$

wobei man D durch $D \mod p$ ersetzen kann. Ob über p ein oder zwei Primideale liegen hängt davon ab, ob D ein Quadratrest modulo p ist und ob p ungerade ist, und p ist prim genau dann, wenn D kein Quadratrest modulo p ist.

Bei $D = 1 \mod 4$ hat man

$$R/(p) = \mathbb{Z}/(p)[\omega]/(\omega^2 - \omega - \frac{D-1}{4}) .$$

Ist p ungerade, so ist 2 eine Einheit in $\mathbb{Z}/(p)$ und man kann quadratisch ergänzen. Dann ist

$$\omega^2 - \omega - \frac{D-1}{4} = (\omega - \frac{1}{2})^2 - \frac{1}{4} - \frac{D-1}{4} = (\omega - \frac{1}{2})^2 - \frac{D}{4} .$$

Der Faserring hat daher die Form $\mathbb{Z}/(p)[Y]/(Y^2 - \frac{D}{4})$ und nach Multiplikation der Gleichung mit der Einheit 4 kann man dies als $\mathbb{Z}/(p)[Z]/(Z^2 - D)$ schreiben, so dass es wieder darum geht, ob D ein Quadratrest modulo p ist.

Ist hingegen $p = 2$, so schreibt sich die Gleichung als $\omega^2 + \omega + c$, wobei $c = 1$ ist, wenn $D = 5 \mod 8$ ist, und $c = 0$, wenn $D = 1 \mod 8$. Im ersten Fall ist die Gleichung irreduzibel über $\mathbb{Z}/(2)$ und 2 ist prim in R, im zweiten Fall ist die Gleichung reduzibel und 2 zerfällt in zwei Primideale.

Damit können wir entscheiden, wie viele Primideale in A_D über einer Primzahl p liegen. Wir wollen darüberhinaus genau beschreiben, wie das Zerlegungsverhalten einer Primzahl in einer quadratischen Erweiterung aussieht, und beginnen mit der Situation, wo p die Diskriminante teilt.

Lemma 20.12. *(Verzweigungsverhalten) Sei D eine quadratfreie Zahl und A_D der zugehörige quadratische Zahlbereich. Die Primzahl p sei ein Teiler der Diskriminante $\triangle$ von A_D. Dann gibt es oberhalb von p genau ein Primideal $\mathfrak{p}$ und es ist $\mathfrak{p}^2 = (p)A_D$.*

Beweis. Sei zunächst $D = 2, 3 \mod 4$, so dass $\triangle = 4D$ ist und als Primteiler p der Diskriminante 2 und die Teiler von D in Frage kommen. Es ist

$$A_D/(p) = (\mathbb{Z}[X]/(X^2 - D)/(p)) = (\mathbb{Z}/(p))[X]/(X^2 - D) .$$

Bei p steht hier $(\mathbb{Z}/(p))[X]/(X^2)$ und dieser Ring hat das einzige Primideal (X) mit $X^2 = 0$. Diesem Primideal entspricht in A_D das Primideal $\mathfrak{p} = (p, X)$. Es ist $\mathfrak{p}^2 = (p)$: Einerseits gilt für $f \in \mathfrak{p}^2$ im Faserring modulo p die Beziehung $f \in (X^2) = 0$, woraus $f \in (p)$ folgt. Andererseits ist $X^2 = D = up$ (in A_D). Da D quadratfrei ist, ist u teilerfremd zu p und daher kann man mit $1 = ru + sp$ schreiben

$$p = p(ru + sp) = rup + sp^2 = rX^2 + sp^2 \in \mathfrak{p}^2 .$$

Bei $p = 2$ gilt in $\mathbb{Z}/(2)[X]$ die Beziehung $(X - D)^2 = X^2 - D^2 = X^2 - D$, so dass eine analoge Situation vorliegt.

Sei jetzt $D = 1 \mod 4$ und sei p ein Primteiler von $\triangle = D$. Es ist

$$A_D/(p) = (\mathbb{Z}[\omega]/(\omega^2 - \omega - \frac{D-1}{4})/(p)) = (\mathbb{Z}/(p))[\omega]/(\omega^2 - \omega - \frac{D-1}{4}) .$$

Da D ungerade ist, ist 2 eine Einheit in $\mathbb{Z}/(p)$, so dass man die Gleichung modulo p schreiben kann als

$$(\omega - \frac{1}{2})^2 - \frac{1}{4} - \frac{D-1}{4} = (\omega - \frac{1}{2})^2 - \frac{D}{4} = (\omega - \frac{1}{2})^2 ,$$

so dass wieder eine analoge Situation vorliegt. □

Zu einem Ideal $\mathfrak{a}$ bezeichnet $\bar{\mathfrak{a}}$ das konjugierte Ideal, das aus allen konjugierten Elementen aus $\mathfrak{a}$ besteht.

Satz 20.13. *(Verhalten von Primzahlen in quadratischen Erweiterungen) Sei D eine quadratfreie Zahl und A_D der zugehörige quadratische Zahlbereich. Dann gibt es für eine Primzahl p die folgenden drei Möglichkeiten:*

(1) *p ist prim in A_D.*
(2) *Es gibt ein Primideal $\mathfrak{p}$ in A_D derart, dass $(p) = \mathfrak{p}^2$ ist.*
(3) *Es gibt ein Primideal $\mathfrak{p}$ in A_D derart, dass $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ ist mit $\mathfrak{p} \neq \bar{\mathfrak{p}}$.*

Beweis. Sei $R = A_D$. Wir betrachten den Restklassenring $L = R/(p)$, der eine quadratische Erweiterung des Körpers $\mathbb{Z}/(p)$ ist. Damit gibt es nach Lemma 19.9 die drei Möglichkeiten:

(1) L ist ein Körper.
(2) L ist von der Form $L = \mathbb{Z}/(p)[\epsilon]/\epsilon^2$.
(3) L ist der Produktring $L \cong \mathbb{Z}/(p) \times \mathbb{Z}/(p)$.

Im ersten Fall ist p ein Primelement in R. Im zweiten Fall besitzt L genau einen Restklassenkörper als einzigen nicht-trivialen Restklassenring. Nach der in Lemma 20.12 bewiesenen Korrespondenz gibt es also genau ein Primideal $\mathfrak{p}$ mit $(p) \subset \mathfrak{p}$ (das dem Ideal (ϵ) im Restklassenring entspricht). Dann ist $\mathfrak{p}^2 = (p)$(siehe den Beweis von 20.12).

Im dritten Fall besitzt L zwei Restklassenkörper und damit zwei maximale Ideale, deren Durchschnitt, das zugleich deren Produkt ist, das Nullideal ist. Zurückübersetzt nach R heißt das, dass es zwei verschiedene Primideale $\mathfrak{p}$ und $\mathfrak{q}$ gibt mit $(p) \subset \mathfrak{p}, \mathfrak{q}$ und mit $(p) = \mathfrak{p} \cap \mathfrak{q}$. Nach Aufgabe 18.8 ist $\mathfrak{p} \cap \mathfrak{q} = \mathfrak{p} \cdot \mathfrak{q}$. Mit $(p) \subset \mathfrak{p}$ ist auch $(p) \subset \bar{\mathfrak{p}}$. Wir zeigen, dass $\bar{\mathfrak{p}} = \mathfrak{q}$ ist, d.h., dass die beiden Primideale über p konjugiert vorliegen. Da nach dem Lemma 20.12 bei p der zweite Fall vorliegt, wissen wir, dass p die Diskriminate nicht teilt.

Bei $D = 2, 3 \mod 4$ ist p ungerade und D ist ein Quadratrest modulo p. Seien a und $-a$ die beiden verschiedenen (!) Quadratwurzeln modulo p. Dann werden die beiden Primideale durch $(p, a \pm \sqrt{D})$ beschrieben, und diese sind konjugiert.

Bei $D = 1 \mod 4$ und p ungerade ist nach der Bemerkung 20.11 über die explizite Beschreibung der Faserringe D wieder ein Quadratrest modulo p. Seien a und $-a$ die beiden verschiedenen (!) Quadratwurzeln modulo p. Dann ist $\omega - \frac{1}{2} = \pm\frac{a}{2}$ und daher sind die beiden Primideale gleich $(p, \omega \pm a - \frac{1}{2}) = (p, \frac{a \pm \sqrt{D}}{2})$, so dass wieder ein konjugiertes Paar vorliegt.

Bei $D = 1 \mod 4$ und $p = 2$ ist nach der Bemerkung 20.11 $D = 1 \mod 8$. Die Nullstellen des beschreibenden Polynoms sind dann 0 und 1. Daher sind die Primideale darüber gegeben durch $(2, \omega)$ und $(2, \omega - 1)$. Es ist $(2, \omega) = (2, \frac{\sqrt{D}+1}{2})$ und $(2, \omega - 1) = (2, \frac{\sqrt{D}+1}{2} - 1) = (2, \frac{\sqrt{D}-1}{2})$, so dass wieder ein konjugiertes Paar vorliegt. □

21. Vorlesung

Wir beschreiben nun die Ideale in einem quadratischen Zahlbereich genauer. Eine Strukturtheorie ist wichtig in Hinblick auf die Endlichkeit der Klassenzahl. Wir wissen bereits aufgrund von Korollar 18.7, dass jedes von null verschiedene Ideal von zwei Elementen über $\mathbb{Z}$ erzeugt wird. Genauer gilt.

Satz 21.1. *(Basis für Ideale) Sei A_D ein quadratischer Zahlbereich mit Ganzheitsbasis $1, \omega$ (siehe Satz 20.9 und die daran anschließende Bemerkung) und sei $\mathfrak{a}$ ein von Null verschiedenes Ideal in A_D. Dann besitzt $\mathfrak{a}$ eine $\mathbb{Z}$-Basis aus zwei Elementen a und b, wobei $a \in \mathbb{N}$ gewählt werden kann mit $(a) = \mathbb{Z} \cap \mathfrak{a}$ und $b = \alpha + \beta\omega$ mit*

$$\beta = \min\{|\tilde{\beta}| : \tilde{\alpha} + \tilde{\beta}\omega \in \mathfrak{a},\, \tilde{\beta} \neq 0\}\,.$$

Beweis. Seien $a \in \mathbb{Z}$ und $b = \alpha + \beta\omega$ wie im Satz beschrieben gewählt. Da a und β nicht null sind folgt, dass a und b linear unabhängig über $\mathbb{Q}$ sind. Es bleibt also zu zeigen, dass jedes Element $\tilde{\alpha} + \tilde{\beta}\omega \in \mathfrak{a}$ sich als $n_1 a + n_2 b$ schreiben lässt mit $n_1, n_2 \in \mathbb{Z}$. Es gibt eine Darstellung

$$\tilde{\alpha} + \tilde{\beta}\omega = q_1 a + q_2 b = q_1 a + q_2(\alpha + \beta\omega) = q_1 a + q_2\alpha + q_2\beta\omega$$

mit $q_1, q_2 \in \mathbb{Q}$. Dann ist $\tilde{\beta} = q_2\beta$. Die Zahlen β und $\tilde{\beta}$ beschreiben beide einen ω-Koeffizient von Elementen in $\mathfrak{a}$, und β war betragsmäßig minimal gewählt, so dass q_2 ganzzahlig sein muss (alle ω-Koeffizienten bilden ein Ideal in $\mathbb{Z}$). Wir ziehen in der obigen Gleichung $q_2 b \in \mathfrak{a}$ ab und erhalten

$$q_1 a = \tilde{\alpha} + \tilde{\beta}\omega - q_2 b = \tilde{\alpha} + \tilde{\beta}\omega - q_2(\alpha + \beta\omega) = \tilde{\alpha} - q_2\alpha\,,$$

und dies gehört zu $\mathbb{Z} \cap \mathfrak{a}$. Also handelt es sich um ein ganzzahliges Vielfaches von a und somit ist auch $q_1 \in \mathbb{Z}$. □

In der soeben konstruierten $\mathbb{Z}$-Basis von $\mathfrak{a}$ können wir sowohl a als auch β positiv wählen. Der Restklassenring $A_D/\mathfrak{a}$ ist eine endliche Erweiterung des

endlichen Ringes $\mathbb{Z}/(a)$, also selbst endlich. Im folgenden Diagramm sind die beiden horizontalen Abbildungen injektiv.

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & A_D \\ \downarrow & & \downarrow \\ \mathbb{Z}/(a) & \longrightarrow & A_D/\mathfrak{a}\,. \end{array}$$

Wir können die Anzahl von $A_D/\mathfrak{a}$ mittels einer $\mathbb{Z}$-Basis des Ideals ausdrücken. Wegen der surjektiven Abbildung $A_D/(a) \to A_D/\mathfrak{a}$ und aufgrund von Korollar 18.9 wissen wir, dass der Restklassenring maximal a^2 Elemente besitzt.

Satz 21.2. *(Elemente im Restklassenring) Sei A_D ein quadratischer Zahlbereich mit $\mathbb{Z}$-Basis 1 und ω und sei $\mathfrak{a}$ ein von Null verschiedenes Ideal in A_D. Es sei a und $b = \alpha + \beta\omega$ eine $\mathbb{Z}$-Basis (mit a, β positiv) wie im Satz 21.1 konstruiert. Dann werden die Elemente im Restklassenring $A_D/\mathfrak{a}$ eindeutig durch die Elemente*

$$\{r + s\omega : \, 0 \leq r < a, \, 0 \leq s < \beta\}$$

repräsentiert. Insbesondere besitzt der Restklassenring $a \cdot \beta$ Elemente.

Beweis. Sei $r + s\omega$ ein beliebiges Element in A_D. Durch Addition von Vielfachen von $b = \alpha + \beta\omega$ kann man erreichen, dass die zweite Komponente zwischen 0 und $\beta - 1$ liegt. Durch Addition von Vielfachen von a kann man dann erreichen, dass auch die erste Komponente zwischen 0 und $a - 1$ liegt, ohne die zweite Komponente zu verändern. Es wird also jede Restklasse durch Elemente im angegebenen Bereich repräsentiert.

Seien nun $r + s\omega$ und $\tilde{r} + \tilde{s}\omega$ im angegebenen Bereich und angenommen, dass sie das gleiche Element im Restklassenring repräsentieren. Sei $\tilde{s} \geq s$. Dann gehört die Differenz $\tilde{r} - r + (\tilde{s} - s)\omega$ zu $\mathfrak{a}$ und die zweite Komponente liegt zwischen 0 und $\beta - 1$. Aufgrund der Wahl von β muss diese Komponente null sein. Dann ist aber $\tilde{r} - r$ ein Vielfaches von a und wegen $|\tilde{r} - r| < a$ muss $\tilde{r} - r = 0$ sein, so dass also die beiden Elemente übereinstimmen und der Repräsentant eindeutig ist. □

Definition 21.3. Sei $D \neq 0, 1$ quadratfrei und A_D der zugehörige quadratische Zahlbereich. Sei $\mathfrak{a}$ ein von Null verschiedenes Ideal in A_D. Dann nennt man die (endliche) Anzahl des Restklassenringes $A_D/\mathfrak{a}$ die *Norm* von $\mathfrak{a}$. Sie wird mit

$$N(\mathfrak{a})$$

bezeichnet.

Mit der Norm lässt sich obiger Satz wie folgt ausdrücken.

Korollar 21.4. *Sei A_D ein quadratischer Zahlbereich mit $\mathbb{Z}$-Basis 1 und ω und sei $\mathfrak{a}$ ein von Null verschiedenes Ideal in A_D. Es sei a und $b = \alpha + \beta\omega$ eine $\mathbb{Z}$-Basis von $\mathfrak{a}$ (mit a, β positiv) wie im Satz 21.1 konstruiert. Dann ist*

$$N(\mathfrak{a}) = a\beta\,.$$

Beweis. Dies folgt unmittelbar aus Satz 21.2. □

Korollar 21.5. *Sei A_D ein quadratischer Zahlbereich mit $\mathbb{Z}$-Basis 1 und ω und sei $\mathfrak{a}$ ein von Null verschiedenes Ideal in A_D. Es sei $u = u_1 + u_2\omega$ und $v = v_1 + v_2\omega$ eine $\mathbb{Z}$-Basis von $\mathfrak{a}$. Dann ist*

$$N(\mathfrak{a}) = |\det \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix}|\,.$$

Beweis. Die Aussage ist für eine Basis der Form a und $b = \alpha + \beta\omega$, wie sie im Satz 21.1 konstruiert wurde, richtig. Für eine beliebige Basis u, v gibt es eine Übergangsmatrix M mit

$$u = Ma \text{ und } v = Mb\,.$$

Dabei ist M ganzzahlig und ihre Determinante hat den Betrag 1, so dass sich der Betrag der Determinante der Basis nicht ändert. □

Für ein Element und das davon erzeugte Hauptideal stimmen die beiden Normbegriffe überein.

Satz 21.6. *Sei A_D ein quadratischer Zahlbereich und sei $f \neq 0$ ein Element. Setze $\mathfrak{a} = (f)$. Dann gilt $N(\mathfrak{a}) = |N(f)|$.*

Beweis. Sei $f = f_1 + f_2\omega$ mit

$$\omega = \begin{cases} \sqrt{D}, & \text{falls } D = 2, 3 \mod 4 \\ \frac{1+\sqrt{D}}{2}, & \text{falls } D = 1 \mod 4\,. \end{cases}$$

Die Norm von f ist dann $N(f) = f\bar{f} =$

$$\begin{cases} (f_1 + f_2\sqrt{D})(f_1 - f_2\sqrt{D}) = f_1^2 - f_2^2 D, & D = 2, 3 \mod 4 \\ (f_1 + \frac{1}{2}f_2 + \frac{f_2\sqrt{D}}{2})(f_1 + \frac{1}{2}f_2 - \frac{f_2\sqrt{D}}{2}) = (f_1 + \frac{1}{2}f_2)^2 - \frac{f_2^2}{4}D, & D = 1 \mod 4\,. \end{cases}$$

Wir berechnen nun die Norm des von f erzeugten Ideals $\mathfrak{a} = (f)$ mit Hilfe des Korollars 21.5. Eine $\mathbb{Z}$-Basis des Ideals ist offenbar gegeben durch f und $f\omega$, wobei

$$f\omega = f_1\omega + f_2\omega^2 = \begin{cases} f_2 D + f_1\omega, & \text{falls } D = 2, 3 \mod 4 \\ f_2\frac{D-1}{4} + (f_1 + f_2)\omega, & \text{falls } D = 1 \mod 4\,. \end{cases}$$

Im ersten Fall haben wir

$$|\det \begin{pmatrix} f_1 & f_2 D \\ f_2 & f_1 \end{pmatrix}| = |f_1^2 - f_2^2 D|$$

und im zweiten Fall ist

$$|\det \begin{pmatrix} f_1 & f_2\frac{D-1}{4} \\ f_2 & f_1 + f_2 \end{pmatrix}| = |f_1(f_1 + f_2) - f_2^2\frac{D-1}{4}| = |f_1^2 + f_1 f_2 + \frac{1}{4}f_2^2 - \frac{1}{4}f_2^2 D|\,,$$

was mit den obigen Ergebnissen übereinstimmt. □

Satz 21.7. *Sei A_D ein quadratischer Zahlbereich und sei $\mathfrak{a}$ ein von Null verschiedenes Ideal in A_D. Dann gilt*

$$\mathfrak{a}\bar{\mathfrak{a}} = (N(\mathfrak{a}))\,.$$

Beweis. Sei $\mathfrak{a}$ durch eine $\mathbb{Z}$-Basis $a, b = \alpha + \beta\omega$ wie im Satz 21.1 gegeben. Das konjugierte Ideal $\bar{\mathfrak{a}}$ hat die Basis a und $\bar{b}$. Das Produktideal $\mathfrak{a}\bar{\mathfrak{a}}$ hat die vier Erzeuger

$$a^2, N(b), a\bar{b}, ab\,.$$

Wir behaupten, dass dieses Ideal gleich dem von $(a\beta)$ erzeugten Ideal ist, was ja nach Korollar 21.4 die Norm von $\mathfrak{a}$ ist. Zunächst teilt β sowohl a als auch α: Wegen $a\omega \in \mathfrak{a}$ hat man nämlich eine Darstellung

$$a\omega = \gamma a + \delta(\alpha + \beta\omega)$$

mit $\gamma, \delta \in \mathbb{Z}$. Daraus folgt durch Koeffizientenvergleich $a = \delta\beta$ und andererseits $\gamma a + \delta\alpha = 0$, woraus nach Kürzen mit δ sich $\alpha = -\gamma\beta$ ergibt. Insbesondere ist

$$\mathfrak{a} = (a, \alpha + \beta\omega) = (\beta\delta, -\beta\gamma + \beta\omega) = (\beta)(\delta, -\gamma + \omega)\,.$$

Mit dem Ideal $\mathfrak{b} = (\delta, -\gamma + \omega)$ können wir wegen $\mathfrak{a}\bar{\mathfrak{a}} = (\beta^2)\mathfrak{b}\bar{\mathfrak{b}}$ und wegen $N(\mathfrak{a}) = a\beta = \delta\beta^2 = \beta^2 N(\mathfrak{b})$ annehmen, dass $\beta = 1$ ist.

In dieser neuen Situation müssen wir $\mathfrak{a}\bar{\mathfrak{a}} = (a)$ zeigen. Aufgrund von $N(b) \in \mathfrak{a} \cap \mathbb{Z} = (a)$ haben wir die Inklusion $\mathfrak{a}\bar{\mathfrak{a}} \subseteq (a)$. Wir betrachten die Inklusionskette (in A_D)

$$(a^2, N(b), a(b + \bar{b})) \subseteq (a^2, N(b), ab, a\bar{b}) = \mathfrak{a}\bar{\mathfrak{a}} \subseteq (a)\,.$$

Es sei $c \in \mathbb{Z}$ der Erzeuger des Ideals links. Wir behaupten zunächst, dass die linke Inklusion eine Gleichheit ist. Dafür betrachten wir die Norm und die Spur von ab/c und erhalten

$$N(\frac{ab}{c}) = \frac{N(a)N(b)}{N(c)} = \frac{a^2 N(b)}{c^2} \in \mathbb{Z}\,.$$

und

$$S(\frac{ab}{c}) = \frac{1}{c}S(ab) = \frac{1}{c}(ab + a\bar{b}) \in \mathbb{Z}\,.$$

Damit sind die Norm und die Spur ganz über $\mathbb{Z}$, nach Lemma 20.8 ist das Element selbst ganz und damit ist ab ein Vielfaches von c. Wir wissen also

$$\frac{ab}{c} = \frac{a(\alpha + \omega)}{c} = \frac{\alpha}{c}a + \frac{a}{c}\omega \in A_D$$

und damit ist $\frac{a}{c} \in \mathbb{Z}$. Also wird a von c geteilt und in der Inklusionskette gilt Gleichheit. □

Korollar 21.8. *(Multiplikativität der Norm) Sei A_D ein quadratischer Zahlbereich und seien $\mathfrak{a}$ und $\mathfrak{b}$ von Null verschiedene Ideale in A_D. Dann gilt*

$$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})\,.$$

Beweis. Wir wenden Satz 21.7 wiederholt für Ideale an und erhalten

$$(N(\mathfrak{ab})) = (\mathfrak{ab})\overline{(\mathfrak{ab})} = \mathfrak{ab}\overline{\mathfrak{a}}\,\overline{\mathfrak{b}} = \mathfrak{a}\overline{\mathfrak{a}}\mathfrak{b}\overline{\mathfrak{b}} = (N(\mathfrak{a}))(N(\mathfrak{b})) = (N(\mathfrak{a})N(\mathfrak{b}))\,.$$

Da die Norm eines Ideals stets positiv ist folgt aus dieser Idealidentität die Gleichheit $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$. □

22. Vorlesung

In dieser und der nächsten Vorlesung beweisen wir zwei Versionen zur eindeutigen Primfaktorzerlegung in Zahlbereichen, die beide Abschwächungen zur eindeutigen Primfaktorzerlegung in $\mathbb{Z}$ sind. Die eine besagt, dass für einen Zahlbereich die eindeutige Primfaktorzerlegung von Elementen „lokal“ gilt (Satz 22.17 und Bemerkung 22.19). Die zweite Version besagt, dass man auf der Ebene der Ideale eine eindeutige Faktorzerlegung in Primideale erhält (Satz von Dedekind 23.13). Für die erste Version benötigen wir die Begriffe Nenneraufnahme, Lokalisierung und diskreter Bewertungsring.

Nenneraufnahme

Definition 22.1. Sei R ein kommutativer Ring. Eine Teilmenge $S \subseteq R$ heißt *multiplikatives System*, wenn die beiden Eigenschaften

(1) $1 \in S$
(2) Wenn $f, g \in S$, dann ist auch $fg \in S$

gelten.

Beispiel 22.2. Sei R ein kommutativer Ring und $\mathfrak{p}$ ein Primideal. Dann ist das Komplement $R - \mathfrak{p}$ ein multiplikatives System. Dies folgt unmittelbar aus der Definition.

Beispiel 22.3. Sei R ein kommutativer Ring und $f \in R$ ein Element. Dann bilden die Potenzen f^n, $n \in \mathbb{N}$, ein multiplikatives System.

Beispiel 22.4. Sei R ein Integritätsbereich. Dann bilden alle von null verschiedenen Elemente in R ein multiplikatives System, das mit $R^* = R - \{0\}$ bezeichnet wird.

Definition 22.5. Sei R ein Integritätsbereich und sei $S \subseteq R$ ein multiplikatives System, $0 \notin S$. Dann nennt man den Unterring

$$R_S := \left\{ \frac{f}{g} : f \in R,\, g \in S \right\} \subseteq Q(R)$$

die *Nenneraufnahme* zu S.

Für die Nenneraufnahme an einem Element f schreibt man einfach R_f statt $R_{\{f^n : n \in \mathbb{N}\}}$. Man kann eine Nenneraufnahme auch dann definieren, wenn R kein Integritätsbereich ist, siehe Aufgabe 22.1.

Definition 22.6. Sei R ein Integritätsbereich und sei $\mathfrak{p}$ ein Primideal. Dann nennt man die Nenneraufnahme an $S = R - \mathfrak{p}$ die *Lokalisierung* von R an $\mathfrak{p}$. Man schreibt dafür $R_\mathfrak{p}$. Es ist also

$$R_\mathfrak{p} := \{\frac{f}{g} : f \in R,\, g \notin \mathfrak{p}\} \subseteq Q(R)\,.$$

Definition 22.7. Ein kommutativer Ring R heißt *lokal*, wenn R genau ein maximales Ideal besitzt.

Der folgende Satz zeigt, dass diese Namensgebung Sinn macht.

Satz 22.8. *Sei R ein Integritätsbereich und sei $\mathfrak{p}$ ein Primideal in R. Dann ist die Lokalisierung $R_\mathfrak{p}$ ein lokaler Ring mit maximalem Ideal*

$$\mathfrak{p}R_\mathfrak{p} := \{\frac{f}{g} : g \notin \mathfrak{p}\}\,.$$

Beweis. Die angegebene Menge ist in der Tat ein Ideal in der Lokalisierung $R_\mathfrak{p} = \{\frac{f}{g} : f \in R,\, g \notin \mathfrak{p}\}$. Wir zeigen, dass das Komplement nur aus Einheiten besteht, so dass es sich um ein maximales Ideal handeln muss. Sei also $q = \frac{f}{g} \in R_\mathfrak{p}$, aber nicht in $\mathfrak{p}R_\mathfrak{p}$. Dann sind $f, g \notin \mathfrak{p}$ und somit gehört der inverse Bruch $\frac{g}{f}$ ebenfalls zur Lokalisierung. □

Satz 22.9. *(Durchschnitt von Lokalisierungen) Sei R ein Integritätsbereich mit Quotientenkörper $Q(R)$. Dann gilt*

$$R = \bigcap_{\mathfrak{m}\ \mathit{maximal}} R_\mathfrak{m}\,,$$

wobei der Durchschnitt über alle maximale Ideale läuft und in $Q(R)$ genommen wird.

Beweis. Die Inklusion $\subseteq$ ist klar. Sei also $q \in Q(R)$ und sei angenommen, q gehöre zum Durchschnitt rechts. Für jedes maximale Ideal $\mathfrak{m}$ ist also $q \in R_\mathfrak{m} \subset Q(R)$, d.h. es gibt $f_\mathfrak{m} \notin \mathfrak{m}$ und $a_\mathfrak{m} \in R$ mit $q = a_\mathfrak{m}/f_\mathfrak{m}$. Wir betrachten das Ideal

$$(f_\mathfrak{m} : \mathfrak{m} \text{ maximal})\,.$$

Dieses Ideal ist in keinem maximalen Ideal enthalten, also muss es nach dem Lemma von Zorn das Einheitsideal sein. Es gibt also endlich viele maximale Ideale $\mathfrak{m}_i$, $i = 1, \ldots, n$, mit $r_1 f_1 + \ldots + r_n f_n = 1$, wobei $f_i = f_{\mathfrak{m}_i}$ gesetzt wurde. Damit ist

$$q = \frac{a_1}{f_1} = \ldots = \frac{a_n}{f_n}\,.$$

Wir schreiben

$$q = q(r_1 f_1 + \ldots + r_n f_n) = qr_1 f_1 + \ldots + qr_n f_n = a_1 r_1 + \ldots + a_n r_n\,.$$

Also gehört q zu R. □

Satz 22.10. *Sei R ein normaler Integritätsbereich und sei $S \subseteq R$ ein multiplikatives System. Dann ist auch die Nenneraufnahme R_S normal.*

Beweis. Siehe Aufgabe 22.7. □

Diskrete Bewertungsringe

Definition 22.11. Ein *diskreter Bewertungsring* R ist ein Hauptidealbereich mit der Eigenschaft, dass es bis auf Assoziiertheit genau ein Primelement in R gibt.

Lemma 22.12. *Ein diskreter Bewertungsring ist ein lokaler, noetherscher Hauptidealbereich mit genau zwei Primidealen, nämlich* 0 *und dem maximalen Ideal* $\mathfrak{m}$.

Beweis. Ein diskreter Bewertungsring ist kein Körper. In einem Hauptidealbereich, der kein Körper ist, wird jedes maximale Ideal von einen Primelement erzeugt, und die Primerzeuger zu verschiedenen maximalen Idealen können nicht assoziiert sein. Also gibt es genau ein maximales Ideal. Nach Satz 19.1 ist ein Hauptidealbereich insbesondere ein Dedekindbereich, so dass es als weiteres Primideal nur noch das Nullideal gibt. □

Definition 22.13. Zu einem Element $f \in R$, $f \neq 0$, in einem diskreten Bewertungsring mit Primelement p heißt die Zahl $n \in \mathbb{N}$ mit der Eigenschaft $f = up^n$, wobei u eine Einheit bezeichne, die *Ordnung* von f. Sie wird mit $\operatorname{ord}(f)$ bezeichnet.

Die Ordnung ist also nichts anderes als der Exponent zum (bis auf Assoziiertheit) einzigen Primelement in der Primfaktorzerlegung. Sie hat folgende Eigenschaften.

Lemma 22.14. *Sei R ein diskreter Bewertungsring mit maximalem Ideal $\mathfrak{m} = (p)$. Dann hat die Ordnung*

$$R - \{0\} \longrightarrow \mathbb{N},\ f \longmapsto \operatorname{ord}(f)\,,$$

folgende Eigenschaften.

(1) $\operatorname{ord}(fg) = \operatorname{ord}(f) + \operatorname{ord}(g)$.
(2) $\operatorname{ord}(f+g) \geq \min\{\operatorname{ord}(f), \operatorname{ord}(g)\}$.
(3) $f \in \mathfrak{m}$ *genau dann, wenn* $\operatorname{ord}(f) \geq 1$.
(4) $f \in R^\times$ *genau dann, wenn* $\operatorname{ord}(f) = 0$.

Beweis. Siehe Aufgabe 22.12. □

Wir wollen eine wichtige Charakterisierung für diskrete Bewertungsringe beweisen, die insbesondere beinhaltet, dass ein normaler lokaler Integritätsbereich mit genau zwei Primidealen bereits ein diskreter Bewertungsring ist. Dazu benötigen wir einige Vorbereitungen.

Lemma 22.15. *Sei R ein kommutativer Ring und sei $f \in R$ nicht nilpotent. Dann gibt es ein Primideal $\mathfrak{p}$ in R mit $f \notin \mathfrak{p}$.*

Beweis. Wir betrachten die Menge der Ideale

$$M = \{\mathfrak{a} \text{ Ideal } : f^r \notin \mathfrak{a} \text{ für alle } r\}\,.$$

Diese Menge ist nicht leer, da sie das Nullideal enthält. Ferner ist sie induktiv geordnet (bzgl. der Inklusion): ist nämlich $\mathfrak{a}_i$ eine total geordnete Teilmenge, so ist deren Vereinigung ebenfalls ein Ideal, das keine Potenz von f enthält. Nach dem Lemma von Zorn gibt es daher maximale Elemente in M.

Wir behaupten, dass ein solches maximales Element $\mathfrak{p}$ ein Primideal ist. Sei dazu $g, h \in R$ und $g, h \in \mathfrak{p}$, und sei $g, h \notin \mathfrak{p}$ angenommen. Dann hat man echte Inklusionen

$$\mathfrak{p} \subset \mathfrak{p} + (g), \mathfrak{p} + (h)\,.$$

Wegen der Maximalität können die beiden Ideale rechts nicht zu M gehören, und das bedeutet, dass es Exponenten $r, s \in \mathbb{N}$ gibt mit

$$f^r \in \mathfrak{p} + (g) \text{ und } f^s \in \mathfrak{p} + (h)\,.$$

Dann ergibt sich der Widerspruch

$$f^r f^s \in \mathfrak{p} + (gh) \subseteq \mathfrak{p}\,.$$

□

Lemma 22.16. *Sei R ein noetherscher lokaler kommutativer Ring. Es sei vorausgesetzt, dass das maximale Ideal $\mathfrak{m}$ das einzige Primideal von R ist. Dann gibt es einen Exponenten $n \in \mathbb{N}$ mit*

$$\mathfrak{m}^n = 0\,.$$

Beweis. Wir behaupten zunächst, dass jedes Element in R eine Einheit oder nilpotent ist. Sei hierzu $f \in R$ keine Einheit. Dann ist $f \in \mathfrak{m}$. Angenommen, f ist nicht nilpotent. Dann gibt es nach Lemma 22.15 ein Primideal $\mathfrak{p}$ mit $f \notin \mathfrak{p}$. Damit ergibt sich der Widerspruch $\mathfrak{p} \neq \mathfrak{m}$.

Es ist also jedes Element im maximalen Ideal nilpotent. Insbesondere gibt es für ein endliches Erzeugendensystem $f_1, \ldots, f_k$ von $\mathfrak{m}$ eine natürliche Zahl m mit $f_i^m = 0$ für alle $i = 1, \ldots, k$. Sei $n = km$. Dann ist ein beliebiges Element aus $\mathfrak{m}^n$ von der Gestalt

$$(\sum_{i=1}^{k} a_{i1} f_i)(\sum_{i=1}^{k} a_{i2} f_i) \cdots (\sum_{i=1}^{k} a_{in} f_i)\,.$$

Ausmultiplizieren ergibt eine Linearkombination mit Monomen $f_1^{r_1} \cdots f_k^{r_k}$ und $\sum_{i=1}^{k} r_i = n$, so dass ein f_i mit einem Exponenten $\geq n/k = m$ vorkommt. Daher ist das Produkt 0. □

Satz 22.17. *Sei R ein noetherscher lokaler Integritätsbereich mit der Eigenschaft, dass es genau zwei Primideale $0 \subset \mathfrak{m}$ gibt. Dann sind folgende Aussagen äquivalent.*

(1) *R ist ein diskreter Bewertungsring.*
(2) *R ist ein Hauptidealbereich.*
(3) *R ist faktoriell.*
(4) *R ist normal.*
(5) *$\mathfrak{m}$ ist ein Hauptideal.*

Beweis. (1) $\Rightarrow$ (2) folgt direkt aus der Definition 22.11.

(2) $\Rightarrow$ (3) folgt aus Satz 3.7.

(3) $\Rightarrow$ (4) folgt aus Satz 17.10.

(4) $\Rightarrow$ (5). Sei $f \in \mathfrak{m}$, $f \neq 0$. Dann ist $R/(f)$ ein noetherscher lokaler Ring mit nur einem Primideal (nämlich $\tilde{\mathfrak{m}} = \mathfrak{m}R/(f)$). Daher gibt es nach Lemma 22.15 ein $n \in \mathbb{N}$ mit $\tilde{\mathfrak{m}}^n = 0$. Zurückübersetzt nach R heißt das, dass $\mathfrak{m}^n \subseteq (f)$ gilt. Wir wählen n minimal mit den Eigenschaften

$$\mathfrak{m}^n \subseteq (f) \text{ und } \mathfrak{m}^{n-1} \not\subseteq (f)\,.$$

Wähle $g \in \mathfrak{m}^{n-1}$ mit $g \notin (f)$ und betrachte

$$h := \frac{f}{g} \in Q(R) (\text{es ist } g \neq 0)\,.$$

Das Inverse, also $h^{-1} = \frac{g}{f}$, gehört nicht zu R, sonst wäre $g \in (f)$. Da R nach Voraussetzung normal ist, ist h^{-1} auch nicht ganz über R. Nach dem Modulkriterium Lemma 17.5 für die Ganzheit gilt insbesondere für das maximale Ideal $\mathfrak{m} \subset R$ die Beziehung

$$h^{-1}\mathfrak{m} \not\subseteq \mathfrak{m}$$

ist. Nach Wahl von g ist aber auch

$$h^{-1}\mathfrak{m} = \frac{g}{f}\mathfrak{m} \subseteq \frac{\mathfrak{m}^n}{f} \subseteq R\,.$$

Daher ist $h^{-1}\mathfrak{m}$ ein Ideal in R, das nicht im maximalen Ideal enthalten ist. Also ist $h^{-1}\mathfrak{m} = R$. Das heißt einerseits $h \in \mathfrak{m}$ und andererseits gilt für ein beliebiges $x \in \mathfrak{m}$ die Beziehung $h^{-1}x \in R$, also $x = h(h^{-1}x)$, also $x \in (h)$ und somit $(h) = \mathfrak{m}$.

(5) $\Rightarrow$ (1). Sei $\mathfrak{m} = (\pi)$. Dann ist π ein Primelement und zwar bis auf Assoziiertheit das einzige. Sei $f \in R$, $f \neq 0$ keine Einheit. Dann ist $f \in \mathfrak{m}$ und daher $f = \pi g_1$. Dann ist g_1 eine Einheit oder $g_1 \in \mathfrak{m}$. Im zweiten Fall ist wieder $g_1 = \pi g_2$ und $f = \pi^2 g_2$.

Wir behaupten, dass man $f = \pi^k u$ mit einer Einheit u schreiben kann. Andernfalls könnte man $f = \pi^n g_n$ mit beliebig großem n schreiben. Nach Lemma 22.15 gibt es ein $m \in \mathbb{N}$ mit $(\pi^m) = \mathfrak{m}^m \subseteq (f)$. Bei $n \geq m+1$ ergibt sich $\pi^m = af = a\pi^{m+1}b$ und der Widerspruch $1 = ab\pi$.

Es lässt sich also jede Nichteinheit $\neq 0$ als Produkt einer Potenz des Primelements mit einer Einheit schreiben. Insbesondere ist R faktoriell. Für ein

beliebiges Ideal $\mathfrak{a} = (f_1, \ldots, f_s)$ ist $f_i = \pi^{n_i} u_i$ mit Einheiten u_i. Dann sieht man leicht, dass $\mathfrak{a} = (\pi^n)$ ist mit $n = \min_i\{n_i\}$. □

Korollar 22.18. *Sei R ein Dedekindbereich und sei $\mathfrak{m}$ ein maximales Ideal in R. Dann ist die Lokalisierung*

$$R_{\mathfrak{m}}$$

ein diskreter Bewertungsring.

Beweis. Die Lokalisierung $R_{\mathfrak{m}}$ ist lokal nach Satz 22.8, so dass es lediglich die zwei Primideale 0 und $\mathfrak{m}R_{\mathfrak{m}}$ gibt. Ferner ist R noethersch. Da R normal ist, ist nach Satz 22.10 auch die Lokalisierung $R_{\mathfrak{m}}$ normal. Wegen Satz 22.17 ist $R_{\mathfrak{m}}$ ein diskreter Bewertungsring. □

Bemerkung 22.19. Korollar 22.18 besagt in Verbindung mit Satz 22.17, dass wenn man bei einem Dedekindbereich und spezieller einem Zahlbereich R zur Lokalisierung $R_{\mathfrak{m}}$ an einem maximalen Ideal $\mathfrak{m}$ übergeht, dass dort die eindeutige Primfaktorzerlegung gilt.

Korollar 22.20. *Sei R ein Dedekindbereich. Dann ist R der Durchschnitt von diskreten Bewertungsringen.*

Beweis. Nach Satz 22.9 ist

$$R = \bigcap_{\mathfrak{m}} R_{\mathfrak{m}}\,,$$

wobei $\mathfrak{m}$ durch alle maximalen Ideale von R läuft. Nach Satz 22.17 sind die beteiligten Lokalisierungen $R_{\mathfrak{m}}$ allesamt diskrete Bewertungsringe. □

23. Vorlesung

Definition 23.1. Sei R ein Zahlbereich, $\mathfrak{p} \neq 0$ ein Primideal in R und $f \in R$, $f \neq 0$. Dann heißt die Ordnung $\mathrm{ord}(f)$ im diskreten Bewertungsring $R_{\mathfrak{p}}$ die *Ordnung* von f am Primideal $\mathfrak{p}$ (oder an der Primstelle $\mathfrak{p}$ oder in $R_{\mathfrak{p}}$). Sie wird mit $\mathrm{ord}_{\mathfrak{p}}(f)$ bezeichnet.

Lemma 23.2. *Sei R ein Zahlbereich und $\mathfrak{p} \neq 0$ ein Primideal in R. Dann hat die Ordnung an $\mathfrak{p}$, also*

$$R - \{0\} \longrightarrow \mathbb{N},\ f \longmapsto \mathrm{ord}_{\mathfrak{p}}(f)\,,$$

folgende Eigenschaften.

(1) $\mathrm{ord}_{\mathfrak{p}}(fg) = \mathrm{ord}_{\mathfrak{p}}(f) + \mathrm{ord}_{\mathfrak{p}}(g)$.
(2) $\mathrm{ord}_{\mathfrak{p}}(f+g) \geq \min\{\mathrm{ord}_{\mathfrak{p}}(f), \mathrm{ord}_{\mathfrak{p}}(g)\}$.
(3) $f \in \mathfrak{p}$ *genau dann, wenn* $\mathrm{ord}_{\mathfrak{p}}(f) \geq 1$.

Beweis. (1) und (2) folgen direkt aus Lemma 22.14. Bei (3) ist zu beachten, dass für $f \in R$ gilt, dass $f \in \mathfrak{p}$ ist genau dann, wenn $f \in \mathfrak{p}R_{\mathfrak{p}}$ ist. Letzteres bedeutet nämlich, dass $f = q_1 f_1 + \ldots + q_n f_n$ ist mit $f_i \in \mathfrak{p}$ und $q_i \in R_{\mathfrak{p}}$, also $q_i = \frac{r_i}{s_i}$ mit $s_i \notin \mathfrak{p}$. Mit dem Hauptnenner $s = s_1 \cdots s_n$ ist dann $sf =$

$a_1 f_1 + \ldots + a_n f_n \in \mathfrak{p}$, woraus $f \in \mathfrak{p}$ folgt. Damit folgt die Behauptung aus Lemma 22.14(3). □

Definition 23.3. Sei R ein Zahlbereich und $f \in R$, $f \neq 0$. Dann heißt die Abbildung, die jedem Primideal $\mathfrak{p} \neq 0$ in R die Ordnung $\mathrm{ord}_{\mathfrak{p}}(f)$ zuordnet, der durch f definierte *Hauptdivisor*. Er wird mit $\mathrm{div}(f)$ bezeichnet und als formale Summe

$$\mathrm{div}(f) = \sum_{\mathfrak{p}} \mathrm{ord}_{\mathfrak{p}}(f) \cdot \mathfrak{p}$$

geschrieben.

Lemma 23.4. *Sei R ein Zahlbereich. Dann hat die Abbildung, die einem Ringelement den Hauptdivisor zuordnet, also*

$$R - \{0\} \longrightarrow \text{Hauptdivisoren},\ f \longmapsto \mathrm{div}(f)\,,$$

folgende Eigenschaften.

(1) $\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g)$.
(2) $\mathrm{div}(f+g) \geq \min\{\mathrm{div}(f), \mathrm{div}(g)\}$.

Hierbei sind die Operationen rechts punktweise definiert.

Beweis. Dies folgt direkt aus Lemma 23.2 durch Betrachtung an den einzelnen Primidealen. □

Lemma 23.5. *Sei R ein Zahlbereich und $f \in R$, $f \neq 0$. Dann ist nur für endlich viele Primideale $\mathfrak{p} \neq 0$ in R die Ordnung $\mathrm{ord}_{\mathfrak{p}}(f)$ von null verschieden. Das heißt, dass der Hauptdivisor $\mathrm{div}(f) = \sum_{\mathfrak{p}} \mathrm{ord}_{\mathfrak{p}}(f) \cdot \mathfrak{p}$ eine endliche Summe ist.*

Beweis. Sei $\mathfrak{p} \neq 0$ ein Primideal in R und $f \notin \mathfrak{p}$. Dann ist f in $R_{\mathfrak{p}}$ eine Einheit. Damit ist $\mathrm{ord}_{\mathfrak{p}}(f) = 0$. Da der Restklassenring $R/(f)$ endlich ist nach Satz 18.12, folgt sofort, dass f nur in endlich vielen Primidealen enthalten ist, und nur für diese ist $\mathrm{ord}_{\mathfrak{p}}(f) > 0$. □

Definition 23.6. Sei R ein Zahlbereich. Ein *effektiver Divisor* ist eine formale Summe

$$\sum_{\mathfrak{p}} n_{\mathfrak{p}} \cdot \mathfrak{p}\,,$$

die sich über alle Primideale $\mathfrak{p} \neq 0$ aus R erstreckt und wobei $n_{\mathfrak{p}}$ natürliche Zahlen sind mit $n_{\mathfrak{p}} = 0$ für fast alle $\mathfrak{p}$.

Obiges Lemma zeigt, dass ein Hauptdivisor zu einem ganzen Element wirklich ein effektiver Divisor ist. Wir werden im Weiteren sehen, dass die Frage, welche Divisoren Hauptdivisoren sind, eng mit der Frage nach der Faktorialität von Zahlbereichen zusammenhängt. Der Zugang über Divisoren hat den Vorteil, dass er erlaubt (siehe weiter unten), eine Gruppe, die sogenannte *Divisorenklassengruppe* einzuführen, die die Abweichung von der Faktorialität messen kann.

Definition 23.7. Sei R ein Zahlbereich und $\mathfrak{a} \neq 0$ ein von null verschiedenes Ideal in R. Dann nennt man den Divisor

$$\operatorname{div}(\mathfrak{a}) = \sum_{\mathfrak{p}} m_{\mathfrak{p}} \cdot \mathfrak{p}$$

mit

$$m_{\mathfrak{p}} = \operatorname{ord}_{\mathfrak{p}}(\mathfrak{a}) = \min\{\operatorname{ord}_{\mathfrak{p}}(f) : f \in \mathfrak{a},\, f \neq 0\}$$

den *Divisor zum Ideal* $\mathfrak{a}$.

Bemerkung 23.8. Man kann den Divisor zu einem Ideal auch durch

$$\operatorname{div}(\mathfrak{a}) = \min\{\operatorname{div}(f) : f \in \mathfrak{a},\, f \neq 0\}$$

definieren, wobei das Minimum über Divisoren komponentenweise erklärt ist. Es gibt im Allgemeinen kein Element, das an allen Primstellen simultan das Minimum annimmt. Da zu einem einzelnen Element $0 \neq f \in \mathfrak{a}$ der zugehörige Hauptdivisor nur an endlich vielen Stellen von null verschieden ist, gilt das erst recht für den Divisor zu einem Ideal.

Die Ordnung $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{a})$ kann man auch als Ordnung des Ideals $\operatorname{ord}(\mathfrak{a}R_{\mathfrak{p}})$ im diskreten Bewertungsring $R_{\mathfrak{p}}$ ansehen. Dieses Ideal hat einen Erzeuger p^k, wobei p ein Primelement im diskreten Bewertungsring ist; die Ordnung ist dann k.

Lemma 23.9. *Sei R ein Zahlbereich. Dann erfüllt die Zuordnung (für von null verschiedene Ideale)*

$$\mathfrak{a} \longmapsto \operatorname{div}(\mathfrak{a})$$

folgende Eigenschaften:

(1) $\operatorname{div}(\mathfrak{p}) = 1 \cdot \mathfrak{p}$ *für ein Primideal* $\mathfrak{p} \neq 0$.
(2) $\operatorname{div}(\mathfrak{a} \cdot \mathfrak{b}) = \operatorname{div}(\mathfrak{a}) + \operatorname{div}(\mathfrak{b})$.
(3) *Für* $\mathfrak{a} \subseteq \mathfrak{b}$ *ist* $\operatorname{div}(\mathfrak{a}) \geq \operatorname{div}(\mathfrak{b})$.
(4) $\operatorname{div}(\mathfrak{a} + \mathfrak{b}) = \min\{\operatorname{div}(\mathfrak{a}), \operatorname{div}(\mathfrak{b})\}$.

Beweis. (1) Für jedes Element $f \in \mathfrak{p}$ gilt auch $f \in \mathfrak{p}R_{\mathfrak{p}}$ und daher ist $\operatorname{ord}_{\mathfrak{p}}(f) \geq 1$. Umgekehrt besitzt der diskrete Bewertungsring $R_{\mathfrak{p}}$ ein Element p, das das maximale Ideal $\mathfrak{p}R_{\mathfrak{p}}$ erzeugt und die Ordnung eins hat. Man kann schreiben $p = a/b$ mit $a, b \in R$ und $b \notin \mathfrak{p}$. Dabei ist $a \in \mathfrak{p}$ und a hat in $R_{\mathfrak{p}}$ die Ordnung eins.

Sei nun $\mathfrak{q} \neq \mathfrak{p}$ ein weiteres Primideal $\neq 0$. Da beide maximal sind gibt es ein Element $g \in \mathfrak{p}$, $g \notin \mathfrak{q}$. Dieses hat dann in $\mathfrak{q}$ die Ordnung 0.

(2) Fixiere ein Primideal $\mathfrak{p}$. Sei $h \in \mathfrak{a} \cdot \mathfrak{b}$ und schreibe $h = \sum_{i=1}^{k} r_i f_i g_i$ mit $f_i \in \mathfrak{a}$ und $g_i \in \mathfrak{b}$. Dann ist nach Lemma 23.4

$$\begin{aligned} \operatorname{div}(h) &\geq \min\{\operatorname{div}(r_i f_i g_i) : i = 1, \ldots, k\} \\ &\geq \min\{\operatorname{div}(f_i) + \operatorname{div}(g_i) : i = 1, \ldots, k\} \\ &\geq \operatorname{div}(\mathfrak{a}) + \operatorname{div}(\mathfrak{b}). \end{aligned}$$

Für die Umkehrung schreiben wir $\operatorname{div}(\mathfrak{a}) = \sum_{\mathfrak{q}} n_{\mathfrak{q}} \cdot \mathfrak{q}$ und $\operatorname{div}(\mathfrak{b}) = \sum_{\mathfrak{q}} m_{\mathfrak{q}} \cdot \mathfrak{q}$. Zu fixiertem $\mathfrak{p}$ gibt es ein $f \in \mathfrak{a}$ und ein $g \in \mathfrak{b}$ mit $\operatorname{ord}_{\mathfrak{p}}(f) = n_{\mathfrak{p}}$ und $\operatorname{ord}_{\mathfrak{p}}(g) = m_{\mathfrak{p}}$. Dann ist $fg \in \mathfrak{ab}$ und

$$\operatorname{ord}_{\mathfrak{p}}(fg) = \operatorname{ord}_{\mathfrak{p}}(f) + \operatorname{ord}_{\mathfrak{p}}(g) = n_{\mathfrak{p}} + m_{\mathfrak{p}}\,.$$

(3) Das ist trivial.

(4) Die Abschätzung „$\geq$“ folgt aus $\operatorname{div}(f+g) \geq \min\{\operatorname{div}(f), \operatorname{div}(g)\}$. Die Abschätzung „$\leq$“ folgt aus Teil (3). □

Definition 23.10. Sei R ein Zahlbereich und

$$D = \sum_{\mathfrak{p}} n_{\mathfrak{p}} \cdot \mathfrak{p}$$

ein effektiver Divisor (wobei $\mathfrak{p}$ durch die Menge der Primideale $\neq 0$ läuft). Dann nennt man

$$\{f \in R : \operatorname{div}(f) \geq D\}$$

das *Ideal zum Divisor* D. Es wird mit $\operatorname{Id}(D)$ bezeichnet.

In der vorstehenden Definition verwenden wir die Konvention, dass in Ungleichungen der Ausdruck $\operatorname{div}(0)$ als ∞ zu verstehen ist. Damit gehört also 0 zu $\operatorname{Id}(D)$. Es ergibt sich sofort, dass es sich in der Tat um ein Ideal handelt. Es ist auch nicht das Nullideal, da wir zu den endlich vielen Primidealen $\mathfrak{p}_i$, $i = 1, \ldots, k$, mit $n_i = n_{\mathfrak{p}_i} > 0$ Elemente $0 \neq f_i \in \mathfrak{p}_i$ wählen können. Dann gehört aber das Produkt $f_1^{n_1} \cdots f_k^{n_k}$ zu dem zu D gehörenden Ideal.

Der folgende Satz zeigt, dass die beiden soeben eingeführten Zuordnungen zwischen den effektiven Divisoren und den von null verschiedenen Idealen in einem Zahlbereich invers zueinander sind. Dies sollte man als eine einfache und übersichtliche Beschreibung für die Menge aller Ideale ansehen.

Satz 23.11. *(Ideale und effektive Divisoren) Sei R ein Zahlbereich. Dann sind die Zuordnungen*

$$\mathfrak{a} \longmapsto \operatorname{div}(\mathfrak{a}) \quad \textit{und} \quad D \longmapsto \operatorname{Id}(D)$$

zueinander inverse Abbildungen zwischen der Menge der von null verschiedenen Ideale und der Menge der effektiven Divisoren. Diese Bijektion übersetzt das Produkt von Idealen in die Summe von Divisoren.

Beweis. Wir starten mit einem Ideal $\mathfrak{a} \neq 0$ und vergleichen $\mathfrak{a}$ und $\operatorname{Id}(\operatorname{div}(\mathfrak{a}))$. Sei zunächst $f \in \mathfrak{a}$. Es ist dann $\operatorname{ord}_{\mathfrak{p}}(f) \geq \min\{\operatorname{ord}_{\mathfrak{p}}(g) : g \in \mathfrak{a}\}$ für jedes Primideal $\mathfrak{p} \neq 0$, so dass natürlich $\operatorname{div}(f) \geq \operatorname{div}(\mathfrak{a})$ gilt. Also ist $f \in \operatorname{Id}(\operatorname{div}(\mathfrak{a}))$. Ist hingegen $f \notin \mathfrak{a}$, so gibt es (nach Aufgabe 22.7) auch ein Primideal $\mathfrak{p} \neq 0$ mit $f \notin \mathfrak{a}R_{\mathfrak{p}}$. Da $R_{\mathfrak{p}}$ ein diskreter Bewertungsring ist, gilt $\operatorname{ord}_{\mathfrak{p}}(f) < \operatorname{ord}_{\mathfrak{p}}(\mathfrak{a})$. Also ist $\operatorname{div}(f) \not\geq \operatorname{div}(\mathfrak{a})$ und somit $f \notin \operatorname{Id}(\operatorname{div}(\mathfrak{a}))$.

Wir starten nun mit einem effektiven Divisor D und vergleichen D mit $\operatorname{div}(\operatorname{Id}(D))$. Die Abschätzung $D \leq \operatorname{div}(\operatorname{Id}(D))$ ist trivial. Für die andere

Richtung fixieren wir ein Primideal $\mathfrak{p}$ und bezeichnen mit $n_\mathfrak{p}$ die Ordnung von D an dieser Primstelle. Wir haben ein $f \in \mathrm{Id}(D)$ zu finden, das an der Stelle $\mathfrak{p}$ die Ordnung $n_\mathfrak{p}$ besitzt. Es sei $p \in \mathfrak{p}$ ein Element in R derart, dass p in $R_\mathfrak{p}$ das maximale Ideal erzeugt. Es seien $\mathfrak{q}_1, \ldots, \mathfrak{q}_k$ alle Primideale $\neq \mathfrak{p}$, an denen D von null verschieden ist. Da alle von null verschiedenen Primideale in R maximal sind, gibt es zu jedem $\mathfrak{q}_i$ ein h_i mit $h_i \in \mathfrak{q}_i$ und $h_i \notin \mathfrak{p}$. Dann hat, für hinreichend große ν_i, das Element

$$f = p^{n_\mathfrak{p}} \prod_{i=1}^{k} h_i^{\nu_i}$$

einerseits die Eigenschaft $\mathrm{div}(f) \geq D$, also $f \in \mathrm{Id}(D)$, und andererseits die Eigenschaft $\mathrm{ord}_\mathfrak{p}(f) = \mathrm{ord}_\mathfrak{p}(p^{n_\mathfrak{p}}) = n_\mathfrak{p}$ wie gewünscht, da die h_i in $\mathfrak{p}$ die Ordnung null haben.

Der Zusatz folgt aus Lemma 23.9. □

Korollar 23.12. *Sei R ein Zahlbereich und seien $\mathfrak{a}$ und $\mathfrak{b}$ Ideale in R. Dann gilt $\mathfrak{a} \subseteq \mathfrak{b}$ genau dann, wenn es ein Ideal $\mathfrak{c}$ gibt mit $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$.*

Beweis. Die Implikation „$\Leftarrow$“ gilt in beliebigen kommutativen Ringen. Die andere Implikation ist richtig, wenn $\mathfrak{a} = 0$ ist. Wir können also annehmen, dass die beteiligten Ideale von null verschieden sind. Die Bedingung impliziert nach Lemma 23.9, dass $\mathrm{div}(\mathfrak{a}) \geq \mathrm{div}(\mathfrak{b})$ ist. Somit ist $\mathrm{div}(\mathfrak{a}) = \mathrm{div}(\mathfrak{b}) + E$ mit einem effektiven Divisor E. Nach dem Bijektionssatz (Satz 23.11) übersetzt sich dies zurück zu $\mathfrak{a} = \mathfrak{b} \cdot \mathrm{Id}(E)$, so dass mit $\mathfrak{c} = \mathrm{Id}(E)$ die rechte Seite erfüllt ist. □

Satz 23.13. *(Eindeutige Idealzerlegung nach Dedekind) Sei R ein Zahlbereich und $\mathfrak{a} \neq 0$ ein Ideal in R. Dann gibt es eine Produktdarstellung*

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}$$

mit (bis auf die Reihenfolge) eindeutig bestimmten Primidealen $\mathfrak{p}_i \neq 0$ aus R und eindeutig bestimmten Exponenten r_i, $i = 1, \ldots, k$.

Beweis. Wir benutzen die bijektive Beziehung (Satz 23.11) zwischen Idealen $\neq 0$ und effektiven Divisoren. Auf der Seite der Divisoren haben wir offenbar eine eindeutige Darstellung

$$\mathrm{div}(\mathfrak{a}) = \sum_{i=1}^{k} r_i \mathfrak{p}_i$$

mit geeigneten Primidealen $\mathfrak{p}_i$. Wendet man auf diese Darstellung die Abbildung $D \mapsto \mathrm{Id}(D)$ an, so erhält man links das Ideal zurück. Es genügt also zu zeigen, dass der Divisor rechts auf das Ideal $\mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}$ abgebildet wird. Dies folgt aber sofort aus Teil (1) und (2) des Lemmas 23.9. □

Korollar 23.14. *Sei R ein Zahlbereich und $f \in R$, $f \neq 0$. Dann gibt es eine Produktdarstellung für das Hauptideal*

$$(f) = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}$$

mit (bis auf die Reihenfolge) eindeutig bestimmten Primidealen $\mathfrak{p}_i \neq 0$ aus R und eindeutig bestimmten Exponenten r_i, $i = 1, \ldots, k$.

Beweis. Dies folgt direkt aus Satz 23.13. □

24. Vorlesung

Die Menge der effektiven Divisoren bilden mit der natürlichen Addition ein kommutatives Monoid, aber keine Gruppe, da ja die Koeffizienten $n_\mathfrak{p}$ alle nichtnegativ sind. Lässt man auch negative ganze Zahlen zu, so gelangt man zum Begriff des Divisors, die eine Gruppe bilden. Auch den Begriff des Hauptdivisors kann man so erweitern, dass er nicht nur für ganze Elemente aus R, sondern auch für rationale Elemente, also Elemente aus dem Quotientenkörper $Q(R)$, definiert ist.

Definition 24.1. Sei R ein Zahlbereich. Ein *Divisor* ist eine formale Summe

$$\sum_\mathfrak{p} n_\mathfrak{p} \cdot \mathfrak{p}\,,$$

die sich über alle Primideale $\mathfrak{p} \neq 0$ aus R erstreckt und wobei $n_\mathfrak{p}$ ganze Zahlen sind mit $n_\mathfrak{p} = 0$ für fast alle $\mathfrak{p}$.

Für einen diskreten Bewertungsring lässt sich die Ordnung $\mathrm{ord} : R\setminus\{0\} \to \mathbb{N}$, $f \mapsto \mathrm{ord}(f)$, zu einer Ordnungsfunktion auf dem Quotientenkörper fortsetzen,

$$\mathrm{ord} : Q(R) \setminus \{0\} \longrightarrow \mathbb{Z}, q \longmapsto \mathrm{ord}(q)\,,$$

siehe Aufgabe 24.1.

Definition 24.2. Sei R ein Zahlbereich und $q \in Q(R)$, $q \neq 0$. Dann heißt die Abbildung, die jedem Primideal $\mathfrak{p} \neq 0$ in R die Ordnung $\mathrm{ord}_\mathfrak{p}(q)$ zuordnet, der durch q definierte *Hauptdivisor*. Er wird mit $\mathrm{div}(q)$ bezeichnet und als formale Summe

$$\mathrm{div}(q) = \sum_\mathfrak{p} \mathrm{ord}_\mathfrak{p}(q) \cdot \mathfrak{p}$$

geschrieben.

Die Menge der Divisoren bildet eine additive freie Gruppe, die wir mit $\mathrm{Div}(R)$ bezeichnen. Sie enthält die Gruppe der Hauptdivisoren als Untergruppe (siehe Aufgabe 24.2), die wir mit H bezeichnen. Da wir im letzten Abschnitt eine Bijektion zwischen effektiven Divisoren und von null verschiedenen Idealen (und von effektiven Hauptdivisoren mit von null verschiedenen Hauptidealen) gestiftet haben, liegt die Frage nahe, welche (Ideal-ähnlichen) Objekte den Divisoren entsprechen. Wir wollen also wissen, durch welche Objekte wir das Fragezeichen im folgenden Diagramm ersetzen müssen.

$$\begin{array}{ccc} \mathrm{Ideale}(R) & \xrightarrow{\sim} & \text{E-Div}(R) \\ \downarrow & & \downarrow \\ ? & \xrightarrow{\sim} & \mathrm{Div}(R) \end{array}$$

Da wir einen Divisor D stets schreiben können als $D = E - F$ mit effektiven Divisoren E und F, liegt die Vermutung nahe, nach etwas wie dem Inversen (bzgl. der Multiplikation) eines Ideals zu suchen.

Definition 24.3. Sei R ein Zahlbereich mit Quotientenkörper $Q(R)$. Dann nennt man einen endlich erzeugten R- Untermodul $\mathfrak{f}$ des R- Moduls $Q(R)$ ein *gebrochenes Ideal*.

Lemma 24.4. *Sei R ein Zahlbereich mit Quotientenkörper $Q(R)$ und sei $\mathfrak{f} \subseteq Q(R)$ eine Teilmenge. Dann sind folgende Aussagen äquivalent.*

(1) *$\mathfrak{f}$ ist ein gebrochenes Ideal.*
(2) *Es gibt ein Ideal $\mathfrak{a}$ und ein Element $r \in R$, $r \neq 0$, so dass $\mathfrak{f} = \mathfrak{a}/r = \{\frac{a}{r} : a \in \mathfrak{a}\}$ gilt.*

Beweis. Sei zunächst $\mathfrak{f}$ ein gebrochenes Ideal. Dann ist

$$\mathfrak{f} = R(\frac{a_1}{r_1}, \ldots, \frac{a_n}{r_n}) .$$

Nach Übergang zu einem Hauptnenner kann man annehmen, dass $r = r_1 = \ldots = r_n$ ist. Dann hat man mit dem Ideal $\mathfrak{a} = (a_1, \ldots, a_n)$ eine Beschreibung der gewünschten Art.

Ist umgekehrt $\mathfrak{f} = \frac{\mathfrak{a}}{r}$, so ist dies natürlich ein endlich erzeugter R-Untermodul von $Q(R)$. □

Wie für Ideale spielen diejenigen gebrochenen Ideale, die von einem Element erzeugt sind, eine besondere Rolle.

Definition 24.5. Sei R ein Zahlbereich mit Quotientenkörper $Q(R)$. Dann nennt man ein gebrochenes Ideal der Form $\mathfrak{f} = Rq$ mit $q \in Q(R)$ ein *gebrochenes Hauptideal*.

Aus Lemma 24.4 ergibt sich sofort, dass für einen Hauptidealbereich jedes gebrochene Ideal ein gebrochenes Hauptideal ist.

Definition 24.6. Sei R ein Zahlbereich mit Quotientenkörper $Q(R)$. Dann definiert man für gebrochene Ideale $\mathfrak{f}$ und $\mathfrak{g}$ das *Produkt* $\mathfrak{f}\cdot\mathfrak{g}$ als den von allen Produkten erzeugten R-Untermodul von $Q(R)$, also

$$\mathfrak{f}\cdot\mathfrak{g} = R\langle gf :\ f\in\mathfrak{f},\, g\in\mathfrak{g}\rangle\,,$$

wobei das Produkt in $Q(R)$ zu nehmen ist.

Wird das gebrochene Ideal $\mathfrak{f}$ als R-Modul von $f_1,\dots,f_n$ erzeugt und wird das gebrochene Ideal $\mathfrak{g}$ von $g_1,\dots,g_m$ erzeugt, so wird das Produkt $\mathfrak{fg}$ von den Produkten f_ig_j, $1\le i\le n, 1\le j\le m$, erzeugt. Also ist das Produkt in der Tat wieder endlich erzeugt und damit ein gebrochenes Ideal. Für Ideale stimmt natürlich das Idealprodukt mit dem hier definierten Produkt von gebrochenen Idealen überein. Das Produkt von gebrochenen Hauptidealen ist wieder ein gebrochenes Hauptideal. Man kann direkt zeigen, oder aber den Bijektionssatz weiter unten benutzen, dass die Menge der von null verschiedenen gebrochenen Ideale eine Gruppe bilden, und die von null verschiedenen gebrochenen Hauptideale darin eine Untergruppe.

Ein gebrochenes Ideal $\mathfrak{f}$ ist ein sogenannter *invertierbarer Modul*. D.h. es ist *lokal isomorph* zum Ring selbst. Mit diesen Formulierungen ist folgendes gemeint: für ein maximales Ideal (also für ein von null verschiedenes Primideal) $\mathfrak{p}$ ist $\mathfrak{f}R_\mathfrak{p} = \mathfrak{f}_\mathfrak{p}$ (dies ist die Lokalisierung eines Moduls an einem Primideal) ein endlich erzeugter $R_\mathfrak{p}$-Modul ($\neq 0$), der zugleich im Quotientenkörper liegt. Solche Moduln sind isomorph zu $R_\mathfrak{p}$. Siehe Aufgabe 24.9.

Definition 24.7. Sei R ein Zahlbereich und

$$D = \sum_\mathfrak{p} n_\mathfrak{p}\cdot\mathfrak{p}$$

ein Divisor (wobei $\mathfrak{p}$ durch die Menge der Primideale $\neq 0$ läuft). Dann nennt man

$$\{f\in Q(R) : \operatorname{div}(f)\ge D\}$$

das *gebrochene Ideal zum Divisor* D. Es wird mit $\mathrm{Id}(D)$ bezeichnet.

Das folgende Lemma zeigt, dass man in der Tat ein gebrochenes Ideal erhält, und dass diese Definition mit der früheren Definition 23.10 verträglich ist.

Lemma 24.8. *Sei R ein Zahlbereich und $D=\sum_\mathfrak{p} n_\mathfrak{p}\cdot\mathfrak{p}$ ein Divisor. Dann ist die Menge $\{f\in Q(R):\operatorname{div}(f)\ge D\}$ ein gebrochenes Ideal. Ist D ein effektiver Divisor, dann ist das so definierte gebrochene Ideal ein Ideal und stimmt mit dem Ideal überein, das einem effektiven Divisor gemäß der Definition Definition 23.10 zugeordnet wird.*

Beweis. Sei $\mathfrak{f} = \{f\in Q(R) : \operatorname{div}(f)\ge D\}$. Gemäß der Konvention, dass $\operatorname{div}(0)=\infty$ zu interpretieren ist, ist $0\in\mathfrak{f}$. Für zwei Elemente $f_1,f_2\in Q(R)$ mit $\operatorname{div}(f_1),\operatorname{div}(f_2)\ge D$ gilt

$$\operatorname{div}(f_1+f_2)\ge\min\{\operatorname{div}(f_1),\operatorname{div}(f_2)\}\ge D$$

und

$$\operatorname{div}(rf) = \operatorname{div}(r) + \operatorname{div}(f) \geq D \text{ für } r \in R\,,$$

da ja $\operatorname{div}(r)$ effektiv ist. Also liegt in der Tat ein R-Modul vor.

Sei nun E ein effektiver Divisor. Wir haben zu zeigen, dass

$$\{f \in Q(R) : \operatorname{div}(f) \geq E\} = \{f \in R : \operatorname{div}(f) \geq E\}$$

ist, wobei die Inklusion $\supseteq$ klar ist. Sei also $f \in Q(R)$ und angenommen, der zugehörige Hauptdivisor $\operatorname{div}(f)$ sei $\geq E$. Dann ist $\operatorname{div}(f)$ insbesondere effektiv. Die Effektivität bedeutet $\operatorname{ord}_{\mathfrak{p}}(f) \geq 0$ für jedes von null verschiedene Primideal $\mathfrak{p}$ und dies bedeutet $f \in R_{\mathfrak{p}}$. Das heißt, dass f zu jedem diskreten Bewertungsring zu jedem maximalen Ideal von R gehört. Dies bedeutet aber nach Bemerkung 22.19, dass $f \in R$ ist. □

Definition 24.9. Sei R ein Zahlbereich und $\mathfrak{f} \neq 0$ ein von null verschiedenes gebrochenes Ideal. Dann nennt man den Divisor

$$\operatorname{div}(\mathfrak{f}) = \sum_{\mathfrak{p}} m_{\mathfrak{p}} \cdot \mathfrak{p}$$

mit

$$m_{\mathfrak{p}} = \min\{\operatorname{ord}_{\mathfrak{p}}(f) :\ f \in \mathfrak{f},\ f \neq 0\}$$

den *Divisor zum gebrochenen Ideal* $\mathfrak{f}$.

Da das gebrochene Ideal $\mathfrak{f}$ nach Definition endlich erzeugt ist, muss man das Minimum nur über eine endliche Menge nehmen. Insbesondere ist der zugehörige Divisor wohldefiniert. Für ein Ideal stimmt diese Definition offensichtlich mit der alten überein.

Lemma 24.10. *Sei R ein Zahlbereich. Dann gelten folgende Aussagen.*

(1) *Sei $\mathfrak{f}$ ein gebrochenes Ideal mit einer Darstellung $\mathfrak{f} = \frac{\mathfrak{a}}{h}$ mit $h \in R$ und einem Ideal $\mathfrak{a} \subseteq R$. Dann ist*

$$\operatorname{div}(\mathfrak{f}) = \operatorname{div}(a) - \operatorname{div}(h)\,.$$

(2) *Zu einem Divisor D gibt es ein $h \in R$ derart, dass $D + \operatorname{div}(h)$ effektiv ist.*

(3) *Zu einem Divisor D mit $E = D + \operatorname{div}(h)$ effektiv ist*

$$\operatorname{Id}(D) = \frac{\operatorname{Id}(E)}{h}\,.$$

Beweis. Siehe Aufgabe 24.10. □

Auch die Einzelheiten des Beweises des folgenden Satzes überlassen wir dem Leser, siehe Aufgabe 24.11.

Satz 24.11. *Sei R ein Zahlbereich. Dann sind die Zuordnungen*

$$\mathfrak{f} \longmapsto \operatorname{div}(\mathfrak{f}) \quad \textit{und} \quad D \longmapsto \operatorname{Id}(D)$$

zueinander inverse Abbildungen zwischen der Menge der von null verschiedenen gebrochenen Ideale und der Menge der Divisoren. Diese Bijektion ist ein Isomorphismus von Gruppen.

Beweis. Wir haben zu zeigen, dass die hintereinandergeschalteten Abbildungen die Identität ergeben. Dies kann man mittels Lemma 24.10 auf den effektiven Fall (Satz 23.11) zurückführen. □

25. Vorlesung

Definition 25.1. Sei R ein Zahlbereich. Es sei $\operatorname{Div}(R)$ die Gruppe der Divisoren und $H \subseteq \operatorname{Div}(R)$ sei die Untergruppe der Hauptdivisoren. Dann nennt man die Restklassengruppe

$$\operatorname{KG}(R) = \operatorname{Div}(R)/H$$

die *Divisorenklassengruppe* von R.

Die Divisorenklassengruppe wird häufig auch als *Idealklassengruppe* oder einfach als *Klassengruppe* bezeichnet. Sie ist kommutativ. Ihre Elemente sind Äquivalenzklassen und werden durch Divisoren repräsentiert, wobei zwei Divisoren genau dann die gleiche Klasse repräsentieren, wenn ihre Differenz ein Hauptdivisor ist. Ein späteres Hauptresultat wird sein, dass die Klassengruppe endlich ist. Sie ist eine wesentliche (ko)-homologische Invariante eines Zahlbereichs und enthält wesentliche Informationen über diesen. Generell lässt sich sagen, dass ihre Größe zum Ausdruck bringt, wie weit ein Zahlbereich von der Faktorialität entfernt ist. Der nächste Satz charakterisiert die Faktorialität dadurch, dass die Klassengruppe trivial ist.

Satz 25.2. *(Charakterisierung von faktoriell) Sei R ein Zahlbereich und es bezeichne $\operatorname{KG}(R)$ die Divisorenklassengruppe von R. Dann sind folgende Aussagen äquivalent.*

(1) *R ist ein Hauptidealbereich.*
(2) *R ist faktoriell.*
(3) *Es ist $\operatorname{KG}(R) = 0$.*

Beweis. Die Implikation (1) $\Rightarrow$ (2) wurde schon (in Lemma 3.7) allgemeiner bewiesen.

(2) $\Rightarrow$ (3). Sei also R faktoriell, und sei $\mathfrak{p}$ ein Primideal $\neq 0$. Sei $f \in \mathfrak{p}$, $f \neq 0$, mit Primfaktorzerlegung $f = p_1 \cdots p_s$. Da $\mathfrak{p}$ ein Primideal ist, muss einer der Primfaktoren zu $\mathfrak{p}$ gehören, sagen wir $p = p_1 \in \mathfrak{p}$. Dann ist $(p) \subseteq \mathfrak{p}$. Das von p erzeugte Ideal ist ein Primideal, und in einem Zahlbereich ist jedes von null verschiedene Primideal maximal (nach Satz 18.13), so dass hier $(p) = \mathfrak{p}$ gelten

muss. Auf der Seite der Divisoren gilt aufgrund des Bijektionssatzes (Satz 23.11) $\operatorname{div}(p) = 1\mathfrak{p}$, so dass ein Hauptdivisor vorliegt. Also sind alle Erzeuger der Divisorengruppe Hauptdivisoren und somit ist überhaupt $\operatorname{Div}(R) = H$ und die Divisorenklassengruppe ist trivial.

(3) $\Rightarrow$ (1). Sei nun $\operatorname{KG}(R) = 0$ vorausgesetzt. Wir zeigen zunächst, dass jedes Primideal $\mathfrak{p} \neq 0$ ein Hauptideal ist. Nach Voraussetzung ist der Divisor $\mathfrak{p}$ ein Hauptdivisor, so dass $\mathfrak{p} = \operatorname{div}(p)$ gilt mit einem $p \in R$. Aufgrund des Bijektionssatzes (Satz 23.11) entspricht dies auf der Idealseite der Gleichung $\mathfrak{p} = (p)$, so dass jedes Primideal ein Hauptideal ist. Für ein beliebiges Ideal $\mathfrak{a} \subseteq R$, $\mathfrak{a} \neq 0$, ist nach Zerlegungssatz (Satz 23.13)

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k} .$$

Dies bedeutet aber, mit $\mathfrak{p}_i = (p_i)$, dass $\mathfrak{a}$ ein Hauptideal ist, das von $p_1^{r_1} \cdots p_k^{r_k}$ erzeugt wird. Also liegt ein Hauptidealbereich vor. □

Wir kennen bereits die euklidischen Bereiche $\mathbb{Z}[i]$ und $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$, die Hauptidealbereiche sind und deren Klassengruppe somit null ist. Der Bereich $\mathbb{Z}[\sqrt{-5}]$ ist hingegen nicht faktoriell und somit kann seine Klassengruppe nicht null sein. Wir werden später sehen, dass die Klassengruppe davon einfach $\mathbb{Z}/(2)$ ist, und wir werden allgemein beweisen, dass die Klassengruppe von quadratischen Zahlbereichen immer eine endliche Gruppe ist. Zunächst charakterisieren wir diejenigen imaginär-quadratischen Zahlbereiche, für die die Norm eine euklidische Funktion ist. Wir werden später Beispiele sehen, wo der Ganzheitsring zwar faktoriell, aber nicht euklidisch ist.

Definition 25.3. Sei $D \neq 0, 1$ quadratfrei und A_D der zugehörige quadratische Zahlbereich. Dann heißt A_D *normeuklidisch*, wenn die Normfunktion auf A_D eine euklidische Funktion ist.

Wir charakterisieren für imaginär-quadratischen Zahlbereiche (also $D < 0$, wann A_D normeuklidisch ist.

Satz 25.4. *(Charakterisierung von normeuklidisch) Sei $D < 0$ quadratfrei und A_D der zugehörige quadratische Zahlbereich. Dann sind folgende Aussagen äquivalent.*

(1) *A_D ist euklidisch.*
(2) *A_D ist normeuklidisch.*
(3) $D = -1, -2, -3, -7, -11$.

Beweis. (1) $\Rightarrow$ (3). Sei A_D euklidisch mit euklidischer Funktion δ. Es sei $z \in A_D$, $z \neq 0$, keine Einheit, so gewählt, dass $\delta(z)$ unter allen Nichteinheiten den minimalen Wert annimmt. Für jedes $w \in A_D$ ist dann

$$w = qz + r \text{ mit } r = 0 \text{ oder } \delta(r) < \delta(z) .$$

Wegen der Wahl von z bedeutet dies $r = 0$ oder r ist eine Einheit. Wir betrachten die Restklassenabbildung

$$\varphi : A_D \longrightarrow A_D/(z)\,.$$

Dabei ist $\varphi(w) = \varphi(r)$. Ab $\mid D \mid \geq 4$ gibt es nur die beiden Einheiten 1 und -1, so dass das Bild von φ überhaupt nur aus $0, 1, -1$ besteht. Also ist nach Satz 21.6

$$N(z) = \mid A_D/(z) \mid \leq 3$$

Bei $D = 2, 3 \mod 4$ hat jedes Element aus A_D die Form $z = a + b\sqrt{D}$ $(a, b \in \mathbb{Z})$ mit Norm $N(z) = a^2 + \mid D \mid b^2$. Damit ist (bei $\mid D \mid \geq 4$) $N(z) \leq 3$ nur bei $b = 0$ und $\mid a \mid = 1$ möglich, doch dann liegt eine Einheit vor, im Widerspruch zur Wahl von z. In diesem Fall verbleiben also nur die Möglichkeiten $D = -1, -2$.

Bei $D = 1 \mod 4$ hat jedes Element aus A_D die Form $z = a + b\frac{1+\sqrt{D}}{2}$ $(a, b \in \mathbb{Z})$ mit Norm $N(z) = (a + \frac{b}{2})^2 + \frac{|D|b^2}{4}$. Damit ist bei $\mid D \mid \geq 12$ die Bedingung $N(z) \leq 3$ wieder nur bei $b = 0$ und $\mid a \mid = 1$ möglich, so dass erneut eine Einheit vorliegt. Es verbleiben die Möglichkeiten $D = -3, -7, -11$.

(3) $\Leftrightarrow$ (2). Der Ganzheitsring A_D ist genau dann normeuklidisch, wenn es zu jedem $f \in \mathbb{Q}[\sqrt{D}]$ ein $z \in A_D$ gibt mit $\mid N(f - z) \mid < 1$. Dies bedeutet anschaulich, dass es zu jedem Punkt der komplexen Ebene stets Gitterpunke aus A_D gibt mit einem Abstand kleiner als eins. Im Fall $D = 2, 3 \mod 4$ ist $A_D = \mathbb{Z}[\sqrt{D}]$ und es liegt ein rechteckiges Gitter vor, wobei der maximale Abstand im Mittelpunkt eines Gitterrechteckes angenommen wird. Der Abstand zu jedem Eckpunkt ist dort $\sqrt{\frac{1}{4} + \frac{|D|}{4}}$, und dies ist nur für $D = -1, -2$ kleiner als eins.

Im Fall $D = 1 \mod 4$ wird die komplexe Ebene überdeckt von kongruenten gleichschenkligen Dreiecken, mit einer Grundseite der Länge eins und Schenkeln der Länge $\frac{1}{2}\sqrt{1 + |D|}$. und deren Eckpunkte jeweils Elemente aus A_D sind. Der Punkt innerhalb eines solchen Dreiecks mit maximalem Abstand zu den Eckpunkten ist der Mittelpunkt des Umkreises, also der Schnittpunkt der Mittelsenkrechten. Wir berechnen ihn für das Dreieck mit den Eckpunkten $(0, 0), (1, 0), (\frac{1}{2}, \frac{\sqrt{|D|}}{2})$. Die Mittelsenkrechte zur Grundseite ist durch $x = \frac{1}{2}$ gegeben, und die Mittelsenkrechte zum linken Schenkel wird durch $(\frac{1}{4}, \frac{\sqrt{|D|}}{4}) + t(\sqrt{\mid D \mid}, -1)$ beschrieben. Gleichsetzen ergibt

$$\frac{1}{4} + t\sqrt{\mid D \mid} = \frac{1}{2} \text{ bzw. } t\sqrt{\mid D \mid} = \frac{1}{4} \text{ und } t = \frac{1}{4\sqrt{\mid D \mid}}\,.$$

Damit ist die zweite Koordinate gleich $\frac{\sqrt{|D|}}{4} - \frac{1}{4\sqrt{|D|}}$ und der gemeinsame Abstand zu den drei Eckpunkten ist die Wurzel aus

$$\frac{1}{4} + \left(\frac{\sqrt{|\,D\,|}}{4} - \frac{1}{4\sqrt{|\,D\,|}}\right)^2 = \frac{1}{4} + \frac{|\,D\,|}{16} + \frac{1}{16\,|\,D\,|} - \frac{1}{8} = \frac{1}{16}(2 + |\,D\,| + \frac{1}{|\,D\,|}).$$

Dies ist kleiner als eins genau dann, wenn $|\,D\,| + \frac{1}{|D|} < 14$ ist, was genau bei $D > -13$ der Fall ist und den Möglichkeiten $D = -3, -7, -11$ entspricht.

(2) $\Rightarrow$ (1) ist trivial. □

Bemerkung 25.5. Für ein vorgegebenes quadratfreies D kann man grundsätzlich effektiv entscheiden, ob der quadratische Zahlbereich A_D faktoriell ist oder nicht. Für $D < 0$ ist dies genau für

$$D = -1, -2, -3, -7, -11, -19, -43, -67, -163$$

der Fall. Es war bereits von Gauß vermutet worden, dass dies alle sind, es wurde aber erst 1967 von Heegner und Stark bewiesen. Man weiß auch, für welche von diesen D der Ganzheitsbereich euklidisch ist, nämlich (wie in 25.4 gezeigt) für $D = -1, -2, -3, -7, -11$, aber nicht für die anderen vier Werte.

Für $D > 0$ wird vermutet, dass für unendlich viele Werte der Ganzheitsbereich faktoriell ist. Für $D < 100$ liegt ein faktorieller Bereich für die Werte

$$D = 2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 23, 29, 31, 33, 37, 38, 41, 43, 46, 47,$$

$$53, 57, 59, 61, 62, 67, 69, 71, 73, 77, 83, 86, 89, 93, 94, 97$$

vor. Dagegen weiß man (Chatland und Davenport 1950), für welche positiven D der Ganzheitsbereich A_D euklidisch ist, nämlich für

$$D = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\,.$$

26. Vorlesung

Hermann Minkowski (1864-1909)

Unser Ziel ist es, zu zeigen, dass die Klassengruppe eines quadratischen Zahlbereichs endlich ist. Zu dem Beweis benötigt man Methoden aus der konvexen Geometrie und einige topologische Begriffe, die im folgenden aufgeführt werden. Man spricht in diesem Zusammenhang von der Geometrie der Zahlen, die mit dem Namen von Minkowski verbunden ist. Der grundlegende Satz ist der Gitterpunktsatz von Minkowski, den wir in diesem Abschnitt vorstellen und beweisen wollen. Im Fall eines quadratischen Zahlbereichs bilden die ganzen Zahlen ein zweidimensionales Gitter, nämlich $\mathbb{Z} \oplus \mathbb{Z}\omega$, das wir in einem zweidimensionalen reellen Vektorraum auffassen werden. Der Gitterpunktsatz macht eine Aussage darüber, dass gewisse Teilmengen mit hinreichend großem Flächeninhalt (oder allgemeiner Volumen) mindestens zwei Gitterpunkte enthalten müssen.

Wir erinnern zunächst an einige Grundbegriffe aus der konvexen Geometrie, der Topologie und der Maßtheorie.

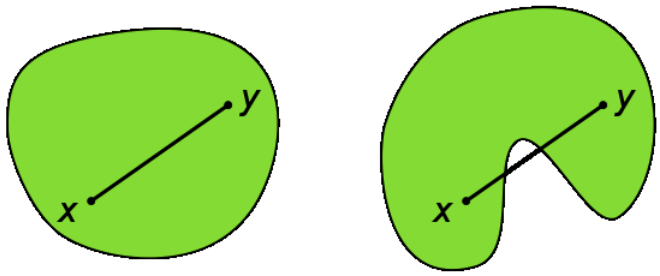
Definition 26.1. Seien $v_1, \ldots, v_n$ linear unabhängige Vektoren im $\mathbb{R}^n$. Dann heißt die Untergruppe $\mathbb{Z}v_1 \oplus \ldots \oplus \mathbb{Z}v_n$ ein *Gitter* im $\mathbb{R}^n$.

Manchmal spricht man auch von einem vollständigen Gitter.

Definition 26.2. Eine Teilmenge $T \subseteq \mathbb{R}^n$ heißt *konvex*, wenn mit je zwei Punkten $P, Q \in T$ auch jeder Punkt der Verbindungsstrecke, also jeder Punkt der Form

$$rP + (1-r)Q \text{ mit } r \in [0,1]\,,$$

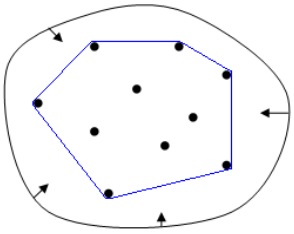
ebenfalls zu T gehört.



Der Durchschnitt von konvexen Teilmengen ist wieder konvex (Aufgabe 26.3). Daher kann man definieren:

Definition 26.3. Zu einer Teilmenge $U \subseteq \mathbb{R}^n$ heißt die kleinste konvexe Teilmenge T, die U umfasst, die *konvexe Hülle* von T.

Die konvexe Hülle ist einfach der Durchschnitt von allen konvexen Teilmengen, die U umfassen.



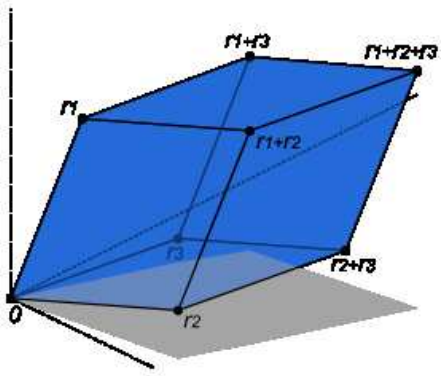
Im zweidimensionalen kann man sich die konvexe Hülle so vorstellen, dass man eine Schnur um die fixierten Punkte aus U legt und die Schnur dann zusammen zieht.

Definition 26.4. Zu einem durch linear unabhängige Vektoren $v_1, \ldots, v_n$ gegebenen Gitter bezeichnet man die konvexe Hülle der Vektoren $e_1v_1 + \ldots + e_nv_n$ mit $e_i \in \{0, 1\}$ als die *Grundmasche* (oder *Fundamentalmasche*) des Gitters.

Die in der vorstehenden Definition auftauchenden Vektoren sind die Eckpunkte des von den Basisvektoren $v_1, \ldots, v_n$ erzeugten Parallelotops. Die Elemente der Grundmasche selbst sind alle Vektoren der Form

$$r_1v_1 + \ldots + r_nv_n \text{ mit } r_i \in [0, 1]$$

Wir werden die Grundmasche häufig mit $\mathfrak{M}$ bezeichnen. Zu einem Gitterpunkt P nennt man die Menge $P+\mathfrak{M}$ eine *Masche* des Gitters. Ein beliebiger Punkt $Q \in \mathbb{R}^n$ hat eine eindeutige Darstellung $Q = t_1v_1+\ldots+t_nv_n$ und damit ist $Q = (\lfloor t_1 \rfloor v_1 + \ldots + \lfloor t_n \rfloor v_n) + ((t_1 - \lfloor t_1 \rfloor)v_1 + \ldots + (t_n - \lfloor t_n \rfloor)v_n)$, wobei der erste Summand zum Gitter gehört und der zweite Summand zur Grundmasche. Insbesondere haben zwei verschiedene Maschen nur Randpunkte, aber keine inneren Punkte gemeinsam.



Definition 26.5. Eine Teilmenge $T \subseteq \mathbb{R}^n$ heißt *zentralsymmetrisch*, wenn mit jedem Punkt $P \in T$ auch der Punkt $-P$ zu T gehört.

Der Begriff der Kompaktheit sollte aus den Anfängervorlesungen bekannt sein.

Definition 26.6. Ein topologischer Raum X heißt *kompakt*, wenn es zu jeder offenen Überdeckung

$$X = \bigcup_{i \in I} U_i \quad \text{mit } U_i \text{ offen und einer beliebigen Indexmenge}$$

eine endliche Teilmenge $J \subseteq I$ gibt derart, dass

$$X = \bigcup_{i \in J} U_i$$

ist.

Für eine Teilmenge im $\mathbb{R}^n$ ist eine Teilmenge T genau dann kompakt, wenn sie abgeschlossen und beschränkt ist.

Die endliche Vereinigung von kompakten Mengen ist kompakt. Abgeschlossene Teilmengen von kompakten Mengen sind wieder kompakt. Zu zwei disjunkten kompakten Mengen X und Y in einem metrischen Raum Z gibt es einen Minimalabstand d. D.h. zu jede zwei Punkten $x \in X$ und $y \in Y$ ist $d(x, y) \geq d$.

Wir stellen einige Grundbegriffe aus der Maßtheorie zusammen.

Nicht jeder Teilmenge des $\mathbb{R}^n$ kann man sinnvollerweise ein Maß zuordnen. In der Maßtheorie werden die sogenannten Borelmengen eingeführt, und diesen Borelmengen kann ein Maß, das sogenannte Borel-Lebesque Maß λ zugeordnet werden. Die Borelmengen umfassen unter anderem alle offenen Mengen, alle abgeschlossenen Mengen (insbesondere alle kompakten Mengen). Borelmengen sind unter abzählbarer Vereinigung und abzählbaren Durchschnitten abgeschlossen, und mit einer Borelmenge ist auch deren Komplement eine Borelmenge.

Das Borel-Lebesque Maß λ hat seine Werte in $\overline{\mathbb{R}}_{\geq 0} = \mathbb{R}_{\geq 0} \cup \{\infty\}$ und ist durch folgende Eigenschaften charakterisiert (der Nachweis der Existenz erfordert einigen Aufwand):

(1) Für einen Quader Q mit den Seitenlängen $s_1, \ldots, s_n$ ist $\lambda(Q) = s_1 \cdot s_2 \cdots s_n$.
(2) Für eine abzählbare Familie von disjunkten Borelmengen T_i, $i \in I$, ist $\lambda(\bigcup_{i \in I} T_i) = \sum_{i \in I} \lambda(T_i)$.
(3) Das Borel-Lebesque Maß λ ist translationsinvariant, d.h. für eine Borelmenge T und einen Vektor $v \in \mathbb{R}^n$ ist auch die um v verschobene Menge $v + T$ eine Borelmenge mit $\lambda(v + T) = \lambda(T)$.

Weitere wichtige Eigenschaften sind:

- Für $U \subseteq T$ ist $\lambda(U) \leq \lambda(T)$.
- Teilmengen, die in einem echten linearen Unterraum des $\mathbb{R}^n$ liegen, haben das Maß 0.
- Ein einzelner Punkt und damit auch jede abzählbare Ansammlung von Punkten hat das Maß 0.

- Unter einer linearen Abbildung $L : \mathbb{R}^n \to \mathbb{R}^n$ verhält sich das Borel-Lebesque Maß so: zu einer Borelmenge T ist auch das Bild $L(T)$ eine Borelmenge mit $\lambda(L(T)) = |\det(L)| \cdot \lambda(T)$.

Eine Basis $v_1, \ldots, v_n$ von $\mathbb{R}^n$ liefert ein Gitter $\Gamma \subset \mathbb{R}^n$ zusammen mit der Grundmasche $\mathfrak{M}$, nämlich das durch die v_i aufgespannte Parallelotop. Dessen Volumen (also dessen Borel-Lebesgue-Maß) wird im Folgenden eine Rolle spielen. Das Volumen berechnet sich wie folgt: man schreibt die Vektoren v_i (die ja jeweils n Einträge haben) als Spalten einer quadratischen $n \times n$-Matrix M. Dann ist

$$\mathrm{Vol}(\mathfrak{M}) = |\det(M)| .$$

Dies folgt aus (bzw. ist äquivalent mit) der oben zitierten Aussage, wie sich das Borel-Lebesgue-Maß unter linearen Abbildung verhält, wenn man sie auf die lineare Abbildung anwendet, die die Einheitsvektoren e_i auf v_i schickt.

Zu einem Gitter $\Gamma \subset \mathbb{R}^n$ gibt es keine eindeutig definierte Gitterbasis und damit auch keine eindeutig definierte Grundmasche. Wenn bspw. v_1, v_2 eine Basis eines zweidimensionalen Gitters bilden, so ist auch $v_1, v_2 + tv_1$ ($t \in \mathbb{Z}$) eine Basis desselben Gitters. Wenn man also von einer Grundmasche eines Gitters spricht, so meint man in Wirklichkeit die Grundmasche zu einer fixierten Basis eines Gitters. Wichtig ist dabei, dass das Volumen einer Grundmasche nur vom Gitter selbst abhängt, nicht aber von der Gitterbasis!

Sei nämlich $w_1, \ldots, w_n$ eine weitere Gitterbasis. Dann gibt es zunächst eine quadratische invertierbare reellwertige Matrix A, die den Basiswechsel beschreibt, also $w = Av$. Da die w_i zum Gitter gehören muss diese Matrix ganzzahlig sein. Aus dem gleichen Grund muss die inverse Matrix ganzzahlig sein. Damit muss die Determinante von $A¿$ aber entweder 1 oder -1 sein. Nach der Formel für das Maß unter linearen Abbildungen haben also die Parallelotope zur Basis v und zur Basis w das gleiche Volumen. Man spricht daher auch vom Volumen (oder Kovolumen) des Gitters.

Satz 26.7. *(Gitterpunktsatz von Minkowski) Sei Γ ein Gitter im $\mathbb{R}^n$ mit Grundmasche $\mathfrak{M}$. Es sei T eine konvexe, kompakte, zentralsymmetrische Teilmenge in $\mathbb{R}^n$, die zusätzlich die Volumenbedingung*

$$\mathrm{Vol}(T) \geq 2^n \,\mathrm{Vol}(\mathfrak{M})$$

erfülle. Dann enthält T mindestens einen von null verschiedenen Gitterpunkt.

Beweis. Wir betrachten das verdoppelte Gitter 2Γ. Ist $v_1, \ldots, v_n$ eine Basis für Γ, so ist $2v_1, \ldots, 2v_n$ eine Basis für 2Γ, und für das Volumen gilt $\mathrm{Vol}(2\Gamma) = 2^n \,\mathrm{Vol}(\Gamma)$. Wir bezeichnen die Grundmasche von 2Γ mit $\mathfrak{N}$. Zu jeder Masche $\mathfrak{N}_Q = Q + \mathfrak{N}$, $Q \in 2\Gamma$, betrachten wir den Durchschnitt $T_Q = T \cap \mathfrak{N}_Q$. Da T kompakt und insbesondere beschränkt ist, gibt es nur endlich viele Maschen derart, dass dieser Durchschnitt nicht leer ist. Seien diese Maschen (bzw. ihre Ausgangspunkte) mit $\mathfrak{N}_i$ (bzw. Q_i), $i \in I$, bezeichnet (da der Nullpunkt aufgrund der Konvexität und der Zentralsymmetrie zu T gehört,

umfasst I zumindest 2^n Elemente). Die in die Grundmasche $\mathfrak{N}$ verschobenen Durchschnitte bezeichnen wir mit

$$\tilde{T_i} := T_i - Q_i \,.$$

Wir behaupten zunächst, dass die $\tilde{T_i}$ nicht paarweise disjunkt sind. Sei also angenommen, sie wären paarweise disjunkt. Mindestens eines der T_i hat positives Volumen, sagen wir für $i = 1$. Wegen der angenommenen Disjunktheit sind insbesondere

$$X := \tilde{T_1} \text{ und } Y := \bigcup_{i \in I, i \neq 1} \tilde{T_i}$$

disjunkt zueinander. Wir haben also zwei disjunkte kompakte Teilmengen, und diese besitzen einen Minimalabstand d (d.h. zu jedem Punkt aus X liegen in einer d-Umgebung keine Punkte aus Y).

Sei $x \in X$ ein innerer Punkt (den es gibt, da X positives Volumen besitzt) und sei $y \in Y$. Mit S sei die Verbindungstrecke von x nach y bezeichnet, die ganz in $\mathfrak{N}$ verläuft. Wir wählen einen Punkt $s \in S$, der weder zu Xnoch zu Y gehört (solche Punkte gibt es wegen des Minimalabstandes). Da s sowohl zu X als auch zu Y einen Minimalabstand besitzt, gibt es eine ϵ-Umgebung B von s, die disjunkt zu X und Y ist. Wir können ferner annehmen, dass B ganz innerhalb von $\mathfrak{N}$ liegt (wegen der Wahl von x). Als eine Ballumgebung hat B ein positives Volumen, was zu folgendem Widerpruch führt.

$$\begin{aligned}
\mathrm{Vol}(\mathfrak{N}) &\geq \mathrm{Vol}(X \cup Y \cup B) \\
&= \mathrm{Vol}(\bigcup_{i \in I} \tilde{T_i}) + \mathrm{Vol}(B) \\
&> \sum_{i \in I} \mathrm{Vol}(\tilde{T_i}) \\
&= \sum_{i \in I} \mathrm{Vol}(T_i) \\
&= \mathrm{Vol}(T) \\
&\geq 2^n \,\mathrm{Vol}(\mathfrak{M}) \\
&= \mathrm{Vol}(\mathfrak{N}).
\end{aligned}$$

Es gibt also Indizes $i \neq j$ und einen Punkt $z \in \tilde{T_i} \cap \tilde{T_j}$ (z muss selbst nicht zu T gehören). Sei

$$z_i := z + Q_i \in T_i \text{ und } z_j := z + Q_j \in T_j \,.$$

Wegen $Q_i, Q_j \in 2\Gamma$ ist auch $Q_i - Q_j \in 2\Gamma$ und daher

$$0 \neq \frac{Q_i - Q_j}{2} \in \Gamma \,.$$

Aus $z_i \in T$ folgt (wegen der Zentralsymmetrie) auch $-z_i \in T$ und wegen der Konvexität von T ergibt sich

$$\begin{aligned}
\frac{Q_i - Q_j}{2} &= \frac{1}{2}(z - z_i) - \frac{1}{2}(z - z_j) \\
&= -\frac{1}{2} z_i + \frac{1}{2} z_j
\end{aligned}$$

$$\in \quad T.$$

Wir haben also einen von null verschiedenen Gitterpunkt in T gefunden. $\square$

27. Vorlesung

Wir beweisen nun die Endlichkeit der Klassenzahl für die Ganzheitsringe in quadratischen Zahlkörpern. Es sei bemerkt, dass diese Aussage für alle Zahlbereiche gilt, nicht nur für die quadratischen, wir beschränken uns aber auf diese. Wir folgen hier weitgehend dem Skript von Bruns (siehe Literaturliste).

Lemma 27.1. *Sei R ein quadratischer Zahlbereich. Dann gibt es nur endlich viele Ideale $\mathfrak{a}$ in R, deren Norm unterhalb einer gewissen Zahl liegt.*

Beweis. Es genügt zu zeigen, dass es zu einer natürlichen Zahl n nur endlich viele Ideale $\mathfrak{a}$ in R mit $N(\mathfrak{a}) = n$ gibt. Sei also $\mathfrak{a}$ ein solches Ideal. Dann ist $n \in \mathfrak{a}$ nach Korollar 21.4 und damit entspricht $\mathfrak{a}$ einem Ideal aus R/n. Dieser Ring ist aber nach Lemma 18.12 endlich und besitzt somit überhaupt nur endlich viele Ideale. $\square$

Bemerkung 27.2. Sei D quadratfrei und A_D der zugehörige quadratische Zahlbereich mit Diskriminante $\triangle$. Wir wollen ein von null verschiedenes Ideal $\mathfrak{a}$ aus A_D als ein Gitter $\Gamma_{\mathfrak{a}}$ vom Rang zwei in $\mathbb{R}^2$ auffassen. Bei $D < 0$, also im imaginär-quadratischen Fall, verwenden wir die Einbettung

$$\mathfrak{a} \subseteq A_D \subset L = \mathbb{Q}[\sqrt{D}] \subset \mathbb{C} \cong \mathbb{R}^2 .$$

Wir identifizieren also das Ideal mit seinem Bild unter diesen Inklusionen. Dem Element $q_1 + q_2\sqrt{D}$ entspricht in der reellen Ebene das Element

$$(q_1, q_2\sqrt{-D}) = (q_1, q_2\sqrt{|\,D\,|}) .$$

Bei $D > 0$, also im reell-quadratischen Fall, verwenden wir stattdessen die Einbettung

$$L = \mathbb{Q}[\sqrt{D}] \longrightarrow \mathbb{R}^2,\ q_1 + q_2\sqrt{D} \longmapsto (q_1, q_2\sqrt{D}).$$

Man beachte, dass in der zweiten Komponente die Wurzel $\sqrt{D}$ mitgeschleppt wird, und dass diese Abbildung lediglich eine $\mathbb{Q}$-lineare Abbildung ist, während im imaginär-quadratischen Fall ein Ringhomomorphismus vorliegt.

Das Ideal $\mathfrak{a}$ sei nun (bei positivem oder negativem D) durch die $\mathbb{Z}$-Basis (a, b) erzeugt, mit $(a) = \mathbb{Z} \cap \mathfrak{a}$ und $b = \alpha + \beta u$ wie in Satz 21.1 beschrieben. Hierbei sei $1, u$ die übliche $\mathbb{Z}$-Basis von A_D, also $u = \sqrt{D}$ bzw. $u = \frac{1+\sqrt{D}}{2}$. Das Basiselement u wird auf $(0, \sqrt{|\,D\,|})$ bzw. auf $(\frac{1}{2}, \frac{\sqrt{|D|}}{2})$ geschickt. Daher wird das zum Ideal gehörige Gitter $\Gamma_{\mathfrak{a}}$ (in $\mathbb{R}^2$) aufgespannt durch

$$(a, 0) \text{ und } (\alpha, \beta\sqrt{|\,D\,|}) \text{ bei } D = 2, 3 \mod 4$$

und

$$(a,0) \text{ und } (\alpha + \frac{\beta}{2}, \beta\frac{\sqrt{|\,D\,|}}{2}) \text{ bei } D = 1 \mod 4\,.$$

Wir setzen zunächst die Norm des Ideals mit dem Flächeninhalt des Gitters in Verbindung.

Lemma 27.3. *Sei D eine quadratfreie Zahl, sei A_D der zugehörige quadratische Zahlbereich und sei $\varphi : A_D \to \mathbb{R}^2$ die in Bemerkung 27.2 beschriebene Einbettung. Es sei $\mathfrak{a} \neq 0$ ein Ideal und $\Gamma_\mathfrak{a} \subset \mathbb{R}^2$ das zugehörige Gitter. Dann ist der Flächeninhalt der Grundmasche des Gitters gleich*

$$\mu(\Gamma_\mathfrak{a}) = \frac{1}{2}\sqrt{|\triangle|}N(\mathfrak{a})\,.$$

Beweis. Das Ideal $\mathfrak{a}$ sei erzeugt durch die $\mathbb{Z}$-Basis (a,b) mit $(a) = \mathbb{Z} \cap \mathfrak{a}$ und $b = \alpha + \beta u$ wie in Satz 21.1 beschrieben. In Bemerkung 27.2 wurde die zugehörige Gitterbasis ausgerechnet. Der Flächeninhalt eines Gitters wird gegeben durch den Betrag der Determinante von zwei Basiselementen des Gitters. Daher ist bei $D = 2, 3 \mod 4$

$$\mu(\Gamma_\mathfrak{a}) = |\det\begin{pmatrix} a & \alpha \\ 0 & \beta\sqrt{|D|}\end{pmatrix}| = a\beta\sqrt{|D|} = a\beta\frac{\sqrt{|\triangle|}}{2} = \frac{1}{2}N(\mathfrak{a})\sqrt{|\triangle|}\,,$$

wobei wir Korollar 21.4 und die Diskriminantengleichung (Lemma 20.10) $\triangle = 4D$ benutzt haben.

Bei $D = 1 \mod 4$ ist

$$\mu(\Gamma_\mathfrak{a}) = |\det\begin{pmatrix} a & \alpha + \frac{\beta}{2} \\ 0 & \frac{\beta\sqrt{|D|}}{2}\end{pmatrix}| = \frac{a\beta\sqrt{|D|}}{2} = \frac{1}{2}N(\mathfrak{a})\sqrt{|\triangle|}$$

aus den gleichen Gründen. □

Lemma 27.4. *Sei D eine quadratfreie Zahl, sei A_D der zugehörige quadratische Zahlbereich mit Diskriminante $\triangle$. Es sei $\mathfrak{a} \neq 0$ ein Ideal. Dann gibt es ein $f \in \mathfrak{a}$, $f \neq 0$, mit der Eigenschaft*

$$|N(f)| \leq \begin{cases} \frac{2}{\pi}\sqrt{|\triangle|}N(\mathfrak{a}) & \text{bei } D < 0 \\ \frac{1}{2}\sqrt{|\triangle|}N(\mathfrak{a}) & \text{bei } D > 0\,. \end{cases}$$

Beweis. Wir wollen den Gitterpunktsatz von Minkowski (Satz 26.7) auf das Gitter $\Gamma = \Gamma_\mathfrak{a}$ anwenden, das in Bemerkung 27.2 konstruiert wurde. Nach Lemma 27.3 hat die Grundmasche des Gitters den Flächeninhalt $\frac{\sqrt{|\triangle|}N(\mathfrak{a})}{2}$. Sei $D < 0$. Als Menge K betrachten wir den Kreis um den Nullpunkt mit Radius $\sqrt{\frac{2}{\pi}\sqrt{|\triangle|}N(\mathfrak{a})}$. Der Kreis ist kompakt, zentralsymmetrisch und konvex, und sein Flächeninhalt ist bekanntlich $2\sqrt{|\triangle|}N(\mathfrak{a})$. Dies ist so groß wie das Vierfache des Flächeninhalts der Grundmasche des Gitters. Also gibt es

einen von null verschiedenen Gitterpunkt $x \in \Gamma \cap K$, und $x = \varphi(f)$ mit $f \in \mathfrak{a}$. Die Norm von f (also das Quadrat des komplexen Betrags) ist dann $N(f) \leq \frac{2}{\pi}\sqrt{|\triangle|}N(\mathfrak{a})$, wie behauptet.

Sei nun $D > 0$. Für einen Punkt $x = (x_1, x_2) = (y_1, y_2\sqrt{D})$ (mit $y_1, y_2 \in \mathbb{Q}$) besitzt das Element $y = \varphi^{-1}(x)$ (aus $Q(A_D)$) die Norm

$$N(y) = y_1^2 - y_2^2 D = (x_1 - x_2)(x_1 + x_2)\,.$$

Die Bedingung $|N(y)| = |(x_1 - x_2)(x_1 + x_2)| = c$ beschreibt also in jedem Quadranten eine gedrehte Hyperbel. Diese Hyperbeln schließen das (konvexe, kompakte, zentralsymmetrische) Quadrat mit den Eckpunkten $(\pm\sqrt{c}, \pm\sqrt{c})$ ein. Wir setzen $c = \frac{1}{2}\sqrt{|\triangle|}N(\mathfrak{a})$. Dann hat das Quadrat K mit diesen Eckpunkten den Flächeninhalt $2\sqrt{|\triangle|}N(\mathfrak{a})$ und enthält nach dem Gitterpunktsatz von Minkowski (Satz 26.7) einen von null verschiedenen Gitterpunkt $x \in \Gamma_{\mathfrak{a}} \cap K$. Dieser entspricht einem Element $f \in \mathfrak{a}$, $f \neq 0$, und

$$|N(f)| = x_1^2 - x_2^2 \leq x_1^2 \leq c = \frac{1}{2}\sqrt{|\triangle|}N(\mathfrak{a})\,.$$

□

Lemma 27.5. *Sei D eine quadratfreie Zahl und sei A_D der zugehörige quadratische Zahlbereich mit Diskriminante $\triangle$. Dann enthält jede Idealklasse aus der Klassengruppe ein Ideal $\mathfrak{a} \subseteq A_D$, das die Normschranke*

$$N(\mathfrak{a}) \leq \begin{cases} \frac{2\sqrt{|\triangle|}}{\pi} & \text{bei } D < 0 \\ \frac{\sqrt{|\triangle|}}{2} & \text{bei } D > 0\,. \end{cases}$$

erfüllt.

Beweis. Sei c eine Idealklasse. Die inverse Klasse c^{-1} wird repräsentiert durch ein Ideal $\mathfrak{b} \subseteq R$ (Lemma 24.4). Nach Lemma 27.4 enthält $\mathfrak{b}$ ein Element f, $f \neq 0$, mit

$$|N(f)| \leq \begin{cases} \frac{2}{\pi}\sqrt{|\triangle|}N(\mathfrak{b}) & \text{bei } D < 0 \\ \frac{1}{2}\sqrt{|\triangle|}N(\mathfrak{b}) & \text{bei } D > 0\,. \end{cases}$$

Wir setzen $\mathfrak{a} = (f)\mathfrak{b}^{-1}$. Dies ist ein Ideal, da ja $\mathfrak{b}^{-1}$ alle Elemente aus $\mathfrak{b}$ nach R multipliziert (Aufgabe 25.1). Nach Korollar 21.8 und nach Satz 21.6 ist

$$N(\mathfrak{a})N(\mathfrak{b}) = N(\mathfrak{a}\mathfrak{b}) = N((f)) = |N(f)|\,.$$

Daher ist

$$N(\mathfrak{a}) = N(f\mathfrak{b}^{-1}) = \frac{|N(f)|}{N(\mathfrak{b})} \leq \begin{cases} \frac{2}{\pi}\sqrt{|\triangle|} & \text{bei } D < 0 \\ \frac{1}{2}\sqrt{|\triangle|} & \text{bei } D > 0\,. \end{cases}$$

□

Satz 27.6. *(Endlichkeit der Klassenzahl) Sei $R = A_D$ ein quadratischer Zahlbereich. Dann ist die Klassengruppe von R eine endliche Gruppe.*

Beweis. Nach Lemma 27.5 wird jede Klasse in der Klassengruppe repräsentiert durch ein Ideal mit einer Norm, die durch die dort angegebene Schranke beschränkt ist. D.h., dass die Ideale mit Norm unterhalb dieser Schranke alle Klassen repräsentieren. Nach Lemma 27.1 gibt es aber überhaupt nur endlich viele Ideale mit Norm unterhalb einer gegebenen Schranke. □

Das im Beweis verwendete Lemma bietet prinzipiell eine Abschätzung für die Anzahl der Klassengruppe.

Definition 27.7. Sei A_D ein quadratischer Zahlbereich. Dann nennt man die Anzahl der Elemente in der Klassengruppe von A_D die *Klassenzahl* von A_D.

Korollar 27.8. *Sei $R = A_D$ ein quadratischer Zahlbereich und sei $\mathfrak{a}$ ein Ideal in R. Dann gibt es ein $n \geq 1$ derart, dass $\mathfrak{a}^n$ ein Hauptideal ist.*

Beweis. Für das Nullideal ist die Aussage richtig, sei also $\mathfrak{a}$ von null verschieden. Die zugehörige Idealklasse $[\mathfrak{a}]$ besitzt aufgrund von Satz 27.6 in der Idealklassengruppe endliche Ordnung, d.h., dass für ein $n \geq 1$

$$[\mathfrak{a}]^n = [\mathfrak{a}^n] = 0$$

ist. Dies bedeutet aber gerade, dass $\mathfrak{a}^n$ ein Hauptideal ist. □

Wir formulieren noch explizit die beiden folgenden Kriterien für Faktorialität.

Korollar 27.9. *Sei D eine quadratfreie Zahl und sei A_D der zugehörige quadratische Zahlbereich mit Diskriminante $\triangle$. Es sei vorausgesetzt, dass jedes Primideal $\mathfrak{p}$ in A_D mit der Normbedingung*

$$N(\mathfrak{p}) \leq \begin{cases} \frac{2\sqrt{|\triangle|}}{\pi} & \text{bei } D < 0 \\ \frac{\sqrt{|\triangle|}}{2} & \text{bei } D > 0\,. \end{cases}$$

ein Hauptideal sei. Dann ist A_D faktoriell.

Beweis. Es sei $\mathfrak{a}$ ein Ideal $\neq 0$ unterhalb der angegebenen Normschranke. Nach dem Satz von Dedekind 23.6 ist $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_k$ mit Primidealen $\mathfrak{p}_i$, und wegen der Multiplikativität der Norm (Korollar 21.8) sind die Normen dieser Primideale ebenfalls unter der Schranke. Da all diese Primideale nach Voraussetzung Hauptideale sind, ist auch $\mathfrak{a}$ ein Hauptideal. Da nach Lemma 27.5 jede Idealklasse durch ein Ideal unterhalb der Normschranke repräsentiert wird, bedeutet dies, dass jede Idealklasse durch ein Hauptideal repräsentiert wird. Das heißt die Klassengruppe ist trivial und damit ist nach Satz 25.2 der Ring A_D faktoriell. □

Korollar 27.10. *Sei D eine quadratfreie Zahl und sei A_D der zugehörige quadratische Zahlbereich mit Diskriminante $\triangle$. Es sei vorausgesetzt, dass*

jede Primzahl p mit

$$p \leq \begin{cases} \frac{2\sqrt{|\triangle|}}{\pi} & \text{bei } D < 0 \\ \frac{\sqrt{|\triangle|}}{2} & \text{bei } D > 0\,. \end{cases}$$

in A_D eine Primfaktorzerlegung besitzt. Dann ist A_D faktoriell.

Beweis. Es sei $\mathfrak{p}$ ein Primideal derart, dass $N(\mathfrak{p})$ unterhalb der angegebenen Schranke liegt, und es sei $\mathbb{Z}p = (\mathfrak{p}) \cap \mathbb{Z}$ mit einer Primzahl p. Nach Satz 20.13 gibt es die drei Möglichkeiten

$$p = \mathfrak{p} \text{ oder } p = \mathfrak{p}^2 \text{ oder } p = \mathfrak{p}\overline{\mathfrak{p}}\,.$$

Die Norm von $\mathfrak{p}$ ist p oder p^2, so dass auch p unterhalb der Schranke ist und somit nach Voraussetzung eine Primfaktorzerlegung für p besteht. Daraus folgt aber, dass $\mathfrak{p}$ ein Hauptideal ist. Aus Korollar 27.9 folgt die Behauptung. □

Beispiel 27.11. Sei $R = \mathbb{Z}[\sqrt{-5}]$, also $D = -5$ und $\triangle = -20$. Jede Idealklasse enthält ein Ideal $\mathfrak{a}$ der Norm $N(\mathfrak{a}) \leq \frac{2\sqrt{20}}{\pi}$, so dass nur Ideale mit Norm 2 zu betrachten sind. Ein Ideal $\mathfrak{a}$ mit $N(\mathfrak{a}) = 2$ ist ein Primideal $\mathfrak{p}$ mit $\mathfrak{p} \cap \mathbb{Z} = (2)$. Daher ist

$$\mathfrak{p} = (2, 1 + \sqrt{-5}) = (2, 1 - \sqrt{-5})$$

die einzige Möglichkeit. Insbesondere ist $\mathfrak{p}^2 = (2)$ und $\mathfrak{p}$ ist kein Hauptideal. Daher ist die Idealklassengruppe isomorph zu $\mathbb{Z}/(2)$, wobei das Nullelement durch die Hauptdivisoren (oder Hauptideale) repräsentiert werden und das andere Element durch $\mathfrak{p}$.

Beispiel 27.12. Sei $R = A_{-19}$ der quadratische Zahlbereich zu $D = -19$, also $A_{-19} = \mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ bzw.

$$A_{-19} \cong \mathbb{Z}[Y]/(Y^2 - Y + 5)\,.$$

Wir wissen aufgrund von Satz 25.4, dass R nicht euklidisch ist. Dennoch ist R faktoriell und damit (Satz 25.2) ein Hauptidealbereich und die Klassengruppe ist trivial. Hierfür benutzen wir Korollar 27.10, d.h. wir haben für alle Primzahlen $p \leq \frac{2\sqrt{|\triangle|}}{\pi}$ zu zeigen, dass sie eine Primfaktorzerlegung in R besitzen. Diese Abschätzung wird nur von $p = 2$ erfüllt. Für $p = 2$ ist der Restklassenring

$$R/(2) \cong \mathbb{Z}/(2)[Y]/(Y^2 + Y + 1)$$

ein Körper, so dass 2 träge in R ist und insbesondere eine Primfaktorzerlegung besitzt.

Anhang 1: Bildlizenzen

Die Bilder dieses Textes stammen aus Commons (also http://commons.wikimedia.org), und stehen unter unterschiedlichen Lizenzen, die zwar alle die Verwendung hier erlauben, aber unterschiedliche Bedingungen an die Verwendung und Weitergabe stellen. Es folgt eine Auflistung der verwendeten Bilder dieses Textes (nach der Seitenzahl geordnet, von links nach rechts, von oben nach unten) zusammen mit ihren Quellen, Urhebern (Autoren) und Lizenzen. Dabei ist *Quelle* so zu verstehen, dass sich, wenn man

http://commons.wikimedia.org/wiki/File:

unmittelbar davor setzt, die entsprechende Datei auf Commons ergibt. *Autor* benennt den Urheber des Werkes, falls dieser bekannt ist. *Benutzer* meint den Hochlader der Datei; wenn keine weitere Information über den Autor vorliegt, so gilt der Benutzer als Urheber. Die Angabe des Benutzernamen ist so zu verstehen, dass sich, wenn man

http://commons.wikimedia.org/wiki/User:

unmittelbar davor setzt, die Benutzerseite ergibt. Wenn das Bild ursprünglich in einem anderen Wikimedia-Projekt hochgeladen wurde, so wird die Domäne (bspw. *de.wikipedia.org*) explizit angegeben.

Die *Lizenz* ist die auf der Dateiseite auf Commons angegebene Lizenz. Dabei bedeuten

- GFDL: Gnu Free Documentation License (siehe den angehängten Text, falls diese Lizenz vorkommt)
- CC-BY-SA-2.5 (3.0): Creative Commons Attribution ShareAlike 2.5 (oder 3.0)
- PD: gemeinfrei (public domain)

Abbildungsverzeichnis

Quelle = Gaussian integer lattice.png, Autor = Gunther (= Benutzer Gunther auf Commons), Lizenz = CC-by-sa 3.0 8

Quelle = Ferdinand Gotthold Max Eisenstein.jpg , Autor = Benutzer Poulos auf fr-wikipedia.org, Lizenz = PD 10

Quelle = Eisenstein integer lattice.png , Autor = Gunther (= Benutzer Gunther auf Commons), Lizenz = CC-by-sa 3.0 10

Quelle = Euklid-von-Alexandria 1.jpg , Autor = Benutzer Luestling auf Commons, Lizenz = PD 12

Quelle = Anillo cíclico.png , Autor = Romero Schmidtke (= Benutzer FrancoGG auf es.wikipedia.org), Lizenz = CC-by-sa 3.0 16

Quelle = Leonhard Euler by Handmann .png, Autor = Emanuel Handmann (= Benutzer QWerk auf Commons), Lizenz = PD 17

Quelle = Joseph-Louis Lagrange.jpeg, Autor = Benutzer Katpatuka auf Commons, Lizenz = PD 17

Quelle = Pierre de Fermat.jpg, Autor = Benutzer Magnus Manske auf en.wikipedia.org, Lizenz = PD 18

Quelle = Tablero producto anillos cíclicos 2.png, Autor = Romero Schmidtke (= Benutzer FrancoGG auf es.wikipedia.org), Lizenz = CC-by-sa 3.0 20

Quelle = Carl Friedrich Gauss.jpg, Autor = Benutzer Bcrowell auf Commons, Lizenz = PD 31

Quelle = Carl Jacobi.jpg, Autor = Benutzer Stern auf Commons, Lizenz = PD 38

Quelle = Kapitolinischer Pythagoras adjusted.jpg, Autor = Galilea (= Benutzer Skies auf de.wikipedia.org), Lizenz = CC-by-sa 3.0 42

Quelle = Pell right triangles.svg, Autor = David Eppstein, Lizenz = PD 42

Quelle = Ternas pitagoricas.png, Autor = Arkady (= Benutzer Kordas auf es.wikipedia.org), Lizenz = CC-by-sa 3.0 43

Quelle = Andrew wiles1-3.jpg, Autor = C. J. Mozzochi, Princeton N.J (= Benutzer Nyks auf Commons), Lizenz = copyright C. J. Mozzochi, Princeton N.J, http://www.mozzochi.org/deligne60/Deligne1/DSC0024.jpg 47

Quelle = Georg Friedrich Bernhard Riemann.jpeg, Autor = Benutzer Ævar Arnfjörð Bjarmason auf Commons, Lizenz = PD 48

Quelle = Zeta.png, Autor = Benutzer Anarkman auf Commons, Lizenz = CC-by-sa 3.0 49

Quelle = Hadamard2.jpg, Autor = Benutzer Gian- auf en.wikipedia.org, Lizenz = PD 52

Quelle = De La Vallée Poussin.jpg, Autor = Benutzer Sonuwe auf Commons, Lizenz = PD 52

Quelle = PrimeNumberTheorem.png, Autor = FredStober, Lizenz = PD 53

Quelle = Peter Gustav Lejeune Dirichlet.jpg, Autor = Benutzer Magnus Manske auf Commons, Lizenz = PD 53

Quelle = Chebyshev.jpg, Autor = Benutzer VindicatoR auf pl.wikipedia.org, Lizenz = PD 54

Quelle = Bertrand.jpg, Autor = Benutzer Wladyslaw Sojka auf Commons, Lizenz = PD 58

Quelle = Marin Mersenne.jpeg, Autor = Benutzer Maksim auf Commons, Lizenz = PD 58

Quelle = 20010219-001-01.jpg, Autor = Benutzer FunkMonk auf Commons, Lizenz = PD 62

Quelle = Pentagon construct.gif, Autor = TokyoJunkie (= Benutzer Mosmas auf PD), Lizenz = en.wikipedia.org 64

Quelle = Carl Louis Ferdinand von Lindemann.jpg, Autor = Benutzer JdH auf Commons, Lizenz = PD 69

Quelle = Noether.jpg, Autor = Benutzer Anarkman auf PD, Lizenz = 84

Quelle = Dedekind.jpeg, Autor = Jean-Luc W, Lizenz = PD 85

Quelle = Dedekind stamp.jpg, Autor = Deutsche Post der DDR (= Benutzer Le Corbeau auf PD), Lizenz = 109

Quelle = Hermann Minkowski 2.jpg , Autor = Feitscherg, Lizenz = PD 118

Quelle = Convex set.svg , Autor = Oleg Alexandrov, Lizenz = PD 118

Quelle = Non Convex set.svg , Autor = Kilom691, Lizenz = CC-by-sa 3.0 118

Quelle = ConvexHull.png , Autor = Benutzer Maksim auf Commons, Lizenz = PD 119

Quelle = Determinant parallelepiped.svg, Autor = Claudio Rocchini, Lizenz = CC-by-sa 3.0 119