Zahlentheorie

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

Sommersemester 2025

1. Vorlesung - Teilbarkeit in kommutativen Ringen

´

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

$$0 = 0 + 0$$

$$1 = 1 + 0$$

$$2 = 1 + 1$$

$$3$$

$$4 = 4 + 0$$

$$5 = 4 + 1$$

$$6$$

$$7$$

$$8 = 4 + 4$$

$$9 = 9 + 0$$

$$10 = 9 + 1$$

$$11$$

$$12$$

$$13 = 9 + 4$$

$$14$$

$$15$$

$$\begin{aligned} 16 &= 16+0 \\ 17 &= 16+1 \\ 18 &= 9+9 \end{aligned}$$

$$19$$

$$20 = 16+4$$

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 Zahlen der ersten Reihe alle den Rest 3 bei Division durch 4 haben, und die Zahlen der zweiten Reihe (von 2 abgesehen) den Rest 1. Hier zeigt sich bereits, dass es sinnvoll ist, zu anderen Ringen überzugehen, um Fragen über natürliche oder ganze Zahlen zu beantworten. Die Restabbildung zur *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

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

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 Summen von zwei 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 notwendig 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*

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

(einem Unterring der komplexen Zahlen). Dort können wir

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

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

Die Frage nach den Summen von zwei Quadraten werden wir abschließend in Satz 9.10 beantworten.

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 $a \cdot b$.

Oben hatten wir im Zusammenhang mit der Abbildung $\mathbb{Z} \to \mathbb{Z}/(4)$ den Begriff Ringhomomorphismus erwähnt, den wir hier kurz anführen.

Definition 1.4. Es seien R und S Ringe. Eine Abbildung

$$\varphi\colon R \longrightarrow S$$

heißt *Ringhomomorphismus* , wenn folgende Eigenschaften gelten:

(1) $\varphi(a + b) = \varphi(a) + \varphi(b)$.
(2) $\varphi(1) = 1$.
(3) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Teilbarkeitsbegriffe

Definition 1.5. Es 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 $c \in R$ derart gibt, dass $b = c \cdot a$ ist. Man schreibt dafür auch $a|b$.

Lemma 1.6. *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 1.21. □

Definition 1.7. Ein Element u in einem kommutativen Ring R heißt *Einheit*, wenn es ein Element $v \in R$ mit $uv = 1$ gibt.

Bemerkung 1.8. 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 (bezüglich 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 bestimmen. Es ist $\mathbb{Z}^\times = \{1, -1\}$ und $(\mathbb{Z}/(4))^\times = \{1, 3\}$. Im Ring der Gaußschen Zahlen gibt es vier Einheiten: $1, -1, \mathrm{i}, -\mathrm{i}$, siehe die nächste Vorlesung.

Definition 1.9. Zwei Elemente a und b eines kommutativen Ringes R heißen *assoziiert*, wenn es eine Einheit $u \in R$ derart gibt, dass $a = ub$ ist.

Bemerkung 1.10. Die Assoziiertheit ist eine Äquivalenzrelation. Siehe Aufgabe 1.4.

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

Lemma 1.11. *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 1.22. □

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

Definition 1.12. 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 1.13. Eine Nichteinheit $p \neq 0$ in einem kommutativen Ring R heißt *prim* (oder ein *Primelement*), wenn folgendes gilt: Teilt p ein Produkt ab mit $a, b \in R$, so teilt p 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.

Integritätsbereiche

Vor dem nächsten Lemma erinnern wir an den Begriff des Integritätsbereiches. Häufig wird die Teilbarkeitstheorie nur für Integritätsbereiche entwickelt.

Definition 1.14. Ein kommutativer, nullteilerfreier, von 0 verschiedener Ring heißt *Integritätsbereich*.

Ein *Nullteiler* ist ein Element x mit der Eigenschaft, dass es ein von 0 verschiedenes Element y mit $xy = 0$ gibt. Die Null ist in einem vom Nullring verschieden Ring stets ein Nullteiler. *Nullteilerfrei* bedeutet, dass die 0 der einzige Nullteiler ist bzw. dass alle von 0 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 1.15. 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 0 verschiedenen Elemente Einheiten (und insbesondere Nichtnullteiler). Körper sind also insbesondere Integritätsbereiche. In einem Körper ist die Teilbarkeitsbeziehung uninteressant, da jedes von 0 verschiedene Element jedes andere Element teilt.

Lemma 1.16. *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 $1 = sb$, sodass also b eine Einheit ist. □

1. Arbeitsblatt

Übungsaufgaben

Aufgabe 1.1. Finde die kleinste natürliche Zahl, die sich auf mehrfache Weise als Summe von zwei Quadratzahlen darstellen lässt.

Aufgabe 1.2. Es seien x und y natürliche Zahlen, die man beide als eine Summe von zwei Quadratzahlen darstellen kann. Zeige, dass man auch das Produkt xy als Summe von zwei Quadratzahlen darstellen kann.

Aufgabe 1.3. Finde zwei natürliche Zahlen, deren Summe 65 und deren Produkt 1000 ist.

Aufgabe 1.4. Zeige, dass die Assoziiertheit in einem kommutativen Ring eine Äquivalenzrelation ist.

Aufgabe 1.5. Zeige, dass in einem kommutativen Ring R folgende Teilbarkeitsbeziehungen gelten.

(1) Sind a und b assoziiert, so gilt $a|c$ genau dann, wenn $b|c$.
(2) Ist R ein Integritätsbereich, so gilt hiervon auch die Umkehrung.

Aufgabe 1.6. Es sei R ein kommutativer Ring und seien f, g Nichtnullteiler in R. Zeige, dass das Produkt fg ebenfalls ein Nichtnullteiler ist.

Aufgabe 1.7. Zeige, dass im Polynomring $K[X]$ über einem Körper K die Variable X irreduzibel und prim ist.

Aufgabe 1.8. Bestimme im Polynomring $K[X]$, wobei K ein Körper sei, die Einheiten und die Assoziiertheit. Gibt es in den Assoziiertheitsklassen besonders schöne Vertreter?

Im Polynomring $K[X]$ über einem Körper wird oft mit folgender Definition von irreduzibel gearbeitet.

Ein nichtkonstantes Polynom $P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in K[X]$, wobei K einen Körper bezeichne, heißt *irreduzibel*, wenn es keine Produktdarstellung

$$P = QR$$

gibt, die die Gradbedingung

$$0 < \deg(Q) < \deg(P)$$

erfüllt.

Aufgabe 1.9. Es sei K ein Körper und sei $K[X]$ der Polynomring über K. Zeige, dass die irreduziblen Polynome genau die irreduziblen Elemente in $K[X]$ sind.

Aufgabe 1.10. Es sei K ein Körper und sei $K[X]$ der Polynomring über K und sei $P \in K[X]$ ein Polynom, das eine Zerlegung in Linearfaktoren besitze. Es sei T ein Teiler von P. Zeige, dass T ebenfalls eine Zerlegung in Linearfaktoren besitzt, wobei die Vielfachheit eines Linearfaktors $X - a$ in T durch seine Vielfachheit in P beschränkt ist.

Aufgabe 1.11. Bestimme im Polynomring $F_2[X]$ alle irreduziblen Polynome vom Grad $2, 3, 4$.

Aufgabe 1.12. Was bedeutet die Eigenschaft, dass man in einem Integritätsbereich „kürzen“ kann? Beweise diese Eigenschaft.

Aufgabe 1.13. Es sei R ein kommutativer Ring und $f \in R$. Zeige, dass die Multiplikation mit f, also die Abbildung

$$\mu_f \colon R \longrightarrow R,\ x \longmapsto fx,$$

ein Gruppenhomomorphismus von $(R, +, 0)$ ist. Charakterisiere mit Hilfe der Multiplikationsabbildung, wann f ein Nichtnullteiler und wann f eine Einheit ist.

Aufgabe 1.14. Es sei R ein kommutativer Ring mit endlich vielen Elementen. Zeige, dass R genau dann ein Integritätsbereich ist, wenn R ein Körper ist.

Aufgabe 1.15. Wir betrachten die Menge $R = C(\mathbb{R}, \mathbb{R})$ der stetigen Funktionen von $\mathbb{R}$ nach $\mathbb{R}$. Zeige, dass R (mit naheliegenden Verknüpfungen) ein kommutativer Ring ist. Handelt es sich um einen Integritätsbereich?

Aufgabe 1.16. Es seien X und Y topologische Räume und

$$\varphi\colon\ X \longrightarrow Y$$

eine stetige Abbildung. Zeige, dass dies einen Ringhomomorphismus

$$C(Y, \mathbb{R}) \longrightarrow C(X, \mathbb{R}),\ f \longmapsto f \circ \varphi,$$

induziert.

Aufgabe 1.17. Es sei M ein metrischer Raum und $R = C(M, \mathbb{R})$ der Ring der stetigen Funktion auf M. Zeige, dass zwei zueinander assoziierte Elemente $f, g \in R$ die gleiche Nullstellenmenge besitzen, und dass die Umkehrung nicht gelten muss.

Aufgabe 1.18. Zeige, dass es stetige Funktionen

$$f, g\colon\ \mathbb{R}_{\geq 0} \longrightarrow \mathbb{R},$$

mit $fg = 0$ derart gibt, dass für alle $\delta > 0$ weder $f|_{[0,\delta]}$ noch $g|_{[0,\delta]}$ die Nullfunktion ist.

Die Begriffe teilen, irreduzibel und prim machen in jedem Monoid Sinn (nicht nur im multiplikativen Monoid eines Ringes). In den folgenden Aufgaben werden Teilbarkeitseigenschaften in einigen kommutativen Monoiden besprochen.

Aufgabe 1.19. Betrachte die natürlichen Zahlen $\mathbb{N}$ als kommutatives Monoid mit der Addition und neutralem Element 0. Bestimme die irreduziblen Elemente und die Primelemente von diesem Monoid. Gilt die eindeutige Primfaktorzerlegung?

Aufgabe 1.20. Betrachte die Menge M derjenigen positiven Zahlen, die modulo 4 den Rest 1 haben. Zeige, dass M mit der Multiplikation ein kommutatives Monoid ist. Bestimme die irreduziblen Elemente und die Primelemente von M. Zeige, dass in M jedes Element Produkt von irreduziblen Elementen ist, aber keine eindeutige Primfaktorzerlegung in M gilt.

Aufgaben zum Abgeben

Aufgabe 1.21. (4 Punkte)

Beweise die folgenden Eigenschaften zur Teilbarkeit in einem kommutativen Ring R

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

Aufgabe 1.22. (4 Punkte)

Zeige, dass in einem kommutativen Ring R folgende Teilbarkeitsbeziehungen gelten.

(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.

Aufgabe 1.23. (4 Punkte)

Bestimme im Polynomring $F_3[X]$ alle irreduziblen Polynome vom Grad 3.

Aufgabe 1.24. (2 Punkte)

Zeige, dass es im Ring der stetigen Funktionen $R = C(\mathbb{R}, \mathbb{R})$ Nichtnullteiler gibt, die unendlich viele Nullstellen besitzen.

Aufgabe 1.25. (3 Punkte)

Betrachte die Menge G der positiven geraden Zahlen zusammen mit 1. Zeige, dass G ein kommutatives Monoid ist. Bestimme die irreduziblen Elemente und die Primelemente von G. Zeige, dass in G jedes Element Produkt von irreduziblen Elementen ist, aber keine eindeutige Primfaktorzerlegung in G gilt.

Die Aufgabe zum Aufgeben

Für eine Lösung des folgenden Collatz-Problems haben verschiedene Autoren einen Preis ausgesetzt. Lösungen bitte an die Autoren. Für akzeptierte und prämierte Erstlösungen gibt es hier zusätzlich 200 Punkte, und Sie wären damit automatisch zur Klausur zugelassen.

Aufgabe 1.26. (200 Punkte)

Für positive ganze Zahlen n betrachten wir folgenden Algorithmus.

Wenn n gerade ist, so ersetze n durch die Hälfte.

Wenn n ungerade ist, so multipliziere n mit 3 und addiere dann 1 dazu.

Frage (Collatz-Problem): Ist es wahr, dass man bei jeder Startzahl n früher oder später bei 1 landet?

2. Vorlesung - Ideale und euklidische Ringe

Ideale

Alle Vielfachen der 5, also $\mathbb{Z}5$, bilden ein Ideal im Sinne der folgenden Definition.

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

(1) $0 \in \mathfrak{a}$.
(2) Für alle $a, b \in \mathfrak{a}$ ist auch $a + b \in \mathfrak{a}$.
(3) Für alle $a \in \mathfrak{a}$ und $r \in R$ ist auch $ra \in \mathfrak{a}$.

Definition 2.2. 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 2.3. 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 2.4. *Es 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 2.20. □

Definition 2.5. Ein kommutativer Ring, in dem jedes Ideal ein Hauptideal ist, heißt *Hauptidealring*. Ein integrer Hauptidealring heißt *Hauptidealbereich*.

Grösster gemeinsamer Teiler

Definition 2.6. Es 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 2.7. Eine Einheit ist immer ein gemeinsamer Teiler für jede Auswahl von Elementen. Ist t ein gemeinsamer Teiler der $a_1, \ldots, a_k$ und u eine Einheit, so ist auch ut ein gemeinsamer Teiler der $a_1, \ldots, a_k$. Ein größter gemeinsamer Teiler muss im Allgemeinen nicht existieren. Die Elemente $a_1, \ldots, a_k$ sind *teilerfremd* genau dann, wenn jeder gemeinsame Teiler davon eine Einheit ist.

Lemma 2.8. *Es 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. Es 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, ebenso in einem Polynomring in einer Variablen über einem Körper. 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

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

Ringe, in denen man eine Division mit Rest sinnvoll durchführen kann, bekommen einen eigenen Namen.

Definition 2.9. Ein *euklidischer Bereich* (oder *euklidischer Ring*) ist ein Integritätsbereich R, für den eine Abbildung $\delta \colon R \setminus \{0\} \to \mathbb{N}$ existiert, die die folgende Eigenschaft erfüllt:

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

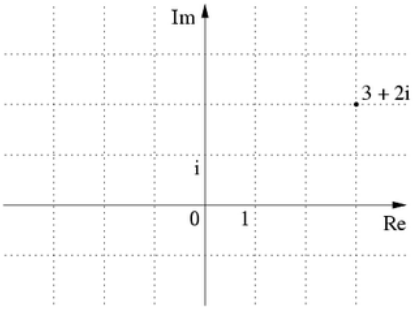
$$a = qb + r \text{ und } r = 0 \text{ oder } \delta(r) < \delta(b) \, .$$

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 2.10. 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 2.11. 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.



Gaußsche Zahlen als Gitterpunkte in der komplexen Zahlenebene

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 $N(z) = z\cdot\overline{z}$ schreiben, wobei $\overline{z}$ die komplexe Konjugation 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 2.12. *Der Ring der Gaußschen Zahlen ist mit der Normfunktion ein euklidischer Bereich.*

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

$$\frac{w}{z} = \frac{w\overline{z}}{z\overline{z}} = q_1 + q_2\mathrm{i}.$$

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

$$q_1 + q_2\mathrm{i} = a_1 + a_2\mathrm{i} + (q_1 - a_1) + (q_2 - a_2)\mathrm{i}$$

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

$$\begin{aligned} N((q_1 - a_1) + (q_2 - a_2)\mathrm{i}) &= (q_1 - a_1)^2 + (q_2 - a_2)^2 \\ &\leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 \\ &< 1. \end{aligned}$$

Multiplikation mit z ergibt

$$w = z(a_1 + a_2\mathrm{i}) + z((q_1 - a_1) + (q_2 - a_2)\mathrm{i}).$$

Der rechte Summand gehört dabei zu $\mathbb{Z}[\mathrm{i}]$, da man ihn als $w - z(a_1 + a_2\mathrm{i})$ schreiben kann. Aus der Multiplikativität der Norm folgt

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

□

Aufgabe 2.16 zeigt, dass die Division mit Rest im Allgemeinen nicht eindeutig sein muss.

Für eine unvollständige Liste von Primfaktorzerlegungen im Ring der Gaußschen Zahlen siehe den Link auf der Kursseite.

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

Lemma 2.13. *Es sei R ein euklidischer Bereich mit einer multiplikativen euklidischen Funktion*

$$N\colon R \setminus \{0\} \longrightarrow \mathbb{N}_+$$

(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. Es 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, sodass $r = 0$ sein muss und damit ist h eine Einheit. Also ist f irreduzibel. □

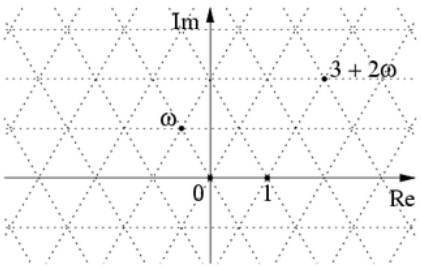
Wir werden später sehen, dass in euklidischen Bereichen irreduzible Elemente bereits prim sind. Das vorstehende Lemma ist also ein Kriterium für Primelemente. Die Umkehrung gilt übrigens nicht. Z. B. ist 3 ein Primelement in $\mathbb{Z}[\mathrm{i}]$, aber $N(3) = 9$ ist keine Primzahl.

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

Beispiel 2.14. Die Eisenstein-Zahlen sind komplexe Zahlen der Form

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

mit ganzen Zahlen a und b.



Eisenstein-Zahlen als Punkte eines Dreiecksgitters in der komplexen Zahlenebene

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 $\omega^3 = 1$), sodass 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 2.15. *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 $\omega = \frac{-1+\sqrt{3}\mathrm{i}}{2}$ 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. Es 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

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

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 2.16. *Ein euklidischer Bereich ist ein Hauptidealbereich.*

Beweis. Es sei I ein von 0 verschiedenes Ideal. Betrachte die nichtleere Menge

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

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. Dabei ist die Inklusion „$\supseteq$“ klar. Zum Beweis der Inklusion „$\subseteq$“ sei $a \in I$ 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. □

2. Arbeitsblatt

Übungsaufgaben

Aufgabe 2.1. Zeige, dass ein kommutativer Ring genau dann ein Körper ist, wenn er genau zwei Ideale enthält.

Aufgabe 2.2. Es seien $x, y \in R$ Elemente in einem kommutativen Ring R. Welche der folgenden Formulierungen sind zu

$$Rx \subseteq Ry$$

äquivalent.

(1) x teilt y.
(2) x wird von y geteilt.
(3) y wird von x geteilt.
(4) x ist ein Vielfaches von y.
(5) x ist ein Vielfaches von x.
(6) y teilt x.
(7) $Rx \cap Ry = Rx$.
(8) Jedes Vielfache von y ist auch ein Vielfaches von x.
(9) Jeder Teiler von y ist auch ein Teiler von x.
(10) Ein Maikäfer ist ein Schmetterling.

Aufgabe 2.3.
(a) Zeige, dass ein Ideal in einem kommutativen Ring R eine Untergruppe von R ist.
(b) Zeige, dass für $R = \mathbb{Z}$ die Begriffe Untergruppe und Ideal zusammenfallen.
(c) Man gebe eine Beispiel für einen kommutativen Ring R und eine Untergruppe $U \subseteq R$, die kein Ideal ist.

Aufgabe 2.4. Zeige, dass es zu ganzen Zahlen d, n mit $d > 0$ eindeutig bestimmte ganze Zahlen q, r mit $0 \leq r < d$ und mit

$$n = dq + r$$

gibt.

Aufgabe 2.5. Zeige, dass der Kern eines Ringhomomorphismus

$$\varphi\colon\ R \longrightarrow S$$

ein Ideal in R ist.

Aufgabe 2.6. Zeige, dass $\mathbb{Z}[X]$ und der Polynomring in zwei Variablen $K[X,Y]$ über einem Körper K keine Hauptidealbereiche sind.

Aufgabe 2.7. Es sei $T \subseteq \mathbb{R}$ eine Teilmenge. Zeige, dass im Ring der stetigen Funktionen

$$R = C(\mathbb{R},\mathbb{R})$$

die Teilmenge

$$I = \{f \in R \mid f(x) = 0 \text{ für alle } x \in T\}$$

ein Ideal in R ist.

Aufgabe 2.8. Wir betrachten das Ideal zu $T = \{0\} \subseteq \mathbb{R}$ im Sinne von Aufgabe 2.7. Ist dies ein Hauptideal?

Aufgabe 2.9. Es sei R ein kommutativer Ring und $a_1, a_2, \ldots, a_n, b, f \in R$ Elemente. Zeige die folgenden Aussagen.

(a) Wenn b ein größter gemeinsamer Teiler der $a_1, a_2, \ldots, a_n$ ist, so ist auch fb ein größter gemeinsamer Teiler der $fa_1, fa_2, \ldots, fa_n$.
(b) Wenn f ein Nichtnullteiler ist, so gilt hiervon auch die Umkehrung.

Aufgabe 2.10. Es seien $a, b \in R$ zwei irreduzible, nicht assoziierte Elemente in einem Integritätsbereich. Zeige, dass a und b teilerfremd sind.

Aufgabe 2.11. Es sei R ein Integritätsbereich und $p \in R$, $p \neq 0$. Zeige, dass p genau dann irreduzibel ist, wenn es genau zwei Hauptideale oberhalb von (p) gibt, nämlich (p) selbst und $(1) = R$.

Aufgabe 2.12. Es seien r und s teilerfremde Zahlen. Zeige, dass jede Lösung (x,y) der Gleichung

$$rx + sy = 0$$

die Gestalt $(x,y) = v(s,-r)$ mit einer eindeutig bestimmten Zahl v besitzt.

Aufgabe 2.13. Zeige durch ein Beispiel, dass die in Aufgabe 2.12 bewiesene Aussage ohne die Voraussetzung teilerfremd nicht stimmt.

Aufgabe 2.14. Zeige, dass die Untergruppen von $\mathbb{Z}$ genau die Teilmengen der Form

$$\mathbb{Z}d = \{kd \mid k \in \mathbb{Z}\}$$

mit einer eindeutig bestimmten nicht-negativen Zahl d sind.

Der Begriff des größten gemeinsamen Teilers wird innerhalb der ganzen Zahlen häufig wie folgt definiert.

Es seien $a_1, \ldots, a_k$ natürliche Zahlen. Eine natürliche Zahl g heißt *größter gemeinsamer Teiler* der $a_1, \ldots, a_k$, wenn g ein gemeinsamer Teiler ist und wenn g unter allen gemeinsamen Teilern der $a_1, \ldots, a_k$ der (bezüglich der Ordnungsrelation auf den natürlichen Zahlen) Größte ist.

Aufgabe 2.15. Es sei $a_1, \ldots, a_n$ eine Menge von ganzen Zahlen. Zeige, dass der nichtnegative größte gemeinsame Teiler der a_i (im Sinne der allgemeinen Ringdefinition) mit demjenigen gemeinsamen Teiler übereinstimmt, der bezüglich der Ordnungsrelation $\geq$ der größte gemeinsame Teiler ist.

Aufgabe 2.16. Zeige anhand der beiden Gaußschen Zahlen $1 + \mathrm{i}$ und 2, dass bei einem euklidischen Bereich die Division mit Rest nicht eindeutig sein muss. Man gebe vier gleichberechtigte Darstellungen für die Division mit Rest von „$1 + \mathrm{i}$ durch 2“ an.

Aufgabe 2.17. Es sei R ein euklidischer Bereich mit euklidischer Funktion δ. Zeige, dass ein Element $f \in R$ ($f \neq 0$) mit $\delta(f) = 0$ eine Einheit ist.

Aufgaben zum Abgeben

Aufgabe 2.18. (3 Punkte)

Es sei $n \in \mathbb{N}_+$ und seien n (verschiedene) natürliche Zahlen gegeben. Zeige, dass es eine nichtleere Teilmenge dieser Zahlen derart gibt, dass die zugehörige Summe ein Vielfaches von n ist.

Aufgabe 2.19. (3 Punkte)

Alle Flöhe leben auf einem unendlichen Zentimeter-Band. Ein Flohmännchen springt bei jedem Sprung 78 cm und die deutlich kräftigeren Flohweibchen springen mit jedem Sprung 126 cm. Die Flohmännchen Florian, Flöhchen und Carlo sitzen in den Positionen $-123,55$ und -49. Die Flohweibchen Flora und Florentina sitzen in Position 17 bzw. 109. Welche Flöhe können sich treffen?

Aufgabe 2.20. (3 Punkte)

Beweise folgende Aussagen für einen kommutativen Ring R.

(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.

Aufgabe 2.21. (3 Punkte)

Führe in $\mathbb{Z}[\mathrm{i}]$ die Division mit Rest „ $5+7\mathrm{i}$ durch $2-3\mathrm{i}$“ im Sinne von Lemma 2.12 durch.

Aufgabe 2.22. (2 Punkte)

Zeige, dass im Ring $\mathbb{Z}[\sqrt{-2}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{2}\mathrm{i}$ die Norm eine euklidische Funktion ist.

Aufgabe 2.23. (6 Punkte)

Es sei R ein Integritätsbereich. Betrachte die beiden folgenden Bedingungen:

(1) Es gibt ein Primelement $p \in R$ mit der Eigenschaft, dass sich jedes Element $f \in R$, $f \neq 0$, eindeutig als $f = up^i$ darstellen lässt mit einer Einheit u und $i \in \mathbb{N}$.
(2) R ist ein euklidischer Bereich mit einer surjektiven euklidischen Funktion $\delta : R\backslash\{0\} \to \mathbb{N}$, die zusätzlich die beiden folgenden Eigenschaften erfüllt.
   (a) Es gilt $\delta(fg) = \delta(f) + \delta(g)$ für alle $f, g \in R \setminus \{0\}$.
   (b) Es gilt $f|g$ genau dann, wenn $\delta(f) \leq \delta(g)$ für alle $f, g \in R\backslash\{0\}$.

Zeige, dass beide Bedingungen äquivalent sind. Können Sie Beispiele für solche Ringe angeben?

3. Vorlesung - Euklidischer Algorithmus und Hauptidealbereiche

Euklid (4. Jahrhundert v. C.)

Der euklidische Algorithmus

Euklidische Bereiche heißen so, weil in ihnen der euklidische Algorithmus ausgeführt werden kann.

Definition 3.1. Es seien 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*.[1]

Satz 3.2. *Es seien Elemente $r_0 = a, r_1 = b \neq 0$ eines euklidischen Bereiches 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) Es sei $k \geq 2$ der erste Index derart, dass $r_k = 0$ ist. Dann ist

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

[1] Da wir einen euklidischen Bereich ohne Eindeutigkeitsbedingung in der Division mit Rest definiert haben, ist diese Restfolge nicht unbedingt eindeutig bestimmt. Die relevanten Eigenschaften hängen aber nicht von Auswahlen ab und in allen wichtigen Beispielen ist die Division mit Rest eindeutig.

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, sodass 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

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

□

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:

$$\begin{aligned} 1071 &= 1 \cdot 1029 + 42, \\ 1029 &= 24 \cdot 42 + 21, \\ 42 &= 2 \cdot 21 + 0. \end{aligned}$$

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 $\mathbb{C}$ oder in $\mathbb{Q}[\mathrm{i}]$)

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

Die beste Approximation für diese komplexe Zahl mit einer ganzen Gaußschen Zahl ist 1, sodass 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, sodass 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.

Das Lemma von Bezout und das Lemma von Euklid

Satz 3.3. *Es 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 $r_1a_1 + r_2a_2 + \cdots + r_na_n = d$. Insbesondere besitzen teilerfremde Elemente $a_1, \ldots, a_n$ eine Darstellung der 1.*

Beweis. Es 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. Es 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 $I = (a_1, \ldots, a_n) = R$. □

Die vorstehende Aussage heißt *Lemma von Bezout*. In einem euklidischen Bereich kann man mit dem euklidischen Algorithmus eine Darstellung des größten gemeinsamen Teilers bestimmen, indem man rückwärts durch den Algorithmus wandert, siehe beispielsweise Aufgabe 3.4. Die folgende Aussage heißt *Lemma von Euklid*.

Lemma 3.4. *Es 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 dem Lemma von Bezout Elemente $r, s \in R$ mit $ra + sb = 1$. Die Voraussetzung, dass a das Produkt bc teilt, schreiben wir als $bc = da$. Damit gilt

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

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

Die Faktorialität von Hauptidealbereichen

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

Beweis. Ein Primelement in einem Integritätsbereich ist nach Lemma 1.16 stets irreduzibel. Es 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 dem Lemma von Euklid den anderen Faktor b. □

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

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

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

Die Vereinigung dieser Ideale ist aber nach Aufgabe 3.15 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 ein 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

$$a = u \cdot p_1 \cdots p_k = v \cdot q_1 \cdots q_m$$

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

Es 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 $k-1 \;=\; m-1$ und dass jedes p_i zu einem q_j assoziiert ist. □

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

Definition 3.8. Ein Integritätsbereich heißt *faktorieller Bereich*, wenn die beiden folgenden 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. *Es 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 0 sein können und u, v Einheiten sind). Dann gilt $a|b$ genau dann, wenn $r_i \leq s_i$ für alle Exponenten $i = 1, \ldots, k$ ist.

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

$$b \;=\; a\big(vu^{-1}p_1^{s_1-r_1} \cdots p_k^{s_k-r_k}\big)$$

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

Beispiel 3.11. Wir betrachten den Ring $R \;=\; \mathbb{Z}[\sqrt{-3}]$, der aus allen komplexen Zahlen der Form

$$a + b\sqrt{3}\mathrm{i} \text{ mit } a, b \in \mathbb{Z}$$

besteht und ein Unterring des Ringes der Eisensteinzahlen $\mathbb{Z}[\frac{1+\sqrt{3}\mathrm{i}}{2}]$ ist. Letzterer Ring ist nach Satz 2.15 euklidisch und ein Hauptidealbereich. Dagegen

gilt in R noch nicht einmal die eindeutige Faktorzerlegung in irreduzible Elemente. Es ist nämlich

$$\left(1+\sqrt{3}\mathrm{i}\right)\left(1-\sqrt{3}\mathrm{i}\right) \;=\; 4 \;=\; 2\cdot 2$$

und in beiden Zerlegungen sind die Faktoren irreduzibel, da es in R (und im Eisensteinring) keine Elemente mit Betragsquadrat 2 gibt. Im Ring der Eisensteinzahlen sind wegen

$$1+\sqrt{3}\mathrm{i} \;=\; \frac{1+\sqrt{3}\mathrm{i}}{2}\cdot 2$$

die Faktoren zueinander assoziiert, aber nicht in R, da es dort die Einheit $\frac{1+\sqrt{3}\mathrm{i}}{2}$ nicht gibt. Das Ideal

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

ist in R kein Hauptideal.

Restklassenringe von Hauptidealbereichen

Satz 3.12. *Es 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 $p=0$), siehe Aufgabe 3.24, und (3) impliziert natürlich (2). Es sei also (1) erfüllt und sei $a\in R/(p)$ von 0 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 $(a,p)=(b)$ schreiben, da wir in einem Hauptidealring sind. Es folgt $p=cb$. Da c keine Einheit ist und p prim (also nach Lemma 1.16 auch 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. □

3. Arbeitsblatt

Übungsaufgaben

Aufgabe 3.1. Bestimme in $\mathbb{Z}$ mit Hilfe des euklidischen Algorithmus den größten gemeinsamen Teiler von 1983 und 1528.

Aufgabe 3.2. Bestimme in $\mathbb{Z}$ mit Hilfe des euklidischen Algorithmus den größten gemeinsamen Teiler von 3711 und 4115.

Aufgabe 3.3. Bestimme in $\mathbb{Z}$ mit Hilfe des euklidischen Algorithmus den größten gemeinsamen Teiler von 71894 und 45327.

Aufgabe 3.4. Man bestimme den größten gemeinsamen Teiler von 3146 und 1515 und man gebe eine Darstellung des ggT von 3146 und 1515 mittels dieser Zahlen an.

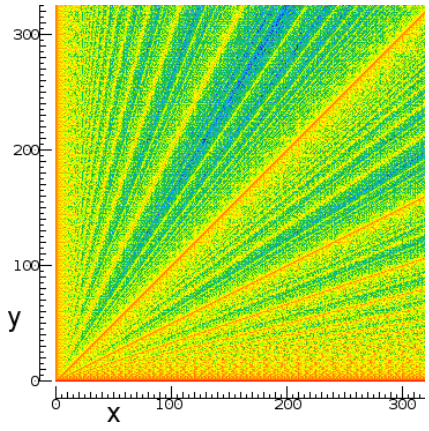
Die Folge der *Fibonacci-Zahlen* f_n ist rekursiv durch

$$f_1 := 1\,, f_2 := 1 \text{ und } f_{n+2} := f_{n+1} + f_n$$

definiert.

Aufgabe 3.5. Wende auf zwei aufeinander folgende Fibonacci-Zahlen den euklidischen Algorithmus an. Welche Gesetzmäßigkeit tritt auf?

Aufgabe 3.6. Die Beschreibungsseite des folgenden Bildes behauptet, etwas mit dem euklidischen Algorithmus zu tun zu haben. Erläutere dies. Welche Eigenschaften des euklidischen Algorithmus sind in dem Bild sichtbar? Beweise diese Eigenschaften des Algorithmus.



Aufgabe 3.7. Die Wasserspedition „Alles im Eimer“ verfügt über 77-, 91- und 143-Liter Eimer, die allerdings keine Markierungen haben. Sie erhält den Auftrag, insgesamt genau einen Liter Wasser von der Nordsee in die Ostsee zu transportieren. Wie kann sie den Auftrag erfüllen?

Aufgabe 3.8. Bestimme in $\mathbb{C}[X]$ mit Hilfe des euklidischen Algorithmus den größten gemeinsamen Teiler der beiden Polynome $X^3 + (2 - \mathrm{i})X^2 + 4$ und $(3 - \mathrm{i})X^2 + 5X - 3$.

Aufgabe 3.9. Bestimme in $\mathbb{Q}[X]$ mit Hilfe des euklidischen Algorithmus den größten gemeinsamen Teiler der beiden Polynome $2X^4 - 7X^2 + \frac{5}{2}X + 3$ und $X^3 + 1$.

Aufgabe 3.10. Bestimme in $\mathbb{F}_7[X]$ mit Hilfe des euklidischen Algorithmus den größten gemeinsamen Teiler der beiden Polynome $P = X^3 + 6X^2 + 4$ und $Q = X^2 + 3X + 2$.

Aufgabe 3.11. Bestimme in $\mathbb{Z}/(11)[X]$ den (normierten) größten gemeinsamen Teiler der beiden Polynome

$$X^4 + 2X^3 + 2X^2 + 3 \quad \text{und} \quad X^2 + 7X + 10\,.$$

Aufgabe 3.12. Bestimme in $\mathbb{Z}[\mathrm{i}]$ mit Hilfe des euklidischen Algorithmus den größten gemeinsamen Teiler von $5 + 2\mathrm{i}$ und $3 + 7\mathrm{i}$.

Aufgabe 3.13. Bestimme in $\mathbb{Z}[\mathrm{i}]$ mit Hilfe des euklidischen Algorithmus den größten gemeinsamen Teiler von $23 + 2\mathrm{i}$ und $1 + 23\mathrm{i}$.

Aufgabe 3.14. Zeige, dass im Polynomring $K[X, Y]$ nicht das Lemma von Bezout gilt.

Aufgabe 3.15. Es sei R ein kommutativer Ring und sei

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \ldots$$

eine aufsteigende Kette von Idealen. Zeige, dass die Vereinigung $\bigcup_{n\in\mathbb{N}} \mathfrak{a}_n$ ebenfalls ein Ideal ist. Zeige durch ein einfaches Beispiel, dass die Vereinigung von Idealen im Allgemeinen kein Ideal sein muss.

Aufgabe 3.16. Zeige, dass in einem Hauptidealbereich R zu beliebigen Elementen $a_1, \ldots, a_n \in R$ sowohl ein größter gemeinsame Teiler als auch ein kleinstes gemeinsames Vielfaches existieren. Wie kann man sie berechnen, wenn die Primfaktorzerlegungen der Elemente bekannt sind?

Für $\mathbb{Z}$ lässt sich die Existenz einer Zerlegung in Primzahlen, also in irreduzible Elemente, einfach direkt zeigen.

Aufgabe 3.17. Zeige durch Induktion, dass jede natürliche Zahl $n \geq 2$ eine Zerlegung in Primzahlen besitzt.

Aufgabe 3.18. Finde einen Primfaktor der Zahl $2^{25} + 1$.

Aufgabe 3.19. Bestimme die Primfaktorzerlegung von 1728.

Aufgabe 3.20. Wir betrachten das kleine Einmaleins als eine Verknüpfungstabelle, in der alle Produkte $i \cdot j$ mit $1 \leq i, j \leq 9$ stehen. Bestimme die Primfaktorzerlegung des Produktes über alle Einträge in der Tabelle.

Aufgabe 3.21. Man gebe zwei Primfaktoren von $2^{35} - 1$ an.

Aufgabe 3.22. Es sei p eine Primzahl. Zeige, dass

$$\binom{p}{k} \equiv 0 \mod p$$

für alle $k = 1, \ldots, p-1$ ist.

Aufgabe 3.23. Es seien $a, b \in \mathbb{N}_+$. Zeige, dass

$$a^b = b^a$$

genau dann gilt, wenn

$$a = b$$

ist oder wenn $a = 2$ und $b = 4$ ist (oder umgekehrt).

Aufgabe 3.24. Es sei R ein kommutativer Ring und $p \in R$, $p \neq 0$. Zeige, dass p genau dann ein Primelement ist, wenn der Restklassenring $R/(p)$ ein Integritätsbereich ist.

Aufgaben zum Abgeben

Aufgabe 3.25. (2 Punkte)

Finde einen Primfaktor der Zahl $2^{25} - 1$.

Aufgabe 3.26. (3 Punkte)

Bestimme in $\mathbb{Z}[\mathrm{i}]$ mit Hilfe des euklidischen Algorithmus den größten gemeinsamen Teiler von $35 + 18\mathrm{i}$ und $8 + 11\mathrm{i}$.

Aufgabe 3.27. (3 Punkte)

Bestimme in $\mathbb{F}_5[X]$ mit Hilfe des euklidischen Algorithmus den größten gemeinsamen Teiler der beiden Polynome $P = X^4 + 3X^3 + X^2 + 4X + 2$ und $Q = 2X^3 + 4X^2 + X + 3$.

In der folgenden Aufgabe wird der Logarithmus verwendet.

Aufgabe 3.28. (4 (3+1) Punkte)

Betrachte die reellen Zahlen $\mathbb{R}$ als $\mathbb{Q}$-Vektorraum. Zeige, dass die Menge der reellen Zahlen $\ln p$, wobei p durch die Menge der Primzahlen läuft, linear unabhängig ist. Bleibt das Ergebnis gültig, wenn man den natürlichen Logarithmus ln durch einen Logarithmus zu einer anderen Basis ersetzt?

Aufgabe 3.29. (3 (2+1) Punkte)

Es sei $r \in \mathbb{N}$.

(a) Finde r aufeinander folgende natürliche Zahlen (also $n, n+1, \ldots, n+r-1$), die alle nicht prim sind.
(b) Finde unendlich viele solcher primfreien r-„Intervalle“.

Aufgabe 3.30. (4 Punkte)

Es seien a und b positive natürliche Zahlen. Es seien $r_n\,, n \in \mathbb{N}$, und $s_n\,, n \in \mathbb{N}$, Folgen von positiven natürlichen Zahlen derart, dass die Teilbarkeitsbeziehung

$$a^{r_n} | b^{s_n}$$

für alle n gilt. Es sei vorausgesetzt, dass die Quotientenfolge r_n/s_n gegen 1 konvergiert. Zeige, dass a ein Teiler von b ist.

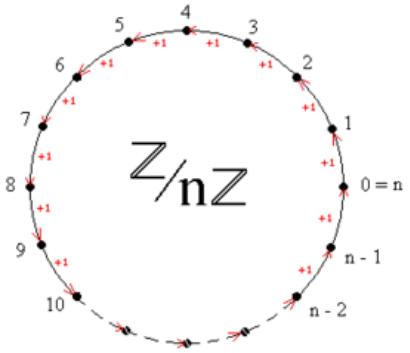
Aufgabe 3.31. (6 (2+2+2) Punkte)

Zu einer natürlichen Zahl n bezeiche $T(n)$ die Anzahl der positiven Teiler von n. Zeige die folgenden Aussagen über $T(n)$.

(a) Es sei $n = p_1^{r_1} \cdots p_k^{r_k}$ die Primfaktorzerlegung von n. Dann ist
$$T(n) = (r_1 + 1)(r_2 + 1) \cdots (r_k + 1).$$
(b) Für teilerfremde Zahlen n und m gilt $T(nm) = T(n)T(m)$.
(c) Bestimme die Anzahl der Teiler von 20!.

4. Vorlesung - Restklassenringe und prime Restklassengruppen

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



Für die Restklassenringe $\mathbb{Z}/(n)$ verwenden wir $\{0, 1, 2, \ldots, n-1\}$ als kanonisches Repräsentantensystem.

Satz 4.1. *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 Satz 3.3 eine Darstellung der 1, es gibt also ganze 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 dem inversen Element $a^{-1} = r$.

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, sodass also
$$ar - 1 = sn$$

gilt. Dann ist aber wieder $ar - sn = 1$ und a und n sind teilerfremd. □

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

Beweis. Dies folgt unmittelbar aus Satz 3.12. □

Wir geben noch einen zweiten Beweis.

Die Zahl $n \geq 2$ ist genau dann prim, wenn sie teilerfremd zu jeder Zahl a, $0 < a < n$, ist. Dies ist nach Satz 4.1 genau dann der Fall, wenn in $\mathbb{Z}/(n)$ jedes von 0 verschiedene Element eine Einheit ist.

Die eulersche Phi-Funktion

Leonhard Euler (1707-1783)

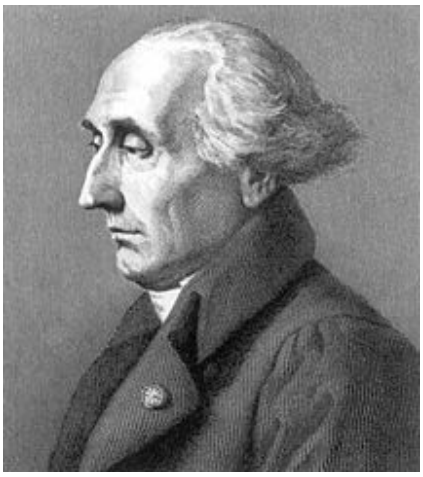
Definition 4.3. Zu einer natürlichen Zahl n bezeichnet $\varphi(n)$ die Anzahl der Elemente von $(\mathbb{Z}/(n))^\times$. Man nennt $\varphi(n)$ die *Eulersche Funktion.*

Bemerkung 4.4. Die Eulersche Funktion $\varphi(n)$ gibt also für $n \geq 1$ nach Satz 4.1 an, wie viele Zahlen r, $0 \leq r < n$, zu n teilerfremd sind.

Satz 4.5. *Es 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 dem 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. *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 $p-1$, und nach dem 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 0 steht. □

Pierre de Fermat (1607/08-1665)

Beispiel 4.7. Es sei beispielsweise $p = 5$. Dann ist für

$$a = 1 \ : \ 1^5 = 1 \mod 5$$

$$a = 2 \ : \ 2^5 = 32 = 2 \mod 5$$

$$a = 3 \ : \ 3^5 = 243 = 3 \mod 5$$

$$a = 4 \ : \ 4^5 = 1024 = 4 \mod 5 \, .$$

Endliche Körper und der Satz von Wilson

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

Satz 4.9. *Es sei K ein endlicher Körper. Dann ist das Produkt aller von 0 verschiedenen 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 als

$$1(-1)x_1 x_1^{-1} \cdots x_k x_k^{-1}$$

schreiben. 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 $1 = -1$. □

Die folgende Aussage heißt *Satz von Wilson*.

Korollar 4.10. *Es sei p eine Primzahl. Dann ist $(p-1)! = -1 \bmod p$.*

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 $\mathbb{Z}/(p)$. □

Der Chinesische Restsatz

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

Lemma 4.11. *Es 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

$$\ker\phi \;=\; (n) \;\subseteq\; (k) \;=\; \ker\varphi.$$

Aufgrund des Homomorphiesatzes hat man daher einen kanonischen Ringhomomorphismus von links unten nach rechts oben. □

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

Definition 4.12. Es 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. *Es sei n eine positive natürliche Zahl mit kanonischer Primfaktorzerlegung*

$$n \;=\; p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$$

(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 Ringisomorphismus

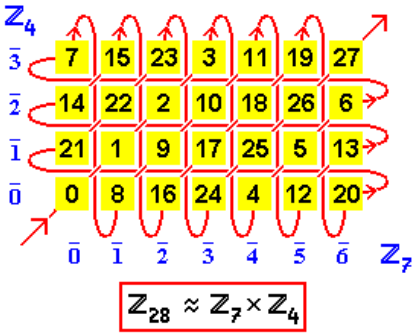
$$\mathbb{Z}/(n) \;\cong\; \mathbb{Z}/(p_1^{r_1}) \times \mathbb{Z}/(p_2^{r_2}) \times \cdots \times \mathbb{Z}/(p_k^{r_k}).$$

Zu gegebenen ganzen Zahlen $(a_1, a_2, \ldots, a_k)$ 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. Es sei x eine natürliche Zahl, die im Produktring (rechts) zu 0 wird, also modulo $p_i^{r_i}$ den Rest 0 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 dem Exponenten r_i vorkommen. Also muss x nach Korollar 3.10 ein Vielfaches des Produktes sein, 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

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

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

$(0,0,1)$: Hier betrachtet man die Vielfachen von 15, 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 Einheitengruppe 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. *Es 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. Es sei $(xy)^k = 1$. Wir müsen zeigen, dass k ein Vielfaches von nm ist. Es ist

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

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 3.4, dass k ein Vielfaches von m ist. Ebenso ergibt sich, dass k ein Vielfaches von n ist, sodass 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 $x^n = 1$ für alle $x \in G$ ist.

Lemma 4.16. *Es 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. Es sei

$$n = \operatorname{ord}(G) = p_1^{r_1} \cdots p_k^{r_k}$$

die Primfaktorzerlegung der Gruppenordnung. Der Exponent der Gruppe ist

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

Es 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. □

4. Arbeitsblatt

Übungsaufgaben

Aufgabe 4.1. Bestimme alle Lösungen der linearen Kongruenz $12x = 3 \mod 21$.

Aufgabe 4.2. Bestimme alle Lösungen der linearen Kongruenz $13x = 11 \mod 141$.

Aufgabe 4.3. Berechne die Restklasse von 2^{1563} modulo 23.

Aufgabe 4.4. Berechne 3^{1457} in $\mathbb{Z}/(13)$.

Aufgabe 4.5. Charakterisiere diejenigen positiven ungeraden Zahlen n mit der Eigenschaft, dass bei dem in Aufgabe 1.26 beschriebenen Algorithmus genau zwei ungerade Zahlen auftreten (nämlich n und 1, aber beliebig viele gerade Zahlen).

Aufgabe 4.6. Es sei p eine Primzahl. Beweise durch Induktion den kleinen Fermat, also die Aussage, dass $a^p - a$ ein Vielfaches von p für jede ganze Zahl a ist.

Aufgabe 4.7. Bestimme den Rest von 27! modulo 31.

Aufgabe 4.8. Bestimme die Zerlegung von $X^{p-1}-1$ in irreduzible Polynome im Polynomring $\mathbb{Z}/(p)[X]$. Beweise aus dieser Zerlegung den Satz von Wilson.

Aufgabe 4.9. Es seien $a, b \geq 2$ und sei $n = ab$.

(a) Zeige, dass die beiden Polynome $X^a - 1$ und $X^b - 1$ Teiler des Polynoms $X^n - 1$ sind.
(b) Es sei $a \neq b$. Ist $(X^a - 1)(X^b - 1)$ stets ein Teiler von $X^n - 1$?
(c) Man gebe drei Primfaktoren von $2^{30} - 1$ an.

Aufgabe 4.10. (a) Finde mit Hilfe des euklidischen Algorithmus eine Darstellung der 1 für die beiden Zahlen 19 und 109.

(b) Nach dem Chinesischen Restsatz haben wir die Isomorphie

$$\mathbb{Z}/(2071) \cong \mathbb{Z}/(19) \times \mathbb{Z}/(109).$$

Welche Restklasse modulo 2071 entspricht dem Restklassenpaar $(1, 0)$ und welche dem Paar $(0, 1)$?

(c) Bestimme diejenige Restklasse modulo 2071, die modulo 19 den Rest 5 hat und die modulo 109 den Rest 10 hat.

Aufgabe 4.11. (a) Bestimme für die Zahlen 3, 11 und 13 modulare Basislösungen, finde also die kleinsten positiven Zahlen, die in

$$\mathbb{Z}/(3) \times \mathbb{Z}/(11) \times \mathbb{Z}/(13)$$

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

$$x = 2 \mod 3, \quad x = 5 \mod 11 \text{ und } x = 6 \mod 13\,.$$

Aufgabe 4.12. (a) Bestimme für die Zahlen 2, 9 und 25 modulare Basislösungen, finde also die kleinsten positiven Zahlen, die in

$$\mathbb{Z}/(2) \times \mathbb{Z}/(9) \times \mathbb{Z}/(25)$$

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

$$x = 0 \mod 2, \quad x = 3 \mod 9 \text{ und } x = 5 \mod 25\,.$$

Aufgabe 4.13. (a) Bestimme für die Zahlen 4, 5 und 11 modulare Basislösungen, finde also die kleinsten positiven Zahlen, die in

$$\mathbb{Z}/(4) \times \mathbb{Z}/(5) \times \mathbb{Z}/(11)$$

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

$$x = 3 \mod 4, \quad x = 2 \mod 5 \text{ und } x = 10 \mod 11\,.$$

Aufgabe 4.14. Man berechne in $\mathbb{Z}/(80)$ die Elemente

(a) $3^{1234567}$,
(b) $2^{1234567}$,
(c) $5^{1234567}$.

Aufgabe 4.15. Es seien R und $S_1, \ldots, S_n$ kommutative Ringe mit dem Produktring

$$S = S_1 \times \cdots \times S_n.$$

Zeige, dass ein Ringhomomorphismus

$$\varphi\colon R \longrightarrow S$$

dasselbe ist wie eine Familie von Ringhomomorphismen

$$\varphi_i\colon R \longrightarrow S_i$$

für $i = 1, \ldots, n$.

Aufgabe 4.16. Man gebe eine surjektive Abbildung

$$\varphi\colon \mathbb{Z} \longrightarrow \mathbb{Z}/(3)$$

an, die mit der Multiplikation verträglich (also ein Monoidhomomorphismus) ist, aber kein Ringhomomorphismus ist.

Aufgabe 4.17. Es sei n eine positive natürliche Zahl mit der Faktorzerlegung

$$n = 2^r \cdot 5^s \cdot d,$$

wobei d zu n teilerfremd sei ($r, s = 0$ und $d = 1$ sind erlaubt). Zeige, dass die Periodenlänge der Dezimalentwicklung von $\frac{1}{n}$ gleich der multiplikativen Ordnung von 10 in $\mathbb{Z}/(d)$ ist.

Aufgabe 4.18. Es sei R ein kommutativer Ring, der einen Körper der positiven Charakteristik $p > 0$ enthalte (dabei ist p eine Primzahl). Zeige, dass die Abbildung

$$R \longrightarrow R,\ f \longmapsto f^p,$$

ein Ringhomomorphismus ist, den man den *Frobeniushomomorphismus* nennt.

Tipp: Benutze Aufgabe 3.22.

Aufgabe 4.19. Es sei p eine Primzahl und sei $f(x)$ ein Polynom mit Koeffizienten in $\mathbb{Z}/(p)$ vom Grad $d \geq p$. Zeige, dass es ein Polynom $g(x)$ mit einem Grad $< p$ derart gibt, dass für alle Elemente $a \in \mathbb{Z}/(p)$ die Gleichheit

$$f(a) = g(a)$$

gilt.

Aufgabe 4.20. Zeige, dass eine Untergruppe einer zyklischen Gruppe wieder zyklisch ist.

Aufgabe 4.21. Zeige, dass eine Restklassengruppe einer zyklischen Gruppe wieder zyklisch ist.

Aufgabe 4.22. Es sei

$$G = H_1 \times \cdots \times H_n$$

die Produktgruppe der endlichen Gruppen $H_1, \ldots, H_n$. Zeige die folgenden Aussagen.

(1)
$$\exp G = \mathrm{kgV}(\exp H_i, i = 1, \ldots, n).$$

(2) G ist genau dann zyklisch, wenn alle H_i zyklisch sind und wenn deren Ordnungen paarweise teilerfremd sind.

Aufgabe 4.23. Es seien $n_1, \ldots, n_k$ positive natürliche Zahlen und es sei

$$G = \mathbb{Z}/(n_1) \times \mathbb{Z}/(n_2) \times \cdots \times \mathbb{Z}/(n_k)$$

die Produktgruppe. Bestimme den Exponenten von G.

Aufgabe 4.24. Wir betrachten die endliche Permutationsgruppe S_n zu einer Menge mit n Elementen.

(a) Zeige, dass es in S_n Elemente der Ordnung n gibt.
(b) Man gebe ein Beispiel für eine Permutationsgruppe S_n und einem Element darin, dessen Ordnung größer als n ist.

Aufgabe 4.25. Zeige, dass es in der Restklassengruppe $\mathbb{Q}/\mathbb{Z}$ zu jedem $n \in \mathbb{N}_+$ Elemente gibt, deren Ordnung gleich n ist.

Aufgabe 4.26. Für eine Gruppe G bezeichne $T(G)$ die Menge aller Elemente mit endlicher Ordnung in G. Zeige folgende Aussagen.

(1) Ist G abelsch, so ist $T(G)$ eine Untergruppe von G.
(2) Ist $T(G)$ eine Untergruppe, so ist $T(G)$ ein Normalteiler in G.
(3) Es gibt eine Gruppe G, für die $T(G)$ keine Untergruppe von G ist.

Aufgaben zum Abgeben

Aufgabe 4.27. (3 Punkte)

Formuliere und beweise (bekannte) Teilbarkeitskriterien für Zahlen im Dezimalsystem für die Teiler $k = 2, 3, 5, 9, 11$.

Aufgabe 4.28. (4 Punkte)

Es sei p eine ungerade Primzahl. Beweise unter Verwendung des Satzes von Wilson, dass

$$1^2 \cdot 3^2 \cdot 5^2 \cdots (p-4)^2 \cdot (p-2)^2 \;=\; (-1)^{\frac{p+1}{2}} \mod p$$

gilt.

Aufgabe 4.29. (3 Punkte)

Es sei $f(x) = x^7 + 2x^3 + 3x + 4 \in (\mathbb{Z}/(5))[x]$. Finde ein Polynom $g(x) \in (\mathbb{Z}/(5))[x]$ vom Grad < 5, das für alle Elemente aus $\mathbb{Z}/(5)$ mit $f(x)$ übereinstimmt.

Aufgabe 4.30. (3 Punkte)

(a) Bestimme für die Zahlen 2, 3 und 7 modulare Basislösungen, finde also die kleinsten positiven Zahlen, die in

$$\mathbb{Z}/(2) \times \mathbb{Z}/(3) \times \mathbb{Z}/(7)$$

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

$$x = 1 \mod 2, \quad x = 2 \mod 3 \text{ und } x = 2 \mod 7\,.$$

5. Vorlesung - Die primen Restklassengruppen

Endliche Untergruppen eines Körpers

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 $\varphi(n)$ ausgedrückt. Wir erinnern kurz an eine wichtige Tatsache für die Anzahl der Nullstellen eines Polynoms über einem Körper.

Satz 5.1. *Es sei K ein Körper und sei $K[X]$ der Polynomring über K. Es sei $P \in K[X]$ ein Polynom ($\neq 0$) vom Grad d. Dann besitzt P maximal d Nullstellen.*

Satz 5.2. *Es sei $U \subseteq K^\times$ eine endliche Untergruppe der multiplikativen Gruppe eines Körpers K. Dann ist U zyklisch.*

Beweis. Es 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 Satz 5.1 ist die Anzahl der Nullstellen aber maximal gleich dem Grad, sodass $n = e$ folgt. Nach Lemma 4.16 ist dann U zyklisch. □

Die reellen Zahlen besitzen überhaupt nur die beiden endlichen multiplikativen Untergruppen $\{1\}$ und $\{1, -1\}$. Im komplexen Fall liegen die endlichen multiplikativen Untergruppen auf dem Einheitskreis, es handelt sich um die Gruppen μ_k der k-ten Einheitswurzeln, also um

$$\{e^{2\pi i \frac{j}{k}},\ j = 0, 1, \ldots, k-1\}.$$

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

Satz 5.3. *Es sei p eine Primzahl. Dann ist die Einheitengruppe $(\mathbb{Z}/(p))^\times$ zyklisch mit der Ordnung $p-1$. Es gibt also 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 5.2, da $\mathbb{Z}/(p)$ ein endlicher Körper ist. □

Definition 5.4. Eine Einheit $g \in (\mathbb{Z}/(n))^\times$ heißt *primitiv* (oder eine *primitive Einheit*), wenn sie die Einheitengruppe erzeugt.

Bemerkung 5.5. Der Satz 5.3 besagt 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 Primzahl p und eine Einheit $g \in (\mathbb{Z}/(p))^\times$ bedeutet die Eigenschaft, primitiv zu sein, dass ein Gruppenisomorphismus

$$(\mathbb{Z}/(p-1), +, 0) \longrightarrow ((\mathbb{Z}/(p))^\times, \cdot, 1),\ i \longmapsto g^i,$$

vorliegt. 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.

Korollar 5.6. *Es 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

$$\mathbb{Z}/(p-1) \,=\, (\mathbb{Z}/(p))^{\times}.$$

Daher geht es um die Anzahl der Erzeuger der additiven Gruppe $\mathbb{Z}/(p-1)$. Ein Element aus $\mathbb{Z}/(p-1)$ ist ein Gruppenerzeuger genau dann, wenn es in $\mathbb{Z}/(p-1)$ (als Ring betrachtet) eine Einheit ist. Deshalb ist die Anzahl gerade $\varphi(p-1)$. □

Die Einheitengruppen der Restklassenringe

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

Satz 5.7. *Es 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 Ringisomorphismus des Chinesischen Restsatzes $\mathbb{Z}/(n) \cong \mathbb{Z}/(p_1^{r_1}) \times \mathbb{Z}/(p_2^{r_2}) \times \cdots \times \mathbb{Z}/(p_k^{r_k})$ einen Gruppenisomorphismus 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 $\mathbb{Z}/(p_i^{r_i})$ für alle $i = 1, \ldots, k$ zyklisch sind.

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). □

Bemerkung 5.8. Aus der 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, sodass 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

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

Die Einheitengruppen nach Primzahlpotenzen

Ausgehend von Satz 5.7 ist es wichtig, die Einheitengruppe von $\mathbb{Z}/(p^r)$ zu verstehen.

Lemma 5.9. *Es sei p eine Primzahl und $r \geq 1$. Dann ist der durch die kanonische Projektion*

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

induzierte Gruppenhomomorphismus

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

der Einheitengruppen surjektiv.

Beweis. Es 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. *Es sei $p \geq 3$ eine Primzahl und $r \geq 1$. Dann ist der Kern des Einheiten-Homomorphismus*

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

zyklisch der Ordnung p^{r-1}.

Beweis. Wir zeigen, dass das Element $a = 1+p$, das offensichtlich zum Kern von

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

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, sodass 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 $2 \leq k \leq p^{r-2}$. 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. Es 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 $k \geq 2$). Es 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. *Es 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

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

surjektiv. Die Einheitengruppe $(\mathbb{Z}/(p))^\times$ ist zyklisch aufgrund von Satz 5.3. 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 $w \in (\mathbb{Z}/(p^r))^\times$ (nämlich eine gewisse Potenz von u), das genau die Ordnung $p-1$ besitzt.

Auf der anderen Seite gibt es nach Lemma 5.10 ein Element $a \in (\mathbb{Z}/(p^r))^\times$, 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 aw ist 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

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

sodass 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 im Beweis zu 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 stets 5 ein Element der Ordnung 2^{r-2}. Jede Einheit in $\mathbb{Z}/(2^r)$ hat somit eine Darstellung der Form $\pm 5^i$.

5. Arbeitsblatt

Übungsaufgaben

Aufgabe 5.1. Bestimme die multiplikative Ordnung aller Einheiten im Restklassenkörper $\mathbb{Z}/(11)$.

Aufgabe 5.2. Bestimme sämtliche primitive Einheiten im Restklassenkörper $\mathbb{Z}/(13)$.

Aufgabe 5.3. Bestimme sämtliche primitive Einheiten im Restklassenkörper $\mathbb{Z}/(23)$.

Aufgabe 5.4. Finde primitive Einheiten in den Restklassenkörpern $\mathbb{Z}/(13)$, $\mathbb{Z}/(17)$ und $\mathbb{Z}/(19)$.

Aufgabe 5.5. Bestimme in der Einheitengruppe $(\mathbb{Z}/(17))^\times$ zu jeder möglichen Ordnung k ein Element $x \in (\mathbb{Z}/(17))^\times$, das die Ordnung k besitzt. Man gebe auch eine Untergruppe

$$H \subseteq (\mathbb{Z}/(17))^\times$$

an, die aus vier Elementen besteht.

Aufgabe 5.6. Es sei p eine ungerade Primzahl und $\mathbb{Z}/(p)$ der zugehörige Restklassenkörper. Zeige, dass das Produkt von zwei primitiven Einheiten niemals primitiv ist.

Aufgabe 5.7. Es sei $n \in \mathbb{N}_+$. Zeige, dass die Gruppe der n-ten Einheitswurzeln in $\mathbb{C}$ und die Gruppe $\mathbb{Z}/(n)$ isomorph sind.

Aufgabe 5.8. Beweise ausschließlich durch Anzahlbetrachtungen Lemma 5.9, dass also der kanonische Homomorphismus $(\mathbb{Z}/(p^r))^\times \to (\mathbb{Z}/(p))^\times$ surjektiv ist (p Primzahl).

Aufgabe 5.9. Bestimme eine primitive Einheit $v \in \mathbb{Z}/(5)$ und ein Urbild $u \in \mathbb{Z}/(25)$ von v, das in $\mathbb{Z}/(25)$ nicht primitiv ist.

Aufgabe 5.10.
(a) Finde ein primitives Element in $\mathbb{Z}/(3)$, in $\mathbb{Z}/(9)$ und in $\mathbb{Z}/(27)$.
(b) Finde eine ganze Zahl, die in $\mathbb{Z}/(3)$ primitiv ist, aber nicht in $\mathbb{Z}/(9)$.
(c) Zeige, dass jede ganze Zahl, die in $\mathbb{Z}/(9)$ primitiv ist, auch in $\mathbb{Z}/(27)$ primitiv ist.

Aufgabe 5.11. Bestimme alle primitiven Elemente von $\mathbb{Z}/(27)$.

Aufgabe 5.12. Es sei p eine Primzahl und $r \geq 2$. Beschreibe explizit die Elemente im Kern der Abbildung

$$(\mathbb{Z}/(p^r))^\times \longrightarrow \left(\mathbb{Z}/(p^{r-1})\right)^\times.$$

Aufgabe 5.13. Es sei p eine Primzahl. Wir betrachten den kanonischen Ringhomomorphismus

$$\mathbb{Z}/(p^2) \longrightarrow \mathbb{Z}/(p)$$

und den zugehörigen Gruppenhomomorphismus

$$\left(\mathbb{Z}/(p^2)\right)^\times \longrightarrow (\mathbb{Z}/(p))^\times$$

der Einheitengruppen. Es sei v eine primitive Einheit von $\mathbb{Z}/(p)$. Zeige, dass unter den Urbildern von v in $\mathbb{Z}/(p^2)$ ein Element keine primitive Einheit von $\mathbb{Z}/(p^2)$ ist, und $p-1$ Elemente primitive Einheiten sind.

Aufgabe 5.14. Es sei p eine ungerade Primzahl und $r \geq s \geq 2$ Wir betrachten den kanonischen Ringhomomorphismus

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

und den zugehörigen Gruppenhomomorphismus

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

der Einheitengruppen. Es sei v eine primitive Einheit von $\mathbb{Z}/(p^s)$. Zeige, dass sämtliche Urbilder von v in $\mathbb{Z}/(p^r)$ primitive Einheiten von $\mathbb{Z}/(p^s)$ sind.

In der folgenden Aufgabe bezeichnet $\mathbb{F}_{121}$ den Körper mit 121 Elementen. Darüber hinaus muss muss man nichts über ihn wissen.

Aufgabe 5.15. Finde ein primitives Element in $\mathbb{Z}/(11)$ und in $\mathbb{Z}/(121)$. Man gebe ferner ein Element der Ordnung 10 und ein Element der Ordnung 11 in $\mathbb{Z}/(121)$ an. Gibt es Elemente der Ordnung 10 und der Ordnung 11 auch in $\mathbb{F}_{121}$?

Aufgabe 5.16. In dieser Aufgabe geht es um den Restklassenring $\mathbb{Z}/(360)$.

(a) Schreibe $\mathbb{Z}/(360)$ als Produktring (im Sinne des chinesischen Restsatzes).
(b) Wie viele Einheiten besitzt $\mathbb{Z}/(360)$?
(c) Schreibe das Element 239 in komponentenweiser Darstellung. Begründe, warum es sich um eine Einheit handelt und finde das Inverse in komponentenweiser Darstellung.
(d) Berechne die Ordnung von 239 in $\mathbb{Z}/(360)$.

Aufgabe 5.17. Zeige, dass die eulersche Funktion φ für natürliche Zahlen n, m die Eigenschaft

$$\varphi(\mathrm{ggT}(m,n)) \cdot \varphi(\mathrm{kgV}(m,n)) \;=\; \varphi(n) \cdot \varphi(m)$$

erfüllt.

Aufgabe 5.18. Es sei $\varphi(n)$ die Eulersche Funktion. Zeige die Abschätzung

$$\varphi(n) \geq \frac{\sqrt{n}}{2}.$$

In den nächsten Aufgaben werden die folgenden Begriffe verwendet.

Ein Element a eines kommutativen Ringes R heißt *nilpotent*, wenn $a^n = 0$ für eine natürliche Zahl n ist.

Ein Element e eines kommutativen Ringes heißt *idempotent*, wenn $e^2 = e$ gilt.

Aufgabe 5.19. Es sei $p \in \mathbb{Z}$ eine Primzahl und $n \in \mathbb{N}$. Zeige, dass der Restklassenring $\mathbb{Z}/(p^n)$ nur die beiden trivialen idempotenten Elemente 0 und 1 besitzt.

Aufgabe 5.20. Bestimme die nilpotenten Elemente, die idempotenten Elemente und die Einheiten von $\mathbb{Z}/(60)$.

Aufgabe 5.21.
(a) Finde die Zahlen $z \in \{0, 1, \ldots, 9\}$ mit der Eigenschaft, dass die letzte Ziffer ihres Quadrates (in der Dezimaldarstellung) gleich z ist.
(b) Finde die Zahlen $z \in \{0, 1, \ldots, 99\}$ mit der Eigenschaft, dass die beiden letzten Ziffern ihres Quadrates (in der Dezimaldarstellung) gleich z ist.

Aufgabe 5.22. Es sei R ein kommutativer Ring und es seien $f, g \in R$ nilpotente Elemente. Zeige, dass dann die Summe $f + g$ ebenfalls nilpotent ist.

Aufgabe 5.23. Es sei R ein kommutativer Ring und sei $f \in R$. Es sei f sowohl nilpotent als auch idempotent. Zeige, dass $f = 0$ ist.

Aufgabe 5.24. Es sei R ein kommutativer Ring und $f \in R$ ein nilpotentes Element. Zeige, dass $1 + f$ eine Einheit ist.

Aufgabe 5.25.
(a) Es sei K ein Körper. Zeige, dass die Einheitengruppe von K nicht zyklisch unendlich ist.
(b) Es sei R ein kommutativer Ring, dessen Charakteristik nicht zwei sei. Zeige, dass die Einheitengruppe von R nicht zyklisch unendlich ist.
(c) Beschreibe einen kommutativen Ring, dessen Einheitengruppe zyklisch unendlich ist.

Aufgaben zum Abgeben

Aufgabe 5.26. (3 Punkte)

Beweise die *eulersche Formel* für die eulersche Funktion, das ist die Aussage, dass

$$\varphi(n) = n \cdot \prod_{p|n,\ p \text{ prim}} \left(1 - \frac{1}{p}\right)$$

gilt.

Aufgabe 5.27. (5 Punkte)

Bestimme die nilpotenten Elemente, die idempotenten Elemente und die Einheiten in $\mathbb{Z}/(72)$.

Aufgabe 5.28. (3 Punkte)

Zeige, dass für natürliche Zahlen k und n mit $k \mid n$ der kanonische Homomorphismus

$$(\mathbb{Z}/(n))^\times \longrightarrow (\mathbb{Z}/(k))^\times$$

surjektiv ist.

Aufgabe 5.29. (4 Punkte)

Es sei n eine natürliche Zahl. Charakterisiere diejenigen Teiler k von n mit der Eigenschaft, dass für den kanonischen Ringhomomorphismus

$$\varphi\colon\ \mathbb{Z}/(n) \longrightarrow \mathbb{Z}/(k)$$

gilt, dass a in $\mathbb{Z}/(n)$ genau dann eine Einheit ist, wenn $\varphi(a)$ in $\mathbb{Z}/(k)$ eine Einheit ist.

Aufgabe 5.30. (3 Punkte)

Bestimme eine primitive Einheit $v \in \mathbb{Z}/(7)$ und ein Urbild $u \in \mathbb{Z}/(49)$ von v, das in $\mathbb{Z}/(49)$ nicht primitiv ist.

Aufgabe 5.31. (4 Punkte)

Es sei p eine fixierte Primzahl. Zu jeder ganzen Zahl $n \neq 0$ bezeichne $\nu_p(n)$ den Exponenten, mit dem die Primzahl p in der Primfaktorzerlegung von n vorkommt.

(a) Zeige: die Abbildung $\nu_p\colon\ \mathbb{Z} \setminus \{0\} \to \mathbb{N}$ ist surjektiv.
(b) Zeige: es gilt $\nu_p(nm) = \nu_p(n) + \nu_p(m)$.

(c) Finde eine Fortsetzung $\nu_p\colon \mathbb{Q}\setminus\{0\}\to\mathbb{Z}$ der gegebenen Abbildung, die ein Gruppenhomomorphismus ist (wobei $\mathbb{Q}^\times=\mathbb{Q}\setminus\{0\}$ mit der Multiplikation und $\mathbb{Z}$ mit der Addition versehen ist).
(d) Beschreibe den Kern des unter c) beschriebenen Gruppenhomomorphismus.

6. Vorlesung - Quadratreste

Der Charakterisierungssatz für zyklische Einheitengruppen

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. Bei $r=3$ ist dies eine direkte Berechnung. Generell ist für $r\geq 3$ die Abbildung

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

surjektiv (da genau die ungeraden Elemente die Einheiten sind). Da eine Restklassengruppe einer zyklischen Gruppe nach Aufgabe 4.21 wieder zyklisch ist, folgt, dass $(\mathbb{Z}/(2^r))^\times$ nicht zyklisch sein kann. □

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 5.11, Bemerkung 5.12 und der Isomorphie

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

Es sei also umgekehrt n mit der Eigenschaft gegeben, 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

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

führt. Da Restklassengruppen von zyklischen Gruppen wieder zyklisch sind, folgt nach Lemma 6.1, 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 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 nichtquadratischen Resten (häufig wird auch von quadratischen Nichtresten gesprochen).

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

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

gibt. Im anderen Fall heißt k ein *nichtquadratischer Rest* 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 nichtquadratischer Rest. 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 kennenlernen werden, und mit deren Hilfe man effektiver entscheiden kann, ob ein Quadratrest vorliegt oder nicht.

Beispiel 6.4. In $\mathbb{Z}/(11)$ sind die Zahlen $0, 1, 4, 9, 16 = 5, 25 = 3$ Quadratreste, die Zahlen $2, 6, 7, 8, 10$ sind nichtquadratische Reste.

Satz 6.5. *Es 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 Satz 4.13. □

Satz 6.6. *Es sei p eine ungerade Primzahl und sei $k \in \mathbb{Z}/(p^r)$. Dann gelten folgende Aussagen.*

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 den additiven Erzeuger 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, 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), ist auch die erste Komponente, also b_1, ein Vielfaches von 2 und so muss b insgesamt ein Vielfaches der 2 sein.

Es sei nun $k = p^s u$, $1 \leq s \leq r-1$, und zunächst angenommen, dass k ein Quadrat in $\mathbb{Z}/(p^r)$ ist. D.h wir können k als $k = x^2$ mit $x = p^t v$, schreiben, 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 6.7. *Es 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, sodass der Ringhomomorphismus

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

für $r \geq 3$ zeigt, dass die numerische Bedingung notwendig ist. Es 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

$$a = \pm 5^i.$$

schreiben. 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 6.8. *Es 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 5.3 ist die Einheitengruppe zyklisch der geraden Ordnung $p-1$. Identifiziert man $((\mathbb{Z}/(p))^\times, 1, \cdot)$ mit $(\mathbb{Z}/(p-1), 0, +)$, so entspricht -1 dem Element $\frac{p-1}{2}$, und -1 besitzt genau dann eine Quadratwurzel, wenn $\frac{p-1}{2}$ in $\mathbb{Z}/(p-1)$ ein Vielfaches von 2 ist. Dies ist aber genau dann der Fall, wenn $\frac{p-1}{2}$ selbst gerade ist, was zu $p = 1 \mod 4$ äquivalent ist. □

6. Arbeitsblatt

Übungsaufgaben

Aufgabe 6.1. Man gebe für die Einheitengruppe $(\mathbb{Z}/(16))^\times$ explizit einen Isomorphismus zu einem Produkt von (additiven) zyklischen Gruppen an.

Aufgabe 6.2. Welche Ziffern treten im Dezimalsystem als Endziffern von Quadratzahlen auf?

Aufgabe 6.3. Bestimme sämtliche quadratische Reste modulo der Primzahlen < 20.

Aufgabe 6.4. Es sei p eine Primzahl mit $p = 1 \mod 4$. Zeige unter Verwendung des Satzes von Wilson, dass $\frac{p-1}{2}!$ eine Quadratwurzel von -1 ist.

Aufgabe 6.5. Finde Quadratwurzeln für 2 modulo p für alle Primzahlen p mit $p = \pm 1 \mod 8$ und $p \leq 32$.

Aufgabe 6.6. Es sei p eine ungerade Primzahl. Zeige, dass eine primitive Einheit von $\mathbb{Z}/(p)$ nie ein quadratischer Rest ist. Bestimme für die Primzahlen ≤ 20, ob darin jeder nichtquadratische Rest primitiv ist.

Aufgabe 6.7. Finde die kleinste Primzahl p derart, dass es in $\mathbb{Z}/(p)$ ein Element a gibt, das weder primitiv noch ein Quadrat noch gleich -1 ist.

Aufgabe 6.8. Wie viele Quadrate und wie viele primitive Elemente besitzt $\mathbb{Z}/(31)$?

Wie viele Elemente besitzt $\mathbb{Z}/(31)$, die weder primitiv noch ein Quadrat sind?

Es sei x ein primitives Element von $\mathbb{Z}/(31)$. Liste explizit alle Elemente x^i auf, die weder primitiv noch ein Quadrat sind.

Aufgabe 6.9. Bestimme die Quadrate in $\mathbb{Z}/(35)$.

Aufgabe 6.10.

(1) Finde die kleinste Zahl n mit der Eigenschaft, dass es eine Zahl $k < n$ gibt, die selbst kein Quadrat ist, aber ein Quadratrest modulo n.
(2) Finde die kleinste Primzahl p mit der Eigenschaft, dass es eine Zahl $k < p$ gibt, die selbst kein Quadrat ist, aber ein Quadratrest modulo p.
(3) Finde die größte Primzahl p mit der Eigenschaft, dass die einzigen Quadratreste modulo p die Quadratzahlen $k < p$ sind.
(4) Untersuche
$$n = 8, 16, 32$$
in Hinblick auf die Eigenschaft, ob es neben den Quadraten noch weitere Quadratreste modulo n gibt.
(5) Finde die größte (?) Zahl n mit der Eigenschaft, dass die einzigen Quadratreste modulo n die Quadratzahlen $k < n$ sind.

Aufgabe 6.11. Bestätige Satz 6.6 für $\mathbb{Z}/(25)$.

Aufgaben zum Abgeben

Aufgabe 6.12. (3 Punkte)

Es sei n eine natürliche Zahl derart, dass $(\mathbb{Z}/(n))^\times$ zyklisch ist. Zeige, dass die Anzahl der primitiven Elemente gleich $\varphi(\varphi(n))$ ist, wobei φ die Eulersche Funktion bezeichnet. Wie groß ist deren Anzahl, wenn $(\mathbb{Z}/(n))^\times$ nicht zyklisch ist?

Aufgabe 6.13. (3 Punkte)

Es sei p eine Primzahl und $e \in \mathbb{N}$. Zeige, dass das Potenzieren

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

genau dann eine Bijektion ist, wenn e und $p-1$ teilerfremd sind.

Aufgabe 6.14. (2 Punkte)

Bestätige Satz 6.6 für $\mathbb{Z}/(27)$.

Aufgabe 6.15. (3 Punkte)

Es sei p eine Primzahl und $\mathbb{F}_p = \mathbb{Z}/(p)$ der zugehörige Restklassenkörper. Konstruiere Ringe

$$\mathbb{F}_p[\mathrm{i}] = \mathbb{F}_p \oplus \mathbb{F}_p\mathrm{i} = \{a + b\mathrm{i} \mid a, b \in \mathbb{F}_p\}$$

in der gleichen Weise, wie man die komplexen Zahlen definiert. Charakterisiere, für welche p diese Konstruktion einen Körper liefert.

7. Vorlesung - Das Quadratische Reziprozitätsgesetz I

Quadratische Reste modulo einer Primzahl

Modulo 2 ist jede Zahl ein quadratischer Rest. Für ungerade Primzahlen kann man ebenfalls sofort eine Aussage über die Anzahl der Quadratreste machen.

Satz 7.1. *Es 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“, sodass 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 aus genau 2 Elementen und damit besteht das Bild aus $\frac{p-1}{2}$ Elementen. □

Bemerkung 7.2. Wenn zu einer Primzahl p eine primitive Einheit $g \in (\mathbb{Z}/(p))^\times$ vorliegt, so hat man einen Gruppenisomorphismus

$$(\mathbb{Z}/(p-1), 0, +) \longrightarrow \big((\mathbb{Z}/(p))^\times, 1, \cdot\big),\, i \longmapsto g^i.$$

Dabei entsprechen die Quadrate rechts denjenigen Elementen links, die ein Vielfaches der 2 sind. Bei p ungerade besitzt die Hälfte der Elemente links diese Eigenschaft. Insbesondere ist ein Element $k \in (\mathbb{Z}/(p))^\times$ genau dann ein Quadratrest, wenn es von der Form

$$k = g^{2j}$$

ist.

Definition 7.3. 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. Für Vielfache von p definiert man manchmal das Legendre-Symbol ebenfalls, und zwar mit dem Wert 0.

Lemma 7.4. *Es 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. □

Die folgende Aussage heißt das *Euler-Kriterium* für quadratische Reste.

Satz 7.5. *Es 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 $\left(k^{\frac{p-1}{2}}\right)^2 = k^{p-1} = 1$ nach Lemma 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 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. □

Das Quadratische Reziprozitätsgesetz

Es 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 nichtquadratischer Rest ist.

Carl Friedrich Gauss (1777-1855)

Satz 7.6. *Es seien p und q verschiedene ungerade Primzahlen. Dann gilt:*

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

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

In Worten: Wenn p und q beide den Rest 3 modulo 4 haben, so ist p modulo q ein quadratischer Rest genau dann, wenn q modulo p ein nichtquadratischer Rest ist. In allen anderen Fällen ist p modulo q ein quadratischer Rest genau dann, wenn q modulo p ein quadratischer Rest ist.

Beispiel 7.7. Betrachten wir die beiden Primzahlen 11 und 19, die beide modulo 4 den Rest 3 haben. Es ist $19 = 8$ modulo 11 und dies ist nach Beispiel 6.4 kein Quadratrest. Gemäß dem Reziprozitätsgesetz muss also 11 modulo 19 ein quadratischer Rest sein. In der Tat ist

$$7^2 = 49 = 11 \mod 19.$$

Betrachtet man hingegen die Primzahlen 11 und 13, so hat 11 modulo 4 den Rest 3 und 13 hat modulo 4 den Rest 1. Es ist $13 = 2 \mod 11$ ein nichtquadratischer Rest, und daher ist auch 11 ein nichtquadratischer Rest modulo 13.

Die beiden folgenden Sätze werden die Ergänzungssätze zum quadratischen Reziprozitätsgesetz genannt, da sie klären, wann die -1 und wann die 2 quadratische Reste sind. In der algorithmischen Bestimmung von Quadratresten sind diese beiden Fälle ebenfalls unerlässlich.

Satz 7.8. *Für eine ungerade Primzahl p gilt:*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1\,, \text{ falls } p = 1 \mod 4\,, \\ -1\,, \text{ sonst (also bei } p = 3 \mod 4)\,. \end{cases}$$

Beweis. Die Gleichung von links und rechts wurde bereits in Satz 6.8 bewiesen. Die erste Gleichung ist auch ein Spezialfall von Satz 7.5 und die zweite Gleichung ist elementar. □

Satz 7.9. *Für eine ungerade Primzahl p gilt:*

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

Beweis. Dies wird weiter unten bewiesen. □

Die Elemente im Restklassenkörper $\mathbb{Z}/(p)$ werden zumeist durch die Zahlen von 0 bis $p-1$ repräsentiert. Für das Vorzeichenlemma von Gauß ist es sinnvoll, ein anderes Repräsentantensystem (für die von 0 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*

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

Beispiel 7.10. In $\mathbb{Z}/(11)$ ist $S_+ = \{1, 2, 3, 4, 5\}$ und $S_- = \{-1, -2, -3, -4, -5\}$. Für $k = 3$ muss man, um die Gaußschen Vorzeichen zu bestimmen, die ersten fünf Vielfachen berechnen und schauen, ob sie zur negativen oder zur positiven Hälfte gehören. Es ist

$$3 \in S_+,\ 6 = -5 \in S_-,\ 9 = -2 \in S_-,\ 12 = 1 \in S_+,\ 15 = 4 \in S_+\,,$$

die Vorzeichen sind also der Reihe nach

$$1, -1, -1, 1, 1\,.$$

Ihr Produkt ist 1, und mit dem folgenden Gaußschen Vorzeichenlemma folgt, dass 3 ein Quadratrest modulo 11 ist. In der Tat ist $3 = 5^2 \mod 11$.

Die folgende Aussage heißt *Gaußsches Vorzeichenlemma*.

Lemma 7.11. *Für eine ungerade Primzahl p und eine zu p teilerfremde Zahl k gilt mit den zuvor 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

$$\begin{aligned} t!k^t &= \left(\prod_{i=1}^t i\right)\left(\prod_{i=1}^t k\right) \\ &= \prod_{i=1}^t ik \\ &= \prod_{i=1}^t \epsilon_i s_i \\ &= \left(\prod_{i=1}^t \epsilon_i\right)\left(\prod_{i=1}^t s_i\right) \\ &= \left(\prod_{i=1}^t \epsilon_i\right) t! \mod p. \end{aligned}$$

Durch kürzen mit $t!$ (das ist eine Einheit) ergibt sich

$$k^t = \prod_{i=1}^t \epsilon_i \mod p,$$

und das Euler-Kriterium, 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 7.12. *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 Lemma 7.11 und müssen bestimmen, wie viele der Zahlen $2i$, $i = 1, \ldots, t = \frac{p-1}{2}$, in S_- liegen. Nun ist $2i \in S_-$ genau dann, wenn $2i > \frac{p-1}{2}$ ist (alle zu betrachtenden Vielfachen von 2 sind kleiner als p). Dies ist äquivalent zu $i > \frac{p-1}{4}$ und wir müssen das kleinste i mit dieser Eigenschaft finden. Ist $p-1$ ein Vielfaches von 4, so ist $\frac{p-1}{4}+1$ das kleinste i und insgesamt gibt es in diesem Fall

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

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

Es sei also nun $p = 3, 7 \mod 8$ bzw. $p = 3 \mod 4$. Dann ist das kleinste i derart, dass $i > \frac{p-1}{4}$ ist, gleich $\frac{p-1}{4} + \frac{1}{2}$, und es gibt insgesamt

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

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. □

7. Arbeitsblatt

Übungsaufgaben

Aufgabe 7.1. Es sei n eine ungerade Zahl. Zeige, dass es in $\mathbb{Z}/(n)$ maximal $\frac{n+1}{2}$ Quadratreste gibt. Wie sieht dies bei n gerade aus?

Aufgabe 7.2. Betrachte die Quadratrestgruppe

$$\mathbb{Q}^\times/\mathbb{Q}^{\times 2},$$

wobei $\mathbb{Q}^{\times 2}$ die Untergruppe der Quadrate bezeichne. Zeige, dass es zu jeder Restklasse $x \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ einen Repräsentanten aus $\mathbb{Z}$ gibt.

Aufgabe 7.3. Es sei K ein endlicher Körper mit $2 \neq 0$. Zeige, dass die Anzahl von K ungerade ist, und dass es in K genau $\frac{\#(K)+1}{2}$ Quadrate gibt.

Aufgabe 7.4. Es sei p eine ungerade Primzahl und sei k eine zu p teilerfremde natürliche Zahl. Es sei

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

die zu k gehörende Permutation auf der Einheitengruppe $(\mathbb{Z}/(p))^\times$ und $\operatorname{sgn}(\pi_k)$ das Signum dieser Permutation. Zeige

$$\left(\frac{k}{p}\right) = \operatorname{sgn}(\pi_k).$$

Aufgabe 7.5. Berechne zu $p = 13$ und $k = 3$ die Vielfachen $ik \mod 13$ für $i = 1, \ldots, 6$ und repräsentiere sie durch Zahlen zwischen -6 und 6. Berechne damit die Vorzeichen $\epsilon_i = \epsilon_i(3)$ und bestätige das Gaußsche Vorzeichenlemma an diesem Beispiel.

Aufgabe 7.6. Berechne zu $p = 17$ und $k = 5$ die Vielfachen $ik \mod 17$ für $i = 1, \ldots, 8$ und repräsentiere sie durch Zahlen zwischen -8 und 8. Berechne damit die Vorzeichen $\epsilon_i = \epsilon_i(5)$ und bestätige das Gaußsche Vorzeichenlemma an diesem Beispiel.

Aufgabe 7.7. Wie viele Lösungen hat die Gleichung

$$x^5 = a$$

in $\mathbb{Z}/(19)$ für ein gegebenes $a \in \mathbb{Z}/(19)$?

Aufgabe 7.8. Beweise mit Hilfe des Gaußschen Vorzeichenlemmas eine Modulobedingung für die ungeraden Primzahlen p mit der Eigenschaft, dass 3 ein Quadrat modulo p ist.

Aufgabe 7.9. Charakterisiere, für welche Primzahlen p die Zahl -2 ein Quadratrest modulo p ist.

Aufgabe 7.10. Finde die Lösungen der Kongruenz

$$6x^2 + 4x + 1 = 0 \mod 35.$$

Aufgaben zum Abgeben

Aufgabe 7.11. (7 (1+1+1+4) Punkte)

Für einen Körper K bezeichnet $K^{\times 2} \subseteq K^\times$ die Untergruppe aller Quadrate. Bestimme für die folgenden Körper die Restklassengruppe

$$K^\times / K^{\times 2}\,.$$

(1) K ist ein endlicher Körper.
(2) $K = \mathbb{R}$.
(3) $K = \mathbb{C}$.
(4) $K = \mathbb{Q}$.

Die folgende Aufgabe verallgemeinert das Eulersche Kriterium für beliebige Potenzreste.

Aufgabe 7.12. (4 Punkte)

Es sei p eine Primzahl und sei e eine natürliche Zahl. Zeige, dass ein Element $k \in (\mathbb{Z}/(p))^\times$ genau dann eine e-te Wurzel besitzt, wenn $k^{\frac{p-1}{e}} = 1$ ist.

Aufgabe 7.13. (3 Punkte)

Berechne zu $p = 23$ und $k = 8$ die Vielfachen $ik \mod 23$ für $i = 1, \ldots, 11$ und repräsentiere sie durch Zahlen zwischen -11 und 11. Berechne damit die Vorzeichen $\epsilon_i = \epsilon_i(8)$ und bestätige das Gaußsche Vorzeichenlemma an diesem Beispiel.

Aufgabe 7.14. (3 Punkte)

Beweise mit Hilfe des Gaußschen Vorzeichenlemmas eine Modulobedingung für die ungeraden Primzahlen p mit der Eigenschaft, dass 5 ein Quadrat modulo p ist.

Aufgabe 7.15. (4 Punkte)

Finde die Lösungen der Kongruenz

$$5x^2 + 5x + 4 = 0 \mod 91.$$

Aufgabe 7.16. (4 Punkte)

Zeige, dass im Restklassenring $\mathbb{Z}/(n)$ die Äquivalenz gilt, dass zwei Elemente a, b genau dann assoziiert sind, wenn $(a) = (b)$ ist.

Finde eine Charakterisierung für diese Äquivalenzrelation, die auf den Primfaktorzerlegungen von n, a und b aufbaut.

Die folgende Aufgabe setzt eine gewisse Routine im Umgang mit kommutativen Ringen voraus.

Aufgabe 7.17. (4 Punkte)

Man gebe ein Beispiel von zwei Elementen a und b eines kommutativen Ringes derart, dass $(a) = (b)$ ist, dass aber a und b nicht assoziiert sind.

8. Vorlesung - Das Quadratische Reziprozitätsgesetz II

Beweis des quadratischen Reziprozitätsgesetzes

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

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

Beweis. (1) Zur Berechnung von $\epsilon_i = \epsilon_i(k)$ muss man bestimmen, ob der betragsmäßig kleinste Repräsentant von $a = ki$ in $\mathbb{Z}/(p)$ positiv oder negativ ist. Dies hängt davon ab, ob a zu einem Intervall der Form $[\ell p, \ell p + \frac{p}{2}]$ oder der Form $[\ell p + \frac{p}{2}, (\ell+1)p]$ gehört (wobei die Ränder wegen den Voraussetzungen unproblematisch sind). Dies hängt davon ab, ob $\left\lfloor \frac{2a}{p} \right\rfloor$ gerade oder ungerade ist.

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

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

die Behauptung.

(3) Es 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 $\frac{(t+1)t}{2} = \frac{(p+1)}{2}\cdot\frac{(p-1)}{2}\cdot\frac{1}{2} = \frac{p^2-1}{8}$ folgt mit dem zweiten Ergänzungssatz 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. □

Wir können nun das quadratische Reziprozitätsgesetz beweisen.

Satz 8.2. *Es seien p und q verschiedene ungerade Primzahlen. Dann gilt:*

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

Beweis. Es sei $t = \frac{p-1}{2}$ und $u = \frac{q-1}{2}$. Nach Lemma 8.1 (3) gilt $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{S(p,q)+S(q,p)}$, sodass also $tu = S(p,q)+S(q,p)$ zu zeigen ist. Betrachte

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

Diese Menge besitzt tu Elemente. Es ist ferner $0 \notin M$, 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 $1 \leq j = \left\lfloor \frac{qi}{p} \right\rfloor$ der Fall ist. Zu jedem i, $1 \leq i \leq t$, gibt es also genau $\left\lfloor \frac{qi}{p} \right\rfloor$ Elemente in M_+. Damit hat M_+ genau

$$\sum_{i=1}^{t} \left\lfloor \frac{qi}{p} \right\rfloor = S(q,p)$$

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. Es 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. Es 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

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

Jetzt kann $\left(\frac{2}{q}\right)$ nach dem zweiten Ergänzungsgesetz 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, sodass 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 $13 = 5 \mod 8$ und dies das Vorzeichen -1 ergibt.

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 (der Rest $13 \mod 4$ 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 aus, 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:

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

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 $\mathbb{Z}/(13)$ 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

$$\begin{aligned}
\left(\frac{19}{127}\right) &= -\left(\frac{127}{19}\right) \\
&= -\left(\frac{13}{19}\right) \\
&= -\left(\frac{19}{13}\right) \\
&= -\left(\frac{6}{13}\right) \\
&= (-1)\left(\frac{2}{13}\right)\left(\frac{3}{13}\right) \\
&= (-1)(-1)\left(\frac{13}{3}\right) \\
&= (-1)(-1)\left(\frac{1}{3}\right) \\
&= (-1)(-1)1 \\
&= 1.
\end{aligned}$$

Setzt man alles zusammen, so ergibt sich

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

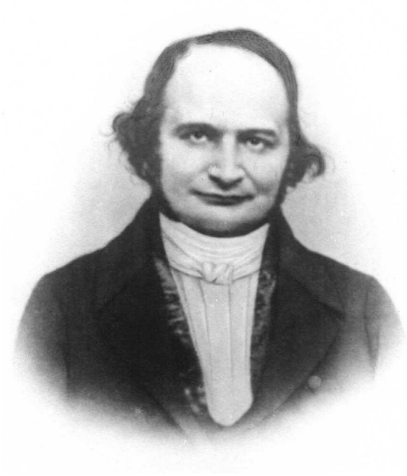
und damit die Erkenntnis, dass die obige Gleichung keine Lösung besitzt.

Das Jacobi-Symbol

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 modulo einer Primzahl ist oder nicht, ohne die Primfaktorzerlegungen der Zahlen, die bei der sukzessiven Anwendung des Reziprozitätsgesetzes auftreten, 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, wobei der Fall, dass k nicht teilerfremd zu n ist, ausdrücklich erlaubt ist. 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. Die Definition des Jacobi-Symbols nimmt Bezug auf die Primfaktorzerlegung von n, was wir eigentlich vermeiden wollten. Der Punkt ist aber, dass man das Jacobi-Symbol berechnen kann, auch wenn man die Primfaktorzerlegung gar nicht kennt.

Lemma 8.7. *Es 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 $\left(\frac{k_1k_2}{n}\right) = \left(\frac{k_1}{n}\right)\left(\frac{k_2}{n}\right)$.
(3) Es ist

$$\left(\frac{k}{n_1n_2}\right) = \left(\frac{k}{n_1}\right)\left(\frac{k}{n_2}\right).$$

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. *Es 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 Aufgaben bewiesen. □

Bemerkung 8.9. Es 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 (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, sodass man schließlich das Resultat erhält.

Wenn p eine Primzahl ist, so kann man mit diesem Algorithmus, also unter Verwendung des Jacobi-Symbols, entscheiden, ob k ein Quadratrest modulo p ist. In den Zwischenschritten braucht man nicht die Primfaktorzerlegungen auszurechnen.

8. Arbeitsblatt

Übungsaufgaben

Aufgabe 8.1. Berechne für $p = 17$ und $k = 5$ den Ausdruck

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

Berechne damit $\left(\frac{k}{p}\right)$ mit Hilfe von Lemma 8.1.

Aufgabe 8.2. Bestimme mit Hilfe des quadratischen Reziprozitätsgesetzes und seiner Zusätze, ob 17 ein quadratischer Rest modulo 19 ist, oder nicht.

Aufgabe 8.3. Bestimme mit Hilfe des quadratischen Reziprozitätsgesetzes und seiner Zusätze, ob 23 ein quadratischer Rest modulo 73 ist, oder nicht.

Aufgabe 8.4. Bestimme mit Hilfe des quadratischen Reziprozitätsgesetzes und seiner Zusätze, ob 50 ein quadratischer Rest modulo 83 ist, oder nicht.

Aufgabe 8.5. Berechne mit Hilfe des quadratischen Reziprozitätsgesetzes und seiner Ergänzungssätze das Legendre-Symbol

$$\left(\frac{563}{1231}\right).$$

Bemerkung: 563 und 1231 sind Primzahlen.

Aufgabe 8.6. Berechne mit Hilfe des quadratischen Reziprozitätsgesetzes und seiner Ergänzungssätze das Legendre-Symbol

$$\left(\frac{2333}{3673}\right).$$

Aufgabe 8.7. Berechne mit Hilfe des quadratischen Reziprozitätsgesetzes und seiner Ergänzungssätze das Legendre-Symbol

$$\left(\frac{1489}{2437}\right).$$

Aufgabe 8.8. Zeige, dass -3 genau dann ein Quadratrest modulo einer Primzahl $p \neq 2$ ist, wenn $p = 0, 1 \mod 3$ ist.

Aufgabe 8.9. Beschreibe mittels geeigneter Kongruenzbedingungen diejenigen ungeraden Primzahlen p mit der Eigenschaft, dass 7 ein Quadratrest modulo p ist.

Gibt es unendlich viele solche Primzahlen?

Aufgabe 8.10. Es sei n eine ungerade natürliche Zahl und sei k eine zu n teilerfremde Zahl, die modulo n ein Quadratrest ist. Zeige, dass für das Jacobi-Symbol

$$\left(\frac{k}{n}\right) = 1$$

gilt.

Aufgabe 8.11. Man gebe ein Beispiel an, wo das Jacobi-Symbol den Wert 1 hat, aber kein Quadratrest vorliegt.

Aufgabe 8.12. Suche für die folgenden zusammengesetzten Zahlen n eine zu n teilerfremde Zahl a derart, dass

$$a^{\frac{n-1}{2}} \neq \left(\frac{a}{n}\right)$$

in $\mathbb{Z}/(n)$ gilt.

(a) $n = 49$.
(b) $n = 75$.

Aufgabe 8.13. Zeige für eine positive ungerade Zahl n die Gleichung

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

Aufgaben zum Abgeben

Aufgabe 8.14. (4 Punkte)

Bestimme die Menge M der Reste modulo 40 mit der Eigenschaft, dass für jede ungerade Primzahl p gilt: 10 ist ein Quadratrest modulo p genau dann, wenn $p \mod 40$ zu M gehört.

Aufgabe 8.15. (5 Punkte)

Finde eine ungerade Primzahl p mit der Eigenschaft, dass alle Zahlen $a \leq 10$ Quadratreste modulo p sind.

Aufgabe 8.16. (3 Punkte)

Berechne mit Hilfe des quadratischen Reziprozitätsgesetzes und seiner Ergänzungssätze das Legendre-Symbol

$$\left(\frac{337}{1339}\right).$$

Aufgabe 8.17. (3 Punkte)

Zeige für eine positive ungerade Zahl n die Gleichung

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

Aufgabe 8.18. (3 Punkte)

Zeige für zwei ungerade positive Zahlen n und m die Beziehung

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

9. Vorlesung - Summe von Quadraten

Summe von zwei Quadraten - Primzahlen

In diesem Abschnitt werden wir die Frage beantworten, welche ganze Zahlen sich als 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 verwenden und schließen dabei an Vorlesung 2 an. Zunächst betrachten wir den Fall, wo $n = p$ eine ungerade Primzahl ist. Es gilt die folgende Charakterisierung.

Satz 9.1. *Es 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) Es ist $p = 1 \mod 4$.

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 ganzen 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 0 verschieden sind, ist $N(x + y\mathrm{i}) \geq 2$ und $x + y\mathrm{i}$ ist keine Einheit, also ist die Zerlegung nicht trivial. Da der Ring der Gaußschen Zahlen nach Lemma 2.12 euklidisch ist, sind nach Satz 3.5 prim und unzerlegbar äquivalent.

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

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

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

$$\begin{aligned} &\cong \mathbb{Z}[X]/(X^2+1,p) \\ &\cong (\mathbb{Z}/(p)[X])/(X^2+1). \end{aligned}$$

Dieser Restklassenring ist endlich und somit nach Aufgabe 1.14 genau dann ein Körper, wenn er ein Integritätsbereich ist. Dies ist wiederum äquivalent dazu, dass p prim in $\mathbb{Z}$[i] ist (man kann auch mit Satz 3.12 schließen). 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 $\mathbb{Z}/(p)$ besitzt, was bedeutet, dass -1 kein Quadrat in $\mathbb{Z}/(p)$ ist.

Die Äquivalenz (4) $\Leftrightarrow$ (5) wurde schon im Satz 6.8 gezeigt. □

Bemerkung 9.2. Es sei p eine Primzahl, die modulo 4 den Rest 1 besitzt, sodass es nach Satz 9.1 eine Darstellung von p 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 6.4).
(2) Die Abbildung $\mathbb{Z}$[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 $a-$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 $N(z) = p$. Eine Zerlegung $p = zw$ führt ja generell auf $N(z)N(w) = N(p) = p^2$. Mit $z = x + y\mathrm{i}$ gilt dann $p = x^2 + y^2$.

Beispiel 9.3. Es sei $p = 13$ (man sieht natürlich sofort eine Darstellung). Mit dem in Bemerkung 9.2 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 $(13, 5-\mathrm{i})$ in $\mathbb{Z}$[i]. Division in $\mathbb{Q}$[i] 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 in $\mathbb{Z}$[i]. Damit ist die Division mit Rest

$$13 = 2\cdot(5-\mathrm{i}) + r$$

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.

Bemerkung 9.4. Wenn für eine Primzahl p eine Darstellung

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

als Summe von zwei Quadraten bekannt ist, so kann man daraus einfach eine Quadratwurzel der -1 in $\mathbb{Z}/(p)$ finden. In diesem Fall gibt es einen surjektiven Ringhomomorphismus

$$\varphi\colon \mathbb{Z}[\mathrm{i}] \longrightarrow \mathbb{Z}[\mathrm{i}]/(x + \mathrm{i}y) \cong \mathbb{Z}/(p).$$

Die Isomorphie rechts rührt dabei von

$$\mathbb{Z} \longrightarrow \mathbb{Z}/(p) \longrightarrow \mathbb{Z}[\mathrm{i}]/(x + \mathrm{i}y)$$

her, wobei die Surjektivität darauf beruht, dass $\mathbb{Z}[\mathrm{i}]/(x + \mathrm{i}y)$ ein Körper ist und es in $\mathbb{Z}/(p)$ schon zwei Quadratwurzeln der -1 gibt. Die Eigenschaft

$$\mathrm{i}^2 = -1$$

überträgt sich auf das Bild, und dort gilt

$$\varphi(\mathrm{i}) = -x \cdot y^{-1}.$$

Beispiel 9.5. Wir wollen in $\mathbb{Z}/(29)$ eine Quadratwurzel für -1 mit Hilfe von Bemerkung 9.4 finden. Es ist

$$29 = 5^2 + 2^2 = (5 + 2\mathrm{i})(5 - 2\mathrm{i}).$$

Im Restklassenkörper

$$\mathbb{Z}[\mathrm{i}]/(5 + 2\mathrm{i}) \cong \mathbb{Z}/(29)$$

ist

$$\mathrm{i} = -5 \cdot 2^{-1} = -5 \cdot 15 = -75 = 12.$$

In der Tat ist

$$12^2 = 144 = -1 \mod 29$$

Primfaktorzerlegung für Gausssche Zahlen

Aus Satz 9.1 können wir problemlos ableiten, wie sich die Primzahlen in $\mathbb{Z}[\mathrm{i}]$ verhalten:

Korollar 9.6. *Die Primzahlen aus $\mathbb{Z}$ haben in $\mathbb{Z}[\mathrm{i}]$ folgendes Zerlegungsverhalten.*

(a) Es ist

$$2 = -\mathrm{i}(1 + \mathrm{i})^2,$$

und $1 + \mathrm{i}$ ist prim in $\mathbb{Z}[\mathrm{i}]$.

(b) Für $p = 1 \mod 4$ ist

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

mit gewissen eindeutig bestimmten $x, y \in \mathbb{N}_+$, wobei beide Faktoren prim sind.

(c) Für $p = 3 \mod 4$ ist p prim in $\mathbb{Z}[\mathrm{i}]$.

Beweis. Aufgrund von Satz 9.1 gibt es im zweiten Fall eine Darstellung

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

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 2.13 prim. Die Eindeutigkeit ergibt sich aus der eindeutigen Primfaktorzerlegung im Ring der Gaußschen Zahlen und der Kenntnis der Einheiten. □

Bemerkung 9.7. Für eine Gaußsche Zahl $z \in \mathbb{Z}[\mathrm{i}]$ 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 2.13 das Element z selbst prim.
(2) Bestimme die (ganzzahligen) Primfaktoren von $N(z)$. Schreibe

$$N(z) = z\overline{z} = 2^r p_1 \cdots p_s q_1 \cdots q_t,$$

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 $2^r = (-\mathrm{i})^r(1 + \mathrm{i})^{2r}$. Damit ist

$$z\overline{z} = (-\mathrm{i})^r(1 + \mathrm{i})^{2r} u_1\overline{u_1} \cdots u_s\overline{u_s} q_1 \cdots q_t.$$

(4) Liste die möglichen Primfaktoren von z (und zugleich von $\overline{z}$) auf: das sind $1 + \mathrm{i}$ (falls 2 mit positivem Exponenten vorkommt), die u_i und $\overline{u_i}$ sowie die q_j (da $\mathbb{Z}[\mathrm{i}]$ ein Hauptidealbereich ist und somit nach Satz 3.7 die eindeutige Primfaktorzerlegung gilt, setzt sich die Primfaktorzerlegung von z und von $\overline{z}$ bis auf Einheiten aus Primfaktoren der rechten Seite zusammen).
(5) Durch $(1 + \mathrm{i})^r$ und die q_j kann man sofort durchdividieren, da diese Faktoren jeweils sowohl von z als auch von $\overline{z}$ ein Faktor sind.
(6) Für die möglichen Primfaktoren u_i und $\overline{u_i}$ muss man (durch Division mit Rest) überprüfen, ob sie Primfaktoren von z sind oder nicht (wenn nicht, so teilen sie $\overline{z}$). Statt Division kann man auch die möglichen Kombinationen ausmultiplizieren.

Beispiel 9.8. Es ist

$$N(17 + 13\mathrm{i}) = 17^2 + 13^2 = 289 + 169 = 458 = 2 \cdot 229,$$

wobei 229 eine Primzahl ist. Wegen

$$229 = 225 + 4 = 15^2 + 2^2$$

besitzt 229 in $\mathbb{Z}[\mathrm{i}]$ die Primfaktorzerlegung

$$229 = (15 + 2\mathrm{i})(15 - 2\mathrm{i})$$

und somit ergibt sich die Primfaktorzerlegung

$$17 + 13\mathrm{i} \;=\; (1+\mathrm{i})(15-2\mathrm{i}).$$

Summe von zwei Quadraten

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

Lemma 9.9. *(a) $2 = 1+1$ ist eine Summe von zwei Quadraten.*

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

(c) Ist $n = r^2m$, und ist m eine Summe von zwei 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 9.10. *Es sei n eine positive natürliche Zahl. Wir schreiben $n = r^2m$, 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 Lemma 9.9 und nach Satz 9.1 die Summe zweier Quadrate. Es sei umgekehrt angenommen, dass n die Summe zweier Quadrate ist, sodass also eine Zerlegung $n = (x+\mathrm{i}y)(x-\mathrm{i}y)$ vorliegt. Es 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. □

Beispiel 9.11. Nach Satz 9.10 ist

$$1000 \;=\; 100 \cdot 2 \cdot 5$$

eine Summe von zwei Quadraten und

$$108 \;=\; 36 \cdot 3$$

keine Summe von zwei Quadraten.

Summe von drei und von vier Quadraten

Die beiden folgenden Sätze heißen *Dreiquadratesatz* bzw. *Vierquadratesatz* (oder Satz von Lagrange).

Satz 9.12. *Eine natürliche Zahl n lässt sich genau dann als Summe von drei Quadratzahlen darstellen, wenn n* nicht *die Form*

$$4^i(8j+7)$$

mit $i, j \in \mathbb{N}$ besitzt.

Satz 9.13. *Jede natürliche Zahl lässt sich als Summe von vier Quadratzahlen darstellen.*

Das Waringsche Problem ist die Frage, ob man für jeden Exponenten k eine Zahl g mit der Eigenschaft finden kann, dass jede natürliche Zahl eine Darstellung als Summe von maximal g (nichtnegativen) k-ten Potenzen besitzt. Bei $k = 2$ ist $g = 4$. Dieses Problem wurde von Hilbert positiv gelöst. Beispielsweise kann man jede natürliche Zahl als Summe von 9 Kuben darstellen. Für 23 braucht man wirklich 9 Kuben. Man weiß ferner, dass man bis auf endlich viele Ausnahmen jede Zahl als eine Summe von sieben Kubikzahlen schreiben kann, und vermutet sogar, dass man bis auf endlich viele Ausnahmen jede Zahl als eine Summe von nur vier Kubikzahlen schreiben kann. Die 7373170279850 ist die größte bekannte Zahl, die man nicht als Summe von vier Kubikzahlen darstellen kann.

9. Arbeitsblatt

Übungsaufgaben

Aufgabe 9.1. Zeige, dass eine Primzahl p höchstens eine Darstellung als Summe von zwei Quadraten besitzt.

Aufgabe 9.2. Zeige, dass eine ganze Zahl n genau dann die Differenz zweier Quadratzahlen ist, wenn der Exponent von 2 in der Primfaktorzerlegung von n gleich 0 oder ≥ 2 ist.

Aufgabe 9.3. Bestimme für eine oder mehrere Gaußsche Zahlen in diesem Diagramm die Primfaktorzerlegung und trage das Ergebnis (mit Begründung) in den vorgesehenen Link ein. Man beschränke sich dabei auf Zahlen unterhalb der Hauptdiagonalen.

Die Gitterpunkte im farbig hinterlegten Bereich und entlang seines Randes sind als Link anklickbar. Gaußsche Ebene, 1. Quadrant

Aufgabe 9.4. Bestimme in $\mathbb{Z}[i]$ die Primfaktorzerlegung von $8-i$. Begründe, warum die Faktoren prim sind.

Aufgabe 9.5. Zeige, dass die komplexen Zahlen $\mathbb{C}$ die Restklassendarstellung

$$\mathbb{C} \cong \mathbb{R}[X]/(X^2+1)$$

besitzen.

Aufgabe 9.6. Zeige, dass der Ring der Gaußschen Zahlen $\mathbb{Z}[\mathrm{i}]$ die Restklassendarstellung

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

besitzt.

Aufgabe 9.7. Es sei $n \in \mathbb{N}_+$. Zeige, dass der Restklassenring $\mathbb{Z}[\mathrm{i}]/(n)$ genau n^2 Elemente besitzt.

Aufgabe 9.8. Es sei R ein kommutativer Ring und sei $\mathfrak{a}$ ein Ideal mit dem Restklassenring $S = R/\mathfrak{a}$. Zu einem Ideal $I \subseteq R$ welches $\mathfrak{a}$ enthält, sei $I' = IR/\mathfrak{a}$ das zugehörige Ideal in S. Zeige, dass es eine kanonische Ringisomorphie

$$R/I \cong S/I'$$

gibt.

Aufgabe 9.9. Es sei R ein kommutativer Ring und sei $\mathfrak{a}$ ein Ideal mit dem Restklassenring

$$S = R/\mathfrak{a}.$$

Zeige, dass die Ideale von S eindeutig denjenigen Idealen von R entsprechen, die $\mathfrak{a}$ umfassen.

Aufgabe 9.10. Bestimme mit Hilfe von Bemerkung 9.4 eine Quadratwurzel von -1 in $\mathbb{Z}/(41)$.

Aufgabe 9.11. Zu einer natürlichen Zahl n bezeichne $r(n)$ die Anzahl der Möglichkeiten, sie als Summe von zwei Quadratzahlen darzustellen, d.h. $r(n)$ ist die Anzahl der 2-Tupel

$$(x_1, x_2) \in \mathbb{Z}^2 \text{ mit } x_1^2 + x_2^2 = n.$$

Beweise die Beziehung

$$r(2n) = r(n).$$

Zeige, dass die vorstehende Aussage nicht gilt, wenn man nur Lösungen in $\mathbb{N}^2$ betrachtet.

Aufgabe 9.12. Zu einer natürlichen Zahl n bezeichne $r(n)$ die Anzahl der Möglichkeiten, sie als Summe von vier Quadratzahlen darzustellen, d.h. $r(n)$ ist die Anzahl der 4-Tupel

$$(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4 \text{ mit } x_1^2 + x_2^2 + x_3^2 + x_4^2 = n.$$

Es sei u eine ungerade positive Zahl. Beweise die Beziehung

$$r(2u) \ = \ 3r(u).$$

Zeige, dass die vorstehende Aussage nicht gilt, wenn man nur Lösungen in $\mathbb{N}^4$ betrachtet.

Aufgabe 9.13. Es sei n eine natürliche Zahl, die modulo 8 den Rest 7 besitzt. Zeige, dass n nicht als Summe von drei Quadraten darstellbar ist.

Aufgabe 9.14. Bestimme für jede natürliche Zahl $n \leq 30$, ob sie sich als eine Summe von drei Quadratzahlen darstellen lässt.

Aufgabe 9.15. Bestimme für jede natürliche Zahl $n \leq 10$, auf wie viele verschiedene Arten sie sich als Summe von vier Quadratzahlen darstellen lässt, d.h. man bestimme die Anzahl der 4-Tupel

$$(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4 \text{ mit } x_1^2 + x_2^2 + x_3^2 + x_4^2 = n.$$

Aufgaben zum Abgeben

Aufgabe 9.16. (3 Punkte)

Bestimme für die Zahlen n zwischen 155 und 159, ob n die Summe von zwei ganzzahligen Quadraten ist. Man gebe alle möglichen Darstellungen an.

Aufgabe 9.17. (2 Punkte)

Finde für alle Zehnerpotenzen ≥ 10 eine Darstellung als Summe von zwei positiven Quadraten.

Aufgabe 9.18. (3 Punkte)

Bestimme die Primfaktorzerlegung der Gaußschen Zahl $39 + 52\mathrm{i}$.

Aufgabe 9.19. (4 Punkte)

Es sei n eine natürliche Zahl, in deren Primfaktorzerlegung r Faktoren vorkommen. Wie viele Darstellungen als Summe von zwei Quadratzahlen besitzt n maximal?

Aufgabe 9.20. (4 Punkte)

Zeige: In $\mathbb{Z}/(p)$, wobei p eine Primzahl ist, lässt sich jedes Element als Summe von zwei Quadraten schreiben.

Aufgabe 9.21. (3 Punkte)

Es sei p eine Primzahl mit $p = 1 \mod 4$ und sei $p = x^2+y^2$ eine Darstellung als Summe von zwei Quadraten, $x, y \in \mathbb{N}$. Es sei k ein ungerader Teiler von x. Zeige: Dann ist k ein Quadratrest modulo p.

Aufgabe 9.22. (3 Punkte)

Zeige, dass man die 239 als eine Summe von neun Kubikzahlen darstellen kann, aber nicht als eine Summe von acht Kubikzahlen.

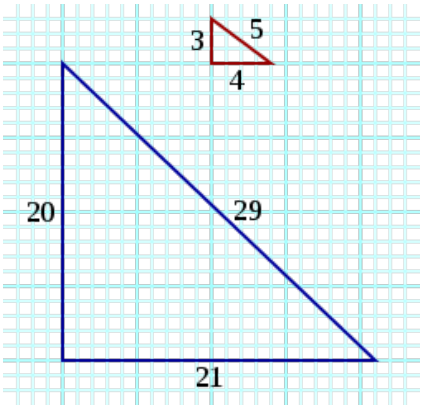
10. Vorlesung - Pythagoreische Tripel

Pythagoreische Tripel

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

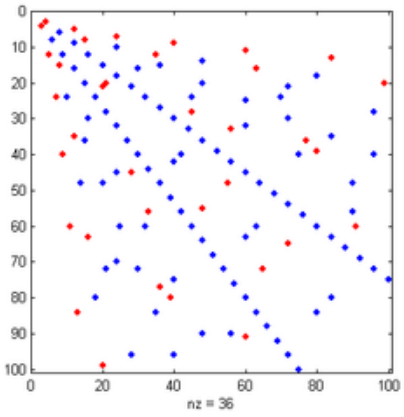
$$x^2 + y^2 = z^2.$$

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



Bemerkung 10.2. Lösungstripel, bei denen (mindestens) ein Eintrag 0 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 Katheten und z ist die Seitenlänge der Hypotenuse). 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

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

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

$$0 \;=\; (x^2-1) + t^2(x+1)^2 \;=\; (x+1)\big((x-1) + t^2(x+1)\big).$$

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

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

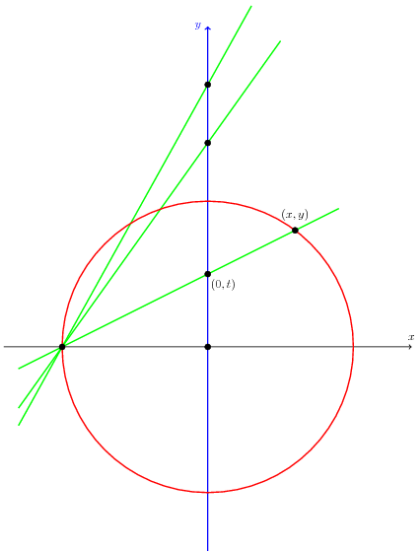
die zu

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

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 Aufgabe 10.4 zu beweisen. □

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

Beweis. Die Parametrisierung

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

ist stetig, da sie komponentenweise durch rationale Funktionen gegeben ist. Es sei $s \in S^1$ ein Punkt des Einheitskreises. Der Punkt $(-1,0)$ (der Punkt, der von der Parametrisierung nicht erfasst wird), ist selbst rational. Es sei also $s \neq (-1,0)$ und sei $t \in \mathbb{R}$ eine reelle Zahl mit $\varphi(t) = s$. Es 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. □

Die Formeln des folgenden Satzes zur Berechnung der pythagoreischen Tripel heißen auch *indische Formeln.*

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

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

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

Beweis. Es sei (x,y,z) ein pythagoreisches Tripel. Der Fall $z = 0$ ist ausgeschlossen. Dann ist $\left(\frac{x}{z},\, \frac{y}{z}\right)$ 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

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

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

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

Sei $t = \frac{u}{v}$ mit ganzen teilerfremden Zahlen $u, v,\ v > 0$. Wir ersetzen q durch

$$\tilde{q} = \frac{q}{v^2}$$

und haben dann

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

Da u und v teilerfremd sind, sind auch u, v, v^2-u^2 paarweise teilerfremd. Ein Primteiler des Nenners von $\tilde{q}$ teilt $2uv$ und v^2-u^2. Daher kommt nur 2 in Frage. In diesem Fall wären aber v^2-u^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. □

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

Beispiel 10.7. Wenn man einen rationalen Punkt auf dem Einheitskreis sucht, der möglichst nahe an dem irrationalen Punkt $\left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right)$ liegen soll, so kann man

$$t = \frac{\frac{1}{\sqrt{2}}}{1+\frac{1}{\sqrt{2}}} = \frac{1}{1+\sqrt{2}} = 0,414213...$$

berechnen. Die rationale Approximation

$$t' = \frac{414213}{1000000}$$

führt zum rationalen Punkt

$$\left(\frac{828427590631}{1171572409369}, \frac{828426000000}{1171572409369}\right)$$

auf dem Einheitskreis und zum pythagoreischen Tripel

$$\begin{aligned} x &= v^2 - u^2 \\ &= 1000000^2 - 414213^2 \\ &= 1000000000000 - 171572409369 \\ &= 828427590631, \end{aligned}$$

$$y = 2 \cdot 414213 \cdot 1000000 = 828426000000$$

und

$$\begin{aligned} z &= u^2 + v^2 \\ &= 414213^2 + 1000000^2 \\ &= 1171572409369. \end{aligned}$$

In der Tat ist

$$\begin{aligned} & 828427590631^2 + 828426000000^2 \\ = \; & 686292272918683718978161 + 686289637476000000000000 \\ = \; & 1372581910394683718978161 \\ = \; & 1171572409369^2, \end{aligned}$$

wie man unmittelbar nachrechnet.

Höhere Fermat-Gleichungen

Die folgende Aussage heißt *Satz von Euler*.

Satz 10.8. *Die diophantische Gleichung*

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

hat keine ganzzahlige nichttriviale Lösung.

Beweis. Es 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 positiven 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 also 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 10.9. *Die Fermat-Quartik*

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

besitzt keine ganzzahlige nichttriviale Lösung.

Beweis. Dies folgt sofort aus dem Satz von Euler. □

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 10.10. *Die diophantische Gleichung*

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

besitzt für kein $n \geq 3$ eine ganzzahlige nichttriviale Lösung.

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

10. Arbeitsblatt

Übungsaufgaben

Aufgabe 10.1. Es seien x und y ungerade. Zeige, dass $x^2 + y^2$ keine Quadratzahl ist.

Aufgabe 10.2. Es sei (x, y, z) ein pythagoreisches Tripel. Zeige, dass x oder y ein Vielfaches von 3 ist.

Aufgabe 10.3. (a) Man gebe ein Beispiel für rationale Zahlen $a, b, c \in]0, 1[$ mit

$$a^2 + b^2 = c^2.$$

(b) Man gebe ein Beispiel für rationale Zahlen $a, b, c \in]0, 1[$ mit

$$a^2 + b^2 \neq c^2.$$

(c) Man gebe ein Beispiel für irrationale Zahlen $a, b \in]0,1[$ und eine rationale Zahl $c \in]0,1[$ mit

$$a^2 + b^2 = c^2.$$

Aufgabe 10.4. Zeige, dass die in Satz 10.4 beschriebene rationale Parametrisierung des Einheitskreises injektiv ist.

Aufgabe 10.5. Skizziere ein Dreieck D derart, dass eine Höhe das Dreieck D in zwei verschiedene rechtwinklige Dreiecke D_1 und D_2 unterteilt so, dass die Seitenlängen von D_1 und D_2 jeweils pythagoreische Tripel bilden. Man gebe die Seitenlängen an.

Aufgabe 10.6. Zeige, dass die Menge

$$S^1_{\mathbb{Q}} = \{z \in \mathbb{Q}[\mathrm{i}] \mid |z| = 1\}$$

mit der Multiplikation in $\mathbb{Q}[\mathrm{i}]$ eine kommutative Gruppe ist.

Aufgabe 10.7. Es sei

$$S^1_{\mathbb{Q}} = \{z \in \mathbb{Q}[\mathrm{i}] \mid |z| = 1\}$$

der rationale Einheitskreis mit der aus $\mathbb{Q}[\mathrm{i}]^\times$ ererbten Gruppenstruktur. Berechne die ersten vier Potenzen von $\frac{3}{5} + \frac{4}{5}\mathrm{i} \in S^1_{\mathbb{Q}}$.

Aufgabe 10.8. Zeige, dass der Einheitskreis

$$S^1_{\mathbb{R}} = \{z \in \mathbb{R}[\mathrm{i}] \cong \mathbb{C} \mid |z| = 1\}$$

isomorph zu $\mathbb{R}/\mathbb{Z}$ ist.

Aufgabe 10.9. Es sei

$$n = r^2 + s^2 = (r + \mathrm{i}s)(r - \mathrm{i}s)$$

eine Summen von zwei Quadraten mit der zugehörigen Zerlegung in $\mathbb{Z}[\mathrm{i}]$. Berechne n^2 auf zwei verschiedene Weisen und zeige damit, dass

$$\frac{r^2 - s^2 + 2rs\mathrm{i}}{n}$$

ein Punkt auf dem rationalen Einheitskreis ist.

Aufgabe 10.10. Zeige, dass der rationale Einheitskreis (als Gruppe) nicht endlich erzeugt ist.

Aufgabe 10.11. Zeige, dass die beiden kommutativen Gruppen $(\mathbb{Q}, 0, +)$ und $(\mathbb{Q}_+, 1, \cdot)$ nicht isomorph sind.

Aufgabe 10.12. Zeige, dass der Gruppenhomomorphismus

$$\mathbb{Q}[\mathrm{i}]^\times \longrightarrow (\mathbb{Q}_+, 1, \cdot),\ x + \mathrm{i}y \longmapsto x^2 + y^2,$$

nicht surjektiv ist.

Aufgabe 10.13. Zeige mit Hilfe des pythagoreischen Tripels $(9, 40, 41)$, dass es ein rechtwinkliges Dreieck gibt, dessen Seitenlängen alle rational sind und dessen Flächeninhalt gleich 5 ist.

Aufgabe 10.14. Zeige, dass es kein rechtwinkliges Dreieck gibt, dessen Seitenlängen alle rational sind und dessen Flächeninhalt gleich 2 ist.

Aufgabe 10.15. Zeige mit Hilfe der Aussage, dass $x^4 - y^4 = z^2$ keine ganzzahlige nichttriviale Lösung besitzt, dass es kein rechtwinkliges Dreieck gibt, dessen Seitenlängen alle rational sind und dessen Flächeninhalt gleich 1 ist.

Aufgabe 10.16. Zeige, dass die quadratische Gleichung

$$x^2 - 5y^2 = 2$$

keine ganzzahlige Lösung besitzt.

Aufgabe 10.17. Zeige, dass in $\mathbb{Z}/(29)$ die Gleichung

$$x^4 + y^4 + z^4 = 0$$

nur die triviale Lösung $(0, 0, 0)$ besitzt.

Aufgabe 10.18. Finde eine nichttriviale ganzzahlige Lösung für das Gleichungssystem $ab = c$ und $(a-1)d = c-1$.

Aufgabe 10.19. Finde mindestens eine ganzzahlige Lösung $(x, y) \in \mathbb{N}_+ \times \mathbb{N}_+$ für die diophantische Gleichung

$$x^k + 1 = y^n$$

für $k, n \geq 2$.

Aufgabe 10.20. Zeige: Um den Satz von Wiles für alle Exponenten $n \geq 3$ zu zeigen, genügt es, ihn für alle ungeraden Primzahlen als Exponenten zu beweisen.

Aufgabe 10.21. Zeige unter Verwendung des Satzes von Wiles, dass die diophantische Gleichung

$$x^n + y^n + z^n = 0$$

für $n \geq 2$ keine von $(0,0,0)$ verschiedene Lösung besitzt.

Aufgabe 10.22. Bestätige die folgenden Identitäten.

(1)
$$1 + 2^3 = 3^2.$$

(2)
$$2^5 + 7^2 = 3^4.$$

(3)
$$13^2 + 7^3 = 2^9.$$

Aufgabe 10.23. Bestätige die folgende Identität.

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5.$$

Aufgabe 10.24. Bestätige die Gleichung

$$(-2 + \mathrm{i})^3 + (-2 - \mathrm{i})^3 = (1 + \mathrm{i})^4.$$

Aufgaben zum Abgeben

Aufgabe 10.25. (4 Punkte)

Es sei

$$S^1_{\mathbb{Q}} = \{z \in \mathbb{Q}[\mathrm{i}] \mid |z| = 1\}$$

der rationale Einheitskreis mit der aus $\mathbb{Q}[\mathrm{i}]^\times$ ererbten Gruppenstruktur. Zeige, dass die Gruppen $S^1_{\mathbb{Q}}$ und $\mathbb{Q}/\mathbb{Z}$ nicht isomorph sind.

Aufgabe 10.26. (3 Punkte)

Bestimme in $\mathbb{Z}/(11)$ alle Lösungen (x, y) der Gleichung

$$x^2 + y^2 = 1.$$

Aufgabe 10.27. (4 Punkte)

Bestimme in $\mathbb{Z}/(7)$ alle Lösungen (x, y) der diophantischen quadratischen Gleichung

$$3x^2 + 2y^2 + 5xy + 4x + 8y + 6 = 0.$$

Aufgabe 10.28. (4 Punkte)

Approximiere die (obere) primitive dritte Einheitswurzel auf dem rationalen Einheitskreis mit einem Fehler von maximal 1/1000000.

11. Vorlesung - Primzahlen und ihre Verteilung I

´

Die Unendlichkeit der Primzahlen

Satz 11.1. *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

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

Diese Zahl ist durch keine der Primzahlen p_i teilbar, da bei Division von N durch p_i immer ein Rest 1 verbleibt. Damit sind die Primfaktoren von N, die es nach Korollar 3.9 geben muss, nicht in der Ausgangsmenge enthalten - Widerspruch. □

Eine Liste aller Primzahlen ≤ 100000 findet sich hier.

Kann man über Satz 11.1 hinaus weitere und feinere Aussagen darüber machen, wie viele 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 (und zwar nach Korollar 23.11 (Maß- und Integrationstheorie (Osnabrück 2022-2023)) gegen $\frac{\pi^2}{6}$), es gibt also in einem 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 $\operatorname{Re}(s) > 1$ durch

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

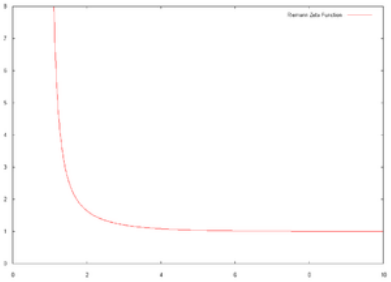
definiert.

Für den Nachweis der Konvergenz der riemannschen Zetafunktion siehe Kurs:Analysis (Osnabrück 2021-2023)/Teil II/Vorlesung 31. Wir erinnern an die Konvergenz der geometrischen Reihe.

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

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

Beweis. Dies wird in der Grundvorlesung Analysis bewiesen, siehe Kurs:Analysis (Osnabrück 2021-2023)/Teil I/Vorlesung 9. □



Lemma 11.4. *Es sei T eine endliche Menge von Primzahlen und sei s eine komplexe Zahl mit* $\operatorname{Re}(s) > 0$. *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. Es sei $T = \{p_1, \ldots, p_k\}$. Es ist $|p^{-s}| < 1$ nach Voraussetzung über den Realteil. Unter Verwendung von Satz 11.3 und Lemma 15.2 (Analysis (Osnabrück 2021-2023)) ergibt sich

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

□

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. Es wäre dann $M(T) = \mathbb{N}$. 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. *Es sei s eine komplexe Zahl mit* $\operatorname{Re}(s) > 1$. *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 Menge der 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 Lemma 11.4 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 nach Beispiel 9.3 (Analysis (Osnabrück 2021-2023)) divergiert. Also divergiert auch das Produkt links. □

Wir können nun die oben formulierte Frage beantworten.

Satz 11.7. *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

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

Die Potenzreihenentwicklung des natürlichen Logarithmus ist

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

für $|x| < 1$. Angewendet auf den vorstehenden Ausdruck ergibt das

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

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 die geometrische Reihe benutzt wurde. Damit ist insgesamt

$$\sum_{i=1}^{k} \left(\sum_{j=2}^{\infty} \frac{(p_i^{-1})^j}{j}\right) \leq \sum_{i=1}^{k} \frac{2}{p_i^2} \leq 2 \sum_{n\in\mathbb{N}_+} \frac{1}{n^2}.$$

Da die Summe der reziproken Quadrate nach Beispiel 9.12 (Analysis (Osnabrück 2021-2023)) 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

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

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.

Bemerkung 11.9. Die Frage, ob es unendlich viele Primzahlzwillinge gibt, besitzt verschiedene schwächere Varianten. Man kann sich zum Beispiel fragen, ob es unendlich oft vorkommt, dass es in einem Zehnerintervall zwei Primzahlen gibt, oder dass es in einem Hunderterintervall zwei Primzahlen gibt, und so weiter. Die ersten Primzahlen vermitteln dabei ein Bild, dass Primzahlen ziemlich häufig sind. Sie werden aber zunehmend seltener, sodass es für hohe Hunderterintervalle, sagen wir für die Zahlen von

$$1000000000000000 \text{ bis } 1000000000000100$$

ziemlich unwahrscheinlich ist, eine Primzahl zu enthalten, geschweige denn zwei Primzahlen. Bis vor 2013 war es nicht bekannt, ob es überhaupt eine Zahl m mit der Eigenschaft gibt, dass es unendlich viele Intervalle der Länge m gibt, die zwei Primzahlen enthalten ($m = 2$ wäre die positive Lösung des Primzahlzwillingsproblems). Im Jahr 2013 bewies Zhang Yitang, dass man $m = 70000000$ nehmen kann, dass es also unendlich viele Intervalle der Form

$$[k, k+70000000]$$

gibt, in denen zwei Primzahlen liegen. Dieses Resultat ist ein Durchbruch in der Primzahlzwillingforschung, da es erstmals zeigt, dass sich Primzahlen unendlich oft „ziemlich nahe“ kommen. Zwischenzeitlich wurde die Schranke von 70000000 auf 252 gesenkt, siehe http://arxiv.org/pdf/1402.4849v2.pdf.

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, die folgende Funktion einzuführen, die *Primzahlfunktion* genannt wird.

Definition 11.10. Die für $x \in \mathbb{R}$ definierte Funktion

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

heißt *Primzahlfunktion*.

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

Jacques Salomon Hadamard (1865 Versailles - 1963 Paris)

Bemerkung 11.11. Die Primzahlfunktion zählt also, wie viele 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.

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.

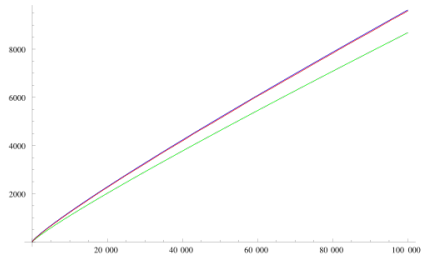
Satz 11.12. *Es gilt die asymptotische Abschätzung*

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

Das heißt

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

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



Den Primzahlsatz kann man auch so verstehen, dass die Wahrscheinlichkeit, dass eine Zahl in der Größenordnung x eine Primzahl ist, gleich $\frac{1}{\ln x}$ ist. In der Tat ist sogar das Integral dazu, also der sogenannte *Integrallogarithmus* $\mathrm{Li}(x) = \int_2^x \frac{1}{\ln t} dt$, eine bessere Approximation für $\pi(x)$ als $x/\ln x$. Für $x = 1000000$ ist $\pi(x) = 78498$, $\mathrm{Li}(x) = 78628$ und $\frac{x}{\ln x} = 72382$ (die beiden letzten Werte gerundet).

Peter Gustav Lejeune Dirichlet (1805-1859)

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

Satz 11.13. *Es 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. □

Generationenübergreifend forschen. Hier Paul Erdős und Terence Tao.

Der folgende Satz wurde 2004 von Ben Green und Terence Tao bewiesen.

Satz 11.14. *Zu jedem k gibt es arithmetische Progressionen der Länge k, die nur aus Primzahlen bestehen.*

Beweis. Dies können wir hier nicht beweisen. □

Eine arithmetische Progression innerhalb der Primzahlen der Länge 7 ist

$$7, 157, 307, 457, 607, 757, 907\,.$$

Die derzeit längste bekannte arithmetische Progression besitzt 27 Glieder, nämlich

$$224\,584\,605\,939\,537\,911 + 81\,292\,139 \cdot 223\,092\,870 \cdot n, \text{ für } n = 0, \ldots, 26\,.$$

11. Arbeitsblatt

Übungsaufgaben

Aufgabe 11.1. Finde die kleinste Zahl N der Form $N = p_1 \cdot p_2 \cdot \ldots \cdot p_r + 1$, die keine Primzahl ist, wobei $p_1, p_2, \ldots, p_r$ die ersten r Primzahlen sind.

Aufgabe 11.2. Berechne den Ausdruck

$$n^2 + n + 41$$

für $n = 0, 1, 2, \ldots$. Handelt es sich dabei um Primzahlen?

Aufgabe 11.3. Es sei K ein Körper und sei $K[X]$ der Polynomring über K. Zeige, dass es unendlich viele normierte irreduzible Polynome in $K[X]$ gibt.

Aufgabe 11.4. Zeige, dass die Reihe

$$\sum_{n=1}^{\infty} \frac{1}{n^s}$$

für reelles $s \leq 1$ divergiert.

Aufgabe 11.5. Zeige, dass die Reihe

$$\sum_{n=1}^{\infty} \frac{1}{n^s}$$

für eine komplexe Zahl s mit $\operatorname{Re}(s) > 1$ absolut konvergiert.

Aufgabe 11.6. Berechne den Wert der Reihe

$$\sum_{n \in M(\{3,5,7\})} \frac{1}{n^4} .$$

Für die folgende Aufgabe ist Aufgabe 7.36 (Analysis (Osnabrück 2021-2023)) hilfreich.

Aufgabe 11.7. Es sei $(f_n)_{n \in \mathbb{N}}$ die Folge der Fibonacci-Zahlen. Zeige, dass die Reihe der Kehrwerte

$$\sum_{n \in \mathbb{N}_+} \frac{1}{f_n}$$

konvergiert.

Aufgabe 11.8. Zeige, dass das uneigentliche Integral

$$\int_2^{\infty} \frac{1}{x \ln x}$$

divergiert.

Welche Beziehung besteht zwischen der vorstehenden Aufgabe und Satz 11.7?

Aufgabe 11.9. Zeige, dass es außer $3, 5, 7$ kein weiteres Zahlentripel der Form $p, p+2, p+4$ gibt, in dem alle drei Zahlen Primzahlen sind.

Aufgabe 11.10. Zeige, dass es eine gerade Zahl g, $2 \leq g \leq 252$, mit der Eigenschaft gibt, dass es unendlich viele Primzahlen p derart gibt, dass auch $p + g$ eine Primzahl ist.

Aufgabe 11.11. Zeige, dass es unendlich viele Primzahlen gibt, die modulo 4 den Rest 1 besitzen.

Aufgabe 11.12. Zeige unter Verwendung des Satzes von Dirichlet, dass eine Primzahl q modulo unendlich vieler Primzahlen p ein quadratischer Rest ist, aber auch modulo unendlich vieler Primzahlen ein nichtquadratischer Rest.

Aufgabe 11.13. Finde neben

$$1 = 1^2 < 25 = 5^2 < 49 = 7^2$$

weitere teilerfremde Quadratzahlen

$$a^2 < b^2 < c^2 < 1000$$

mit

$$c^2 - b^2 = b^2 - a^2.$$

Es gibt innerhalb der Quadratzahlen keine arithmetische Progression der Länge 4.

Aufgabe 11.14. Zeige, dass es keine unendlich lange arithmetische Progression gibt, die nur aus Primzahlen besteht.

Aufgabe 11.15. Man gebe ein Beispiel für eine Teilmenge $T \subseteq \mathbb{N}_+$ derart, dass die Reihe $\sum_{n \in T} \frac{1}{n}$ konvergiert, und dass es in T arithmetische Progressionen beliebiger Länge gibt.

Aufgaben zum Abgeben

Aufgabe 11.16. (3 Punkte)

Zeige, dass es unendlich viele Primzahlen gibt, die modulo 4 den Rest 3 besitzen.

Aufgabe 11.17. (6 Punkte)

Von wie vielen Zahlen ist „durchschnittlich“ die Zahl 7 der kleinste Primteiler? Erläutere dabei, warum diese Frage durchaus einen Sinn macht. Beschreibe alle Zahlen, deren kleinster Primteiler 7 ist (begründe!).

Beantworte die entsprechenden Fragen für eine beliebige Primzahl. Bis zu welcher Primzahl p muss man gehen, damit durchschnittlich mindestens 80% (oder 85% oder 90%) aller Zahlen einen Primteiler $\leq p$ besitzen.

Aufgabe 11.18. (3 Punkte)

Bestimme die kleinste Primzahl p_k derart, dass

$$\prod_{i=1}^{k} \frac{1}{1-p_i^{-1}} = \frac{p_1}{p_1-1} \cdot \frac{p_2}{p_2-1} \cdots \frac{p_k}{p_k-1} \geq 5$$

ist.

Aufgabe 11.19. (3 Punkte)

Es sei $a > 1$ eine reelle Zahl. Zeige, dass die Anzahl

$$\pi(ax) - \pi(x)$$

unbeschränkt ist.

Aufgabe 11.20. (3 Punkte)

Berechne das unendliche Produkt

$$\prod_{p \in \mathbb{P},\, p \geq 7} \frac{1}{1-p^{-2}} .$$

12. Vorlesung - Primzahlen und ihre Verteilung II

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. Es geht um Abschätzungen der Form

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

mit geeigneten Konstanten c und C. Diese 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 durch

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

gegeben.

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 allgemeinen binomischen Formel ergibt sich die Abschätzung

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

Diese beiden Beobachtungen ergeben zusammen 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

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

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

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

□

In der folgenden Aussage, die *Legendres Identität* heißt, bezeichnen wir den p-Exponenten mit ν_p.

Lemma 12.3. *Für eine Primzahl p und eine natürliche Zahl n ist*

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

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. □

Wir kommen nun zu den *Abschätzungen von Tschebyschow.*

Satz 12.4. *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 die Abschätzung $2\sqrt{x} > \ln(x)$ und somit

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

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

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

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

Wir betrachten nun die Abschätzung nach unten. Nach Legendres Identität ist

$$\begin{aligned}\nu_p\left(\binom{2n}{n}\right) &= \nu_p\left(\frac{(2n)!}{n!n!}\right)\\ &= \nu_p((2n)!) - 2\nu_p(n!)\\ &= \left\lfloor\frac{2n}{p}\right\rfloor + \cdots + \left\lfloor\frac{2n}{p^k}\right\rfloor - 2\left(\left\lfloor\frac{n}{p}\right\rfloor + \cdots + \left\lfloor\frac{n}{p^k}\right\rfloor\right)\\ &= \sum_{j=1}^{k}\left(\left\lfloor\frac{2n}{p^j}\right\rfloor - 2\left\lfloor\frac{n}{p^j}\right\rfloor\right).\end{aligned}$$

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 letzten Summe 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

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

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 0). 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 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 mit

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

gibt. 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. Man spricht vom *Bertrandschen Postulat*.

Joseph Bertrand (1822-1900 Paris)

Satz 12.7. *Für jede positive natürliche Zahl n gibt es eine Primzahl zwischen $n+1$ und $2n$.*

Beweis. Dies werden wir hier nicht beweisen. Die Aussage 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.

12. Arbeitsblatt

Übungsaufgaben

Aufgabe 12.1. Zeige, dass für jedes $x \in \mathbb{R}$ die Abschätzungen

$$0 \leq \lfloor 2x \rfloor - 2 \lfloor x \rfloor \leq 1$$

gelten.

Aufgabe 12.2. Bestimme die Anzahl der hinteren Nullen in der Dezimalentwicklung von 100!.

Aufgabe 12.3. Bestimme die Primfaktorzerlegung von 10!.

Aufgabe 12.4. Bestimme die Primfaktorzerlegung von

$$\binom{20}{10}.$$

Aufgabe 12.5. Zeige mit Hilfe des Bertrandschen Postulats, dass für jedes $n \geq 2$ der Binomialkoeffizient

$$\binom{2n}{n}$$

einen Primfaktor größer als n besitzt.

Aufgabe 12.6. Zeige, dass für $n \geq 2$ die Fakultät $n!$ keine Quadratzahl ist.

Aufgabe 12.7. Es sei $n \in \mathbb{N}_+$. Zeige, dass das Produkt von n aufeinanderfolgenden natürlichen Zahlen von $n!$ geteilt wird.

Zur Erinnerung.

Aufgabe 12.8. Zeige, dass die Logarithmen zur Basis b die folgenden Rechenregeln erfüllen.

(1) Es ist $\log_b(b^x) = x$ und $b^{\log_b(y)} = y$, das heißt der Logarithmus zur Basis b ist die Umkehrfunktion zur Exponentialfunktion zur Basis b.
(2) Es gilt $\log_b(y \cdot z) = \log_b y + \log_b z$.
(3) Es gilt $\log_b y^u = u \cdot \log_b y$ für $u \in \mathbb{R}$.
(4) Es gilt

$$\log_a y = \log_a \left(b^{\log_b y}\right) = \log_b y \cdot \log_a b.$$

Aufgabe 12.9. Es sei $\varphi(n)$ die Eulersche Funktion. Zeige, dass die Folge $\frac{\varphi(n)}{n}$, $n \in \mathbb{N}$, sowohl in 1 als auch in $\frac{1}{3}$ einen Häufungspunkt besitzt.

Aufgaben zum Abgeben

Aufgabe 12.10. (4 Punkte)

Es sei $\varphi(n)$ die Eulersche Funktion. Zeige, dass die Folge $\frac{\varphi(n)}{n}$, $n \in \mathbb{N}$, sowohl in 1 als auch in 0 einen Häufungspunkt besitzt.

Aufgabe 12.11. (5 Punkte)

Beweise Korollar 12.5, also die Aussage, dass

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

ist, mit Hilfe von Korollar 11.6 über die Riemannsche ζ-Funktion.

Aufgabe 12.12. (4 Punkte)

Bestimme anhand des Beweises der Abschätzungen von Tschebyschow einen expliziten Wert für c mit $\pi(x) \geq c\frac{x}{\ln(x)}$.

Aufgabe 12.13. (4 Punkte)

Zeige unter Verwendung der Abschätzungen von Tschebyschow, dass es (zumindest für x hinreichend groß) mehr Primzahlen zwischen x und x^2 als zwischen 1 und x gibt.

13. Vorlesung - Spezielle Primzahlen I

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. Eine Mersenne-Zahl besitzt im Zweiersystem die Ziffernentwicklung $11111\ldots1111$. Das ist auch die Anzahl der Spiele in einem im K.-o.-System ausgetragenen Pokalwettbewerb mit 2^n Mannschaften.

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

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

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

$X = 2^a$ 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 Mersenne-Zahl $M_n = 2^n - 1$ 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 Mersenne-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 des 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 52 Mersenne-Primzahlen gefunden. Die größte ist

$$2^{136279841} - 1\,.$$

Es ist 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. Für eine Rekordliste siehe Mersenne-Primzahlen.

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 all 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, also eine Mersenne-Primzahl ist. Euler bewies, dass auf diese Weise alle geraden vollkommenen Zahlen erzeugt werden können. Bevor wir 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 von n 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. *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

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

□

Damit können wir den Satz von Euklid-Euler beweisen.

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

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

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

gegeben. Daher ist ihre Summe gleich

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

also ist n vollkommen. Es 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 nach Lemma 13.6 die Teilersumme gleich dem Produkt der beiden Teilersummen. Daher ist einerseits

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

und andererseits wegen der Vollkommenheit $\sigma(n) = 2n = 2^k u$. Insgesamt ergibt sich also $\big(2^k-1\big)\sigma(u) = 2^k u$. 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

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

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. Die Summe der echten Teiler von $220 = 2\cdot 2\cdot 5\cdot 11$ ist

$$1+2+4+5+10+11+20+22+44+55+110 \;=\; 284$$

und die Summe der echten Teiler von $284 = 2\cdot 2\cdot 71$ ist

$$1+2+4+71+142 \;=\; 220.$$

Zwei verschiedene Zahlen sind genau dann befreundet, wenn

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

ist. Der folgende Satz erlaubt es, einige weitere befreundete Zahlenpaare zu finden, aber keineswegs alle. Man spricht von der *Regel von Thabit*.

Satz 13.9. *Es 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 $m+n$. Die Primzahlen a und b sind teilerfremd und somit ist nach Lemma 13.6

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

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

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

□

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

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

Zahlentheoretische Funktionen

Definition 13.10. Eine Funktion

$$\mathbb{N}_+ \longrightarrow \mathbb{C}$$

nennt man *zahlentheoretische Funktion*.

Eine zahlentheoretische Funktion ist also einfach eine komplexwertige Folge. Im zahlentheoretischen Kontext sind die beiden folgenden Definitionen wichtig.

Definition 13.11. Eine zahlentheoretische Funktion

$$f\colon \mathbb{N}_+ \longrightarrow \mathbb{C}$$

heißt *multiplikativ*, wenn für teilerfremde Zahlen m, n stets

$$f(mn) = f(m)f(n)$$

gilt.

An multiplikativen zahlentheoretischen Funktionen haben wir bisher die eulersche φ-Funktion, die Teileranzahlfunktion (siehe Aufgabe 3.31) und die Teilersummenfunktion (siehe Lemma 13.6) kennengelernt.

Definition 13.12. Zu zahlentheoretischen Funktionen $f, g\colon \mathbb{N}_+ \to \mathbb{C}$ heißt die durch

$$(f * g)(n) := \sum_{d \text{ teilt } n} f(d)g\Big(\frac{n}{d}\Big)$$

definierte Funktion die *Faltung* von f und g.

Diese Summe kann man auch in der Form

$$\sum_{n=de} f(d)g(e)$$

schreiben. Summiert wird nur über die positiven Teilerpaare, was bei dieser Schreibweise übersehen werden könnte.

Lemma 13.13. *Zu multiplikativen zahlentheoretischen Funktionen $f, g\colon \mathbb{N}_+ \to \mathbb{C}$ ist auch die Faltung $f * g$ multiplikativ.*

Beweis. Es seien f, g multiplikativ und es seien m, n teilerfremde natürliche Zahlen. Zu einer Faktorzerlegung

$$de = mn$$

gibt es aufgrund der Teilerfremdheit eine eindeutige Aufspaltung $d = ru$ und $e = sv$ mit r, u und s, v teilerfremd und mit $rs = m$ und $uv = n$. Daher ist

$$(f * g)(m \cdot n) = \sum_{d \cdot e = m \cdot n} f(d)g(e)$$

$$
\begin{aligned}
&= \sum_{rs=m,\, uv=n} f(ru)g(sv) \\
&= \sum_{rs=m,\, uv=n} f(r)f(u)g(s)g(v) \\
&= \left(\sum_{r\cdot s=m} f(r)g(s)\right) \cdot \left(\sum_{u\cdot v=n} f(u)g(v)\right) \\
&= (f*g)(m)\cdot(f*g)(n),
\end{aligned}
$$

also ist auch $f * g$ multiplikativ. □

Definition 13.14. Die zahlentheoretische Funktion $\mathbb{N}_+ \to \mathbb{C}$, die für 1 den Wert 1 und sonst überall den Wert 0 besitzt, wird mit I bezeichnet. Sie heißt die *Faltungseinheit*.

Definition 13.15. Die zahlentheoretische Funktion $\mathbb{N}_+ \to \mathbb{C}$, die überall den Wert 1 besitzt, wird mit U bezeichnet.

Definition 13.16. Die zahlentheoretische Funktion $\mu\colon \mathbb{N}_+ \to \mathbb{C}$, die durch

$$
\mu(n) := \begin{cases} 0, \text{ falls in der Primfaktorzerlegung von } n \text{ manche Primfaktoren mehrfach auftreten,} \\ (-1)^k, \text{ falls } n = p_1 \cdots p_k \text{ mit verschiedenen Primfaktoren.} \end{cases}
$$

gegeben ist, heißt *Möbius-Funktion*.

Lemma 13.17. *Für die Faltung von zahlentheoretischen Funktionen gelten die folgenden Aussagen.*

(1) Die Faltung ist eine kommutative und assoziative Verknüpfung.
(2) Die Faltungseinheit I ist das neutrale Element der Verküpfung.
(3) Es ist

$$U * \mu = I.$$

Beweis. Siehe Aufgabe 13.11. □

13. Arbeitsblatt

Übungsaufgaben

Aufgabe 13.1. Eine natürliche Zahl n ist genau dann vollkommen, wenn die Stammbruchsummenbedingung

$$\sum_{d|n,\, d\neq 1} \frac{1}{d} = 1$$

gilt. Schreibe für einige vollkommene Zahlen die Stammbruchsumme hin.

Aufgabe 13.2. Es sei n eine gerade vollkommene Zahl. Berechne die eulersche Funktion $\varphi(n)$.

In den folgenden Aufgaben werden einige Begriffe verwendet, die mit dem Begriff der vollkommenen Zahl in Verbindung stehen.

Eine natürliche Zahl n heißt *defizient*, wenn die Summe der Teiler kleiner als $2n$ ist.

Eine natürliche Zahl n heißt *abundant*, wenn die Summe der Teiler größer als $2n$ ist.

Eine natürliche abundante Zahl heißt *sonderbar*, wenn sie nicht als eine Teilsumme von ihren echten Teilern darstellbar ist.

Aufgabe 13.3. Zeige: eine Primzahlpotenz p^r ist defizient.

Aufgabe 13.4. Es sei $n > 6$ ein Produkt von zwei verschiedenen Primzahlen. Zeige, dass dann n defizient ist.

Aufgabe 13.5. Zeige ohne Verwendung der Regel von Thabit, dass die beiden Zahlen 220 und 284 befreundet sind.

Aufgabe 13.6. Zeige, dass für $k \geq 2$ die beiden Zahlen $a = 3 \cdot 2^{k-1} - 1$ und $b = 3 \cdot 2^k - 1$ teilerfremd sind.

Aufgabe 13.7. Man gebe ein Beispiel für zwei nicht befreundete Zahlen m und n mit

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

Aufgabe 13.8. Ergänze die folgende Tabelle um weitere Zeilen.

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

Aufgabe 13.9. Zeige, dass die zahlentheoretische Möbius-Funktion multiplikativ ist.

Aufgabe 13.10. Zeige, dass eine zahlentheoretische multiplikative Funktion durch ihre Werte an Primzahlpotenzen festgelegt ist.

Aufgabe 13.11. Zeige, dass für die Faltung von zahlentheoretischen Funktionen die folgenden Aussagen gelten.

(1) Die Faltung ist eine kommutative und assoziative Verknüpfung.
(2) Die Faltungseinheit I ist das neutrale Element der Verküpfung.
(3) Es ist
$$U * \mu = I.$$

Aufgabe 13.12. Zeige
$$U * U = T,$$
wobei T die Teileranzahlfunktion bezeichnet.

Aufgabe 13.13. Zeige, dass eine zahlentheoretische Funktion $f\colon \mathbb{N}_+ \to \mathbb{C}$ genau dann invertierbar bezüglich der Faltung ist, wenn
$$f(1) \neq 0$$
ist.

In den folgenden Aufgaben bezeichnet $E\colon \mathbb{N}_+ \to \mathbb{C}$ die Abbildung mit $E(n) = n$ für alle $n \in \mathbb{N}_+$.

Aufgabe 13.14. Zeige, dass zwischen der Möbius-Funktion μ, der Identität E und der eulerschen φ-Funktion die Beziehung
$$\mu * E = \varphi$$
besteht.

Aufgabe 13.15. Zeige, dass zwischen den zahlentheoretischen Funktionen U, E, σ die Beziehung
$$U * E = \sigma$$
besteht.

Aufgabe 13.16. Zeige, dass die Menge der zahlentheoretischen Funktionen mit der komponentenweisen Addition und der Faltung einen kommutativen Ring bildet.

Aufgaben zum Abgeben

Aufgabe 13.17. (3 Punkte)

Finde einen Primfaktor der folgenden drei Zahlen

$$2^{33} - 1,\ 2^{91} - 1,\ 2^{13} + 1\,.$$

Aufgabe 13.18. (4 Punkte)

Es sei n eine gerade vollkommene Zahl, $n \neq 6$. Zeige, dass n die Summe von aufeinanderfolgenden ungeraden Kubikzahlen ist.

Aufgabe 13.19. (3 Punkte)

Es sei n eine ungerade Zahl mit der Eigenschaft, dass in ihrer Primfaktorzerlegung nur zwei verschiedene Primfaktoren vorkommen. Zeige, dass dann n defizient ist.

Aufgabe 13.20. (4 Punkte)

Finde eine ungerade abundante Zahl n.

Aufgabe 13.21. (3 Punkte)

Finde die kleinste sonderbare Zahl.

Aufgabe 13.22. (3 Punkte)

Zeige, dass der Quotient

$$\frac{\sigma(n)}{n}$$

unbeschränkt ist.

14. Vorlesung - Spezielle Primzahlen II

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

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

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

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

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*

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

hat, wobei die p_i verschiedene Fermatsche Primzahlen sind.

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

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

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

die alle prim sind, 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. *Es 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. Es 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 zum quadratischen Reziprozitätsgesetz, dass 2 ein Quadratrest modulo p ist. Es 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. Es sei $m > n$. Dann ist

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

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-Primzahlen gibt.

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

Satz 14.9. *Es 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 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. *Es 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 in $\mathbb{Z}/(q)$ und nach Lemma 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 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, und die die Eigenschaft besitzt, dass für jede zu n teilerfremde ganze Zahl a

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

gilt, 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 $n \geq 3$ ist genau dann eine Carmichael-Zahl, wenn jeder Primteiler p von n einfach ist und $p-1$ die Zahl $n-1$ teilt.*

Beweis. Es sei $n = p_1^{r_1} \cdots p_k^{r_k}$ die kanonische Primfaktorzerlegung. Nach dem chinesischen Restsatz ist

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

Es 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 in $\mathbb{Z}/(p_i^{r_i})$ (was nach Satz 5.11 möglich ist; für $p_1 = 2$ 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_i 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_i in $(\mathbb{Z}/(p_i^{r_i}))^\times$ (auch bei $p = 2$), und es ergibt sich der Widerspruch $p|(n-1)$. Also sind alle Exponenten einfach.

Für die Umkehrung ist nach Voraussetzung $r_i = 1$. Es sei wieder

$$a = (a_1, \ldots, a_k)$$

eine Einheit. Dann ist

$$\begin{aligned} a^{n-1} &= \left(a_1^{n-1}, \ldots, a_k^{n-1}\right) \\ &= \left(\left(a_1^{p_1-1}\right)^{\frac{n-1}{p_1-1}}, \ldots, \left(a_k^{p_k-1}\right)^{\frac{n-1}{p_k-1}}\right) \\ &= (1, \ldots, 1) \end{aligned}$$

$$= \ 1.$$

Also ist n eine Carmichael-Zahl. □

Beispiel 14.15. Die kleinste Carmichael-Zahl ist

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

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

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

14. Arbeitsblatt

Übungsaufgaben

Aufgabe 14.1. Bestimme für alle $n \leq 30$, ob das regelmäßige n-Eck mit Zirkel und Lineal konstruierbar ist oder nicht.

Aufgabe 14.2. Man gebe eine Liste aller natürlichen Zahlen n zwischen 100 und 200 mit der Eigenschaft, dass das regelmäßige n-Eck mit Zirkel und Lineal konstruierbar ist.

Aufgabe 14.3. Welche der Winkel

$$1^\circ, \, 2^\circ, \, 3^\circ, \, 4^\circ, \ldots, 10^\circ$$

sind mit Zirkel und Lineal konstruierbar?

Aufgabe 14.4. Welche der Winkel

$$10^\circ, \, 20^\circ, \, 30^\circ, \, 40^\circ, \ldots, 350^\circ$$

sind mit Zirkel und Lineal konstruierbar?

Aufgabe 14.5. Finde die kleinste Zahl $n \geq 100$ derart, dass zugleich das reguläre n-Eck mit Zirkel und Lineal konstruierbar ist und dass n eine Summe von zwei Quadraten ist.

Aufgabe 14.6.
(a) Zeige, dass die Endziffer einer Sophie-Germain-Primzahl p im Zehnersystem nicht 7 sein kann.
(b) Zeige, dass die Zahlen $1, 3, 5, 9$ als Endziffer einer Sophie-Germain-Primzahl auftreten können.

Aufgabe 14.7. Es sei p eine Sophie-Germain-Primzahl und $q = 2p + 1$. Es sei a gegeben mit $2 \leq a \leq q - 2$. Zeige, dass a genau dann eine primitive Einheit modulo q ist, wenn es kein Quadratrest modulo q ist.

Aufgabe 14.8. Es sei p eine Sophie-Germain-Primzahl, $q = 2p + 1$. Zeige, dass q ein Teiler von $M_p + 2 = 2^p + 1$ genau dann ist, wenn $q = \pm 3 \mod 8$ ist.

Aufgabe 14.9. Zeige: Für eine Primzahl p ist die Mersennesche Zahl M_p quasiprim zur Basis 2.

Aufgabe 14.10. Zeige, dass 1105 und 1729 Carmichael-Zahlen sind.

Aufgabe 14.11. Es sei p eine Primzahl > 3 mit der Eigenschaft, dass auch $2p - 1$ und $3p - 2$ prim sind. Zeige, dass dann

$$n = p(2p - 1)(3p - 2)$$

eine Carmichael-Zahl ist.

Aufgaben zum Abgeben

Aufgabe 14.12. (3 Punkte)

Beschreibe die Konstruktion mit Zirkel und Lineal eines regelmäßigen Fünfecks, wie sie in der folgenden Animation dargestellt ist.

Konstruktion eines regulären Fünfecks mit Zirkel und Lineal

Aufgabe 14.13. (3 Punkte)

Es sei p eine Sophie-Germain-Primzahl. Zeige, dass 2 eine Primitivwurzel modulo $q = 2p+1$ ist genau dann, wenn $p = 1 \mod 4$ ist.

Aufgabe 14.14. (3 Punkte)

Es sei n eine Carmichael-Zahl. Zeige, dass n ungerade und mindestens drei Primfaktoren besitzt.

Aufgabe 14.15. (3 Punkte)

Es sei n eine natürliche Zahl. Zeige, dass das Potenzieren

$$\mathbb{Z}/(n) \longrightarrow \mathbb{Z}/(n),\, a \longmapsto a^n,$$

genau dann die Identität ist, wenn n eine Primzahl, eine Carmichael-Zahl oder gleich 1 ist.

15. Vorlesung - Quotientenkörper und Körpererweiterungen

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.

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

In der unteren Zeile stehen Körper, und zwar ist

$$\mathbb{Q} \subseteq \mathbb{Q}[\mathrm{i}]$$

eine endliche Körpererweiterung vom Grad 2 (d.h. die $\mathbb{Q}$-Vektorraumdimension von $\mathbb{Q}[\mathrm{i}]$ ist 2). Ferner ist $\mathbb{Q}$ der kleinste Körper, der die ganzen Zahlen $\mathbb{Z}$ enthält, und ebenso ist $\mathbb{Q}[\mathrm{i}]$ der kleinste Körper, der die Gaußschen Zahlen $\mathbb{Z}[\mathrm{i}]$ enthält. Die Gaußschen Zahlen sind, in einem zu präzisierenden Sinne, die „ganzen Zahlen“ im Körper $\mathbb{Q}[\mathrm{i}]$.

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

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

vor. Hier ist $\omega = \frac{-1+\sqrt{3}\mathrm{i}}{2}$ 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, während nach Aufgabe 5.21 $\mathbb{Z}[\sqrt{-3}]$ nicht faktoriell ist.

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 mit den Worten umschrieben haben, dass $\mathbb{Q}$ der kleinste Körper ist, der $\mathbb{Z}$ enthält.

Der Quotientenkörper

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

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

mit natürlichen Identifizierungen und Operationen definiert.

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 einen 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 kommutativer 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 $Q(R)$ über die Elemente $\frac{r}{1}$ wieder. 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. Es 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-Algebrahomomorphismus von $R[X]$ in eine weitere R-Algebra B ist durch die Zuordnung $X \mapsto f$ gegeben, wobei $f \in B$ ein beliebiges fixiertes Element ist. Diese Abbildung nennt man den *Einsetzungshomomorphismus*. Er schickt ein Polynom $\sum_{i=0}^{n} r_i X^i$ mit $r_i \in R$ auf $\sum_{i=0}^{n} r_i f^i \in B$, wobei die r_i via dem Strukturhomomorphismus als Elemente in B aufgefasst werden.

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

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 (siehe Vorlesung 17) und algebraisch äquivalent.

Definition 15.4. Es sei K ein Körper und A eine K-Algebra. Es sei $f \in A$ ein über K algebraisches Element. Dann heißt das normierte Polynom $P \in K[X]$ mit $P(f) = 0$, welches von minimalem Grad mit dieser Eigenschaft ist, 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 0 verschiedenes Polynom P mit rationalen Koeffizienten und mit $P(z) = 0$ gibt. 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 Ferdinand von Lindemann 1882 gezeigt.

Definition 15.7. Es 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 endlichdimensionaler Vektorraum über K ist.

Definition 15.9. Es sei $K \subseteq L$ eine endliche Körpererweiterung. Dann nennt man die K-Vektorraumdimension von L den *Grad* der Körpererweiterung.

Ein Element $f \in L$ einer Körpererweiterung

$$K \subseteq L$$

definiert durch Multiplikation eine K-lineare Abbildung

$$\varphi_f\colon\ L \longrightarrow L,\ y \longmapsto fy.$$

Über diese Konstruktion werden Norm und Spur von f erklärt.

Bemerkung 15.10. Zu einer linearen Abbildung

$$\varphi\colon\ V \longrightarrow V$$

eines endlichdimensionalen 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 durch

$$S(\varphi) = \lambda_{1,1} + \lambda_{2,2} + \cdots + \lambda_{n,n}$$

gegeben, und dies ist nach Aufgabe 14.16 (Lineare Algebra (Osnabrück 2024-2025)) ebenfalls unabhängig von der Wahl der Basis.

Definition 15.11. Es sei $K \subseteq L$ eine endliche Körpererweiterung. Zu einem Element $f \in L$ nennt man die Determinante der K-linearen Abbildung

$$\mu_f\colon\ L \longrightarrow L,\ y \longmapsto fy,$$

die *Norm* von f. Sie wird mit $N(f)$ bezeichnet.

Definition 15.12. Es sei $K \subseteq L$ eine endliche Körpererweiterung. Zu einem Element $f \in L$ nennt man die Spur der K-linearen Abbildung

$$\mu_f\colon\ L \longrightarrow L,\ y \longmapsto fy,$$

die *Spur* von f. Sie wird mit $\operatorname{Spur}(f)$ bezeichnet.

Lemma 15.13. *Es sei $K \subseteq L$ eine endliche Körpererweiterung. Dann hat die Norm*

$$N\colon\ L \longrightarrow K,\ f \longmapsto N(f),$$

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) Dies folgt aus dem Determinantenmultiplikationssatz und aus Lemma 8.2 (Körper- und Galoistheorie (Osnabrück 2018-2019)).

(2) Zu einer beliebigen Basis von L wird die Multiplikation mit einen Element $f \in K$ durch die Diagonalmatrix beschrieben, bei der jeder Diagonaleintrag f ist. Die Determinante ist daher f^n nach Lemma 16.4 (Lineare Algebra (Osnabrück 2024-2025)).

(3) Die eine Richtung ist klar, sei also $f \neq 0$. Dann ist f eine Einheit in L und daher ist die Multiplikation mit f eine bijektive K-lineare Abbildung $L \to L$, und deren Determinante ist $\neq 0$ nach Satz 16.11 (Lineare Algebra (Osnabrück 2024-2025)). □

Lemma 15.14. *Es sei $K \subseteq L$ eine endliche Körpererweiterung vom Grad n. Dann hat die Spur*

$$S\colon L \longrightarrow K,\, f \longmapsto S(f),$$

folgende Eigenschaften:

1. *Die Spur ist 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 $K \subseteq L$ eine endliche und einfache Körpererweiterung, so ist

$$L = K[f] \cong K[X]/(P),$$

wobei P das Minimalpolynom von f ist.

Satz 15.15. *Es sei $K \subseteq L = K[f]$ eine einfache endliche Körpererweiterung vom Grad n. Dann hat das Minimalpolynom P von f die Gestalt*

$$P = X^n - S(f)X^{n-1} + \cdots + (-1)^n N(f).$$

Beweis. Das Minimalpolynom und das charakteristische Polynom der durch f definierten K-linearen Multiplikationsabbildung

$$\mu_f\colon L \longrightarrow L,\, y \longmapsto fy,$$

haben beide den Grad n. Nach dem Satz von Cayley-Hamilton annulliert das charakteristische Polynom die lineare Abbildung und ist somit ein Vielfaches des Minimalpolynoms, sodass sie übereinstimmen. Diese lineare Abbildung

μ_f sei bezüglich einer Basis $v_1, \ldots, v_n$ von L durch die Matrix $(\lambda_{ij})_{ij}$ gegeben. Dann ist das charakteristische Polynom gleich

$$\begin{aligned}\chi_{\mu_f}\chi_{\mu_f} &= \det \begin{pmatrix} X-\lambda_{1,1} & \cdots & -\lambda_{1,n} \\ \vdots & \ddots & \vdots \\ -\lambda_{n,1} & \cdots & X-\lambda_{n,n} \end{pmatrix} \\ &= X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0.\end{aligned}$$

Zum Koeffizienten a_{n-1} leisten (in der Leibniz-Formel zur Berechnung der Determinante) 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 $X^n - \sum_{i=1}^n \lambda_{i,i}X^{n-1} + \ldots$, sodass 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. Es 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 0 sind, ist eine Körpererweiterung stets separabel (siehe Aufgabe 15.33), und wir haben den folgenden *Satz vom primitiven Element* zur Verfügung.

Satz 15.17. *Es sei $K \subseteq L$ eine endliche separable Körpererweiterung. Dann wird L von einem Element erzeugt, d.h. es gibt ein $f \in L$ 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.

□

15. Arbeitsblatt

Übungsaufgaben

Aufgabe 15.1. Es sei R ein Integritätsbereich und K ein Körper mit $R \subseteq K$. Zeige, dass dann auch $Q(R) \subseteq K$ gilt.

Aufgabe 15.2. Es sei R ein faktorieller Bereich mit Quotientenkörper $K = Q(R)$. Zeige, dass jedes Element $f \in K$, $f \neq 0$, eine im Wesentlichen eindeutige Produktzerlegung

$$f = up_1^{r_1} \cdots p_n^{r_n}$$

mit einer Einheit $u \in R$ und ganzzahligen Exponenten r_i besitzt.

Aufgabe 15.3. Es sei R ein faktorieller Bereich mit Quotientenkörper $K = Q(R)$. Es sei $a \in K$ ein Element mit $a^n \in R$ für eine natürliche Zahl $n \geq 1$. Zeige, dass dann schon a zu R gehört.

Aufgabe 15.4. Betrachte die rationalen Zahlen $(\mathbb{Q}, +, 0)$ als kommutative Gruppe. Zeige, dass sie nicht endlich erzeugt ist.

Aufgabe 15.5. Betrachte die rationalen Zahlen $(\mathbb{Q}, +, 0)$ als kommutative Gruppe. Es sei $G \subseteq \mathbb{Q}$ eine endlich erzeugte Untergruppe. Zeige, dass G zyklisch ist.

Aufgabe 15.6. Bestimme einen Erzeuger für die Untergruppe $H \subseteq (\mathbb{Q}, +, 0)$, die durch die rationalen Zahlen

$$\frac{8}{7}, \frac{5}{11}, \frac{7}{10}$$

erzeugt wird.

Eine solche Untergruppe von $\mathbb{Q}$ nennt man auch ein *gebrochenes Ideal*.

Aufgabe 15.7. Bestimme einen Erzeuger für das gebrochene Ideal $\mathfrak{f} \subseteq \mathbb{Q}$, das durch die rationalen Zahlen

$$\frac{3}{7}, \frac{5}{6}, \frac{3}{10}$$

erzeugt wird.

Aufgabe 15.8. Es sei $\mathbb{P}$ die Menge der Primzahlen und

$$\alpha \colon \mathbb{P} \longrightarrow \mathbb{Z}$$

eine Abbildung. Zeige, dass die Menge

$$G_\alpha = \left\{ q \in \mathbb{Q}^\times \mid \exp_p(q) \geq \alpha(p) \text{ für alle } p \right\} \cup \{0\}$$

eine Untergruppe von $(\mathbb{Q}, 0, +)$ ist.

Aufgabe 15.9. Es sei

$$\varphi\colon\ (\mathbb{Q},0,+) \longrightarrow (\mathbb{Q}\setminus\{0\},1,\cdot)$$

ein Gruppenhomomorphismus. Zeige, dass φ trivial ist.

Aufgabe 15.10. Es sei

$$\varphi\colon\ (\mathbb{Q}\setminus\{0\},1,\cdot) \longrightarrow (\mathbb{Q},0,+)$$

ein Gruppenhomomorphismus. Zeige, dass φ nicht injektiv ist.

Aufgabe 15.11. Zeige, dass es einen surjektiven Gruppenhomomorphismus

$$\varphi\colon\ (\mathbb{Q}\setminus\{0\},1,\cdot) \longrightarrow (\mathbb{Q},0,+)$$

gibt.

Aufgabe 15.12. Zeige, dass $2^{1/5} \in \mathbb{R}$ algebraisch über $\mathbb{Q}$ ist und bestimme das Minimalpolynom davon.

Aufgabe 15.13. Zeige, dass es nur abzählbar viele algebraische Zahlen gibt.

Aufgabe 15.14. Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung. Zeige, dass es einen (injektiven) Ringhomomorphismus $L \to \mathbb{C}$ gibt.

Aufgabe 15.15. Es seien $\mathbb{Q} \subseteq K \subset \mathbb{C}$ und $\mathbb{Q} \subseteq L \subset \mathbb{C}$ zwei endliche Körpererweiterungen von $\mathbb{Q}$ vom Grad d bzw. e. Es seien d und e teilerfremd. Zeige, dass dann

$$K \cap L = \mathbb{Q}$$

ist.

Aufgabe 15.16. Berechne in

$$\mathbb{Z}/(7)[X]/(X^3+4X^2+X+5)$$

das Produkt

$$(2x^2+5x+3)\cdot(3x^2+x+6)$$

(x bezeichne die Restklasse von X).

Aufgabe 15.17. Bestimme das Inverse von $2x^2+3x-1$ im Körper $\mathbb{Q}[X]/(X^3-5)$ (x bezeichnet die Restklasse von X).

Aufgabe 15.18. Es sei $K \subseteq L$ eine endliche Körpererweiterung. Zeige, dass jedes Element $f \in L$ algebraisch über K ist.

Aufgabe 15.19. Es sei $z = a + b\mathrm{i} \in \mathbb{C}$, $a, b \in \mathbb{R}$, eine algebraische Zahl. Zeige, dass auch die konjugiert-komplexe Zahl $\overline{z} = a - b\mathrm{i}$ sowie der Real- und der Imaginärteil von z algebraisch sind. Man bestimme den Grad der Körpererweiterung

$$\mathbb{A} \cap \mathbb{R} \subseteq \mathbb{A}.$$

Aufgabe 15.20. Bringe für die Körpererweiterung $\mathbb{R} \subseteq \mathbb{C}$ die Konzepte Norm und Spur mit dem Betrag und dem Realteil einer komplexen Zahl in Verbindung.

Aufgabe 15.21. Wir betrachten die quadratische Körpererweiterung $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{3}] = L$. Erstelle die Matrix der Multiplikationsabbildung zu $-4 + 9\sqrt{3}$ bezüglich der $\mathbb{Q}$-Basis $1, \sqrt{3}$ von L.

Aufgabe 15.22. Erstelle die Multiplikationsmatrix zum Element $7x^2-4x+5$ in der kubischen Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[X]/\left(X^3 - 6X^2 + 5X - 8\right).$$

Aufgabe 15.23. Es sei $K \subseteq L$ eine endliche Körpererweiterung. Zeige, dass die Abbildung

$$L \longrightarrow \mathrm{End}_K(L),\ f \longmapsto \mu_f,$$

ein injektiver Ringhomomorphismus ist.

Aufgabe 15.24. Berechne für das Element $2 + 4x + 5x^2$ in der Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[X]/\left(X^3 - 3X + 1\right) =: L$$

die Norm und die Spur.

Aufgabe 15.25. Bestimme für sämtliche Elemente der Körpererweiterung

$$\mathbb{Z}/(2) \subseteq \mathbb{Z}/(2)[X]/\left(X^2 + X + 1\right)$$

die Multiplikationsmatrizen bezüglich der Basis $1, x$ sowie ihre Norm und ihre Spur.

Aufgabe 15.26. Bestimme für sämtliche Elemente der Körpererweiterung

$$\mathbb{Z}/(3) \subseteq \mathbb{Z}/(3)[X]/\big(X^2-2\big)$$

die Multiplikationsmatrizen bezüglich der Basis $1, x$ sowie ihre Norm und ihre Spur.

Aufgabe 15.27. Es sei K ein Körper und sei $K[X]$ der Polynomring über K. Es sei $F \in K[X]$ und $a \in K$. Zeige, dass a genau dann eine mehrfache Nullstelle von F ist, wenn $F'(a) = 0$ ist, wobei F' die formale Ableitung von F bezeichnet.

Aufgabe 15.28. Es sei K ein Körper und $L = K(X)$ der Quotientenkörper des Polynomrings $K[X]$. Zeige, dass $K \subset L$ eine einfache, aber keine endliche Körpererweiterung ist.

Aufgaben zum Abgeben

Aufgabe 15.29. (4 Punkte)

Es sei K ein Körper und A eine kommutative K-Algebra, die außerdem ein Integritätsbereich sei. Es sei $f \in A$ ein über K algebraisches Element. Es sei $P \in K[X]$ ein normiertes Polynom mit $P(f) = 0$. Dann ist P das Minimalpolynom von f genau dann, wenn es irreduzibel ist.

Aufgabe 15.30. (2 Punkte)

Erstelle die Multiplikationsmatrix zum Element $7x^2+3x-8$ in der kubischen Körpererweiterung

$$\mathbb{Q} = \mathbb{Q}[X]/\big(X^3+9X^2-2X+5\big).$$

Aufgabe 15.31. (3 Punkte)

Es sei K ein Körper und sei $P = X^n - c \in K[X]$ ein irreduzibles Polynom. Es sei

$$f = a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_1X + a_0$$

ein Element in der einfachen endlichen Körpererweiterung $K \subseteq L = K[X]/(P)$ vom Grad n. Zeige, dass die Spur von f gleich na_0 ist.

In der folgenden Aufgabe werden verschiedene äquivalente Bedingungen an ein Polynom gestellt, die man alle als Definition eines separablen Polynoms nehmen kann. Man darf verwenden, dass es zu jedem Körper einen Erweiterungskörper gibt, in dem ein vorgegebenes Polynom in Linearfaktoren zerfällt.

Aufgabe 15.32. (4 Punkte)

Es sei K ein Körper und sei $F \in K[X]$ ein Polynom vom Grad n. Zeige, dass die folgenden Aussagen äquivalent sind:

(1) F und die (formale) Ableitung F' sind teilerfremd.
(2) F und die (formale) Ableitung F' erzeugen das Einheitsideal.
(3) F besitzt in keinem Erweiterungskörper $K \subseteq L$ mehrfache Nullstellen.
(4) Es gibt einen Erweiterungskörper $K \subseteq L$ derart, dass F als Polynom in $L[X]$ in n verschiedene Linearfaktoren zerfällt.

Aufgabe 15.33. (3 (1+1+1) Punkte)

Es sei K ein Körper und sei $F \in K[X]$ ein irreduzibles Polynom.

(a) Man gebe eine einfache Charakterisierung dafür, dass F separabel ist.
(b) Zeige, dass in Charakteristik null jedes irreduzible Polynom separabel ist.
(c) Man gebe ein Beispiel, dass das in positiver Charakteristik nicht immer stimmen muss.

16. Vorlesung - Moduln

Diskriminanten

Definition 16.1. Es 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 $b_1, \ldots, b_n$ durch

$$\triangle(b_1, \ldots, b_n) = \det\left(\mathrm{Spur}\,(b_i b_j)_{i,j}\right)$$

definiert.

Die Produkte $b_i b_j$, $1 \leq i, j \leq n$, sind dabei Elemente in L, von denen man jeweils 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, sodass sich die Diskriminante als Invariante eines Zahlkörpers erweist.

Bei einem Basiswechsel verhält sich die Diskriminante wie folgt.

Lemma 16.2. *Es sei $K \subseteq L$ eine endliche Körpererweiterung vom Grad n und seien $b_1, \ldots, b_n$ und $c_1, \ldots, c_n$ 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 $c_i = \sum_{j=1}^n t_{ij} b_j$ für jedes i. Damit gilt

$$c_i c_k = \left(\sum_{j=1}^n t_{ij} b_j \right) \left(\sum_{m=1}^n t_{km} b_m \right) = \sum_{j,m} t_{ij} t_{km} b_j b_m.$$

Wir schreiben $c_{ik} := S(c_i c_k)$ und $b_{jm} := S(b_j b_m)$. Wegen der K-Linearität der Spur gilt

$$c_{ik} = S(c_i c_k) = S\left(\sum_{j,m} t_{ij} t_{km} b_j b_m \right) = \sum_{j,m} t_{ij} t_{km} S(b_j b_m) = \sum_{j,m} t_{ij} t_{km} b_{jm}.$$

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 und Satz 17.5 (Lineare Algebra (Osnabrück 2024-2025)). □

Lemma 16.3. *Es 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 0.

Es sei angenommen, dass die Diskriminante 0 ist. Das bedeutet, dass das durch die Matrix $S(b_i b_j)_{ij}$ definierte lineare Gleichungssystem eine nichttriviale Lösung $(\lambda_1, \ldots, \lambda_n) \in K^n$ besitzt. Es ist also

$$\sum_{j=1}^n \lambda_j S(b_i b_j) = 0$$

für jedes i. Es sei $x = \sum_{j=1}^n \lambda_j b_j \neq 0$. Dann ist für jedes i

$$S(b_i x) = S\left(b_i \left(\sum_{j=1}^n \lambda_j b_j \right) \right) = S\left(\sum_{j=1}^n \lambda_j b_i b_j \right) = \sum_{j=1}^n \lambda_j S(b_i b_j) = 0.$$

Da x eine Einheit in L ist, ist auch $b_i x$, $i = 1, \ldots, n$, eine K-Basis von L und es folgt, dass die Spur auf dieser Basis und somit überall den Wert 0 hat. Dies ist aber bei einer separablen Erweiterung nicht möglich: In Charakteristik 0 folgt dies sofort aus Lemma 15.14 (2). □

Beschreibung von Spur und Norm mit Einbettungen

Satz 16.4. *Es 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 wird L durch ein Element erzeugt, es ist also

$$L = \mathbb{Q}(x) \cong \mathbb{Q}[X]/(F)$$

mit einem irreduziblen Polynom $F \in \mathbb{Q}[X]$ vom Grad n. Da F irreduzibel ist und da die Ableitung $F' \neq 0$ ist und kleineren Grad besitzt, folgt, dass F und F' teilerfremd sind. Nach Satz 20.10 (Lineare Algebra (Osnabrück 2024-2025)) 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

$$\rho_i \colon L \cong \mathbb{Q}[X]/(F) \longrightarrow \mathbb{C},\ X \longmapsto z_i.$$

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 keinen weiteren Ringhomomorphismus $L \to \mathbb{C}$ geben, da ein solcher durch $X \mapsto z$ gegeben ist und $F(z) = 0$ sein muss. □

Man beachte im vorstehenden Satz, dass das Bild von verschiedenen Einbettungen

$$\rho_i \colon L \longrightarrow \mathbb{C}$$

der gleiche Unterkörper von $\mathbb{C}$ sein kann. Dies gilt bereits für quadratische Erweiterungen wie $\mathbb{Q}[\mathrm{i}]$. Man hat die beiden Einbettung $\rho_1, \rho_2 \colon \mathbb{Q}[\mathrm{i}] \to \mathbb{C}$, wobei die eine Abbildung i auf i und die andere i auf $-\mathrm{i}$ schickt. Das Bild ist aber in beiden Fällen gleich.

Wenn das Bild einer Einbettung ganz in den reellen Zahlen liegt, so spricht man auch von einer reellen Einbettung. 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. *Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung und $z \in L$ ein Element. Es seien*

$$\rho_1, \ldots, \rho_n \colon L \longrightarrow \mathbb{C}$$

die verschiedenen komplexen Einbettungen und es sei $M = \{y_1, \ldots, y_k\}$ *die Menge der verschiedenen Werte* $\rho_i(z)$*. Dann gilt in* $\mathbb{C}[X]$ *für das Minimalpolynom* G *von* z *die Gleichung*

$$G = (X - y_1)(X - y_2) \cdots (X - y_k).$$

Beweis. Es sei $K \subseteq L$ der von z erzeugte Unterkörper von L. Es ist dann

$$K \cong \mathbb{Q}[X]/(G)$$

mit dem (normierten) Minimalpolynom G von z, und K (bzw. G) haben den Grad m über $\mathbb{Q}$. Gemäß Satz 16.4 gibt es m Einbettungen $\sigma\colon K \to \mathbb{C}$, die den komplexen Nullstellen M' von G entsprechen, und daher ist

$$G = \prod_{\sigma} (X - \sigma(z)).$$

Die n Einbettungen $\rho_i\colon L \to \mathbb{C}$ induzieren jeweils eine Einbettung $\sigma_i = \rho_i|_K\colon K \to \mathbb{C}$ und somit ist $\rho_i(z) = \sigma_i(z)$, also $M \subseteq M'$. Andererseits lässt sich eine Einbettung $\sigma\colon K \to \mathbb{C}$ zu einer Einbettung $L \to \mathbb{C}$ fortsetzen, da L über K separabel ist und nach dem Satz vom primitiven Element 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. *Es sei* $\mathbb{Q} \subseteq L$ *eine endliche Körpererweiterung vom Grad* n *und seien* $\rho_i\colon L \to \mathbb{C}$ *die* n *verschiedenen komplexen Einbettungen. Es sei* $z \in L$ *und* $z_i = \rho_i(z)$, $i = 1, \ldots, n$*. Dann ist*

$$N(z) = z_1 \cdots z_n \text{ und } \operatorname{Spur}(z) = z_1 + \cdots + z_n\,.$$

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. Es sei R ein kommutativer Ring und $M = (M, +, 0)$ eine *additiv* geschriebene kommutative Gruppe. Man nennt M einen *R- Modul* , wenn eine Operation

$$R \times M \longrightarrow M,\ (r, v) \longmapsto rv = r \cdot v,$$

(*Skalarmultiplikation* genannt) festgelegt ist, 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. Es sei R ein kommutativer Ring und M ein R-Modul. Eine Teilmenge $U \subseteq M$ heißt R- *Untermodul* , wenn sie eine Untergruppe von $(M, 0, +)$ ist und wenn für jedes $u \in U$ und $r \in R$ auch $ru \in U$ ist.

Definition 16.9. Es sei R ein kommutativer Ring und M ein R-Modul. Eine Familie $v_i \in M$, $i \in I$, 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. Es 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. *Es 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. *Es sei R ein kommutativer Ring und $\mathfrak{p}$ ein Ideal in R. Dann ist $\mathfrak{p}$ genau dann ein Primideal, wenn der Restklassenring $R/\mathfrak{p}$ ein Integritätsbereich ist.*

Beweis. Es sei zunächst $\mathfrak{p}$ ein Primideal. Dann ist insbesondere $\mathfrak{p} \subset R$ und somit ist der Restklassenring $R/\mathfrak{p}$ nicht der Nullring. Es 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 Integritätsbereich, so handelt es sich nicht um den Nullring und daher ist $\mathfrak{p} \neq R$. Es 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 kein weiteres Ideal gibt.

Lemma 16.15. *Es sei R ein kommutativer Ring und $\mathfrak{m}$ ein Ideal in R. Dann ist $\mathfrak{m}$ genau dann ein maximales Ideal, wenn der Restklassenring $R/\mathfrak{m}$ ein Körper ist.*

Beweis. Nach Aufgabe 9.9 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. *Es sei R ein kommutativer Ring und $\mathfrak{m}$ ein maximales Ideal in R. Dann ist $\mathfrak{m}$ ein Primideal.*

Beweis. Dies folgt sofort aus den Charakterisierungen für Primideale und für maximale Ideale mit den Restklassenringen. □

16. Arbeitsblatt

Übungsaufgaben

Aufgabe 16.1. Berechne die Diskriminante zur Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[\mathrm{i}]$$

zur Basis 1 und i und zur Basis $2 - 5\mathrm{i}$ und $4 + 7\mathrm{i}$.

Aufgabe 16.2. Berechne explizit die Diskriminante des quadratischen Zahlbereichs A_{-7}. Stelle die Multiplikationsmatrix bezüglich einer geeigneten Basis für das Element

$$f = \frac{3}{2} + \frac{5}{2}\sqrt{-7}$$

auf und berechne damit die Spur und die Norm von f.

Aufgabe 16.3. Es sei p eine Primzahl und sei

$$L = \mathbb{Q}[X]/\left(X^3 - p\right)$$

der durch das irreduzible Polynom $X^3 - p$ definierte Erweiterungskörper von $\mathbb{Q}$. Es sei

$$f = 2 + 3x - 4x^2.$$

(a) Finde die Matrix bezüglich der $\mathbb{Q}$-Basis $1, x, x^2$ von L der durch die Multiplikation mit f definierten $\mathbb{Q}$-linearen Abbildung.
(b) Berechne die Norm und die Spur von f.
(c) Bestimme das Minimalpolynom von f.
(d) Finde das Inverse von f.
(e) Berechne die Diskriminante der Basis $1, f, f^2$.

Aufgabe 16.4. Beweise Lemma 16.6 unter der zusätzlichen Voraussetzung, dass L von z erzeugt wird.

Aufgabe 16.5. Es sei G eine kommutative Gruppe. Zeige, dass G auf genau eine Weise die Struktur eines $\mathbb{Z}$-Moduls trägt. Kommutative Gruppen und $\mathbb{Z}$-Moduln sind also äquivalente Objekte.

Aufgabe 16.6. Es seien R und A kommutative Ringe. Zeige, dass A genau dann eine R-Algebra ist, wenn A ein R-Modul ist, für den zusätzlich

$$r(ab) = (ra)b \text{ für alle } r \in R,\ a, b \in A$$

gilt.

Aufgabe 16.7. Es sei $\mathfrak{a}$ ein Ideal in einem kommutativen Ring R. Zeige, dass $\mathfrak{a}$ genau dann ein Primideal ist, wenn $\mathfrak{a}$ der Kern eines Ringhomomorphismus $\varphi\colon R \to K$ in einen Körper K ist.

Aufgabe 16.8. Zeige, dass jeder Restklassenring eines Hauptidealringes wieder ein Hauptidealring ist. Man gebe ein Beispiel, dass ein Restklassenring eines Hauptidealbereiches kein Hauptidealbereich sein muss.

Ein Ideal $\mathfrak{a}$ in einem kommutativen Ring R heißt *Radikal* (oder *Radikalideal*), wenn folgendes gilt: Falls $f^n \in \mathfrak{a}$ ist für ein $n \in \mathbb{N}$, so ist bereits $f \in \mathfrak{a}$.

Aufgabe 16.9. Zeige, dass ein Primideal ein Radikal ist.

Aufgabe 16.10. Zeige, dass ein Ideal $\mathfrak{a}$ in einem kommutativen Ring R genau dann ein Radikal ist, wenn der Restklassenring $R/\mathfrak{a}$ reduziert ist.

Es sei R ein kommutativer Ring und $\mathfrak{a} \subseteq R$ ein Ideal. Dann nennt man die Menge

$$\{f \in R \mid \text{es gibt ein } r \text{ mit } f^r \in \mathfrak{a}\}$$

das *Radikal* zu $\mathfrak{a}$. Es wird mit $\operatorname{rad}(\mathfrak{a})$ bezeichnet.

Aufgabe 16.11. Bestimme in $\mathbb{Z}$ das Radikal zum Ideal $\mathbb{Z}27$.

Aufgabe 16.12. Es sei R ein kommutativer Ring und $S \subseteq R$ ein Unterring. Bestätige oder widerlege die folgenden Aussagen.

(1) Zu einem Ideal $\mathfrak{a} \subseteq R$ ist auch $\mathfrak{a} \cap S$ ein Ideal (in S).
(2) Zu einem Radikal $\mathfrak{a} \subseteq R$ ist auch $\mathfrak{a} \cap S$ ein Radikal.
(3) Zu einem Primideal $\mathfrak{a} \subseteq R$ ist auch $\mathfrak{a} \cap S$ ein Primideal.
(4) Zu einem maximalen Ideal $\mathfrak{a} \subseteq R$ ist auch $\mathfrak{a} \cap S$ ein maximales Ideal.

Aufgaben zum Abgeben

Aufgabe 16.13. (8 (1+1+2+2+2) Punkte)

Es sei p eine Primzahl und sei

$$L = \mathbb{Q}[X]/\left(X^3 - p\right)$$

der durch das irreduzible Polynom $X^3 - p$ definierte Erweiterungskörper von $\mathbb{Q}$. Es sei

$$f = 2 + 3x - 4x^2.$$

(a) Finde die Matrix bezüglich der $\mathbb{Q}$-Basis $1, x, x^2$ von L der durch die Multiplikation mit f definierten $\mathbb{Q}$-linearen Abbildung.
(b) Berechne die Norm und die Spur von f.
(c) Bestimme das Minimalpolynom von f.
(d) Finde das Inverse von f.
(e) Berechne die Diskriminante der Basis $1, f, f^2$.

Aufgabe 16.14. (3 Punkte)

Es sei $(G, +, 0)$ eine kommutative Gruppe. Es sei

$$E := \operatorname{End}(G) = \operatorname{Hom}(G, G)$$

die Menge der Gruppenhomomorphismen von G nach G (also die Gruppenendomorphismen auf G). Definiere auf E eine Addition und eine Multiplikation derart, dass E zu einem (in der Regel nicht kommutativen) Ring wird.

Aufgabe 16.15. (3 Punkte)

Es sei $(M,+,0)$ eine kommutative Gruppe und sei $E = \mathrm{End}_{\mathbb{Z}}(M)$ der zugehörige Endomorphismenring. Es sei R ein kommutativer Ring. Zeige, dass eine R-Modulstruktur auf M äquivalent ist zu einem Ringhomomorphismus $R \to \mathrm{End}_{\mathbb{Z}}(M)$.

Aufgabe 16.16. (4 Punkte)

Es seien R und S kommutative Ringe und sei $\varphi\colon R \to S$ ein Ringhomomorphismus. Es sei $\mathfrak{p}$ ein Primideal in S. Zeige, dass das Urbild $\varphi^{-1}(\mathfrak{p})$ ein Primideal in R ist.

Zeige durch ein Beispiel, dass das Urbild eines maximalen Ideales kein maximales Ideal sein muss.

Aufgabe 16.17. (3 Punkte)

Es sei R ein kommutativer Ring und sei $\mathfrak{a} \neq R$ ein Ideal in R. Zeige: $\mathfrak{a}$ ist genau dann ein maximales Ideal, wenn es zu jedem $g \in R$, $g \notin \mathfrak{a}$, ein $f \in \mathfrak{a}$ und ein $r \in R$ mit $rg + f = 1$ gibt.

17. Vorlesung - Ganzheit

Ganzheit

Definition 17.1. Es seien R und S kommutative Ringe und sei $R \subseteq S$ eine Ringerweiterung. Für ein Element $x \in S$ heißt eine Gleichung der Form

$$x^n + r_{n-1}x^{n-1} + r_{n-2}x^{n-2} + \cdots + r_1 x + r_0 = 0,$$

wobei die Koeffizienten r_i, $i = 0, \ldots, n-1$, zu R gehören, eine *Ganzheitsgleichung* für x.

Definition 17.2. Es seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Ein Element $x \in S$ heißt *ganz* (über R), 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 17.2.

Die einfachsten Ganzheitsgleichungen haben die Form $x^n - r = 0$ mit $r \in R$ bzw. $x^n = r$. Wenn also ein Element einer Ringerweiterung eine Wurzel eines Elementes aus R ist, so ist diese Wurzel ganz über dem Grundring. Trivialerweise sind die Elemente aus R ganz über R.

Beispiel 17.3. In der Ringerweiterung $\mathbb{Z} \subseteq \mathbb{Z}[\mathrm{i}]$ ist i ganz über $\mathbb{Z}$, wie die Ganzheitsgleichung

$$\mathrm{i}^2 = -1$$

zeigt. Auch für ein beliebiges Element $z = a + b\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$ kann man direkt eine Ganzheitsgleichung angeben, nämlich

$$(a + b\mathrm{i})^2 - 2a(a + b\mathrm{i}) + a^2 + b^2 = 0.$$

Beispiel 17.4. Es sei R ein kommutativer Ring und

$$P = X^n + r_{n-1}X^{n-1} + \cdots + r_2X^2 + r_1X + r_0 \in R[X]$$

ein normiertes Polynom über R. Dann ist in der Ringerweiterung

$$R \subseteq R[X]/(P)$$

die Restklasse x von X im Restklassenring $S = R[X]/(P)$ ganz über R, da ja P unmittelbar die Ganzheitsgleichung

$$x^n + r_{n-1}x^{n-1} + \cdots + r_2x^2 + r_1x + r_0 = 0$$

liefert.

Definition 17.5. Es seien R und S kommutative Ringe und sei $R \subseteq S$ eine Ringerweiterung. Dann heißt S *ganz* über R, wenn jedes Element $x \in S$ ganz über R ist.

Definition 17.6. Es 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.

S ist genau dann ganz über R, wenn der ganze Abschluss von R in S gleich S ist.

Wir wollen zeigen, dass die Summe und das Produkt von zwei ganzen Elementen wieder ganz ist. Der vermutlich erste Gedanke, die jeweiligen Ganzheitsgleichungen miteinander „geschickt“ zu kombinieren, führt nicht zum Ziel. Stattdessen braucht man das folgende Kriterium für die Ganzheit.

Lemma 17.7. *Es 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

$$x^n + r_{n-1}x^{n-1} + r_{n-2}x^{n-2} + \cdots + r_1x + r_0 = 0$$

ergibt sich

$$x^n \;=\; -r_{n-1}x^{n-1} - r_{n-2}x^{n-2} - \cdots - r_1 x - r_0.$$

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

$$R[x] \;=\; R + Rx + Rx^2 + \cdots + Rx^{n-2} + Rx^{n-1}$$

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 $xM \subseteq M$. Es 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,

$$x \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \;=\; \begin{pmatrix} r_{1,1} & r_{1,2} & \ldots & r_{1,n} \\ r_{2,1} & r_{2,2} & \ldots & r_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ r_{n,1} & r_{n,2} & \ldots & r_{n,n} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}.$$

Dies schreiben wir als

$$0 \;=\; \begin{pmatrix} x - r_{1,1} & -r_{1,2} & \ldots & -r_{1,n} \\ -r_{2,1} & x - r_{2,2} & \ldots & -r_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ -r_{n,1} & -r_{n,2} & \ldots & x - r_{n,n} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}.$$

Nennen wir diese Matrix A (die Einträge sind aus S), und sei A^{adj} die adjungierte Matrix. Dann gilt $A^{\mathrm{adj}}Ay \;=\; 0$ (y bezeichne den Vektor $(y_1, \ldots, y_n)$) und nach der Cramerschen Regel ist $A^{\mathrm{adj}}A \;=\; (\det A)E_n$, also gilt $((\det A)E_n)y \;=\; 0$. Es ist also $(\det A)y_j \;=\; 0$ für alle j und damit

$$(\det A)z \;=\; 0$$

für alle $z \in M$. 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, sodass eine Ganzheitsgleichung vorliegt. $\square$

Korollar 17.8. *Es seien R und S kommutative Ringe und sei $R \subseteq S$ 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. Es seien $x_1 \in S$ und $x_2 \in S$ ganz über R. Nach der Charakterisierung der Ganzheit gibt es endliche R-Unteralgebren $T_1, T_2 \subseteq S$ mit $x_1 \in T_1$ und $x_2 \in T_2$. Es 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

$$\Big(\sum r_{ij} y_i z_j\Big)\Big(\sum s_{kl} y_k z_l\Big) = \sum r_{ij} s_{kl} y_i y_k z_j z_l,$$

und für die Produkte gilt $y_i y_k \in T_1$ und $z_j z_l \in T_2$, sodass 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. □

Normale Integritätsbereiche

Definition 17.9. Es 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 17.10. Ein Integritätsbereich heißt *normal*, wenn er ganz-abgeschlossen in seinem Quotientenkörper ist.

Definition 17.11. Es sei R ein Integritätsbereich und $Q(R)$ sein Quotientenkörper. Dann nennt man den ganzen Abschluss von R in $Q(R)$ die *Normalisierung* von R.

Wichtige Beispiele für normale Ringe werden durch faktorielle Ringe geliefert.

Satz 17.12. *Es sei R ein faktorieller Integritätsbereich. Dann ist R normal.*

Beweis. Es sei $K = Q(R)$ der Quotientenkörper von R und $q \in K$ ein Element, das die Ganzheitsgleichung

$$q^n + r_{n-1} q^{n-1} + r_{n-2} q^{n-2} + \cdots + r_1 q + r_0 = 0$$

mit $r_i \in R$ erfüllt. Wir schreiben $q = a/b$ mit $a, b \in R$, $b \neq 0$, wobei wir annehmen können, dass die Darstellung gekürzt ist, dass also a und $b \in R$ keinen gemeinsamen Primteiler besitzen. Wir müssen zeigen, dass b eine Einheit in R ist, da dann $q = ab^{-1}$ zu R gehört.

Wir multiplizieren die obige Ganzheitsgleichung mit b^n und erhalten in R

$$a^n + (r_{n-1} b) a^{n-1} + \big(r_{n-2} b^2\big) a^{n-2} + \cdots + \big(r_1 b^{n-1}\big) a + (r_0 b^n) = 0.$$

Wenn b keine Einheit ist, dann gibt es 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 17.13. *Es sei R ein normaler Integritätsbereich und $a \in R$. Wenn es ein Element $x \in Q(R)$ mit $x^k = a$ gibt, 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. □

Die einfachsten Beispiele für irrationale reelle Zahlen sind $\sqrt{2}, \sqrt{3}, \sqrt{5}$ u.s.w. Diese Beobachtung wird durch die folgende Aussage wesentlich verallgemeinert.

Korollar 17.14. *Es sei $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ die kanonische Primfaktorzerlegung der natürlichen Zahl n. Es 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 daraus nach Satz 17.12 resultierenden Normalität kann es auch kein $x \in Q(\mathbb{Z}) = \mathbb{Q}$ mit $x^k = n$ geben. Daher ist die reelle Zahl $n^{\frac{1}{k}}$ irrational. □

Der ganze Abschluss in Erweiterungskörpern

Lemma 17.15. *Es 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. Es sei $f \in L$. Nach Voraussetzung ist L endlich über K. Daher erfüllt f eine Ganzheitsgleichung der Form

$$f^n + q_{n-1}f^{n-1} + \cdots + q_1 f + q_0 = 0$$

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

$$(rf)^n + q_{n-1}r(rf)^{n-1} + \cdots + q_1 r^{n-1}(rf) + q_0 r^n = 0.$$

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. □

Insbesondere zeigt die vorstehende Aussage, dass bei einer echten Körpererweiterung $K \subseteq L$ auch der ganze Abschluss von R echt größer als R ist. Für uns steht die Situation, wo $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung der rationalen Zahlen und S der ganze Abschluss von $\mathbb{Z}$ in L ist, im Mittelpunkt.

17. Arbeitsblatt

Übungsaufgaben

Aufgabe 17.1. Finde eine irreduzible Ganzheitsgleichung (über $\mathbb{Z}$) für die Eisensteinzahl $\omega = \frac{-1+\sqrt{-3}}{2}$.

Aufgabe 17.2. Es sei R ein kommutativer Ring und A eine R-Algebra. Zeige, dass wenn R ein Körper ist, die Begriffe algebraisch und ganz für ein Element $x \in A$ übereinstimmen. Zeige ferner, dass für einen Integritätsbereich, der kein Körper ist, diese beiden Begriffe auseinander fallen.

Aufgabe 17.3. Bestimme das Minimalpolynom der komplexen Zahl $\sqrt{2}-\sqrt{5}$ über $\mathbb{Q}$.

Aufgabe 17.4. Es seien R und S Integritätsbereiche und sei $R \subseteq S$ eine ganze Ringerweiterung. Es sei $f \in R$ ein Element, das in S eine Einheit ist. Zeige, dass f dann schon in R eine Einheit ist.

Aufgabe 17.5. Es sei $R \subseteq S$ eine ganze Ringerweiterung und sei $f \in R$. Zeige: Wenn f, aufgefasst in S, eine Einheit ist, dann ist f eine Einheit in R.

Aufgabe 17.6. Man gebe ein Beispiel einer ganzen Ringerweiterung $R \subseteq S$, wo es einen Nichtnullteiler $f \in R$ gibt, der ein Nullteiler in S wird.

Aufgabe 17.7. Es sei K ein Körper und sei A eine endlichdimensionale K-Algebra. Zeige direkt (ohne Lemma 17.7), dass A ganz über K ist.

Aufgabe 17.8. Es sei $R \subseteq S$ eine Ringerweiterung zwischen endlichen kommutativen Ringen R und S. Zeige, dass eine ganze Ringerweiterung vorliegt.

Aufgabe 17.9. Es sei R ein kommutativer Ring und

$$S = R[X_1, \ldots, X_n]/\mathfrak{a}$$

eine (als Algebra) endlich erzeugte R-Algebra, die ganz über R sei. Zeige, dass S ein endlich erzeugter R-Modul ist.

Aufgabe 17.10.

(1) Es sei R ein Integritätsbereich. Zeige, dass R ganz-abgeschlossen im Polynomring $R[X]$ ist.
(2) Man gebe ein Beispiel für einen kommutativen Ring R, der im Polynomring nicht ganz-abgeschossen ist.

Aufgabe 17.11. Es sei R ein Integritätsbereich. Zeige, dass R genau dann normal ist, wenn er mit seiner Normalisierung übereinstimmt.

Aufgabe 17.12. Es sei R ein Integritätsbereich. Es sei angenommen, dass die Normalisierung von R gleich dem Quotientenkörper $Q(R)$ ist. Zeige, dass dann R selbst schon ein Körper ist.

Aufgabe 17.13. Es sei K ein Körper und sei $R_i \subseteq K$, $i \in I$, eine Familie von normalen Unterringen. Zeige, dass auch der Durchschnitt $\bigcap_{i\in I} R_i$ normal ist.

Aufgabe 17.14. Es sei R ein normaler Integritätsbereich und $a \in R$. Es sei vorausgesetzt, dass a keine Quadratwurzel in R besitzt. Zeige, dass das Polynom $X^2 - a$ prim in $R[X]$ ist. Tipp: Verwende den Quotientenkörper $Q(R)$. Warnung: Prim muss hier nicht zu irreduzibel äquivalent sein.

Aufgabe 17.15. Es sei R ein Integritätsbereich mit Normalisierung R^{norm}. Zeige, dass durch

$$\mathfrak{f} = \{g \in R \mid gR^{\mathrm{norm}} \subseteq R\}$$

ein Ideal in R gegeben ist.

Aufgabe 17.16. Es sei k eine fixierte positive ganze Zahl und betrachte den Unterring

$$R = \mathbb{Z}[k\mathrm{i}] = \{a + ck\mathrm{i} \mid a, c \in \mathbb{Z}\} \subseteq \mathbb{Z}[\mathrm{i}].$$

Zeige die Isomorphie $R \cong \mathbb{Z}[X]/(X^2 + k^2)$ und dass $\mathbb{Z}[\mathrm{i}]$ ganz über R ist.

In den folgenden Aufgaben wird der Polynomring $K[X,Y]$ in zwei Variablen über einem Körper K verwendet. Diesen kann man definieren als $(K[X])[Y]$. Die Elemente in ihm, also die Polynome in zwei Variablen, haben die Gestalt

$$P = \sum_{i,j} a_{ij} X^i Y^j.$$

Wir interessieren uns für Restklassenringe vom Typ $R = K[X,Y]/(F)$. Die Nullstellenmenge von$F$ besteht aus der Menge derjenigen Punkte (x,y) in der Ebene, für die $F(x,y) = 0$ ist (dieses Nullstellengebilde ist eine geometrische Version des Ringes R).

Aufgabe 17.17. Es sei K ein Körper und betrachte den Restklassenring

$$R = K[X,Y]/(X^2 - Y^3).$$

Dies ist ein Integritätsbereich nach Aufgabe 17.14. Zeige, dass die Normalisierung von R gleich dem Polynomring $K[T]$ ist. Skizziere die Nullstellenmenge von $F = X^2 - Y^3$ in der reellen Ebene und finde eine Parametrisierung dieses Gebildes.

Polynomringe kann man entsprechend über jedem Grundring und mit beliebig vielen Variablen definieren.

Aufgabe 17.18. Es sei

$$P = X^2 - 3X + 7$$

und

$$Q = Y^3 - Y^2 + 4Y - 5.$$

Begründe, dass die Ringerweiterung

$$\mathbb{Z} \subseteq \mathbb{Z}[X,Y]/(P,Q)$$

ganz ist und finde eine Ganzheitsgleichung für $x+y$ und für xy (kleine Buchstaben bezeichnen die Restklassen der Variablen).

Aufgaben zum Abgeben

Aufgabe 17.19. (3 Punkte)

Es sei R ein normaler Integritätsbereich und $R \subseteq S$ eine ganze Ringerweiterung. Sei $f \in R$. Zeige, dass für das von f erzeugte Hauptideal gilt:

$$R \cap (f)S = (f)R.$$

Aufgabe 17.20. (3 Punkte)

Es seien R, S, T kommutative Ringe und seien $\varphi : R \to S$ und $\psi : S \to T$ Ringhomomorphismen derart, dass S ganz über R und T ganz über S ist. Zeige, dass dann auch T ganz über R ist.

Aufgabe 17.21. (4 Punkte)

Bestimme das Inverse von

$$2 + 3\sqrt{5} + \sqrt{7} + 3\sqrt{35}$$

im Körper $\mathbb{Q}[\sqrt{5}, \sqrt{7}]$.

Aufgabe 17.22. (4 Punkte)

Zeige, dass für natürliche Zahlen $a, b \geq 1$ und $n \geq 2$ die Zahl $a^n - b^n$ nicht ein Teiler von $a^n + b^n$ ist.

Aufgabe 17.23. (5 Punkte)

Es sei K ein Körper und betrachte den Ringhomomorphismus $\varphi\colon R = K[X, Y] \to K[T]$, der durch die Einsetzung

$$X \longmapsto (T-1)(T+1) \text{ und } Y \longmapsto T(T-1)(T+1)$$

gegeben ist. Finde ein von 0 verschiedenes Polynom $F \in K[X, Y]$ derart, dass F unter φ auf 0 abgebildet wird. Skizziere die Nullstellenmenge von F in der reellen Ebene.

Aufgabe 17.24. (4 Punkte)

Definiere unter Anlehnung an die Parametrisierung der pythagoreischen Tripel einen Ringhomomorphismus

$$\mathbb{Z}[X, Y, Z]/(X^2 + Y^2 - Z^2) \longrightarrow \mathbb{Z}[U, V].$$

Zeige, dass dieser injektiv, aber nicht surjektiv ist.

18. Vorlesung - Zahlbereiche

Zahlbereiche

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. Es 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*. Diese Zahlbereiche sind der Gegenstand 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, siehe Korollar 22.18, Satz 22.17, Bemerkung 22.19 einerseits und Satz 23.14 andererseits.)
(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. Siehe Satz 14.2 (Algebraische Zahlentheorie (Osnabrück 2020-2021)) und Satz 26.6 (Algebraische Zahlentheorie (Osnabrück 2020-2021)).)
(4) Was passiert mit den Primzahlen in den Zahlbereichen? Gibt es eine Regelmäßigkeit, wie diese in R zerlegt werden? (siehe Korollar 18.11.)
(5) Was kann man über die Einheiten in einem Zahlbereich sagen? (Siehe Satz 28.7 (Algebraische Zahlentheorie (Osnabrück 2020-2021)).)
(6) Inwiefern reflektieren Eigenschaften von Zahlbereichen Eigenschaften der ganzen Zahlen selbst?

Satz 18.2. *Es sei R ein Zahlbereich. Dann ist R ein normaler Integritätsbereich.*

Beweis. Nach Lemma 17.15 ist L der Quotientenkörper des Ganzheitsrings R. Ist $q \in Q(R) = L$ ganz über R, so ist q nach Aufgabe 17.20 auch ganz über $\mathbb{Z}$ und gehört selbst zu R. □

Ein Ganzheitsring ist im Allgemeinen nicht faktoriell.

Lemma 18.3. *Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung und es sei $R \subseteq L$ ein Unterring mit den folgenden Eigenschaften:*

(1) R ist ganz über $\mathbb{Z}$.

(2) Es ist $Q(R) = L$.
(3) R ist normal.

Dann ist R der Ring der ganzen Zahlen von L.

Beweis. Siehe Aufgabe 18.1. □

Beispiel 18.4. Wir betrachten die Körpererweiterung $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{-3}]$, der die Ringe

$$\mathbb{Z}[\sqrt{-3}] = A \subseteq \mathbb{Z}[\omega] = B \subseteq \mathbb{Q}[\sqrt{-3}]$$

enthält, wobei $\omega = -\frac{1}{2} + \frac{\mathrm{i}}{2}\sqrt{3}$ ist, d.h. $\mathbb{Z}[\omega]$ ist der Ring der Eisenstein-Zahlen. Der Quotientenkörper von beiden Ringen ist $\mathbb{Q}[\sqrt{-3}]$. Das Element ω erfüllt die Ganzheitsgleichung

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

und somit ist $\mathbb{Z}[\omega]$ ganz über $\mathbb{Z}$. Ferner ist $\mathbb{Z}[\omega]$ normal. Dies ergibt sich aus Satz 2.15, Satz 2.16, Satz 3.7 und Satz 17.12. Nach Lemma 18.3 ist also insgesamt der Ring der Eisenstein-Zahlen der Ring der ganzen Zahlen in $\mathbb{Q}[\sqrt{-3}]$.

Lemma 18.5. *Es sei R ein Zahlbereich. Dann enthält jedes von 0 verschiedene Ideal $\mathfrak{a} \subseteq R$ eine Zahl $m \in \mathbb{Z}$ mit $m \neq 0$.*

Beweis. Es sei $0 \neq f \in \mathfrak{a}$. Dieses Element ist nach der Definition eines Zahlbereiches ganz über $\mathbb{Z}$ und erfüllt demnach eine Ganzheitsgleichung

$$f^n + k_{n-1}f^{n-1} + k_{n-2}f^{n-2} + \cdots + k_1 f + k_0 = 0$$

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. Es sei also in obiger Gleichung $k_0 \neq 0$. Dann ist

$$f\left(f^{n-1} + k_{n-1}f^{n-2} + k_{n-2}f^{n-3} + \cdots + k_1\right) = -k_0$$

und somit ist $k_0 \in (f) \cap \mathbb{Z} \subseteq \mathfrak{a}$. □

Satz 18.6. *Es 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.

Es 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 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.

Gruppenstruktur von Idealen

In $\mathbb{Z}[\mathrm{i}]$ ist jedes Ideal ein Hauptideal und es ist

$$(a+b\mathrm{i}) = \{m(a+b\mathrm{i}) + n\mathrm{i}(a+b\mathrm{i}) \mid m,n \in \mathbb{Z}\} \cong \mathbb{Z}^2$$

(die letzte Gleichung setzt voraus, dass es sich nicht um das Nullideal handelt). Eine ähnlich einfache Gruppenstruktur gilt für jedes Ideal in einem Zahlbereich, was wir jetzt beweisen werden.

Lemma 18.7. *Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n und R der zugehörige Zahlbereich. Es sei $\mathfrak{a}$ ein von 0 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 18.5 ein Element $0 \neq m \in \mathfrak{a} \cap \mathbb{Z}$. Nach (dem Beweis von) Lemma 17.15 kann man $v_i = \frac{r_i}{n_i}$ mit $r_i \in R$ und $n_i \in \mathbb{Z} \setminus \{0\}$ schreiben. Dann sind die $m(n_i v_i) \in \mathfrak{a}$ und sie bilden ebenfalls eine $\mathbb{Q}$-Basis von L. □

Satz 18.8. *Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n und R der zugehörige Zahlbereich. Es sei $\mathfrak{a}$ ein von 0 verschiedenes Ideal in R. Es 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

$$\mathfrak{a} = \mathbb{Z}b_1 + \cdots + \mathbb{Z}b_n.$$

Beweis. Zunächst sind wegen Aufgabe 18.5 die Spuren zu Elementen aus R ganzzahlig und somit sind auch die in Frage stehenden Diskriminanten ganzzahlig. Man kann also die Diskriminanten bzw. ihre Beträge untereinander der Größe nach vergleichen.

Es sei $f \in \mathfrak{a}$ ein beliebiges Element. Wir müssen zeigen, dass sich f als eine $\mathbb{Z}$-Linearkombination $f = k_1b_1 + \cdots + k_nb_n$ 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

$$f = q_1b_1 + \cdots + q_nb_n$$

mit rationalen Zahlen $q_i \in \mathbb{Q}$. Es 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 (echt) zwischen 0 und 1. Dann ist auch

$$c_1 = f - kb_1 = \delta b_1 + \sum_{i=2}^{n} q_i b_i,\ b_2, \ldots, b_n$$

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 0 sind, ist dies ein Widerspruch zur Minimalität der Diskriminante. □

Korollar 18.9. *Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n und R der zugehörige Zahlbereich. Es sei $\mathfrak{a}$ ein von 0 verschiedenes Ideal in R. Dann ist $\mathfrak{a}$ eine freie abelsche Gruppe vom Rang n, d.h. es gibt Elemente $b_1, \ldots, b_n \in \mathfrak{a}$ mit*

$$\mathfrak{a} = \mathbb{Z}b_1 + \cdots + \mathbb{Z}b_n,$$

wobei die Koeffizienten in einer Darstellung eines Elementes aus $\mathfrak{a}$ eindeutig bestimmt sind.

Beweis. Nach Lemma 18.7 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 (ganzzahlige) Betrag der Diskriminante minimal ist. Für diese gilt nach Satz 18.8, dass sie ein $\mathbb{Z}$-Erzeugendensystem von $\mathfrak{a}$ bilden. Die lineare Unabhängigkeit über $\mathbb{Q}$ sichert die Eindeutigkeit der Koeffizienten. □

Korollar 18.10. *Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n und R der zugehörige Zahlbereich. Dann ist R eine freie abelsche Gruppe vom Rang n, d.h. es gibt Elemente $b_1, \ldots, b_n \in R$ mit*

$$R = \mathbb{Z}b_1 + \cdots + \mathbb{Z}b_n$$

derart, dass die Koeffizienten in einer Darstellung eines Elementes eindeutig bestimmt sind.

Beweis. Dies folgt direkt aus Korollar 18.9, angewendet auf das Ideal $\mathfrak{a} = R$. □

Ein solches System von Erzeugern $b_1, \ldots, b_n$ nennt man auch eine *Ganzheitsbasis* von R.

Korollar 18.11. *Es 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 $R/(p)$ 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 18.10 ist $R \cong \mathbb{Z}^n$ (als abelsche Gruppen), wobei die Standardbasis der Ganzheitsbasis $a_1, \ldots, a_n$ entsprechen möge. Das von m in R erzeugte Ideal besteht aus allen $\mathbb{Z}$-Linearkombinationen der $ma_1, \ldots, ma_n$ und somit entspricht das Ideal (unter dieser Identifizierung) der von $(m, 0, \ldots, 0), (0, m, 0, \ldots, 0), \ldots, (0, \ldots, 0, m)$ erzeugten Untergruppe von $\mathbb{Z}^n$. Die Restklassengruppe $R/(m)$ ist demnach gleich $(\mathbb{Z}/(m))^n$ und besitzt m^n Elemente. Aufgrund der Ganzheit ist nach Aufgabe 17.19 $mR \cap \mathbb{Z} = m\mathbb{Z}$ und aufgrund des Homomorphiesatzes hat man einen injektiven Ringhomomorphismus

$$\mathbb{Z}/(m) \longrightarrow R/(m),$$

sodass $R/(m)$ eine von 0 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 nach Aufgabe 9.9 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). □

Noethersche Ringe und Dedekind-Bereiche

Emmy Noether (1882-1935)

Definition 18.12. Ein kommutativer Ring R heißt *noethersch*, wenn jedes Ideal darin endlich erzeugt ist.

Korollar 18.13. *Jeder Zahlbereich ist ein noetherscher Ring.*

Beweis. Nach Korollar 18.9 ist jedes von 0 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 18.14. *Zu einem Ideal $\mathfrak{a} \neq 0$ in einem Zahlbereich R ist der Restklassenring $R/\mathfrak{a}$ endlich.*

Beweis. Nach Lemma 18.5 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 Korollar 18.11 endlich (mit m^n Elementen), also besitzt der Ring rechts auch nur endlich viele Elemente. □

Satz 18.15. *Es sei R ein Zahlbereich. Dann ist jedes von 0 verschiedene Primideal von R bereits ein maximales Ideal.*

Beweis. Es 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 18.14 endlich. Ein endlicher Integritätsbereich ist aber nach Aufgabe 1.14 bereits ein Körper, sodass nach Lemma 16.15 ein maximales Ideal vorliegt. □

Richard Dedekind (1831-1916)

Die bisher etablierten Eigenschaften von Zahlbereichen lassen sich im folgenden Begriff zusammenfassen.

Definition 18.16. Einen Integritätsbereich R nennt man einen *Dedekindbereich*, wenn er noethersch und normal ist und wenn jedes von 0 verschiedene Primideal darin maximal ist.

Die Eigenschaft, dass jedes von 0 verschiedene Primideal maximal ist, bedeutet, dass die maximalen Ketten von Primidealen die Form $0 \subset \mathfrak{m}$ besitzen (wenn ein Körper vorliegt, so gibt es nur das einzige Primideal 0). Man sagt auch, dass die *Krulldimension* des Ringes gleich 1 ist.

Korollar 18.17. *Jeder Zahlbereich ist ein Dedekindbereich.*

Beweis. Dies folgt aus Satz 18.2, aus Korollar 18.13 und aus Satz 18.15. □

18. Arbeitsblatt

Übungsaufgaben

Aufgabe 18.1. Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung und es sei $R \subseteq L$ ein Unterring mit den folgenden Eigenschaften:

(1) R ist ganz über $\mathbb{Z}$.
(2) Es ist $Q(R) = L$.
(3) R ist normal.

Dann ist R der Ring der ganzen Zahlen von L.

Aufgabe 18.2. Es sei R ein Zahlbereich und es sei $R \subseteq S$ eine endliche Erweiterung von kommutativen Ringen. Es sei S ein normaler Integritätsbereich. Zeige, dass S ebenfalls ein Zahlbereich ist.

Aufgabe 18.3. Es sei R ein Zahlbereich und sei $f \in R$. Zeige, dass $N(f) \in (f)$ ist, dass also die Norm zum von f erzeugten Hauptideal gehört. Zeige durch ein Beispiel, dass dies für die Spur nicht gelten muss.

Aufgabe 18.4. Es sei R ein Zahlbereich und sei $f \in R$. Zeige, dass die Spur und die Norm von f ganzzahlig sind.

In den drei folgenden Aufgaben wird der Begriff des primitiven Polynoms verwendet:

Ein Polynom $F \in \mathbb{Z}[X]$ heißt *primitiv*, wenn die Koeffizienten von F teilerfremd sind.

Aufgabe 18.5. Es sei $F \in \mathbb{Z}[X]$ ein Polynom. Zeige, dass man F als $F = n\tilde{F}$ mit $n \in \mathbb{N}$ und primitivem $\tilde{F}$ schreiben kann.

Aufgabe 18.6. Es sei $F \in \mathbb{Z}[X]$ ein irreduzibles Polynom. Dann ist F, aufgefasst als Polynom in $\mathbb{Q}[X]$, ebenfalls irreduzibel.

Aufgabe 18.7. Es seien $F, G \in \mathbb{Z}[X]$ primitive Polynome. Zeige, dass dann auch das Produkt FG primitiv ist.

Aufgabe 18.8. Es sei R ein faktorieller Zahlbereich und $\mathbb{Z} \subseteq R$ die zugehörige Erweiterung. Zu einer Primzahl p sei

$$p = q_1^{r_1} \cdots q_k^{r_k}$$

die Primfaktorzerlegung von p in R (die q_i seien also paarweise nicht assoziiert). Zeige, dass die Primideale $\mathfrak{p}$ von R mit der Eigenschaft $\mathfrak{p} \cap \mathbb{Z} = (p)$ genau die Primideale der Form $\mathfrak{p} = (q_i)$ sind.

Aufgabe 18.9. Es sei R ein Zahlbereich und sei $f_1, \ldots, f_n \in R$ eine $\mathbb{Z}$-Basis von R. Zeige, dass dann der Betrag der Diskriminante

$$|\triangle(f_1, \ldots, f_n)|$$

minimal ist unter allen Diskriminanten von linear unabhängigen n-Tupeln aus R.

Aufgabe 18.10. Berechne die Diskriminante der Gaußschen Zahlen. Man gebe zwei wesentlich verschiedene $\mathbb{Z}$-Basen von $\mathbb{Z}[\mathrm{i}]$ an und überprüfe, dass die Diskriminanten übereinstimmen.

Aufgabe 18.11. Man gebe ein Beispiel für einen Dedekindbereich, wo jeder Restklassenring $\neq 0$ unendlich ist, und für einen Dedekindbereich, der einen Körper enthält und wo alle echten Restklassenringe endlich sind.

Aufgabe 18.12. Es sei R ein noetherscher, kommutativer Ring. Zeige, dass dann auch jeder Restklassenring $R/\mathfrak{a}$ noethersch ist.

Aufgabe 18.13. Es sei K ein Körper und sei

$$K[X_n,\, n \in \mathbb{N}]$$

der Polynomring über K in unendlich vielen Variablen. Man beschreibe darin ein nicht endlich erzeugtes Ideal und eine unendliche, echt aufsteigende Idealkette.

Die folgenden Aufgaben benutzen das Produkt von Idealen.

Zu zwei Idealen $\mathfrak{a}$ und $\mathfrak{b}$ in einem kommutativen Ring wird das *Produkt* durch

$$\mathfrak{ab} \,=\, \{a_1b_1 + a_2b_2 + \cdots + a_kb_k \mid a_i \in \mathfrak{a},\, b_i \in \mathfrak{b}\}$$

definiert.

Für das n-fache Produkt eines Ideals $\mathfrak{a}$ mit sich selbst schreibt man $\mathfrak{a}^n$.

Aufgabe 18.14. Zeige, dass das Produkt von Hauptidealen wieder ein Hauptideal ist.

Aufgabe 18.15. Es seien $\mathfrak{a}, \mathfrak{b} \subseteq R$ Ideale in einem kommutativen Ring R. Zeige, dass die Beziehung

$$\mathfrak{a} \cdot \mathfrak{b} \,\subseteq\, \mathfrak{a} \cap \mathfrak{b}$$

gilt.

Aufgabe 18.16. Es sei $\mathfrak{a} \subseteq R$ ein Ideal in einem kommutativen Ring R. Zeige, dass die Potenzen $\mathfrak{a}^n$, $n \in \mathbb{N}_+$, alle dasselbe Radikal besitzen.

Aufgabe 18.17. Es seien I und J Ideale in einem kommutativen Ring R und sei $n \in \mathbb{N}$. Zeige die Gleichheit

$$(I+J)^n \,=\, I^n + I^{n-1}J + I^{n-2}J^2 + \cdots + I^2J^{n-2} + IJ^{n-1} + J^n.$$

Aufgabe 18.18. Es sei K ein Körper. Wir betrachten in $K[X,Y]$ die beiden Primideale

$$\mathfrak{p} \,=\, (X) \,\subset\, (X,Y) \,=\, \mathfrak{m}.$$

Zeige, dass es kein Ideal $\mathfrak{a}$ mit

$$\mathfrak{p} \,=\, \mathfrak{a} \cdot \mathfrak{m}$$

gibt.

Es sei

$$\varphi\colon\ A \longrightarrow B$$

ein Ringhomomorphismus zwischen den kommutativen Ringen A und B. Zu einem Ideal $\mathfrak{a} \subseteq A$ nennt man das von $\varphi(\mathfrak{a})$ erzeugte Ideal das *Erweiterungsideal* von $\mathfrak{a}$ unter φ. Es wird mit $\mathfrak{a}B$ bezeichnet.

Aufgabe 18.19. Es sei

$$\varphi\colon\ A \longrightarrow B$$

ein Ringhomomorphismus und es seien $\mathfrak{a}_1, \mathfrak{a}_2$ Ideale in A. Beweise für die Erweiterungsideale die Gleichheiten

$$(\mathfrak{a}_1 + \mathfrak{a}_2)B \ = \ \mathfrak{a}_1 B + \mathfrak{a}_2 B$$

und

$$(\mathfrak{a}_1 \cdot \mathfrak{a}_2)B \ = \ (\mathfrak{a}_1 B) \cdot (\mathfrak{a}_2 B).$$

Aufgaben zum Abgeben

Aufgabe 18.20. (5 Punkte)

Es sei $R = \mathbb{Z}[X]/(X^4 + X^3 + X^2 + X + 1)$. Bestimme die Primideale in R, die über den Primzahlen $p = 2, 3, 5, 7$ liegen.

Aufgabe 18.21. (3 Punkte)

Es sei p eine Primzahl. Betrachte die endliche Körpererweiterung

$$\mathbb{Q} \subseteq L = \mathbb{Q}[X]/(X^3 - p)$$

vom Grad 3. Sei $f = aX^2 + bX + c \in L$ ein Element davon mit $a, b, c \in \mathbb{Q}$. Berechne das Minimalpolynom von f und man gebe die Koeffizienten davon explizit an. Bestimme insbesondere die Norm und die Spur von f.

Welche Bedingungen an a, b, c ergeben sich aus der Voraussetzung, dass f ganz über $\mathbb{Z}$ ist?

Aufgabe 18.22. (3 Punkte)

Es sei R ein Dedekindbereich und seien $\mathfrak{p}$ und $\mathfrak{q}$ verschiedene Primideale $\neq 0$. Dann gibt es einen Ringisomorphismus

$$R/\mathfrak{p} \cap \mathfrak{q} \longrightarrow R/\mathfrak{p} \times R/\mathfrak{q}.$$

Aufgabe 18.23. (4 Punkte)

Es sei R ein Dedekindbereich und seien $\mathfrak{p}$ und $\mathfrak{q}$ zwei verschiedene Primideale. Dann ist

$$\mathfrak{p} \cap \mathfrak{q} \ = \ \mathfrak{p} \cdot \mathfrak{q}.$$

Aufgabe 18.24. (4 Punkte)

Zeige: Ein kommutativer Ring R ist genau dann noethersch, wenn es in R keine unendliche echt aufsteigende Idealkette

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \mathfrak{a}_3 \subset \ldots$$

gibt.

19. Vorlesung - Endliche Körper

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 die folgende Aussage.

Satz 19.1. *Hauptidealbereiche sind Dedekindbereiche.*

Beweis. Die Normalität folgt aus Satz 3.7 und Satz 17.12. Die Eigenschaft noethersch folgt, da in einem Hauptidealbereich jedes Ideal sogar von einem Element erzeugt wird. Die Maximalität der von 0 verschiedenen Primideale folgt aus Satz 3.12. □

Definition 19.2. Es 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 $\mathbb{Z}$-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 $R = \mathbb{Z}[X]/(F)$, so wird die „Faser“ (diese Terminologie lässt sich genauer begründen) über p durch den Restklassenring $(\mathbb{Z}/(p))[X]/(\overline{F})$ beschrieben (den wir auch den *Faserring* über p nennen), wobei $\overline{F}$ 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

$$R/pR \cong (\mathbb{Z}/(p))[X]/(\overline{F}),$$

die auf allgemeinen Gesetzen für Ideale beruht. Sie besagt insbesondere, dass p ein Primelement in R genau dann ist, wenn $\overline{F}$ irreduzibel in $(\mathbb{Z}/(p))[X]$ ist. Insgesamt liegt eine endliche Erweiterung

$$\mathbb{Z}/(p) \subseteq (\mathbb{Z}/(p))[X]/(\overline{F})$$

vor. Dabei sind beide Ringe endlich (besitzen also nur endlich viele Elemente), und links steht ein endlicher Körper, sodass 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 $\overline{F}$).

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 $\varphi\colon \mathbb{Z} \to \mathbb{R}$, 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 0 oder von positiver Charakteristik $p > 0$. Jeder Körper umfasst einen kleinsten Körper, das ist der Körper der rationalen Zahlen $\mathbb{Q}$ bei Charakteristik 0 oder $\mathbb{Z}/(p)$ bei Charakteristik p.

Wir erinnern ferner an den Begriff des Frobeniushomomorphismus (siehe Aufgabe 4.18): Für einen Ring R der Charakteristik p (p eine 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. *Es 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 die Charakteristik 0 besitzen, und als Charakteristik eines Körpers kommt ansonsten nach Lemma 13.5 (Elemente der Algebra (Osnabrück 2024-2025)) 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. Es sei n die Dimension, $n \geq 1$. Dann hat man eine $\mathbb{Z}/(p)$-Vektorraumisomorphie

$$K \cong (\mathbb{Z}/(p))^n$$

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 19.7.

Lemma 19.4. *Es sei K ein Körper der Charakteristik p, es sei $q = p^e$, $e \geq 1$. Es sei*

$$M = \{x \in K \mid x^q = x\}.$$

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 benutzt haben. Insbesondere ist also $0, 1, -1 \in M$. Es ist $z^q = F^e(z)$ und der Frobeniushomomorphismus

$$F\colon K \longrightarrow K,\ x \longmapsto x^p,$$

ist ein Ringhomomorphismus nach Aufgabe 4.18. 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

$$\left(x^{-1}\right)^q = (x^q)^{-1} = x^{-1},$$

sodass auch das Inverse zu M gehört und in der Tat ein Körper vorliegt. □

Lemma 19.5. *Es sei K ein Körper der Charakteristik $p > 0$, sei $q = p^e$, $e \geq 1$. Das Polynom $X^q - X$ zerfalle über K in Linearfaktoren. Dann ist*

$$M = \{x \in K \mid x^q = x\}$$

ein Unterkörper von K mit q Elementen.

Beweis. Nach Lemma 19.4 ist M ein Unterkörper von K, und nach Satz 5.1 besitzt er höchstens q Elemente. Es ist also zu zeigen, dass $F = X^q - X$ keine mehrfache Nullstellen hat. Dies folgt aber aus der formalen Ableitung $F' = -1$ und Aufgabe 15.27. □

Wenn es also einen Erweiterungskörper $\mathbb{Z}/(p) \subseteq K$ gibt, über dem 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. *Es 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. Es sei $F = P_1 \cdots P_r$ die Zerlegung in Primpolynome in $K[X]$, und sei P_1 nicht linear. Dann ist

$$K \longrightarrow K[Y]/(P_1(Y)) =: K'$$

eine Körpererweiterung von K nach Satz 3.12. Wegen $P_1(Y) = 0$ in K' ist die Restklasse y von Y in K' eine Nullstelle von P_1. Daher gilt nach Lemma 19.8 (Lineare Algebra (Osnabrück 2024-2025)) 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 $K \subset K' \subset K'' \subset \ldots$, die stationär wird, sobald F in Linearfaktoren zerfällt. □

Satz 19.7. *Es 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 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. Es seien K und L zwei Körper mit q Elementen. Es sei $x \in K^\times$ ein primitives Element, das nach Satz 5.2 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. Es 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. *Es sei K ein Körper und $K \subseteq L$ 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 $L = K \times K$.

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 (mit $u \notin K$). 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 man ist im zweiten Fall, da ja $\epsilon^2 = 0$ gilt. Es sei also $c \neq d$ vorausgesetzt. Dann induzieren die beiden K-Algebrahomomorphismen $\varphi_1 \colon L \to K$, $u \mapsto c$, und $\varphi_2 \colon L \to K$, $u \mapsto d$, einen Homomorphismus

$$\varphi = \varphi_1 \times \varphi_2 \colon L \longrightarrow K \times K.$$

Dieser ist surjektiv, da $\varphi(1) = (1, 1)$ und

$$\varphi(u) = (c, d)$$

ist und diese Bildvektoren linear unabhängig über K 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. □

19. Arbeitsblatt

Übungsaufgaben

Aufgabe 19.1. Konstruiere einen Körper $\mathbb{F}_9$ mit 9 Elementen.

Aufgabe 19.2. Bestimme in $\mathbb{F}_9$ für jedes Element $\neq 0$ die multiplikative Ordnung. Man gebe insbesondere die primitiven Einheiten an.

Aufgabe 19.3. Es sei p eine Primzahl und F ein Körper mit p^2 Elementen. Welche Ringhomomorphismen zwischen $\mathbb{Z}/(p^2)$ und F gibt es? Man betrachte beide Richtungen.

Aufgabe 19.4. Es sei K ein Körper der positiven Charakteristik p. Sei $F\colon K \to K$ der Frobeniushomomorphismus. Zeige, dass genau die Elemente aus $\mathbb{Z}/(p)$ invariant unter F sind.

Aufgabe 19.5. Es sei K ein Körper der positiven Charakteristik p. Sei

$$\varphi = F^e\colon K \longrightarrow K,\, x \longmapsto x^{p^e}$$

die e-te Iteration des Frobeniushomomorphismus. Zeige, dass es maximal p^e Elemente gibt, die unter φ invariant sind, und dass diese Elemente einen Unterkörper von K bilden.

Aufgabe 19.6. Gehe zur Seite

Endliche Körper/Nicht Primkörper/Einige Operationstafeln

und erstelle für einen der dort angegebenen Körper Additions- und Multiplikationstafeln.

Aufgabe 19.7. Konstruiere endliche Körper mit $4, 8, 9, 16, 25, 27, 32, 49, 64, 81, 121, 125$ und 128 Elementen.

Aufgabe 19.8. Es sei $K \subseteq L$ eine Körpererweiterung von endlichen Körpern. Zeige, dass dies eine einfache Körpererweiterung ist.

Aufgabe 19.9. (a) Zeige, dass durch

$$K = \mathbb{Z}/(7)[T]/(T^3 - 2)$$

ein Körper mit 343 Elementen gegeben ist.

(b) Berechne in K das Produkt $(T^2+2T+4)(2T^2+5)$.
(c) Berechne das (multiplikativ) Inverse zu $T+1$.

Aufgabe 19.10. (a) Bestimme die Primfaktorzerlegung des Polynoms $F = X^3+X+2$ in $\mathbb{Z}/(5)[X]$.
(b) Zeige, dass durch

$$K = \mathbb{Z}/(5)[T]/(T^2-2)$$

ein Körper mit 25 Elementen gegeben ist.
(c) Bestimmen die Primfaktorzerlegung von $F = X^3+X+2$ über $K = \mathbb{Z}/(5)[T]/(T^2-2)$.

Aufgabe 19.11. Bestimme die Matrix des Frobeniushomomorphismus

$$\Phi\colon \mathbb{F}_{49} \longrightarrow \mathbb{F}_{49}$$

bezüglich einer geeigneten $\mathbb{F}_7$-Basis von $\mathbb{F}_{49}$.

Aufgabe 19.12. Es sei $\mathbb{F}_q$ ein endlicher Körper der Charakteristik ungleich 2. Zeige unter Verwendung der Isomorphiesätze, dass genau die Hälfte der Elemente aus $\mathbb{F}_q^\times$ ein Quadrat in $\mathbb{F}_q$ ist.

Aufgabe 19.13. Formuliere und beweise eine Version des Eulerschen Kriteriums für beliebige endliche Körper.

Aufgabe 19.14. Es sei K ein endlicher Körper der Charakteristik $p \neq 2$.

(a) Zeige, dass es in K Elemente gibt, die keine Quadratwurzel besitzen.
(b) Zeige, dass es eine endliche nichttriviale Körpererweiterung $K \subseteq L$ vom Grad zwei gibt.

Aufgabe 19.15. Es sei p eine Primzahl und $q = p^n$, $n \geq 2$. Zeige, dass $\mathbb{Z}/(p^n)$ kein Vektorraum über $\mathbb{Z}/(p)$ sein kann.

Aufgabe 19.16. Betrachte die kommutativen Ringe $\mathbb{Z}/(13)$, $\mathbb{Z}/(169)$ und $\mathbb{F}_{169}$. Bestimme alle Ringhomomorphismen zwischen diesen drei Ringen.

Aufgabe 19.17. Man gebe eine vollständige Liste aller kommutativer Ringe mit 6 Elementen.

Aufgabe 19.18. Es sei R ein Zahlbereich und es sei $\mathfrak{p} \neq 0$ ein Primideal. Zeige, dass die Norm von $\mathfrak{p}$ eine echte Primzahlpotenz ist.

Aufgabe 19.19. Es sei p eine Primzahl, $q = p^e$ mit $e \geq 1$ und sei $\mathbb{F}_q$ der Körper mit q Elementen und $R = \mathbb{F}_q[X]$ der Polynomring darüber. Zeige, dass jeder Restklassenring $R/\mathfrak{a}$ zu einem Ideal $\mathfrak{a} \neq 0$ endlich ist.

Aufgabe 19.20. Bestimme alle Lösungen der Gleichung

$$x^2 + y^2 + xy = 1$$

für die Körper $K = \mathbb{F}_2$, $\mathbb{F}_4$ und $\mathbb{F}_8$.

Aufgabe 19.21. Es sei K ein endlicher Körper mit q Elementen.

(1) Zeige, dass die Polynomfunktionen

$$\varphi_d \colon K \longrightarrow K,\, x \longmapsto x^d,$$

mit $0 \leq d < q$ linear unabhängig sind.

(2) Zeige, dass die Exponentialfunktionen

$$\psi_b \colon K \longrightarrow K,\, x \longmapsto b^x,$$

mit $0 \leq b < q$ linear unabhängig sind.

Aufgaben zum Abgeben

Aufgabe 19.22. (3 Punkte)

Es sei R ein Zahlbereich und sei $f_1, \ldots, f_n \in R$ eine $\mathbb{Z}$-Basis von R mit Diskriminante

$$\triangle(f_1, \ldots, f_n)\,.$$

Es sei $h \in R$. Zeige, dass $hf_1, \ldots, hf_n$ eine $\mathbb{Z}$-Basis des Hauptideals (h) bildet und dass gilt:

$$\min\{|\triangle(b_1, \ldots, b_n)| : (b_1, \ldots, b_n)\, \mathbb{Z}\text{-Basis von } (h)\} = N(h)^2\, |\triangle(f_1, \ldots, f_n)|\,.$$

Aufgabe 19.23. (3 Punkte)

Finde möglichst viele (nicht isomorphe) kommutative Ringe mit vier Elementen. Beweise, dass die Liste vollständig ist.

Aufgabe 19.24. (4 Punkte)

Es sei p eine Primzahl und $e, d \in \mathbb{N}_+$. Zeige: $\mathbb{F}_{p^d}$ ist genau dann ein Unterkörper von $\mathbb{F}_{p^e}$, wenn e ein Vielfaches von d ist.

Aufgabe 19.25. (4 Punkte)

Sei q eine echte Primzahlpotenz und $\mathbb{F}_q$ der zugehörige endliche Körper. Zeige, dass in $\mathbb{F}_{q^2}$ jedes Element aus $\mathbb{F}_q$ ein Quadrat ist.

Aufgabe 19.26. (7 Punkte)

Es sei K ein Körper und $K \subseteq L$ eine Ringerweiterung vom Grad drei. Klassifiziere die möglichen Typen von L, ähnlich wie in Lemma 19.9.

20. Vorlesung - Quadratische Zahlbereiche

Quadratische Zahlbereiche

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 keineswegs einfach, sondern zeigen bereits die Reichhaltigkeit der algebraischen Zahlentheorie.

Definition 20.2. Eine ganze Zahl heißt *quadratfrei*, wenn jeder Primfaktor von ihr nur mit einem einfachen Exponenten 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 quadratische Körpererweiterung der rationalen Zahlen wird durch ein normiertes irreduzibles Polynom beschrieben, das man durch quadratisches Ergänzen auf die Form $X^2 - q$ bringen kann. Durch Multiplikation mit einem Quadrat (siehe Aufgabe 7.2) kann man q durch eine quadratfreie ganze Zahl ersetzen. Die quadratische Körpererweiterung kann man als $\mathbb{Q} = \mathbb{Q}[\sqrt{D}]$ mit einer quadratfreien Zahl $D \neq 0, 1$ ansetzen. 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. Es sei $D \neq 0, 1$ quadratfrei und sei 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. Es sei $D \neq 0,1$ 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 $\sqrt{D} = \mathrm{i}\sqrt{-D}$ mit $\sqrt{-D}$ reell. Die Konjugation schickt dies dann auf $-\sqrt{D} = -\mathrm{i}\sqrt{-D}$, sodass 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 $x \in L$ über die Determinante und die Spur der Multiplikationsabbildung $f\colon L \to L$ 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 durch

$$\begin{pmatrix} a & bD \\ b & a \end{pmatrix}$$

gegeben. Somit ist

$$N(z) = a^2 - b^2 D = (a + b\sqrt{D})(a - b\sqrt{D}) = z\overline{z}$$

und

$$S(z) = 2a = (a + b\sqrt{D}) + (a - b\sqrt{D}) = z + \overline{z}.$$

Lemma 20.8. *Es 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 18.6, aus Satz 15.15, und aus der Gestalt des Minimalpolynoms (nämlich gleich $f^2 - S(f)f + N(f)$, falls $f \notin \mathbb{Q}$) im quadratischen Fall. □

Wir kommen zur expliziten Beschreibung eines quadratischen Zahlbereiches.

Satz 20.9. *Es sei $D \neq 0,1$ 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. Es 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 $a = \frac{n}{2}$ mit $n \in \mathbb{Z}$ ist. Sei $b = \frac{r}{s}$ 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), sodass $x \in \mathbb{Z}[\sqrt{D}]$ ist.

Es 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, sodass 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, sodass 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 Variable und eine Gleichung beschreiben. Für $D = 2, 3 \mod 4$ ist

$$A_D \cong \mathbb{Z}[\sqrt{D}] \cong \mathbb{Z}[X]/(X^2 - D).$$

Für

$$D = 1 \mod 4$$

setzt man häufig $\omega = \frac{1+\sqrt{D}}{2}$ für den Algebra-Erzeuger. Dieser Erzeuger erfüllt $\omega^2 - \omega - \frac{D-1}{4} = 0$. Wir haben also

$$A_D \cong \mathbb{Z}[\omega]/\left(\omega^2 - \omega - \frac{D-1}{4}\right).$$

Wir 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. *Es sei $D \neq 0,1$ 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 nach Satz 20.9 $A_D = \mathbb{Z}[X]/(X^2 - D)$ 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 komponentenweise 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

$$A_D = \mathbb{Z}[\omega]/\left(\omega^2 - \omega - \frac{D-1}{4}\right)$$

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

$$2\left(1 + \frac{D-1}{2}\right) - 1 = 2 + D - 1 - 1 = D.$$

□

Primideale in quadratischen Zahlbereichen

Bemerkung 20.11. Das Verhalten von Primzahlen in einer quadratischen Erweiterung lässt sich aus der oben erzielten Beschreibung mit Gleichungen erhalten.

Generell wird bei $R = \mathbb{Z}[X]/(F)$ das Verhalten von p in R durch $(\mathbb{Z}/(p))[X]/(\overline{F})$ beschrieben, wobei $\overline{F}$ bedeutet, dass die ganzzahligen Koeffizienten durch ihre Restklasse modulo p ersetzt werden. Wir nennen den Ring

$$R/(p) = \mathbb{Z}/(p)[X]/(\overline{F}) = \mathbb{Z}[X](p, F)$$

den *Faserring* über p.

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. Die prinzipiellen Möglichkeiten werden in Lemma 19.9 beschrieben. 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

$$R/(p) = \mathbb{Z}/(p)[\omega]/\left(\omega^2 - \omega - \frac{D-1}{4}\right).$$

Ist p ungerade, so ist 2 eine Einheit in $\mathbb{Z}/(p)$ und man kann quadratisch ergänzen. Dann ist

$$\omega^2 - \omega - \frac{D-1}{4} = \left(\omega - \frac{1}{2}\right)^2 - \frac{1}{4} - \frac{D-1}{4} = \left(\omega - \frac{1}{2}\right)^2 - \frac{D}{4}.$$

Der Faserring hat daher die Form $\mathbb{Z}/(p)[Y]/\left(Y^2 - \frac{D}{4}\right)$ und nach Multiplikation der Gleichung mit der Einheit 4 kann man dies als $\mathbb{Z}/(p)[Z]/(Z^2 - D)$ schreiben, sodass 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 darüber hinaus 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. *Es sei $D \neq 0, 1$ 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. Es sei zunächst $D = 2,3 \mod 4$, sodass $\triangle = 4D$ nach Lemma 20.10 ist und als Primteiler p der Diskriminante 2 und die Teiler von D in Frage kommen. Es ist

$$A_D/(p) = (\mathbb{Z}[X]/(X^2 - D)/(p)) = (\mathbb{Z}/(p))[X]/\big(X^2 - D\big).$$

Bei $p|D$ 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) mit $u \in \mathbb{Z}$. 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 $(X - D)^2 = X^2 - D^2 = X^2 - D$, sodass eine analoge Situation vorliegt.

Es sei jetzt $D = 1 \mod 4$ und sei p ein Primteiler von $\triangle = D$. Es ist

$$\begin{aligned} A_D/(p) &= \left(\mathbb{Z}[\omega]/\left(\omega^2 - \omega - \frac{D-1}{4}\right)\right)/(p) \\ &= (\mathbb{Z}/(p))[\omega]/\left(\omega^2 - \omega - \frac{D-1}{4}\right). \end{aligned}$$

Da D ungerade ist, ist 2 eine Einheit in $\mathbb{Z}/(p)$, sodass man die Gleichung modulo p als

$$\left(\omega - \frac{1}{2}\right)^2 - \frac{1}{4} - \frac{D-1}{4} = \left(\omega - \frac{1}{2}\right)^2 - \frac{D}{4} = \left(\omega - \frac{1}{2}\right)^2$$

schreiben kann, sodass wieder eine analoge Situation vorliegt. □

Zu einem Ideal $\mathfrak{a}$ bezeichnet $\overline{\mathfrak{a}}$ das *konjugierte Ideal*, das aus allen konjugierten Elementen aus $\mathfrak{a}$ besteht.

Satz 20.13. *Es sei $D \neq 0, 1$ 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 $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ mit $\mathfrak{p} \neq \overline{\mathfrak{p}}$ ist.

Beweis. Es 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, nämlich $\mathbb{Z}/(p)$. Nach der in Aufgabe 9.9 bewiesenen Korrespondenz gibt es also genau ein Primideal $\mathfrak{p}$ mit $(p) \subseteq \mathfrak{p}$ (das dem Ideal (ϵ) im Restklassenring entspricht). Dann ist $\mathfrak{p} = (p, \epsilon)$ (wobei hier ϵ ein Repräsentant in R sei) und $\mathfrak{p}^2 = (p)$.

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 18.23 ist $\mathfrak{p} \cap \mathfrak{q} = \mathfrak{p} \cdot \mathfrak{q}$. Mit $(p) \subset \mathfrak{p}$ ist auch $(p) \subset \overline{\mathfrak{p}}$. Wir zeigen, dass $\overline{\mathfrak{p}} = \mathfrak{q}$ ist, d.h., dass die beiden Primideale über p konjugiert vorliegen. Da nach Lemma 20.12 bei $p|\triangle$ 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. Es 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. Es seien a und $-a$ die beiden verschiedenen (!) Quadratwurzeln von D modulo p. Dann ist $\omega - \frac{1}{2} = \pm\frac{a}{2}$ und daher sind die beiden Primideale gleich $\left(p, \omega \pm a - \frac{1}{2}\right) = \left(p, \frac{a \pm \sqrt{D}}{2}\right)$, sodass 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 $(2, \omega) = \left(2, \frac{\sqrt{D}+1}{2}\right)$ und $(2, \omega - 1) = \left(2, \frac{\sqrt{D}+1}{2} - 1\right) = \left(2, \frac{\sqrt{D}-1}{2}\right)$, sodass wieder ein konjugiertes Paar vorliegt. □

20. Arbeitsblatt

Übungsaufgaben

Aufgabe 20.1. Bestimme den (Isomorphietyp des) Ganzheitsringes der quadratischen Körpererweiterung

$$\mathbb{Q} \subset \mathbb{Q}[X]/\left(X^2 + \frac{3}{2}X - \frac{5}{7}\right).$$

Aufgabe 20.2. Zeige, dass die Konjugation auf $\mathbb{Q}[\sqrt{D}]$ ein Körperautomorphismus und auf A_D ein Ringautomorphismus ist. Zeige, dass der Invariantenring gleich $\mathbb{Q}$ bzw. gleich $\mathbb{Z}$ ist.

Aufgabe 20.3. Es sei R ein quadratischer Zahlbereich. Zeige, dass die 1 Teil einer Ganzheitsbasis von R ist.

Aufgabe 20.4. Bestimme die Konjugation für $\sqrt{D}$ bzw. für ω in den verschiedenen expliziten Beschreibungen für die quadratischen Zahlbereiche.

Aufgabe 20.5. Bestimme die Spur für $\sqrt{D}$ bzw. für ω in den verschiedenen expliziten Beschreibungen für die quadratischen Zahlbereiche.

Aufgabe 20.6. Bestimme die Norm für $\sqrt{D}$ bzw. für ω in den verschiedenen expliziten Beschreibungen für die quadratischen Zahlbereiche.

Aufgabe 20.7. Es seien D und E zwei verschiedene quadratfreie Zahlen und seien A_D und A_E die zugehörigen quadratischen Zahlbereiche. Zeige

$$A_D \cap A_E = \mathbb{Z}.$$

Aufgabe 20.8. Bestimme ein Element aus $\mathbb{Z}[\sqrt{-11}]$, das unter allen Nichteinheiten minimale Norm besitzt. Begründe, dass dieses Element irreduzibel ist.

Aufgabe 20.9. Es sei $D \neq 0,1$ quadratfrei. Bestimme die Restklassengruppe $A_D/\mathbb{Z}[\sqrt{D}]$.

Aufgabe 20.10. Es sei D eine quadratfreie Zahl mit $D = 1 \mod 4$, und sei A_D der zugehörige quadratische Zahlbereich. Man gebe eine Ganzheitsgleichung für $\frac{1+\sqrt{D}}{2}$ über $\mathbb{Z}$ an. Man zeige, dass es keine echten Zwischenringe $\mathbb{Z}[\sqrt{D}] \subset R \subset A_D$ gibt.

Aufgabe 20.11. Bestimme für die quadratischen Zahlbereiche A_D mit negativem D sämtliche Einheiten.

Aufgabe 20.12. Für welche quadratfreien Zahlen mit

$$D = 1 \mod 4$$

ist $\frac{1+\sqrt{D}}{2}$ eine Einheit im quadratischen Zahlbereich A_D?

Aufgabe 20.13. Zeige, dass in $R = \mathbb{Z}[\sqrt{7}]$ das Element $8+3\sqrt{7}$ eine Einheit ist.

Aufgabe 20.14. Finde ein quadratfreies D derart, dass die natürliche Inklusion

$$\mathbb{Z}[\sqrt{D}] \subseteq A_D$$

die Eigenschaft besitzt, dass es zwei verschiedene Primideale $\mathfrak{q}$ und $\mathfrak{q}'$ in A_D gibt, die beide über dem gleichen Primideal $\mathfrak{p} \subset \mathbb{Z}[\sqrt{D}]$ liegen. Was ist $\mathfrak{p} \cap \mathbb{Z}$?

Aufgabe 20.15. Es sei R ein quadratischer Zahlbereich. Zeige, dass es nur endlich viele Primzahlen mit der Eigenschaft gibt, dass der Faserring über $\mathbb{Z}/(p)$ nicht reduziert ist.

Aufgabe 20.16. Es sei R ein quadratischer Zahlbereich. Zeige, dass die Konjugation zu jeder Primzahl p einen $\mathbb{Z}/(p)$-Algebraisomorphismus des Faserringes über p in sich selbst induziert. Beschreibe diesen in den drei möglichen Fällen im Sinne von Lemma 19.9 bzw. Satz 20.13.

Aufgaben zum Abgeben

Aufgabe 20.17. (5 Punkte)

Es sei $D \neq 0, 1$ eine quadratfreie Zahl und betrachte die quadratische Erweiterung $\mathbb{Z} \subset \mathbb{Z}[\sqrt{D}]$. Es sei p ein Primfaktor von D und es sei vorausgesetzt, dass weder p noch $-p$ ein Quadratrest modulo D/p ist. Dann ist p irreduzibel in $\mathbb{Z}[\sqrt{D}]$, aber nicht prim.

Aufgabe 20.18. (3 Punkte)

Es sei $R = \mathbb{Z}[\sqrt{7}]$. Bestimme die Primideale in R, die über $p = 29$ liegen und zeige, dass es sich um Hauptideale handelt.

Aufgabe 20.19. (4 Punkte)

Es sei $R = \mathbb{Z}[\sqrt{15}]$. Bestimme die Primideale in R, die über $p = 17$ liegen (man gebe Idealerzeuger an). Handelt es sich um Hauptideale?

Aufgabe 20.20. (3 Punkte)

Zeige, dass 2 im Ring $\mathbb{Z}[\sqrt{5}]$ irreduzibel, aber nicht prim ist. Wie sieht es in A_5 aus?

21. Vorlesung - Ideale in quadratischen Zahlbereichen

Ideale und ihre Norm in einem quadratischen Zahlbereich

Wir beschreiben nun die Ideale in einem quadratischen Zahlbereich genauer. Eine Strukturtheorie ist wichtig in Hinblick auf die Endlichkeit der Klassenzahl. Wir wissen aufgrund von Korollar 18.9, dass jedes von 0 verschiedene Ideal von zwei Elementen über $\mathbb{Z}$ erzeugt wird. Genauer gilt.

Satz 21.1. *Es sei A_D ein quadratischer Zahlbereich mit Ganzheitsbasis $1, \omega$ (im Sinne von Satz 20.9) und sei $\mathfrak{a}$ ein von 0 verschiedenes Ideal in A_D. Dann besitzt $\mathfrak{a}$ eine $\mathbb{Z}$-Basis aus zwei Elementen a und b, wobei $a \in \mathbb{N}$ mit $(a) = \mathbb{Z} \cap \mathfrak{a}$ und*

$$b = \alpha + \beta\omega$$

mit

$$\beta = \min\{|\tilde{\beta}| : \tilde{\alpha} + \tilde{\beta}\omega \in \mathfrak{a}, \tilde{\beta} \neq 0\}$$

gewählt werden kann.

Beweis. Es seien $a \in \mathbb{N}$ und $b = \alpha + \beta\omega$ wie im Satz beschrieben gewählt. Da a und β nicht 0 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 $n_1 a + n_2 b$ mit $n_1, n_2 \in \mathbb{Z}$ schreiben lässt. 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-Koeffizienten von Elementen in $\mathfrak{a}$, und β war betragsmäßig minimal gewählt, sodass 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.

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & A_D \\ \downarrow & & \downarrow \\ \mathbb{Z}/(a) & \longrightarrow & A_D/\mathfrak{a}\,. \end{array}$$

Wegen der surjektiven Abbildung $A_D/(a) \to A_D/\mathfrak{a}$ und aufgrund von Korollar 18.11 wissen wir, dass der Restklassenring maximal a^2 Elemente besitzt.

Beispiel 21.2. Wir betrachten im quadratischen Zahlbereich R zu $D = -5$ das Ideal

$$\mathfrak{p} = (2, 1+\sqrt{-5}).$$

Da es sich nicht um das Einheitsideal handelt, ist unmittelbar klar, dass bereits eine $\mathbb{Z}$-Basis im Sinne von Satz 21.1 vorliegt. Die Normen der beiden Elemente sind

$$N(2) = 4$$

und

$$N(1+\sqrt{-5}) = (1+\sqrt{-5})(1-\sqrt{-5}) = 6.$$

Der Restklassening ist

$$A_{-5}/\mathfrak{p} = A_{-5}/(2, 1+\sqrt{-5}) = \mathbb{Z}/(2)[\sqrt{-5}]/\left(1+\sqrt{-5}\right) = \mathbb{Z}/(2)$$

und besitzt zwei Elemente. Da dieser Restklassenring ein Körper ist, ist $\mathfrak{p}$ ein maximales Ideal.

Satz 21.3. *Es 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*

$$\{r + s\omega \mid 0 \leq r < a,\, 0 \leq s < \beta\}$$

repräsentiert. Insbesondere besitzt der Restklassenring $a \cdot \beta$ Elemente.

Beweis. Es 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.

Es seien nun $r + s\omega$ und $\tilde{r} + \tilde{s}\omega$ im angegebenen Bereich und angenommen, dass sie das gleiche Element im Restklassenring repräsentieren. Es 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 0 sein. Dann ist aber $\tilde{r} - r$ ein Vielfaches von a und wegen $|\tilde{r} - r| < a$ muss $\tilde{r} - r = 0$ sein, sodass also die beiden Elemente übereinstimmen und der Repräsentant eindeutig ist. □

Definition 21.4. Es sei $D \neq 0, 1$ quadratfrei und A_D der zugehörige quadratische Zahlbereich. Es sei $\mathfrak{a}$ ein von 0 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 Satz 21.3 wie folgt ausdrücken.

Korollar 21.5. *Es sei A_D ein quadratischer Zahlbereich mit $\mathbb{Z}$-Basis 1 und ω und sei $\mathfrak{a}$ ein von 0 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 21.3. □

Korollar 21.6. *Es sei A_D ein quadratischer Zahlbereich mit $\mathbb{Z}$-Basis 1 und ω und sei $\mathfrak{a}$ ein von 0 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*

$$N(\mathfrak{a}) = \left|\det \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix}\right|.$$

Beweis. Die Aussage ist für eine $\mathbb{Z}$-Basis der Form a und $b = \alpha + \beta\omega$, wie sie im Satz 21.1 konstruiert wurde, richtig. Für eine beliebige $\mathbb{Z}$-Basis u, v gibt es eine Übergangsmatrix M mit $u = Ma$ und $v = Mb$. Dabei ist M ganzzahlig und ihre Determinante hat den Betrag 1, sodass sich der Betrag der Determinante der Basis nicht ändert. □

Für ein Element und das davon erzeugte Hauptideal stimmen die beiden Normbegriffe überein.

Satz 21.7. *Es 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. Es 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

$$\begin{array}{ll} & N(f) \\ = & f\overline{f} \\ = & \begin{cases} \left(f_1 + f_2\sqrt{D}\right)\left(f_1 - f_2\sqrt{D}\right) = f_1^2 - f_2^2 D, & \text{falls } D = 2, 3 \mod 4, \\ \left(f_1 + \frac{1}{2}f_2 + \frac{f_2\sqrt{D}}{2}\right)\left(f_1 + \frac{1}{2}f_2 - \frac{f_2\sqrt{D}}{2}\right) = \left(f_1 + \frac{1}{2}f_2\right)^2 - \frac{f_2^2}{4}D, & \text{falls } D = 1 \mod 4. \end{cases} \end{array}$$

Wir berechnen nun die Norm des von f erzeugten Ideals $\mathfrak{a} = (f)$ mit Hilfe von Korollar 21.6. Eine $\mathbb{Z}$-Basis des Ideals ist offenbar durch f und $f\omega$ gegeben, wobei

$$f\omega = f_1\omega + f_2\omega^2 = \begin{cases} f_2 D + f_1\omega, & \text{falls } D = 2, 3 \mod 4, \\ f_2\frac{D-1}{4} + (f_1 + f_2)\omega, & \text{falls } D = 1 \mod 4 \end{cases}$$

ist. Im ersten Fall haben wir

$$\left|\det \begin{pmatrix} f_1 & f_2 D \\ f_2 & f_1 \end{pmatrix}\right| = \left|f_1^2 - f_2^2 D\right|$$

und im zweiten Fall ist

$$\begin{aligned}\left|\det\begin{pmatrix} f_1 & f_2\frac{D-1}{4} \\ f_2 & f_1+f_2 \end{pmatrix}\right| &= \left|f_1(f_1+f_2)-f_2^2\frac{D-1}{4}\right| \\ &= \left|f_1^2+f_1f_2+\frac{1}{4}f_2^2-\frac{1}{4}f_2^2D\right|,\end{aligned}$$

was mit den obigen Ergebnissen übereinstimmt. □

Beispiel 21.8. Wir betrachten im quadratischen Zahlbereich R zu $D = -5$ das Ideal

$$\mathfrak{p} = (2, 1+\sqrt{-5}).$$

Wir behaupten, dass es kein Hauptideal ist und verwenden dabei, dass die Norm dieses Ideals nach Beispiel 21.2 gleich 2 ist. Wäre nämlich $\mathfrak{p} = (f)$ mit einem $f \in R$, so müsste nach Satz 21.7 auch

$$|N(f)| = 2$$

gelten. Allerdings ist die Norm von $f = a+b\sqrt{-5}$ gleich $N(f) = a^2+5b^2$ und dies kann nicht gleich 2 sein.

Beispiel 21.9. Wir betrachten im quadratischen Zahlbereich R zu $D = -5$ das Ideal $\mathfrak{p} = (2, 1+\sqrt{-5})$, das nach Beispiel 21.8 kein Hauptideal ist. Es sei S der ganze Abschluss von R (oder von $\mathbb{Z}$) im Erweiterungskörper $L = \mathbb{Q}[\sqrt{-5}, \sqrt{2}]$ vom Grad vier über $\mathbb{Q}$. Wir haben also eine Kette

$$\mathbb{Z} \subset R \subset S$$

von Zahlbereichen. Wir behaupten, dass das Erweiterungsideal

$$\mathfrak{p}S = \big(2, 1+\sqrt{-5}\big)S$$

ein Hauptideal in S ist, und zwar behaupten wir, dass $\sqrt{2}$ ein Idealerzeuger davon ist. Dazu betrachten wir zunächst das rationale Element $z = \frac{\sqrt{2}+\sqrt{2}\cdot\sqrt{-5}}{2} = \frac{1+\sqrt{-5}}{\sqrt{2}} \in L$. Wegen

$$z^2 = \left(\frac{\sqrt{2}+\sqrt{2}\cdot\sqrt{-5}}{2}\right)^2 = \frac{2-2\cdot 5+4\sqrt{-5}}{4} = -2+\sqrt{-5} \in R$$

erfüllt z eine Ganzheitsgleichung über R und gehört somit zu S (ebenso, wenn im Zähler ein Minuszeichen steht). Die Gleichheit

$$\mathfrak{p}S = \left(\sqrt{2}\right)$$

folgt einerseits aus

$$2 = \sqrt{2}\cdot\sqrt{2}$$

und

$$1+\sqrt{-5} = z\cdot\sqrt{2}$$

und andererseits aus

$$-\sqrt{2}\cdot 2+\frac{1-\sqrt{-5}}{\sqrt{2}}(1+\sqrt{-5}) = -\sqrt{2}\cdot 2+\frac{6}{\sqrt{2}}$$

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

Satz 21.10. *Es sei A_D ein quadratischer Zahlbereich und sei $\mathfrak{a}$ ein von 0 verschiedenes Ideal in A_D. Dann gilt*

$$\mathfrak{a}\overline{\mathfrak{a}} = (N(\mathfrak{a})).$$

Beweis. Es sei $\mathfrak{a}$ durch eine $\mathbb{Z}$-Basis $a, b = \alpha + \beta\omega$ wie im Satz 21.1 gegeben. Das konjugierte Ideal $\overline{\mathfrak{a}}$ hat die Basis a und $\overline{b}$. Das Produktideal $\mathfrak{a}\overline{\mathfrak{a}}$ hat die vier Erzeuger

$$a^2, N(b), a\overline{b}, ab\,.$$

Wir behaupten, dass dieses Ideal gleich dem von $(a\beta)$ erzeugten Ideal ist, was ja nach Korollar 21.5 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 einerseits $a = \delta\beta$ 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

$$\mathfrak{a}\overline{\mathfrak{a}} = (\beta^2)\mathfrak{b}\overline{\mathfrak{b}}$$

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 $\mathfrak{a}\overline{\mathfrak{a}} = (a)$ zeigen. Aufgrund von $N(b) \in \mathfrak{a} \cap \mathbb{Z} = (a)$ haben wir die Inklusion $\mathfrak{a}\overline{\mathfrak{a}} \subseteq (a)$. Wir betrachten die Inklusionskette (in A_D)

$$\big(a^2, N(b), a\big(b + \overline{b}\big)\big) \subseteq \big(a^2, N(b), ab, a\overline{b}\big) = \mathfrak{a}\overline{\mathfrak{a}} \subseteq (a).$$

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 $\frac{ab}{c}$ und erhalten

$$N\left(\frac{ab}{c}\right) = \frac{N(a)N(b)}{N(c)} = \frac{a^2 N(b)}{c^2} \in \mathbb{Z}$$

und

$$S\left(\frac{ab}{c}\right) = \frac{1}{c}S(ab) = \frac{1}{c}(ab + a\overline{b}) \in \mathbb{Z}.$$

Damit gehören die Norm und die Spur zu $\mathbb{Z}$ und damit ist nach Lemma 20.8 das Element selbst ganz und somit 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 21.11. *Es sei A_D ein quadratischer Zahlbereich und seien $\mathfrak{a}$ und $\mathfrak{b}$ von Null verschiedene Ideale in A_D. Dann gilt*

$$N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b}).$$

Beweis. Wir wenden Satz 21.10 wiederholt für Ideale an und erhalten

$$(N(\mathfrak{ab})) = (\mathfrak{ab})\overline{(\mathfrak{ab})} = \mathfrak{ab}\overline{\mathfrak{a}}\overline{\mathfrak{b}} = \mathfrak{a}\overline{\mathfrak{a}}\mathfrak{b}\overline{\mathfrak{b}} = (N(\mathfrak{a}))(N(\mathfrak{b})).$$

Da die Norm eines Ideals stets positiv ist folgt aus dieser Idealidentität die Gleichheit $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$. □

Die obige Definition der Norm eines Ideals, die wir nur für quadratische Zahlbereiche gefasst haben, lässt sich auf beliebige Zahlbereiche erweitern. Dafür gelten entsprechende Eigenschaften, was wir im Rahmen dieser Vorlesung nicht ausführen werden.

Definition 21.12. Zu einem Ideal $\mathfrak{a} \neq 0$ in einem Zahlbereich R heißt die (endliche) Anzahl des Restklassenringes $R/\mathfrak{a}$ die *Norm* von $\mathfrak{a}$. Sie wird mit

$$N(\mathfrak{a})$$

bezeichnet.

21. Arbeitsblatt

Übungsaufgaben

Aufgabe 21.1. Es sei R ein quadratischer Zahlbereich mit der $\mathbb{Z}$-Basis 1 und ω und einem von 0 verschiedenen Ideal $\mathfrak{a}$. Zeige, dass

$$\{s \mid \text{Es gibt } r + s\omega \in \mathfrak{a}\}$$

ein Ideal in $\mathbb{Z}$ ist.

Aufgabe 21.2. Es sei R ein quadratischer Zahlbereich und $f \in \mathfrak{a}$, wobei $\mathfrak{a}$ ein von 0 verschiedenes Ideal bezeichnet. Zeige, dass $N(f)$ ein Vielfaches der Norm von $\mathfrak{a}$ ist.

Aufgabe 21.3. Es sei R ein quadratischer Zahlbereich und $\mathfrak{a}$ ein von 0 verschiedenes Ideal in R. Zeige

$$N(\mathfrak{a}) = \mathrm{GgT}(\{N(f) \mid f \in \mathfrak{a}\}).$$

Aufgabe 21.4. Es sei $R = A_D$ ein quadratischer Zahlbereich und $f \in R$ mit $(f) \cap \mathbb{Z} = (N(f))$. Zeige auf zwei verschiedene Arten, dass es (mit der Notation des Beweises von Satz 21.1) eine $\mathbb{Z}$-Basis des Ideals (f) gibt mit $\beta = 1$.

Aufgabe 21.5. Es sei R ein quadratischer Zahlbereich und $\mathfrak{a}$ ein Ideal in R mit der Eigenschaft, dass die Norm von $\mathfrak{a}$ eine Primzahl ist. Zeige, dass $\mathfrak{a}$ ein maximales Ideal ist.

Aufgabe 21.6. Es sei R ein quadratischer Zahlbereich und $\mathfrak{m}$ ein maximales Ideal in R. Zeige, dass es eine Primzahl p derart gibt, das $\mathfrak{m}$ eine $\mathbb{Z}$-Basis der Form p und $\alpha + p\omega$ oder der Form p und $\alpha + \omega$ besitzt.

Aufgabe 21.7. Es sei $A_{10} = \mathbb{Z}[\sqrt{10}]$ der quadratische Zahlbereich zu $D \in 10$. Bestimme gemäß Satz 21.1 eine $\mathbb{Z}$-Basis des Ideals $(3 + 4\sqrt{10})$ und bestimme damit die Norm des Ideals.

Aufgabe 21.8. Es sei $A_{-10} = \mathbb{Z}[\sqrt{-10}]$ der quadratische Zahlbereich zu $D = -10$. Man zeige, dass das Ideal $(6 + 5\sqrt{-10}, 3 - 2\sqrt{10})$ ein Hauptideal ist und man gebe dafür einen Erzeuger an.

Aufgabe 21.9. Es sei $A_7 = \mathbb{Z}[\sqrt{7}]$ der quadratische Zahlbereich zu $D = 7$. Bestimme gemäß Satz 21.1 eine $\mathbb{Z}$-Basis des Ideals $(3 + 2\sqrt{7})$ und bestimme damit die Norm des Ideals.

Aufgabe 21.10. Es sei $D = 2, 3 \mod 4$ eine quadratfreie Zahl und $f = n + m\sqrt{D}$. Es sei t der größte gemeinsame Teiler von n und m. Bestimme $(f) \cap \mathbb{Z}$ und β im Sinne von Satz 21.1.

Aufgabe 21.11. Es sei R ein Zahlbereich. Zeige unter Verwendung der Norm, dass jedes Element $f \in R$, $f \neq 0$, eine Faktorisierung in irreduzible Elemente besitzt.

Aufgabe 21.12. Es sei R ein quadratischer Zahlbereich und $\mathfrak{a} \subseteq R$ ein von 0 verschiedenes Ideal. Zeige, dass $\mathfrak{a}$ genau dann ein Hauptideal ist, wenn es ein Element $f \in \mathfrak{a}$ mit $|N(f)| = N(\mathfrak{a})$ gibt.

Aufgabe 21.13. Es sei $D \neq 0, 1$ eine quadratfreie Zahl mit $D = 1 \mod 4$. Es sei $\mathfrak{a} = (\omega)$ das Hauptideal im quadratischen Zahlbereich A_D. Zeige, dass der Durchschnitt $\mathfrak{a} \cap \mathbb{Z}[\sqrt{D}]$ kein Hauptideal in $\mathbb{Z}[\sqrt{D}]$ ist.

Aufgabe 21.14. Charakterisiere für den Ring

$$R = \mathbb{Z}[\frac{-1+\sqrt{3}\mathrm{i}}{2}] \cong \mathbb{Z}[Y]/(Y^2+Y+1)$$

der Eisenstein-Zahlen die Primzahlen aus $\mathbb{Z}$, die in R verzweigt sind, träge sind oder zerfallen.

Aufgabe 21.15. Es sei p eine Primzahl und betrachte die quadratische Erweiterung $\mathbb{Z}[\sqrt{p}]$. Zeige, dass dies eine dichte Untergruppe der reellen Zahlen ist.

Aufgaben zum Abgeben

Aufgabe 21.16. (3 Punkte)

Es sei H eine (additive) Untergruppe der reellen Zahlen $\mathbb{R}$. Zeige, dass entweder $H = \mathbb{Z}a$ mit einer eindeutig bestimmten nichtnegativen reellen Zahl a ist, oder aber H dicht in $\mathbb{R}$ ist.

Aufgabe 21.17. (3 Punkte)

Es sei R ein vom Nullring verschiedener kommutativer Ring. Zeige unter Verwendung des Lemmas von Zorn, dass es maximale Ideale in R gibt.

Aufgabe 21.18. (3 Punkte)

Es sei R ein quadratischer Zahlbereich und $\mathfrak{a} \subseteq \mathfrak{b}$ zwei von 0 verschiedene Ideale. Zeige, dass die Norm von $\mathfrak{b}$ die Norm von $\mathfrak{a}$ teilt.

Aufgabe 21.19. (4 Punkte)

Es sei D eine quadratfreie Zahl, sei $R = \mathbb{Z}[\sqrt{D}]$ und sei A_D der zugehörige Ganzheitsring. Zeige, dass für jede ungerade Primzahl p ein Isomorphismus

$$\mathbb{Z}[\sqrt{D}]/(p) \longrightarrow (A_D)/(p)$$

vorliegt. Zeige durch ein Beispiel, dass dies bei $p = 2$ nicht sein muss.

22. Vorlesung - Nenneraufnahme, Lokalisierung, Bewertungsringe

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 23.14). Für die erste Version benötigen wir die Begriffe Nenneraufnahme, Lokalisierung und diskreter Bewertungsring.

Nenneraufnahme

Definition 22.1. Es 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.

Es handelt sich also einfach um ein Untermonoid des multiplikativen Monoids eines Ringes.

Beispiel 22.2. Es 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 22.3. Es sei R ein Integritätsbereich. Dann bilden alle von 0 verschiedenen Elemente in R ein multiplikatives System, das mit $R^* = R \setminus \{0\}$ bezeichnet wird.

Beispiel 22.4. Es sei R ein kommutativer Ring und $\mathfrak{p}$ ein Primideal. Dann ist das Komplement $R \setminus \mathfrak{p}$ ein multiplikatives System. Dies folgt unmittelbar aus der Definition.

Definition 22.5. Es sei R ein Integritätsbereich und sei $S \subseteq R$ ein multiplikatives System, $0 \notin S$. Dann nennt man den Unterring

$$R_S := \left\{ \frac{f}{g} \mid f \in R, g \in S \right\} \subseteq Q(R)$$

die *Nenneraufnahme* zu S.

Für die Nenneraufnahme an einem Element f schreibt man einfach R_f statt $R_{\{f^n \mid n \in \mathbb{N}\}}$. Man kann eine Nenneraufnahme auch dann definieren, wenn R kein Integritätsbereich ist, siehe Aufgabe 22.12.

Definition 22.6. Es sei R ein Integritätsbereich und sei $\mathfrak{p}$ ein Primideal. Dann nennt man die Nenneraufnahme an $S = R \setminus \mathfrak{p}$ die *Lokalisierung* von R an $\mathfrak{p}$. Man schreibt dafür $R_{\mathfrak{p}}$. Es ist also

$$R_{\mathfrak{p}} := \left\{ \frac{f}{g} \mid f \in R,\, g \notin \mathfrak{p} \right\} \subseteq Q(R).$$

Für eine Primzahl $p \in \mathbb{Z}$ besteht $\mathbb{Z}_{(p)}$ aus allen rationalen Zahlen, die man ohne p im Nenner schreiben kann.

Definition 22.7. Ein kommutativer Ring R heißt *lokal*, wenn R genau ein maximales Ideal besitzt.

Der folgende Satz zeigt, dass diese Namensgebung Sinn ergibt.

Lemma 22.8. *Es 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*

$$\mathfrak{p}R_{\mathfrak{p}} := \left\{ \frac{f}{g} \mid f \in \mathfrak{p},\, g \notin \mathfrak{p} \right\}.$$

Beweis. Die angegebene Menge ist in der Tat ein Ideal in der Lokalisierung

$$R_{\mathfrak{p}} = \left\{ \frac{f}{g} \mid f \in R,\, g \notin \mathfrak{p} \right\}.$$

Wir zeigen, dass das Komplement von $\mathfrak{p}R_{\mathfrak{p}}$ nur aus Einheiten besteht, sodass es sich um ein maximales Ideal handeln muss. Es 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. □

Das Ideal $\mathfrak{p}R_{\mathfrak{p}}$ ist dabei das Erweiterungsideal zu $\mathfrak{p}$ unter dem Ringhomomorphismus $R \to R_{\mathfrak{p}}$.

Satz 22.9. *Es sei R ein Integritätsbereich mit Quotientenkörper $Q(R)$. Dann gilt*

$$R = \bigcap_{\mathfrak{m}\ maximal} R_{\mathfrak{m}},$$

wobei der Durchschnitt über alle maximale Ideale läuft und in $Q(R)$ genommen wird.

Beweis. Die Inklusion $\subseteq$ ist klar. Es 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 $q = \frac{a_{\mathfrak{m}}}{f_{\mathfrak{m}}}$. 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 $\mathfrak{m}_i$, $i = 1, \ldots, n$ und $r_i \in R$ mit

$$r_1 f_1 + \cdots + r_n f_n = 1,$$

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

$$q = q(r_1 f_1 + \cdots + r_n f_n) = q r_1 f_1 + \cdots + q r_n f_n = a_1 r_1 + \cdots + a_n r_n.$$

Also gehört q zu R. □

Satz 22.10. *Es sei R ein normaler Integritätsbereich und sei $S \subseteq R$ ein multiplikatives System. Dann ist auch die Nenneraufnahme R_S normal.*

Beweis. Siehe Aufgabe 22.33. □

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.

Wir wollen zeigen, dass zu einem Zahlbereich R die Lokalisierung an einem jeden Primideal ein diskreter Bewertungsring ist.

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, sodass 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 R mit Primelement p heißt die Zahl $n \in \mathbb{N}$ mit der Eigenschaft $f = up^n$, wobei u eine Einheit bezeichnet, 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. *Es sei R ein diskreter Bewertungsring mit maximalem Ideal $\mathfrak{m} = (p)$. Dann hat die Ordnung*

$$R \setminus \{0\} \longrightarrow \mathbb{N},\ f \longmapsto \operatorname{ord}(f),$$

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) Es ist $f \in \mathfrak{m}$ *genau dann, wenn* $\operatorname{ord}(f) \geq 1$ *ist.*
(4) Es ist $f \in R^\times$ *genau dann, wenn* $\operatorname{ord}(f) = 0$ *ist.*

Beweis. Siehe Aufgabe 22.37. □

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. *Es 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

$$M = \{\mathfrak{a} \text{ Ideal } \mid f^r \notin \mathfrak{a} \text{ für alle } r\}.$$

Diese Menge ist nicht leer, da sie das Nullideal enthält. Ferner ist sie induktiv geordnet (bezüglich der Inklusion). Ist nämlich $\mathfrak{a}_i$, $i \in I$, eine total geordnete Teilmenge von M, 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. Es sei dazu $g, h \in R$ und $gh \in \mathfrak{p}$, und sei $g, h \notin \mathfrak{p}$ angenommen. Dann hat man echte Inklusionen

$$\mathfrak{p} \subseteq \mathfrak{p} + (g), \mathfrak{p} + (h).$$

Wegen der Maximalität können die beiden Ideale rechts nicht zu M gehören, und das bedeutet, dass es Exponenten $r, s \in \mathbb{N}$ mit

$$f^r \in \mathfrak{p} + (g) \text{ und } f^s \in \mathfrak{p} + (h)$$

gibt. Dann ergibt sich der Widerspruch

$$f^r f^s \in \mathfrak{p} + (gh) \subseteq \mathfrak{p}.$$

□

Lemma 22.16. *Es 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. Es 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 $\mathfrak{p}$ in R 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

$$\left(\sum_{i=1}^{k} a_{i1} f_i\right)\left(\sum_{i=1}^{k} a_{i2} f_i\right) \cdots \left(\sum_{i=1}^{k} a_{in} f_i\right).$$

Ausmultiplizieren ergibt eine Linearkombination mit Monomen $f_1^{r_1} \cdots f_k^{r_k}$ und $\sum_{i=1}^{k} r_i = n$, sodass ein f_i mit einem Exponenten $\geq n/k = m$ vorkommt. Daher ist das Produkt 0. □

Satz 22.17. *Es 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) ⇒ (2) folgt direkt aus der Definition 22.11.

(2) ⇒ (3) folgt aus Satz 3.7.

(3) ⇒ (4) folgt aus Satz 17.12.

(4) ⇒ (5). Es 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 22.16 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

$$h := \frac{f}{g} \in Q(R)$$

(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 17.7 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. Es 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 einem $k \in \mathbb{N}$ und einer Einheit u schreiben kann. Andernfalls könnte man $f = \pi^n g_n$ mit beliebig großem n schreiben. Nach Lemma 22.16 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. *Es 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 Lemma 22.8, sodass es lediglich die beiden 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. *Es 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 Korollar 22.18 sind die beteiligten Lokalisierungen $R_{\mathfrak{m}}$ allesamt diskrete Bewertungsringe. □

22. Arbeitsblatt

Übungsaufgaben

Aufgabe 22.1. Es sei R ein Integritätsbereich und $S \subseteq R$ ein multiplikatives System. Zeige, dass die Primideale in R_S genau denjenigen Primidealen in R entsprechen, die mit S einen leeren Durchschnitt haben.

Aufgabe 22.2. Es sei R ein kommutativer Ring. Zeige, dass die Menge aller Nichtnullteiler in R ein multiplikatives System bildet.

Aufgabe 22.3. Es sei $A \subseteq \mathbb{Q}$ die Menge derjenigen rationalen Zahlen, die eine abbrechende Dezimalentwicklung besitzen. Zeige, dass A ein Unterring von $\mathbb{Q}$ ist und bestimme die Einheiten von A.

Aufgabe 22.4. Es sei $\mathbb{Z}_n$ die Nenneraufnahme zu n ($\mathbb{Z}_n$ besteht also aus allen rationalen Zahlen, die man mit einer Potenz von n als Nenner schreiben kann). Zeige, dass es nur endlich viele Unterringe R mit

$$\mathbb{Z} \subseteq R \subseteq \mathbb{Z}_n$$

gibt, und charakterisiere diese unter Verwendung der Primfaktorzerlegung von n.

Aufgabe 22.5. Es sei R ein Zahlbereich und seien $f, g \in \mathbb{Z}$ teilerfremde Zahlen. Zeige, dass für den (im Quotientenkörper $Q(R)$ genommenen) Durchschnitt

$$R_f \cap R_g = R$$

gilt.

Aufgabe 22.6. Es sei $T \subseteq \mathbb{P}$ eine Teilmenge der Primzahlen. Zeige, dass die Menge

$$R_T = \{q \in \mathbb{Q} \mid q \text{ lässt sich mit einem Nenner schreiben, in dem nur Primzahlen aus } T \text{ vorkommen}\}$$

ein Unterring von $\mathbb{Q}$ ist. Was ergibt sich bei $T = \emptyset$, $T = \{3\}$, $T = \{2, 5\}$, $T = \mathbb{P}$?

Aufgabe 22.7. Bestimme die Unterringe der rationalen Zahlen $\mathbb{Q}$, die lokal sind.

Aufgabe 22.8. Zeige, dass jeder Unterring von $\mathbb{Q}$ eine Nenneraufnahme ist.

Aufgabe 22.9. Es sei R ein Integritätsbereich und sei $S \subseteq R$ ein multiplikatives System, $0 \notin S$.

(1) Zeige, dass die Nenneraufnahme zu S, also R_S mit
$$R_S := \left\{ \frac{f}{g} \mid f \in R,\, g \in S \right\} \subseteq Q(R)$$
ein Unterring von $Q(R)$ ist.
(2) Zeige, dass nicht jeder Unterring von $Q(R)$ eine Nenneraufnahme ist.

Aufgabe 22.10. Es sei $R \subseteq S$ eine ganze Erweiterung von Integritätsbereichen und sei $F \subseteq R$ ein multiplikatives System. Zeige, dass dann auch die zugehörige Erweiterung $R_F \subseteq S_F$ ganz ist.

Aufgabe 22.11. Es sei $D \neq 0,1$ eine quadratfreie Zahl, sei $R = \mathbb{Z}[\sqrt{D}]$ und sei A_D der zugehörige Ganzheitsring. Zeige, dass nach Nenneraufnahme an 2 ein Ringisomorphismus
$$R_2 \longrightarrow (A_D)_2$$
vorliegt.

Aufgabe 22.12. Es sei R ein kommutativer Ring und $S \subseteq R$ ein multiplikatives System. Man definiert die *Nenneraufnahme*
$$R_S$$
schrittweise wie folgt. Es sei zunächst M die Menge der formalen Brüche mit Nenner in S, also
$$M = \left\{ \frac{r}{s} \mid r \in R,\, s \in S \right\}.$$
Zeige, dass durch
$$\frac{r}{s} \sim \frac{r'}{s'} \text{ genau dann, wenn es ein } t \in S \text{ mit } trs' = tr's \text{ gibt},$$
eine Äquivalenzrelation auf M definiert ist. Wir bezeichnen mit R_S die Menge der Äquivalenzklassen. Definiere auf R_S eine Ringstruktur und definiere einen Ringhomomorphismus $R \to R_S$.

Aufgabe 22.13. Es sei R ein kommutativer Ring und sei $e \in R$ ein idempotentes Element. Zeige, dass es eine natürliche Ringisomorphie
$$R_e \cong R/(1-e)$$
gibt.

Aufgabe 22.14. Es sei R ein kommutativer Ring, $f \in R$ ein Element und R_f die zugehörige Nenneraufnahme. Zeige, dass f genau dann nilpotent ist, wenn R_f der Nullring ist.

Aufgabe 22.15. Es seien R und A kommutative Ringe und sei $S \subseteq R$ ein multiplikatives System. Es sei

$$\varphi\colon\ R \longrightarrow A$$

ein Ringhomomorphismus derart, dass $\varphi(s)$ eine Einheit in A ist für alle $s \in S$. Zeige: Dann gibt es einen eindeutig bestimmten Ringhomomorphismus

$$\tilde{\varphi}\colon\ R_S \longrightarrow A,$$

der φ fortsetzt.

Aufgabe 22.16. Es sei R ein kommutativer Ring, $S \subseteq R$ ein multiplikatives System und M ein R-Modul. Definiere die „Nenneraufnahme“

$$M_S$$

und zeige, dass sie ein R_S-Modul ist.

Aufgabe 22.17. Es sei R ein kommutativer Ring. Zeige, dass R genau dann ein lokaler Ring ist, wenn $a+b$ nur dann eine Einheit ist, wenn a oder b eine Einheit ist.

Lemma 22.8 gilt auch ohne die Voraussetzung, dass R ein Integritätsbereich ist.

Aufgabe 22.18. Es sei R ein kommutativer Ring und sei $\mathfrak{p}$ ein Primideal in R. Zeige, dass die Lokalisierung $R_{\mathfrak{p}}$ ein lokaler Ring mit maximalem Ideal

$$\mathfrak{p}R_{\mathfrak{p}} := \left\{ \frac{f}{g} \mid f \in \mathfrak{p},\, g \notin \mathfrak{p} \right\}$$

ist.

Aufgabe 22.19. Es sei R ein Integritätsbereich. Zeige, dass die folgenden Eigenschaften äquivalent sind.

(1) R ist normal.
(2) Für jedes Primideal $\mathfrak{p}$ ist die Lokalisierung $R_{\mathfrak{p}}$ normal.
(3) Für jedes maximale Ideal $\mathfrak{m}$ ist die Lokalisierung $R_{\mathfrak{m}}$ normal.

Aufgabe 22.20. Es sei K ein Körper und sei

$$\nu\colon\ (K^\times,\cdot,1) \longrightarrow (\mathbb{Z},+,0)$$

ein surjektiver Gruppenhomomorphismus mit $\nu(f+g) \geq \min\{\nu(f),\nu(g)\}$ für alle $f,g \in K^\times$. Zeige, dass

$$R = \left\{f \in K^\times \mid \nu(f) \geq 0\right\} \cup \{0\}$$

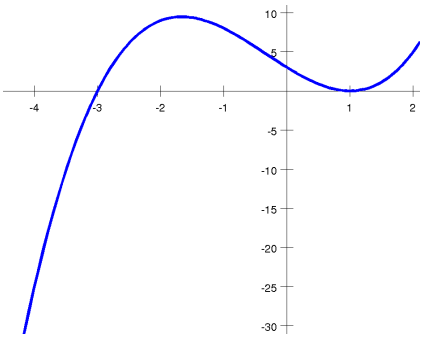
ein diskreter Bewertungsring ist.

Aufgabe 22.21. Es sei R ein diskreter Bewertungsring mit Quotientenkörper Q. Zeige, dass es keinen echten Zwischenring zwischen R und Q gibt.

Aufgabe 22.22. Es sei R ein diskreter Bewertungsring. Definiere zu einem Element $q \in Q(R)$, $q \neq 0$, die Ordnung

$$\operatorname{ord}(q) \in \mathbb{Z}.$$

Dabei soll die Definition mit der Ordnung für Elemente aus R übereinstimmen und einen Gruppenhomomorphismus $Q(R) \setminus \{0\} \to \mathbb{Z}$ definieren. Was ist der Kern dieses Homomorphismus?



Aufgabe 22.23. Es sei $f \in \mathbb{C}[X]$, $f \neq 0$, und $a \in \mathbb{C}$. Zeige, dass die folgenden „Ordnungen“ von f an der Stelle a übereinstimmen.

(1) Die Verschwindungsordnung von f an der Stelle a, also die maximale Ordnung einer Ableitung mit $f^{(k)}(a) = 0$.
(2) Der Exponent des Linearfaktors $X-a$ in der Zerlegung von f in irreduzible Polynome.
(3) Die Ordnung von f an der Lokalisierung $\mathbb{C}[X]_{(X-a)}$ von $\mathbb{C}[X]$ am maximalen Ideal $(X-a)$.

Aufgabe 22.24. Bestimme ein Polynom $P \in \mathbb{C}[X]$ minimalen Grades, das an der Stelle 3 mit der Ordnung zwei verschwindet, das an der Stelle i mit der Ordnung fünf verschwindet und das an den Stellen $0, 3-2\mathrm{i}$ und $7\mathrm{i}$ einfach verschwindet.

Aufgabe 22.25. Es sei K ein Körper und $K(T)$ der Körper der rationalen Funktionen über K. Finde einen diskreten Bewertungsring $R \subseteq K(T)$ mit $Q(R) = K(T)$ und mit $R \cap K[T] = K$.

Aufgabe 22.26. Es sei R ein kommutativer Ring und sei $\mathfrak{p}$ ein Primideal. Dann ist der Restklassenring $S = R/\mathfrak{p}$ ein Integritätsbereich mit Quotientenkörper $Q = Q(S)$ und $R_{\mathfrak{p}}$ ist ein lokaler Ring mit dem maximalen Ideal $\mathfrak{p}R_{\mathfrak{p}}$. Zeige, dass eine natürliche Isomorphie

$$Q(S) \cong R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$$

vorliegt.

Den in der vorstehenden Aufgabe beschriebenen Körper nennt man auch den *Restekörper* von $\mathfrak{p}$

man bezeichnet ihn mit $\kappa(\mathfrak{p})$. Die Abbildung

$$R \longrightarrow \kappa(\mathfrak{p}),\, f \longmapsto f \mod \mathfrak{p},$$

(aufgefasst in diesem Körper) heißt auch die *Auswertungsabbildung* (oder *Evaluationsabbildung*) an der Stelle $\mathfrak{p}$.

Aufgabe 22.27. Es sei R ein kommutativer Ring und

$$\varphi\colon\, R \longrightarrow K$$

ein Ringhomomorphismus in einen Körper K. Zeige, dass es eine eindeutig bestimmte Faktorisierung

$$R \longrightarrow \kappa(\mathfrak{p}) \longrightarrow K$$

mit einem Restekörper $\kappa(\mathfrak{p})$ zu einem Primideal $\mathfrak{p}$ gibt.

Aufgabe 22.28. Zeige, dass zu $a \in \mathbb{C}$ der Einsetzungshomomorphismus

$$\mathbb{C}[X] \longrightarrow \mathbb{C},\, X \longmapsto a,$$

mit der Evaluationsabbildung (in den Restekörper $\mathbb{C}[X]_{(X-a)}/(X-a)\mathbb{C}[X]_{(X-a)}$) zum Primideal $(X-a)$ übereinstimmt.

Aufgabe 22.29. Es sei R ein diskreter Bewertungsring mit Quotientenkörper Q. Charakterisiere die endlich erzeugten R-Untermoduln von Q. Auf welche Form kann man ein Erzeugendensystem bringen?

Aufgabe 22.30. Es sei R ein Integritätsbereich mit Quotientenkörper $K = Q(R)$. Es sei $R = \bigcap_{i \in I} R_i$, wobei die $R_i \subseteq K$, $i \in I$, alle diskrete Bewertungsringe seien. Zeige: R ist normal.

Aufgabe 22.31. Beschreibe die nilpotenten Elemente von $\mathbb{Z}/(n)$ und die Reduktion von $\mathbb{Z}/(n)$.

Aufgaben zum Abgeben

Aufgabe 22.32. (4 Punkte)

Es seien n und k teilerfremde Zahlen und sei $\mathbb{Z} \subseteq R$ ein kommutativer Ring. Zeige, dass es eine Ringisomorphie

$$R/(n) \cong (R_k)/(n)$$

gibt.

Aufgabe 22.33. (3 Punkte)

Es sei R ein normaler Integritätsbereich und sei $S \subseteq R$ ein multiplikatives System. Zeige, dass dann auch die Nenneraufnahme R_S normal ist.

Aufgabe 22.34. (3 Punkte)

Es sei R ein Integritätsbereich, sei $f \in R$ und sei $\mathfrak{a}$ ein Ideal. Zeige, dass $f \in \mathfrak{a}$ genau dann ist, wenn für alle Lokalisierungen $R_{\mathfrak{p}}$ gilt, dass $f \in \mathfrak{a}R_{\mathfrak{p}}$ ist.

Aufgabe 22.35. (7 Punkte)

Es sei $n \geq 2$ eine natürliche Zahl. Zeige, dass die folgenden Aussagen äquivalent sind.

(1) n ist die Potenz einer Primzahl.
(2) Der Restklassenring $\mathbb{Z}/(n)$ ist zusammenhängend.
(3) Der Restklassenring $\mathbb{Z}/(n)$ ist lokal.
(4) Die Reduktion von $\mathbb{Z}/(n)$ ist ein Körper.
(5) Jeder Nullteiler von $\mathbb{Z}/(n)$ ist nilpotent.
(6) Der Restklassenring $\mathbb{Z}/(n)$ besitzt genau ein Primideal.
(7) Der Restklassenring $\mathbb{Z}/(n)$ besitzt genau ein maximales Ideal.

Aufgabe 22.36. (4 Punkte)

Es sei $D \neq 1$ quadratfrei und $D = 1 \mod 4$. Finde in $\mathbb{Z}[\sqrt{D}]$ ein Primideal $\mathfrak{p}$ derart, dass die Lokalisierung an $\mathfrak{p}$ kein diskreter Bewertungsring ist.

Aufgabe 22.37. (4 Punkte)

Es sei R ein diskreter Bewertungsring mit maximalem Ideal $\mathfrak{m} = (p)$. Zeige, dass die Ordnung

$$R \setminus \{0\} \longrightarrow \mathbb{N},\ f \longmapsto \operatorname{ord}(f),$$

folgende Eigenschaften besitzt.

(1) $\operatorname{ord}(fg) = \operatorname{ord}(f) + \operatorname{ord}(g)$.
(2) $\operatorname{ord}(f+g) \geq \min(\operatorname{ord}(f), \operatorname{ord}(g))$.
(3) Es ist $f \in \mathfrak{m}$ genau dann, wenn $\operatorname{ord}(f) \geq 1$ ist.
(4) Es ist $f \in R^\times$ genau dann, wenn $\operatorname{ord}(f) = 0$ ist.

23. Vorlesung - Ideale und effektive Divisoren in Zahlbereichen

Die Ordnung an einem Primideal

Zu einem Zahlbereich R und einem Primideal $\mathfrak{p} \neq 0$ ist nach Korollar 22.18 die Lokalisierung $R_\mathfrak{p}$ ein diskreter Bewertungsring und somit ergibt sich insgesamt eine Abbildung

$$R \setminus \{0\} \longrightarrow R_\mathfrak{p} \setminus \{0\} \xrightarrow{\operatorname{ord}} \mathbb{N}.$$

Definition 23.1. Es sei R ein Zahlbereich, $\mathfrak{p} \neq 0$ ein Primideal in R und $f \in R$, $f \neq 0$. Dann heißt die Ordnung $\operatorname{ord}(f)$ 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 $\operatorname{ord}_\mathfrak{p}(f)$ bezeichnet.

Lemma 23.2. *Es sei R ein Zahlbereich und $\mathfrak{p} \neq 0$ ein Primideal in R. Dann hat die Ordnung an $\mathfrak{p}$, also die Abbildung*

$$R \setminus \{0\} \longrightarrow \mathbb{N},\ f \longmapsto \operatorname{ord}_\mathfrak{p}(f),$$

folgende Eigenschaften.

(1) $\operatorname{ord}_\mathfrak{p}(fg) = \operatorname{ord}_\mathfrak{p}(f) + \operatorname{ord}_\mathfrak{p}(g)$.
(2) $\operatorname{ord}_\mathfrak{p}(f+g) \geq \min(\operatorname{ord}_\mathfrak{p}(f), \operatorname{ord}_\mathfrak{p}(g))$.
(3) Es ist $f \in \mathfrak{p}$ genau dann, wenn $\operatorname{ord}_\mathfrak{p}(f) \geq 1$.

Beweis. (1) und (2) folgen direkt aus Lemma 22.14. Bei (3) ist zu beachten, dass für $f \in R$ gilt, dass $f \in \mathfrak{p}$ genau dann gilt, wenn $f \in \mathfrak{p}R_\mathfrak{p}$ ist. Letzteres bedeutet nämlich, dass $f = q_1 f_1 + \cdots + q_n f_n$ mit $f_i \in \mathfrak{p}$ und $q_i \in R_\mathfrak{p}$ ist, 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 $sf = a_1 f_1 + \cdots + a_n f_n \in \mathfrak{p}$, woraus $f \in \mathfrak{p}$ folgt. Damit folgt die Behauptung aus Lemma 22.14. □

Definition 23.3. Es 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 $\operatorname{ord}_{\mathfrak{p}}(f)$ zuordnet, der durch f definierte *Hauptdivisor*. Er wird mit $\operatorname{div}(f)$ bezeichnet und als formale Summe

$$\operatorname{div}(f) = \sum_{\mathfrak{p}} \operatorname{ord}_{\mathfrak{p}}(f) \cdot \mathfrak{p}$$

geschrieben.

Die Ordnung an einem Primideal nennt man in diesem Zusammenhang auch die Verschwindungsordnung. Die Ordnung ist ja genau dann positiv, wenn f zum Primideal $\mathfrak{p}$ gehört, und dies ist genau dann der Fall, wenn unter der Abbildung

$$R \longrightarrow R/\mathfrak{p} \longrightarrow Q(R/\mathfrak{p})$$

das Element f auf 0 abgebildet wird, also an dieser Stelle verschwindet. Eine höhere Verschwindungsordnung bedeutet, dass f nicht nur einfach, sondern mit einer gewissen Vielfachheit verschwindet. Der Hauptdivisor zu f notiert also, mit welcher Verschwindungsordnung die Funktion f an den verschiedenen Primstellen verschwindet.

Bemerkung 23.4. Es sei R ein faktorieller Zahlbereich. Dann lässt sich der Hauptdivisor zu einem Ringelement $f \in R$, $f \neq 0$, unmittelbar aus der Primfaktorzerlegung ablesen. Wenn

$$f = up_1^{r_1} \cdots p_k^{r_k}$$

mit einer Einheit u und paarweise nicht assoziierten Primelementen p_i ist, so ist der Hauptdivisor zu f gleich

$$\operatorname{div}(f) = \sum_{i=1}^{k} r_i(p_i).$$

Dies beruht einfach darauf, dass die Ordnung von f in der Lokalisierung $R_{(p_i)}$ gleich r_i ist.

Lemma 23.5. *Es sei R ein Zahlbereich. Dann hat die Abbildung, die einem Ringelement $\neq 0$ den Hauptdivisor zuordnet, also*

$$R \setminus \{0\} \longrightarrow \text{Hauptdivisoren}, \ f \longmapsto \operatorname{div}(f),$$

folgende Eigenschaften.

(1)

$$\operatorname{div}(fg) = \operatorname{div}(f) + \operatorname{div}(g).$$

(2)

$$\operatorname{div}(f+g) \geq \min(\operatorname{div}(f), \operatorname{div}(g)).$$

Hierbei sind die Operationen rechts punktweise definiert.

Beweis. Dies folgt direkt aus Lemma 23.2 durch Betrachtung an den einzelnen Primidealen. □

Lemma 23.6. *Es 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 $\operatorname{ord}_{\mathfrak{p}}(f)$ von 0 verschieden. Das heißt, dass der Hauptdivisor $\operatorname{div}(f) = \sum_{\mathfrak{p}} \operatorname{ord}_{\mathfrak{p}}(f) \cdot \mathfrak{p}$ eine endliche Summe ist.*

Beweis. Es 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 $\operatorname{ord}_{\mathfrak{p}}(f) = 0$. Da der Restklassenring $R/(f)$ nach Satz 18.14 endlich ist, folgt sofort, dass f nur in endlich vielen Primidealen enthalten ist, und nur für diese ist $\operatorname{ord}_{\mathfrak{p}}(f) > 0$. □

Effektive Divisoren

Definition 23.7. Es 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 $\mathfrak{p}$.

Lemma 23.6 zeigt, dass ein Hauptdivisor zu einem Ringelement 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.

Ein effektiver Divisor gibt für jede Primstelle eine Verschwindungsordnung an. Eine naheliegende Frage ist dann, ob dieses Ordnungsverhalten durch eine Funktion realisiert werden kann, also ob der Divisor ein Hauptdivisor ist.

Definition 23.8. Es sei R ein Zahlbereich und $\mathfrak{a} \neq 0$ ein von 0 verschiedenes Ideal in R. Dann nennt man den Divisor

$$\operatorname{div}(\mathfrak{a}) = \sum_{\mathfrak{p}} m_{\mathfrak{p}} \cdot \mathfrak{p}$$

mit

$$m_{\mathfrak{p}} = \operatorname{ord}_{\mathfrak{p}}(\mathfrak{a}) := \min\left(\operatorname{ord}_{\mathfrak{p}}(f) | f \in \mathfrak{a},\, f \neq 0\right)$$

den *Divisor zum Ideal* $\mathfrak{a}$.

Bemerkung 23.9. Man kann den Divisor zu einem Ideal auch durch

$$\operatorname{div}(\mathfrak{a}) = \min\left\{\operatorname{div}(f) \mid f \in \mathfrak{a},\, f \neq 0\right\}$$

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 0 verschieden ist, gilt das erst recht für den Divisor zu einem Ideal.

Die Ordnung $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})$ kann man auch als Ordnung des Ideals $\mathrm{ord}(\mathfrak{a}R_{\mathfrak{p}})$ im diskreten Bewertungsring $R_{\mathfrak{p}}$ ansehen. Dabei ist $\mathfrak{a}R_{\mathfrak{p}}$ das Erweiterungsideal zu $\mathfrak{a}$ in $R_{\mathfrak{p}}$. Dieses Ideal hat einen Erzeuger p^k, wobei p ein Primelement im diskreten Bewertungsring ist; die Ordnung ist dann k.

Lemma 23.10. *Es sei R ein Zahlbereich. Dann erfüllt die Zuordnung (für von 0 verschiedene Ideale)*

$$\mathfrak{a} \longmapsto \mathrm{div}(\mathfrak{a})$$

folgende Eigenschaften.

(1)

$$\mathrm{div}(\mathfrak{p}) = 1 \cdot \mathfrak{p}$$

für ein Primideal $\mathfrak{p} \neq 0$.

(2)

$$\mathrm{div}(\mathfrak{a} \cdot \mathfrak{b}) = \mathrm{div}(\mathfrak{a}) + \mathrm{div}(\mathfrak{b}).$$

(3) Für $\mathfrak{a} \subseteq \mathfrak{b}$ ist $\mathrm{div}(\mathfrak{a}) \geq \mathrm{div}(\mathfrak{b})$.

(4)

$$\mathrm{div}(\mathfrak{a} + \mathfrak{b}) = \min\{\mathrm{div}(\mathfrak{a}), \mathrm{div}(\mathfrak{b})\}.$$

Beweis. (1) Für jedes Element $f \in \mathfrak{p}$ gilt auch $f \in \mathfrak{p}R_{\mathfrak{p}}$ und daher ist $\mathrm{ord}_{\mathfrak{p}}(f) \geq 1$. 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 $p = \frac{a}{b}$ mit $a, b \in R$ und $b \notin \mathfrak{p}$ schreiben. Dabei ist $a \in \mathfrak{p}$ und a hat in $R_{\mathfrak{p}}$ die Ordnung 1.

Es 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 $h = \sum_{i=1}^{k} f_i g_i$ mit $f_i \in \mathfrak{a}$ und $g_i \in \mathfrak{b}$. Dann ist nach Fakt

$$\begin{aligned} \mathrm{div}(h) &\geq \min\{\mathrm{div}(f_i g_i) : i = 1, \ldots, k\} \\ &\geq \min\{\mathrm{div}(f_i) + \mathrm{div}(g_i) : i = 1, \ldots, k\} \\ &\geq \mathrm{div}(\mathfrak{a}) + \mathrm{div}(\mathfrak{b}). \end{aligned}$$

Für die Umkehrung schreiben wir $\mathrm{div}(\mathfrak{a}) = \sum_{\mathfrak{q}} n_{\mathfrak{q}} \cdot \mathfrak{q}$ und $\mathrm{div}(\mathfrak{b}) = \sum_{\mathfrak{q}} m_{\mathfrak{q}} \cdot \mathfrak{q}$. Zu fixiertem $\mathfrak{p}$ gibt es ein $f \in \mathfrak{a}$ und ein $g \in \mathfrak{b}$ mit $\mathrm{ord}_{\mathfrak{p}}(f) = n_{\mathfrak{p}}$ und $\mathrm{ord}_{\mathfrak{p}}(g) = m_{\mathfrak{p}}$. Dann ist $fg \in \mathfrak{a}\mathfrak{b}$ und

$$\mathrm{ord}_{\mathfrak{p}}(fg) = \mathrm{ord}_{\mathfrak{p}}(f) + \mathrm{ord}_{\mathfrak{p}}(g) = n_{\mathfrak{p}} + m_{\mathfrak{p}}.$$

(3) Das ist trivial.

(4) Die Abschätzung „$\geq$“ folgt aus $\mathrm{div}(f+g) \geq \min(\mathrm{div}(f), \mathrm{div}(g))$. Die Abschätzung „$\leq$“ folgt aus Teil (3). □

Definition 23.11. Es 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

$$\{f \in R \mid \operatorname{div}(f) \geq D\}$$

das *Ideal zum Divisor* D. Es wird mit $\mathrm{Id}(D)$ 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 $\mathrm{Id}(D)$. 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 $0 \neq f_i \in \mathfrak{p}_i$ mit $\operatorname{ord}_{\mathfrak{p}_i}(f_i) = 1$ 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 0 verschiedenen Idealen in einem Zahlbereich invers zueinander sind. Dies sollte man als eine einfache und übersichtliche Beschreibung für die Menge aller Ideale ansehen.

Satz 23.12. *Es sei R ein Zahlbereich. Dann sind die Zuordnungen*

$$\mathfrak{a} \longmapsto \operatorname{div}(\mathfrak{a}) \text{ und } D \longmapsto \mathrm{Id}(D)$$

zueinander inverse Abbildungen zwischen der Menge der von 0 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 $\mathrm{Id}(\operatorname{div}(\mathfrak{a}))$. Es sei zunächst $f \in \mathfrak{a}$. Es ist dann $\operatorname{ord}_{\mathfrak{p}}(f) \geq \min\{\operatorname{ord}_{\mathfrak{p}}(g) \mid g \in \mathfrak{a}\}$ für jedes Primideal $\mathfrak{p} \neq 0$, sodass natürlich $\operatorname{div}(f) \geq \operatorname{div}(\mathfrak{a})$ gilt. Also ist $f \in \mathrm{Id}(\operatorname{div}(\mathfrak{a}))$. Ist hingegen $f \notin \mathfrak{a}$, so gibt es nach Aufgabe 22.34 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 $f \notin \mathrm{Id}(\operatorname{div}(\mathfrak{a}))$. Insbesondere ist die Abbildung injektiv. Die Surjektivität ergibt sich aus Lemma 23.10 (1) in Verbindung mit Lemma 23.10 (2), was auch den Zusatz ergibt. □

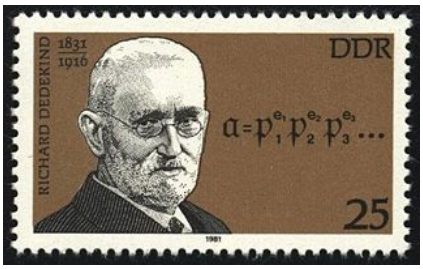
Korollar 23.13. *Es sei R ein Zahlbereich und seien $\mathfrak{a}$ und $\mathfrak{b}$ Ideale in R. Dann gilt $\mathfrak{a} \subseteq \mathfrak{b}$ genau dann, wenn es ein Ideal $\mathfrak{c}$ mit $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ gibt. Bei $\mathfrak{b} \neq 0$ ist $\mathfrak{c}$ eindeutig bestimmt.*

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 0 verschieden sind. Die Bedingung impliziert nach Lemma 23.10 (3), dass $\operatorname{div}(\mathfrak{a}) \geq \operatorname{div}(\mathfrak{b})$ ist. Somit ist

$$\operatorname{div}(\mathfrak{a}) = \operatorname{div}(\mathfrak{b}) + E$$

mit einem effektiven Divisor E. Nach Satz 23.12 übersetzt sich dies zurück zu $\mathfrak{a} = \mathfrak{b} \cdot \operatorname{Id}(E)$, sodass mit $\mathfrak{c} = \operatorname{Id}(E)$ die rechte Seite erfüllt ist. □



DDR Briefmarke

Die folgende Aussage heißt *Satz von Dedekind*. Sie liefert für jeden Zahlbereich auf der Idealebene einen Ersatz für die eindeutige Primfaktorzerlegung.

Satz 23.14. *Es 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 Satz 23.12, also die bijektive Beziehung zwischen Idealen $\neq 0$ und effektiven Divisoren. Auf der Seite der Divisoren haben wir offenbar eine eindeutige Darstellung

$$\operatorname{div}(\mathfrak{a}) = \sum_{i=1}^{k} r_i \mathfrak{p}_i$$

mit geeigneten Primidealen $\mathfrak{p}_i$. Wendet man auf diese Darstellung die Abbildung $D \mapsto \operatorname{Id}(D)$ 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 direkt aus Satz 23.12. □

Korollar 23.15. *Es 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 23.14. □

23. Arbeitsblatt

Übungsaufgaben

Aufgabe 23.1. Bestimme den Hauptdivisor zu 840 in $\mathbb{Z}$.

Aufgabe 23.2. Bestimme den Hauptdivisor zu 840 in $\mathbb{Z}[\mathrm{i}]$.

Aufgabe 23.3. Bestimme den Hauptdivisor zur Gaußschen Zahl $5+7\mathrm{i}$.

Aufgabe 23.4. Es sei R ein Zahlbereich und sei $f \in R$ als ein Produkt

$$f = up_1^{\nu_1} \cdots p_r^{\nu_r}$$

mit Primelementen p_i und einer Einheit u gegeben. Zeige, dass dann für den zugehörigen Hauptdivisor die Gleichheit

$$\operatorname{div}(f) = \nu_1(p_1) + \cdots + \nu_r(p_r)$$

gilt, wobei die (p_i) die von p_i erzeugten Primideale bezeichnen.

Aufgabe 23.5. Es sei R ein Zahlbereich und $f \in R$, $f \neq 0$. Zeige, dass der Hauptdivisor $\operatorname{div}(f)$ mit dem Divisor zum Hauptideal (f) übereinstimmt.

Aufgabe 23.6. Es sei R ein Zahlbereich und $\mathfrak{a} \subseteq R$ ein von 0 verschiedenes Ideal mit einem Erzeugendensystem $\mathfrak{a} = (f_1, \ldots, f_n)$. Zeige

$$\operatorname{div}(\mathfrak{a}) = \min\{\operatorname{div}(f_i) \mid i = 1, \ldots, n\}.$$

Aufgabe 23.7. Es sei R ein Zahlbereich und seien $f, g \in R$ von 0 verschiedene Elemente. Zeige, dass f genau dann ein Teiler von g ist, wenn für die Hauptdivisoren die Beziehung

$$\operatorname{div}(f) \leq \operatorname{div}(g)$$

gilt.

Aufgabe 23.8. Es sei R ein kommutativer Ring und seien $\mathfrak{a}, \mathfrak{b} \subseteq R$ Ideale mit $\mathfrak{a} + \mathfrak{b} = R$. Zeige, dass

$$\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$$

gilt.

Aufgabe 23.9. Es sei R ein Zahlbereich und sei $f \in R$, $f \neq 0$. Es sei $(f) = \mathfrak{p}_1 \cdots \mathfrak{p}_k$ die Zerlegung in Primideale und es sei vorausgesetzt, dass f eine Primfaktorzerlegung besitzt. Zeige, dass die Primideale $\mathfrak{p}_i$ Hauptideale sind.

Aufgabe 23.10. Es sei $\mathfrak{a}$ ein Ideal $\neq 0$ in einem Zahlbereich mit der eindeutigen Primidealzerlegung

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}.$$

Zeige, dass

$$\mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k} \cong \mathfrak{p}_1^{r_1} \cap \ldots \cap \mathfrak{p}_k^{r_k}$$

gilt.

Aufgabe 23.11. Es sei $\mathfrak{a}$ ein Ideal $\neq 0$ in einem Zahlbereich mit der eindeutigen Primidealzerlegung

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}.$$

Zeige, dass es einen natürlichen Ringisomorphismus

$$R/\mathfrak{a} \cong R/\mathfrak{p}_1^{r_1} \times \cdots \times R/\mathfrak{p}_k^{r_k}$$

gibt.

Aufgaben zum Abgeben

Aufgabe 23.12. (4 Punkte)

Es sei $R = \mathbb{Z}[\sqrt{-5}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{-5}$ der quadratische Zahlbereich zu $D = -5$. Betrachte in R die Zerlegung

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Zeige, dass die beteiligten Elemente irreduzibel, aber nicht prim sind, und bestimme für jedes dieser vier Elemente die Primoberideale. Bestimme die Hauptdivisoren zu diesen Elementen.

Aufgabe 23.13. (3 Punkte)

Es sei R ein Zahlbereich und $f, g \in R$, $f, g \neq 0$. Zeige ohne Verwendung des Bijektionssatzes, dass die Hauptdivisoren $\operatorname{div}(f)$ und $\operatorname{div}(g)$ genau dann gleich sind, wenn f und g assoziiert sind.

Aufgabe 23.14. (3 Punkte)

Es sei R ein Zahlbereich und sei $f \in R$, $f \neq 0$. Zeige die beiden folgenden Äquivalenzen:

Das Element f ist genau dann prim, wenn der zugehörige Hauptdivisor $\operatorname{div}(f)$ die Gestalt $1\mathfrak{p}$ mit einem Primideal $\mathfrak{p} \neq 0$ besitzt.

Das Element f ist genau dann irreduzibel, wenn $\operatorname{div}(f)$ minimal unter allen effektiven Hauptdivisoren $\neq 0$ ist.

24. Vorlesung - Gebrochene Ideale und Divisoren in Zahlbereichen

Divisoren und gebrochene Ideale

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; diese bilden eine Gruppe. 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. Es 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 mit $n_{\mathfrak{p}} = 0$ für fast alle $\mathfrak{p}$ sind.

Für einen diskreten Bewertungsring lässt sich die Ordnung $\operatorname{ord}\colon R \setminus \{0\} \to \mathbb{N}$, $q \mapsto \operatorname{ord}(q)$, zu einer Ordnungsfunktion auf dem Quotientenkörper fortsetzen,

$$\operatorname{ord}\colon Q(R) \setminus \{0\} \longrightarrow \mathbb{Z},\ q \longmapsto \operatorname{ord}(q),$$

siehe Aufgabe 22.22.

Definition 24.2. Es 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 $\operatorname{ord}_{\mathfrak{p}}(q)$ zuordnet, der durch q definierte *Hauptdivisor*. Er wird mit $\operatorname{div}(q)$ bezeichnet und als formale Summe

$$\operatorname{div}(q) = \sum_{\mathfrak{p}} \operatorname{ord}_{\mathfrak{p}}(q) \cdot \mathfrak{p}$$

geschrieben.

Wenn man die rationale Funktion $q \in Q(R)$ als $q = \frac{f}{g}$ ansetzt, so gilt

$$\operatorname{div}(q) = \operatorname{div}(f) - \operatorname{div}(g),$$

da dies punktweise an jedem Primideal gilt. Bei

$$\operatorname{ord}_{\mathfrak{p}}(q) < 0$$

sagt man auch, dass q einen *Pol* an der Stelle $\mathfrak{p}$ besitzt, und zwar mit der Polordnung $-\operatorname{ord}_{\mathfrak{p}}(q)$.

Die Menge der Divisoren bildet eine additive kommutative freie Gruppe, die wir mit $\operatorname{Div}(R)$ bezeichnen. Es liegt (siehe Aufgabe 24.1) unmittelbar ein Gruppenhomomorphismus

$$(Q(R))^\times \longrightarrow \operatorname{Div}(R),\ q \longmapsto \operatorname{div}(q),$$

vor. Das Bild unter dieser Abbildung ist die Untergruppe der Hauptdivisoren, die wir mit H bezeichnen.

Da wir in der letzten Vorlesung eine Bijektion zwischen effektiven Divisoren und von 0 verschiedenen Idealen (und von effektiven Hauptdivisoren mit von 0 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.

$$\begin{array}{ccc} \text{Ideale}(R) & \xrightarrow{\sim} & \text{E-Div}(R) \\ \downarrow & & \downarrow \\ ? & \xrightarrow{\sim} & \operatorname{Div}(R) \end{array}$$

Da wir einen Divisor D stets als $D = E - F$ mit effektiven Divisoren E und F schreiben können, liegt die Vermutung nahe, nach etwas wie dem Inversen (bezüglich der Multiplikation) eines Ideals zu suchen. Im Fall eines faktoriellen Zahlbereichs entsprechen sich (bis auf die Einheiten) Elemente und Hauptdivisoren, und zwar sowohl auf der Ringebene (siehe Bemerkung 23.4) als auch auf der Ebene des Quotientenkörpers. Zu einer rationale Funktion q bzw. dem Hauptdivisor $\operatorname{div}(q)$ gehört in diesem Fall einfach der von q erzeugte R-Untermodul qR von $Q(R)$. Im Fall der rationalen Zahlen sind dies Untergruppen der Form $\frac{1}{10}\mathbb{Z}$ oder $\frac{7}{3}\mathbb{Z}$. Für allgemeine Zahlbereiche führt die folgende Definition zum Ziel.

Definition 24.3. Es 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. *Es 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 $\mathfrak{a}$ in R und ein Element $r \in R$, $r \neq 0$, sodass

$$\mathfrak{f} = \frac{\mathfrak{a}}{r} = \left\{ \frac{a}{r} \mid a \in \mathfrak{a} \right\}$$

gilt.

Beweis. Es sei zunächst $\mathfrak{f}$ ein gebrochenes Ideal. Dann ist

$$\mathfrak{f} = R\left(\frac{a_1}{r_1}, \ldots, \frac{a_n}{r_n}\right).$$

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. Es 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. Es 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 die Produkte in $Q(R)$ zu nehmen sind.

Wird das gebrochene Ideal $\mathfrak{f}$ als R-Modul von $f_1, \ldots, f_n$ erzeugt und wird das gebrochene Ideal $\mathfrak{g}$ von $g_1, \ldots, g_m$ erzeugt, so wird das Produkt $\mathfrak{fg}$ von den Produkten $f_i g_j$, $1 \leq i \leq n$, $1 \leq j \leq m$, 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 0 verschiedenen gebrochenen Ideale eine Gruppe bilden, und die von 0 verschiedenen gebrochenen Hauptideale darin eine Untergruppe.

Bemerkung 24.7. Zu einem gebrochenen Ideal $\mathfrak{f} \neq 0$ in einem Zahlbereich R nennt man

$$\mathfrak{f}^{-1} := \{q \in Q(R) \mid q \cdot \mathfrak{f} \subseteq R\}$$

das zugehörige *inverse gebrochene Ideal*. Es ist klar, dass dies ein von 0 verschiedener R-Untermodul von $Q(R)$ ist, die endliche Erzeugtheit ist etwas schwieriger zu zeigen. Zunächst beachte man, dass zu zwei gebrochenen Idealen mit der Beziehung $\mathfrak{g} = r\mathfrak{f}$ mit $r \in Q(R)$, $r \neq 0$, für die inversen Ideale die Beziehung $\mathfrak{g}^{-1} = r^{-1}\mathfrak{f}^{-1}$ gilt. Wenn nun $\mathfrak{f}$ durch $\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n}$ erzeugt wird,

so ist $\mathfrak{f} \cong \frac{\mathfrak{f}}{a} = \mathfrak{g}$ mit $a = a_1 \cdots a_n$ und $\mathfrak{g}$ besitzt ein Erzeugendensystem der Form $\frac{1}{c_1}, \ldots, \frac{1}{c_n}$ mit $c_i \in R$. Die Bedingung

$$q\frac{1}{c_i} \in R$$

impliziert $q \in R$. Daher ist das inverse gebrochene Ideal selbst ein Ideal, also endlich erzeugt.

Für das Produkt ist offenbar

$$\mathfrak{f} \cdot \mathfrak{f}^{-1} \subseteq R,$$

es ist aber nicht unmittelbar klar, dass hier sogar Gleichheit gilt. Dies folgt daraus, dass man die Gleichheit lokal testen kann, die Produktbildung lokal ist und die Lokalisierungen diskrete Bewertungsringe sind.

Beispiel 24.8. Wir betrachten im quadratischen Zahlbereich $\mathbb{Z}[\sqrt{-5}]$ das Ideal

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

Aufgrund der Gleichung

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

ist beispielsweise

$$\frac{1-\sqrt{-5}}{2} \cdot \mathfrak{a} \subseteq R, \ \frac{3}{1+\sqrt{-5}} \cdot \mathfrak{a} \subseteq R, \ 1 \cdot \mathfrak{a} \subseteq R\,.$$

Wir behaupten, dass das inverse gebrochene Ideal $\mathfrak{a}^{-1}$ gleich

$$\mathfrak{f} = R\left(1, \frac{1-\sqrt{-5}}{2}\right)$$

ist, wobei sich die Inklusion $\mathfrak{f} \subseteq \mathfrak{a}^{-1}$ aus der vorstehenden Zeile ergibt. Andererseits gilt wegen

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

für das Produkt

$$\mathfrak{a} \cdot \mathfrak{f} = R,$$

und dies impliziert nach Aufgabe 24.15 die Gleichheit $\mathfrak{f} = \mathfrak{a}^{-1}$.

Ein gebrochenes Ideal $\mathfrak{f} \neq 0$ in einem Zahlbereich 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 0 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 (über dem diskreten Bewertungsring $R_{\mathfrak{p}}$) sind isomorph zu $R_{\mathfrak{p}}$. Siehe Aufgabe 22.16.

Definition 24.9. Es 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

$$\{f \in Q(R) \mid \operatorname{div}(f) \geq D\}$$

das *gebrochene Ideal zum Divisor* D. Es wird mit $\operatorname{Id}(D)$ bezeichnet.

Das folgende Lemma zeigt, dass man in der Tat ein gebrochenes Ideal erhält, und dass diese Definition mit der früheren Definition 23.11 verträglich ist.

Lemma 24.10. *Es sei R ein Zahlbereich und $D = \sum_{\mathfrak{p}} n_{\mathfrak{p}} \cdot \mathfrak{p}$ ein Divisor. Dann ist die Menge $\{f \in Q(R) \mid \operatorname{div}(f) \geq D\}$ 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 23.11 zugeordnet wird.*

Beweis. Es sei $\mathfrak{f} = \{f \in Q(R) \mid \operatorname{div}(f) \geq D\}$. 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 $\operatorname{div}(f_1), \operatorname{div}(f_2) \geq D$ gilt

$$\operatorname{div}(f_1 + f_2) \geq \min(\operatorname{div}(f_1), \operatorname{div}(f_2)) \geq D$$

und

$$\operatorname{div}(rf) = \operatorname{div}(r) + \operatorname{div}(f) \geq D$$

für $r \in R$, da ja $\operatorname{div}(r)$ effektiv ist. Also liegt in der Tat ein R-Modul vor.

Bevor wir die endliche Erzeugtheit nachweisen, betrachten wir die zweite Aussage. Es sei also E ein effektiver Divisor. Wir müssen zeigen, dass

$$\{f \in Q(R) \mid \operatorname{div}(f) \geq E\} = \{f \in R \mid \operatorname{div}(f) \geq E\}$$

ist, wobei die Inklusion $\supseteq$ klar ist. Es 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 0 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 Satz 22.9, dass $f \in R$ ist.

Zum Nachweis der endlichen Erzeugtheit bemerken wir, dass es zu jedem Divisor D ein $r \in R$ derart gibt, dass $D' = D + \operatorname{div}(r)$ effektiv ist. Das zu D' gehörige gebrochene Ideal ist dann ein Ideal, also endlich erzeugt, und dies überträgt sich auf das gebrochene Ideal zu D. □

Definition 24.11. Es sei R ein Zahlbereich und $\mathfrak{f} \neq 0$ ein von 0 verschiedenes gebrochenes Ideal. Dann nennt man den Divisor

$$\operatorname{div}(\mathfrak{f}) = \sum_{\mathfrak{p}} m_{\mathfrak{p}} \cdot \mathfrak{p}$$

mit

$$m_{\mathfrak{p}} = \min\left(\mathrm{ord}_{\mathfrak{p}}\left(f\right) | f \in \mathfrak{f},\ f \neq 0\right)$$

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 24.12. *Es sei R ein Zahlbereich. Dann gelten folgende Aussagen.*

(1) Es 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

$$\mathrm{div}\left(\mathfrak{f}\right) = \mathrm{div}\left(\mathfrak{a}\right) - \mathrm{div}\left(h\right).$$

(2) Zu einem Divisor D gibt es ein $h \in R$ derart, dass $D + \mathrm{div}\left(h\right)$ effektiv ist.

(3) Zu einem Divisor D mit $E = D + \mathrm{div}\left(h\right)$ effektiv ist

$$\mathrm{Id}(D) = \frac{\mathrm{Id}(E)}{h}.$$

Beweis. Siehe Aufgabe 24.18. □

Auch die Einzelheiten des Beweises des folgenden Satzes überlassen wir dem Leser, siehe Aufgabe 24.19.

Satz 24.13. *Es sei R ein Zahlbereich. Dann sind die Zuordnungen*

$$\mathfrak{f} \longmapsto \mathrm{div}(\mathfrak{f}) \quad \textit{und} \quad D \longmapsto \mathrm{Id}(D)$$

zueinander inverse Abbildungen zwischen der Menge der von 0 verschiedenen gebrochenen Ideale und der Menge der Divisoren. Diese Bijektion ist ein Isomorphismus von Gruppen.

Beweis. Wir müssen zeigen, dass die hintereinandergeschalteten Abbildungen jeweils die Identität ergeben. Dies kann man mittels Lemma 24.12 auf den effektiven Fall zurückführen. Die Zuordnung $\mathfrak{f} \mapsto \mathrm{div}(\mathfrak{f})$ führt die Multiplikation von gebrochenen Idealen in die Addition von Divisoren über, da dies an jedem diskreten Bewertungsring $R_{\mathfrak{p}}$ gilt. Wegen der Bijektivität liegt dann auch links eine Gruppe vor und die Abbildungen sind Gruppenisomorphismen. □

24. Arbeitsblatt

Übungsaufgaben

Aufgabe 24.1. Es sei R ein Zahlbereich. Zeige, dass die Abbildung, die einem Element $q \in Q(R)$, $q \neq 0$, den Hauptdivisor $\operatorname{div}(q)$ zuordnet, folgende Eigenschaften besitzt.

(1) Es ist $\operatorname{div}(q_1 q_2) = \operatorname{div}(q_1) + \operatorname{div}(q_2)$.
(2) Es ist $\operatorname{div}(q_1 + q_2) \geq \min\{\operatorname{div}(q_1), \operatorname{div}(q_2)\}$.

Zeige insbesondere, dass diese Zuordnung einen Gruppenhomomorphismus

$$Q(R) \setminus \{0\} \longrightarrow \operatorname{Div}(R)$$

definiert und dass die Hauptdivisoren eine Untergruppe der Divisoren bilden.

Aufgabe 24.2. Beweise, dass es zu einem Zahlbereich R einen Gruppenisomorphismus

$$Q(R)^\times / R^\times \longrightarrow H$$

gibt, wobei H die Gruppe der Hauptdivisoren bezeichnet.

Aufgabe 24.3. Es sei R ein Zahlbereich. Man bestimme die Mächtigkeit der folgenden Mengen.

(a) R.
(b) $Q(R)$.
(c) Die Menge der Primideale in R.
(d) Die Menge der Ideale in R.
(e) Die Menge der gebrochenen Ideale.
(f) Die Menge der R-Untermoduln von $Q(R)$.
(g) Die Divisorengruppe $\operatorname{Div}(R)$.
(h) Die Hauptdivisorengruppe.

Aufgabe 24.4. Es sei R ein Zahlbereich. Man bestimme für die folgenden Gruppen, ob sie frei sind.

(a) R.
(b) Der Quotientenkörper $(Q(R), +, 0)$.
(c) Die Einheitengruppe des Quotientenkörpers $Q(R) \setminus \{0\}$.
(d) Die Gruppe $(\mathbb{Q}_+, \cdot, 1)$ der positiven rationalen Zahlen.
(e) Die Gruppe der gebrochenen Idealen $\neq 0$.
(f) Die Divisorengruppe $\operatorname{Div}(R)$.
(g) Die Hauptdivisorengruppe.

Aufgabe 24.5. Es sei R ein Zahlbereich und $f \in Q(R)$, $f \neq 0$. Zeige, dass $f \in R$ genau dann gilt, wenn der Hauptdivisor $\operatorname{div}(f)$ ein effektiver Divisor ist.

Aufgabe 24.6. Es sei R ein quadratischer Zahlbereich. Definiere zu einem Divisor D den „konjugierten Divisor“ $\overline{D}$. Zeige, dass für $q \in Q(R)$, $q \neq 0$, die Beziehung

$$\overline{\operatorname{div}(q)} = \operatorname{div}(\overline{q})$$

gilt.

Aufgabe 24.7. Es sei $R = A_{14} = \mathbb{Z}[\sqrt{14}]$ der quadratische Zahlbereich zu $D = 14$. Berechne zu

$$q = \frac{3}{5} - \frac{1}{7}\sqrt{14}$$

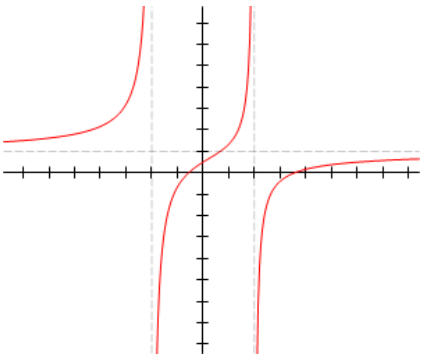
den zugehörigen Hauptdivisor.

Aufgabe 24.8. Es sei

$$R = \mathbb{Z}[\sqrt{-6}] \cong \mathbb{Z}[X]/(X^2+6).$$

Berechne den Hauptdivisor zu

$$q = \frac{4}{5} + \frac{2}{3}\sqrt{-6}.$$



Aufgabe 24.9. Bestimme eine rationale Funktion $\mathbb{C} \to \mathbb{C}$, die an der Stelle $2-\mathrm{i}$ einen Pol der Ordnung 4, in $-3+5\mathrm{i}$ eine Nullstelle der Ordnung 2 und in -3 einen Pol der Ordnung 3 besitzt.

Aufgabe 24.10. Es sei $f \neq 0$ eine rationale Funktion $f\colon \mathbb{C} \to \mathbb{C}$. Zeige, dass f in $a \in \mathbb{C}$ genau dann eine Nullstelle der Ordnung k besitzt, wenn f^{-1} in a einen Pol der Ordnung k besitzt.

Aufgabe 24.11. Bestimme einen Erzeuger für das gebrochene Ideal $\mathfrak{f} \subseteq \mathbb{Q}$, das durch die rationalen Zahlen

$$\frac{4}{7}, \frac{7}{10}, \frac{13}{8}$$

erzeugt wird.

Aufgabe 24.12. Der Floh Kurt lebt auf einem unendlichen Lineal und befindet sich in der Nullposition. Er verfügt über drei Sprünge, nämlich

$$\frac{11}{77}, \frac{25}{49}, \frac{82}{15}.$$

Berechne das zugehörige gebrochene Ideal, das seinem Lebensraum entspricht.

Aufgabe 24.13. Es sei $R = \mathbb{Z}[\mathrm{i}]$. Berechne einen Erzeuger für das gebrochene Ideal aus $Q(R) = \mathbb{Q}[\mathrm{i}]$, das durch die beiden Erzeuger

$$\frac{5}{7} \text{ und } \frac{-8+6\mathrm{i}}{5}$$

gegeben ist.

Aufgabe 24.14. Es sei $\mathfrak{f} \subseteq Q(R)$ ein gebrochenes Ideal zu einem Zahlbereich R. Zeige, dass

$$\mathfrak{f}^{-1} = \{q \in Q(R) \mid q \cdot \mathfrak{f} \subseteq R\}$$

ebenfalls ein gebrochenes Ideal ist.

Aufgabe 24.15. Es seien $\mathfrak{f}$ und $\mathfrak{g}$ gebrochene Ideale in einem Zahlbereich R. Es gelte

$$\mathfrak{f} \cdot \mathfrak{g} = R.$$

Zeige, dass dann

$$\mathfrak{g} = \mathfrak{f}^{-1}$$

ist.

Aufgabe 24.16. Es sei $\mathfrak{a} \subseteq R$ ein Ideal in einem Zahlbereich R mit dem zugehörigen effektiven Divisor E. Zeige, dass das inverse gebrochene Ideal

$$\mathfrak{a}^{-1} = \{q \in Q(R) \mid q \cdot \mathfrak{a} \subseteq R\}$$

gleich dem zu $-E$ gehörenden gebrochenen Ideal $\mathrm{Id}(-E)$ ist.

Aufgabe 24.17. Es sei R ein Zahlbereich und es seien $\mathfrak{f}$ und $\mathfrak{g}$ gebrochene Ideale.

(1) Zeige, dass wenn es ein $r \in Q(R)$, $r \neq 0$, mit
$$\mathfrak{g} = r\mathfrak{f}$$
gibt, dass dann die Multiplikation mit r, also
$$Q(R) \longrightarrow Q(R),\ f \longmapsto rf,$$
einen R-Modulisomorphismus
$$\mathfrak{f} \longrightarrow \mathfrak{g}$$
induziert.

(2) Zeige, dass wenn es irgendeinen R-Modulisomorphismus
$$\varphi\colon \mathfrak{f} \longrightarrow \mathfrak{g}$$
gibt, dass es dann schon ein $r \in Q(R)$ mit
$$\mathfrak{g} = r\mathfrak{f}$$
gibt, und dass der Isomorphismus eine Multiplikation ist.

Aufgabe 24.18. Beweise Lemma 24.12.

Aufgabe 24.19. Führe die Einzelheiten im Beweis zu Satz 24.13 aus.

Aufgabe 24.20. Es sei R ein Zahlbereich und $\mathfrak{a}$ ein Ideal in R. Zeige, dass es ein von 0 verschiedenes Ideal $\mathfrak{b}$ derart gibt, dass $\mathfrak{ab}$ ein Hauptideal ist.

Aufgabe 24.21. Beweise das Lemma von Dickson, das besagt, dass eine nichtleere Teilmenge $T \subseteq \mathbb{N}^r$ nur endlich viele minimale Elemente besitzt.

Aufgaben zum Abgeben

Aufgabe 24.22. (4 Punkte)

Es sei $R = A_{-13} = \mathbb{Z}[\sqrt{-13}]$ der quadratische Zahlbereich zu $D = -13$. Berechne zu
$$q = \frac{2}{3} - \frac{5}{7}\sqrt{-13}$$
den zugehörigen Hauptdivisor und stelle ihn als Differenz zweier effektiver Divisoren dar.

Aufgabe 24.23. (4 Punkte)

Die Flöhin Paola lebt in der komplexen Ebene und befindet sich im Nullpunkt. Sie verfügt über drei Sprünge, nämlich

$$\frac{3}{4} - \frac{2}{5}\mathrm{i},\ 2 + \frac{2}{3}\mathrm{i},\ \frac{1}{7} + 7\mathrm{i}\,.$$

Man gebe eine einfache Beschreibung des gebrochenen Ideals, das ihrem Lebensraum entspricht.

Aufgabe 24.24. (4 Punkte)

Zeige direkt, dass die gebrochenen Ideale $\neq 0$ eine Gruppe bilden, und dass die gebrochenen Hauptideale darin eine Untergruppe bilden.

Aufgabe 24.25. (3 Punkte)

Es sei $\mathfrak{a} = (f_1, \ldots, f_n)$ (mit $f_i \neq 0$) ein Ideal in einem Zahlbereich R und sei vorausgesetzt, dass das inverse gebrochene Ideal $\mathfrak{a}^{-1}$ die Gestalt

$$\mathfrak{a}^{-1} = (f_1^{-1}, \ldots, f_n^{-1})$$

hat. Zeige, dass $\mathfrak{a}$ ein Hauptideal sein muss.

25. Vorlesung - Die Divisorenklassengruppe von Zahlbereichen

Die Divisorenklassengruppe

Definition 25.1. Es sei R ein Zahlbereich. Es sei $\mathrm{Div}\,(R)$ die Gruppe der Divisoren und $H \subseteq \mathrm{Div}\,(R)$ sei die Untergruppe der Hauptdivisoren. Dann nennt man die Restklassengruppe

$$\mathrm{DKG}\,(R) = \mathrm{Div}\,(R)/H$$

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. Sie heißen *Divisorklassen* oder *Idealklassen*. Ein späteres Hauptresultat - das wir aber nur für quadratische Zahlbereiche beweisen werden - 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. *Es sei R ein Zahlbereich und es bezeichne $\mathrm{DKG}\,(R)$ die Divisorenklassengruppe von R. Dann sind folgende Aussagen äquivalent.*

(1) R ist ein Hauptidealbereich.
(2) R ist faktoriell.
(3) Es ist $\mathrm{DKG}\,(R) = 0$.

Beweis. Die Implikation (1) $\Rightarrow$ (2) folgt aus Satz 3.7.

(2) $\Rightarrow$ (3). Es 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 nach Satz 18.15 jedes von 0 verschiedene Primideal maximal, sodass hier $(p) = \mathfrak{p}$ gelten muss. Auf der Seite der Divisoren gilt aufgrund von Satz 23.12 $\mathrm{div}\,(p) = 1\mathfrak{p}$, sodass ein Hauptdivisor vorliegt. Also sind alle Erzeuger der Divisorengruppe Hauptdivisoren und somit ist überhaupt

$$\mathrm{Div}(R) = H$$

und die Divisorenklassengruppe ist trivial.

(3) $\Rightarrow$ (1). Es sei nun $\mathrm{DKG}\,(R) = 0$ vorausgesetzt. Wir zeigen zunächst, dass jedes Primideal $\mathfrak{p} \neq 0$ ein Hauptideal ist. Nach Voraussetzung ist der Divisor $\mathfrak{p}$ ein Hauptdivisor, sodass $\mathfrak{p} = \mathrm{div}(p)$ mit einem $p \in R$ gilt. Aufgrund von Satz 23.12 entspricht dies auf der Idealseite der Gleichung $\mathfrak{p} = (p)$, sodass jedes Primideal ein Hauptideal ist. Für ein beliebiges Ideal $\mathfrak{a} \subseteq R$, $\mathfrak{a} \neq 0$, ist nach Satz 23.14

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}.$$

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 0 ist. Der Bereich $\mathbb{Z}[\sqrt{-5}]$ ist hingegen nicht faktoriell und somit kann seine Klassengruppe nicht 0 sein. Wir werden in Beispiel 27.11 sehen, dass die Klassengruppe davon einfach $\mathbb{Z}/(2)$ ist, und wir werden in Satz 27.6 allgemein beweisen, dass die Klassengruppe von quadratischen Zahlbereichen immer eine endliche Gruppe ist.

Beispiel 25.3. Wir behaupten, dass im quadratischen Zahlbereich $R = \mathbb{Z}[\sqrt{-5}]$ das Ideal

$$\mathfrak{p} = (2, 1 + \sqrt{-5})$$

kein Hauptideal ist, was in Beispiel 21.8 gezeigt wurde, aber die Eigenschaft besitzt, dass das Quadrat davon ein Hauptideal ist. Insbesondere definiert

die zugehörige Idealklasse ein von 0 verschiedenes Element in der Divsorenklassengruppe mit der Eigenschaft, dass das Doppelte davon trivial ist. Es ist

$$\mathfrak{p}^2 \,=\, (4, 2+2\sqrt{-5}, -4+2\sqrt{-5}) \,=\, (2).$$

Dabei ist die Inklusion $\subseteq$ klar und die umgekehrte Inklusion $\supseteq$ ergibt sich aus

$$-4+(2+2\sqrt{-5})-(-4+2\sqrt{-5}) \,=\, 2.$$

Wir betrachten nun das Ideal

$$\mathfrak{q} \,=\, (7, 3+\sqrt{-5}).$$

Der Restklassenring ist

$$\mathbb{Z}/(7)[X]/(X^2+5, 3+X) \,\cong\, \mathbb{Z}/(7),$$

sodass ein Primideal mit der Norm 7 vorliegt, das kein Hauptideal ist, da es kein Element mit Norm 7 gibt. Die beiden Ideale $\mathfrak{p}$ und $\mathfrak{q}$ definieren die gleiche Idealklasse. Dazu betrachten wir die Multiplikation

$$Q(R) \longrightarrow Q(R),\, h \longmapsto h\frac{3+\sqrt{-5}}{2}.$$

Wegen

$$2\cdot\frac{3+\sqrt{-5}}{2} \,=\, 3+\sqrt{-5} \,\in\, \mathfrak{q}$$

und

$$(1+\sqrt{-5})\cdot\frac{3+\sqrt{-5}}{2} \,=\, \frac{-2+4\sqrt{-5}}{2} \,=\, -1+2\sqrt{-5} \,=\, -7+2(3+\sqrt{-5}) \,\in\, \mathfrak{q}$$

induziert dies einen injektiven R-Modulhomomorphismus

$$\mathfrak{p} \longrightarrow \mathfrak{q},$$

der wegen

$$7 \,=\, -(-1+2\sqrt{-5})+2(3+\sqrt{-5})$$

auch surjektiv ist. Somit ist

$$\mathfrak{p}\cdot\left(\frac{3+\sqrt{-5}}{2}\right) \,=\, \mathfrak{q}$$

als gebrochene Ideale. In Beispiel 27.11 wird darüber hinaus gezeigt, dass die Klassengruppe von R gleich $\mathbb{Z}/(2)$ ist.

Normeuklidische Bereiche

Wir betrachten diejenigen imaginär-quadratischen Zahlbereiche (also $D < 0$), für die die Norm eine euklidische Funktion ist. Wir werden in Bemerkung 25.6 Beispiele sehen, wo der Ganzheitsring zwar faktoriell, aber nicht euklidisch ist.

Definition 25.4. Es 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.

Da eine euklidische Funktion nur positive Werte annimmt, kann die Norm allenfalls im imaginär-quadratischen Fall euklidisch sein, da im reell-imaginär quadratischen Fall die Norm auch negative Werte annimmt. Die Euklidizität der Norm bedeutet, dass es zu $a, b \in R$, $b \neq 0$, Elemente z und r mit

$$a = zb + r$$

und $r = 0$ oder

$$N(r) < N(b).$$

Dies kann man auch so sehen, dass es für jedes rationale Element $\frac{a}{b} \in Q(R)$ eine ganzzahlige Approximation $z \in R$ mit

$$N\Big(\frac{a}{b} - z\Big) < 1$$

gibt. Mit Hilfe dieser geometrischen Interpretation charakterisiert der nächste Satz explizit diejenigen imaginär-quadratischen Zahlbereiche, für die A_D normeuklidisch ist.

Satz 25.5. *Es 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) Es ist $D = -1, -2, -3, -7, -11$.

Beweis. (1) $\Rightarrow$ (3). Es 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

$$\varphi\colon\ A_D \longrightarrow A_D/(z).$$

Dabei ist $\varphi(w) = \varphi(r)$. Ab $|D| \geq 4$ gibt es nur die beiden Einheiten 1 und -1, sodass das Bild von φ überhaupt nur aus $0, 1, -1$ besteht. Also ist nach Satz 21.7

$$N(z) = |A_D/(z)| \leq 3$$

Bei $D = 2, 3 \mod 4$ hat nach Satz 20.9 jedes Element aus A_D die Form $z = a + b\sqrt{D}$ ($a, b \in \mathbb{Z}$) mit Norm $N(z) = a^2 + |D|\, b^2$. Damit ist (bei $|D| \geq 4$) $N(z) \leq 3$ nur bei $b = 0$ und $|a| = 1$ 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 nach Satz 20.9 jedes Element aus A_D die Form $z = a + b\frac{1+\sqrt{D}}{2}$ ($a, b \in \mathbb{Z}$) mit Norm $N(z) = \left(a + \frac{b}{2}\right)^2 + \frac{|D|b^2}{4}$. Damit ist bei $|D| \geq 13$ die Bedingung $N(z) \leq 3$ wieder nur bei $b = 0$ und $|a| = 1$ möglich, sodass 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 $z \in A_D$ mit $|N(f - z)| < 1$ gibt. Dies bedeutet anschaulich, dass es zu jedem Punkt von $\mathbb{Q}[\sqrt{D}] \subseteq \mathbb{C}$ stets Gitterpunke aus A_D gibt mit einem Abstand kleiner als eins.[2] 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 $\frac{1}{2}\sqrt{1 + |D|}$, 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 $(0,0), (1,0), \left(\frac{1}{2}, \frac{\sqrt{|D|}}{2}\right)$. Die Mittelsenkrechte zur Grundseite ist durch $x = \frac{1}{2}$ gegeben, und die Mittelsenkrechte zum linken Schenkel wird durch $\left(\frac{1}{4}, \frac{\sqrt{|D|}}{4}\right) + t\left(\sqrt{|D|}, -1\right)$ beschrieben. Gleichsetzen ergibt

$$\frac{1}{4} + t\sqrt{|D|} = \frac{1}{2} \text{ bzw. } t\sqrt{|D|} = \frac{1}{4} \text{ und } t = \frac{1}{4\sqrt{|D|}}\,.$$

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 Quadratwurzel aus

$$\frac{1}{4} + \left(\frac{\sqrt{|D|}}{4} - \frac{1}{4\sqrt{|D|}}\right)^2 = \frac{1}{4} + \frac{|D|}{16} + \frac{1}{16\,|D|} - \frac{1}{8} = \frac{1}{16}\left(2 + |D| + \frac{1}{|D|}\right).$$

Dies (und ebenso die Quadratwurzel) ist kleiner als 1 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. $\square$

[2] Da $\mathbb{Q}[\sqrt{D}]$ dicht in der komplexen Ebene $\mathbb{C}$ liegt, gilt dies ebenso für alle komplexen Zahlen.

Bemerkung 25.6. 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 nach Satz 25.5 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

$$2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 23, 29, 31, 33, 37, 38, 41, 43, 46, 47,$$

$$53, 57, 59, 61, 62, 67, 69, 71, 73, 77, 83, 86, 89, 93, 94, 97$$

vor. Dagegen weiß man (Chatland und Davenport 1950), für welche positiven D der Ganzheitsbereich A_D euklidisch ist, nämlich für $D = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$.

25. Arbeitsblatt

Übungsaufgaben

Aufgabe 25.1. Es sei R ein Zahlbereich und es seien $\mathfrak{f}$ und $\mathfrak{g}$ gebrochene Ideale $\neq 0$. Zeige, dass $\mathfrak{f}$ und $\mathfrak{g}$ genau dann als R-Moduln isomorph sind, wenn die zugehörigen Divisoren $\operatorname{div}(\mathfrak{f})$ und $\operatorname{div}(\mathfrak{g})$ in der Divisorenklassengruppe $\operatorname{DKG}(R)$ gleich sind.

Aufgabe 25.2. Es sei A_D ein quadratischer Zahlbereich und sei $\mathfrak{a}$ ein Ideal $\neq 0$ in A_D. Zeige, dass das konjugierte Ideal $\overline{\mathfrak{a}}$ in der Klassengruppe das Inverse zu $\mathfrak{a}$ ist.

Aufgabe 25.3. Bestimme in $\mathbb{Z}[\sqrt{-2}]$ einen größten gemeinsamen Teiler für $22 + 25\sqrt{-2}$ und $43 - 23\sqrt{-2}$.

Aufgabe 25.4. Betrachte in $\mathbb{Z}[\sqrt{-2}]$ die beiden Elemente

$$x = 4 + 7\sqrt{-2} \text{ und } y = 5 + 8\sqrt{-2}\,.$$

Bestimme den größten gemeinsamen Teiler der Normen $N(x)$ und $N(y)$ (in $\mathbb{Z}$) und das von x und y erzeugte Ideal in $\mathbb{Z}[\sqrt{-2}]$.

Aufgabe 25.5. Es sei $R = \mathbb{Z}[\sqrt{-6}] \cong \mathbb{Z}[X]/(X^2+6)$. Berechne den Hauptdivisor zu

$$q = \frac{2}{3} - \frac{1}{4}\sqrt{-6}.$$

Aufgabe 25.6. Es sei $R = A_{-15} = \mathbb{Z}[\frac{1+\sqrt{-15}}{2}]$ der quadratische Zahlbereich zu $D = -15$. Berechne zu

$$g = \frac{3}{10} - \frac{5}{6}\sqrt{-15}$$

den zugehörigen Hauptdivisor und stelle ihn als Differenz zweier effektiver Divisoren dar.

Aufgabe 25.7. Es sei $R = A_{-11} = \mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$ der quadratische Zahlbereich zu $D = -11$. Berechne mittels des euklidischen Algorithmus den größten gemeinsamen Teiler von

$$35 + \sqrt{-11} \text{ und } -89 + 21\sqrt{-11}\,.$$

Aufgabe 25.8. Es sei $R = A_{-7} = \mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ der quadratische Zahlbereich zu $D = -7$. Bestimme die Primfaktorzerlegung von

$$4 + 9\sqrt{-7}\,.$$

Aufgabe 25.9. Es sei D quadratfrei mit $D = 3 \mod 4$ und $D < -1$. Zeige, dass $(2, 1+\sqrt{D})$ ein Primideal im quadratischen Zahlbereich A_D ist, aber kein Hauptideal. Folgere, dass diese Ringe nicht faktoriell sind.

Aufgabe 25.10. Es sei $D < 0$ quadratfrei und A_D der zugehörige imaginärquadratische Zahlbereich. Bestimme für $D \geq -12$ die Nichteinheiten $z \in A_D$ mit minimaler Norm.

Aufgabe 25.11. Im quadratischen Zahlbereich $A_6 \cong \mathbb{Z}[\sqrt{6}]$ gilt

$$2 \cdot 3 = \sqrt{6} \cdot \sqrt{6}.$$

Finde die Primfaktorzerlegungen (?) der beteiligten Faktoren und des Produktes.

Aufgabe 25.12. Im quadratischen Zahlbereich $A_{-6} \cong \mathbb{Z}[\sqrt{-6}]$ gilt

$$-2 \cdot 3 = \sqrt{-6} \cdot \sqrt{-6}.$$

Kann man diese Produkte weiter zerlegen, sind die beteiligten Faktoren prim?

Aufgabe 25.13. Es sei D quadratfrei und betrachte $\mathbb{Z}[\sqrt{D}] \subseteq A_D$. Charakterisiere für die beiden Ringe, wann $\sqrt{D}$ prim ist.

Aufgabe 25.14. Man gebe ein Beispiel von zwei Zahlbereichen R und S, die als Ringe nicht isomorph sind, aber die Eigenschaft haben, dass sowohl die additiven Strukturen $(R, +, 0)$ und $(S, +, 0)$ als Gruppen isomorph als auch die multiplikativen Strukturen $(R, \cdot, 1)$ und $(S, \cdot, 1)$ als Monoide isomorph sind.

Bei den beiden folgenden Aufgaben darf man sich auf quadratische Zahlbereiche beschränken, da wir nur für diese die Multiplikativität der Norm gezeigt haben.

Aufgabe 25.15. Es sei R ein Zahlbereich. Erweitere die (multiplikative) Normabbildung

$$\text{Ideale}\,(R) \longrightarrow (\mathbb{N}_+, \cdot),\ \mathfrak{a} \longmapsto N(\mathfrak{a}),$$

zu einem Gruppenhomomorphismus

$$\text{Gebrochene Ideale}\,(R) \longrightarrow \mathbb{Q}^\times.$$

Aufgabe 25.16. Finde eine (additive) Gruppe G und Gruppenhomomorphismen φ und ψ derart, dass das Diagramm

$$\begin{array}{ccc} \text{Gebrochene Ideale}\,(R) & \xrightarrow{\sim} & \text{Div}\,(R) \\ \text{Norm}\downarrow & & \downarrow\psi \\ \mathbb{Q}^\times & \xrightarrow{\varphi} & G \end{array}$$

kommutiert und dass φ injektiv ist.

Aufgaben zum Abgeben

Aufgabe 25.17. (4 Punkte)

Bestimme in $\mathbb{Z}[\sqrt{-2}]$ einen größten gemeinsamen Teiler für $-169 + 2\sqrt{-2}$ und $-70 + 113\sqrt{-2}$.

Aufgabe 25.18. (3 Punkte)

Es sei R ein Zahlbereich und sei angenommen, dass jede ganze Zahl $n \in \mathbb{Z}$, $n \neq 0$, eine Primfaktorzerlegung in R besitzt. Zeige, dass dann R bereits faktoriell ist.

Aufgabe 25.19. (4 Punkte)

Es sei $D \neq 0, 1$ quadratfrei und A_D der zugehörige quadratische Zahlbereich. Es Es sei p eine Primzahl, die in A_D nicht träge sei. Beweise die Äquivalenz folgender Aussagen.

(1) p besitzt eine Primfaktorzerlegung in A_D.
(2) p ist nicht irreduzibel (also zerlegbar) in A_D.
(3) p oder $-p$ ist die Norm eines Elementes aus A_D.
(4) p oder $-p$ ist die Norm eines Primelementes aus A_D.

Aufgabe 25.20. (4 Punkte)

Es sei $D \leq -2$ quadratfrei und betrachte $R = \mathbb{Z}[\sqrt{D}]$. Zeige, dass die einzige Faktorisierung (bis auf Einheiten) von D durch

$$D = \sqrt{D}\sqrt{D}$$

gegeben ist. Zeige damit, dass $\sqrt{D}$ irreduzibel ist. Zeige ferner, dass falls $-D$ keine Primzahl ist, dann auch $\sqrt{D}$ nicht prim in R ist.

26. Vorlesung - Der Gitterpunktsatz von Minkowski

Gitter und konvexe Mengen

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 dieser Vorlesung 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. Im imaginärquadratischen Fall bietet sich die Einbettung in die komplexen Zahlen an. 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.

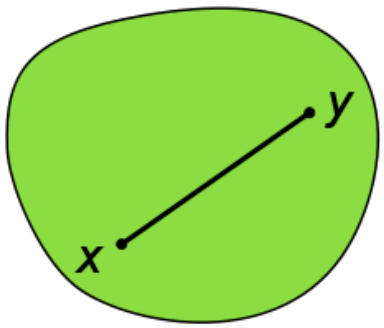
Definition 26.1. Es seien $v_1, \ldots, v_n$ linear unabhängige Vektoren im $\mathbb{R}^n$. Dann heißt die Untergruppe $\mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n$ ein *Gitter* im $\mathbb{R}^n$.

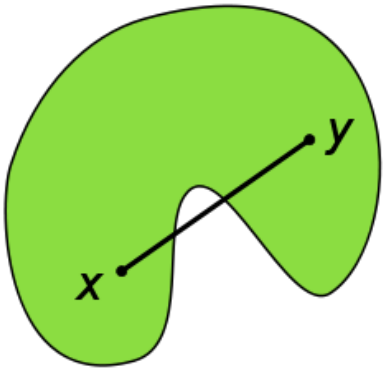
Manchmal spricht man auch von einem vollständigen Gitter. Als Gruppen sind sie isomorph zu $\mathbb{Z}^n$, hier interessieren aber auch Eigenschaften der Einbettung in $\mathbb{R}^n$. Ein Gitter heißt *rational*, wenn die erzeugenden Vektoren zu $\mathbb{Q}^n$ gehören.

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.

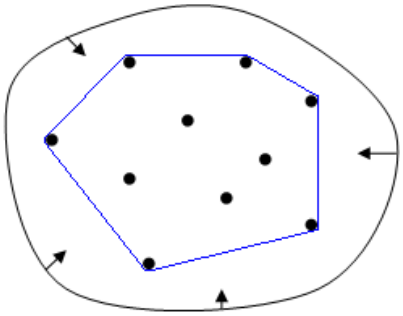




Der Durchschnitt von konvexen Teilmengen ist wieder konvex. Daher kann man definieren:

Definition 26.3. Zu einer Teilmenge $U \subseteq \mathbb{R}^n$ heißt die kleinste konvexe Teilmenge T, die U umfasst, die *konvexe Hülle* von U.

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 $\epsilon_1 v_1 + \cdots + \epsilon_n v_n$ mit $\epsilon_i \in \{0, 1\}$ als die *Grundmasche* (oder *Fundamentalmasche*) des Gitters.

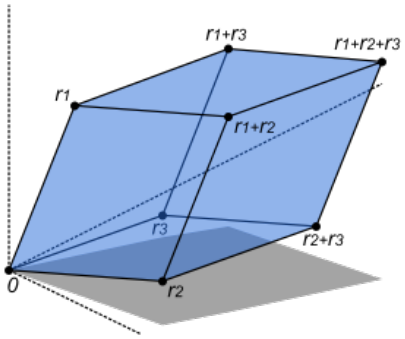
Die in der vorstehenden Definition auftauchenden Vektoren sind die Eckpunkte des von den Basisvektoren $v_1, \ldots, v_n$ erzeugten Parallelotops. Die Elemente der Grundmasche selbst sind alle Vektoren der Form

$$r_1 v_1 + \cdots + r_n v_n \text{ mit } r_i \in [0, 1]$$

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 $Q = t_1v_1 + \cdots + t_nv_n$ und damit ist

$$Q = (\lfloor t_1 \rfloor v_1 + \cdots + \lfloor t_n \rfloor v_n) + ((t_1 - \lfloor t_1 \rfloor)v_1 + \cdots + (t_n - \lfloor t_n \rfloor)v_n),$$

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* (oder *überdeckungskompakt*), wenn es zu jeder offenen Überdeckung

$$X = \bigcup_{i \in I} U_i \quad \text{mit } U_i \text{ offen und einer beliebigen Indexmenge } I$$

eine endliche Teilmenge $J \subseteq I$ derart gibt, 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 (Satz von Heine-Borel).

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, siehe Aufgabe 26.13. D.h. zu je 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-Lebesgue 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-Lebesgue 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 $\lambda\big(\bigcup_{i\in I} T_i\big) = \sum_{i\in I} \lambda(T_i)$.
(3) Das Borel-Lebesgue 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, siehe Lemma 6.11 (Maß- und Integrationstheorie (Osnabrück 2022-2023)).

• Ein einzelner Punkt und damit auch jede abzählbare Ansammlung von Punkten haben das Maß 0.

• Unter einer linearen Abbildung $L\colon \mathbb{R}^n \to \mathbb{R}^n$ verhält sich das Borel-Lebesgue Maß so: Zu einer Borelmenge T ist auch das Bild $L(T)$ eine Borelmenge mit $\lambda(L(T)) = |\det(L)| \cdot \lambda(T)$, siehe Satz 7.2 (Maß- und Integrationstheorie (Osnabrück 2022-2023)).

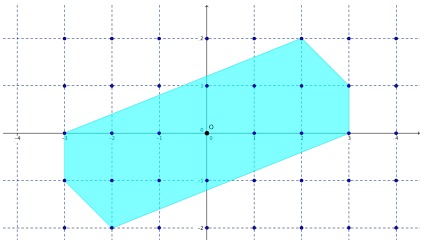
Eine Basis $v_1, \ldots, v_n$ von $\mathbb{R}^n$ liefert ein Gitter $\Gamma \subset \mathbb{R}^n$ zusammen mit der Grundmasche $\mathfrak{M}$, nämlich das durch die v_i aufgespannte Parallelotop. Dessen Volumen (also dessen Borel-Lebesgue-Maß) wird im Folgenden eine Rolle spielen. Das Volumen berechnet 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 Standardektoren 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 beispielsweise 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. 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.



Der folgende Satz heißt *Gitterpunktsatz von Minkowski.*

Satz 26.7. *Es 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*

$$\operatorname{Vol}(T) \geq 2^n \operatorname{Vol}(\mathfrak{M})$$

erfülle. Dann enthält T mindestens einen von 0 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. Wir bezeichnen die Grundmasche von 2Γ mit $\mathfrak{N}$, für ihr Volumen gilt $\operatorname{Vol}(\mathfrak{N}) = 2^n \operatorname{Vol}(\mathfrak{M})$. 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. Es seien diese Maschen (bzw. ihre Ausgangspunkte bzw. ihre Durchschnitte) mit $\mathfrak{N}_i$ (bzw. $Q_i$bzw. T_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. Es sei also angenommen, sie wären paarweise disjunkt. Mindestens eines der T_i (und damit der $\tilde{T}_i$) 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, siehe Aufgabe 26.14). Es sei $x \in X$ ein innerer Punkt (den es gibt, da X konvex ist und ein positives Volumen besitzt) und sei $y \in Y$. Mit S sei die Verbindungsstrecke von x nach y bezeichnet, die ganz in $\mathfrak{N}$ verläuft. Wir wählen einen Punkt $s \in S$, der weder zu X noch 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 Widerspruch führt.

$$\begin{aligned}
\operatorname{Vol}(\mathfrak{N}) &\geq \operatorname{Vol}(X \cup Y \cup B) \\
&= \operatorname{Vol}\left(\bigcup_{i \in I} \tilde{T}_i\right) + \operatorname{Vol}(B) \\
&> \sum_{i \in I} \operatorname{Vol}(\tilde{T}_i) \\
&= \sum_{i \in I} \operatorname{Vol}(T_i) \\
&= \operatorname{Vol}(T) \\
&\geq 2^n \operatorname{Vol}(\mathfrak{M}) \\
&= \operatorname{Vol}(\mathfrak{N}).
\end{aligned}$$

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 $z_j \in T$ folgt (wegen der Zentralsymmetrie) auch $-z_j \in T$ und wegen der Konvexität von T ergibt sich

$$\frac{Q_i - Q_j}{2} = \frac{1}{2}(z_i - z) - \frac{1}{2}(z_j - z) = \frac{1}{2}z_i - \frac{1}{2}z_j \in T.$$

Wir haben also einen von Nullpunkt verschiedenen Gitterpunkt in T gefunden. □

Wir zitieren abschließend ohne Beweis den Hauptsatz über endlich erzeugte kommutative Gruppen. Der anschließende gegebene Spezialfall für die torsionsfreie Situation besagt insbesondere, dass Untergruppen von Gittern als (abstrakte Gruppe) wieder (nicht vollständige) Gitter sind.

Satz 26.8. *Es sei G eine endlich erzeugte kommutative Gruppe. Dann ist G das Produkt von zyklischen Gruppen. D.h. es gibt eine Isomorphie*

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/(n_1) \times \cdots \times \mathbb{Z}/(n_s).$$

Beweis. Dieser Beweis wurde in der Vorlesung nicht vorgeführt. □

Definition 26.9. Eine kommutative Gruppe G heißt *torsionsfrei*, wenn für jedes Element $x \in G$, $x \neq 0$, und $n \in \mathbb{N}_+$ gilt $nx \neq 0$.

Die additiven Gruppen $\mathbb{Z}, \mathbb{Z}^n, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind torsionsfrei, die Restklassengruppen $\mathbb{Z}/(n)$ bei $n \neq 0$ nicht.

Satz 26.10. *Es sei G eine endlich erzeugte torsionsfreie kommutative Gruppe. Dann ist G eine (endlich-erzeugte) freie Gruppe, d.h. es gibt eine Isomorphie*

$$G \cong \mathbb{Z}^r.$$

Beweis. Dieser Beweis wurde in der Vorlesung nicht vorgeführt. □

26. Arbeitsblatt

Übungsaufgaben

Aufgabe 26.1. Wir betrachten im Ring der Gaußschen Zahlen $\mathbb{Z}[\mathrm{i}] \subset \mathbb{C}$ das Ideal $\mathfrak{a} = (1 + 2\mathrm{i}) \subseteq \mathbb{Z}[\mathrm{i}]$.

(a) Skizziere die Situation.
(b) Skizziere mit verschiedenen Farben die verschiedenen Äquivalenzklassen (Nebenklassen) zum Ideal $\mathfrak{a} \subseteq \mathbb{Z}[\mathrm{i}]$.
(c) Wie viele Äquivalenzklassen gibt es? Beschreibe ein Repräsentantensystem.
(d) Erstelle eine Verknüpfungstabelle für die Farben. Welche Farben sind zueinander invers?

Aufgabe 26.2. Skizziere den quadratischen Zahlbereich $A_{-5} = \mathbb{Z}[\sqrt{-5}]$ als Gitter in $\mathbb{C}$. Skizziere ferner das Ideal $\mathfrak{p} = (2, 1+\sqrt{-5})$ als Untergitter.

Aufgabe 26.3. Es sei A_D ein imaginär-quadratischer Zahlbereich mit der Gitterrealisierung

$$A_D = \Gamma = \mathbb{Z} + \mathbb{Z}\omega \subseteq \mathbb{C}$$

mit $\omega = \sqrt{D}$ bzw. $\omega = \frac{1+\sqrt{D}}{2}$. Es sei $\Lambda \subseteq \Gamma$ ein volles Untergitter. Zeige, dass Λ genau dann ein Ideal in A_D ist, wenn

$$\omega\Lambda \subseteq \Lambda$$

gilt.

Aufgabe 26.4. Wir betrachten den Ring der Gaußschen Zahlen als Gitter $\mathbb{Z}[\mathrm{i}] = \mathbb{Z} \oplus \mathbb{Z}\mathrm{i} \subset \mathbb{C}$. Wie sehen die gebrochenen Ideale von $\mathbb{Z}[\mathrm{i}]$ als geometrische Objekte in $\mathbb{C}$ aus?

Aufgabe 26.5. Sind alle Vierecke konvex?

Aufgabe 26.6. Zeige, dass der Durchschnitt von konvexen Mengen im $\mathbb{R}^n$ wieder konvex ist.

Aufgabe 26.7. Charakterisiere die Restklassengruppe eines Gitters $\Gamma \subseteq \mathbb{R}^n$.

Aufgabe 26.8. Es seien $\Gamma_1, \Gamma_2 \subseteq \mathbb{R}^n$ vollständige Gitter. Zeige, dass es eine $\mathbb{R}$-lineare Abbildung

$$\mathbb{R}^n \longrightarrow \mathbb{R}^n$$

gibt, die einen Gruppenisomorphismus

$$\Gamma_1 \longrightarrow \Gamma_2$$

induziert.

Aufgabe 26.9. Es seien $\Gamma_1, \Gamma_2 \subseteq \mathbb{R}^n$ rationale vollständige Gitter. Zeige, dass es eine $\mathbb{Q}$-lineare Abbildung

$$\mathbb{Q}^n \longrightarrow \mathbb{Q}^n$$

gibt, die einen Gruppenisomorphismus

$$\Gamma_1 \longrightarrow \Gamma_2$$

induziert.

Aufgabe 26.10. Es seien $\Gamma_1, \Gamma_2 \subseteq \mathbb{R}^n$ rationale vollständige Gitter. Zeige, dass es ein rationales Gitter $\Gamma \subseteq \mathbb{R}^n$ mit $\Gamma_1, \Gamma_2 \subseteq \Gamma$ gibt.

Aufgabe 26.11. Es sei X ein Hausdorffraum und es sei $Y \subseteq X$ eine Teilmenge, die die induzierte Topologie trage. Es sei Y kompakt. Zeige, dass Y abgeschlossen in X ist.

Aufgabe 26.12. Es sei X ein topologischer Raum und es seien $Y_1, \ldots, Y_n \subseteq X$ kompakte Teilmengen. Zeige, dass auch die Vereinigung $Y = \bigcup_{i=1}^n Y_i$ kompakt ist.

Aufgabe 26.13. Es seien $X, Y \subseteq \mathbb{R}^n$ kompakte Teilmengen. Zeige, dass es Punkte $x \in X$ und $y \in Y$ mit der Eigenschaft gibt, dass für beliebige Punkte $P \in X$ und $Q \in Y$ die Abschätzung

$$d(x,y) \leq d(P,Q)$$

gilt.

Tipp: Man betrachte die Produktmenge $S \times T \subseteq \mathbb{R}^n \times \mathbb{R}^n \cong \mathbb{R}^{2n}$ und darauf die Abbildung $(x,y) \mapsto \sum_{i=1}^n (x_i - y_i)^2$. Man argumentiere dann mit Satz 36.12 (Analysis (Osnabrück 2021-2023)).

Aufgabe 26.14. Es sei X ein metrischer Raum und seien $Y, Z \subseteq X$ kompakte Teilmengen, die zueinander disjunkt seien. Zeige, dass es ein $d > 0$ derart gibt, dass für beliebige Punkte $P \in Y$ und $Q \in Z$ die Abstandsbedingung $d(P,Q) \geq d$ gilt.

Aufgabe 26.15. Zeige, dass ein Körper K genau dann die Charakteristik 0 besitzt, wenn die additive Gruppe $(K, +, 0)$ torsionsfrei ist.

Aufgaben zum Abgeben

Aufgabe 26.16. (4 Punkte)

Alle Springmäuse leben in $\mathbb{Z}^2$ und verfügen über zwei Sprünge, nämlich den Sprung $\pm(3,4)$ und den Sprung $\pm(5,2)$. Wie viele Springmaus-Populationen gibt es? Die Springmäuse Albert, Beate, Erich, Heinz, Sabine und Frida sitzen in den Positionen

$$(14,11),\ (13,15),\ (17,12),\ (15,19),\ (16,16) \text{ und } (12,20)\,.$$

Welche Springmäuse können sich begegnen?

Aufgabe 26.17. (4 Punkte)

Es sei U eine Teilmenge des $\mathbb{R}^n$. Zeige, dass ein Punkt $Q \in \mathbb{R}^n$ genau dann zur konvexen Hülle von U gehört, wenn es endlich viele Punkte $P_i \in U$, $i \in I$, und reelle Zahlen r_i, $i \in I$, mit $r_i \in [0,1]$, $\sum_{i \in I} r_i = 1$ und mit

$$Q = \sum_{i \in I} r_i P_i$$

gibt.

Aufgabe 26.18. (6 Punkte)

Skizziere zum Gitter $\mathbb{Z}^2$ in $\mathbb{R}^2$ drei Teilmengen, die die Maßbedingung des Gitterpunksatzes von Minkowski erfüllen, die den Nullpunkt, aber keine weiteren Gitterpunkte enthalten, und die jeweils zwei der drei Bedingungen konvex, kompakt und zentralsymmetrisch erfüllen.

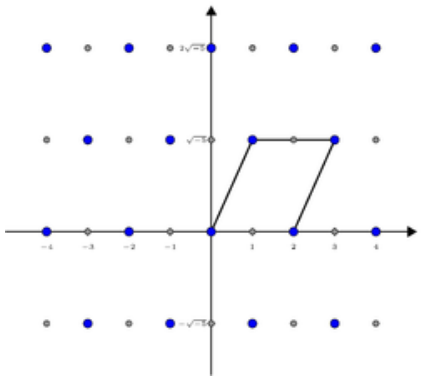
27. Vorlesung - Die Endlichkeit der Klassenzahl

Die Endlichkeit der Klassenzahl für quadratische Zahlkörper

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.

Lemma 27.1. *Es 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. Es sei also $\mathfrak{a}$ ein solches Ideal. Dann ist $n \in \mathfrak{a}$ nach Korollar 21.5 und damit entspricht $\mathfrak{a}$ einem Ideal aus $R/(n)$. Dieser Ring ist aber nach Satz 18.14 endlich und besitzt somit überhaupt nur endlich viele Ideale. $\square$



Das Gitter zum Zahlbereich $\mathbb{Z}[\sqrt{-5}]$ und zum Ideal $(2, 1+\sqrt{-5})$ (blau, mit einer Grundmasche).

Bemerkung 27.2. Es sei $D \neq 0, 1$ quadratfrei und A_D der zugehörige quadratische Zahlbereich mit Diskriminante $\triangle$. Wir wollen ein von 0 verschiedenes Ideal $\mathfrak{a}$ aus A_D als ein (vollständiges) Gitter $\Gamma_{\mathfrak{a}}$ in $\mathbb{R}^2$ auffassen. Bei $D < 0$, also im imaginär-quadratischen Fall, verwenden wir die natürliche 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 nach $\mathbb{C}$ 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 mit $b = \alpha + \beta\omega$ wie in Satz 21.1 beschrieben. Hierbei sei $1, \omega$ die übliche $\mathbb{Z}$-Basis von A_D, also $\omega = \sqrt{D}$ bzw. $\omega = \frac{1+\sqrt{D}}{2}$. Das Basiselement ω wird auf $(0, \sqrt{|D|})$ bzw. auf $\left(\frac{1}{2}, \frac{\sqrt{|D|}}{2}\right)$ geschickt. Daher wird das zum Ideal gehörige Gitter $\Gamma_{\mathfrak{a}}$ (in $\mathbb{R}^2$) durch

$$(a, 0) \text{ und } \left(\alpha, \beta\sqrt{|D|}\right) \text{ bei } D = 2, 3 \mod 4$$

und

$$(a, 0) \text{ und } \left(\alpha + \frac{\beta}{2}, \beta\frac{\sqrt{|D|}}{2}\right) \text{ bei } D = 1 \mod 4$$

aufgespannt.

Wir setzen zunächst die Norm des Ideals mit dem Flächeninhalt des Gitters in Verbindung.

Lemma 27.3. *Es sei $D \neq 0, 1$ eine quadratfreie Zahl, sei A_D der zugehörige quadratische Zahlbereich und sei $\varphi\colon A_D \to \mathbb{R}^2$ 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 durch die $\mathbb{Z}$-Basis (a, b) mit $(a) = \mathbb{Z} \cap \mathfrak{a}$ und

$$b = \alpha + \beta u$$

erzeugt, 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 $D = 2, 3 \mod 4$

$$\mu(\Gamma_\mathfrak{a}) = \left|\det \begin{pmatrix} a & \alpha \\ 0 & \beta\sqrt{|D|} \end{pmatrix}\right| = a\beta\sqrt{|D|} = a\beta\frac{\sqrt{|\triangle|}}{2} = \frac{1}{2}N(\mathfrak{a})\sqrt{|\triangle|},$$

wobei wir Korollar 21.5 und die Diskriminantengleichung $\triangle = 4D$ benutzt haben.

Bei $D = 1 \mod 4$ ist

$$\mu(\Gamma_\mathfrak{a}) = \left|\det \begin{pmatrix} a & \alpha + \frac{\beta}{2} \\ 0 & \frac{\beta\sqrt{|D|}}{2} \end{pmatrix}\right| = \frac{a\beta}{2}\sqrt{|D|} = \frac{1}{2}N(\mathfrak{a})\sqrt{|\triangle|}$$

aus den gleichen Gründen. □

Lemma 27.4. *Es sei $D \neq 0, 1$ 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 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 $\frac{\sqrt{|\triangle|}N(\mathfrak{a})}{2}$.

Es sei $D < 0$. Als Menge T 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, der in Lemma 27.3 berechnet wurde. Also gibt es einen vom Nullpunkt verschiedenen Gitterpunkt $x \in \Gamma \cap T$, 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.

Es 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 somit vier gedrehte Hyperbeln, die jeweils eine Achse senkrecht schneiden. Diese Hyperbeln schließen das (konvexe, kompakte, zentralsymmetrische) Quadrat mit den Eckpunkten $(\pm\sqrt{c}, \pm\sqrt{c})$ ein, das die Hyperbeläste auf den Achsen berührt. Wir setzen $c := \frac{1}{2}\sqrt{|\triangle|}N(\mathfrak{a})$. Dann hat das Quadrat T mit diesen Eckpunkten die Seitenlänge $2\sqrt{c}$ und den Flächeninhalt $2\sqrt{|\triangle|}N(\mathfrak{a})$ und enthält nach dem Gitterpunktsatz von Minkowski einen vom Nullpunkt verschiedenen Gitterpunkt $x \in \Gamma_{\mathfrak{a}} \cap T$. Dieser entspricht einem Element $f \in \mathfrak{a}$, $f \neq 0$, und

$$|N(f)| = \left|x_1^2 - x_2^2\right| \leq x_1^2 \leq c = \frac{1}{2}\sqrt{|\triangle|}N(\mathfrak{a}).$$

□

Lemma 27.5. *Es sei $D \neq 0, 1$ 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. Es sei c eine Idealklasse. Die inverse Klasse c^{-1} wird durch ein Ideal $\mathfrak{b} \subseteq R$ repräsentiert. 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 $\mathfrak{a} := (f)\mathfrak{b}^{-1}$, was nach dem Satz von Dedekind zu $\mathfrak{ab} = (f)$ äquivalent ist. Dieses $\mathfrak{a}$ ist ein Ideal, da ja $\mathfrak{b}^{-1}$ Bemerkung 24.7 alle Elemente aus $\mathfrak{b}$ nach R multipliziert. Nach Korollar 21.11 und nach Satz 21.7 ist

$$N(\mathfrak{a})N(\mathfrak{b}) = N(\mathfrak{ab}) = N((f)) = |N(f)|\,.$$

Daher ist

$$N(\mathfrak{a}) = \frac{|N(f)|}{N(\mathfrak{b})} \leq \begin{cases} \frac{2}{\pi}\sqrt{|\triangle|} & \text{bei } D < 0\,, \\ \frac{1}{2}\sqrt{|\triangle|} & \text{bei } D > 0\,. \end{cases}$$

□

Satz 27.6. *Es sei $R = A_D$ ein quadratischer Zahlbereich. Dann ist die Divisorenklassengruppe von R eine endliche Gruppe.*

Beweis. Nach Lemma 27.5 wird jede Klasse in der Klassengruppe durch ein Ideal mit einer Norm repräsentiert, die durch die dort angegebene Schranke beschränkt ist. D.h., dass die Ideale mit einer Norm unterhalb dieser Schranke alle Klassen repräsentieren. Nach Lemma 27.1 gibt es aber überhaupt nur endlich viele Ideale mit einer Norm unterhalb einer gegebenen Schranke. □

Das im Beweis verwendete Lemma bietet prinzipiell eine Abschätzung für die Anzahl der Klassengruppe.

Definition 27.7. Es 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. *Es 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 0 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. *Es sei $D \neq 0, 1$ 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, das die Normbedingung*

$$N(\mathfrak{p}) \leq \begin{cases} \frac{2\sqrt{|\triangle|}}{\pi} & \text{bei } D < 0\,, \\ \frac{\sqrt{|\triangle|}}{2} & \text{bei } D > 0\,. \end{cases}$$

erfüllt, ein Hauptideal sei. Dann ist A_D faktoriell.

Beweis. Es sei $\mathfrak{a}$ ein Ideal $\neq 0$ unterhalb der angegebenen Normschranke. Nach Satz 23.14 ist $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_k$ mit Primidealen $\mathfrak{p}_i$, und wegen Korollar 21.11 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. *Es sei $D \neq 0,1$ 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 in A_D 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, sodass 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. Es sei $R = \mathbb{Z}[\sqrt{-5}]$, also $D = -5$ und $\triangle = -20$. Jede Idealklasse enthält ein Ideal $\mathfrak{a}$ der Norm

$$N(\mathfrak{a}) \leq \frac{2\sqrt{20}}{\pi},$$

sodass 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. Nach Beispiel 21.8 ist $\mathfrak{p}$ kein Hauptideal. Daher ist die Idealklassengruppe isomorph zu $\mathbb{Z}/(2)$, wobei das Nullelement durch die Hauptdivisoren (oder Hauptideale) repräsentiert wird und das andere Element durch $\mathfrak{p}$.

Beispiel 27.12. Es 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 25.5, dass R nicht euklidisch ist. Dennoch ist R faktoriell und nach 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, sodass 2 träge in R ist und insbesondere eine Primfaktorzerlegung besitzt.

27. Arbeitsblatt

Übungsaufgaben

Aufgabe 27.1. Es sei $R = A_5$ der quadratische Zahlbereich zu $D = 5$. Zeige mittels Korollar 27.10, dass R faktoriell ist.

Aufgabe 27.2. Es sei $R = A_7$ der quadratische Zahlbereich zu $D = 7$. Zeige mittels Korollar 27.10, dass R faktoriell ist.

Aufgabe 27.3. Es sei $R = A_{10}$ der quadratische Zahlbereich zu $D = 10$. Bestimme die Klassengruppe von R.

Aufgabe 27.4. Es sei $R = A_{13}$ der quadratische Zahlbereich zu $D = 13$. Zeige mittels Korollar 27.10, dass R faktoriell ist.

Aufgabe 27.5. Zeige mit Korollar 27.10, dass der Ring der Gaußschen Zahlen $\mathbb{Z}[\mathrm{i}]$ faktoriell ist.

Aufgabe 27.6. Es sei $R = A_{-6}$ der quadratische Zahlbereich zu $D = -6$. Bestimme die Klassengruppe von R.

Aufgabe 27.7. Es sei $R = A_{-7}$ der quadratische Zahlbereich zu $D = -7$. Zeige mittels Korollar 27.10, dass R faktoriell ist.

Aufgabe 27.8. Es sei $R = A_{-14}$ der quadratische Zahlbereich zu $D = -14$. Bestimme die Klassengruppe von R.

Aufgabe 27.9. Es sei $R = A_{-17}$ der quadratische Zahlbereich zu $D = -17$. Bestimme die Klassengruppe von R.

Aufgabe 27.10. Es sei $R = A_{-21}$ der quadratische Zahlbereich zu $D = -21$. Bestimme die Klassengruppe von R.

Aufgabe 27.11. Es sei R ein quadratischer Zahlbereich und $\mathfrak{a} \neq 0$ ein Ideal in R. Zeige, dass es ein Element $f \in \mathfrak{a}$ mit der Eigenschaft gibt, dass für alle maximale Ideale $\mathfrak{m}$ gilt:

$$f \in \mathfrak{m} \text{ genau dann, wenn } \mathfrak{a} \subseteq \mathfrak{m}\,.$$

Aufgabe 27.12. Es sei R ein quadratischer Zahlbereich und $\mathfrak{a} \neq 0$ ein Ideal in R. Zeige, dass es eine natürliche Zahl $m \in \mathbb{N}$ derart gibt, dass das inverse Ideal $\mathfrak{a}^{-1}$ zu $\mathfrak{a}^m$ äquivalent ist.

Aufgabe 27.13. Es sei R ein Zahlbereich und $f \in R$, $f \neq 0$. Definiere eine „Divisorenklassengruppe“ für die Nenneraufnahme R_f. Dabei soll wieder gelten, dass diese Divisorenklassengruppe genau dann 0 ist, wenn R_f faktoriell ist. Ferner soll es einen natürlichen surjektiven Gruppenhomomorphismus

$$\mathrm{DKG}\,(R) \longrightarrow \mathrm{DKG}\,(R_f)$$

geben.

Aufgaben zum Abgeben

Aufgabe 27.14. (4 Punkte)

Es sei $R = A_{-43}$ der quadratische Zahlbereich zu $D = -43$. Zeige mittels Korollar 27.10, dass R faktoriell ist.

Aufgabe 27.15. (4 Punkte)

Es sei $R = A_{-67}$ der quadratische Zahlbereich zu $D = -67$. Zeige mittels Korollar 27.10, dass R faktoriell ist.

Aufgabe 27.16. (5 Punkte)

Es sei R ein quadratischer Zahlbereich. Zeige, dass es ein $f \in R$, $f \neq 0$, mit der Eigenschaft gibt, dass die Nenneraufnahme R_f faktoriell ist.

Aufgabe 27.17. (5 Punkte)

Es sei D quadratfrei und sei A_D der zugehörige quadratische Zahlbereich. Ferner sei D ein Vielfaches von 5 und $D = 2, 3 \mod 4$. Zeige: A_D ist nicht faktoriell.

Tipp: Siehe Aufgabe 25.19.

28. Vorlesung - Quadratische Formen

Der historische Ursprung der quadratischen Zahlbereiche wie auch der Klassengruppe liegt in der besonders von Gauß entwickelten Theorie der quadratischen Formen. In der ersten Vorlesung haben wir gefragt, welche Zahlen als Summe von zwei Quadratzahlen darstellbar sind, also von der Form x^2+y^2 sind, und dies haben wir im weiteren Verlauf mit der Norm im Ring der Gaußschen Zahlen $\mathbb{Z}[\mathrm{i}]$ in Verbindung gebracht. Einen ähnlichen Zusammenhang gibt es zu jeder binären quadratischen Form.

Binäre quadratische Formen

Definition 28.1. Unter einer *binären quadratischen Form* versteht man einen Ausdruck der Gestalt

$$aX^2+bXY+cY^2$$

mit $a,b,c \in \mathbb{Z}$.

Die a,b,c heißen die Koeffizienten der quadratischen Form. Wir fassen eine binäre quadratische Form F als eine Abbildung

$$\mathbb{Z}^2 \longrightarrow \mathbb{Z},\ (x,y) \longmapsto ax^2+bxy+cy^2,$$

auf. Die Matrix

$$\begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix}$$

heißt die *Gramsche Matrix* zur Form F. Mit ihr kann man

$$F(x,y) = (x,\ y) \begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

schreiben.

Definition 28.2. Zu einer binären quadratischen Form

$$aX^2+bXY+cY^2$$

nennt man

$$b^2-4ac$$

die *Diskriminante* der Form.

Die Diskriminante kann man auch als das -4-fache der Determinante von $\begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix}$ ansehen. Wir werden diese Diskriminante bald mit der Diskriminante eines quadratischen Zahlbereiches in Verbindung bringen.

Definition 28.3. Man sagt, dass eine ganze Zahl n durch eine binäre quadratische Form

$$aX^2+bXY+cY^2$$

darstellbar ist, wenn es ganze Zahlen $(x,y) \in \mathbb{Z}^2$ mit

$$n = ax^2 + bxy + cy^2$$

gibt.

Die Zahlen $a, c, a+b+c$ sind unmittelbar darstellbar. Im Allgemeinen ist es schwierig, die Mengen aller darstellbaren Zahlen zu beschreiben. Für die quadratische Form X^2+Y^2 bedeutet die Darstellbarkeit, dass n eine Summe von zwei Quadraten ist. Zur Beantwortung dieser Frage ist die Betrachtung der Faktorzerlegung in $\mathbb{Z}$[i] hilfreich.

Definition 28.4. Eine binäre quadratische Form $aX^2+bXY+cY^2$ heißt *einfach*, wenn die Koeffizienten a, b, c teilerfremd sind.

Wenn g der größte gemeinsame Teiler von a, b, c ist, so nennt man die durch

$$\frac{a}{g}X^2 + \frac{b}{g}XY + \frac{c}{g}Y^2$$

gegebene Form die *Vereinfachung* der ursprünglichen Form. Es handelt sich dann um eine einfache Form.

Zu einer Matrix $M = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ mit ganzzahligen Einträgen $r, s, t, u \in \mathbb{Z}$ und einer binären quadratischen Form $F = aX^2+bXY+cY^2$ erhält man durch die Hintereinanderschaltung

$$\mathbb{Z}^2 \xrightarrow{M} \mathbb{Z}^2 \xrightarrow{F} \mathbb{Z}$$

die neue quadratische Form $F' = F \circ M$. Wenn man die Variablen links mit V, W bezeichnet, so liegt insgesamt die quadratische Form vor, die ein Tupel (v,w) auf

$$\begin{aligned} & a(rv+sw)^2 + b(rv+sw)(tv+uw) + c(tv+uw)^2 \\ = \; & \big(ar^2+brt+ct^2\big)v^2 + (2ars+bru+bst+2ctu)vw + \big(as^2+bsu+cu^2\big)w^2 \end{aligned}$$

abbildet. Die neuen Koeffizienten der transformierten Form sind also

$$a' = ar^2+brt+ct^2, b' = 2ars+bru+bst+2ctu \text{ und } c' = as^2+bsu+cu^2$$

. Dies können wir auch als Matrixgleichung als

$$\begin{pmatrix} a' & \frac{1}{2}b' \\ \frac{1}{2}b' & c' \end{pmatrix} = \begin{pmatrix} r & t \\ s & u \end{pmatrix} \begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix} \begin{pmatrix} r & s \\ t & u \end{pmatrix}$$

schreiben, siehe Aufgabe 28.5. Die Matrix M ist über $\mathbb{Z}$ genau dann invertierbar, wenn ihre Determinante gleich 1 oder gleich -1 ist, siehe Aufgabe 28.1. Bei einer solchen invertierbaren Transformation ändern sich wesentliche Eigenschaften der Form nicht.

Definition 28.5. Zwei binäre quadratische Formen

$$F = aX^2+bXY+cY^2 \text{ und } F' = a'X^2+b'XY+c'Y^2$$

heißen *äquivalent*, wenn es eine ganzzahlige invertierbare 2×2-Matrix M mit

$$F' \;=\; FM$$

gibt.

Definition 28.6. Zwei binäre quadratische Formen

$$F = aX^2 + bXY + cY^2 \text{ und } F' = a'X^2 + b'XY + c'Y^2$$

heißen *strikt äquivalent*, wenn es eine ganzzahlige 2×2-Matrix M mit Determinante 1 und mit

$$F' \;=\; FM$$

gibt.

Die Formen $aX^2+bXY+cY^2$ und $aX^2-bXY+cY^2$ sind zueinander (über die Matrix $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$) äquivalent, aber im Allgemeinen nicht strikt äquivalent.

Lemma 28.7. *(1) Die Äquivalenz und die strikte Äquivalenz von binären quadratischen Formen ist eine Äquivalenzrelation.*

(2) Die Diskriminante einer binären quadratischen Form hängt nur von deren Äquivalenzklasse ab.

(3) Die dargestellen Zahlen hängen nur von der Äquivalenzklasse der Form ab.

Beweis. (1) Diese beiden Aussagen folgen daraus, dass das Produkt invertierbarer Matrizen (über $\mathbb{Z}$) wieder invertierbar ist und aus dem Determinantenmultiplikationssatz.

(2) Wir arbeiten mit der Umrechnungsregel für die Koeffizienten in Matrixform, also

$$\begin{pmatrix} a' & \frac{1}{2}b' \\ \frac{1}{2}b' & c' \end{pmatrix} = \begin{pmatrix} r & t \\ s & u \end{pmatrix} \begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix} \begin{pmatrix} r & s \\ t & u \end{pmatrix}$$

Der Determinantenmultiplikationssatz liefert

$$\begin{aligned} \operatorname{diskr}(F') &= -4 \cdot \det \begin{pmatrix} b' & 2c' \\ 2a' & b' \end{pmatrix} \\ &= -4 \cdot (\pm 1) \det \begin{pmatrix} b & 2c \\ 2a & b \end{pmatrix} (\pm 1) \\ &= -4 \cdot \det \begin{pmatrix} b & 2c \\ 2a & b \end{pmatrix} \\ &= \operatorname{diskr}(F). \end{aligned}$$

(3) Dies folgt unmittelbar aus dem kommutativen Diagramm

$$\begin{array}{ccc} \mathbb{Z}^2 & \xrightarrow{M} & \mathbb{Z}^2 \\ & F' \searrow & \downarrow F \\ & & \mathbb{Z}\,. \end{array}$$

□

Wir brauchen noch ein etwas abstrakteres Konzept von einer quadratischen Form.

Definition 28.8. Es sei R ein kommutativer Ring. Eine *quadratische Form* auf einem R-Modul L ist eine Abbildung

$$Q\colon L \longrightarrow R,$$

die die beiden Eigenschaften

(1)
$$Q(rv) = r^2 Q(v)$$
für alle $r \in R$ und $v \in L$,

(2)
$$Q(u+v) + Q(u-v) = 2Q(u) + 2Q(v)$$
für alle $u, v \in L$,

erfüllt.

Eine binäre quadratische Form auf $\mathbb{Z}^2$ ist eine quadratische Form in diesem Sinne, siehe Aufgabe 28.13. Auf einem freien $\mathbb{Z}$-Modul L vom Rang zwei, der also isomorph zu $\mathbb{Z}^2$ ist, gibt es keine kanonische $\mathbb{Z}$-Basis, so dass eine quadratische Form auf ihm zunächst nicht in der expliziten Form von oben gegeben ist. Erst die Fixierung eines Isomorphismus

$$\mathbb{Z}^2 \longrightarrow L$$

führt Q in die explizite Form über. Bei einer anderen Basis ändern sich zwar die Koeffizienten, doch sind die zugehörigen expliziten binären quadratischen Formen zueinander äquivalent, da sie durch die invertierbaren Basiswechselmatrizen ineinander überführt werden. Insbesondere ist die Diskriminante einer quadratischen Form auf L wohldefiniert.

Binäre quadratische Formen und quadratische Zahlbereiche

Ein quadratischer Zahlbereich $R \subseteq \mathbb{Q}[\sqrt{D}]$ ist nach Korollar 18.10 als Gruppe isomorph zu $\mathbb{Z}^2$. Ferner erfüllt die Norm

$$N\colon \mathbb{Q}[\sqrt{D}] \longrightarrow \mathbb{Q},\ x + y\sqrt{D} \longmapsto x^2 - y^2 D,$$

die Eigenschaften einer quadratischen Form. Die Werte der Norm eingeschränkt auf den Ganzheitsring (und auf jedes Ideal) liegen in $\mathbb{Z}$, deshalb liegt ein freier $\mathbb{Z}$-Modul vom Rang zwei zusammen mit einer quadratischen Form vor.

Beispiel 28.9. Wir bestimmen für die quadratischen Zahlbereiche R die binäre quadratische Form, die auf R durch die Norm gegeben ist. Es sei also R der Ganzheitsring in $K = \mathbb{Q}[\sqrt{D}]$ zu einer quadratfreien Zahl $D \neq 0, 1$.

Es sei zunächst

$$D = 2, 3 \mod 4.$$

Dann ist der Ganzheitsring nach Satz 20.9 gleich $\mathbb{Z}[\sqrt{D}]$ und wir arbeiten mit der $\mathbb{Z}$-Basis $1, \sqrt{D}$. Die Norm eines Elementes $x + y\sqrt{D}$ ist somit

$$N(x + y\sqrt{D}) \ = \ \det \begin{pmatrix} x & Dy \\ y & x \end{pmatrix} \ = \ x^2 - Dy^2$$

und dies ist die explizite Beschreibung der durch die Norm gegebenen quadratischen Form. Ihre Diskriminante ist

$$\operatorname{diskr}(N) \ = \ 4D,$$

was gemäß Lemma 20.10 mit der Diskriminante $\triangle(R)$ des Zahlbereichs übereinstimmt.

Es sei nun

$$D \ = \ 1 \mod 4.$$

Dann ist der Ganzheitsring nach Satz 20.9 gleich $\mathbb{Z}[\omega]$ mit

$$\omega \ = \ \frac{1 + \sqrt{D}}{2}$$

und wir arbeiten mit der $\mathbb{Z}$-Basis $1, \omega$. Die Norm eines Elementes $x + y\omega$ ist wegen

$$(x + y\omega)\omega \ = \ x\omega + y\omega^2 \ = \ x\omega + y\left(\frac{D-1}{4} + \omega\right) \ = \ y\frac{D-1}{4} + (x+y)\omega$$

gleich

$$N(x + y\omega) \ = \ \det \begin{pmatrix} x & \frac{D-1}{4}y \\ y & x+y \end{pmatrix} \ = \ x^2 + xy - \frac{D-1}{4}y^2 \ = \ x^2 + xy + \frac{1-D}{4}y^2$$

und dies ist die explizite Beschreibung der durch die Norm gegebenen quadratischen Form. Ihre Diskriminante ist

$$\operatorname{diskr}(N) \ = \ 1 + (D-1) \ = \ D,$$

was gemäß Lemma 20.10 mit der Diskriminante $\triangle(R)$ des Zahlbereichs übereinstimmt.

Eine solche Interpretation der Norm gilt nicht nur für den ganzen Zahlbereich, sondern auch für jedes Ideal davon.

Lemma 28.10. *Es sei R ein quadratischer Zahlbereich und es sei $\mathfrak{a} \subseteq R$ ein von 0 verschiedenes Ideal in R. Dann wird durch $f \mapsto \frac{N(f)}{N(\mathfrak{a})}$ eine binäre quadratische Form auf $\mathfrak{a}$ definiert, die einfach ist und deren Diskriminante gleich der Diskriminante des Zahlbereiches R ist.*

Beweis. Die Norm ist eine quadratische Form auf $\mathfrak{a}$ mit Werten in $\mathbb{Z}$. Zu jedem Element $f \in \mathfrak{a}$ liegt ein surjektiver Restklassenhomomorphismus

$$R/(f) \longrightarrow R/\mathfrak{a}$$

vor. Beide Restklassenringe sind nach Satz 18.14 endlich, und somit ist die Anzahl von $R/\mathfrak{a}$ ein Teiler der Anzahl von $R/(f)$. Diese Anzahlen sind aber

nach Definition bzw. (bis auf das Vorzeichen) nach Satz 21.7 gleich $N(\mathfrak{a})$ bzw. $N(f)$. Die Quotienten $\frac{N(f)}{N(\mathfrak{a})}$ liegen also in $\mathbb{Z}$ und es liegt eine ganzzahlige quadratische Form vor. Diese ist nach Korollar 18.9 binär.

Mit einer beliebigen $\mathbb{Z}$-Basis s, t des Ideals $\mathfrak{a}$ ist die durch die Norm gegebene binäre quadratische Form durch die Werte $N(s), N(s+t), N(t)$ festgelegt, und zwar lautet die explizite Beschreibung

$$N(s)X^2 + (N(s+t) - N(s) - N(t))XY + N(t)Y^2 \, .$$

Mit der Konjugation gilt

$$\begin{aligned} N(s) &= s\overline{s}, \\ N(t) &= t\overline{t} \end{aligned}$$

und

$$N(s+t) = (s+t)\overline{(s+t)} = s\overline{s} + s\overline{t} + t\overline{s} + t\overline{t}.$$

Somit ist der mittlere Koeffizient der quadratischen Form gleich

$$N(s+t) - N(s) - N(t) = s\overline{t} + t\overline{s}$$

und die Diskriminate der quadratischen Form ist gleich

$$(s\overline{t} + t\overline{s})^2 - 4N(s)N(t) = (s\overline{t} - t\overline{s})^2.$$

Wir ziehen nun die Basis (a, b) des Ideals gemäß Satz 21.1 heran. Die Diskriminante ist dann

$$(a\overline{b} - \overline{a}b)^2 = a^2(\overline{b} - b)^2.$$

Je nach Fall ist die Klammer rechts gleich $2\beta\sqrt{D}$ bzw. gleich $2\beta\omega - \beta$. Im ersten Fall ist das Quadrat davon gleich $4\beta^2 D$. Im zweiten Fall ist das Quadrat davon gleich $\beta^2(2\omega - 1)^2 = \beta^2 D$. Wenn man also die Norm durch die Norm des Ideals dividiert, die ja nach Korollar 21.5 gleich $a\beta$ ist, so ergibt sich in beiden Fällen eine quadratische Form, deren Diskriminante gleich der Diskriminante des Zahlbereiches ist. Die Einfachheit ergibt sich aus Aufgabe 21.3. □

Beispiel 28.11. Wir betrachten im quadratischen Zahlbereich R zu $D = -5$ das Ideal

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

wobei die Erzeuger zugleich eine $\mathbb{Z}$-Basis sind. Die Norm dieses Ideals ist 2 und die durch die Norm gegebene quadratische Form hat bezüglich dieser Basis die Gestalt

$$4x^2 + 4xy + 6y^2 \, .$$

Durch Vereinfachung im Sinne von Lemma 28.10, also Division durch die Norm des Ideals, gelangt man zur quadratischen Form

$$2x^2 + 2xy + 3y^2$$

mit der Diskriminante

$$4 - 4 \cdot 2 \cdot 3 = -20 = 4(-5).$$

Diese Form ist nicht zur Hauptform der Diskriminante -20 aquivalent, denn diese ist x^2+5y^2. Letztere stellt beispielsweise den Wert 5 dar, erstere gemäß Aufgabe 28.23 nicht.

Zwei zueinander äquivalente Ideale definieren eine Äquivalenzklasse von binären quadratischen Formen. Um strikte Äquivalenzklassen zu erhalten, muss man die strikte Äquivalenz von Idealen einführen.

Definition 28.12. Es sei R ein Zahlbereich. Zwei gebrochene Ideale $\mathfrak{f}$ und $\mathfrak{g}$ heißen *strikt äquivalent*, wenn es ein $h \in Q(R)$, $h \neq 0$, mit positiver Norm derart gibt, dass

$$\mathfrak{f} = (h)\mathfrak{g}.$$

Wenn man die strikte Äquivalenzklasse der Form erhalten möchte, so darf man nicht mit einer beliebigen $\mathbb{Z}$-Basis des Ideals arbeiten, da beispielsweise die Vertauschung der Basiselemente die strikte Äquivalenzklasse der Form vertauscht. Stattdessen muss man mit einer orientierten Basis des Ideals arbeiten. Wir repräsentieren die positive Orientierung durch die Basis aus Satz 21.1. Die Übergangsmatrix zwischen zwei orientierungstreuen Basen besitzt die Determinante 1.

Satz 28.13. *Es sei R der quadratische Zahlbereich zur quadratfreien Zahl $D \neq 0, 1$ mit Diskriminante $\triangle = \triangle(R)$. Dann ist die Abbildung*

$$\mathfrak{a} \longmapsto \left(\mathfrak{a}, \frac{N(-)}{N(\mathfrak{a})}\right),$$

die einem (orientierten) Ideal $\neq 0$ die durch die vereinfachte Norm gegebene binäre quadratische Form zuordnet, mit der strikten Äquivalenz von Idealen bzw. Formen verträglich, und stiftet eine Bijektion zwischen den strikten Idealklassen und den strikten Äquivalenzklassen von einfachen quadratischen Formen mit Diskriminante $\triangle$.

Beweis. Dass die Zuordnung aus einem Ideal eine binäre quadratische Form mit der entsprechenden Diskriminante macht, wurde in Lemma 28.10 gezeigt. Es seien $\mathfrak{a}$ und $\mathfrak{b}$ strikt äquivalente Ideale, d.h. es gibt ein $h \in R$ mit positiver Norm und mit $\mathfrak{b} = (h)\mathfrak{a}$. Für jedes $f \in \mathfrak{a}$ gilt nach Satz 21.7 und Korollar 21.11

$$\begin{aligned}
\frac{N(hf)}{N(\mathfrak{b})} &= \frac{N(h)N(f)}{N((h)\mathfrak{a})} \\
&= \frac{N(h)N(f)}{N((h))N(\mathfrak{a})} \\
&= \frac{N(h)N(f)}{|N(h)|\,N(\mathfrak{a})} \\
&= \frac{N(f)}{N(\mathfrak{a})},
\end{aligned}$$

daher ist das Diagramm

$$\begin{array}{ccc} \mathfrak{a} & \xrightarrow{\frac{N(-)}{N(\mathfrak{a})}} & \mathbb{Z} \\ \cdot h \downarrow & \nearrow_{\frac{N(-)}{N(\mathfrak{b})}} & \\ \mathfrak{b} & & \end{array}$$

kommutativ. Da die Multiplikation mit h ein R-Modulisomorphismus und insbesondere ein (orientierter) Gruppenisomorphismus zwischen $\mathfrak{a} \cong \mathbb{Z}^2$ und $\mathfrak{b} \cong \mathbb{Z}^2$ ist, der durch eine Matrix mit Determinante 1 gegeben ist, bedeutet dies, dass die quadratischen Formen strikt äquivalent sind.

Es sei nun eine einfache binäre quadratische Form $ax^2 + bxy + cy^2$ gegeben, deren Diskriminante $b^2 - 4ac$ gleich der Diskriminante des Zahlbereichs, also gleich D bzw. $4D$ sei. Im zweiten Fall ist b gerade und somit ist in beiden Fällen $\frac{b-\sqrt{\triangle}}{2}$ ein Element aus R.

Bei $a > 0$ betrachten wir

$$\mathfrak{a} = \mathbb{Z}a + \mathbb{Z}\frac{b - \sqrt{\triangle}}{2}.$$

Dies ist ein Ideal.

Wegen Korollar 21.6 ist

$$N(\mathfrak{a}) = |-a| = a,$$
$$N(a) = a^2$$

und (für den Fall $D = 2, 3 \mod 4$, auf den wir uns hier beschränken)

$$\begin{aligned} N\left(\frac{b-\sqrt{\triangle}}{2}\right) &= N\left(\frac{b-2\sqrt{D}}{2}\right) \\ &= \left(\frac{b}{2} - \sqrt{D}\right)\left(\frac{b}{2} + \sqrt{D}\right) \\ &= \frac{b^2}{4} - D \\ &= \frac{b^2 - 4D}{4} \\ &= \frac{b^2 - \triangle}{4} \\ &= \frac{b^2 - (b^2 - 4ac)}{4} \\ &= ac \end{aligned}$$

und

$$\begin{aligned} N\left(a + \frac{b-\sqrt{\triangle}}{2}\right) &= N\left(\frac{2a+b}{2} - \sqrt{D}\right) \\ &= \left(\frac{2a+b}{2}\right)^2 - D \\ &= \frac{4a^2 + 4ab + b^2 - 4D}{4} \end{aligned}$$

$$\begin{aligned} &= \frac{4a^2+4ab+b^2-(b^2-4ac)}{4} \\ &= a^2+ab+ac. \end{aligned}$$

Wenn man diese drei charakteristischen Werte durch $N(\mathfrak{a}) = a$ dividiert, so erhält man die Werte a, c und $a+b+c$, was mit den Koeffizienten der vorgegebenen quadratischen Form übereinstimmt.

Für den Fall $a < 0$ setzt man

$$\mathfrak{a} = \sqrt{\triangle} \cdot \left(a\mathbb{Z} + \frac{b-\sqrt{\triangle}}{2}\mathbb{Z} \right),$$

siehe Aufgabe 28.18.

Schließlich seien Ideale $\mathfrak{a}$ und $\mathfrak{a}'$ gegeben mit der Eigenschaft, dass ihre durch die vereinfachte Norm gegebenen quadratischen Formen strikt äquivalent sind. Diese strikte Äquivalenz bedeutet, dass sie durch eine Matrix M mit Determinante 1 miteinander verbunden sind. Es liegt also die Situation

$$\mathfrak{a} \longrightarrow \mathbb{Z}^2 \xrightarrow{M} \mathbb{Z}^2 \longrightarrow \mathfrak{a}'$$

vor. Wir multiplizieren das Ideal $\mathfrak{a}$ mit $N(\mathfrak{a}')$ und das Ideal $\mathfrak{a}'$ mit $N(\mathfrak{a})$. Dann haben beide neuen Ideale die gleiche Norm, die Matrix überträgt sich entsprechend und somit können wir annehmen, dass eine normerhaltende $\mathbb{Z}$-lineare Abbildung

$$\mathfrak{a} \longrightarrow \mathfrak{a}'$$

vorliegt. Diese induziert eine normerhaltende $\mathbb{Q}$-lineare Abbildung

$$\mathbb{Q}[\sqrt{D}] \longrightarrow \mathbb{Q}[\sqrt{D}].$$

Nach Aufgabe 28.19 ist dies die Multiplikation mit einem Element h des Körpers $\mathbb{Q}[\sqrt{D}]$ (die Determinantenbedingung schließt die Konjugation aus). Es ist also

$$\mathfrak{a}' = (h)\mathfrak{a}.$$

Da jedes Ideal positive ganze Zahlen enthält, muss der Faktor h (wie zuvor die Idealnormen) eine positive Norm besitzen. □

Die Konjugation auf R führt ein Ideal $\mathfrak{a}$ in das konjugierte Ideal $\overline{\mathfrak{a}}$ über. Dabei wird die Norm der Elemente und auch die vereinfachte Norm nicht geändert. Die resultierenden quadratischen Formen sind also äquivalent, im Allgemeinen aber nicht strikt äquivalent, da die Determinante der Konjugation gleich -1 ist. Die beiden Ideale müssen aber nicht äquivalent sein.

28. Arbeitsblatt

Übungsaufgaben

Aufgabe 28.1. Zeige, dass eine ganzzahlige 2×2-Matrix M genau dann (als ganzzahlige Matrix) invertierbar ist, wenn ihre Determinante gleich 1 oder -1 ist.

Aufgabe 28.2. Ergänze die Matrix

$$\begin{pmatrix} 7 & 11 \\ & \end{pmatrix}$$

zu einer ganzzahligen Matrix mit Determinante 1.

Aufgabe 28.3. Zeige, dass für die Diskriminante $\triangle$ einer binären quadratischen Form

$$\triangle = 0, 1 \mod 4$$

gilt, und dass diese beiden Möglichkeiten durch die sogenannten *Hauptformen* $X^2 - \frac{\triangle}{4}Y^2$ bzw. $X^2 + XY - \frac{\triangle - 1}{4}Y^2$ realisiert werden.

Aufgabe 28.4. Es sei F eine einfache binäre quadratische Form. Zeige, dass die von der Menge der durch F darstellbaren Zahlen erzeugte Untergruppe gleich $\mathbb{Z}$ ist.

Aufgabe 28.5. Es sei $F = aX^2 + bXY + cY^2$ eine binäre quadratische Form und F' die mittels der Matrix $M = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ transformierte Form $F' = FM$. Zeige, dass für die Koeffizienten die Beziehung

$$\begin{pmatrix} a' & \frac{1}{2}b' \\ \frac{1}{2}b' & c' \end{pmatrix} = \begin{pmatrix} r & t \\ s & u \end{pmatrix} \begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix} \begin{pmatrix} r & s \\ t & u \end{pmatrix}$$

besteht.

Aufgabe 28.6. Es sei $F = aX^2 + bXY + cY^2$ eine binäre quadratische Form und F' die mittels der Matrix $M = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ transformierte Form $F' = FM$. Zeige, dass für die Koeffizienten die Beziehung

$$\begin{pmatrix} b' & 2c' \\ 2a' & b' \end{pmatrix} = \begin{pmatrix} u & s \\ t & r \end{pmatrix} \begin{pmatrix} b & 2c \\ 2a & b \end{pmatrix} \begin{pmatrix} r & s \\ t & u \end{pmatrix}$$

besteht.

Aufgabe 28.7. Zeige, dass die Eigenschaft einer binären quadratischen Form, einfach zu sein, nur von der Äquivalenzklasse der Form abhängt.

Aufgabe 28.8. Zeige, dass man mit der binären quadratischen Form

$$x^2 - 10y^2$$

weder die Zahl 2 noch die Zahl -2 darstellen kann.

Unter einer homogenen Linearform versteht man einen Ausdruck der Form $rX + sY$.

Aufgabe 28.9. Zeige, dass eine binäre quadratische Form $aX^2+bXY+cY^2$ mit $a, b, c \in \mathbb{Z}$ über $\mathbb{C}$ in (homogene) Linearfaktoren zerfällt.

Aufgabe 28.10. Es sei $aX^2 + bXY + cY^2$ eine binäre quadratische Form mit $a, b, c \in \mathbb{Z}$. Charakterisiere mit Hilfe der Diskriminante, ob diese Form über $\mathbb{R}$ in (homogene) Linearfaktoren zerfällt.

Bei $a = 0$ oder $c = 0$ ist die Diskriminante gleich b^2, also ein Quadrat, und die Form zerfällt in $Y(bX + cY)$. Ein ähnliches Verhalten tritt stets aus, wenn die Diskriminante eine Quadratzahl ist. Dieser Fall ist vergleichsweise einfach und hat keine Entsprechung in den quadratischen Zahlbereichen.

Aufgabe 28.11. Es sei $aX^2 + bXY + cY^2$ eine binäre quadratische Form mit $a, b, c \in \mathbb{Z}$. Zeige, dass die Diskriminante genau dann eine Quadratzahl ist, wenn diese Form über $\mathbb{Q}$ in (homogene) Linearfaktoren zerfällt.

Aufgabe 28.12. Zeige, dass eine binäre quadratische Form $aX^2+bXY+cY^2$ mit einer quadratfreien Diskriminante einfach ist.

Aufgabe 28.13. Zeige, dass eine binäre quadratische Form $aX^2+bXY+cY^2$ eine quadratische Form auf dem $\mathbb{Z}$-Modul $\mathbb{Z}^2$ im Sinne der Definition 28.8 ist.

Aufgabe 28.14. Es sei $Q\colon L \to R$ eine quadratische Form auf dem R-Modul L und $M \subseteq L$ ein R-Untermodul. Zeige, dass die Einschränkung von Q auf M ebenfalls eine quadratische Form ist.

Bei der nächsten Aufgabe denke man an $S = \mathbb{Q}$, $R = \mathbb{Z}$, und bei L an den Quotientenkörper eines quadratischen Zahlbereichs zusammen mit der Norm als quadratischer Form (mit Werten in $\mathbb{Q}$) und bei M an ein gebrochenes Ideal von L.

Aufgabe 28.15. Es sei L ein S-Modul und $Q\colon L \to S$ eine quadratische Form. Es sei $R \subseteq S$ ein Unterring und es sei $M \subseteq L$ ein R-Untermodul mit der Eigenschaft, dass die Werte von M unter Q zu R gehören. Zeige, dass die Einschränkung von Q auf M eine quadratische Form über R ist.

Aufgabe 28.16. Es sei $Q\colon L \to R$ eine quadratische Form auf dem R-Modul L, es sei M ein weiterer R-Modul und es sei

$$\varphi\colon M \longrightarrow L$$

ein R-Modulhomomorphismus. Zeige, dass $Q \circ \varphi$ eine quadratische Form auf M ist.

Aufgabe 28.17. Es sei R ein quadratischer Zahlbereich und es seien $\mathfrak{a}$ und $\mathfrak{b}$ äquivalente Ideale aus R. Zeige, dass dann die zugehörigen vereinfachten Normen als quadratische Formen äquivalent sind.

Aufgabe 28.18. Es sei R ein quadratischer Zahlbereich mit Diskriminante $\triangle$ und sei $aX^2 + bXY + cY^2$ eine binäre quadratische Form zu dieser Diskriminante mit $a < 0$. Zeige wie im Beweis zu Satz 28.13, dass

$$\mathfrak{a} = \sqrt{\triangle} \cdot \left(a\mathbb{Z} + \frac{b - \sqrt{\triangle}}{2}\mathbb{Z} \right)$$

ein Ideal in R ist und die Eigenschaft besitzt, dass die Norm darauf die vorgegebene quadratische Form realisiert.

Aufgabe 28.19. Es sei

$$\mathbb{Q} \subseteq L = \mathbb{Q}[\sqrt{D}]$$

eine quadratische Körpererweiterung und es sei

$$\varphi\colon L \longrightarrow L$$

eine $\mathbb{Q}$-lineare Abbildung, die die Norm erhält. Zeige, dass φ die Multiplikation mit einem Element aus L oder aber die Hintereinanderschaltung der Konjugation mit einer solchen Multiplikation ist.

Aufgaben zum Abgeben

Aufgabe 28.20. (3 Punkte)

Ergänze die Matrix

$$\begin{pmatrix} 7892 & 1551 \\ & \end{pmatrix}$$

zu einer ganzzahligen Matrix mit Determinante 1.

Aufgabe 28.21. (1 Punkt)

Berechne die Diskriminante der binären quadratischen Form

$$49X^2 + 65XY + 73Y^2 .$$

Aufgabe 28.22. (3 Punkte)

Bestimme, ob die binäre quadratische Form

$$1547X^2 + 4199XY + 1003Y^2$$

einfach ist oder nicht.

Aufgabe 28.23. (3 Punkte)

Zeige, dass man mit der binären quadratischen Form

$$2x^2 + 2xy + 3y^2$$

die Zahl 5 nicht darstellen kann.

Abbildungsverzeichnis