Skript zur Vorlesung
Algebraische Zahlentheorie

Matthias Wendt

WS 2011/12

Inhaltsverzeichnis

Kapitel 1

Überblick

Algebraische Zahlentheorie beschäftigt sich mit Eigenschaften ganzer algebraischer Zahlen in Zahlkörpern, also endlichen Erweiterungen von $\mathbb{Q}$. Ganze algebraische Zahlen sind dabei Nullstellen von normierten Polynomen mit ganzzahligen Koeffizienten. Die ganzen algebraischen Zahlen in einem Zahlkörper K bilden einen Unterring, den Ganzheitsring $\mathcal{O}_K$ von K, cf. Kapitel 2. Die Untersuchung der strukturellen Eigenschaften dieser Ringe ist das Kernanliegen der Vorlesung. Insbesondere Zahlringe von quadratischen und zyklotomischen Körpern werden in der Vorlesung zur Illustration der definierten Konzepte immer wiederkehren.

Als erstes kann man die additive Struktur von Ganzheitsringen untersuchen, cf. Kapitel 3. Zahlkörper bilden mit Addition und Skalarmultiplikation einen endlich-dimensionalen Vektorraum über $\mathbb{Q}$. Ganzheitsringe haben eine ähnliche Struktur: sie sind endlich erzeugte freie Moduln über $\mathbb{Z}$. Insbesondere kann man eine Ganzheitsbasis, also eine $\mathbb{Z}$-Basis von $\mathcal{O}_K$, angeben. Außerdem erhält man mit der Diskriminante die erste wichtige Invariante von Zahlkörpern.

Als nächstes untersucht man die multiplikative Struktur. Ganze Zahlen kann man in Primfaktoren zerlegen, und diese Zerlegung ist eindeutig. An diesem Punkt unterscheiden sich Ganzheitsringe von $\mathbb{Z}$. Man muß sich von Zahlen bzw. Elementen lösen, und stattdessen Ideale betrachten, cf. Kapitel 4. Diese Ideale kann man dann eindeutig in Primideale faktorisieren. Außerdem sind Ganzheitsringe nicht mehr notwendig Hauptidealringe, d.h. die Zerlegung in irreduzible Elemente ist nicht eindeutig. Wie weit ein Ganzheitsring davon abweicht, ein Hauptidealring zu sein, wird durch die (Ideal-)Klassengruppe gemessen, cf. Kapitel 6. Ein zentraler Satz der algebraischen Zahlentheorie ist die Endlichkeit der Klassengruppe. Klassengruppen tauchen in den unterschiedlichsten Zusammenhängen auf, und es gibt noch viele ungeklärte Fragen.

Der zweite Teil der Untersuchung zur multiplikativen Struktur ist dann den Einheiten gewidmet, also den in $\mathcal{O}_K$ multiplikativ invertierbaren Elementen, cf. Kapitel 7. In $\mathbb{Z}$ hat man nur ± 1, Ganzheitsringe können aber durchaus unendlich viele Einheiten haben. Der Dirichletsche Einheitensatz gibt eine genaue Beschreibung der Einheitengruppe als Produkt einer zyklischen Gruppe von Einheitswurzeln und einer endlich erzeugten freien abelschen Gruppe, deren Rang von der Anzahl reeller und komplexer Einbettungen abhängt.

Der letzte kanonische Themenblock befaßt sich mit Erweiterungen von Zahlringen, cf. Kapitel 9. Es geht um die Frage nach Gesetzmäßigkeiten, nach denen

sich Primzahlen bzw. Primideale in Körpererweiterungen zerlegen lassen. Ein wichtiger Aspekt dieser Frage ist die Verzweigungstheorie.

Am Schluß wird in Kapitel 10 mit der Theorie der lokalen Körper ein wichtiges Hilfsmittel der Zahlentheorie vorgestellt, das zum Beispiel im Lokal-Global-Prinzip für quadratische Formen eine schöne Anwendung findet.

Es gibt zwei Kapitel über die algorithmische Realisierbarkeit der in der Vorlesung behandelten Konzepte, Kapitel 5 und Kapitel 8.

Die Vorlesung setzt einige Konzepte aus Algebra und kommutativer Algebra voraus. Die entsprechenden Begriffe und Ergebnisse sind in einem Anhang Kapitel A zusammengestellt.

Kapitel 2

Ganze Ringerweiterungen

In diesem Kapitel geht es um die Definitionen der zentralen Begriffe der *ganzen algebraischen Zahl* und des *Ganzheitsrings* eines Zahlkörpers. Das Studium der Struktur der Ganzheitsringe ist das zentrale Anliegen der Vorlesung. Allerdings ist schon für die Tatsache, daß Ganzheitsringe wirklich Ringe sind, ein nicht-trivialer Beweis und der Begriff der *ganzen Ringerweiterung* erforderlich.

Definition 2.1. *Ein (algebraischer)* Zahlkörper *ist ein endlicher Erweiterungskörper K von $\mathbb{Q}$. Elemente von K heißen algebraische Zahlen. Alternativ (nach Einbettung) heißt eine komplexe Zahl $x \in \mathbb{C}$* algebraisch*, wenn $\mathbb{Q}(x)$ ein Zahlkörper ist, also wenn es ein Polynom $f \in \mathbb{Q}[X]$ gibt mit $f(x) = 0$. Eine algebraische Zahl x heißt* ganz*, wenn es ein normiertes Polynom $f \in \mathbb{Z}[X]$ gibt mit $f(x) = 0$.*

Definition 2.2. *Sei K ein Zahlkörper. Wir bezeichnen mit*

$$\mathcal{O}_K = \{x \in K \mid \text{ es gibt } a_1, \ldots, a_n \in \mathbb{Z} : x^n + a_1 x^{n-1} + \cdots + a_n = 0\}$$

die Menge der ganzen algebraischen Zahlen in K.

Definition 2.3. *Sei $A \subseteq B$ eine Ringerweiterung, d.h. ein injektiver Ringhomomorphismus. Ein Element $x \in B$ heißt* ganz über A*, wenn x einer normierten Gleichung genügt, d.h. wenn es $a_1, \ldots, a_n \in A$ gibt mit $x^n + a_1 x^{n-1} + \cdots + a_n = 0$. Die Menge*

$$\{x \in B \mid \text{ es gibt } a_1, \ldots, a_n \in A : x^n + a_1 x^{n-1} + \cdots + a_n = 0\}$$

heißt ganzer Abschluß *von A in B. Die Ringerweiterung $A \subseteq B$ heißt* ganze Ringerweiterung*, wenn alle Elemente von B ganz über A sind.*

Insbesondere ist $\mathcal{O}_K$ der ganze Abschluß von $\mathbb{Z}$ in der Ringerweiterung $\mathbb{Z} \subseteq \mathbb{Q} \subseteq K$. Es ist nicht offensichtlich, daß $\mathcal{O}_K$ ein Ring ist, oder daß allgemeiner der ganze Abschluß eines Rings wieder ein Ring ist. Das soll im Folgenden bewiesen werden; das entscheidende Hilfsmittel ist der folgende Satz, der im Spezialfall von Körpererweiterungen aus der Algebra bekannt ist.

Satz 2.4. *Sei $A \subseteq R$ eine Ringerweiterung, $x \in R$. Die folgenden Aussagen sind äquivalent:*

(i) x *ist ganz über* A*.*

(ii) Der Unterring

$$A[x] = \left\{ \sum_{i=0}^{n} a_i x^i \mid n \in \mathbb{N}, a_i \in A \right\} \subseteq R$$

ist ein endlich erzeugter A*-Modul.*

(iii) Es gibt einen Teilring $B \subseteq R$*, der* $A[x]$ *enthält und als* A*-Modul endlich erzeugt ist.*

Beweis. (i) $\Rightarrow$ (ii): Nach Voraussetzung ist $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ für geeignete $a_1, \ldots, a_n \in A$. Mit der resultierenden Gleichung

$$x^n = -(a_1 x^{n-1} + \cdots + a_n)$$

kann man x^m für beliebige $m \in \mathbb{N}$ als Linearkombination von $1, x, \ldots, x^{n-1}$ ausdrücken. Also ist $A[x]$ als A-Untermodul von R durch die endliche Menge $1, x, \ldots, x^{n-1}$ erzeugt. Insbesondere ist $A[x]$ auch ein Unterring.

(ii) $\Rightarrow$ (iii): $B = A[x]$ erfüllt die Bedingungen.

(iii) $\Rightarrow$ (i): Sei $y_1, \ldots, y_n$ ein Erzeugendensystem von B als A-Modul. Nach Voraussetzung ist B ein Ring, also ist $xy_i \in B$, also

$$xy_i = \sum_{j=1}^{n} a_{ij} y_j$$

für alle $i = 1, \ldots, n$. Die y_i sind damit Lösungen des linearen Gleichungssystems

$$\sum_{j=1}^{n} (\delta_{ij} x - a_{ij}) Y_j = 0, \quad i = 1, \ldots, n.$$

Sei d die Determinante der Koeffizientenmatrix, also das charakteristische Polynom der Matrix (a_{ij}). Nach Lemma A.7 gilt $dy_i = 0$ für $i = 1, \ldots, n$. Da die y_i den Modul B erzeugen ist $d \cdot 1 = 0$, da 1 eine Linearkombination von y_i ist. Die Ganzheitsgleichung für x ist dann die Gleichung $d = \det(\delta_{ij} x - a_{ij}) = 0$. □

Korollar 2.5. *Seien* $A \subseteq B$ *und* $B \subseteq C$ *ganze Ringerweiterungen. Dann ist* $A \subseteq C$ *eine ganze Ringerweiterung.*

Beweis. Sei $x \in C$. Nach Voraussetzung ist x ganz über B, erfüllt also eine Gleichung

$$x^n + b_1 x^{n-1} + \cdots + b_n = 0, \quad b_i \in B.$$

Da B ganz über A ist, sind $A[b_i]$ endlich erzeugte A-Moduln für $i = 1, \ldots, n$. Induktiv ist $A[x, b_1, \ldots, b_n]$ endlich erzeugter A-Modul. Mit Satz 2.4 und $x \in A[x, b_1, \ldots, b_n]$ folgt x ganz über A. □

Definition 2.6. *Sei* $A \subseteq B$ *eine Ringerweiterung. Dann heißt* A ganz-abgeschlossen in B *wenn* A *gleich seinem ganzen Abschluß in der Ringerweiterung* $A \subseteq B$ *ist.*

Wenn A *ein Integritätsbereich mit Quotientenkörper* K *ist, dann heißt* A ganz-abgeschlossen*, wenn* A *ganz-abgeschlossen in* K *ist.*

Satz 2.7. *Sei $A \subseteq B$ eine Ringerweiterung. Der ganze Abschluß von A in B ist wieder ein Ring. Dieser Ring ist ganz-abgeschlossen in B und ganz über A.*

Beweis. Der ganze Abschluß enthält offensichtlich A, ist also eine ganze Ringerweiterung von A.

Wenn $x, y \in B$ ganz sind, ist nach Satz 2.4 der Unterring $A[x, y]$ ein endlich erzeugter A-Modul. Dieser enthält $x+y$, $x-y$ und xy, also sind diese Elemente wieder ganz über B.

Aus Korollar 2.5 folgt, daß der ganze Abschluß ganz-abgeschlossen ist. □

Korollar 2.8. *Sei K ein Zahlkörper. Die Menge $\mathcal{O}_K$ der ganzen algebraischen Zahlen in K ist ein Ring, der* Ganzheitsring von K. *Ganzheitsringe von Zahlkörpern sind ganz-abgeschlossen.*

Übungsaufgaben

Übungsaufgabe 2.1. *Geben Sie eine Basis des $\mathbb{Q}$-Vektorraums $\mathbb{Q}(\sqrt{1+i})$ an. Wie sieht in dieser Basis die darstellende Matrix für die Multiplikation mit $\sqrt{1+i}$ aus?*

Übungsaufgabe 2.2. *Bestimmen Sie die Galoisgruppe der Gleichung $X^4 = 2$.*

Übungsaufgabe 2.3. *Ist die Körpererweiterung $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ normal?*

Übungsaufgabe 2.4. *Zeigen Sie mit Hilfe des Eisenstein-Kriteriums, daß für eine Primzahl p das p-te zyklotomische Polynom*

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$$

irreduzibel über $\mathbb{Z}$ ist.

Übungsaufgabe 2.5. *Sind die folgenden Zahlen ganz über $\mathbb{Z}$?*

$$\frac{\sqrt[3]{2}}{3} \qquad \frac{3+2\sqrt{6}}{1-\sqrt{6}} \qquad \frac{-19+4\sqrt{-5}}{21} \qquad \frac{3+2\zeta_3}{1+\zeta_3} \qquad \frac{\sqrt[3]{3}+2\sqrt[3]{9}}{3}$$

Dabei ist ζ_3 eine primitive dritte Einheitswurzel.

Übungsaufgabe 2.6. *Sei B ein Integritätsbereich, $A \subseteq B$ eine ganze Ringerweiterung. Dann ist B ein Körper genau dann, wenn A ein Körper ist.*

Übungsaufgabe 2.7. *Ist der Ring $\mathbb{Z}[X]/(X^2+4)$ ganz-abgeschlossen?*

Übungsaufgabe 2.8. *Sei k ein Körper. Ist der Ring $k[X,Y]/(Y^2 - X^2(X+1))$ ganz-abgeschlossen?*

Übungsaufgabe 2.9. *Sei R ein Ring, G eine endliche Gruppe von Ringautomorphismen von R. Bezeichne*

$$R^G = \{x \in R \mid \sigma(x) = x \text{ für alle } \sigma \in G\}$$

den Unterring der G-Invarianten von R. Zeigen Sie, daß R ganz über R^G ist.

Hinweis: *Betrachten Sie für $x \in R$ das Polynom*

$$p(t) = \prod_{\sigma \in G} (X - \sigma(x)).$$

Übungsaufgabe 2.10. *Sei A ein ganz-abgeschlossener Integritätsbereich mit Quotientenkörper K. Sei B der ganze Abschluß von A in einer endlichen Erweiterung L/K. Dann läßt sich jedes Element von L als Quotient b/a mit $b \in B$ und $a \in A, a \neq 0$ schreiben.*

Übungsaufgabe 2.11. *Faktorielle Ringe sind ganz-abgeschlossen.*

Kapitel 3

Ganzheitsbasis und Diskriminante

In diesem Kapitel geht es um die additive Struktur von Ganzheitsringen. Die additive Gruppe eines Ganzheitsrings ist eine endlich erzeugte freie abelsche Gruppe. Das wichtigste Hilfsmittel für den Beweis ist die *Spurpaarung*, aus ihr ergibt sich die *Diskriminante* des Zahlkörpers. Wir bestimmen explizit die Ganzheitsringe *quadratischer* und *zyklotomischer* Zahlkörper.

Zuerst wollen wir die Struktur der additiven Gruppe von Ganzheitsringen $\mathcal{O}_K$ studieren. Für Körper ist dies der Satz vom primitiven Element.

Satz 3.1. *Sei L/K eine endliche separable Körpererweiterung. Dann existiert ein Element $x \in L$, so daß $L = K(x)$ ist. Insbesondere ist also $1, x, \ldots, x^{[L:K]-1}$ eine Basis des K-Vektorraums L.*

Dieser Satz gilt, wie wir später sehen werden, nicht für Zahlringe. Es gilt aber der folgende Satz.

Satz 3.2. *Sei $K/\mathbb{Q}$ ein Zahlkörper, $\mathcal{O}_K$ der Ganzheitsring. Dann gilt $\mathcal{O}_K \cong \mathbb{Z}^{[K:\mathbb{Q}]}$, d.h. $\mathcal{O}_K$ ist eine freie abelsche Gruppe vom Rang $[K : \mathbb{Q}]$.*

Die Isomorphie im Satz ist eine Isomorphie von abelschen Gruppen bzw. $\mathbb{Z}$-Moduln, nicht von Ringen! Außerdem ist wichtig, daß als Grundring hier der Hauptidealring $\mathbb{Z}$ benutzt wird. Wir werden später sehen, daß für eine Erweiterung L/K die Erweiterung der Ganzheitsringe $\mathcal{O}_L/\mathcal{O}_K$ nicht notwendigerweise frei als $\mathcal{O}_K$-Modul ist. Es gibt also mehrere Gründe, warum der Satz vom primitiven Element für Zahlringe nicht gilt.

3.1 Beispiel 1: Quadratische Zahlkörper

Wir betrachten zunächst das einfachste Beispiel, quadratische Zahlkörper. Das sind Zahlkörper der Form $\mathbb{Q}(\sqrt{d})$ für $d \in \mathbb{Z}$ quadratfrei. Diese Körper sind Galoiserweiterungen von $\mathbb{Q}$ mit Galoisgruppe $\mathbb{Z}/2\mathbb{Z}$. Das nichttriviale Element σ von $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$ wirkt durch "Konjugation":

$$\sigma : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d}) : a + b\sqrt{d} \mapsto a - b\sqrt{d}.$$

Satz 3.3. *Sei d eine quadratfreie Zahl, $K = \mathbb{Q}(\sqrt{d})$ der dazugehörige quadratische Zahlkörper. Dann gilt:*

(i) Für $d \equiv 2, 3 \mod 4$ ist $\mathcal{O}_K = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$.

(ii) Für $d \equiv 1 \mod 4$ ist

$$\mathcal{O}_K = \left\{ \frac{u + v\sqrt{d}}{2} \mid u, v \in \mathbb{Z}, u \equiv v \mod 2 \right\}.$$

Beweis. Wir bezeichnen mit σ das nichttriviale Element von $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$. Sei $\alpha = a + b\sqrt{d}$, $a, b \in \mathbb{Q}$ eine ganze algebraische Zahl, Nullstelle des normierten Polynoms $P(X)$. Dann ist wegen $P(\sigma(\alpha)) = \sigma(P(\alpha)) = 0$ auch $\sigma(\alpha) = a - b\sqrt{d}$ ganz. Damit ist

$$Q(X) = (X - \alpha)(X - \sigma(\alpha)) = X^2 - (a + b\sqrt{d} + a - b\sqrt{d})X + (a + b\sqrt{d})(a - b\sqrt{d})$$

$$= X^2 - 2aX + a^2 - b^2 d \in \mathbb{Q}[X]$$

ein Teiler von $P(X)$. Nach dem Gauß-Lemma ist $Q(X) \in \mathbb{Z}[X]$, wir erhalten also die Bedingungen

$$2a \in \mathbb{Z}, a^2 - b^2 d \in \mathbb{Z}.$$

Aus diesen Bedingungen folgt $(2a)^2 - (2b)^2 d \in \mathbb{Z}$, und dann $(2b)^2 d \in \mathbb{Z}$. Mit d quadratfrei ist also auch $2b \in \mathbb{Z}$. Sei nun

$$a = \frac{u}{2}, b = \frac{v}{2}, u, v \in \mathbb{Z}, \text{ dann ist}$$

$$\left(\frac{u}{2}\right)^2 - \left(\frac{v}{2}\right)^2 d = \frac{u^2 - v^2 d}{4} \in \mathbb{Z}.$$

Nun rechnen wir in Restklassen modulo 4. Die Quadrate u^2 und v^2 sind notwendigerweise 0 oder 1 modulo 4. Eine explizite Fallunterscheidung liefert die Behauptung. □

Übungsaufgabe 3.1. *Sei d quadratfrei, $K = \mathbb{Q}(\sqrt{d})$ der dazugehörige quadratische Zahlkörper. Dann ist $\mathcal{O}_K$ eine freie abelsche Gruppe vom Rang 2.*

(i) Für $d \equiv 2, 3 \mod 4$ ist $\{1, \sqrt{d}\}$ eine Basis von $\mathcal{O}_K$.

(ii) Für $d \equiv 1 \mod 4$ ist $\{1, \frac{1+\sqrt{d}}{2}\}$ eine Basis von $\mathcal{O}_K$.

3.2 Spurpaarung und Diskriminante

Im Beispiel spielte das Minimalpolynom des Elementes α eine wichtige Rolle. Unangenehm speziell sind die Teilbarkeitsargumente.

Für eine endliche, separable Körpererweiterung L/K und ein Element $\alpha \in L$ ist das Minimalpolynom $\mathrm{Min}(\alpha)$ das normierte Polynom minimalen Grades mit Nullstelle α.

Lemma 3.4. *Sei L/K endlich, separabel, und sei $\alpha \in L$. Bezeichne*

$$m_\alpha : K(\alpha) \to K(\alpha) : x \mapsto \alpha x$$

die Multiplikation mit α. Dann ist

$$\mathrm{Min}(\alpha) = \det(X\,\mathrm{id} - m_\alpha).$$

Beweis. Das charakteristische Polynom hat den Grad $[K(\alpha) : K]$, ist normiert und hat nach Cayley-Hamilton α als Nullstelle. □

Definition 3.5. *Sei L/K eine endliche Körpererweiterung, $\alpha \in L$. Das charakteristische Polynom von α ist*

$$P_\alpha(X) = \det(X\,\mathrm{id} - m_\alpha),$$

wobei $m_\alpha : L \to L$ die Multiplikationsabbildung ist. Die Norm von α ist

$$N_{L/K}(\alpha) = \det(m_\alpha),$$

die Spur von α ist

$$\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}(m_\alpha).$$

Es gilt $P_\alpha(X) = X^{[L:K]} - \mathrm{Tr}(\alpha)X^{[L:K]-1} + \cdots + (-1)^{[L:K]}N_{L/K}(\alpha)$.

Beispiel 3.6. *Sei d quadratfrei, wir wählen für $\mathbb{Q}(\sqrt{d})$ die Basis $1, \sqrt{d}$. Dann ist die darstellende Matrix für die Multiplikation mit $\alpha = a + b\sqrt{d}$, $a, b \in \mathbb{Q}$, gegeben durch*

$$\begin{pmatrix} a & bd \\ b & a \end{pmatrix}.$$

Dann ist

$$P_\alpha(X) = X^2 - 2aX + a^2 - b^2 d,\ \mathrm{Tr}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(\alpha) = 2a,\ N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(\alpha) = a^2 - b^2 d.$$

□

Übungsaufgabe 3.2. *Sei K ein Zahlkörper, $\alpha \in \mathcal{O}_K$. Dann ist $\alpha \in \mathcal{O}_K^\times$ genau dann, wenn $N_{L/K}(\alpha) = \pm 1$ ist.*

Lemma 3.7. *Sei L/K eine separable Körpererweiterung vom Grad $d = [L : K]$, und $\alpha \in L$ ein Element. Seien $\sigma_1, \ldots, \sigma_d : L \to \overline{K}$ die K-Einbettungen von L in einen gewählten algebraischen Abschluß $\overline{K}$ von K. Dann gilt*

(i) $P_\alpha(X) = \mathrm{Min}(\alpha)^{[L:K(\alpha)]} = \prod_{i=1}^d (X - \sigma_i(\alpha))$,

(ii) $\mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^d \sigma_i(\alpha)$,

(iii) $N_{L/K}(\alpha) = \prod_{i=1}^d \sigma_i(\alpha)$.

Bemerkung 3.8. *Die Elemente $\sigma_i(\alpha)$, $i = 1, \ldots, d$, sind genau die (verschiedenen) Nullstellen von* $\mathrm{Min}(\alpha)$*, jeweils $[L : K(\alpha)]$-mal.*

Beweis. Zuerst überzeugen wir uns von der Gleichheit $P_\alpha(X) = \mathrm{Min}(\alpha)^{[L:K(\alpha)]}$. Wir wählen $1, \alpha, \ldots, \alpha^{m-1}$, $m = [K(\alpha) : K] = \deg \mathrm{Min}(\alpha)$, als Basis von $K(\alpha)$. Für $n = d/m = [L : K(\alpha)]$ sei $y_1, \ldots, y_n$ eine Basis von $L/K(\alpha)$. Dann ist

$$y_1, y_1\alpha, \ldots, y_1\alpha^{m-1}; \ldots; y_n, y_n\alpha, \ldots, y_n\alpha^{m-1}$$

eine Basis von L/K. Die darstellende Matrix zur Multiplikation mit α in L hat in dieser Basis Blockdiagonalform, die einzelnen Blöcke sind immer darstellende Matrizen für Multiplikation mit α in $K(\alpha)$, also folgt $P_\alpha(X) = \mathrm{Min}(\alpha)^{[L:K(\alpha)]}$.

Der zweite Teil von (i) folgt induktiv aus dem ersten Teil, Lemma 3.4 und dem Vietaschen Wurzelsatz. Aussagen (ii) und (iii) folgen dann aus (i). □

Korollar 3.9. *Sei A ein ganz-abgeschlossener Integritätsbereich mit Quotientenkörper K, sei L/K eine endliche separable Körpererweiterung und B der ganze Abschluß von A in L. Für jedes $\alpha \in B$ ist $P_\alpha(X) \in A[X]$. Insbesondere sind Norm und Spur von ganzen Elementen wieder ganz.*

Beweis. Wir übernehmen die Bezeichnungen aus Lemma 3.7. Wenn α die Gleichung $X^n + a_1X^{n-1} + \cdots + a_n = 0$, $a_j \in A$ erfüllt, dann erfüllt jedes $\sigma_i(\alpha)$ diese Gleichung: die Operation der Galoisgruppe des Zerfällungskörpers vertauscht die $\sigma_i(\alpha)$, ist ein Homomorphismus, und läßt die Koeffizienten der Gleichung invariant. Mit $P_\alpha(X) = \prod(X - \sigma_i(\alpha))$ und Satz 2.7 sind die Koeffizienten von $P_\alpha(X)$ ganz über A, und liegen gleichzeitig in K. Da A ganz-abgeschlossen ist, sind die Koeffizienten in A. □

Definition 3.10. *Sei L/K eine endliche separable Körpererweiterung vom Grade $n = [L : K]$. Die* Spurpaarung *ist die symmetrische bilineare Abbildung*

$$\langle -, - \rangle : L \times L \to K : (x, y) \mapsto \mathrm{Tr}_{L/K}(xy).$$

Für eine Basis $x_1, \ldots, x_n$ von L heißt

$$D(x_1, \ldots, x_n) = \det(\mathrm{Tr}(x_i x_j))$$

Diskriminante der Basis $x_1, \ldots, x_n$.

Bemerkung 3.11. *Offensichtlich folgt aus Korollar 3.9, daß man die Spurpaarung und Diskriminante auch in der folgenden allgemeineren Situation definieren kann: A ist ein ganz-abgeschlossener Integritätsbereich, $A \subseteq B$ ist eine Ringerweiterung, wobei B ein freier A-Modul vom Rang n ist.*

Beispiel 3.12. *Sei $L = K[X]/(X^2 + pX + q)$, wir wählen als Basis $1, X$. Wir haben die folgenden darstellenden Matrizen:*

$$m_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad m_X = \begin{pmatrix} 0 & -q \\ 1 & -p \end{pmatrix}, \quad m_{X^2} = m_X^2 = \begin{pmatrix} -q & pq \\ -p & p^2 - q \end{pmatrix}.$$

Damit haben wir

$$D(1, X) = \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(X) \\ \mathrm{Tr}(X) & \mathrm{Tr}(X^2) \end{pmatrix} = \det \begin{pmatrix} 2 & -p \\ -p & p^2 - 2q \end{pmatrix} = p^2 - 4q.$$

Dies ist die bekannte Diskriminante der quadratischen Gleichung. □

Übungsaufgabe 3.3. *Sei $K(\theta)/K$ eine endliche separable Körpererweiterung, und seien $\sigma_1, \ldots, \sigma_n : K(\theta) \to \overline{K}$ die verschiedenen K-Einbettungen von $K(\theta)$ in einen gewählten algebraischen Abschluß $\overline{K}$ von K. Zeigen Sie*

$$D(1, \theta, \ldots, \theta^{n-1}) = \prod_{i<j} (\sigma_i(\theta) - \sigma_j(\theta))^2 .$$

Hinweis: *Determinanten-Formel für Vandermonde-Matrizen.*

Man sieht dieser Berechnung der Diskriminante an, daß für eine separable Körpererweiterung $K(\theta)/K$ immer $D(1, \theta, \ldots, \theta^{n-1}) \neq 0$ gilt, da $\sigma_i(\theta) - \sigma_j(\theta) \neq 0$ für alle $i \neq j$.

Proposition 3.13. *Sei $K(x)/K$ eine separable Körpererweiterung, und $f(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in K[X]$ das Minimalpolynom von x. Dann ist*

$$D(1, x, \ldots, x^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{K(x)/K}(f'(x)),$$

wobei $f'(X)$ die Ableitung von $f(X)$ ist.

Beweis. Wir bezeichnen mit $\sigma_1, \ldots, \sigma_n$ die verschiedenen K-Einbettungen von $K(x)$ in einen gewählten algebraischen Abschluß $\overline{K}$. Aus der Produktregel folgt

$$f'(X) = \left(\prod_i (X - \sigma_i(x)) \right)' = \sum_i \prod_{j \neq i} (X - \sigma_j(x)),$$

insbesondere $f'(\sigma_i(x)) = \prod_{j \neq i} (\sigma_i(x) - \sigma_j(x))$.

Mit Übungsaufgabe 3.3 folgt nun

$$\begin{aligned} D(1, x, \ldots, x^{n-1}) &= \prod_{i<j} (\sigma_i(x) - \sigma_j(x))^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} (\sigma_i(x) - \sigma_j(x)) \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_i \left(\prod_{j \neq i} (\sigma_i(x) - \sigma_j(x)) \right) \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_i f'(\sigma_i(x)) = (-1)^{\frac{n(n-1)}{2}} N_{K(x)/K}(f'(x)). \end{aligned}$$

□

Proposition 3.14. *Sei A ein ganz-abgeschlossener Integritätsbereich mit Quotientenkörper K, L/K eine endliche separable Erweiterung vom Grade $n = [L : K]$, und sei B der ganze Abschluß von A in L. Dann existieren freie A-Moduln M und M' vom Rang n, so daß $M' \subseteq B \subseteq M$. Genauer erfüllen für ein Element $x \in B$ mit $L = K(x)$ und $d = D(1, x, \ldots, x^{n-1})$ die folgenden Moduln die Behauptung:*

$$M' = A[x], \qquad M = (1/d)A[x].$$

Beweis. Sei x' ein primitives Element von L/K. Nach Übungsaufgabe 2.10 ist $x' = x/a$, $x \in B$, $a \in A$. So finden wir ein $x \in B$ mit $L = K(x)$, insbesondere ist $1, x, \ldots, x^{n-1}$ eine K-Basis von L. Damit ist $M' = A[x]$ ein freier Untermodul von B vom Rang n.

Mit Übungsaufgabe 3.3 folgt aus der Separabilität von L/K für die Diskriminante $D(1, x, \ldots, x^{n-1}) \neq 0$.

Ein Element $y \in B$ kann als

$$y = \sum_{j=0}^{n-1} c_j x^j = \sum_{j=0}^{n-1} dc_j \left(\frac{x^j}{d}\right), c_j \in K$$

geschrieben werden. Es ist zu zeigen, daß $dc_j \in B$, also dc_j ganz über A. In der normalen Hülle L' von L/K können wir dann die zu y bzw. x konjugierten Elemente $y_1, \ldots, y_n$ bzw. $x_1, \ldots, x_n$ betrachten. Mit der richtigen Indexwahl gilt $y_i = \sum_{j=0}^{n-1} c_j x_i^j$. Die c_j sind also Lösungen des linearen Gleichungssystems

$$\sum_{j=0}^{n-1} x_i^j X_j = y_i, i = 1, \ldots, n,$$

Nach der Cramerschen Regel Lemma A.7 ist $\det(x_i^j)c_j = e_j$, wobei e_j die Determinante der Matrix ist, die aus (x_i^j) durch Ersetzung der j-ten Spalte durch $(y_1, \ldots, y_n)$ hervorgeht. Da x_i^j und y_i ganz über A sind, sind auch $\det(x_i^j)$ und e_j ganz. Aus Übungsaufgabe 3.3 ist aber

$$d = D(1, x, \ldots, x^{n-1}) = \prod_{i<j} (x_i - x_j)^2 = \det(x_i^j)^2.$$

Also ist $dc_j = \det(x_i^j)e_j$ ganz über A, und die Behauptung ist bewiesen. □

Bemerkung 3.15. *Eine Bilineare-Algebra-Interpretation des Beweises: Der Modul M ergibt sich aus dem Modul M' durch Übergang zur bzgl. der Spurpaarung dualen Basis. Dafür ist notwendig, daß die Spurpaarung nicht-ausgeartet ist.*

3.3 Noethersche Ringe

Wir wissen nun, daß der ganze Abschluß ein Untermodul eines freien Moduls von endlichem Rang ist. Als nächstes wollen wir zeigen, daß der ganze Abschluß von A ein endlich erzeugter A-Modul ist. Für beliebige Ringe ist das falsch, deswegen betrachtet man noethersche Ringe.

Bemerkung 3.16. *Bei Vektorräumen ist der Rang gleich der Dimension, und für eine Inklusion von Vektorräumen $V \subseteq W$ gilt $\dim V \leq \dim W$. Bei Ringen ist das nicht mehr richtig. Ein Beispiel hierfür ist der Polynomring $k[x, y]$. Das Ideal (x, y) ist ein $k[x, y]$-Modul vom Rang 2. Der Ring $k[x, y]$ selbst hat aber Rang 1.*

Proposition 3.17. *Sei R ein Ring, M ein R-Modul. Dann sind die folgenden Aussagen äquivalent.*

(i) Jeder R-Untermodul von M ist endlich erzeugt.

(ii) Jede aufsteigende Kette von R-Untermoduln

$$N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots$$

stabilisiert, d.h. es gibt ein $i \in \mathbb{N}$ so daß für alle $j \geq i$ gilt $N_i = N_j$.

(iii) Jede nichtleere Familie von R-Untermoduln von M hat ein maximales Element bezüglich Inklusion.

Beweis. (i) $\Rightarrow$ (ii): Wir betrachten den Untermodul $N = \bigcup_i N_i \subseteq M$. Nach Voraussetzung ist $N = (x_1, \ldots, x_n)$ endlich erzeugt. Dann existiert ein i mit $x_1, \ldots, x_n \in N_i$, also $N \subseteq N_i$. Damit ist die Behauptung bewiesen.

(ii) $\Rightarrow$ (iii): Sei $\mathcal{N}$ eine nichtleere Familie von R-Untermoduln von M. Wenn $N_1 \in \mathcal{N}$ nicht schon maximal ist, existiert $N_2 \in \mathcal{N}$ mit $N_1 \subseteq N_2$. Dieses Verfahren kann man fortsetzen, es bricht nach Voraussetzung nach endlich vielen Schritten ab, und liefert ein maximales Element N_i.

(iii) $\Rightarrow$ (i): Sei $N \subseteq M$ ein Untermodul, der nicht endlich erzeugt ist. Wir betrachten die Familie $\mathcal{M}$ der endlich erzeugten Untermoduln von M, die außerdem in N enthalten sind. Wegen $0 \in \mathcal{M}$ ist die Familie nicht leer. Nach Voraussetzung existiert ein maximales Element $N' \subsetneq N$. Für ein Element $x \in N \setminus N'$ ist $N' + xR$ immer noch endlich erzeugt und in N enthalten. Dies ist ein Widerspruch zur Maximalität von N'. □

Definition 3.18. *Sei R ein Ring. Ein R-Modul M heißt* noethersch*, wenn M die äquivalenten Bedingungen von Proposition 3.17 erfüllt sind. Der Ring R heißt* noethersch*, wenn R als R-Modul noethersch ist.*

Proposition 3.19. *Sei R ein Ring, und sei $0 \to M_1 \to M_2 \to M_3 \to 0$ eine exakte Sequenz von R-Moduln. Dann ist M_2 noethersch genau dann, wenn M_1 und M_3 noethersch sind.*

Beweis. Sei M_2 noethersch. Jeder R-Untermodul $N \subseteq M_1 \subseteq M_2$ ist nach Voraussetzung endlich erzeugt, also ist M_1 noethersch. Es gibt eine inklusionserhaltende Bijektion zwischen den R-Untermoduln von M_3 und den R-Untermoduln von M_2, die M_1 enthalten. Mit Teil (ii) von Proposition 3.17 sieht man, daß M_3 auch noethersch ist.

Nun nehmen wir an, daß M_1 und M_3 noethersch sind. Sei $N \subseteq M_2$ ein Untermodul. Wir bezeichnen die Abbildung $M_2 \to M_3$ mit π. Dann ist nach Voraussetzung $\pi(N) \subseteq M_3$ endlich erzeugt. Wir wählen Urbilder $x_1, \ldots, x_n$ dieser Erzeuger in N. Für ein beliebiges Element $y \in N$ kann man dann

$$\pi(y) = \sum_{i=1}^{n} a_i \pi(x_i), a_i \in R$$

schreiben. Es folgt

$$y - \sum_{i=1}^{n} a_i x_i \in N \cap M_1.$$

Der Modul $N \cap M_1$ ist nach Voraussetzung endlich erzeugt. Man sieht, daß die $x_1, \ldots, x_n$ und die Erzeuger von $N \cap M_1$ zusammen den Modul N erzeugen. □

Übungsaufgabe 3.4. *Sei R ein noetherscher Ring, M ein endlich erzeugter R-Modul. Dann ist M noethersch.*

Korollar 3.20. *Sei A ein noetherscher Integritätsbereich mit Quotientenkörper K, und L/K eine endliche separable Körpererweiterung. Dann ist der ganze Abschluß B von A in L als A-Modul endlich erzeugt und ein noetherscher Ring. Insbesondere ist für jeden Zahlkörper K der Ganzheitsring $\mathcal{O}_K$ ein noetherscher Ring und endlich erzeugter $\mathbb{Z}$-Modul.*

Die Allgemeinheit hier hat ihren Grund. Noethersche Ringe spielen eine grundlegende Rolle in der algebraischen Geometrie und Zahlentheorie. In der algebraischen Geometrie ist das obige Korollar die Auflösung von Singularitäten in Kodimension 1. In der Zahlentheorie hat dieser Satz auch Konsequenzen für relative Erweiterungen von Zahlkörpern L/K: der Ganzheitsring $\mathcal{O}_L$ ist nach dem obigen Satz als $\mathcal{O}_K$-Modul endlich erzeugt.

3.4 Ganzheitsbasis

Wir haben zum Beweis von Satz 3.2 schon den wichtigsten Schritt getan. Wir wissen, daß $\mathcal{O}_K$ ein endlich erzeugter $\mathbb{Z}$-Modul ist. Der Satz ist nun eine Konsequenz aus der Theorie der Moduln über Hauptidealringen, cf. Kapitel A.

Beweis von Satz 3.2: Der Ganzheitsring $\mathcal{O}_K$ ist ein $\mathbb{Z}$-Untermodul von K, also torsionsfrei. Die Behauptung des Satzes ergibt sich aus Korollar 3.20 und Korollar A.15. Die Aussage zum Rang folgt aus Proposition 3.14. □

Definition 3.21. *Sei K ein Zahlkörper. Eine $\mathbb{Z}$-Basis von $\mathcal{O}_K$ heißt* Ganzheitsbasis. *Die Diskriminante einer Ganzheitsbasis heißt* Diskriminante des Zahlkörpers *und wird mit d_K bezeichnet.*

Für die Wohldefiniertheit der Diskriminante brauchen wir noch ein Lemma:

Lemma 3.22. *Sei B/A eine Ringerweiterung, wobei A ganz-abgeschlossen und B ganz über A ist. Sei $x_1, \ldots, x_n$ eine Menge paarweise A-linear unabhängiger Elemente in B, und seien $y_1, \ldots, y_n$ durch $y_i = \sum a_{ij} x_j$, $a_{ij} \in A$ gegeben. Dann gilt*

$$D(y_1, \ldots, y_n) = \det(a_{ij})^2 D(x_1, \ldots, x_n).$$

Insbesondere ist also $x_1, \ldots, x_n$ genau dann eine Ganzheitsbasis, wenn für ihre Diskriminante $D(x_1, \ldots, x_n) = d_K$ gilt.

Korollar 3.23. *Sei K ein Zahlkörper, $M \subseteq \mathcal{O}_K$ ein $\mathbb{Z}$-Untermodul dessen Index $[\mathcal{O}_K : M]$ endlich ist. Dann gilt für jede $\mathbb{Z}$-Basis $x_1, \ldots, x_n$ von M*

$$D(x_1, \ldots, x_n) = [\mathcal{O}_K : M]^2 \cdot d_K.$$

Insbesondere ist $x_1, \ldots, x_n$ eine Ganzheitsbasis, wenn $D(x_1, \ldots, x_n)$ quadratfrei ist. Dies ist eine zentrale Bemerkung, aus der ein Algorithmus zur Bestimmung von Ganzheitsbasen hervorgeht. Dazu vielleicht später mehr.

Beispiel 3.24. *Sei $K = \mathbb{Q}(\sqrt{d})$. Wenn $d \equiv 2, 3 \mod 4$, dann ist $d_K = 4d$. Wenn $d \equiv 1 \mod 4$, dann ist $d_K = d$. Aus Übungsaufgabe 3.1 kennen wir eine Ganzheitsbasis von $\mathcal{O}_K$. In Beispiel 3.12 wurde bereits die Diskriminante für die $\mathbb{Q}$-Basis $1, \sqrt{d}$ berechnet. Die analoge Rechnung liefert dann auch den Fall $d \equiv 1 \mod 4$.* □

Übungsaufgabe 3.5 (Stickelbergerscher Diskriminantensatz)**.** *Für jeden Zahlkörper K ist $d_K \equiv 0, 1 \mod 4$.*

Der folgende Satz gilt auch allgemeiner über beliebigen Zahlkörpern K, sofern L_1 bzw. L_2 Ganzheitsbasen besitzen.

Satz 3.25. *Seien L_1, L_2 zwei Galois-Erweiterungen von $\mathbb{Q}$, $n_i = [L_i : \mathbb{Q}]$ und $L_1 \cap L_2 = \mathbb{Q}$. Seien $x_1, \ldots, x_{n_1}$ und $y_1, \ldots, y_{n_2}$ Ganzheitsbasen von $\mathcal{O}_{L_1}$ bzw. $\mathcal{O}_{L_2}$. Wenn d_{L_1} und d_{L_2} teilerfremd sind, dann ist $x_i y_j$ eine Ganzheitsbasis von $\mathcal{O}_{L_1 L_2}$ und*

$$d_{L_1 L_2} = d_{L_1}^{n_2} d_{L_2}^{n_1}.$$

Beweis. Es ist nach Voraussetzung $L_1 \cap L_2 = \mathbb{Q}$, also $[L_1 L_2 : \mathbb{Q}] = n_1 n_2$. Für $x_1, \ldots, x_{n_1}$ eine Basis von L_1 und $y_1, \ldots, y_{n_2}$ eine Basis von L_2 ist $x_i y_j$ eine $\mathbb{Q}$-Basis des Kompositums $L_1 L_2$. Sei nun $\alpha = \sum_{i,j} a_{ij} x_i y_j$ ein ganzes Element in $L_1 L_2$.

Wir wählen Bezeichnungen für die Elemente der Galoisgruppen

$$\mathrm{Gal}(L_1 L_2 / L_2) = \{\sigma_1, \ldots, \sigma_{n_1}\}, \qquad \mathrm{Gal}(L_1 L_2 / L_1) = \{\tau_1, \ldots, \tau_{n_2}\}.$$

$$\mathrm{Gal}(L_1 L_2 / \mathbb{Q}) = \{\sigma_k \tau_l \mid k = 1, \ldots, n_1; l = 1, \ldots, n_2\}.$$

Wir betrachten die Matrix $T = (\tau_l y_j)$, für die gilt $\det T^2 = d_{L_2}$. Außerdem gilt

$$(\tau_1 \alpha, \ldots, \tau_{n_2} \alpha)^t = T \left(\sum a_{i1} x_i, \ldots, \sum a_{i n_2} x_i \right)^t.$$

Bezeichne $T^* = \det T T^{-1}$ die adjungierte Matrix, dann folgt

$$T^* (\tau_1 \alpha, \ldots, \tau_{n_2} \alpha)^t = \det(T) \left(\sum a_{i1} x_i, \ldots, \sum a_{i n_2} x_i \right)^t.$$

Die linke Seite ist ein Vektor mit ganzen Elementen, damit folgt

$$d_{L_2} \sum_i a_{ij} x_i \in \mathcal{O}_{L_1}, \text{ also } d_{L_2} a_{ij} \in \mathbb{Z}.$$

Das gleiche Argument zeigt symmetrisch $d_{L_1} a_{ij} \in \mathbb{Z}$, also wegen der Teilerfremdheit $a_{ij} \in \mathbb{Z}$. Die $x_i y_j$ bilden also eine Ganzheitsbasis. In dieser Basis kann man auch die Determinante sehen. □

Korollar 3.26. *Seien d_1, d_2 teilerfremde quadratfreie Zahlen, $d_1 \equiv 1 \mod 4$, und sei $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$.*

(i) Für $d_2 \equiv 2, 3 \mod 4$ ist

$$1, \sqrt{d_2}, \frac{1 + \sqrt{d_1}}{2}, \frac{\sqrt{d_2} + \sqrt{d_1 d_2}}{2}$$

eine Ganzheitsbasis von $\mathcal{O}_K$. Die Diskriminante ist $d_K = 16 d_1^2 d_2^2$.

(ii) Für $d_2 \equiv 1 \mod 4$ ist

$$1, \frac{1 + \sqrt{d_1}}{2}, \frac{1 + \sqrt{d_2}}{2}, \frac{1 + \sqrt{d_1} + \sqrt{d_2} + \sqrt{d_1 d_2}}{4}$$

eine Ganzheitsbasis von $\mathcal{O}_K$. Die Diskriminante ist $d_K = d_1^2 d_2^2$.

3.5 Beispiel 2: Zyklotomische Körper

Eine Zahl $x \in \overline{\mathbb{Q}}$ heißt n-te Einheitswurzel, wenn $x^n = 1$. Eine n-te Einheitswurzel heißt primitiv, wenn $x^m \neq 1$ für $m < n$. Primitive n-te Einheitswurzeln werden meist mit ζ_n bezeichnet. Die Gruppe der n-ten Einheitswurzeln mit Multiplikation ist zyklisch von Ordnung n; die Erzeuger sind genau die primitiven n-ten Einheitswurzeln. Die Anzahl der primitiven n-ten Einheitswurzeln ist $\phi(n)$, die Eulersche ϕ-Funktion.

Das Minimalpolynom von ζ_n ist das n-te zyklotomische Polynom $\Phi_n(X)$ und es gilt $\deg \Phi_n(X) = \phi(n)$. Die Körper $\mathbb{Q}(\zeta_n)$ heißt n-ter zyklotomischer Körper bzw. n-ter Kreisteilungskörper. Die Erweiterung $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ ist galoissch mit Galoisgruppe $(\mathbb{Z}/n\mathbb{Z})^\times$, der Isomorphismus wird vermittelt durch

$$(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) : i \mapsto (\zeta_n \mapsto \zeta_n^i).$$

Das Ziel dieses Abschnitts ist die Bestimmung der Ganzheitsringe zyklotomischer Körper. Wir bemerken $\zeta_2 = -1 \in \mathbb{Q}$, und daraus folgt $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{2n})$ für n ungerade. Wir können also im Folgenden $4 \mid n$ annehmen, wenn n gerade ist.

Satz 3.27. *Sei ζ_n eine primitive n-te Einheitswurzel, $K = \mathbb{Q}(\zeta_n)$ der dazugehörige zyklotomische Zahlkörper. Dann ist $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$, d.h. jedes Element von $\mathcal{O}_K$ kann eindeutig als $\mathbb{Z}$-Linearkombination von $1, \zeta_n, \ldots, \zeta_n^{n-2}$ dargestellt werden.*

Es gilt

$$d_K = (-1)^{s\frac{\phi(n)}{2}} \frac{n^{\phi(n)}}{\prod_{q|n} q^{\frac{\phi(n)}{q-1}}},$$

wobei s die Anzahl von Primzahlen $q \mid n$ bezeichnet.

Beweis. Der Satz ist eine Konsequenz aus Satz 3.25, Proposition 3.31 und Lemma 3.30. □

Wir machen ein paar Vorüberlegungen und Rechnungen in $\mathcal{O}_K$.

Lemma 3.28. *(i)*

$$p = \Phi_{p^k}(1) = \prod_{i \in (\mathbb{Z}/p^k\mathbb{Z})^\times} (1 - \zeta_{p^k}^i) = N_{K/\mathbb{Q}}(1 - \zeta_{p^k})$$

(ii)

$$1 - \zeta_{p^k}^i = (1 + \zeta_{p^k} + \cdots + \zeta_{p^k}^{i-1})(1 - \zeta_{p^k}).$$

(iii) Für $i, j \in \mathbb{Z}$ invertierbar in $\mathbb{Z}/p^k\mathbb{Z}$ gibt es l mit $j \equiv il \mod p^k$ und man erhält

$$\frac{1 - \zeta_{p^k}^j}{1 - \zeta_{p^k}^i} = \frac{1 - \zeta_{p^k}^{il}}{1 - \zeta_{p^k}^i} = 1 + \zeta_{p^k}^i + \zeta_{p^k}^{2i} + \cdots + \zeta_{p^k}^{(l-1)i} \in \mathcal{O}_K.$$

(iv) Alle $1 - \zeta_{p^k}^i$, $i \in (\mathbb{Z}/p^k\mathbb{Z})^\times$ sind assoziiert, d.h. $1 - \zeta_{p^k}^i = u_i(1 - \zeta_{p^k})$ für $u_i \in \mathcal{O}_K^\times$.

(v) $1-\zeta_{p^k}$ *ist keine Einheit in* $\mathcal{O}_K$.

Beweis. (i) folgt aus

$$\Phi_{p^k}(X) = \frac{X^{p^k}-1}{X^{p^{k-1}}-1} = X^{(p-1)p^{k-1}} + \cdots + X^{p^{k-1}} + 1.$$

(ii) ist einfach ausmultiplizieren, daraus folgt auch (iii). (iv) folgt aus symmetrischer Anwendung von (iii). (v) Mit $1-\zeta_p$ sind alle $1-\zeta_p^i$ Einheiten und mit (i) ist p eine Einheit in $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$. □

Proposition 3.29. *Satz 3.27 gilt für* $n = p$ *eine ungerade Primzahl.*

Beweis. Die Elemente $1, \zeta_p, \ldots, \zeta_p^{p-2}$ sind $\mathbb{Q}$-linear, damit auch $\mathbb{Z}$-linear unabhängig, da $\Phi_p(X)$ irreduzibel vom Grad $p-1$ ist. Sei nun $x = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2} \in \mathcal{O}_K$, $a_i \in \mathbb{Q}$ ein ganzes Element.

Wir zeigen zuerst $\mathrm{Tr}(x(1-\zeta_p)) \in (1-\zeta_p)\mathcal{O}_K \cap \mathbb{Z}$. Seien $\sigma_1, \ldots, \sigma_{p-1}$ die verschiedenen $\mathbb{Q}$-Einbettungen von $\mathbb{Q}(\zeta_p)$ in $\overline{\mathbb{Q}}$. Dann gilt mit Lemma 3.28 (iii) $1-\zeta_p^i = (1-\zeta_p)(1+\zeta_p+\cdots+\zeta_p^{i-1})$ auch

$$\mathrm{Tr}(x(1-\zeta_p)) = \sum_{i=1}^{p-1} \sigma_i(x)(1-\sigma_i(\zeta_p)) = (1-\zeta_p)\sum_{i=1}^{p-1}\sigma_i(x)\sum_{j=0}^{i-1}\zeta_p^j \in (1-\zeta_p)\mathcal{O}_K \cap \mathbb{Z}.$$

Als nächstes zeigen wir $\mathrm{Tr}(x(1-\zeta_p)) = a_0 p$. Man liest $\mathrm{Tr}(\zeta_p^i) = -1$ am Minimalpolynom $\Phi_p(X)$ ab. Damit ist $\mathrm{Tr}(a_i(\zeta_p^i - \zeta_p^{i+1})) = 0$ für $i > 0$ und man erhält

$$\mathrm{Tr}(x(1-\zeta_p)) = \mathrm{Tr}\left(\sum_{i=0}^{p-2} a_i(\zeta_p^i - \zeta_p^{i+1})\right) = \mathrm{Tr}(a_0(1-\zeta_p)) = a_0(p-1+1) = a_0 p.$$

Nun zeigen wir $(1-\zeta_p)\mathcal{O}_K \cap \mathbb{Z} = p\mathbb{Z}$. Mit $x = 1$ ist die Inklusion $p\mathbb{Z} \subseteq (1-\zeta_p)\mathcal{O}_K \cap \mathbb{Z}$ klar. Wenn die zweite Inklusion nicht gilt, ist $1 \in (1-\zeta_p)\mathcal{O}_K$, also $1-\zeta_p$ eine Einheit in $\mathcal{O}_K$, was im Widerspruch zu Lemma 3.28 (v) steht. Alternativ sieht man das mit Lemma 3.28 (i).

Zusammenfassend haben wir $a_0 \in \mathbb{Z}$ gezeigt. Dies ist der Anfang einer Induktion. Wir nehmen an $a_0, a_1, \ldots, a_{i-1} \in \mathbb{Z}$. Dann ist

$$x\zeta_p^{p-i} = a_0\zeta_p^{p-i} + a_1\zeta_p^{p-i+1} + \cdots + a_{i-1}\zeta_p^{p-1} + a_i + a_{i+1}\zeta_p + \cdots + a_{p-2}\zeta_p^{p-i-2}.$$

Mit $\zeta_p^{p-1} = -\zeta_p^{p-2} - \cdots - 1$ können wir das zu

$$x\zeta_p^{p-i} = (a_i - a_{i-1}) + a_1'\zeta_p + \cdots + a_{p-2}'\zeta_p^{p-2}$$

umschreiben. Das gleiche Argument wie oben liefert dann $a_i - a_{i-1} \in \mathbb{Z}$, also $a_i \in \mathbb{Z}$. □

Lemma 3.30. *Sei* $p^k > 2$ *eine Primzahlpotenz,* ζ_{p^k} *eine primitive* p^k*-te Einheitswurzel und* $K = \mathbb{Q}(\zeta_{p^k})$ *der dazugehörige zyklotomische Körper. Dann ist*

$$D(1, \zeta_{p^k}, \ldots, \zeta_{p^k}^{\phi(p^k)-1}) = (-1)^{\frac{\phi(p^k)}{2}} p^{p^{k-1}(k(p-1)-1)}.$$

Beweis. Wir bemerken zuerst $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$. Nach Proposition 3.13 ist

$$D(1, \zeta_{p^k}, \ldots, \zeta_{p^k}^{\phi(p^k)-1}) = (-1)^{\frac{\phi(p^k)(\phi(p^k)-1)}{2}} N_{\mathbb{Q}(\zeta_{p^k})/\mathbb{Q}}(\Phi'_{p^k}(\zeta_{p^k})).$$

Für die Ableitung $\Phi'_{p^k}(X)$ folgt aus $X^{p^k} - 1 = (X^{p^{k-1}} - 1)\Phi_{p^k}(X)$

$$p^k X^{p^k-1} = p^{k-1} X^{p^{k-1}-1} \Phi_{p^k}(X) + (X^{p^{k-1}} - 1)\Phi'_{p^k}(X),$$

und damit durch Einsetzen von $X = \zeta_{p^k}$ insbesondere

$$p^k \zeta_{p^k}^{p^k-1} = (\zeta_{p^k}^{p^{k-1}} - 1)\Phi'_{p^k}(\zeta_{p^k}).$$

Auf diese Gleichung wendet man die Norm an und erhält

$$p^{k\phi(p^k)} N_{\mathbb{Q}(\zeta_{p^k})/\mathbb{Q}}(\zeta_{p^k})^{p^k-1} = N_{\mathbb{Q}(\zeta_{p^k})/\mathbb{Q}}(\zeta_{p^k}^{p^{k-1}} - 1) N_{\mathbb{Q}(\zeta_{p^k})/\mathbb{Q}}(\Phi'_{p^k}(\zeta_{p^k})).$$

Die Normen sind

$$N_{\mathbb{Q}(\zeta_{p^k})/\mathbb{Q}}(\zeta_{p^k}) = (-1)^{\phi(p^k)} = 1, \qquad N_{\mathbb{Q}(\zeta_{p^k})/\mathbb{Q}}(\zeta_{p^k}^{p^{k-1}} - 1) = p^{p^{k-1}}.$$

Zusammenfassend erhalten wir unter Berücksichtigung von $\frac{\phi(p^k)(\phi(p^k)-1)}{2} \equiv \frac{\phi(p^k)}{2} \mod 2$ die Behauptung. □

Übungsaufgabe 3.6. *Überzeugen Sie sich von den behaupteten Normberechnungen im Beweis von Lemma 3.30.*

Proposition 3.31. *Satz 3.27 gilt für $n = p^k$ eine Primzahlpotenz.*

Beweis. Im Beweis benutzen wir die Bezeichnung $d = D(1, \zeta_{p^k}, \ldots, \zeta_{p^k}^{\phi(p^k)-1})$.

Sei $x = x_0 + x_1\zeta_{p^k} + \cdots + x_{\phi(p^k)-1}\zeta_{p^k}^{\phi(p^k)-1} \in \mathcal{O}_K$. Es genügt zu zeigen, daß für jede Primzahl $q \in \mathbb{Z}$ aus $x \in q\mathcal{O}_K$ schon $x_i \in q\mathbb{Z}$ folgt. Seien nämlich b_i die Nenner von $x_i = a_i/b_i$ und l das kleinste gemeinsame Vielfache der b_i. Wir nehmen an $l > 1$. Sei q^r eine Primzahlpotenz mit $q^r \mid b_i \mid l$ und $q \nmid l/b_i$. Dann ist $lx \in q^r\mathcal{O}_K$, und mit der Behauptung angewendet auf lx folgt $q \mid a_i l/b_i$, wegen $q \nmid l/b_i$ also $q \mid a_i$. Dies ist ein Widerspruch, also $l = 1$ und $x_i \in \mathbb{Z}$.

Als nächstes zeigen wir wie in Proposition 3.14, daß $dx_j \in \mathbb{Z}$ ist. Seien $\sigma_1, \ldots, \sigma_{\phi(p^k)}$ die $\mathbb{Q}$-Einbettungen von K in einen gewählten algebraischen Abschluß $\overline{\mathbb{Q}}$. Dann gilt für alle $i = 1, \ldots, \phi(p^k)$

$$\sigma_i(x) = \sum_{j=0}^{\phi(p^k)-1} x_j \sigma_i(\zeta_{p^k}^j).$$

Die x_i sind also Lösungen des entsprechenden linearen Gleichungssystems und für die Determinante der Koeffizientenmatrix gilt $\det(\sigma_i(\zeta_{p^k}^j))^2 = d$. Wir bezeichnen mit α_j die Determinante der Matrix, die aus $(\sigma_i(\zeta_{p^k}^j))$ durch Ersetzung der j-ten Spalte durch die $(\sigma_1(x), \ldots, \sigma_{\phi(p^k)}(x))$ entsteht und bemerken, daß $\alpha_j \in \mathcal{O}_K$ ist. Mit der Cramerschen Regel Lemma A.7 folgt

$$dx_j = \alpha_j \det(\sigma_i(\zeta_{p^k}^j)) \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}.$$

Nun zeigen wir für alle Primzahlen $q \neq p$, daß aus $x \in q\mathcal{O}_K$ schon $x_i \in q\mathbb{Z}$ folgt. Aus dem vorherigen Abschnitt wissen wir $q \mid da_i$, wobei a_i der Zähler von $x_i = a_i/b_i$ ist. Aus Lemma 3.30 folgt $q \nmid d$, also $q \mid a_i$ und $q \mid x_i$.

Es bleibt noch zu zeigen, daß aus $x \in p\mathcal{O}_K$ schon $x_i \in p\mathbb{Z}$ folgt. Dafür betrachten wir das Polynom $h(X) = x_0 + x_1X + \cdots + x_{\phi(p^k)-1}X^{\phi(p^k)-1}$ bzw. seine Taylor-Entwicklung an $X = 1 - \xi$ wobei $\xi = 1 - \zeta_{p^k}$:

$$x = h(\zeta_{p^k}) = h(1-\xi) = \sum_{i=0}^{\phi(p^k)-1} (-1)^i \xi^i \frac{h^{(i)}(1)}{i!}.$$

Mit Lemma 3.28 (i) und (iv) folgt $p = u(1-\zeta_{p^k})^{\phi(p^k)}$ und damit $\xi^{\phi(p^k)} \mid p \mid x$. Damit haben wir auch $\xi \mid h(1)$, also $h(1) \in \xi\mathcal{O}_K \cap \mathbb{Q} = p\mathbb{Z}$. Weiterhin haben wir

$$\xi \mid \frac{p}{\xi} \mid -\frac{x - h(1)}{\xi} = \sum_{i=1}^{\phi(p^k)-1} (-1)^{i-1} \xi^{i-1} \frac{h^{(i)}(1)}{i!}$$

Also $\xi \mid h'(1)$ und damit $p \mid h'(1)$. Induktiv folgt

$$p \mid \frac{h^{(i)}(1)}{i!} \text{ für alle } i = 0, \ldots, \phi(p^k) - 1.$$

Es gilt (mit der Konvention $\binom{n}{k} = 0$ für $k > n$)

$$\frac{h^{(i)}(1)}{i!} = \sum_{j=0}^{\phi(p^k)-1} \binom{j}{i} x_j$$

und daraus lesen wir induktiv ab, daß $p \mid x_i$ für alle $i = 0, \ldots, \phi(p^k) - 1$. □

Auch in diesem Beweis haben wir gesehen, daß die Primfaktoren, die quadratisch in der Diskriminante vorkommen eine besondere Rolle bei der Bestimmung des Ganzheitsrings spielen.

Übungsaufgaben

Übungsaufgabe 3.7. *Bestimmen Sie die Einheiten in $\mathbb{Z}[\rho]$, wobei ρ eine primitive dritte Einheitswurzel ist.*

Übungsaufgabe 3.8. *Sei θ eine Wurzel von $x^3 - 3x^2 + 3 = 0$. Berechnen Sie Norm und Spur von $\theta^2 - 2\theta$ in $\mathbb{Q}(\theta)/\mathbb{Q}$.*

Übungsaufgabe 3.9. *Seien $M/L/K$ endliche separable Erweiterungen.*

1. *Die Spur induziert einen Homomorphismus $\mathrm{Tr}_{L/K} : L \to K$ der additiven Gruppen und es gilt $\mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L} = \mathrm{Tr}_{M/K}$. Die Komposition $K \hookrightarrow L \xrightarrow{\mathrm{Tr}_{L/K}} K$ ist Multiplikation (in der additiven Gruppe) mit $[L : K]$.*
2. *Die Norm induziert einen Homomorphismus $N_{L/K} : L^\times \to K^\times$ der multiplikativen Gruppen und es gilt $N_{L/K} \circ N_{M/L} = N_{M/K}$. Die Komposition $K^\times \hookrightarrow L^\times \xrightarrow{N_{L/K}} K^\times$ ist Multiplikation (in der multiplikativen Gruppe) mit $[L : K]$.*

Übungsaufgabe 3.10. *Wir betrachten das Polynom $f(X) = X^3+pX+q$, und den dazugehörigen Ring $K[X]/(X^3+pX+q)$. Berechnen Sie $D(1, X, X^2)$.*

Übungsaufgabe 3.11. *Zeigen Sie für $f(X) = X^n + pX + q$ und den Ring $K[X]/(X^n + pX + q)$:*

$$D(1, X, \ldots, X^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \left(n^n q^{n-1} + (-1)^n (n-1)^{(n-1)} p^n \right).$$

Übungsaufgabe 3.12. *Zeigen Sie, daß $\mathbb{Q}$ als $\mathbb{Z}$-Modul torsionsfrei aber nicht frei ist.*

Übungsaufgabe 3.13. *Bestimmen Sie eine Ganzheitsbasis von $\mathcal{O}_K$ wobei $K = \mathbb{Q}(\sqrt[3]{2})$.*

Übungsaufgabe 3.14. *Berechnen Sie eine Ganzheitsbasis für $\mathcal{O}_{\mathbb{Q}(\theta)}$, wobei θ eine Wurzel der Gleichung $x^3 + 2x + 1 = 0$ ist.*

Übungsaufgabe 3.15 (Dedekind)**.** *Sei $K = \mathbb{Q}(\theta)$ wobei $\theta^3 - \theta^2 - 2\theta - 8 = 0$.*

(i) Zeigen Sie, daß $\beta = (\theta^2 + \theta)/2$ ganz ist.

(ii) Berechnen Sie $D(1, \theta, \beta)$. Folgern Sie, daß $1, \theta, \beta$ eine Ganzheitsbasis von $\mathcal{O}_K$ ist.

(iii) Zeigen Sie, daß für jedes Element $x \in \mathcal{O}_K$ die Diskriminante $D(1, x, x^2)$ gerade ist.

Insbesondere gibt es in $\mathcal{O}_K$ keine Ganzheitsbasis der Form $1, x, x^2$.

Kapitel 4

Ideale in Dedekindringen

In diesem Kapitel beginnen wir das Studium der multiplikativen Struktur von Ganzheitsringen. Wir zeigen allgemeiner, daß Ideale in *Dedekind-Ringen* eindeutig in Primideale faktorisiert werden können. Wir untersuchen auch im Detail, wie diese Faktorisierung für quadratische Körper aussieht.

Definition 4.1. *Sei R ein Ring. Ein* Ideal *$I \subseteq R$ ist ein R-Untermodul von R. Ein Ideal $I \subsetneq R$ heißt* maximal*, wenn es maximal bezüglich der Inklusion von R-Untermoduln ist. Ein Ideal $I \subsetneq R$ heißt* prim*, wenn für $a, b \in R$ mit $ab \in I$ schon $a \in I$ oder $b \in I$ gilt.*

Für eine Menge $S \subseteq R$ heißt

$$(S) = \left\{ \sum_{i=1}^{n} \lambda_i s_i \mid n \in \mathbb{N}, \lambda_i \in R, s_i \in S \right\}$$

das von S erzeugte Ideal. Ein Ideal I heißt Hauptideal, wenn es ein Element $a \in R$ gibt mit $I = (a)$.

Übungsaufgabe 4.1. *Sei R ein Ring. Ein Ideal $I \subseteq R$ ist genau dann maximal, wenn R/I ein Körper ist. Ein Ideal $I \subseteq R$ ist genau dann prim, wenn R/I ein Integritätsbereich ist.*

Definition 4.2. *Sei R ein Ring und $I_1, I_2 \subseteq R$ Ideale von R. Dann sind Summe und Produkt wie folgt definiert:*

$$I_1 + I_2 = \{x + y \mid x \in I_1, y \in I_2\}$$

$$I_1 \cdot I_2 = \left\{ \sum_{i=1}^{n} x_i y_i \mid n \in \mathbb{N}, x_i \in I_1, y_i \in I_2 \right\}.$$

Zu bemerken ist, daß $I_1 \cdot I_2 \subseteq I_1 \cap I_2$. Teilbarkeit von Idealen $I_1 \mid I_2$ übersetzt sich damit in Inklusion $I_1 \subseteq I_2$.

4.1 Der Zwei-Quadrate-Satz

Wir betrachten den Körper der Gaußschen Zahlen $K = \mathbb{Q}(i)$. Der Ganzheitsring $\mathcal{O}_K = \mathbb{Z}[i]$ heißt Ring der ganzen Gaußschen Zahlen. Für $a + bi \in \mathbb{Z}[i]$ ist

$N_{\mathbb{Q}(i)/\mathbb{Q}}(a+bi) = a^2+b^2 \in \mathbb{Z}.$, insbesondere ist eine Zahl genau dann Summe von zwei Quadraten, wenn sie Norm einer ganzen Gaußschen Zahl ist. Dies führt zum Zwei-Quadrate-Satz.

Lemma 4.3. *Der Ring $\mathbb{Z}[i]$ ist ein Hauptidealring.*

Beweis. Wir zeigen, daß $\mathbb{Z}[i]$ ein euklidischer Ring bezüglich der Norm $N(a+bi) = N_{\mathbb{Q}(i)/\mathbb{Q}}(a+bi) = a^2+b^2$ ist. Der euklidische Algorithmus zeigt dann die Behauptung.

Seien $x, y \in \mathbb{Z}[i]$, $y \neq 0$. Zu zeigen ist die Existenz von $q, r \in \mathbb{Z}[i]$ mit $x = qy + r$ und $N(r) < N(y)$. Alternativ genügt es, ein q mit $N(x/y - q) < 1$ zu finden. Aber $\mathbb{Z}[i]$ ist ein Gitter in $\mathbb{Q}(i)$, erzeugt von 1 und i. Der Abstand eines beliebigen Punktes x/y vom nächsten Gitterpunkt q ist damit nicht länger als die halbe Länge der Diagonale der Grundmasche $(0,0), (1,0), (0,i), (1,i)$, also $\sqrt{2}/2 < 1$. □

Lemma 4.4. *Für eine Primzahl p gilt*

(i) (2) *ist Quadrat eines Primideals in $\mathbb{Z}[i]$.*

(ii) (p) *ist prim in $\mathbb{Z}[i]$ genau dann, wenn $p \equiv 3 \mod 4$.*

(iii) (p) *ist Produkt von zwei Primidealen in $\mathbb{Z}[i]$ genau dann, wenn $p \equiv 1 \mod 4$.*

Beweis. Wir haben $\mathbb{Z}[i] = \mathbb{Z}[X]/(X^2+1)$. Wir wollen nun in jedem Fall bestimmen, welche Ideale über den jeweiligen Idealen (p) liegen. Dafür benutzen wir die Bijektion zwischen Idealen über (p) und den Idealen im Quotientenring $\mathbb{Z}[i]/(p)$

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

Es muß also in jedem Fall bestimmt werden, wie sich das Polynom X^2+1 über dem Körper $\mathbb{F}_p$ zerlegt.

Für (2) haben wir $\mathbb{F}_2[X]/(X^2+1) = \mathbb{F}_2[X]/(X+1)^2$, das Ideal (2) ist also das Quadrat des Ideals $(2, i+1) = (i+1)$.

Für eine ungerade Primzahl p und einen Erzeuger u von $\mathbb{F}_p^\times = \mathbb{Z}/(p-1)\mathbb{Z}$ ist $-1 = u^{\frac{p-1}{2}}$. Damit ist -1 ein Quadrat in $\mathbb{F}_p$ genau dann, wenn $\frac{p-1}{2}$ gerade ist, also wenn $p - 1 \equiv 0 \mod 4$.

Wenn $p \equiv 3 \mod 4$ ist -1 kein Quadrat, also X^2+1 irreduzibel über $\mathbb{F}_p$. Dann ist $\mathbb{F}_p[X]/(X^2+1)$ ein Körper, und das Ideal (p) ist ein Primideal.

Wenn $p \equiv 1 \mod 4$ ist $-1 = v^2$ mit $v = u^{\frac{p-1}{4}}$ und X^2+1 zerfällt über $\mathbb{F}_p$ in zwei Linearfaktoren $X^2+1 = (X+v)(X-v)$. Damit zerfällt auch das Ideal (p) in zwei Primidealfaktoren $(p) = (p, i+v)(p, i-v)$. □

Satz 4.5. *Sei n eine ganze Zahl mit Primfaktorisierung $n = \prod_p p^{v_p(n)}$. Die Zahl n kann genau dann als Summe von zwei Quadraten geschrieben werden, wenn für alle $p \equiv 3 \mod 4$ gilt $v_p(n) \equiv 0 \mod 2$.*

Beweis. Die Norm $N_{\mathbb{Q}(i)/\mathbb{Q}}$ ist multiplikativ. Wir können uns also auf $n = p^k$ eine Primzahlpotenz einschränken. Mit $2 = 1^2 + 1^2$ gilt die Aussage für $p = 2$. In den Fallunterscheidungen nutzen wir Lemma 4.4.

Im Fall $p \equiv 1 \mod 4$ ist $(p) = \mathfrak{p}_1\mathfrak{p}_2$ ein Produkt von zwei Primidealen. Die Primideale sind Hauptideale, cf. Lemma 4.3. Damit ist $p = p_1 p_2$ Produkt von

zwei Elementen, die jeweils Norm p haben, da $p^2 = N(p) = N(p_1)N(p_2)$ und $N(p_i) > 1$. Insbesondere läßt sich jede Primzahl $p \equiv 1 \mod 4$ als Summe von zwei Quadraten darstellen.

Im Fall $p \equiv 3 \mod 4$ ist die Zerlegbarkeit in zwei Quadrate in die Bedingung eingebaut, das liefert die Implikation $\Leftarrow$. Für $\Rightarrow$ bemerken wir, daß aus $N_{\mathbb{Q}(i)/\mathbb{Q}}(a+bi) \in p\mathbb{Z}$ mit $p \equiv 3 \mod 4$ schon folgt $a + bi \in p\mathbb{Z}[i]$. Mit $N_{\mathbb{Q}(i)/\mathbb{Q}}(p) = p^2$ ist dann aber $N_{\mathbb{Q}(i)/\mathbb{Q}}(a+bi) \in p^2\mathbb{Z}$. □

Was sind die wesentlichen Elemente des Beweises? Die Grundidee ist, daß die Frage nach Summen von zwei Quadraten durch die Norm der Gaußschen Zahlen ausgedrückt werden kann: welche Primzahlen in $\mathbb{Z}$ sind Normen von Elementen in $\mathbb{Z}[i]$. Diese Frage wird beantwortet durch die Faktorisierung von Primzahlen in $\mathbb{Z}[i]$ in verschiedene Primideale und die Tatsache, daß $\mathbb{Z}[i]$ ein Hauptidealring ist. Diese Fragen werden uns im Folgenden beschäftigen. Zuerst studieren wir die Zerlegung von Idealen in Primideale, die eine Verallgemeinerung der Zerlegung von Zahlen in Primzahlen ist.

Übungsaufgabe 4.2. *Auf die gleiche Art kann man den Vier-Quadrate-Satz beweisen: Statt $\mathbb{Q}[i]$ betrachtet man die Quaternionen-Algebra $\mathbb{H}$. Die Norm der Quaternionen ist $N(a+bi+cj+dk) = a^2+b^2+c^2+d^2$. In den Quaternionen gibt es eine Maximalordnung $\mathfrak{H}$, also eine nicht-kommutative Verallgemeinerung des Ganzheitsrings $\mathbb{Z}[i]$. Die Links-Ideale dieser Maximalordnung sind Hauptideale. Über endlichen Körpern gibt es keine nicht-trivialen zentralen einfachen Algebren, darum sind* alle *Primideale in $\mathfrak{H}$ zerlegt. Deswegen läßt sich jede Primzahl als Summe von vier Quadraten darstellen.*

4.2 Dedekind-Ringe

Definition 4.6 (Krull-Dimension)**.** *Sei R ein Ring. Die* Krull-Dimension *von R ist die maximale Länge n einer Kette von Primidealen*

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$$

Beispiel 4.7.

1. *Die Krull-Dimension von Körpern ist* 0*.*
2. *Die Krull-Dimension eines Hauptidealrings ist* 1*, maximale Ketten sind von der Form $(0) \subsetneq (p)$ für p ein Primelement.*
3. *Die Krull-Dimension von $k[x_1, \ldots, x_n]$ ist n. Insbesondere ist $k[x_i \mid i \in \mathbb{N}]$ ein Ring mit unendlicher Krull-Dimension.*

□

Wir untersuchen nun die Krull-Dimension von Ganzheitsringen. Dazu gibt es zwei allgemeine Sätze über das Verhalten von Primidealen in ganzen Erweiterungen, Cohen-Seidenberg going-up bzw. going-down, cf. [AM69, Kapitel 5]. Aus diesen Sätzen der kommutativen Algebra folgt, daß für eine ganze Ringerweiterung $A \subseteq B$ die Krull-Dimensionen von A und B übereinstimmen. Hier betrachten wir nur den Spezialfall von Zahlringen.

Proposition 4.8. *Sei K ein Zahlkörper. Dann ist jedes von* (0) *verschiedene Primideal von $\mathcal{O}_K$ maximal. Insbesondere ist die Krull-Dimension von $\mathcal{O}_K$ gleich* 1*.*

Beweis. Sei $(0) \neq \mathfrak{p} \subseteq \mathcal{O}_K$ ein Primideal. Dann ist $\mathfrak{p} \cap \mathbb{Z}$ auch ein Primideal. Sind nämlich $a, b \in \mathbb{Z} \subseteq \mathcal{O}_K$, folgt aus $ab \in \mathfrak{p}$ schon $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$.

Sei $x \in \mathfrak{p}$ mit Ganzheitsgleichung $x^n + a_1 x^{n-1} + \cdots + a_n = 0$, $a_i \in \mathbb{Z}$. Umstellen liefert $a_n = -x(x^{n-1} + a_1 x^{n-2} + \cdots + a_{n-1}) \in (x) \subseteq \mathfrak{p}$. Damit ist $\mathfrak{p} \cap \mathbb{Z} = (p)$ für p eine Primzahl.

Die Abbildung $\mathbb{Z}/(p) \to \mathcal{O}_K/\mathfrak{p}$ ist wieder eine ganze Ringerweiterung. Mit Übungsaufgabe 2.6 ist $\mathcal{O}_K/\mathfrak{p}$ ein Körper, also $\mathfrak{p}$ ein maximales Ideal. □

Definition 4.9 (Dedekind-Ring)**.** *Ein Integritätsbereich R heißt* Dedekind-Ring*, wenn R noethersch, ganz-abgeschlossen und von Krull-Dimension* 1 *ist.*

Satz 4.10. *Sei K ein Zahlkörper. Dann ist $\mathcal{O}_K$ ein Dedekind-Ring.*

Beweis. Korollar 2.8, Korollar 3.20 und Proposition 4.8. □

4.3 Primidealfaktorisierung gebrochener Ideale

Definition 4.11. *Sei R ein Integritätsbereich mit Quotientenkörper K. Ein* gebrochenes Ideal von R *ist ein R-Untermodul I von K für den ein $0 \neq d \in R$ existiert mit $dI \subseteq R$.*

Die Idealoperationen aus Definition 4.2 können offensichtlich auf gebrochene Ideale fortgesetzt werden. Für einen noetherschen Integritätsbereich ist die obige Definition äquivalent zur Aussage, daß I als R-Modul endlich erzeugt ist. Ein gebrochenes Ideal I heißt *invertierbar*, wenn es ein gebrochenes Ideal I' gibt, so daß $I \cdot I' = R$.

Für ein ganzes Ideal $I \subseteq R$ definieren wir $I^{-1} = \{x \in K \mid xI \subseteq R\}$. Dies ist offensichtlich ein R-Untermodul von K. Für jedes $0 \neq y \in I$ gilt $yI^{-1} \subseteq R$, also ist I^{-1} ein gebrochenes Ideal und es gilt $I \cdot I^{-1} \subseteq R$. Da I ein Ideal ist, gilt $R \subseteq I^{-1}$ und damit $I = IR \subseteq I \cdot I^{-1} \subseteq R$. Ein ganzes Ideal I ist genau dann als gebrochenes Ideal invertierbar, wenn $I \cdot I^{-1} = R$.

Lemma 4.12. *Sei R ein Integritätsbereich, $I \subseteq R$ ein Ideal mit $I = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ für invertierbare Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \subseteq R$. Wenn es Primideale $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ gibt mit $I = \mathfrak{q}_1 \cdots \mathfrak{q}_m$, dann ist $m = n$ und $\mathfrak{q}_i = \mathfrak{p}_{\sigma(i)}$ für eine Permutation $\sigma \in S_n$.*

Beweis. Ohne Beschränkung der Allgemeinheit sei $\mathfrak{p}_1$ minimal unter den $\mathfrak{p}_i$ bezüglich Inklusion. Nach Voraussetzung ist $\mathfrak{p}_1 \supseteq \mathfrak{q}_1 \cdots \mathfrak{q}_m$.

Aus der Definition von Primideal folgt damit bereits $\mathfrak{p}_1 \supseteq \mathfrak{q}_i$ für ein i, ohne Beschränkung $i = 1$. Wenn nämlich $\mathfrak{q}_i \not\subseteq \mathfrak{p}_1$ für alle i, dann gibt es $x_i \in \mathfrak{q}_i \setminus \mathfrak{p}_1 \cap \mathfrak{q}_i$. Also ist $x_1 \cdots x_n \in \mathfrak{q}_1 \cdots \mathfrak{q}_m \subseteq \mathfrak{p}_1$, und wegen $\mathfrak{p}_1$ prim $x_i \in \mathfrak{p}_1$ für ein i. Widerspruch.

Ein symmetrisches Argument liefert $\mathfrak{q}_1 \supseteq \mathfrak{p}_i$ für ein i, wegen Minimalität ist $i = 1$, also $\mathfrak{p}_1 = \mathfrak{q}_1$. Nun nutzt man die Invertierbarkeit von $\mathfrak{p}_1$ und betrachtet $\mathfrak{p}_2 \cdots \mathfrak{p}_n = \mathfrak{p}_1^{-1} \cdot I = \mathfrak{q}_2 \cdots \mathfrak{q}_m$. Induktiv folgt die Behauptung. □

Lemma 4.13. *Sei R ein noetherscher Integritätsbereich, $0 \neq I \subsetneq R$ ein Ideal. Dann gibt es von* (0) *verschiedene Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ in R mit $I \subseteq \mathfrak{p}_i$ für alle i und $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq I$.*

Beweis. Sei $\mathcal{M} \neq \emptyset$ die Menge der Ideale, für die die Behauptung nicht gilt. Da R noethersch ist, existiert ein maximales $I \in \mathcal{M}$. Die Behauptung gilt offensichtlich für Primideale, also ist I nicht prim. Wir betrachten $x, y \in R \setminus I$ mit $xy \in I$, also $I + (x) \neq I$ und $I + (y) \neq I$. Aus der Maximalität von I folgt die Existenz von Primidealen $\mathfrak{p}_1, \ldots, \mathfrak{p}_n, \mathfrak{q}_1, \ldots, \mathfrak{q}_m$ mit

$$\mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq I + (x), \mathfrak{q}_1 \cdots \mathfrak{q}_m \subseteq I + (y), \text{ damit}$$

$$\mathfrak{p}_1 \cdots \mathfrak{p}_n \mathfrak{q}_1 \cdots \mathfrak{q}_m \subseteq (I + (x))(I + (y)) = I.$$

Dies ist ein Widerspruch. □

Satz 4.14. *Sei R ein Dedekind-Ring. Dann ist jedes maximale Ideal $\mathfrak{m} \subseteq R$ als gebrochenes Ideal invertierbar, d.h. $\mathfrak{m} \cdot \mathfrak{m}^{-1} = R$.*

Beweis. Da $\mathfrak{m}$ maximal ist, haben wir $\mathfrak{m}\mathfrak{m}^{-1} = \mathfrak{m}$ oder $\mathfrak{m}\mathfrak{m}^{-1} = R$.

Aus $\mathfrak{m}\mathfrak{m}^{-1} = \mathfrak{m}$ folgt $\mathfrak{m}\mathfrak{m}^{-n} = (\mathfrak{m}\mathfrak{m}^{-1})\mathfrak{m}^{-n+1} = \cdots = \mathfrak{m}$. Für $x \in \mathfrak{m}^{-1}$ und $0 \neq y \in \mathfrak{m}$ ist dann $x^n y \in \mathfrak{m}$ für alle n. Wir betrachten das Ideal $(x^n y \mid n \geq 0) \subseteq R$. Da R noethersch ist, ist dieses Ideal endlich erzeugt, es gibt also ein n mit $x^n y = \sum_{i=0}^{n-1} \lambda_i x^i y$. Dies liefert eine Ganzheitsgleichung für x, also ist x ganz über R. Da R ganz-abgeschlossen, ist $x \in R$. Damit folgt $R = \mathfrak{m}^{-1}$.

Sei nun $0 \neq a \in \mathfrak{m}$. Aus Lemma 4.13 folgt die Existenz von Primidealen $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ mit $\mathfrak{m} \supseteq (a) \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_n$. Wir können annehmen, daß n minimal ist. Wie im Beweis von Lemma 4.12 folgt $\mathfrak{p}_i \subseteq \mathfrak{m}$, da R Dedekind-Ring ist, gilt $\mathfrak{p}_i = \mathfrak{m}$. Dann ist $\mathfrak{m} \supseteq (a) \supseteq \mathfrak{m}I$ für $I = \mathfrak{p}_2 \cdots \mathfrak{p}_n$, und $I \not\subseteq (a)$ wegen Minimalität. Wir wählen $b \in I \setminus (a) \cap I$. Aus $\mathfrak{m}I \subseteq (a)$ folgt $\mathfrak{m}b \subseteq (a)$, also $\mathfrak{m}ba^{-1} \subseteq R$ und nach Definition ist $ba^{-1} \in \mathfrak{m}^{-1}$. Nach Wahl von b ist $b \notin (a)$, also $ba^{-1} \notin R$. Widerspruch. □

Satz 4.15. *Sei R ein Integritätsbereich. Dann sind die folgenden Aussagen äquivalent:*

(i) R ist ein Dedekind-Ring.

(ii) Jedes von 0 verschiedene Ideal I kann eindeutig als Produkt von Primidealen geschrieben werden:

$$I = \prod_{\mathfrak{p} \in \mathrm{Spec}(R) \setminus \{(0)\}} \mathfrak{p}^{v_\mathfrak{p}(I)}, \qquad v_\mathfrak{p}(I) \in \mathbb{Z} \text{ fast alle } 0.$$

(iii) Jedes von 0 verschiedene Ideal kann als Produkt von Primidealen geschrieben werden.

(iv) Die Menge der gebrochenen Ideale ungleich 0 ist eine Gruppe.

Beweis. (i) ⇒ (ii): Eindeutigkeit folgt aus der Existenz mit Lemma 4.12. Für $I = R$ ist die Aussage klar. Sei $(0) \subsetneq I \subsetneq R$, und seien $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ Primideale aus Lemma 4.13, so daß n minimal ist. Wenn $n = 1$ ist $I = \mathfrak{p}_1$.

Wir nehmen nun an, daß die Aussage für alle Ideale gilt, die ein Produkt von höchstens $n-1$ Primidealen enthalten. Sei $\mathfrak{m}$ ein maximales Ideal mit $\mathfrak{m} \supseteq I \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_n$. Dann ist wieder $\mathfrak{m} \supseteq \mathfrak{p}_i$ für ein i, ohne Beschränkung $i = n$. Da R Krull-Dimension 1 hat, ist $\mathfrak{m} = \mathfrak{p}_n$ und aus Satz 4.14 folgt

$$R = \mathfrak{m}\mathfrak{m}^{-1} \supseteq I\mathfrak{m}^{-1} \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_n \mathfrak{p}_n^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_{n-1}.$$

Nach Induktionsvoraussetzung ist $I\mathfrak{m}^{-1} = \mathfrak{q}_1 \cdots \mathfrak{q}_m$, also $I = \mathfrak{q}_1 \cdots \mathfrak{q}_m \mathfrak{m}$.

(ii) $\Rightarrow$ (iii) ist klar.

(iii) $\Rightarrow$ (iv): Für ein gebrochenes Ideal I existiert $d \in R$ mit $dI \subseteq R$, es ist also $I = (d)^{-1} \cdot dI$. Nach Voraussetzung sind (d) und dJ Produkte von Primidealen. Es reicht also zu zeigen, daß Primideale von R invertierbar sind.

Sei $\mathfrak{p}$ ein Primideal, $0 \neq a \in \mathfrak{p}$. Nach Voraussetzung ist $(a) = \mathfrak{p}_1 \cdots \mathfrak{p}_n$. Mit (a) sind auch alle $\mathfrak{p}_i$ invertierbar. Da $\mathfrak{p}$ prim ist, folgt aus $\mathfrak{p} \supseteq (a)$ auch $\mathfrak{p} \supseteq \mathfrak{p}_i$ für ein i. Es reicht also zu zeigen, daß invertierbare Primideale von R schon maximal sind.

Sei also $\mathfrak{p}$ ein invertierbares Primideal, und $a \in R \setminus \mathfrak{p}$. Dazu betrachten wir $I_1 = \mathfrak{p} + (a), I_2 = \mathfrak{p} + (a^2)$. Nach Voraussetzung ist

$$I_1 = \mathfrak{p}_1 \cdots \mathfrak{p}_n, I_2 = \mathfrak{q}_1 \cdots \mathfrak{q}_m,$$

wobei $\mathfrak{p}_i \supseteq I_1 \supseteq \mathfrak{p}$ und $\mathfrak{q}_i \supseteq I_2 \supseteq \mathfrak{p}$. Im Quotientenring $R/\mathfrak{p}$ sind die Bilder $(\overline{a})$ und $(\overline{a^2})$ invertierbare Ideale, damit sind auch die Ideale $\mathfrak{p}_i$ und $\mathfrak{q}_i$ invertierbar. Mit Lemma 4.12 (in $R/\mathfrak{p}$) ist $2m = n$ und $\mathfrak{q}_{2i-1} = \mathfrak{q}_{2i} = \mathfrak{p}_i$. Wir erhalten

$$\mathfrak{p} \subseteq \mathfrak{p} + (a^2) = (\mathfrak{p} + (a))^2 \subseteq \mathfrak{p}^2 + (a).$$

Jedes Element $x \in \mathfrak{p}$ kann also als $x = y + za$ mit $y \in \mathfrak{p}^2$ und $z \in R$ geschrieben werden. Aus $za = x - y \in \mathfrak{p}$ und $a \notin \mathfrak{p}$ folgt $z \in \mathfrak{p}$. Damit ist sogar $\mathfrak{p} \subseteq \mathfrak{p}^2 + \mathfrak{p}(a) = \mathfrak{p}(\mathfrak{p} + (a)) \subseteq \mathfrak{p}$. Aus der Gleichheit $\mathfrak{p} = \mathfrak{p}(\mathfrak{p} + (a))$ folgt mit Invertierbarkeit von $\mathfrak{p}$ schon $R = \mathfrak{p} + (a)$. Dies gilt für alle Elemente $a \in R \setminus \mathfrak{p}$, also ist $\mathfrak{p}$ maximal.

(iv) $\Rightarrow$ (i): Zuerst zeigen wir, daß R noethersch ist. Sei $I \subseteq R$ ein Ideal, I^{-1} sein Inverses. Aus $I \cdot I^{-1} = R$ folgt die Existenz von $x_1, \ldots, x_n \in I$, $y_1, \ldots, y_n \in I^{-1}$ mit $\sum x_i y_i = 1$. Für beliebiges $a \in I$ ist dann $a = \sum x_i (y_i a)$ mit $y_i a \in I^{-1} \cdot I = R$, also erzeugen die x_i schon I.

Als nächstes zeigen wir, daß R ganz-abgeschlossen ist. Sei K der Quotientenkörper von R, $x \in K$ ganz über R, d.h. $x^n + a_1 x^{n-1} + \cdots + a_n = 0$. Insbesondere liegt x^n im gebrochenen Ideal I, das von $1, x, \ldots, x^{n-1}$ erzeugt wird. Damit ist $I^2 \subseteq I$, und I invertierbar liefert $I \subseteq R$. Also ist $x \in R$ und R ganz-abgeschlossen.

Zuletzt die Krull-Dimension. Sei $(0) \neq \mathfrak{p} \subseteq R$ ein Primideal, $a \in R \setminus \mathfrak{p}$. Wir betrachten das Ideal $I = \mathfrak{p} + (a)$. Dieses ist invertierbar, also wegen $II^{-1}\mathfrak{p} = \mathfrak{p}$ auch $I^{-1}\mathfrak{p} \supseteq \mathfrak{p}$ und $I^{-1}\mathfrak{p} \subseteq I^{-1}I = R$. Für beliebiges $y \in I^{-1}\mathfrak{p}$ ist $ay \in \mathfrak{p}$, mit $a \notin \mathfrak{p}$ aber $y \in \mathfrak{p}$. Also $I^{-1}\mathfrak{p} = \mathfrak{p}$, und damit $I\mathfrak{p} = \mathfrak{p}$, d.h. $I = R$. Wieder gilt dies für alle $a \in R \setminus \mathfrak{p}$, also ist $\mathfrak{p}$ maximal. □

Korollar 4.16. *Sei R ein Dedekind-Ring. Dann kann jedes von 0 verschiedene gebrochene Ideal I eindeutig als Produkt von Primidealen geschrieben werden:*

$$I = \prod_{\mathfrak{p} \in \mathrm{Spec}(R) \setminus \{(0)\}} \mathfrak{p}^{v_\mathfrak{p}(I)}, \qquad v_\mathfrak{p}(I) \in \mathbb{Z} \text{ fast alle } 0.$$

Es ist $I \subseteq R$ genau dann, wenn für alle $\mathfrak{p}$ gilt $v_\mathfrak{p}(I) \geq 0$.

Korollar 4.17. *Sei R ein Dedekind-Ring, $I, J \subseteq R$ Ideale. Dann gilt*

$$I \cap J = \prod_\mathfrak{p} \mathfrak{p}^{\max(v_\mathfrak{p}(I), v_\mathfrak{p}(J))},$$

$$I + J = \prod_\mathfrak{p} \mathfrak{p}^{\min(v_\mathfrak{p}(I), v_\mathfrak{p}(J))}.$$

Beweis. Aus Satz 4.15 folgt, daß Inklusion von Idealen sich in $\geq$ der Exponenten übersetzt, also $I \subseteq J$ genau dann, wenn für alle $\mathfrak{p}$ gilt $v_\mathfrak{p}(I) \geq v_\mathfrak{p}(J)$.

Wir zeigen nur die erste Formel, die zweite wird analog bewiesen. Wegen $I \cap J \subseteq I$ ist $v_\mathfrak{p}(I \cap J) \geq v_\mathfrak{p}(I)$, analog $v_\mathfrak{p}(I \cap J) \geq v_\mathfrak{p}(J)$. Damit ist

$$I \cap J \subseteq \prod \mathfrak{p}^{\max(v_\mathfrak{p}(I), v_\mathfrak{p}(J))}.$$

Die umgekehrte Inklusion ist klar. □

Korollar 4.18. *Sei R ein Dedekind-Ring, $I \subseteq R$ ein Ideal. Dann ist*

$$R/I \cong \prod R/\mathfrak{p}^{v_\mathfrak{p}(I)}.$$

Beweis. Das ist der Chinesische Restsatz. □

Korollar 4.19. *Ein Dedekind-Ring R ist genau dann faktoriell, wenn R ein Hauptidealring ist.*

Beweis. Die Richtung $\Leftarrow$ ist klar. Sei also R faktoriell, $0 \neq \mathfrak{p}$ ein Primideal, $0 \neq a \in \mathfrak{p}$. Dann können wir $a = \prod_{i=1}^n p_i^{e_i}$ als Produkt von Primelementen schreiben, $n > 0, e_i \geq 1$. Da $\mathfrak{p}$ prim ist, gilt $p_i \in \mathfrak{p}$ für ein i. Da p_i ein Primelement ist, ist (p_i) ein Primideal und aus R Dedekind folgt $(p_i) = \mathfrak{p}$. Also sind alle Primideale Hauptideale. Ein beliebiges (von (0) verschiedenes) Ideal ist nach Satz 4.15 ein Produkt von Primidealen, also ebenfalls ein Hauptideal. □

Beispiel 4.20. *Es gibt Ganzheitsringe, die keine Hauptidealringe, also auch nicht faktoriell sind. Ein Beispiel hierfür ist*

$$\mathcal{O}_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}] = \mathbb{Z}[X]/(X^2+5).$$

Wir faktorisieren zunächst ein paar Ideale (p) für p eine Primzahl.

(i) $p = 2$*: Es gilt* $\mathbb{Z}[X]/(X^2+5, 2) = \mathbb{F}_2[X]/(X^2+1) = \mathbb{F}_2[X]/(X+1)^2$*. Wie im bereits besprochenen Fall* $\mathbb{Z}[i]$ *ist* (2) *Quadrat eines Primideals, hier* $(2, \sqrt{-5}+1)$*.*

(ii) $p = 3$*: Es gilt* $\mathbb{Z}[X]/(X^2+5, 3) = \mathbb{F}_3[X]/(X^2-1) = \mathbb{F}_3[X]/(X-1) \times \mathbb{F}_3[X]/(X+1)$*. Hier zerfällt* (3) *also in ein Produkt von zwei Primidealen:*

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

Dasselbe gilt für alle Primzahlen p, für die -5 modulo p ein Quadrat ist.

(iii) $p = 5$*: Wie im Fall* $p = 2$ *ist* $(5) = (\sqrt{-5})^2$ *das Quadrat eines Primideals.*

(iv) $p = 11$*: Es gilt* $\mathbb{Z}[X]/(X^2+5, 11) = \mathbb{F}_{11}[X]/(X^2+5)$*. Aber* -5 *ist kein Quadrat modulo* 11*, also ist* $\mathbb{F}_{11}[X]/(X^2+5) = \mathbb{F}_{121}$ *ein Körper und* $(11) \subseteq \mathbb{Z}[\sqrt{-5}]$ *auch ein Primideal.*

Als nächstes zeigen wir, daß $\mathfrak{p}_2 = (2, \sqrt{-5}+1)$ *kein Hauptideal ist. Nehmen wir an* $\mathfrak{p}_2 = (x)$*. Dann gibt es* $a, b \in \mathbb{Z}[\sqrt{-5}]$ *mit* $xa = 2$ *und* $xb = \sqrt{-5}+1$*. Wir betrachten die Normen dieser Elemente,* $N = N_{\mathbb{Q}(\sqrt{-5})/\mathbb{Q}}$*:*

$$N(x)N(a) = N(xa) = N(2) = 4, N(x)N(b) = N(xb) = N(\sqrt{-5}+1) = 6.$$

Also muß $N(a) = 2$ sein. Wenn $a = a_1 + a_2\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ Norm 2 hat, ist die Gleichung $a_1^2 + 5a_2^2 = 2$ in $\mathbb{Z}$ lösbar. Diese Gleichung ist aber offensichtlich nicht in $\mathbb{Z}$ lösbar, also ist $\mathfrak{p}_2$ kein Hauptideal.

Zuletzt zur Eindeutigkeit der Faktorisierung. Mit Hilfe von Normargumenten wie eben überzeugt man sich davon, daß die Elemente 2, 3, $\sqrt{-5}+1$ und $\sqrt{-5}-1$ alle irreduzibel sind. Dann läßt sich 6 auf zwei verschiedene Weisen in irreduzible Elemente faktorisieren:

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

Auf der Ebene der Primideale ist die Faktorisierung dann aber wieder eindeutig. Mit der Notation

$$\mathfrak{p}_2 = (2, \sqrt{-5} + 1) = (2, \sqrt{-5} - 1), \mathfrak{p}_{3a} = (3, \sqrt{-5} + 1), \mathfrak{p}_{3b} = (3, \sqrt{-5} - 1),$$

gilt dann $(\sqrt{-5}+1) = \mathfrak{p}_2\mathfrak{p}_{3a}$ und $(\sqrt{-5}-1) = \mathfrak{p}_2\mathfrak{p}_{3b}$. Damit ist die Faktorisierung von (6) in Primidealfaktoren wieder eindeutig (bis auf Reihenfolge der Faktoren):

$$(6) = \mathfrak{p}_2^2\mathfrak{p}_{3a}\mathfrak{p}_{3b}.$$

□

Umfangreichere Gesetzmäßigkeiten zur Zerlegung von Primidealen in Erweiterungen werden später diskutiert werden, cf. Kapitel 9. Hier betrachten wir nur noch die Zerlegung von Primzahlen in quadratischen Erweiterungen von $\mathbb{Z}$.

4.4 Beispiel: Quadratische Zahlkörper

Wir betrachten quadratische Zahlkörper $K = \mathbb{Q}(\sqrt{d})$. Es soll nun darum gehen, die Zerlegung von Idealen $I \subseteq \mathcal{O}_K$ in Primideale am Beispiel zu verstehen. Die interessantesten Ideale sind dabei von der Form (p) mit $p \in \mathbb{Z}$ eine Primzahl.

Wir haben bereits in Lemma 4.4 und Beispiel 4.20 gesehen, wie das geht. Zuerst geben wir eine Präsentation des Ganzheitsrings an.

Lemma 4.21. *Sei d quadratfrei, und $\mathcal{O}_K$ der Ganzheitsring des dazugehörigen quadratischen Zahlkörpers $K = \mathbb{Q}(\sqrt{d})$.*

(i) Wenn $d \equiv 2, 3 \mod 4$, dann ist $\mathcal{O}_K \cong \mathbb{Z}[X]/(X^2 - d)$.

(ii) Wenn $d \equiv 1 \mod 4$, dann ist $\mathcal{O}_K \cong \mathbb{Z}[X]/(X^2 - X + c)$, wobei $c = \frac{1-d}{4}$.

Beweis. (i) Nach Übungsaufgabe 3.1 ist $1, \sqrt{d}$ eine Ganzheitsbasis, also (additiv) $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d}$. Der Ringhomomorphismus $\mathbb{Z}[X] \to \mathcal{O}_K : X \mapsto \sqrt{d}$ induziert den behaupteten Isomorphismus.

(ii) Nach Übungsaufgabe 3.1 ist $1, \frac{1+\sqrt{d}}{2}$ eine Ganzheitsbasis. Das Minimalpolynom von $\frac{1+\sqrt{d}}{2}$ ist genau $X^2 - X + c$. Damit induziert der Ringhomomorphismus $\mathbb{Z}[X] \to \mathcal{O}_K : X \mapsto \frac{1+\sqrt{d}}{2}$ den behaupteten Isomorphismus. □

Wir bezeichnen mit $f_d(X)$ das jeweilige Polynom $f_d(X) = X^2 - d$ bzw. $f_d(X) = X^2 - X + c$ für $d \equiv 2, 3 \mod 4$ bzw. $d \equiv 1 \mod 4$. Die Primidealfaktorisierung kann jetzt mit

$$\mathcal{O}_K/(p) \cong \mathbb{Z}[X]/(f_d(X), p) \cong \mathbb{F}_p[X]/(f_d(X))$$

bestimmt werden, sie hängt also vom Zerlegungsverhalten des Polynoms $f_d(X)$ modulo p ab. Es gibt drei Fälle:

(i) $f_d(X)$ ist Quadrat eines linearen Polynoms. In diesem Fall heißt p *verzweigt* in $\mathbb{Q}(\sqrt{d})$, (p) ist Quadrat eines Primideals.

(ii) $f_d(X)$ ist irreduzibel. In diesem Fall heißt p *träge* in $\mathbb{Q}(\sqrt{d})$, (p) ist auch in $\mathcal{O}_K$ ein Primideal.

(iii) $f_d(X)$ zerfällt in zwei unterschiedliche Linearfaktoren. In diesem Fall heißt p *vollständig zerlegt* in $\mathbb{Q}(\sqrt{d})$, (p) ist ein Produkt von zwei verschiedenen Primidealen.

Diese Begriffe werden später noch ausführlicher diskutiert werden.

Wir machen die Fallunterscheidung p ungerade und $p = 2$.

Proposition 4.22. *Sei p eine ungerade Primzahl.*

(i) p ist verzweigt in $\mathbb{Q}(\sqrt{d})$ genau dann, wenn $p \mid d$.

(ii) p ist träge in $\mathbb{Q}(\sqrt{d})$ genau dann, wenn d kein Quadrat modulo p ist.

(iii) p ist vollständig zerlegt in $\mathbb{Q}(\sqrt{d})$ genau dann, wenn d ein Quadrat modulo p ist.

Beweis. Wir bezeichnen generell mit $\overline{x}$ die Restklasse von $x \in \mathbb{Z}$ in $\mathbb{F}_p$.

(i) Sei $d \equiv 2, 3 \mod 4$. Aus $X^2 - \overline{d} = (X + \overline{a})^2 = X^2 + 2\overline{a}X + \overline{a}^2$ folgt $\overline{a} = 0$ und $-\overline{d} = \overline{a}^2 = 0$, also $p \mid d$. Umgekehrt ist für $p \mid d$ auch $X^2 - \overline{d} = X^2$.

Sei $d \equiv 1 \mod 4$ und $c = \frac{1-d}{4}$. Aus $X^2 - X + \overline{c} = (X + \overline{a})^2 = X^2 + 2\overline{a}X + \overline{a}^2$ folgt $-1 = 2\overline{a}$ und $\overline{a}^2 = \overline{c}$. Zusammen also $4\overline{c} = (2\overline{a})^2 = 1$, und damit $\overline{d} = 0$, i.e. $p \mid d$. Umgekehrt ist für $p \mid d$ auch $4(X^2 - X + c) \equiv 4X^2 - 4X + 1 = (2X - 1)^2$ mod p, wegen p ungerade ist also p verzweigt.

(ii) und (iii): Sei $d \equiv 2, 3 \mod 4$ und $p \nmid d$. Dann zerfällt $X^2 - d$ modulo p genau dann in zwei verschiedene Linearfaktoren $(X - \sqrt{d})$ und $(X + \sqrt{d})$, wenn d ein Quadrat modulo p ist.

Sei $d \equiv 1 \mod 4$ und $p \nmid d$. Dann zerfällt $X^2 - X + c$ modulo p genau dann in zwei verschiedene Linearfaktoren $(X - \frac{1+\sqrt{d}}{2})$ und $(X + \frac{1+\sqrt{d}}{2})$, wenn d ein Quadrat modulo p ist. □

Proposition 4.23. *(i) 2 ist verzweigt in $\mathbb{Q}(\sqrt{d})$ genau dann, wenn $d \equiv 2, 3 \mod 4$ ist.*

(ii) 2 ist träge in $\mathbb{Q}(\sqrt{d})$ genau dann, wenn $d \equiv 5 \mod 8$.

(iii) 2 ist vollständig zerlegt in $\mathbb{Q}(\sqrt{d})$ genau dann, wenn $d \equiv 1 \mod 8$.

Beweis. Für $d \equiv 2, 3 \mod 4$ ist

$$\mathcal{O}_K/(2) \cong \mathbb{F}_2[X]/(X^2 - d) \cong \begin{cases} \mathbb{F}_2[X]/(X^2) & d \equiv 2 \mod 4 \\ \mathbb{F}_2[X]/(X+1)^2 & d \equiv 3 \mod 4 \end{cases}$$

In diesem Fall ist 2 verzweigt.

Für $d \equiv 1 \mod 4$ ist

$$\mathcal{O}_K/(2) \cong \mathbb{F}_2[X]/(X^2 - X + c) \cong \begin{cases} \mathbb{F}_2[X]/(X^2 - X) & d \equiv 1 \mod 8 \\ \mathbb{F}_2[X]/(X^2 + X + 1) & d \equiv 5 \mod 8 \end{cases}$$

Das Polynom $X^2 + X + 1$ ist irreduzibel über $\mathbb{F}_2$, damit ist 2 für $d \equiv 5 \mod 8$ träge. Das Polynom $X^2 - X$ hat zwei unterschiedliche Linearfaktoren, also ist 2 für $d \equiv 1 \mod 8$ vollständig zerlegt. □

Es bleibt also die Frage zu untersuchen, wann d ein Quadrat modulo p ist. Dafür betrachtet man das Legendre-Symbol.

Definition 4.24. *Sei p eine ungerade Primzahl und a eine zu p teilerfremde ganze Zahl. Das* Legendre-Symbol *ist definiert durch*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & x^2 \equiv a \mod p \text{ lösbar} \\ -1 & x^2 \equiv a \mod p \text{ nicht lösbar} \end{cases}$$

Im Wesentlichen gibt das Legendre-Symbol die Restklasse von a in der Gruppe $\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 \cong \mathbb{Z}/2\mathbb{Z}$ der Quadratreste an. Proposition 4.22 kann dann umformuliert werden: Eine Primzahl $p \nmid d$ ist genau dann träge, wenn $\left(\frac{d}{p}\right) = -1$ und genau dann vollständig zerlegt, wenn $\left(\frac{d}{p}\right) = 1$.

Zur Berechnung des Legendre-Symbols gelten folgende Gesetzmäßigkeiten:

Proposition 4.25. *(i) Das Legendre-Symbol ist multiplikativ, d.h.*

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

(ii) (Gaußsches Reziprozitätsgesetz) *Für zwei verschiedene ungerade Primzahlen l und p gilt*

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

(iii) (Ergänzungssätze)

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Den Beweis führen wir hier nicht, cf. [Neu92, Theorem I.8.6]. Wir werden in Proposition 9.36 noch einen Beweis sehen, der auf der Faktorisierung von Idealen in Ganzheitsringen zyklotomischer Körper basiert.

Übungsaufgaben

Übungsaufgabe 4.3. *Zeigen Sie: Für ζ_3 eine primitive dritte Einheitswurzel ist $\mathbb{Z}[\zeta_3]$ ein Hauptidealring. Betrachten Sie dazu die Normabbildung*

$$N : \mathbb{Q}(\zeta_3) \setminus \{0\} \to \mathbb{Q} : x \mapsto x\overline{x}$$

und zeigen Sie die folgenden Aussagen:

1. *Für alle $a, b \in \mathbb{Z}[\zeta_3] \setminus \{0\}$ ist $N(ab) \geq N(a)$.*
2. *Für alle $a, b \in \mathbb{Z}[\zeta_3]$ mit $a \neq 0$ existieren $q, r \in \mathbb{Z}[\zeta_3]$, so daß $b = aq + r$ und $N(r) < N(a)$ gelten. (Division mit Rest)*

3. Folgern Sie daraus die Behauptung.

Übungsaufgabe 4.4. *Sei $f : A \to B$ ein Ringhomomorphismus. Zeigen Sie die folgenden Aussagen:*

(i) Sei $a \in A$ nilpotent. Dann ist $a \in \mathfrak{p}$ für alle Primideale $\mathfrak{p}$.

(ii) Sei $\mathfrak{p} \subseteq B$ prim. Dann ist $f^{-1}(\mathfrak{p})$ prim.

Gilt die Umkehrung von (i)? Gilt (ii) auch für maximale Ideale?

Übungsaufgabe 4.5. *Sei R ein Ring und $I \subseteq R$ ein Ideal. Zeigen Sie, daß es eine bijektive Abbildung zwischen der Menge der Ideale von A/I und Menge der Ideale von R, die I enthalten. Zeigen Sie, daß dies auch für Primideale gilt.*

Übungsaufgabe 4.6. *Sei R ein Ring. Für ein Ideal I definieren wir das* Radikal *von I wie folgt:*

$$\sqrt{I} = \{x \in R \mid \exists n > 0 : x^n \in I\}.$$

Zeigen Sie

(i) $\sqrt{I} \supseteq I$,

(ii) $\sqrt{\sqrt{I}} = \sqrt{I}$,

(iii) $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$,

(iv) falls $\mathfrak{p}$ prim ist, gilt $\sqrt{\mathfrak{p}} = \mathfrak{p}$.

Übungsaufgabe 4.7. *Sei R ein Ring, $\mathfrak{a}, \mathfrak{b}$ und $\mathfrak{c}$ Ideale in R.*

(i) Zeigen Sie $\mathfrak{a} \cdot (\mathfrak{b} + \mathfrak{c}) = (\mathfrak{a} \cdot \mathfrak{b}) + (\mathfrak{a} \cdot \mathfrak{c})$.

(ii) Sei R ein Dedekind-Ring. Zeigen Sie

$$\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = (\mathfrak{a} \cap \mathfrak{b}) + (\mathfrak{a} \cap \mathfrak{c}), \qquad \mathfrak{a} + (\mathfrak{b} \cap \mathfrak{c}) = (\mathfrak{a} + \mathfrak{b}) \cap (\mathfrak{a} + \mathfrak{c}).$$

Übungsaufgabe 4.8. *Sei $K = \mathbb{Q}(\sqrt[3]{2})$. Geben Sie die Primidealfaktorisierung von (7) und (31) in $\mathcal{O}_K$ an. Dabei dürfen Sie annehmen, daß $1, \sqrt[3]{2}, \sqrt[3]{4}$ eine Ganzheitsbasis ist. Erläutern Sie, wo genau diese Voraussetzung benutzt wird.*

Übungsaufgabe 4.9. *(i) Berechnen Sie die folgenden Legendre-Symbole:*

$$\left(\frac{6}{11}\right), \qquad \left(\frac{18}{23}\right), \qquad \left(\frac{205}{307}\right).$$

(ii) Ist (2311) prim in $\mathbb{Z}[\sqrt{1965}]$?

Übungsaufgabe 4.10. *Zeigen Sie, daß $\mathbb{Z}[X]$ kein Dedekind-Ring ist. Geben Sie dazu ein nicht-invertierbares Ideal an.*

Übungsaufgabe 4.11. *Sei R ein Dedekind-Ring. Zeigen Sie, daß jedes Ideal von zwei Elementen erzeugt werden kann.*

Übungsaufgabe 4.12. *Zeigen Sie, daß ein Dedekind-Ring mit endlich vielen Primidealen schon ein Hauptidealring ist.*

Übungsaufgabe 4.13. *Sei* $K = \mathbb{Q}(\sqrt{-5})$, $\mathfrak{m} = (2, \sqrt{-5} + 1)$. *Geben Sie eine* $\mathbb{Z}$*-Basis für* $\mathfrak{m}^{-1}$ *an.*

Übungsaufgabe 4.14. *Sei* $K = \mathbb{Q}(\theta)$ *ein Zahlkörper vom Grad* n, $\mathrm{Min}(\theta)$ *das Minimalpolynom von* θ, *und* p *eine Primzahl mit* $p \nmid D(1, \theta, \ldots, \theta^{n-1})$. *Zeigen Sie*

$$\mathcal{O}_K/(p) \cong \mathbb{F}_p[\theta] = \mathbb{F}_p[X]/(\mathrm{Min}(\theta)).$$

Kapitel 5

Algorithmen I

In diesem Kapitel beschäftigen wir uns mit der algorithmischen Seite der Fragestellungen aus Kapitel 3 und Kapitel 4. Ganzheitsbasen von Zahlkörpern kann man zum Beispiel mit dem Round-two-Algorithmus von Zassenhaus berechnen. Außerdem diskutieren wir, wie Ideale und Idealoperationen dargestellt werden können und geben Algorithmen an, mit denen man Faktorisierungen von Polynomen über endlichen Körpern ausrechnen kann.

Ein Algorithmus ist eine endlich formulierbare Vorschrift zur Lösung eines Problems. Die Behauptung "Algorithmus A löst Problem P" umfaßt dabei zwei Teilbehauptungen: Terminierung und Korrektheit. Terminierung ist dabei die Aussage, daß der Algorithmus für jede mögliche Eingabe nach endlich vielen Schritten ein Ergebnis liefert. Korrektheit ist die Aussage, daß dieses Ergebnis auch wirklich eine Lösung des Ausgangsproblems ist.

Man kann zwischen deterministischen und probabilistischen Algorithmen unterscheiden. Ein Algorithmus ist deterministisch, wenn zu jedem Zeitpunkt der nächste auszuführende Schritt eindeutig bestimmt ist. Andernfalls enthält die Wahl des nächsten Schrittes ein Zufallselement und man spricht von randomisierten oder probabilistischen Algorithmen.

Unter der Komplexität eines Algorithmus versteht man eine Abschätzung des Zeit- und Platzbedarfs des Algorithmus in Abhängigkeit von der Größe der Eingabe. Für probabilistische Algorithmen ersetzt man Zeit- und Platzbedarf durch entsprechende Erwartungswerte.

5.1 Berechnung von Ganzheitsbasen

In diesem Abschnitt geht es um die theoretischen Grundlagen des Round-Two-Algorithmus von Zassenhaus. Wir betrachten einen Zahlkörper K. Eine *$\mathbb{Z}$-Ordnung in K* ist ein Unterring von K, dessen Elemente ganz sind und der als $\mathbb{Z}$-Untermodul von K maximalen Rang hat. Jede Ordnung ist in einer maximalen Ordnung enthalten. Für Zahlkörper gibt es nur eine maximale Ordnung, den Ganzheitsring $\mathcal{O}_K$. Für ein irreduzibles normiertes Polynom $f(X) \in \mathbb{Z}[X]$ ist $\mathbb{Z}[X]/f(X)\mathbb{Z}[X]$ eine Ordnung in $\mathbb{Q}[X]/f(X)\mathbb{Q}[X]$. Der Ansatz zur algorithmischen Berechnung von Ganzheitsbasen ist dann, mit einer solchen Ordnung anzufangen und sie zu einer maximalen Ordnung zu erweitern. Wie wir bereits

gesehen haben, sind dafür die Primzahlen p relevant, für die p^2 die Diskriminante von f (also die Diskriminante einer $\mathbb{Z}$-Basis von $\mathbb{Z}[X]/f(X)\mathbb{Z}[X]$) teilt.

Definition 5.1. *Sei K ein Zahlkörper, $\mathcal{O}$ eine Ordnung in K und p eine Primzahl. Die Ordnung $\mathcal{O}$ heißt* p-maximal*, wenn $p \nmid [\mathcal{O}_K : \mathcal{O}]$. Das* p-Radikal $I_p(\mathcal{O})$ *von $\mathcal{O}$ ist definiert durch $I_p(\mathcal{O}) = \{x \in \mathcal{O} \mid \exists m \geq 1 : x^m \in p\mathcal{O}\}$. Der zu $I_p(\mathcal{O})$ gehörende* Ring der Multiplikatoren *ist definiert durch*

$$[I_p(\mathcal{O})/I_p(\mathcal{O})] = \{x \in K \mid xI_p(\mathcal{O}) \subseteq I_p(\mathcal{O})\}.$$

Die zur Ordnung $\mathcal{O}$ gehörende p-maximale Überordnung *ist definiert durch*

$$\mathcal{O}_p = \{x \in \mathcal{O}_K \mid \exists j \geq 1 : p^j x \in \mathcal{O}\}.$$

Übungsaufgabe 5.1. *Sei $\mathcal{O}$ eine Ordnung. Zeigen Sie, daß $\mathcal{O}_p$ eine Ordnung ist, daß $p \nmid [\mathcal{O}_K : \mathcal{O}_p]$ und daß $[\mathcal{O}_p : \mathcal{O}]$ eine p-Potenz ist.*

Die Bestimmung einer Maximalordnung kann "lokal", d.h. Primzahl für Primzahl, erfolgen. Um die p-maximalen Ordnungen zu bestimmen, wird der Satz von Pohst-Zassenhaus benutzt, den wir im Folgenden beweisen wollen.

Proposition 5.2. *Sei K ein Zahlkörper, $\mathcal{O}$ eine Ordnung in K und p eine Primzahl. Dann gilt:*

(i) $I_p(\mathcal{O})$ ist ein Ideal in $\mathcal{O}$.

(ii) $I_p(\mathcal{O})$ ist das Produkt $\prod \mathfrak{p}_i$ aller Primideale $\mathfrak{p}_i$ von $\mathcal{O}$, die (p) enthalten.

(iii) Es existiert ein m so daß $I_p(\mathcal{O})^m \subseteq p\mathcal{O}$.

Beweis. (i) Mit $x^m, y^n \in p\mathcal{O}$ folgt aus dem binomischen Satz $(x+y)^{n+m} \in p\mathcal{O}$, damit ist $I_p(\mathcal{O})$ unter Addition abgeschlossen.

(ii) Für $x \in I_p(\mathcal{O})$ ist $x^m \in p\mathcal{O} \subseteq \mathfrak{p}_i$, also auch $x \in \mathfrak{p}_i$ für alle Primideale $\mathfrak{p}_i \supseteq (p)$. Da die verschiedenen Primideale paarweise teilerfremd sind, ist $x \in \bigcap \mathfrak{p}_i = \prod \mathfrak{p}_i$.

Sei umgekehrt $x \in \prod \mathfrak{p}_i$. Wir rechnen in $R = \mathcal{O}/p\mathcal{O}$ und wollen in diesem Ring $\overline{x}^n = 0$ zeigen. Der Ring R hat nur endlich viele Ideale, es ist also $(\overline{x}^n) = (\overline{x}^{n+1})$ für ein n, d.h. $\overline{x}^n(1-\overline{x}y) = 0$ für $y \in R$. Da $\overline{x}$ in allen maximalen Idealen von R enthalten ist, kann $(1-\overline{x}y)$ in keinem maximalen Ideal enthalten sein, ist also invertierbar und wir erhalten $\overline{x}^n = 0$, d.h. $x^n \in p\mathcal{O}$.

(iii) Das Ideal $I_p(\mathcal{O})$ ist als $\mathbb{Z}$-Modul endlich erzeugt. Für eine endliche $\mathbb{Z}$-Basis $x_1, \ldots, x_n$ hat man m_i so daß $x_i^{m_i} \in p\mathcal{O}$. Für $m = \sum m_i$ gilt dann $I_p(\mathcal{O})^m \subseteq p\mathcal{O}$. □

Satz 5.3 (Pohst-Zassenhaus)**.** *Sei K ein Zahlkörper, $\mathcal{O}$ eine Ordnung in K und p eine Primzahl. Dann gilt genau eine der folgenden Aussagen:*

(i) $[I_p(\mathcal{O})/I_p(\mathcal{O})] = \mathcal{O}$ ist p-maximal.

(ii) $[I_p(\mathcal{O})/I_p(\mathcal{O})] \supsetneq \mathcal{O}$ und $p \mid [[I_p(\mathcal{O})/I_p(\mathcal{O})] : \mathcal{O}] \mid p^n$.

Beweis. Wir bezeichnen $I_p = I_p(\mathcal{O})$ und $\mathcal{O}' = [I_p(\mathcal{O})/I_p(\mathcal{O})]$. Da I_p ein Ideal ist, gilt $\mathcal{O} \subseteq \mathcal{O}'$. Da $p \in I_p$ gilt für $x \in \mathcal{O}'$ auch $xp \in I_p \subseteq \mathcal{O}$, also ist $\mathcal{O} \subseteq \mathcal{O}' \subseteq \frac{1}{p}\mathcal{O}$. Damit ist $\mathcal{O}'$ eine Ordnung und $[\mathcal{O}' : \mathcal{O}] \mid p^n$.

Sei nun $\mathcal{O}' = \mathcal{O}$. Wir betrachten die p-maximale Überordnung $\mathcal{O}_p$. Wie im Beweis von Proposition 5.2 gilt $p^r\mathcal{O}_p \subseteq \mathcal{O}$ für geeignetes r. Mit $I_p^m \subseteq p\mathcal{O}$ gilt also $\mathcal{O}_p I_p^{mr} \subseteq \mathcal{O}$. Nehmen wir nun an, daß $\mathcal{O}_p \neq \mathcal{O}$ ist. Sei n maximal mit der Eigenschaft $\mathcal{O}_p I_p^n \not\subseteq \mathcal{O}$ (also $\mathcal{O}_p I_p^{n+1} \subseteq \mathcal{O}$), und sei $x \in \mathcal{O}_p I_p^n \setminus \mathcal{O}$. Dann ist $xI_p \subseteq \mathcal{O}$ und für $y \in I_p$ gilt wegen $(xy)^{n+m+1} \in p\mathcal{O}$ auch $xy \in I_p$. Das heißt $xI_p \subseteq I_p$, also $x \in \mathcal{O}' = \mathcal{O}$ im Widerspruch zur Annahme. Die Ordnung $\mathcal{O}'$ ist also p-maximal. □

Lemma 5.4. *Sei K ein Zahlkörper vom Grad $[K:\mathbb{Q}] = n$, $\mathcal{O}$ eine Ordnung in K und $j \in \mathbb{N}$ so daß $p^j \geq n$. Dann ist $I_p(\mathcal{O})/pI_p(\mathcal{O}) = \ker\left(x \mapsto x^{p^j}\right)$.*

Lemma 5.5. *Sei K ein Zahlkörper und $\mathcal{O}$ eine Ordnung in K. Wir betrachten die Abbildung $m : \mathcal{O} \to \mathrm{End}(I_p(\mathcal{O})/pI_p(\mathcal{O})) : \alpha \mapsto (\overline{\beta} \mapsto \overline{\alpha\beta})$. Dann ist $[I_p(\mathcal{O})/I_p(\mathcal{O})] = \frac{1}{p}\ker m$.*

Die algorithmische Realisierung der in den Lemmata beschriebenen Schritte wollen wir hier nicht ausführlicher besprechen. Die Schritte sind lineare Algebra über dem endlichen Körper $\mathbb{F}_p$, man braucht also im Wesentlichen den Gauß-Algorithmus.

Beispiel 5.6. *Wir betrachten das Polynom $f(X) = X^3 + 17X^2 - 2X + 9$. Für eine Wurzel θ von $f(X) = 0$ sind Spurpaarung und Diskriminante der Ordnung $\mathbb{Z}[\theta]$ wie folgt gegeben:*

$$D(1,\theta,\theta^2) = \det\begin{pmatrix} 3 & -17 & 293 \\ -17 & 293 & -5042 \\ 293 & -5042 & 86453 \end{pmatrix} = -3^2 \cdot 5^3 \cdot 163.$$

Interessant sind hier also die Primzahlen $p = 3$ und $p = 5$.

(i) Wir faktorisieren das Ideal (3):

$$\mathbb{Z}[X]/(X^3+17^2-2X+9, 3) \cong \mathbb{F}_3[X]/(X(X+1)^2) \cong \mathbb{F}_3 \times \mathbb{F}_3[X]/((X+1)^2).$$

Also ist das Radikal $I_3(\mathbb{Z}[\theta]) = (3,\theta)(3,\theta+1)$. Der Kern der Abbildung

$$\mathcal{O}/p\mathcal{O} \cong \mathbb{F}_3[X]/(X(X+1)^2) \to \mathrm{End}(I_3/3I_3)$$

ist das von $X(X+1) = X^2 + X$ erzeugte Ideal. Nach dem Lemma ist die neue Basis $1, \theta, \frac{\theta^2+\theta}{3}$. In der neuen Ordnung kommt 3 nicht mehr in der Diskriminante vor, die Ordnung ist also 3-maximal.

(ii) Wir faktorisieren das Ideal (5):

$$\mathbb{Z}[X]/(X^3 + 17X^2 - 2X + 9, 5) \cong \mathbb{F}_5[X]/((X+4)^3).$$

Also ist das Radikal $I_5(\mathbb{Z}[\theta]) = (5, \theta+4)$. Der Kern des Homomorphismus $\mathcal{O}/5\mathcal{O} \to \mathrm{End}(I_5/5I_5)$ ist ein Ideal in $\mathbb{F}_5[X]/(X+4)^3$. Offensichtlich ist dieser Kern das von $(X+4)^2 \equiv X^2 - 2X + 1 \mod 5$ erzeugte Ideal. Wir erhalten also mit dem Lemma die neue Basis $1, \theta, \frac{\theta^2-2\theta+1}{5}$. In der neuen Ordnung kommt 5 nur noch mit Multiplizität 1 vor, also ist diese Ordnung 5-maximal.

□

Wenn man für jede Primzahl p die Ordnung $\mathcal{O}$ zu einer p-maximalen Ordnung $\mathcal{O}_p$ erweitert hat, kann man die Ergebnisse wie folgt zusammensetzen, dabei bezeichnet S die Menge der Primzahlen, die die Diskriminante der Ordnung $\mathcal{O}$ mindestens quadratisch teilen.

Lemma 5.7. *Sei K ein Zahlkörper, $\mathcal{O}$ eine Ordnung in K mit Diskriminante $d_{\mathcal{O}}$, und S die Menge der Primzahlen p mit $p^2 \mid d_{\mathcal{O}}$. Dann gilt*

$$\mathcal{O}_K/\mathcal{O} = \bigoplus_{p \in S} \mathcal{O}_p/\mathcal{O}.$$

Dies ist eine direkte Konsequenz des Elementarteilersatzes Satz A.14. Nehmen wir an, daß wir bereits für alle $p \in S$ Basen $x_{p1}, \ldots, x_{pn}$ von $\mathcal{O}_p$ in Hermite-Normalform bezüglich der Basis $1, \theta, \ldots, \theta^{n-1}$ gegeben haben, d.h.

$$x_{pi} = \sum_{k=1}^{i} \lambda_{pik}\theta^{k-1}, \lambda_{pik} \in \mathbb{Q}, \lambda_{pii}^{-1} = p^{m_{pi}}, m_{pi} \in \mathbb{Z}^{\geq 0}, p^{m_{pi}}\lambda_{pik} \in \mathbb{Z}.$$

Aus dem chinesischen Restsatz folgt die Existenz von μ_{pi} mit

$$\sum_{p \in S} \mu_{pi} \prod_{q \in S, q \neq p} q^{m_{qi}} = 1.$$

Als Basis für $\mathcal{O}_K$ kann man dann die folgenden Linearkombinationen wählen:

$$x_i = \sum_{p \in S} \mu_{pi} x_{pi}.$$

Beispiel 5.8. *Wir beenden das begonnene Beispiel $f(X) = X^3 + 17X^2 - 2X + 9$, wir haben bereits*

$$\mathcal{O}_3 = \mathbb{Z} \oplus \mathbb{Z}\theta \oplus \mathbb{Z}\frac{\theta^2 + \theta}{3}, \mathcal{O}_5 = \mathbb{Z} \oplus \mathbb{Z}\theta \oplus \mathbb{Z}\frac{\theta^2 - 2\theta + 1}{5}.$$

Die ersten beiden Basiselemente sind damit 1 und θ. Für das letzte Basiselement ist $\mu_{33} = -1$ und $\mu_{53} = 2$, da $(-1)\cdot 5 + 2\cdot 3 = 1$. Als letztes Basiselement können wir also das folgende Element wählen:

$$x_3 = -\frac{\theta^2 + \theta}{3} + 2\frac{\theta^2 - 2\theta + 1}{5} = \frac{\theta^2 - 17\theta + 6}{15}.$$

□

Zum Schluss gibt es noch ein einfaches Kriterium von Dedekind, mit dem man bestimmen kann, ob eine Ordnung der Form $\mathbb{Z}[\theta]$ schon p-maximal ist.

Satz 5.9 (Dedekind-Kriterium)**.** *Sei $K = \mathbb{Q}(\theta)$ ein Zahlkörper, $f(X) \in \mathbb{Z}[X]$ das Minimalpolynom von θ und p eine Primzahl. Sei $\overline{f}(X) = \prod_{i=1}^{k} \overline{f_i}(X)^{e_i}$ die Faktorisierung von $f(X)$ in $\mathbb{F}_p[X]$ und $g(X) = \prod_{i=1}^{k} f_i(X)$. Dann gilt*

(i) Das p-Radikal I_p von $\mathbb{Z}[\theta]$ ist durch $I_p = p\mathbb{Z}[\theta] + g(\theta)\mathbb{Z}[\theta]$ gegeben.

(ii) *Sei* $\mathcal{O}' = \{x \in K \mid xI_p \subseteq I_p\}$, $h(X)$ *ein normierter Lift von* $\overline{f}(X)/\overline{g}(X)$. *Wir setzen* $\Delta(X) = (g(X)h(X) - f(X))/p$. *Sei* $F(X)$ *ein normierter Lift von* $\overline{f}(X)/ggT(\overline{g}, \overline{h}, \overline{\Delta})$. *Dann ist*

$$\mathcal{O}' = \mathbb{Z}[\theta] + \frac{1}{p}F(\theta)\mathbb{Z}[\theta].$$

Mit $m = \deg ggT(\overline{g}, \overline{h}, \overline{\Delta})$ *ist* $[\mathcal{O}' : \mathbb{Z}[\theta]] = p^m$.

(iii) *Insbesondere ist* $\mathbb{Z}[\theta]$ *genau dann* p*-maximal, wenn* $m = 0$.

Für einen ausführlichen Beweis verweisen wir auf [Coh93, Theorem 6.1.4]. Hier wollen wir nur ein Beispiel betrachten.

Beispiel 5.10. *Wir betrachten die verschiedenen Schritte am Beispiel des Zahlkörpers* $\mathbb{Q}(\sqrt[3]{175})$. *Die Matrix der Spurpaarung und Diskriminante der Potenzbasis* $1, \theta, \theta^2$ *mit* $\theta = \sqrt[3]{175}$ *sind*

$$\det \begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 525 \\ 0 & 525 & 0 \end{pmatrix} = -3^3 5^4 7^2.$$

Wir betrachten zuerst den Dedekind-Test für $f(X) = X^3 - 175$ *an verschiedenen Primzahlen.*

(i) $p = 2$*: In diesem Fall ist* $f(X) \equiv (X+1)(X^2+X+1) \mod 2$, *also* $g(X) = (X+1)(X^2+X+1)$. *Wir können als normierten Lift von* $\overline{f}(X)/\overline{g}(X)$ *schon* $h(X) = 1$ *wählen. Im Kriterium ist* $\Delta(X) = (g(X) - f(X))/2 = X^2 + X + 88$. *Wegen* $h(X) = 1$ *ist aber* $ggT(\overline{g}, \overline{h}, \overline{\Delta}) = 1$ *und die Potenzordnung* $\mathbb{Z}[\theta]$ *ist* 2*-maximal.*

(ii) $p = 3$*: In diesem Fall ist* $f(X) \equiv (X+2)^3 \mod 3$, *also* $g(X) = X + 2$. *Wir wählen als normierten Lift* $h(X) = X^2 + X + 1 \equiv (X+2)^2 \mod 3$. *Dann ist* $\Delta(X) = (g(X)h(X) - f(X))/3 = X^2 + X + 59$. *Dieses Polynom ist unzerlegbar modulo* 3, *also ist wieder* $ggT(\overline{g}, \overline{h}, \overline{\Delta}) = 1$ *und die Potenzordnung* $\mathbb{Z}[\theta]$ *ist* 3*-maximal.*

(iii) $p = 5$*: In diesem Fall ist* $f(X) \equiv X^3 \mod 5$, *also* $g(X) = X$. *Als normierten Lift können wir* $h(X) = X^2$ *wählen. Dann ist* $\Delta(X) = (g(X)h(X) - f(X))/5 = 35 \equiv 0 \mod 5$. *Hier ist also* $ggT(\overline{g}, \overline{h}, \overline{\Delta}) = X$ *nicht-trivial. Wir wählen* $F(X) = X^2$ *und erhalten (mit* $\sqrt[3]{175^2} = 5\sqrt[3]{245}$*) als Zwischenordnung* $\mathcal{O}' = \mathbb{Z}[\theta] + \sqrt[3]{245}\mathbb{Z}[\theta]$.

(iv) *Wir lassen den Fall* $p = 7$ *weg, wie im Fall* $p = 3$ *zeigt man, daß die Ordnung* 7*-maximal ist. Damit haben wir alle relevanten Primzahlen abgearbeitet.*

Wir wollen noch zeigen, daß die gefundene Ordnung mit Basis $1, \sqrt[3]{175}, \sqrt[3]{245}$ *schon gleich dem Ganzheitsring* $\mathcal{O}_K$ *ist, d.h. auch* 5*-maximal ist. Diese Ordnung enthält offensichtlich die Ordnung* $\mathbb{Z}[\sqrt[3]{245}]$. *Letztere ist* 5*-maximal, was man auch wieder mit dem Dedekind-Kriterium sehen kann: in diesem Fall ist* $\Delta(X) = 49 \equiv 4 \mod 5$ *und* $ggT(\overline{g}, \overline{h}, \overline{\Delta}) = 1$. *Damit ist also die gefundene Ordnung maximal. Die Diskriminante von* $\mathbb{Q}(\sqrt[3]{175})$ *ist dann* $-3^3 5^2 7^2$. □

Damit haben wir alle Bestandteile des Round-Two-Algorithmus beisammen, um den groben Ablauf des Algorithmus zu formulieren. Für eine detailliertere Umsetzung der linearen Algebra in den einzelnen Schritten verweisen wir auf [Coh93, Kapitel 6.1].

Korrektheit des Algorithmus folgt bereits aus den vorherigen Aussagen. Außerdem werden nur endlich viele Schritte benötigt: es gibt nur endlich viele Primzahlen p, so daß die Ordnung nicht p-maximal ist, für jede Primzahl gibt es nur endlich viele Überordnungen, die zu berechnen sind, bis man bei einer p-maximalen Ordnung angekommen ist. Die Komplexität des Algorithmus ist vergleichbar mit derjenigen der Primfaktorisierung der Diskriminante der Potenzbasis $\mathbb{Z}[\theta]$, detailliertere Angaben ersparen wir uns.

Eingabe: Minimalpolynom einer algebraischen Zahl θ, $K = \mathbb{Q}(\theta)$
Ausgabe: Ganzheitsbasis für $\mathcal{O}_K$ und Diskriminante d_K
faktorisiere $D(1, \theta, \ldots, \theta^{n-1}) = D_0 S^2$;
beginne mit Basis θ^{i-1};
while $S \neq 1$ **do**
  $p \longleftarrow$ kleinste Primzahl mit $p \mid S$;
  if *Dedekind-Test zeigt* $\mathbb{Z}[\theta]$ *nicht p-maximal* **then**
    repeat
      Anwendung Lemma 5.4: Berechnung $\mathbb{F}_p$-Basis von I_p/pI_p;
      Anwendung Lemma 5.5: Berechnung $\mathbb{Z}$-Basis von
      $U = \ker(\mathcal{O} \to \mathrm{End}(I_p/pI_p))$;
      neue Ordnung $\mathcal{O}' = U/p$ dargestellt durch Basis x_{pi};
    until *neue Ordnung* $\mathcal{O}'$*=alte Ordnung* $\mathcal{O}$;
  end
  $S \longleftarrow S/p^{v_p(S)}$;
end
Zusammensetzen der Basis x_i aus x_{pi} mit chin. Restsatz;
die x_i bilden eine Ganzheitsbasis in HNF bzgl. θ;
$d_K = D(1, \theta, \ldots, \theta^{n-1}) \cdot G^2$, G die Determinante der Matrix der ω_i;

Algorithm 1: Round-Two-Algorithmus

5.2 Darstellung von Idealen und Idealoperationen

Sei $K = \mathbb{Q}(\theta)$ ein Zahlkörper. Ein Element $x \in K$ kann als Linearkombinationen von Potenzen von θ oder über die darstellende Matrix zur Multiplikation m_x repräsentiert werden. Ein gebrochenes Ideal I in K kann durch Angabe einer $\mathbb{Z}$-Basis $x_1, \ldots, x_n$ von I repräsentiert werden, und jedes Element x_i der Basis als $\mathbb{Q}$-Linearkombination von Potenzen von θ. Wir können gebrochene Ideale in K also durch Matrizen in $M_n(\mathbb{Q})$ repräsentieren, wobei $n = [K : \mathbb{Q}]$. Eine direkte Konsequenz aus der Hermite-Normalform ist die folgende Aussage:

Proposition 5.11. *Sei K ein Zahlkörper vom Grad n, und $x_1, \ldots, x_n \in K$ linear unabhängige Elemente. Für jedes gebrochene Ideal $I \subseteq K$ existiert eine kleinste positive Zahl $d \in \mathbb{Z}$ so daß $dI \subseteq \langle x_1, \ldots, x_n \rangle$, der* Nenner von I

bezüglich der Basis $x_1, \ldots, x_n$ *und eine eindeutige Basis* $y_1, \ldots, y_n$*, so daß für*

$$y_j = \frac{1}{d}\left(\sum_{i=1}^{n} \lambda_{ij} x_i\right),$$

die Koeffizienten λ_{ij} *die folgenden Bedingungen erfüllen:*

$$\lambda_{ij} \in \mathbb{Z}, \quad \lambda_{ij} = 0 \text{ für } i > j, \quad 0 \leq \lambda_{ij} < \lambda_{ii} \text{ für alle } j > i.$$

Die Basis aus der Proposition heißt *HNF-Basis*. Wir können auf diese Weise verschiedene Idealoperationen beschreiben.

1. Ideale vergleichen ist in der HNF-Basis ganz einfach, da die HNF-Basis eindeutig ist: Zwei Ideale sind genau dann gleich, wenn ihre HNF-Basen bzgl. einer gewählten Basis des Zahlkörpers gleich sind.

2. Wir beschreiben die HNF-Basis des Produkts $I_1 I_2$ zweier gebrochener Ideale I_1 und I_2. Wir nehmen an, daß eine $\mathbb{Q}$-Basis $\alpha_1, \ldots, \alpha_n$ von K gegeben ist, und daß die gebrochenen Ideale I_1 und I_2 durch Matrizen M_1 und M_2 gegeben sind, deren Spalten jeweils eine Basis $x_1, \ldots, x_n$ bzw. $y_1, \ldots, y_n$ von I_1 bzw. I_2 beschreiben. Man bildet die Produkte $x_i y_j$, und drückt diese wieder in der Basis $\alpha_1, \ldots, \alpha_n$ aus. Damit erhält man die Spalten eine $(n \times n^2)$-Matrix, deren Hermite-Normalform eine HNF-Basis für das gebrochene Ideal $I_1 I_2$ beschreibt.

3. Die Idealnorm eines (ganzen) Ideals kann auch direkt an der HNF-Basis abgelesen werden. Wenn $\alpha_1, \ldots, \alpha_n$ eine Ganzheitsbasis ist und λ_{ij} die Koeffizienten der HNF-Basis des Ideals $I \subseteq \mathcal{O}_K$, dann ist die Idealnorm gleich dem Produkt $\prod \lambda_{ii}$.

4. Sei $\alpha_1, \ldots, \alpha_n$ eine Ganzheitsbasis von K, und sei das Ideal I durch die Koeffizientenmatrix M gegeben, deren Spalten die Koeffizienten einer $\mathbb{Z}$-Basis $x_1, \ldots, x_n$ von I enthalten. Zuerst betrachtet man die Spurpaarungsmatrix $T = (\mathrm{Tr}(\alpha_i \alpha_j))_{i,j}$ und die Diskriminante $d_K = \det T$. Wir bezeichnen mit δ_j die Elemente von $\mathcal{O}_K$, deren Koeffizienten in der Basis α_i die Spalten von $d_K T^{-1}$ bilden. Wir bezeichnen mit N die Hermite-Normalform der $(n \times n^2)$-Matrix, deren Spalten durch die Produkte $x_i \delta_j$ gegeben sind. Zuletzt sei $P = d_K (N^t T)^{-1}$ und e der Hauptnenner der Einträge von P. Die HNF-Basis von I^{-1} ist durch die Hermite-Normalform von eP gegeben. Dieses Verfahren zur Inversenberechnung erhält seine konzeptionelle Rechtfertigung aus dem Konzept der Differente, das allerdings erst später ausführlich diskutiert wird.

5. Der Durchschnitt von Idealen I_1 und I_2 kann dann mit der Formel $I_1 \cap I_2 = I_1 \cdot I_2 \cdot (I_1 + I_2)^{-1}$ ermittelt werden.

Die Multiplikation und Division von Idealen kann vereinfacht werden, wenn man (wie beim Faktorisierungsproblem der Fall) Ideale *modulo p* multiplizieren bzw. dividieren will.

Lemma 5.12. *Sei K ein Zahlkörper und $\mathcal{O}$ eine Ordnung in K mit Basis $x_1, \ldots, x_n$. Seien I und J Ideale mit $I \cap J \supseteq (p)$ gegeben durch $\mathbb{F}_p$-Basen*

$\alpha_1, \ldots, \alpha_i$ von $I/p\mathcal{O}$ und $\beta_1, \ldots, \beta_j$ von $J/p\mathcal{O}$ als $\mathbb{F}_p$-Linearkombinationen der Restklassen $\overline{x_1}, \ldots, \overline{x_n}$ in $\mathcal{O}/p\mathcal{O}$. Sei M die $(n \times ij)$-Matrix, deren Spalten die $\mathbb{F}_p$-Koeffizienten von $\alpha_i\beta_j$ in den $\overline{x_1}, \ldots, \overline{x_n}$ sind. Dann liefern die Spalten der Zeilen-Stufen-Form der Matrix M eine $\mathbb{F}_p$-Basis für das Ideal $IJ/p\mathcal{O}$.

Für die Division benutzt man ein Lemma, das dem Lemma 5.5 sehr ähnlich sieht.

Lemma 5.13. *Sei K ein Zahlkörper, und $\mathcal{O}$ eine Ordnung in K. Seien I und J zwei Ideale mit $(p) \subseteq I \subseteq J$. Dann ist $IJ^{-1}/p\mathcal{O}$ als $\mathbb{F}_p$-Vektorraum gleich dem Kern der Abbildung*

$$m : \mathcal{O}/p\mathcal{O} \to \mathrm{End}(J/I) : \overline{\beta} \mapsto (\overline{\alpha} \mapsto \overline{\alpha\beta}).$$

Damit ist die Multiplikation und Division von Idealen modulo $p\mathcal{O}$ eine Aufgabe der linearen Algebra über $\mathbb{F}_p$.

5.3 Faktorisierung von Polynomen und Idealen

Wir beschränken uns hier auf Primidealfaktorisierung von (p) in $\mathcal{O}_K$ für den Fall $p \nmid d_K$. In diesem Fall müssen wir nur Polynome über endlichen Körpern faktorisieren. Mit den Idealoperationen aus dem vorangegangenen Kapitel kann man auch für den allgemeinen Fall ähnliche Methoden angeben, siehe dazu [Coh93, Kapitel 6.2].

Wir untersuchen nun also die Faktorisierung von Polynomen über den endlichen Körpern $\mathbb{F}_p$, p eine Primzahl. Wir können annehmen, daß das Polynom $f(X)$ normiert ist. Die Faktorisierung von $f(X)$ erhält man in drei Schritten:

(i) *Quadratfreie Zerlegung:* $f(X)$ wird zerlegt als

$$f(X) = f_1(X)^1 f_2(X)^2 \cdots f_n(X)^n,$$

wobei $f_i(X)$ quadratfrei und paarweise teilerfremd sind.

(ii) *Gradweise Zerlegung:* Für $i = 1, \ldots, n$ wird das (quadratfreie) Polynom $f_i(X)$ als Produkt $f_i(X) = \prod f_{i,d}(X)$ zerlegt, wobei $f_{i,d}(X)$ das Produkt der irreduziblen Faktoren vom Grad d von $f_i(X)$ ist.

(iii) *Endgültige Zerlegung:* Für jedes i und d wird $f_{i,d}(X)$ in $\deg f_{i,d}(X)/d$ verschiedene irreduzible Faktoren vom Grad d zerlegt.

Quadratfreie Zerlegung: Offensichtlich muß $f_i(X) = \prod(X - \alpha_i)$ sein, wobei α_i die Wurzeln mit Multiplizität i durchläuft. Wir betrachten die Ableitung

$$f(X)' = (f_1(X) \cdots f_n(X)^n)' = \sum_i i f_i(X)^{i-1} f_i(X)' \prod_{j \neq i} f_j(X)^j.$$

Es gilt

$$ggT(f(X), f'(X)) = \prod_{p \nmid i} f_i(X)^{i-1} \prod_{p \mid i} f_i(X)^i,$$

da jeder irreduzible Teiler von $f(X)$ ein $f_m(X)^m$ auch m-mal teilt. Dasselbe gilt auch für Summanden $i \neq m$ in $f'(X)$. Für $i = m$ hat man entweder nur $m - 1$ Faktoren wenn $p \nmid i$ und für $p \mid i$ ist der entsprechende Summand 0.

Eingabe: Polynom $f(X) \in \mathbb{F}_p[X]$
Ausgabe: Faktorisierung $f(X) = f_1(X)f_2(X)^2 \cdots f_n(X)^n$
$e \longleftarrow 1$;
$T_0(X) \longleftarrow f(X)$;
while $T_0(X)$ *nicht konstant* **do**
  $T(X) \leftarrow ggT(T_0(X), T_0'(X))$;
  $V(X) \longleftarrow T_0(X)/T(X)$;
  $k \longleftarrow 0$;
  while $V(X)$ *nicht konstant* **do**
    $k \longleftarrow k + 1$;
    if $p \mid k$ **then**
      $T(X) \longleftarrow T(X)/V(X)$;
      $k \longleftarrow k + 1$;
    end
    $W(X) \longleftarrow ggT(T(X), V(X))$;
    $f_{ek}(X) \longleftarrow V(X)/W(X)$;
    $V(X) \longleftarrow W(X)$;
    $T(X) \longleftarrow T(X)/V(X)$;
  end
  // $T(X)$ `ist von der Form` $\sum_{p|j} a_j X^j$
  $T_0(X) \longleftarrow \sum_{p|j} a_j X^{j/p}$;
  $e \longleftarrow pe$;
end

Algorithm 2: Quadratfreie Zerlegung

Zur Terminierung: die innere Schleife terminiert, da in jedem Durchgang der Grad von $V(X)$ oder $T(X)$ kleiner wird. Die äußere Schleife terminiert, weil in jedem Durchgang der Grad von $T_0(X)$ kleiner wird.

Zur Korrektheit: wir bezeichnen für die innere Schleife die $V(X)$ mit $V_{e,k}$ und $T(X)$ mit $T_{e,k}$. Es gilt dann

$$V_{e,k} = \prod_{i \geq k, p^e \nmid i, p^{e-1} \mid i} f_i(X), \qquad T_{e,k} = \prod_{i > k, p^e \nmid i, p^{e-1} \mid i} f_i(X)^{i-k} \prod_{p^e \mid i} f_i(X)^i.$$

Dieser Algorithmus liefert das gewünschte Ergebnis: für $p^e \nmid k$ gilt $f_{ek}(X) = V_{e,k}/V_{e,k+1}$. Wenn $V_{e,k}$ konstant wird, ist $T_{e,k} = \prod_{p^e \mid i} f_i(X)^i = U(X)^p$ eine p-Potenz.

Gradweise Zerlegung: Sei nun $f(X)$ ein quadratfreies Polynom. Wenn f irreduzibel ist, dann ist $\mathbb{F}_p[X]/f(X)\mathbb{F}_p[X] \cong \mathbb{F}_{p^d}$ für $d = \deg f(X)$. Da für alle Elemente $x \in \mathbb{F}_{p^d}^\times$ gilt $x^{p^d-1} = 1$, muß $f(X) \mid X^{p^d} - X$ sein. Außerdem hat jeder irreduzible Faktor von $f(X)$, der nicht schon $X^{p^e} - X$ für $e < d$ teilt, genau Grad d. Damit kann man einen Algorithmus für die gradweise Zerlegung formulieren.

Der Algorithmus terminiert, weil in jedem Durchlauf der Schleife $\deg V(X) - 2(d+1)$ kleiner wird. Im d-ten Durchlauf wird $f_d(X)$ als $ggT(X^{p^d} - X, V(X))$ bestimmt, daraus folgt die Korrektheit.

Mit den gleichen Argumenten wie eben erhält man einen Irreduzibilitätstest für Polynome über $\mathbb{F}_p$:

Eingabe: Quadratfreies Polynom $f(X) \in \mathbb{F}_p[X]$
Ausgabe: Faktorisierung $f(X) = f_1(X) \cdots f_n(X)$,
$f_d(X)$ ist Produkt der irreduziblen Faktoren von $f(X)$ vom Grad d.
$V(X) \longleftarrow f(X)$;
$W(X) \longleftarrow X$;
$d \longleftarrow 0$;
while $2(d+1) \leq \deg V(X)$ **do**
  $d \longleftarrow d+1$;
  $W(X) \longleftarrow W^p(X) \mod V(X)$;
  $f_d(X) = ggT(W(X) - X, V(X))$;
  if $f_d(X) \neq 1$ **then**
    $V(X) \longleftarrow V(X)/f_d(X)$;
    $W(X) \longleftarrow W(X) \mod V(X)$;
  end
end
if $\deg V > 0$ **then**
  $f_{d+1}(X) \longleftarrow V(X)$;
  $f_i(X) \longleftarrow 1$ für alle $i > d+1$;
end

Algorithm 3: Gradweise Zerlegung

Übungsaufgabe 5.2. *Ein Polynom $f(X) \in \mathbb{F}_p[X]$ vom Grad n ist genau dann irreduzibel, wenn $X^{p^n} \equiv X \mod f(X)$ und für alle Primzahlen $q \mid n$ gilt $ggT(X^{p^{n/q}} - X, f(X)) = 1$.*

Entscheiden Sie, ob die folgenden Polynome irreduzibel sind:

$$x^4 + x^2 + x + 1 \mod 2, \quad x^3 + 2x^2 + x + 1 \mod 3, \quad x^3 + 2x + 1 \mod 5.$$

Cantor-Zassenhaus Algorithmus: Dieser Algorithmus zerlegt ein quadratfreies Polynom, das ein Produkt von irreduziblen Faktoren vom Grad d ist. Dabei gibt es eine Unterscheidung zwischen $p = 2$ und p ungerade.

Proposition 5.14. *Sei $f(X)$ ein quadratfreies Polynom, das ein Produkt von irreduziblen Faktoren vom Grad d ist.*

(i) Sei p ungerade. Für jedes beliebige Polynom $T(X) \in \mathbb{F}_p[X]$ ist

$$f(X) = ggT(f(X), T(X)) \cdot$$
$$ggT(f(X), T(X)^{(p^d-1)/2} + 1) \cdot ggT(f(X), T(X)^{(p^d-1)/2} - 1).$$

(ii) Sei $p = 2$. Für jedes Polynom $T(X)$ ist

$$f(X) = ggT(f(X), \sum_{i=1}^{2^{d-1}} T(X)^i) \cdot ggT(f(X), \sum_{i=1}^{2^{d-1}} T(X)^i + 1).$$

Beweis. (i) Die Elemente von $\mathbb{F}_{p^d}$ sind genau die Lösungen von $X^{p^d} - X$. Offensichtlich sind die Elemente von $\mathbb{F}_{p^d}$ auch Lösungen von $T(X)^{p^d} - T(X)$, also $X^{p^d} - X \mid T(X)^{p^d} - T(X)$. Mit dem vorigen Irreduzibilitätskriterium sieht

man, daß jedes irreduzible Polynom vom Grad d schon $X^{p^d} - X$ teilt. Da $f(X)$ quadratfrei ist, folgt $f(X) \mid X^{p^d} - X \mid T(X)^{p^d} - T(X)$. Die Aussage folgt aus

$$T(X)^{p^d} - T(X) = T(X)(T(X)^{(p^d-1)/2} - 1)(T(X)^{(p^d-1)/2} + 1).$$

(ii) wie in (i), aber mit

$$T(X)^{2^d} - T(X) = \left(\sum_{i=1}^{2^{d-1}} T(X)^i\right)\left(\sum_{i=1}^{2^{d-1}} T(X)^i + 1\right).$$

□

Der Cantor-Zassenhaus-Algorithmus ist ein probabilistischer Algorithmus. Er wählt zufällig ein Polynom $g(X)$ und nutzt die folgende Tatsache, siehe [Poh93, Abschnitt II.2].

Lemma 5.15. *Sei $f(X)$ wie in Proposition 5.14. Die Wahrscheinlichkeit, daß der Faktor $ggT(f(X), g(X)^{(p^d-1)/2} - 1)$ für ein zufällig gewähltes Polynom $g(X)$ vom Grad $\leq 2d-1$ nichttrivial ist, ist mindestens $1 - 2^{1-r}$, wenn r die Anzahl der Faktoren von $f(X)$ ist.*

Eingabe: Quadratfreies Polynom $f(X) \in \mathbb{F}_p[X]$, das ein Produkt von irreduziblen Faktoren vom Grad d ist.
Ausgabe: Faktorisierung von $f(X)$ in irreduzible Faktoren
$k \longleftarrow \deg f(X)/d$;
if $k \neq 1$ **then**
  repeat
    Wähle zufälliges normiertes Polynom $T(X) \in \mathbb{F}_p[X]$ mit $\deg T(X) \leq 2d-1$;
    $g(X) \longleftarrow ggT(f(X), T(X)^{(p^d-1)/2} - 1)$;
  until $\deg g(X) \neq 0$ *und* $\deg g(X) \neq \deg f(X)$;
  Faktorisiere $g(X)$ und $f(X)/g(X)$;
end

Algorithm 4: Cantor-Zassenhaus Zerlegungsalgorithmus

Hier ist es mit der Terminierung natürlich schwierig. Man kann die endlich vielen Polynome vom Grad $\leq 2d-1$ auch durchgehen, dann bekommt man einen terminierenden Algorithmus mit schlechten Laufzeiteigenschaften. Wenn das Polynom r Faktoren hat, wird mit Wahrscheinlichkeit $1 - \epsilon$ nach $2\lceil \log \frac{r^2}{\epsilon} \rceil$ Durchläufen ein Faktor gefunden.

5.4 Ganzheitsbasen und Faktorisierung in Pari/GP

Nun wollen wir sehen, wie die bisher diskutierten Konzepte in Pari/GP implementiert sind. Wir betrachten dazu das Beispiel des durch $f(X) = X^3 + 17X^2 - 2X + 9$ definierten Zahlkörpers K, für den wir in Beispiel 5.8 eine Ganzheitsbasis berechnet hatten. Mit Pari/GP sieht das wie folgt aus:

```
? f=Pol([1,17,-2,9]);
? factor(poldisc(f))
%2 = [-1 1] [3 2] [5 3] [163 1]
? nfbasis(f)
%3 = [1,x,1/15*x^2 - 2/15*x+2/5]
? factor(nfdisc(f))
%4 = [-1 1] [5 1] [163 1]
? sqrtint(poldisc(f)/nfdisc(f))
%5 = 15
? g=polredabs(f)
%6 = x^3 - 7*x - 9
? sqrtint(poldisc(g)/nfdisc(g))
%7 = 1
```

Die erste Zeile definiert das Polynom $f(X) = X^3 + 17X^2 - 2X + 9$, die zweite Zeile berechnet die Diskriminante $D(1, X, X^2)$. Die dritte Zeile ermittelt mit dem Befehl `nfbasis` eine Ganzheitsbasis. Das Ergebnis ist nah an der Ganzheitsbasis, die wir in Beispiel 5.8 gefunden haben. Der Befehl `nfdisc` berechnet die Diskriminante des Zahlkörpers, am Besten in Kombination mit `factor` verwenden. In der fünften Zeile sehen wir, daß der Index der Potenzordnung $\mathbb{Z}[\theta]$ in $\mathcal{O}_K$ gleich 15 ist, was wir vorher auch schon berechnet hatten. Dann kommt Information, die wir im Beispiel noch nicht hatten. Der Befehl `polredabs` liefert ein "kleineres" Polynom, das denselben Zahlkörper definiert, in diesem Fall also $X^3 - 7X - 9$. Wie sehen in der siebten Zeile, daß der Zahlring eine Potenzbasis besitzt. Das konnte man dem Ausgangspolynom $f(X)$ nicht ansehen.

Man kann auch zwischen verschiedenen Darstellungen des Zahlkörpers wechseln.

```
? f=Pol([1,17,-2,9]);
? nf=nfinit(f)
? NF=nfinit(f,3)
? NF[2]
%4 = Mod(-x^2 - 2*x - 1, x^3 - 7*x - 9)
? modreverse(NF[2])
%5 = Mod(1/15*x^2 + 13/15*x - 8/5, x^3 + 17*x^2 - 2*x + 9)
```

Die Funktion `nfinit(f)` erzeugt eine Struktur, die alle wesentlichen Informationen über den durch f definierten Zahlkörper enthält. Man kann über `nf.zk` bzw. `nf.disc` auch wieder eine Ganzheitsbasis und die Diskriminante des Zahlkörpers sehen, mit `nf.index` erhält man auch wieder den Index der Potenzordnung $\mathbb{Z}[\theta]$ in $\mathcal{O}_K$. Mit `nfinit(f,3)` wird zuerst das gegebene Polynom mit `polred` reduziert. Nach der dritten Zeile erhält man mit `NF[1]` das gleiche Ergebnis wie mit `nfinit(polredabs(f))`, und mit `NF[2]` die Übersetzung zwischen `nfinit(f)` und `nfinit(polredabs(f))`. Wenn θ eine Wurzel von $f(X) = X^3+17X^2-2X+9 = 0$ und α eine Wurzel von $g(X) = X^3-7X-9 = 0$ bezeichnet, dann bedeutet die Antwort in der vierten Zeile, daß $\theta = -\alpha^2-2\alpha-1$. In der fünften Zeile sieht man mit `modreverse`, daß $\alpha = \frac{1}{15}\theta^2 + \frac{13}{15}\theta - \frac{8}{5}$.

Wir betrachten nun noch die Galoistheorie im Falle unseres Beispielkörpers K.

```
? f=Pol([1,17,-2,9]);
```

```
? polgalois(f)
%2 = [6, -1, 1, "S3"]
? nf=nfinit(f);
? nfgaloisconj(nf)
%4 = [x]~
? nfsubfields(nf)
%5 = [[x^3 + 17*x^2 - 2*x + 9, x], [x, x^3 + 17*x^2 - 2*x + 9]]
```

Der Befehl `polgalois` berechnet die Galoisgruppe des Zerfällungskörpers von f. Insbesondere ist K nicht galoissch. Mit dem Befehl `nfgaloisconj` kann man sehen, welche Elemente der Galoisgruppe den Zahlkörper K invariant lassen, in unserem Fall ist das nur die Identität. Damit gibt es auch keine nichttrivialen Zwischenkörper, wie man ebenfalls mit dem Befehl `nfsubfields(nf)` sehen kann.

Zuletzt betrachten wir Idealfaktorisierungen im Zahlring $\mathcal{O}_K$ für ein paar kleine Primzahlen.

```
? f=Pol([1,17,-2,9]);
? nf=nfinit(f);
? P2=idealprimedec(nf,2)
%3 = [[2, [2, 0, 0]~, 1, 3, [1, 0, 0]~]]
? P3=idealprimedec(nf,3)
%4 = [[3,[-3,-3,1]~,1,1,[1,0,1]~],[3,[-1,1,-1]~,1,1,[2,2,1]~],
[3,[0,-1,-1]~,1,1,[1,1,1]~]]
? P5=idealprimdec(nf,5)
%5 = [[5,[0,0,2]~,1,1,[1,3,1]~],[5,[1,0,-2]~,2,1,[3,2,1]~]]
? idealhnf(nf,idealprimedec(nf,5)[2])
%6 = [5 3 2] [0 1 0] [0 0 1]
? nfbasistoalg(nf,idealtwoelt(nf,P5[1])[2])
%7 = Mod(2/5*x^2 + 36/5*x + 12/5, x^3 + 17*x^2 - 2*x + 9)
? nfbasistoalg(nf,idealtwoelt(nf,P5[2])[2])
%8 = Mod(-2/5*x^2 - 36/5*x - 7/5, x^3 + 17*x^2 - 2*x + 9)
```

Die Antwort in der dritten Zeile hat nur einen Eintrag, also hat (2) nur einen Faktor, das Primideal $\mathfrak{p}$ wird als Liste $[p, a, e, f, b]$ gegeben, wobei p die Primzahl ist, a ein Erzeuger so daß $\mathfrak{p} = p\mathcal{O}_K + a\mathcal{O}_K$, e ist der Verzweigungsindex, f der Trägheitsgrad und b ein Element mit $\mathfrak{p}^{-1} = \mathcal{O}_K + b/p\mathcal{O}_K$. Wir sehen also an der Antwort in der dritten Zeile, daß (2) in $\mathcal{O}_K$ träge ist. In der vierten Zeile sehen wir, daß (3) in $\mathcal{O}_K$ vollständig zerlegt wird. In der fünften Zeile wird (5) faktorisiert. Wir sehen $(5) = \mathfrak{p}_1\mathfrak{p}_2^2$, der Verzweigungsindex von $\mathfrak{p}_2$ ist 2. Mit dem Befehl `idealhnf` kann man dann die HNF-Basis für das Ideal $\mathfrak{p}_2$ ausrechnen, diese HNF-Basis ist bezüglich einer Ganzheitsbasis von $\mathcal{O}_K$ zu verstehen. Zum Schluß wollen wir die Faktoren von (5) durch θ ausdrücken. Dies wird mit `nfbasistoalg` erzielt: wir sehen

$$\mathfrak{p}_1 = \left(5, \frac{2\theta^2 + 36\theta + 12}{5}\right), \mathfrak{p}_2 = \left(5, -\frac{2\theta^2 + 36\theta + 7}{5}\right).$$

Analog findet man Erzeuger für die drei Faktoren von (3):

$$(3, \theta + 3), \quad \left(3, -\frac{2\theta^2 + 41\theta + 19}{5}\right), \quad \left(3, -\frac{4\theta^2 + 67\theta - 2}{5}\right).$$

Kapitel 6

Die Idealklassengruppe

In diesem Kapitel definieren und studieren wir die *Klassengruppe* von Zahlkörpern. Diese Gruppe beschreibt, wie weit der Ganzheitsring $\mathcal{O}_K$ davon abweicht, ein Hauptidealring zu sein. Das wichtigste Ergebnis ist, daß die Klassengruppe eines Zahlkörpers immer endlich ist.

Definition 6.1 (Idealklassengruppe)**.** *Sei R ein Dedekind-Ring. Die* Idealklassengruppe *ist definiert als*

$$\mathrm{Cl}(R) = \frac{\textit{gebrochene Ideale } \neq 0}{\textit{Hauptideale } \neq 0}.$$

Die Klassenzahl *ist die Anzahl der Elemente von* $\mathrm{Cl}(R)$*.*

Es ist klar, daß $\mathrm{Cl}(R)$ eine abelsche Gruppe ist. Klassenzahl 1 bedeutet nach Definition, daß R ein Hauptidealring ist. Ziel dieses Kapitels ist es, zu zeigen, daß die Klassenzahl eines Ganzheitsrings endlich ist. Dies liegt wesentlich daran, daß die Restklassenkörper endlich sind. Klassengruppe und Klassenzahl werden of auch als Eigenschaften des zugehörigen Zahlkörpers betrachtet, damit sollte man aber vorsichtig umgehen.

Ein wichtiges Hilfsmittel für den Beweis der Endlichkeit der Klassengruppe ist die Erweiterung der Norm auf Ideale.

Definition 6.2 (Idealnorm)**.** *Sei K ein Zahlkörper, $\mathcal{O}_K$ der Ganzheitsring, $I \subseteq \mathcal{O}_K$ ein Ideal. Die* Idealnorm *von I ist die Kardinalität von $\mathcal{O}_K/I$:*

$$N(I) = \#(\mathcal{O}_K/I).$$

Nach dem Elementarteilersatz gibt es für jedes Ideal $I \subseteq \mathcal{O}_K$ eine $\mathbb{Z}$-Basis $x_1, \ldots, x_n$ von $\mathcal{O}_K$ und $\lambda_1, \ldots, \lambda_n \in \mathbb{Z}$, so daß $\lambda_1 x_1, \ldots, \lambda_n x_n$ eine $\mathbb{Z}$-Basis von I ist. Dann gilt

$$\mathcal{O}_K/I = \prod_{i=1}^{n} \mathbb{Z}/(\lambda_i), \qquad N(I) = \lambda_1 \cdots \lambda_n.$$

Die Idealnorm ist also immer endlich. Dies gilt allgemeiner für Dedekindringe mit endlichen Restklassenkörpern.

Übungsaufgabe 6.1. *Sei K ein Zahlkörper. Die Idealnorm $N(I) = \#(\mathcal{O}_K/I)$ ist multiplikativ. Insbesondere ist für $I = \prod \mathfrak{p}^{v_\mathfrak{p}(I)}$ die Norm gegeben durch*

$$N(I) = \prod N(\mathfrak{p})^{v_\mathfrak{p}(I)}.$$

Ist $I = (a) \subseteq \mathcal{O}_K$ ein Hauptideal, dann ist $N(I) = N_{K/\mathbb{Q}}(a)$.

Die weitere Vorgehensweise ist nun wie folgt: Zuerst wird der Ring $\mathcal{O}_K$ als Gitter in einen reellen Vektorraum eingebettet. Ideale liefern Teilgitter, deren Grundmaschenvolumen im Wesentlichen durch Diskriminante und Idealnorm gegeben ist. Daraus leitet man Schranken für Normen von Elementen in Idealen ab. Aus diesen Schranken ergibt sich dann die Endlichkeit der Klassenzahl.

6.1 Gitter

Im Folgenden werden Volumina von Teilmengen von $\mathbb{R}^n$ betrachtet. In der Zermelo-Fraenkel-Mengenlehre mit Auswahlaxiom ist das problematisch, man kann nur messbaren Mengen ein Volumen zuordnen. Es gibt auch Axiomensysteme für Mengenlehre, die einen weniger paradoxen Volumenbegriff besitzen. Hier betrachten wir nur konvexe Mengen, das ist auch unproblematisch.

Übungsaufgabe 6.2. *Eine konvexe Teilmenge des $\mathbb{R}^n$ ist Jordan-messbar, also auch Lebesgue-messbar. (Angabe einer Literaturreferenz reicht.)*

Definition 6.3. *Eine Untergruppe $H \subseteq \mathbb{R}^n$ heißt* diskret*, wenn für jede kompakte Teilmenge $K \subseteq \mathbb{R}^n$ der Schnitt $K \cap H$ endlich ist.*

Eine solche Untergruppe ist notwendig abelsch, also ein $\mathbb{Z}$-Modul. Außerdem ist sie notwendig torsionsfrei. Wir zeigen, daß sie auch endlich erzeugt ist:

Proposition 6.4. *Sei $H \subseteq \mathbb{R}^n$ diskret. Dann wird H als $\mathbb{Z}$-Modul von r Vektoren erzeugt, die $\mathbb{R}$-linear unabhängig sind. Es gilt also $H \cong \mathbb{Z}^r$ mit $r \leq n$.*

Beweis. Sei $(e_1, \ldots, e_r)$ eine maximale Menge von $\mathbb{R}$-linear unabhängigen Elementen von H und

$$P = \left\{ x \in \mathbb{R}^n \mid x = \sum_{i=1}^{r} \lambda_i e_i, 0 \leq \lambda_i \leq 1 \right\}.$$

das von den e_i erzeugte Parallelotop. Dieses ist offensichtlich beschränkt und abgeschlossen, also kompakt. Damit ist $P \cap H$ endlich. Nach Wahl der e_i läßt sich jedes $x \in H$ als $x = \sum_{i=1}^r \lambda_i e_i$, $\lambda_i \in \mathbb{R}$ darstellen. Für $j \in \mathbb{Z}$ definieren wir $x(j) = jx - \sum_{i=1}^r \lfloor j\lambda_i \rfloor e_i$, wobei die Gaußklammer $\lfloor \lambda_i \rfloor$ die größte ganze Zahl kleiner oder gleich λ_i bezeichnet, insbesondere $0 \leq j\lambda_i - \lfloor j\lambda_i \rfloor \leq 1$, also $x(j) \in P \cap H$. Wegen $x = x(1) + \sum_{i=1}^r \lfloor \lambda_i \rfloor e_i$ wird H dann durch die endliche Menge $P \cap H$ erzeugt. Da $P \cap H$ endlich ist, gibt es Indizes $j \neq k$ mit $x(j) = x(k)$. Das bedeutet nach Definition $(j-k)\lambda_i = \lfloor j\lambda_i \rfloor - \lfloor k\lambda_i \rfloor$, die λ_i sind also rational. Für den Hauptnenner d ist dann also $dH \subseteq \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_r$. Nach dem Elementarteilersatz gibt es eine $\mathbb{Z}$-Basis $f_1, \ldots, f_r$ von $\mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_r$ und ganze Zahlen $\alpha_1, \ldots, \alpha_r$ so daß die $\alpha_i f_i$ eine Basis von dH bilden. Damit bilden $\alpha_i f_i / d$ eine Basis von H. □

Definition 6.5. *Eine diskrete Untergruppe $H \subseteq \mathbb{R}^n$ vom Rang n heißt* Gitter. *Sei $e_1, \ldots, e_n$ eine $\mathbb{Z}$-Basis von H. Dann heißt*

$$P(e_1, \ldots, e_n) = \left\{ \sum_{i=1}^{n} \lambda_i e_i \mid 0 \leq \lambda_i \leq 1 \right\}$$

Fundamentalparallelotop *oder* Grundmasche *des Gitters H.*

Lemma 6.6. *Für je zwei $\mathbb{Z}$-Basen $e_1, \ldots, e_n$ und $e'_1, \ldots, e'_n$ ist*

$$\operatorname{vol}(P(e_1, \ldots, e_n)) = \operatorname{vol}(P(e'_1, \ldots, e'_n)),$$

wobei vol *das Volumen bezüglich des Standard-Lebesgue-Maßes bezeichnet.*

Beweis. Für je zwei $\mathbb{Z}$-Basen e_i und e'_i gibt es eine Basiswechselmatrix $A \in GL_n\mathbb{Z}$ und es gilt $\operatorname{vol}(P(e_1, \ldots, e_n)) = |\det A| \operatorname{vol}(P(e'_1, \ldots, e'_n))$. □

Das Lemma erlaubt, für ein Gitter $H \subseteq \mathbb{R}^n$ ein Volumen durch $\operatorname{vol}(H) = \operatorname{vol}(P(e_1, \ldots, e_n))$ für eine Basis $e_1, \ldots, e_n$ von H zu definieren.

Satz 6.7 (Minkowski)**.** *Sei $H \subseteq \mathbb{R}^n$ ein Gitter, $S \subseteq \mathbb{R}^n$ eine meßbare Teilmenge mit $\operatorname{vol}(S) > \operatorname{vol}(H)$. Dann existieren verschiedene Punkte $x, y \in S$ mit $x - y \in H$.*

Beweis. Sei $e_1, \ldots, e_n$ eine $\mathbb{Z}$-Basis von H und P das zugehörige Parallelotop. Es gilt $\mathbb{R}^n = \cup_{h \in H}(h + P)$, also $S = \cup_{h \in H}(S \cap (h + P))$. Aus der σ-Additivität folgt $\operatorname{vol}(S) = \sum_{h \in H} \operatorname{vol}(S \cap (h + P))$, aus der Translationsinvarianz des Standard-Lebesgue-Maßes folgt $\operatorname{vol}(S \cap (h + P)) = \operatorname{vol}((-h + S) \cap P)$. Wären die Mengen $(-h + S) \cap P$ für $h \in H$ alle disjunkt, wäre $\operatorname{vol}(S) \leq \operatorname{vol}(P) = \operatorname{vol}(H)$. Also existieren verschiedene $h, h' \in H$ mit $P \cap (-h + S) \cap (-h' + S) \neq \emptyset$. Ein Element z im Schnitt liefert $x = h + z$, $y = h' + z$ und $x - y = h - h' \in H$. □

Korollar 6.8 (Minkowskischer Gitterpunktsatz)**.** *Sei $H \subseteq \mathbb{R}^n$ ein Gitter und $S \subseteq \mathbb{R}^n$ eine konvexe zentralsymmetrische (symmetrisch bzgl. Punktspiegelung an 0) Teilmenge, die eine der beiden folgenden Bedingungen erfüllt:*

(i) $\operatorname{vol}(S) > 2^n \operatorname{vol}(H)$*, oder*

(ii) $\operatorname{vol}(S) \geq 2^n \operatorname{vol}(H)$ *und S ist kompakt.*

Dann folgt $S \cap (H \setminus \{0\}) \neq \emptyset$.

Beweis. (i) Die Menge $S' = \frac{1}{2}S$ erfüllt mit $\operatorname{vol}(S') = 2^{-n} \operatorname{vol}(S) > \operatorname{vol}(H)$ die Bedingungen für Satz 6.7. Es gibt also Punkte $x, y \in S'$ mit $x - y \in H$. Außerdem folgt aus Symmetrie und Konvexität, daß $x - y = \frac{1}{2}(2x + (-2y)) \in S \cap H$.

(ii) Für $\epsilon > 0$ wendet man (i) auf $(1 + \epsilon)S$ an und erhält eine diskrete kompakte (also endliche) nichtleere Menge $(H \setminus \{0\}) \cap (1 + \epsilon)S$. Es gilt

$$\bigcap_{\epsilon > 0} (H \setminus \{0\}) \cap (1 + \epsilon)S \neq \emptyset.$$

(S ist kompakt. Wäre der Schnitt leer, würden die Komplemente der (endlichen) Teilmengen für $\epsilon > 0$ eine offene Überdeckung bilden. Diese hätte eine endliche Teilüberdeckung, damit hätten bereits endlich viele der obigen Teilmengen einen leeren Schnitt, damit gäbe es ein ϵ, für das die entsprechende Teilmenge leer ist.) Aus $\bigcap_{\epsilon > 0}(1 + \epsilon)S = S$ folgt die Behauptung. □

6.2 Die kanonische Einbettung

Sei $K/\mathbb{Q}$ ein Zahlkörper vom Grade $n = [K : \mathbb{Q}]$. Es gibt n verschiedene $\mathbb{Q}$-Einbettungen $K \hookrightarrow \overline{\mathbb{Q}}$ bzw. $K \hookrightarrow \mathbb{C}$.

Offensichtlich operiert die komplexe Konjugation auf diesen Einbettungen. Eine Einbettung $\sigma : K \hookrightarrow \mathbb{C}$ heißt *reell*, wenn sie invariant unter Konjugation ist, d.h. $\sigma = \overline{\sigma}$. Andernfalls heißt $\sigma, \overline{\sigma}$ ein Paar konjugiert komplexer Einbettungen.

Üblicherweise bezeichnet r_1 die Anzahl der reellen Einbettungen und r_2 die Anzahl der Paare konjugiert komplexer Einbettungen. Damit ist dann $n = r_1 + 2r_2$.

Beispiel 6.9. *(i) Sei d quadratfrei, $K = \mathbb{Q}(\sqrt{d})$. Dann gibt es zwei Einbettungen, die durch $\sigma_i(\sqrt{d}) = \pm\sqrt{d}$ gegeben sind. Für $d > 0$ ist $r_1 = 2$, $r_2 = 0$. Für $d < 0$ ist $r_1 = 0$, $r_2 = 1$.*

(ii) Sei ζ_n eine primitive n-te Einheitswurzel, $K = \mathbb{Q}(\zeta_n)$, $n > 2$. Dann gibt es $\phi(n)$ verschiedene Einbettungen. Es ist $r_1 = 0$ und $r_2 = \frac{\phi(n)}{2}$.

□

Körper mit $r_2 = 0$ heißen *total reell*, Körper mit $r_1 = 0$ *total imaginär*.

Die Signatur eines Zahlkörpers kann man mit der Methode von Sturm berechnen. Für ein separables Polynom $f(X) \in \mathbb{R}[X]$ definieren wir induktiv die Sequenz der Polynomreste, auch Sturm-Sequenz von f und f':

$$f_0(X) = f(X), f_1(X) = f'(X), f_{i-1}(X) = f_i(X)Q_i(X) - f_{i+1}(X)$$

Dabei ist f_{i+1} der Rest der Division von f_{i-1} durch f_i mit negativem Vorzeichen. Wegen $ggT(f, f') = 1$ gibt es ein n mit f_n konstant. Für $a \in \mathbb{R}$ keine Nullstelle von f bezeichnen wir mit $v_f(a)$ die Anzahl der Vorzeichenwechsel in der Sequenz $f_0(a), f_1(a), \ldots, f_n(a)$.

Proposition 6.10. *Sei $f(X) \in \mathbb{R}[X]$ ein separables Polynom, $a, b \in \mathbb{R}$ mit $a < b$ keine Nullstellen von f. Die Anzahl der reellen Nullstellen von $f(X)$ im Intervall $[a, b]$ ist gleich $v_f(a) - v_f(b)$.*

Beweis. Wir betrachten das Verhalten der Vorzeichen von $f_i(a)$, wenn a eine Nullstelle von f_i durchläuft. Das Vorzeichen von f_0 ändert sich. Das Vorzeichen von f_1 bleibt gleich, da die Nullstelle einfach ist. Wenn a eine Wurzel von f_i mit $0 < i < n$ ist, gilt $f_{i-1}(a) = -f_{i+1}(a) \neq 0$. Der Beitrag des Teils $f_{i-1}(X), f_i(X), f_{i+1}(X)$ zu $v_f(X)$ ändert sich damit nicht, es verschiebt sich nur die Position des Vorzeichenwechsels. □

Für ein Polynom $f(X) = a_0X^n + \cdots + a_n$, $a_0 \neq 0$ ist der Betrag einer Nullstelle x von f beschränkt durch

$$|x| \leq \max_{i=1,\ldots,n} \left(n \left| \frac{a_i}{a_0} \right| \right)^{\frac{1}{i}}.$$

Damit kann man die Anzahl der reellen Nullstellen eines Polynoms bestimmen.

Beispiel 6.11. *Wir berechnen die Signatur von $f(X) = X^4 - 3X^2 + 5X - 1$. Die Sturm-Sequenz ist*

$$\left(X^4 - 3X^2 + 5X - 1, 4X^3 - 6X + 5, \frac{3}{2}X^2 - \frac{15}{4}X + 1, -10X^2 + \frac{26}{3}X - 5, \right.$$

$$\frac{49}{20}X - \frac{1}{4}, -\frac{1124}{147}X + 5, -\frac{6079}{4496}\Big)$$

Die Werte von $4|a_i|^{\frac{1}{i}}$ *sind durch* 0, $4\sqrt{3} \sim 6,93$, $4\sqrt[3]{5} \sim 6,84$ *und* 4 *gegeben. Der Betrag der Nullstellen ist also durch* 7 *beschränkt. Wir erhalten*

$$v_f(-7) = \left(2218, -1325, \frac{403}{4}, -\frac{1667}{3}, -\frac{87}{5}, \frac{1229}{21}, -\frac{6079}{4496}\right),$$

$$v_f(7) = \left(2288, 1335, \frac{193}{4}, -\frac{1303}{4}, \frac{169}{10}, -\frac{1019}{21}, -\frac{6079}{4496}\right).$$

Der durch $f(X)$ *definierte Zahlkörper hat also* 2 *reelle und* 2 *konjugiert komplexe Einbettungen,* $r_1 = 2$, $r_2 = 1$. □

Definition 6.12. *Die* kanonische Einbettung *ist das Produkt der* $[K : \mathbb{Q}]$ *verschiedenenen Einbettungen*

$$\sigma : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n : x \mapsto (\sigma_1(x), \dots, \sigma_{r_1+r_2}(x)).$$

Satz 6.13. *Sei* K *ein Zahlkörper,* M *ein freier* $\mathbb{Z}$*-Untermodul von* K *vom Rang* n *und* $x_1, \dots, x_n$ *eine* $\mathbb{Z}$*-Basis von* M*. Dann ist* $\sigma(M)$ *ein Gitter in* $\mathbb{R}^n$ *mit Volumen*

$$\operatorname{vol}(\sigma(M)) = \frac{1}{2^{r_2}} \left|\det(\sigma_i(x_j))\right|.$$

Beweis. Das Bild $\sigma(M)$ ist offensichtlich diskret. Wenn $\det \sigma(x_i) \neq 0$, dann ist $\sigma(M)$ ein Gitter mit Volumen $|\det \sigma(x_i)|$. Die Koordinaten von $\sigma(x_i)$ in der Standardbasis von $\mathbb{R}^n$ sind

$$\sigma_1(x_i), \dots, \sigma_{r_1}(x_i), \operatorname{Re}\sigma_{r_1+1}(x_i), \operatorname{Im}\sigma_{r_1+1}(x_i), \dots, \operatorname{Re}\sigma_{r_1+r_2}(x_i), \operatorname{Im}\sigma_{r_1+r_2}(x_i).$$

Es gilt

$$-\frac{1}{2i}\det(\dots, z, \overline{z}, \dots) = \det\left(\dots, \frac{1}{2}(z+\overline{z}), \frac{1}{2i}(z-\overline{z}), \dots\right).$$

Dies wendet man r_2-mal an und erhält mit $\operatorname{Re} z = \frac{1}{2}(z+\overline{z})$ und $\operatorname{Im} z = \frac{1}{2i}(z-\overline{z})$ und einigen Spaltenvertauschungen

$$\frac{1}{2^{r_2}} \left|\det(\sigma_i(x_j))\right| = \left|\det(\sigma(x_j))\right|.$$

Dann folgt aus Übungsaufgabe 3.3, daß $\det(\sigma_i(x_j)) \neq 0$. Also ist $\sigma(M)$ ein Gitter mit dem behaupteten Volumen. □

Korollar 6.14. *Sei* K *ein Zahlkörper mit Diskriminante* d_K *und Ganzheitsring* $\mathcal{O}_K$*. Sei* $I \subseteq \mathcal{O}_K$ *ein Ideal. Dann sind* $\sigma(\mathcal{O}_K)$ *und* $\sigma(I)$ *Gitter und es gilt für die Volumina*

$$\operatorname{vol}(\sigma(\mathcal{O}_K)) = \frac{1}{2^{r_2}}\sqrt{|d_K|}, \qquad \operatorname{vol}(\sigma(I)) = \frac{1}{2^{r_2}}\sqrt{|d_K|}N(I).$$

Beweis. Für $\mathcal{O}_K$ wenden wir Satz 6.13 auf eine Ganzheitsbasis x_i von $\mathcal{O}_K$ an. Die Behauptung folgt dann aus der Definition der Diskriminante d_K.

Nach Definition der Idealnorm ist $\sigma(I)$ ein Untergitter von $\sigma(\mathcal{O}_K)$ vom Index $N(I)$. Das Fundamentalparallelotop von $\sigma(I)$ ist damit eine Vereinigung von $N(I)$ Kopien des Fundamentalparallelotops von $\sigma(\mathcal{O}_K)$. Daraus folgt die Behauptung. Genau sieht man das mit dem Elementarteilersatz, der eine Basis von $\mathcal{O}_K$ und Zahlen $\alpha_1, \ldots, \alpha_n$ liefert, so daß $\alpha_i x_i$ eine Basis von I ist und $N(I) = \prod \alpha_i$. □

Satz 6.15 (Minkowski-Schranke)**.** *Sei K eine Zahlkörper vom Grad $n = r_1 + 2r_2$, d_K die Diskriminante von K und $(0) \neq I \subseteq \mathcal{O}_K$ ein Ideal. Dann gibt es ein Element $0 \neq x \in I$ mit*

$$|N_{K/\mathbb{Q}}(x)| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d_K|} N(I).$$

Beweis. Wir betrachten die kanonische Einbettung $\sigma : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Sei $t \in \mathbb{R}$, $t > 0$, und sei B_t die Menge aus Lemma 6.16. Offensichtlich ist B_t kompakt, konvex und symmetrisch bzgl. Punktspiegelung an 0. Nach Lemma 6.16 ist $\mathrm{vol}(B_t) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!}$. Wir wählen t, so daß (mit Korollar 6.14) gilt

$$2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!} = \mathrm{vol}(B_t) = 2^n \,\mathrm{vol}(\sigma(I)) = 2^{n-r_2} \sqrt{|d_K|} N(I).$$

Umstellen liefert $t^n = 2^{n-r_1} \pi^{-r_2} n! \sqrt{|d_K|} N(I)$. Nach dem Minkowskischen Gitterpunktsatz Korollar 6.8 existiert ein Element $x \in I$ mit $\sigma(x) \in B_t$ und es gilt

$$|N_{K/\mathbb{Q}}(x)| = \prod_{i=1}^{r_1} |\sigma_i(x)| \prod_{j=r_1+1}^{r_1+r_2} |\sigma_j(x)|^2.$$

Daraus folgt dann

$$|N_{K/\mathbb{Q}}(x)| \leq \left(\frac{1}{n} \sum_{i=1}^{r_1} |\sigma_i(x)| + \frac{2}{n} \sum_{j=r_1+1}^{r_1+r_2} |\sigma_j(x)| \right)^n \leq \frac{t^n}{n^n}.$$

Für die erste Ungleichung benutzt man, daß das geometrische Mittel immer kleiner als das arithmetische Mittel ist; die zweite Ungleichung folgt aus der Definition der Menge B_t. Damit erhalten wir die Behauptung. □

Lemma 6.16. *Seien $r_1, r_2 \in \mathbb{N}$, $n = r_1 + 2r_2$, $t \in \mathbb{R}$, und*

$$B_t = \left\{ (y_1, \ldots, y_{r_1}, z_1, \ldots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid \sum_{i=1}^{r_1} |y_i| + 2 \sum_{j=1}^{r_2} |z_j| \leq t \right\}.$$

Dann gilt

$$\mathrm{vol}(B_t) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!}.$$

Beweis. Wir setzen $V(r_1, r_2, t) = \mathrm{vol}(B_t)$. Die Behauptung wird mit Induktion über r_1 und r_2 bewiesen. Wir haben zwei Induktionsanfänge: $V(1, 0, t) = 2t$ ist

die Länge des Intervalls $[-t,t]$, und $V(0,1,t) = \frac{\pi t^2}{4}$ ist die Fläche der Kreisscheibe mit Radius $t/2$.

Wir nehmen nun an, daß die Behauptung für $V(r_1,r_2,t)$. Wir zeigen zuerst die Behauptung für $V(r_1+1,r_2,t)$. Wir haben in diesem Fall

$$B_t = \left\{ (y,y_i,z_j) \in \mathbb{R}\times\mathbb{R}^{r_1}\times\mathbb{C}^{r_2} \mid |y| + \sum_{i=1}^{r_1}|y_i| + 2\sum_{j=1}^{r_2}|z_j| \le t \right\}.$$

Für $(y,y_i,z_j) \in B_t$ ist $|y| \le t$, wir können also ansetzen

$$V(r_1+1,r_2,t) = \int_{-t}^{t} V(r_1,r_2,t-|y|)dy.$$

Mit Induktionsvoraussetzung folgt

$$V(r_1+1,r_2,t) = 2\int_0^t 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{(t-y)^n}{n!}dy = 2^{r_1+1}\left(\frac{\pi}{2}\right)^{r_2}\frac{t^{n+1}}{(n+1)!}.$$

Nun zeigen wir die Behauptung für $V(r_1,r_2+1,t)$. In diesem Fall haben wir

$$B_t = \left\{ (y_i,z_j,z) \in \mathbb{R}^{r_1}\times\mathbb{C}^{r_2}\times\mathbb{C} \mid \sum_{i=1}^{r_1}|y_i| + 2\sum_{j=1}^{r_2}|z_j| + 2|z| \le t \right\}.$$

Wir können wieder zuerst über $d\mu(z)$, das Standard-Lebesgue-Maß auf $\mathbb{C}$, integrieren

$$V(r_1,r_2+1,t) = \int_{|z|\le t/2} V(r_1,r_2,t-2|z|)d\mu(z).$$

Wir rechnen in Polarkoordinaten $z = \rho e^{i\theta}$, $\rho\in\mathbb{R}^+$, $0\le\theta\le 2\pi$; es gilt $d\mu(z) = \rho d\rho d\theta$. Mit der Induktionsvoraussetzung gilt

$$V(r_1,r_2+1,t) = \int_0^{t/2}\int_0^{2\pi} 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{(t-2\rho)^n}{n!}\rho d\rho d\theta$$

Zuerst integrieren wir über $d\theta$, dies liefert einen zusätzlichen Faktor 2π:

$$V(r_1,r_2+1,t) = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{2\pi}{n!}\int_0^{t/2}(t-2\rho)^n\rho d\rho$$

Das Integral über ρ wird jetzt durch Substitution $2\rho = x$ und partielle Integration ausgewertet

$$\int_0^{t/2}(t-2\rho)^n\rho d\rho = \frac{1}{4}\int_0^x (t-x)^n x dx =$$

$$= \frac{1}{4}\left(\frac{-(t-x)^{n+1}}{n+1}x\Big|_0^x - \int_0^x \frac{-(t-x)^{n+1}}{n+1}dx\right) = \frac{1}{4}\frac{t^{n+2}}{(n+1)(n+2)}.$$

Wir erhalten die Behauptung

$$V(r_1,r_2+1,t) = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2+1}\frac{t^{n+2}}{(n+2)!}.$$

□

Korollar 6.17. *Sei K eine Zahlkörper vom Grad $n = r_1 + 2r_2$, d_K die Diskriminante von K. Jede Idealklasse von K enthält ein ganzes Ideal I mit*

$$N(I) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d_K|}.$$

Beweis. Sei J' ein gebrochenes Ideal. Nach Multiplikation mit einem Hauptideal können wir annehmen, daß $J = J'^{-1} \subseteq \mathcal{O}_K$ ein ganzes Ideal ist. Sei $x \in J$ ein Element wie in Satz 6.15. Dann ist $I = xJ' = xJ^{-1}$ ein ganzes Ideal in der Klasse von J', das wegen der Multiplikativität der Norm die Behauptung erfüllt. □

Korollar 6.18. *Sei K ein Zahlkörper vom Grad n mit Diskriminante d_K. Dann gilt für $n \geq 2$*

$$d_K \geq \frac{\pi}{3} \left(\frac{3\pi}{4}\right)^{n-1}.$$

Der Quotient $\frac{n}{\log d}$ wird durch eine von K unabhängige Konstante beschränkt.

Beweis. Es gibt immer ein Ideal $I \neq (0)$ mit $N(I) \geq 1$. Damit liefert Korollar 6.17 $\left(\frac{\pi}{4}\right)^{r_2} \frac{n^n}{n!} \leq \sqrt{|d_K|}$. Mit $\pi/4 < 1$ und $2r_2 \leq n$ folgt

$$|d_K| \geq \left(\frac{\pi}{4}\right)^n \frac{n^{2n}}{(n!)^2} =: a_n.$$

Für die Folge a_n haben wir die Aussagen

$$a_2 = \frac{\pi^2}{4}, \qquad \frac{a_{n+1}}{a_n} = \frac{\pi}{4} \frac{(n+1)^{2n+2}}{((n+1)!)^2} \frac{(n!)^2}{(n)^{2n}} = \frac{\pi}{4} \left(1 + \frac{1}{n}\right)^{2n}.$$

Aus der binomischen Formel folgt

$$\left(1 + \frac{1}{n}\right)^{2n} = 1 + 2 + \text{positive Terme, also } \frac{a_{n+1}}{a_n} \geq \frac{3\pi}{4}.$$

Induktiv folgt nun die Behauptung

$$|d_K| \geq \frac{\pi^2}{4} \left(\frac{3\pi}{4}\right)^{n-2} = \frac{\pi}{3} \left(\frac{3\pi}{4}\right)^{n-1}.$$

Logarithmieren liefert

$$1,166796 \sim \left(\log \frac{3\pi}{4}\right)^{-1} \geq \frac{n}{\log |d_K|}.$$

□

6.3 Endlichkeitssätze

Die folgenden Endlichkeitssätze sind das eigentliche Ziel dieses Kapitels gewesen. Sie sind auch zentrale Aussagen der algebraischen Zahlentheorie. Die Endlichkeit der Klassenzahl ist für quadratische Zahlkörper sicher Gauß schon bekannt gewesen, manche Autoren schreiben auch den allgemeinen Satz über die Endlichkeit der Klassenzahl Gauß zu. Ein Beweis wird in Dirichlets Vorlesungen über Zahlentheorie bzw. Dedekinds Anhang zu den Vorlesungen gegeben. Der hier benutzte Beweis geht auf Minkowski zurück. Für genauere Informationen zur Geschichte sei auf [Die85] verwiesen.

Satz 6.19 (Dirichlet)**.** *Die Klassengruppe eines Zahlkörpers ist endlich.*

Beweis. Nach Korollar 6.17 genügt es, Idealklassen mit beschränkter Norm zu betrachten. Es reicht also, zu zeigen, daß es für gegebene Konstante C nur endlich viele Ideale mit $N(I) < C$ gibt. Aus $N(I) = \#\mathcal{O}_K/I = q$ folgt $q \in I$. Da $\mathcal{O}_K/(q)$ ein endlicher Ring ist, gibt es nur endlich viele Ideale in $\mathcal{O}_K$, die (q) enthalten. □

Satz 6.20 (Hermite-Minkowski)**.** *Sei $K \neq \mathbb{Q}$ ein Zahlkörper. Dann ist $d_K \neq 1$.*

Beweis. Aus Korollar 6.18 folgt $|d_K| \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1} > 1$. □

Satz 6.21 (Hermite)**.** *Für gegebenes $d \in \mathbb{Z}$ gibt es nur endlich viele Zahlkörper mit Diskriminante d.*

Beweis. Nach Korollar 6.18 ist der Grad beschränkt. Es reicht also, zu zeigen, daß es nur endlich viele Zahlkörper mit gegebenem d, r_1 und r_2 gibt. Für $r_1 > 0$ sei B die Menge der $(y_1, \ldots, y_{r_1}, z_1, \ldots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ mit

$$|y_1| \leq 2^n \left(\frac{\pi}{2}\right)^{-r_2} \sqrt{|d|}, |y_i| \leq \frac{1}{2} \text{ für } 2 \leq i \leq r_1, |z_j| \leq \frac{1}{2} \text{ für } 1 \leq j \leq r_2.$$

Für $r_1 = 0$ sei B die Menge $(z_1, \ldots, z_{r_2}) \in \mathbb{C}^{r_2}$ mit

$$|z_1 - \overline{z_1}| \leq 2^n \left(\frac{\pi}{2}\right)^{1-r_2} \sqrt{|d|}, |z_1 + \overline{z_1}| \leq \frac{1}{2}, |z_j| \leq \frac{1}{2} \text{ für } 2 \leq j \leq r_2.$$

Diese Menge ist kompakt, konvex und symmetrisch bzgl. Punktspiegelung an 0. Es gilt $\mathrm{vol}(B) = 2^{n-r_2}\sqrt{|d|}$. Nach dem Minkowskischen Gitterpunktsatz Korollar 6.8 und Korollar 6.14 gibt es ein Element $0 \neq x \in \mathcal{O}_K$ mit $\sigma(x) \in B$.

Wir wollen zeigen, daß $K = \mathbb{Q}(x)$, also x ein primitives Element ist. Im Fall $r_1 > 0$ ist $|\sigma_i(x)| \leq \frac{1}{2}$ für $i \neq 1$. Die Norm $|N_{K/\mathbb{Q}}(x)| = \prod_{i=1}^{n} |\sigma_i(x)|$ ist eine positive ganze Zahl, also ist $|\sigma_1(x)| \geq 1$ und damit $\sigma_1(x) \neq \sigma_i(x)$ für $i \neq 1$. Wäre x nicht primitiv, käme $\sigma_1(x)$ mit Multiplizität $[K : \mathbb{Q}(x)]$ vor, ein Widerspruch.

Im Fall $r_1 = 0$ sieht man analog $|\sigma_1(x)| = |\overline{\sigma_1(x)}| \geq 1$ und damit $\sigma_1(x) \neq \sigma_j(x)$, wenn σ_j nicht gleich σ_1 oder $\overline{\sigma_1}$ ist. Aus der Definition von B folgt aber $\mathrm{Re}\,\sigma_1(x) \leq \frac{1}{4}$. Damit kann $\sigma_1(x)$ nicht reell sein, also $\sigma_1(x) \neq \overline{\sigma_1(x)}$. Wie vorher muß x primitiv sein.

Nach der Definition von B müssen die Konjugierten $\sigma_i(x)$ von x beschränkt sein. Damit sind auch die Koeffizienten des Minimalpolynoms von x durch eine Konstante beschränkt, die nur von d abhängt. In $\mathbb{Z}[X]$ gibt es nur endlich viele Polynome mit Grad n und beschränkten Koeffizienten. Also gibt es nur endlich viele Möglichkeiten für $x \in \mathbb{C}$ und damit nur endlich viele Zahlkörper $K = \mathbb{Q}(x)$. □

6.4 Beispiele

Beispiel 6.22. *Wir wollen die Klassenzahl von $K = \mathbb{Q}(\sqrt{-5})$ berechnen. Es ist $r_1 = 0$ und $r_2 = 1$. Nach Beispiel 3.24 ist $d_K = -20$. Die Minkowski-Schranke ist also*

$$\frac{4}{\pi}\frac{2!}{2^2}\sqrt{20} \sim 2,847$$

Wir betrachten also die Ideale $I \subseteq \mathcal{O}_K$ mit $N(I) = 2$. Nach Beispiel 4.20 ist $(2) = (2, \sqrt{-5}+1)^2$, also ist $\mathfrak{p}_2 = (2, \sqrt{-5}+1)$ das einzige Ideal mit Norm 2.

Die Klassengruppe wird von $\mathfrak{p}_2$ erzeugt, und aus der obigen Faktorisierung haben wir die offensichtliche Relation $\mathfrak{p}_2^2 \sim 1$ in der Klassengruppe. Wir haben in Beispiel 4.20 auch gesehen, daß $\mathfrak{p}_2$ kein Hauptideal ist. Also ist $\mathrm{Cl}(\mathcal{O}_K) \cong \mathbb{Z}/2\mathbb{Z}$. □

Mit der so erhaltenen Information über Idealfaktorisierungen in $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$ kann man Aussagen über Lösungen von Gleichungen machen:

Übungsaufgabe 6.3. *Zeigen Sie, daß die Gleichung $x^2 + 5 = y^3$ keine ganzzahligen Lösungen hat.*

Es gibt nicht viele bekannte Gesetzmäßigkeiten für Größe und Struktur der Klassengruppe. Selbst im Fall quadratischer Zahlkörper gibt es noch offene Fragen.

Satz 6.23 (Baker,Stark-Heegner)**.** *Sei $d < 0$ quadratfrei. Dann ist die Klassenzahl von $\mathbb{Q}(\sqrt{d})$ gleich 1 genau dann, wenn*

$$d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$

Es gibt also nur 9 quadratfreie Zahlen $d < 0$, für die der entsprechende Ganzheitsring $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ ein Hauptidealring ist. Die ersten fünf davon sind euklidisch, die letzten vier nicht. Allgemeiner hat Heilbronn gezeigt, daß für $d \to \infty$ auch die Klassenzahl $h_{\mathbb{Q}(\sqrt{-d})} \to \infty$. Anders gesagt gibt es nur endlich viele quadratfreie $d < 0$ mit beschränkter Klassenzahl. Diese Aussagen wurden bereits von Gauß vermutet.

Zur Klassenzahl reell quadratischer Körper ist sehr wenig bekannt. Vermutungsweise gibt es unendlich viele quadratfreie $d > 0$, für die $\mathbb{Q}(\sqrt{d})$ Klassenzahl 1 hat. Auch diese Vermutung geht auf Gauß zurück. Die (experimentell belegte) Cohen-Lenstra-Heuristik formuliert noch deutlich präzisere Vermutungen über die Struktur von Klassengruppen von quadratischen Zahlkörpern.

Vermutung 6.24 (Cohen-Lenstra-Heuristik, $D < 0$)**.** *Sei p eine ungerade Primzahl. Für $r \in \mathbb{N} \cup \{\infty\}$ sei $(p)_r = \prod_{1 \le k \le r}(1 - p^{-k})$, $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ die Riemannsche Zetafunktion und $A = \prod_{k \ge 2} \zeta(k) \sim 2,29486$. Sei $D < 0$ die Diskriminante eines imaginär quadratischen Zahlkörpers K. Mit $\mathrm{Cl}_o(\mathcal{O}_K)$ bezeichnen wir den ungeraden Teil der Klassengruppe, also die Untergruppe der Elemente mit ungerader Ordnung.*

(i) Die Wahrscheinlichkeit, daß $\mathrm{Cl}_o(\mathcal{O}_K)$ zyklisch ist, ist gleich

$$\frac{\zeta(2)\zeta(3)}{3(2)_\infty A \zeta(6)} \sim 0,977575.$$

(ii) Für eine ungerade Primzahl p ist die Wahrscheinlichkeit für $p \mid h_K$ gleich $f(p) = 1 - (p)_\infty$. Zum Beispiel ist $f(3) \sim 0,43987$, $f(5) \sim 0,23967$, $f(7) \sim 0,16320$.

(iii) Für eine ungerade Primzahl p ist die Wahrscheinlichkeit, daß die p-Sylow-Untergruppe von $\mathrm{Cl}(\mathcal{O}_K)$ isomorph zu einer gegebenen endlichen abelschen p-Gruppe G ist gleich $(p)_\infty / \#\operatorname{Aut}(G)$.

(iv) Die Wahrscheinlichkeit, daß die p-Sylow-Untergruppe der Klassengruppe $\mathrm{Cl}(\mathcal{O}_k)$ *isomorph zum Produkt von r zyklischen Gruppen ist, ist gleich* $p^{-r^2}(p)_\infty/((p)_r)^2$.

Vermutung 6.25 (Cohen-Lenstra-Heuristik, $D > 0$)**.** *Sei* $D > 0$ *die Diskriminante eines reell quadratischen Zahlkörpers* K.

(i) Für eine ungerade Primzahl ist die Wahrscheinlichkeit für $p \mid h_K$ *ist gleich*

$$1 - \frac{(p)_\infty}{1 - \frac{1}{p}}.$$

(ii) Die Wahrscheinlichkeit, daß $\mathrm{Cl}_o(\mathcal{O}_K)$ *isomorph zu einer gegebenen endlichen abelschen Gruppe ungerader Ordnung g ist, ist*

$$m(G) = \frac{1}{2g(2)_\infty A \sharp \operatorname{Aut}(G)}.$$

Es ist $m(\{0\}) \sim 0,75446$, $m(\mathbb{Z}/3\mathbb{Z}) \sim 0,12574$, *und* $m(\mathbb{Z}/5\mathbb{Z}) \sim 0,03772$.

(iii) Für eine ungerade Primzahl ist die Wahrscheinlichkeit, daß die p-Sylow-Untergruppe von $\mathrm{Cl}(D)$ *Rang r hat gleich* $p^{-r(r+1)}(p)_\infty/((p)_r(p)_{r+1})$.

Zuletzt noch das Klassenzahl-Problem für zyklotomische Zahlkörper. Mit Teilbarkeitsargumenten kann man zeigen, daß $x^n + y^n = z^n$ für $n > 2$ keine nicht-trivialen ganzzahligen Lösungen hat ("Fermats letzter Satz"), wenn die Klassenzahl von $\mathbb{Q}(\zeta_n)$ gleich 1 ist. Der folgende Satz zeigt, daß es nur sehr wenige n gibt, für die das zutrifft.

Satz 6.26 (Uchida,Montgomery,Masley,Oldyzko)**.** *Sei* $n \not\equiv 2 \mod 4$. *Die Klassenzahl von* $\mathbb{Q}(\zeta_n)$ *ist gleich* 1 *genau für die folgenden* $n = 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84$.

Für $n \equiv 2 \mod 4$ *ist die Klassenzahl von* $\mathbb{Q}(\zeta_n)$ *gleich* 1 *genau für die folgenden* $n = 6, 10, 14, 18, 22, 26, 30, 34, 38, 42, 50, 54, 66, 70, 90$.

Insbesondere ist für $n = p$ *eine Primzahl die Klassenzahl von* $\mathbb{Q}(\zeta_p)$ *gleich* 1 *genau dann, wenn* $p \leq 19$.

Allgemeiner heißt eine Primzahl regulär, wenn $p \nmid h_{\mathbb{Q}(\zeta_n)}$. Für diese Primzahlen kann man auch Fermats letzten Satz mit Teilbarkeitsargumenten zeigen, cf. [Was97].

6.5 Exkurs: Konjugationsklassen von Matrizen

Die Jordan-Normalform für Matrizen in $GL_n(k)$ impliziert, daß es für gegebene paarweise verschiedene Eigenwerte $\lambda_1, \ldots, \lambda_n$ bis auf Konjugation genau eine Matrix in $GL_n(k)$ mit diesen Eigenwerten gibt, nämlich $\operatorname{diag}(\lambda_1, \ldots, \lambda_n)$. Anders gesagt, für ein gegebenes separables Polynom $f(X) \in k[X]$ gibt es genau eine Matrix mit diesem charakteristischen Polynom. Über allgemeineren Ringen gilt die Jordan-Normalform nicht mehr. Über $\mathbb{Z}$ bekommt man aber immer noch eine Klassifikation von Matrizen bis auf Konjugation: Für ein separables Polynom $f(X) \in \mathbb{Z}[X]$ gibt es eine Bijektion zwischen Konjugationsklassen von

Matrizen in $M_n(\mathbb{Z})$ mit charakteristischem Polynom $f(X)$ und Idealklassen im Ring $\mathbb{Z}[\theta]$, wobei θ eine Wurzel von $f(X)$ ist. Dies wurde von Latimer und MacDuffee gezeigt[1] und von Taussky vereinfacht[2] Wir geben hier den Beweis von K. Conrad[3]

Satz 6.27. *Sei $f(X) \in \mathbb{Z}[X]$ ein irreduzibles Polynom vom Grad n, und α eine Wurzel von f. Dann gibt es eine Bijektion zwischen der Menge der Konjugationsklassen von Matrizen in $M_n(\mathbb{Z})$ mit charakteristischem Polynom f und der Menge der Idealklassen im Ring $\mathbb{Z}[\alpha]$.*

Beweis. Ein gebrochenes Ideal $I \subseteq \mathbb{Q}(\alpha)$ ist ein freier $\mathbb{Z}$-Modul vom Rang $n = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ mit einem zusätzlichen Endomorphismus $m_\alpha : I \to I$.

Einem gebrochenen Ideal $I \subseteq \mathbb{Q}(\alpha)$ können wir dann nach Wahl einer Basis die darstellende Matrix M_α der Multiplikation mit α zuordnen. Nach Cayley-Hamilton ist $f(M_\alpha) = 0$. Wechsel der Basis ändert die Konjugationsklasse von M_α nicht. Für eine $\mathbb{Z}$-Basis $x_1, \ldots, x_n$ von I ist $ax_1, \ldots, ax_n$ eine $\mathbb{Z}$-Basis von $(a) \cdot I$. Damit erhalten wir eine wohldefinierte Abbildung von Idealklassen in $\mathbb{Z}[\alpha]$ in Konjugationsklassen von Matrizen mit charakteristischem Polynom f.

Sei nun eine Matrix $A \in M_n\mathbb{Z}$ gegeben mit charakteristischen Polynom f. Dann hat $\mathbb{Q}^n$ durch den durch A gegebenen Endomorphismus $x \mapsto Ax$ eine $\mathbb{Q}(\alpha)$-Modulstruktur, da A Einträge in $\mathbb{Z}$ hat sogar eine $\mathbb{Z}[\alpha]$-Modulstruktur. Der so definierte K-Vektorraum ist eindimensional, jedes $0 \neq x \in \mathbb{Q}^n$ liefert also einen Isomorphismus $\phi_x : \mathbb{Q}(\alpha) \to \mathbb{Q}^n$. Das Urbild $\phi_x^{-1}(\mathbb{Z}^n)$ ist ein $\mathbb{Z}[\alpha]$-Untermodul von $\mathbb{Q}(\alpha)$, also ein gebrochenes Ideal. Konjugation von Matrizen induziert einen Basiswechsel des entsprechenden Ideals, und für x_1 und x_2 unterscheiden sich die Ideale nur durch das von $x_1 x_2^{-1}$ erzeugte Hauptideal. Wir erhalten also eine wohldefinierte Abbildung von Konjugationsklassen von Matrizen mit charakteristischem Polynom f in Idealklassen in $\mathbb{Z}[\alpha]$.

Die Abbildungen sind offensichtlich invers zueinander. □

Korollar 6.28. *Sei $f(X) \in \mathbb{Z}[X]$ ein irreduzibles Polynom vom Grad n, sei α eine Wurzel von f und sei $\mathbb{Z}[\alpha] = \mathcal{O}_{\mathbb{Q}(\alpha)}$. Dann ist die Menge der Konjugationsklassen von Matrizen in $M_n(\mathbb{Z})$ mit charakteristischem Polynom f endlich.*

Dies ist eine direkte Konsequenz aus Satz 6.27 und Satz 6.19. Offensichtlich kann man $\mathbb{Z}$ durch einen beliebigen Hauptidealring ersetzen. Die Hauptidealringeigenschaft ist aber notwendig, da die Konstruktion freie Moduln benutzte. Außerdem gilt die Aussage für alle irreduziblen Polynome f, auch ohne die Einschränkung daß $\mathbb{Z}[\alpha]$ schon der Ganzheitsring ist. Dafür muß man allerdings Satz 6.19 entsprechend verallgemeinern. Der ursprüngliche Satz von Latimer und MacDuffee ist für beliebige Polynome formuliert, für den Fall daß f nicht irreduzibel ist, ist aber die Menge der Konjugationsklassen nur dann gleich dem Produkt der Klassenzahlen für die irreduziblen Faktoren, wenn diese Faktoren paarweise Resultante ± 1 haben.

Für den Fall zyklotomischer Körper erhalten wir aus Satz 3.27 und Satz 6.26 die folgende Aussage.

[1] C.G. Latimer and C.C. MacDuffee. A correspondence between classes of ideals and classes of matrices. Ann. of Math. (2) 34 (1933), no. 2, 313–316

[2] O. Taussky. On a theorem of Latimer and MacDuffee. Canadian J. Math. 1, (1949). 300–302.

[3] K. Conrad: Ideal classes and matrix conjugation over $\mathbb{Z}$

Korollar 6.29. *Die Anzahl der Konjugationsklassen von Matrizen in $M_{\varphi(n)}(\mathbb{Z})$ mit Ordnung n ist gleich der Klassenzahl von $\mathbb{Q}(\zeta_n)$. Die Menge der n, für die es in $M_{\varphi(n)}(\mathbb{Z})$ eine einzige Konjugationsklasse von Elementen mit Ordnung n gibt, ist endlich.*

Übungsaufgaben

Übungsaufgabe 6.4. *Bestimmen Sie die Signatur (r_1, r_2) für $K = \mathbb{Q}(\theta)$ in den folgenden Fällen:*

(i) $\theta^3 - \theta^2 - 2\theta - 8 = 0$,

(ii) $\theta^4 + \theta^2 + 2\theta + 1 = 0$

Übungsaufgabe 6.5. *Bestimmen Sie alle Ideale in $\mathcal{O}_{\mathbb{Q}(\sqrt{43})}$, die Norm ≤ 7 haben.*

Übungsaufgabe 6.6. *Berechnen Sie die Klassenzahl von $\mathbb{Q}(\sqrt{34})$.*

Übungsaufgabe 6.7. *Zeigen Sie, dass die Gleichung $a^2 - 47b^2 = \pm 19$ Lösungen in den ganzen Zahlen hat. Betrachten Sie dazu den Ganzheitsring von $K = \mathbb{Q}(\sqrt{47})$:*

(a) Geben Sie die Minkowski-Schranke für $\mathcal{O}_K$ an, und bestimmen Sie alle Ideale von $\mathcal{O}_K$, deren Norm unterhalb der Minkowski-Schranke liegt.

(b) Folgern Sie aus (a), dass die Klassenzahl von $\mathbb{Q}(\sqrt{47})$ gleich 1 ist, indem Sie ein Element mit der Norm 2 finden.

(c) Geben Sie die Primidealfaktorisierung von (19) in $\mathcal{O}_K$ an.

(d) Folgern Sie aus (b) und (c), dass in $\mathcal{O}_K$ ein Element mit der Norm ± 19 existieren muss. Wie erhält man die Lösungen der Ausgangsgleichung?

Übungsaufgabe 6.8. *Sei $I \subseteq \mathcal{O}_K$ ein Ideal mit $I^m = (a)$. Zeigen Sie, daß für $L = K(\sqrt[m]{a})$ gilt $I\mathcal{O}_L = (a)$. Insbesondere gibt es zu jedem Zahlkörper K eine endliche Erweiterung L/K, so daß jedes Ideal von $\mathcal{O}_K$ in $\mathcal{O}_L$ ein Hauptideal wird. Anders gesagt existiert für jedes gebrochene Ideal $I \subseteq K$ ein Element $a \in L$ mit $I = K \cap aL$.*

Übungsaufgabe 6.9. *Geben Sie Repräsentanten für die Konjugationsklassen von Matrizen in $M_2(\mathbb{Z})$ mit den folgenden charakteristischen Polynomen an:*

(i) $f(X) = X^2 + 5$.

(ii) $f(X) = X^2 - 34$.

Übungsaufgabe 6.10. *(i) Sei $\phi : A \to B$ ein Homomorphismus von Dedekindringen. Zeigen Sie, daß ϕ einen Homomorphismus der Klassengruppen $\mathrm{Cl}(A) \to \mathrm{Cl(B)}$ induziert.*

(ii) Sei L/K eine Galoiserweiterung globaler Körper. Zeigen Sie, daß die Galoisgruppe $\mathrm{Gal}(L/K)$ durch die Homomorphismen aus (i) auf der Klassengruppe $\mathrm{Cl}(\mathcal{O}_L)$ operiert.

(iii) Sei L/K eine Galoiserweiterung globaler Körper. Zeigen Sie, daß die Elemente im Bild des Homomorphismus $\mathrm{Cl}(\mathcal{O}_K) \to \mathrm{Cl}(\mathcal{O}_\mathrm{L})$ aus (i) invariant unter der Operation von $\mathrm{Gal}(L/K)$ aus (ii) sind.

Kapitel 7

Die Einheitengruppe

In diesem Kapitel untersuchen wir die multiplikative Gruppe des Zahlrings, die Gruppe der Einheiten. Der Einheitensatz von Dirichlet gibt eine vollständige Beschreibung der Struktur dieser abelschen Gruppe. Wir diskutieren wieder die Beispiele quadratischer Körper.

Sei K ein Zahlkörper. Die multiplikativ invertierbaren Elemente von $\mathcal{O}_K$ heißen Einheiten. Die Einheiten bilden eine Gruppe unter der Multiplikation, die mit $\mathcal{O}_K^\times$ bezeichnet wird. Aus Übungsaufgabe 3.2 wissen wir, daß $\alpha \in \mathcal{O}_K$ genau dann eine Einheit in $\mathcal{O}_K$ ist, wenn $N_{K/\mathbb{Q}}(\alpha) = \pm 1$ ist.

7.1 Der Dirichletsche Einheitensatz

Definition 7.1. *Die logarithmische Einbettung ist definiert durch*

$$L : K^\times \to \mathbb{R}^{r_1+r_2} : x \mapsto (\log|\sigma_1(x)|, \ldots, \log|\sigma_{r_1+r_2}(x)|).$$

Diese Abbildung ist die Zusammensetzung des Ringhomomorphismus $\sigma : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ mit der multiplikativen Betragsfunktion und dem Logarithmus. Damit ist sie offensichtlich ein Gruppenhomomorphismus, d.h. $L(xy) = L(x) + L(y)$.

Satz 7.2. *Sei K ein Zahlkörper, r_1 die Anzahl der reellen und r_2 die Anzahl der Paare konjugiert komplexer Einbettungen. Es gilt*

$$\mathcal{O}_K^\times \cong \mathbb{Z}^{r_1+r_2-1} \times \mu_K,$$

wobei μ_K die Gruppe der Einheitswurzeln in K ist.

Beweis. Sei $L : K^\times \to \mathbb{R}^{r_1+r_2}$ die logarithmische Einbettung, $B \subseteq \mathbb{R}^{r_1+r_2}$ eine kompakte Teilmenge und $B' = L^{-1}(B) \cap \mathcal{O}_K^\times$. Wir wollen zeigen, daß B' endlich ist. Da B beschränkt ist, müssen auch für $x \in B'$ die Beträge $|\sigma_i(x)|$ beschränkt sein. Damit sind die Koeffizienten des charakteristischen Polynoms beschränkt. Dieses ist ganzzahlig, also gibt es nur endlich viele mögliche $x \in B'$.

Aus der Endlichkeit von B' folgt, daß $\ker L \cap \mathcal{O}_K^\times$ eine endliche Gruppe ist. Die Elemente sind notwendig Einheitswurzeln. Da außerdem für die Einheitswurzeln $|\sigma(\zeta_m)|^m = |\sigma(\zeta_m^m)| = |1| = 1$ ist, ist $\ker L$ genau die endliche zyklische Gruppe μ_K der in K enthaltenen Einheitswurzeln.

Aus der Endlichkeit von B' folgt auch, daß $L(\mathcal{O}_K^\times)$ eine diskrete Untergruppe von $\mathbb{R}^{r_1+r_2}$ ist, insbesondere ist $L(\mathcal{O}_K^\times)$ frei von Rang $\leq r_1+r_2$. Die exakte Sequenz $1 \to \ker L \to \mathcal{O}_K^\times \to L(\mathcal{O}_K^\times) \to 1$ zerfällt, es bleibt also die Bestimmung des Ranges von $L(\mathcal{O}_K^\times)$.

Wir zeigen zuerst die einfachere Ungleichung $\operatorname{rk} L(\mathcal{O}_K^\times) \leq r_1+r_2-1$. Da für $x \in \mathcal{O}_K^\times$ immer $\pm 1 = N(x) = \prod_{i=1}^{r_1} \sigma_i(x) \prod_{j=r_1+1}^{r_1+r_2} \sigma_j(x)\overline{\sigma_j(x)}$ gilt, liegt das Bild von $\mathcal{O}_K^\times$ immer in der Hyperebene

$$W = \left\{ (y_1, \ldots, y_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2} \mid \sum_{i=1}^{r_1} y_i + 2 \sum_{j=r_1+1}^{r_1+r_2} y_j = 0 \right\}.$$

Für die Ungleichung $\operatorname{rk} L(\mathcal{O}_K^\times) \geq r_1+r_2-1$ reicht es zu zeigen, daß zu jeder von 0 verschiedenen Linearform $f : W \to \mathbb{R}$ eine Einheit u existiert mit $f(L(u)) \neq 0$. Wir setzen $r = r_1+r_2-1$ und schreiben $f(y) = c_1y_1 + \cdots + c_ry_r$, $c_i \in \mathbb{R}$. Sei $\alpha \geq 2^n(2\pi)^{-r_2}\sqrt{|d_K|}$. Für ein gegebenes Tupel $(\lambda_1, \ldots, \lambda_{r+1})$ mit $\lambda_i > 0$ und $\prod_{i=1}^{r_1} \lambda_i \prod_{j=r_1+1}^{r+1} \lambda_j^2 = \alpha$ definieren wir die kompakte, konvexe, zentralsymmetrische Menge

$$B = \{(y_1, \ldots, y_{r_1}, z_1, \ldots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid |y_i| \leq \lambda_i, |z_j| \leq \lambda_{j+r_1}\},$$

$$\operatorname{vol}(B) = \prod_{i=1}^{r_1} 2\lambda_i \prod_{j=r_1+1}^{r_1+r_2} \pi\lambda_j^2 = 2^{r_1}\pi^{r_2}\alpha \geq 2^{n-r_2}\sqrt{|d_K|}.$$

Mit Korollar 6.8 und Korollar 6.14 gibt es ein $x_\lambda \in \mathcal{O}_K$ mit $\sigma(x_\lambda) \in B$. Es gilt

$$1 \leq |N_{K/\mathbb{Q}}(x_\lambda)| = \prod_{i=1}^{n} |\sigma_i(x_\lambda)| \leq \prod_{i=1}^{r_1} \lambda_i \prod_{j=r_1+1}^{r_1+r_2} \lambda_j^2 = \alpha$$

Damit folgt eine Abschätzung für die Norm

$$|\sigma_i(x_\lambda)| = |N(x_\lambda)| \prod_{j \neq i} |\sigma_j(x_\lambda)|^{-1} \geq \prod_{j \neq i} \lambda_j^{-1} = \lambda_i\alpha^{-1}.$$

Zusammen haben wir die Abschätzung $\lambda_i\alpha^{-1} \leq |\sigma_i(x_\lambda)| \leq \lambda_i$ und damit $0 \leq \log\lambda_i - \log|\sigma_i(x_\lambda)| \leq \log\alpha$. Für die Linearform gilt dann

$$\left| f(L(x_\lambda)) - \sum_{i=1}^{r} c_i \log\lambda_i \right| = \left| \sum_{i=1}^{r} c_i(\log|\sigma_i(x_\lambda)| - \log\lambda_i) \right| \leq \left(\sum_{i=1}^{r} |c_i| \right) \log\alpha.$$

Sei nun $\beta > (\sum_{i=1}^{r} |c_i|)\log\alpha$. Für $h \in \mathbb{N}$ seien $\lambda_{i,h} > 0$, $i = 1, \ldots, r$ so daß $\sum_{i=1}^{r} c_i \log\lambda_{i,h} = 2\beta h$ und $\lambda_{r+1,h}$ so daß $\prod_{i=1}^{r_1} \lambda_i \prod_{j=r_1+1}^{r+1} \lambda_j^2 = \alpha$. Wir setzen $\lambda(h) = (\lambda_{1,h}, \ldots, \lambda_{r+1,h})$ und $x_h = x_{\lambda(h)}$. Nach der vorherigen Abschätzung ist $|f(L(x_h)) - 2\beta h| < \beta$, das bedeutet aber $(2h-1)\beta < f(L(x_h)) < (2h+1)\beta$, also sind die Werte $f(L(x_h))$ paarweise verschieden. Da aber $|N(x_h)| \leq \alpha$ gibt es nur endlich viele verschiedene Ideale der Form $(x_h) \subseteq \mathcal{O}_K$. Also existieren h_1, h_2 mit $(x_{h_1}) = (x_{h_2})$, d.h. $u = x_{h_1}^{-1}x_{h_2}$ ist eine Einheit. Nach der vorherigen Beobachtung ist $f(L(u)) = f(L(x_{h_2})) - f(L(x_{h_1})) \neq 0$. Damit gibt es r_1+r_2-1 linear unabhängige Einheiten. □

Für $r_1 > 0$ ist die Gruppe der in K enthaltenen Einheitswurzeln immer gleich $\mathbb{Z}/2\mathbb{Z} = \{\pm 1\}$. Ein Tupel $(u_1, \ldots, u_{r_1+r_2-1})$ heißt System von Fundamentaleinheiten, wenn es eine Basis des freien Summanden $\mathbb{Z}^{r_1+r_2-1} \subseteq \mathcal{O}_K^\times$ ist.

Definition 7.3. *Sei $(u_1, \ldots, u_{r_1+r_2-1})$ ein System von Fundamentaleinheiten von $\mathcal{O}_K$. Dann heißt*

$$R = |\det(\log|\sigma_i(u_j)|)_{i,j=1}^{r_1+r_2-1}|$$

Regulator des Zahlkörpers K.

7.2 Beispiel: Quadratische Zahlkörper

Für imaginär quadratische Zahlkörper ist $r_1 = 0$ und $r_2 = 1$, also gibt es nur endlich viele Einheiten. Die folgenden Fälle treten auf.

Übungsaufgabe 7.1. *Sei $d < 0$ quadratfrei, $K = \mathbb{Q}(\sqrt{d})$. Dann ist*

$$\mathcal{O}_K^\times = \begin{cases} \mu_4 & d = -1 \\ \mu_3 & d = -3 \\ \mu_2 = \{\pm 1\} & \text{sonst} \end{cases}$$

Für reell quadratische Zahlkörper ist $r_1 = 1$ und $r_2 = 0$, die Einheitengruppe ist also isomorph zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$. Ein Erzeuger des unendlichen Summanden kann durch die Forderung $u > 1$ ausgezeichnet werden. Die folgende Aussage ist genau die Umformulierung der Bedingung $N(x) = \pm 1$. Die Einheiten reell quadratischer Zahlkörper stehen also in direktem Zusammenhang mit den Lösungen der sogenannten Pellschen Gleichung.

Proposition 7.4. *(i) Sei $d \equiv 2, 3 \mod 4$. Die Einheiten von $\mathcal{O}_K$ sind genau die Elemente $a + b\sqrt{d}$ für die $a^2 - db^2 = \pm 1$ ist.*

(ii) Sei $d \equiv 1 \mod 4$. Die Einheiten von $\mathcal{O}_K$ sind genau die Elemente $\frac{a+b\sqrt{d}}{2}$ mit $a^2 - db^2 = \pm 4$.

Die Lösungen der Pellschen Gleichung $a^2 - db^2 = \pm 1, \pm 4$ kann man mit Hilfe der Kettenbruchentwicklung für $\sqrt{d}$ bestimmen. Ein endlicher Kettenbruch ist ein Ausdruck der Form

$$[a_0, \ldots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}$$

Für eine unendliche Folge a_i kann man den unendlichen Kettenbruch

$$[a_0, a_1, \ldots] = \lim_{n\to\infty} [a_0, \ldots, a_n]$$

definieren. Der Satz von Euler-Lagrange besagt, daß genau die quadratischen irrationalen Zahlen (Nullstellen von irreduziblen Polynomen in $\mathbb{Q}[X]$ vom Grad 2) durch periodische unendliche Kettenbrüche dargestellt werden können.

Übungsaufgabe 7.2. *Sei α eine quadratische Irrationalzahl. Dann existieren $P_0, Q_0, d \in \mathbb{Z}$ mit*

$$\alpha = \frac{P_0 + \sqrt{d}}{Q_0}, \qquad Q_0 \mid (d - P_0^2).$$

Wir definieren rekursiv:

$$\alpha_k = \frac{P_k + \sqrt{d}}{Q_k}, \qquad a_k = \lfloor \alpha_k \rfloor, \qquad P_{k+1} = a_k Q_k - P_k, \qquad Q_{k+1} = \frac{d - P_{k+1}^2}{Q_k}.$$

Dann ist $[a_0, a_1, \dots]$ eine unendliche Kettenbruchentwicklung von α.

Beispiel 7.5. *Die vorherige Algorithmus zur Kettenbruchentwicklung für $\sqrt{13}$ sieht wie folgt aus:*

$$\alpha_0 = \sqrt{13}, a_0 = 3, P_1 = 3, Q_1 = 4$$

$$\alpha_1 = \frac{3 + \sqrt{13}}{4}, a_1 = 1, P_2 = 1, Q_2 = 3$$

$$\alpha_2 = \frac{1 + \sqrt{13}}{3}, a_2 = 1, P_3 = 2, Q_3 = 3$$

$$\alpha_3 = \frac{2 + \sqrt{13}}{3}, a_3 = 1, P_4 = 1, Q_4 = 4$$

$$\alpha_4 = \frac{1 + \sqrt{13}}{4}, a_4 = 1, P_5 = 3, Q_5 = 1$$

$$\alpha_5 = 3 + \sqrt{13}, a_5 = 6, P_6 = 3, Q_6 = 4$$

Die Kettenbruchentwicklung für $\sqrt{13}$ ist damit $[3; \overline{1, 1, 1, 1, 6}]$. Die endlichen Kettenbrüche sind

$$3, 4, \frac{7}{2}, \frac{11}{3}, \frac{18}{5}, \frac{119}{33}, \frac{137}{38}, \frac{256}{71}, \frac{393}{109}, \frac{649}{180}, \frac{4287}{1189}, \dots$$

In dieser Liste tauchen alle Lösungen für $a^2 - 13b^2 = \pm 1, \pm 4$ auf. Wenn für den Bruch $\frac{a}{b}$ gilt $a^2 - 13b^2 = \pm 4$, dann ist $\frac{a + b\sqrt{13}}{2}$ ein Element mit Norm ± 1. Wenn $a^2 - 13b^2 = \pm 1$ gilt, ist $a + b\sqrt{13}$ ein Element mit Norm ± 1.

Der erste Bruch liefert die Fundamentaleinheit $\frac{3+\sqrt{13}}{2}$. Wenn n die Periode der Kettenbruchentwicklung bezeichnet, liefert der $(n-1)$-te Bruch die Fundamentallösung der Gleichung $a^2 - db^2 = \pm 1$. Hier ist das also der fünfte Bruch, das Lösungstupel ist $(18, 5)$, entsprechend dem Element $18 + 5\sqrt{13}$ mit Norm -1. Die "kleinste" Lösung von $a^2 - 13b^2 = 1$ ist dann durch den zehnten Bruch gegeben, nämlich $(649, 180)$. Die Potenzen von $649 + 180\sqrt{13}$ liefern dann alle Lösungen von $a^2 - 13b^2 = 1$. □

Übungsaufgaben

Übungsaufgabe 7.3. *Zeigen Sie, daß jeder Zahlkörper vom Grad $2k + 1$ nur die Einheitswurzeln ± 1 besitzt.*

Übungsaufgabe 7.4. *Sei $K = \mathbb{Q}(\theta)$ mit $\theta^3 - 2\theta - 3 = 0$. Bestimmen Sie ein Inverses zu $(-\theta^2 - 2\theta - 2)$ in $\mathcal{O}_K$.*

Übungsaufgabe 7.5. *Zeigen Sie, daß die Gleichung* $a^2 - 47b^2 = \pm 19$ *unendlich viele Lösungen hat. Was können Sie über das Vorzeichen auf der rechten Seite aussagen? Geben Sie alle Lösungen der Gleichung an.*

Übungsaufgabe 7.6. *Sei* $n \geq 3$ *und* ζ_n *eine primitive* n*-te Einheitswurzel. Zeigen Sie, daß die folgenden Elemente in* $\mathcal{O}_{\mathbb{Q}(\zeta_n)}$ *Einheiten sind:*

$$\frac{1-\zeta_n^i}{1-\zeta_n}, \qquad ggT(i,n) = 1.$$

Die durch diese Einheiten erzeugte Untergruppe heißt Gruppe der Kreiseinheiten. Diese Untergruppe ist im Allgemeinen nicht die ganze Einheitengruppe, der Index ist im Wesentlichen die Klassenzahl $h_{\mathbb{Q}(\zeta_n)}$*, cf. [Was97, Kap. 8].*

Kapitel 8

Algorithmen II

In diesem Kapitel geht es um die Berechnung von Klassengruppe und Einheitengruppe. Dafür benutzt man die Gittertheorie, insbesondere den LLL-Algorithmus, der die Konstruktion von "kleinen" Gitterbasen ermöglicht. Die Berechnung der Einheitengruppe kann durch eine effektive Variante von Dirichlets Einheitensatz erfolgen. Für die Erzeuger der Klassengruppe braucht man gute Schranken an Idealnormen, für die Relationen der Klassengruppe muß man Normgleichungen lösen.

8.1 Gitter und Normen

Wir werden später sehen, wie Gittertheorie auf Fragestellungen der algebraischen Zahlentheorie – insbesondere die Klassen- und Einheitengruppen – angewendet wird. Wir wollen hier bereits ein wenig auf algorithmische Aspekte der Gittertheorie eingehen. Für ein gegebenes Gitter $\Lambda \subseteq V$ in einem Vektorraum V gibt es verschiedene algorithmische Probleme:

(i) *shortest vector problem (SVP):* Gegeben eine Basis $x_1, \ldots, x_n$ von Λ und eine Norm $\|\cdot\|$ auf V, finde den $\|\cdot\|$-kürzesten Vektor in Λ. Dieses Problem ist NP-hart, also schwierig. Der LLL-Algorithmus kann benutzt werden um "ziemlich kurze" Vektoren zu finden, er löst das Problem aber nur näherungsweise.

(ii) *closest vector problem (CVP):* Gegeben eine Basis $x_1, \ldots, x_n$ von Λ, eine Metrik d auf V und einen Vektor $v \in V$, finde den d-nächsten Gitterpunkt zu v.

(iii) *shortest basis problem:* Gegeben eine Basis $x_1, \ldots, x_n$ von Λ und eine Norm $\|\cdot\|$ auf V, finde eine neue Basis $y_1, \ldots, y_n$, so daß $\max \|y_i\|$ minimal ist. Auch hier kann der LLL-Algorithmus benutzt werden, um gute Näherungslösungen in angemessener Zeit zu finden.

Diese algorithmischen Probleme tauchen in vielen Bereichen immer wieder auf: integer programming/ganzzahlige lineare Optimierung, diophantische Approximierung, algebraische Relationen zwischen transzendenten Zahlen, Faktorisierung von Polynomen in $\mathbb{Z}[X]$ (dies war die ursprüngliche Anwendung des

LLL-Algorithmus), Faktorisierung von ganzen Zahlen. Aufgrund ihrer Schwierigkeit finden Gitteralgorithmen insbesondere auch Anwendung in der Kryptographie.

Wir betrachten jetzt zusätzlich zum Gitter $\Lambda \subseteq \mathbb{R}^n$ noch eine quadratische Form bzw. ein Skalarprodukt auf $\mathbb{R}^n$. Dadurch können wir über die Länge von Vektoren und reduzierte Basen sprechen.

Definition 8.1. *Sei K ein Körper mit Charakteristik $\neq 2$ und V ein K-Vektorraum. Eine Abbildung $q : V \to K$ heißt quadratische Form, wenn die beiden folgenden Aussagen erfüllt sind:*

(i) Für $\lambda \in K$ und $v \in V$ ist $q(\lambda v) = \lambda^2 q(v)$.

(ii) $b(x, y) = \frac{1}{2}(q(x + y) - q(x) - q(y))$ ist eine symmetrische Bilinearform.

Aus der symmetrischen Bilinearform bekommt man die quadratische Form durch $q(x) = b(x, x)$. Im Folgenden sei $K = \mathbb{R}$ und q zusätzlich positiv definit, d.h. $q(v) > 0$ für alle $0 \neq v \in V$. Die Übersetzung zwischen Normen und quadratischen Formen ist durch $\|\cdots\| = \sqrt{q(\cdot)} = \sqrt{b(\cdot, \cdot)}$ gegeben.

Wir betrachten Tupel (Λ, q) wobei λ ein freier $\mathbb{Z}$-Modul vom Rang n und q eine quadratische Form auf $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$. Zwei solche Tupel (Λ, q) und (Λ', q') heißen isomorph (oder isometrisch), wenn es einen Isomorphismus von $\mathbb{Z}$-Moduln $\phi : \Lambda \to \Lambda'$ gibt mit $q'(\phi(v)) = \phi(q(v))$ für alle $v \in \Lambda \otimes_{\mathbb{Z}} \mathbb{R}$. Für eine Basis $x_1, \ldots, x_n$ von Λ heißt die Matrix $q_{ij} = b(x_i, x_j)$ die *Gram-Matrix* zur Basis $x_1, \ldots, x_n$.

Proposition 8.2. *Es gibt eine natürliche Bijektion zwischen*

(i) Isometrieklassen von Tupeln (Λ, q), wobei Λ ein freier $\mathbb{Z}$-Modul vom Rang n und q eine quadratische Form auf $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$, und

(ii) Doppelnebenklassen $O(n) \setminus GL_n(\mathbb{R})/GL_n(\mathbb{Z})$.

Der Schritt (i)⇒(ii) ordnet einem Tupel (Λ, q) und einer Basis $x_1, \ldots, x_n$ die Doppelnebenklasse der Gram-Matrix $Q(x_1, \ldots, x_n)$ zu. Dies bestimmt die Isometrieklasse von (Λ, q) eindeutig. Jede Doppelnebenklasse enthält die Gram-Matrix einer gewählten Basis $x_1, \ldots, x_n$ eines Tupels (Λ, q).

Die Nebenklassen $O(n) \setminus GL_n\mathbb{R}$ haben nach der Polarzerlegung eindeutige positiv definite symmetrische Matrizen als Repräsentanten. Die Wirkung von $GL_n\mathbb{Z}$ auf diesen Nebenklassen $O(n)\setminus GL_n\mathbb{R}$ ist durch Konjugation $Q \mapsto P^t QP$, $P \in GL_n(\mathbb{Z})$.

Wir erinnern kurz an das Gram-Schmidt-Orthogonalisierungsverfahren. Hier wollen wir eine orthogonale Basis eines Vektorraums finden, die Länge der Vektoren soll nicht unbedingt gleich 1 sein.

Proposition 8.3. *Sei $v_1, \ldots, v_n$ die Basis eines euklidischen Vektorraums V. Wir definieren induktiv*

$$v_i^* = v_i - \sum_{j=1}^{i-1} \mu_{ij} v_j^*,\ 1 \leq i \leq n, \qquad \mu_{ij} = \frac{b(v_i, v_j^*)}{b(v_j^*, v_j^*)},\ 1 \leq j < i \leq n.$$

Die $v_1^*, \ldots, v_n^*$ formen eine Orthogonalbasis von V, das Volumen des durch $v_1, \ldots, v_n$ erzeugten Gitters ist durch $\mathrm{vol}(\Lambda)^2 = \prod q(v_i^*)$ gegeben. Hierbei ist das Volumen $\mathrm{vol}(\Lambda)$ bezüglich der Norm q aufzufassen.

Korollar 8.4 (Hadamard-Ungleichung)**.** *Sei (Λ, q) ein Gitter mit quadratischer Form, $v_1, \ldots, v_n$ eine $\mathbb{Z}$-Basis von Λ. Dann gilt* $\operatorname{vol}(\Lambda) \leq \prod \sqrt{|q(v_i)|}$.

Beweis. Es gilt

$$q(v_i) = b(v_i, v_i) = b\left(v_i^* + \sum_{j=1}^{i-1} \mu_{ij} v_j^*, v_i^* + \sum_{j=1}^{i-1} \mu_{ij} v_j^*, \right) = q(v_i^*) + \sum_{j=1}^{i-1} \mu_{ij}^2 q(v_j^*).$$

Damit folgt

$$\operatorname{vol}(\Lambda)^2 = \prod_{i=1}^{n} |q(v_i^*)| \leq \prod_{i=1}^{n} |q(v_i)|.$$

□

Nun geht es um die Frage, wie kurz man die Vektoren einer Basis wählen kann.

Definition 8.5. *Sei $\Lambda \subseteq \mathbb{R}^n$ ein Gitter, q eine quadratische Form auf $\mathbb{R}^n$ und für $i = 1, \ldots, n$ sei $M_i(\Lambda) \in \mathbb{R}$, $M_i(\Lambda) > 0$ minimal mit der Eigenschaft, daß linear unabhängige Elemente $v_1, \ldots, v_i \in \Lambda$ existieren mit $\sqrt{q(v_j)} \leq M_i(\Lambda)$ für $1 \leq j \leq i$. Die $M_1(\Lambda), \ldots, M_n(\Lambda)$ heißen* sukzessive Minima *des Gitters Λ bezüglich q.*

Insbesondere ist M_1 die Länge eines kürzesten Vektors in Λ. Die sukzessiven Minima sind Isometrieinvarianten, sie bleiben also bei einer isometrischen Transformation des Gitters erhalten. Mit den sukzessiven Minima kann man auch einen Reduziertheitsbegriff formulieren: Eine Gitterbasis $x_1, \ldots, x_n$ ist reduziert, wenn die Quotienten $\frac{\|x_i\|}{M_i}$ möglichst klein sind.

Definition 8.6 (Hermite-Konstante)**.** *Für $n \in \mathbb{N}$ ist die* Hermite-Konstante γ_n *wie folgt definiert:*

$$\gamma_n = \sup \left\{ \frac{M_1(\Lambda)^2}{(\operatorname{vol} \Lambda)^{\frac{2}{n}}} \mid \Lambda \subseteq \mathbb{R}^n \text{ Gitter} \right\}.$$

Die Werte der Hermiteschen Konstanten sind nur für $1 \leq n \leq 8$ und 24 bekannt.

$$\gamma_1 = 1, \gamma_2 = \sqrt{\frac{4}{3}}, \gamma_3 = \sqrt[3]{2}, \gamma_4 = \sqrt[4]{4}, \gamma_5 = \sqrt[5]{8},$$

$$\gamma_6 = \sqrt[6]{\frac{64}{3}}, \gamma_7 = \sqrt[7]{64}, \gamma_8 = \sqrt[8]{256}.$$

Für $1 \leq n \leq 8$ werden sie von Gittern zu euklidischen Spiegelungsgruppen realisiert, zum Beispiel wird γ_2 durch die Kachelung der Ebene mit gleichseitigen Dreiecken realisiert. Sukzessive Minima und Gittervolumen stehen in der folgenden Beziehung:

Satz 8.7 (Minkowski-Ungleichung)**.** *Für jedes Gitter $\Lambda \subseteq \mathbb{R}^n$ gilt*

$$\operatorname{vol}(\Lambda) \leq \prod_{i=1}^{n} M_i \leq \gamma_n^{n/2} \operatorname{vol}(\Lambda).$$

Mit den sukzessiven Minima kann außerdem der Gitterpunktsatz von Minkowski deutlich verbessert werden. Dafür definiert man die sukzessiven Minima bezüglich einer konvexen zentralsymmetrischen Menge S durch

$$M_k(\Lambda, S) = \inf \{\lambda > 0 \mid \mathrm{rk}_{\mathbb{Z}} \langle \Lambda \cap \lambda S \rangle \geq k\}.$$

Insbesondere ist $M_1(\Lambda, S) < 1$ genau dann, wenn das Innere von S einen Gitterpunkt enthält, $M_1(\Lambda, S) = 1$ genau dann, wenn der Rand von S einen Gitterpunkt enthält. Mit dem zweiten Satz von Minkowski kann man also durch sukzessive Minima auch eine Bedingung angeben, wann eine konvexe Teilmenge schon eine Gitterbasis enthält.

Satz 8.8 (Zweiter Satz von Minkowski)**.** *Sei $\Lambda \in V$ ein Gitter, S eine konvexe zentralsymmetrische Teilmenge und $M_1, \ldots, M_n$ die sukzessiven Minima von Λ bezüglich S. Dann gilt*

$$\frac{\mathrm{vol}(\Lambda)}{n!} \leq \frac{\mathrm{vol}(S)}{2^n} \prod_{i=1}^{n} M_i \leq \mathrm{vol}\,\Lambda.$$

Für die einfachere Form des Gitterpunktsatzes hat man nur $\frac{\mathrm{vol}(S)}{2^n} M_1 \leq \mathrm{vol}\,\Lambda$.

Für ein Gitter $\Lambda \subseteq \mathbb{R}^n$ und eine quadratische Form q auf $\mathbb{R}^n$ kann man auf der Menge der Basen von Λ eine Ordnungsrelation (eine lexikographische Ordnung) definieren. Für zwei Basen v_i und w_j ist $(v_1, \ldots, v_n) < (w_1, \ldots, w_n)$ genau dann, wenn es $1 \leq j \leq n$ gibt, so daß $q(v_j) < q(w_j)$ und für alle $1 \leq i \leq j-1$ gilt $q(v_i) = q(w_i)$. Ein bezüglich dieser Ordnung minimales Element heißt *Minkowski-reduzierte Basis*. Eine Minkowski-reduzierte Basis besteht aus kürzest-möglichen Vektoren. Die Hermite-Konstanten geben Schranken für die Längen der Vektoren an. Die Berechnung einer Minkowski-reduzierten Basis ist aber aufwendig.

8.1.1 LLL-Algorithmus

Da die Berechnung von Minkowski-reduzierten Basen sehr aufwendig ist, sucht man nach anderen Begriffen von Reduziertheit, die sich leichter berechnen lassen. Ein solcher Begriff mit dem zugehörigen Reduktionsalgorithmus wurde in von Lenstra, Lenstra und Lovász[1] vorgeschlagen. Dieser Algorithmus wird nach seinen Konstrukteuren LLL-Algorithmus bezeichnet.

Definition 8.9. *Sei V ein euklidischer Vektorraum, $\Lambda \subseteq V$ ein Gitter und $b_1, \ldots, b_n$ eine Basis von Λ. Wir bezeichnen mit $b_1^*, \ldots, b_n^*$ die dazugehörige Orthogonalbasis. Die Basis $b_1, \ldots, b_n$ heißt* LLL-reduziert*, wenn die folgenden Bedingungen erfüllt sind:*

(LLL i) $|\mu_{ij}| \leq \frac{1}{2}, \qquad 1 \leq j < i \leq n$

(LLL ii) $q(b_i^* + \mu_{i,i-1} b_{i-1}^*) \geq \frac{3}{4} q(b_{i-1}^*), \qquad 1 < i \leq n.$

Die Notation ist die aus Proposition 8.3.

[1] A.K. Lenstra, H.W. Lenstra, Jr. und L. Lovász. Factoring polynomials with rational coefficients. Math. Ann. 261 (1982), no. 4, 515–534.

Lemma 8.10. *Sei V ein euklidischer Vektorraum, $\Lambda \subseteq V$ ein Gitter in V und $b_1, \ldots, b_n$ eine LLL-reduzierte Basis von Λ. Dann gelten die folgenden Aussagen:*

(i) $q(b_j) \leq 2^{\frac{i-1}{2}} q(b_i^*), \qquad 1 \leq j \leq i \leq n,$

(ii) $\mathrm{vol}(\Lambda) \leq \prod_{i=1}^{n} \sqrt{q(b_i)} \leq 2^{\frac{n(n-1)}{4}} \mathrm{vol}(\Lambda),$

(iii) $\sqrt{q(b_1)} \leq 2^{\frac{n-1}{4}} \sqrt[n]{\mathrm{vol}(\Lambda)},$

(iv) $q(b_1) \leq 2^{n-1} q(x)$ *für alle* $0 \neq x \in \Lambda,$

(v) $q(b_j) \leq 2^{n-1} \max\{q(x_1), \ldots, q(x_k)\}, 1 \leq j \leq k$ *für* $1 \leq t \leq n$ *und* $x_1, \ldots, x_k$ *linear unabhängige Vektoren in* Λ.

Beweis. Zu (i): Die Bedingung (LLL ii) ist unter (LLL i) äquivalent zu

$$q(b_i^*) \geq \left(\frac{3}{4} - \mu_{i,i-1}^2\right) q(b_{i-1}^*) \geq \frac{1}{2} q(b_{i-1}^*).$$

Induktiv erhält man daraus $q(b_j^*) \geq 2^{i-j} q(b_i^*)$ für $i \geq j$. Damit folgt

$$q(b_i) = q(b_i^*) + \sum_{j=1}^{i-1} \mu_{ij} q(b_j^*) \leq \left(1 + \frac{2^i - 2}{4}\right) q(b_i^*) \leq 2^{i-1} q(b_i^*).$$

(ii) folgt aus der Hadamard-Ungleichung Korollar 8.4 und (i).

Zu (iii): aus (ii) haben wir $\sqrt{q(b_1)} \leq 2^{\frac{i-1}{2}} \sqrt{q(b_i^*)}$ für alle $1 \leq i \leq n$. Dann ist

$$\sqrt[n]{\sqrt{q(b_1)}^n} \leq \sqrt[n]{\prod_{i=1}^{n} 2^{\frac{i-1}{2}} \sqrt{q(b_i^*)}} = \sqrt[n]{2^{\frac{n(n-1)}{4}} \mathrm{vol}(\Lambda)} = 2^{\frac{n-1}{4}} \sqrt[n]{\mathrm{vol}(\Lambda)}.$$

(iv) Wir schreiben $x = \sum z_i b_i = \sum s_i b_i^*$ mit $z_i \in \mathbb{Z}$ und $s_i \in \mathbb{R}$. Dann gilt nach Definition von b_i^* schon $z_i = s_i$ für den größten Index i mit $s_i \neq 0$. Also gilt $q(x) \geq s_i q(b_i^*) \geq q(b_i^*)$. Nach (ii) ist $2^{n-1} q(b_i^*) \geq q(b_1)$. Analog erhält man (v). □

Diese Abschätzungen führen zum angegebenen Algorithmus. Dieser Algorithmus liefert zu einer gegebenen Basis in $O(n^6 \log^3 B)$ Schritten eine LLL-reduzierte Basis, wobei n der Rang des Gitters und B eine Schranke für die Größe der Ausgangsbasis ist. Korrektheit des Algorithmus ist offensichtlich, die Terminierung des Algorithmus wird in [Coh93, 2.6.3] diskutiert.

Für die Berechnung der Klassengruppe und die Lösung von Normgleichungen benötigt man effiziente Methoden zur Aufzählung aller Gitterpunkte mit beschränkter Norm. Sei also ein Gitter Λ und eine quadratische Form q gegeben. Gesucht sind alle Gitterpunkte $x \in \Lambda$ mit $q(x) \leq C$. Wir schreiben mit quadratischer Ergänzung

$$q(x) = \sum_{i=1}^{n} q_{ii} \left(x_i + \sum_{j=i+1}^{n} q_{ij} x_j\right)^2.$$

Eingabe: Basisvektoren $b_1, \ldots, b_n$ eines n-dimensionalen Gitters in $\mathbb{R}^m$,
q ein Skalarprodukt
Ausgabe: LLL-reduzierte Basis $b'_1, \ldots, b'_n$, Basiswechselmatrix H
$k \longleftarrow 2$, $k_{\max} \longleftarrow 1$, $b_1^* \longleftarrow b_1$, $B_1 \longleftarrow b(b_1^*, b_1^*)$, $H \longleftarrow I_n$;
while $k \leq n$ **do**
  if $k \not\leq k_{\max}$ **then**
    $k_{\max} \longleftarrow k$;
    for $j = 1$ **to** $k-1$ **do**
      $\mu_{k,j} \longleftarrow \frac{b(b_k, b_j^*)}{B_j}$, $b_k^* \longleftarrow b_k - \mu_{k,j} b_j^*$, $B_k \longleftarrow q(b_k^*)$;
    end
  end
  $noswap \longleftarrow false$;
  repeat
    $RED(k, k-1)$;
    if $B_k < (\frac{3}{4} - \mu_{k,k-1}^2) B_{k-1}$ **then**
      Vertausche b_k und b_{k-1} und die Spalten H_k und H_{k-1};
      if $k > 2$ **then**
        for $j = 1$ **to** $k-2$ **do** Vertausche $\mu_{k,j}$ und $\mu_{k-1,j}$;
      end
      $\mu \longleftarrow \mu_{k,k-1}$, $B \longleftarrow B_k + \mu^2 B_{k-1}$, $\mu_{k,k-1} \longleftarrow \mu B_{k-1}/B$;
      $b \longleftarrow b_{k-1}^*$, $b_{k-1}^* \longleftarrow b_k^* + \mu b$;
      $b_k^* \longleftarrow -\mu_{k,k-1} b_k^* + (B_k/B) b$, $B_k \longleftarrow B_{k-1} B_k / B$, $B_{k-1} \longleftarrow B$;
      for $i = k+1$ **to** $k_{\max}$ **do**
        $t \longleftarrow \mu_{i,k}$, $\mu_{i,k} \longleftarrow \mu_{i,k-1} - \mu t$, $\mu_{i,k-1} \longleftarrow t + \mu_{k,k-1} \mu_{i,k}$;
      end
      $k \longleftarrow \max(2, k-1)$;
    else
      $noswap \longleftarrow true$;
    end
  until $noswap = true$;
  for $l = \max(1, k-2)$ **to** 1 **do** $RED(k, l)$;
  $k \longleftarrow k+1$;
end

Algorithm 5: LLL-Algorithmus

if $|\mu_{k,l}| > \frac{1}{2}$ **then**
  $q \longleftarrow \lfloor \frac{1}{2} + \mu_{k,l} \rfloor$, $b_k \longleftarrow b_k - q b_l$, $H_k \longleftarrow H_k - q H_l$, $\mu_{k,l} \longleftarrow \mu_{k,l} - q$;
  for $i = 1$ **to** $l-1$ **do**
    $\mu_{k,i} \longleftarrow \mu_{k,i} - q \mu_{l,i}$;
  end
end

Algorithm 6: Reduktionsschritt $RED(k, l)$

Eingabe: reelle symmetrische $(n \times n)$-Matrix A entspr. einer quadratischen Form $q(x) = x^t Ax$
Ausgabe: Matrix R mit $A = R^t R$, entsprechend q_{ij} mit $q(x) = \sum_{i=1}^{n} q_{ii} \left(x_i + \sum_{j=i+1}^{n} q_{ij} x_j \right)^2$.
for $1 \le i \le j \le n$ **do** $q_{ij} \longleftarrow a_{ij}$;
$i \longleftarrow 0$;
repeat
  $i \longleftarrow i + 1$;
  for $j = i + 1$ **to** n **do** $q_{ji} \longleftarrow q_{ij}$, $q_{ij} \longleftarrow q_{ij}/q_{ii}$;
  for $i + 1 \le k \le l \le n$ **do** $q_{kl} \longleftarrow q_{kl} - q_{ki} q_{il}$;
until $i = n$;
for $i = 1$ **to** n **do** $r_{ii} \longleftarrow \sqrt{q_{ii}}$;
for $1 \le j < i \le n$ **do** $r_{ij} \longleftarrow 0$;
for $1 \le i < j \le n$ **do** $r_{ij} \longleftarrow r_{ii} q_{ij}$;

Algorithm 7: Cholesky-Zerlegung

Ein Gitterpunkt $x \in \Lambda$ mit $q(x) \le C$ erfüllt dann die folgenden Ungleichungen für $1 \le i \le n$:

$$q_{ii} \left(x_i + \sum_{j=i+1}^{n} q_{ij} x_j \right)^2 \le C - \sum_{\nu=i+1}^{n} q_{\nu\nu} \left(x_\nu + \sum_{j=\nu+1}^{n} q_{\nu j} x_j \right)^2 =: T_i$$

Man bestimmt zuerst alle $x_n \in \Lambda$, für die x_n die obige Ungleichung für $i = n$ erfüllt. Iterativ bestimmt man dann alle möglichen x_{n-1}, etc. Auf diese Weise kann man alle Gitterpunkte mit beschränkter Norm aufzählen. Dieselbe Methode liefert auch einen Algorithmus für das CVP, das Problem des nächsten Vektors, cf. [Poh93, III.4.2]. Wir geben hier den Algorithmus zum Aufzählen von Gitterpunkten von Fincke und Pohst an.

Eingabe: reelle symmetrische $(n \times n)$-Matrix A nach Cholesky-Zerlegung
Ausgabe: alle Vektoren $x \in \mathbb{Z}^n$ mit $Q(x) \le C$
1. $i \longleftarrow n$, $T_i \longleftarrow C$, $U_i \longleftarrow 0$;
2. $Z \longleftarrow \sqrt{T_i/q_{ii}}$, $L_i \longleftarrow \lfloor Z - U_i \rfloor$, $x_i \longleftarrow \lceil -Z - U_i \rceil - 1$;
3. $x_i \longleftarrow x_i + 1$;
if $x_i > L_i$ **then** $i \longleftarrow i + 1$, gehe zu 3;
4. **if** $i > 1$ **then**
  $T_{i-1} \longleftarrow T_i - q_{ii}(x_i + U_i)^2$, $i \longleftarrow i - 1$, $U_i \longleftarrow \sum_{j=i+1}^{n} q_{ij} x_j$;
  gehe zu 2;
end
5. **if** $x \neq 0$ **then**
  Lösung x gefunden mit $q(x) = C - T_1 + q_{11}(x_1 + U_1)^2$;
  gehe zu 3;
end

Algorithm 8: Fincke-Pohst-Algorithmus

Das Auffinden kürzester Gitterpunkte bzw. das Aufzählen von Gitterpunkten mit beschränkter Norm sind NP-vollständig, ist also (unter der Annahme

Eingabe: reelle symmetrische $(n \times n)$-Matrix A entspr. einer quadratischen Form $Q(x) = x^t Ax$, $C >$ eine Konstante
Ausgabe: alle Vektoren $x \in \mathbb{Z}^n$ mit $Q(x) \leq C$
$R \longleftarrow$ Cholesky-Zerlegung von A;
Matrizen $S, U \longleftarrow$ LLL-Reduktion von R^{-1}, i.e. $S^{-1} = U^{-1}R^{-1}$, $U \in GL_n\mathbb{Z}$;
`// bezeichne` s_i `Spalten von` S`,` s'_i `Zeilen von` S^{-1}
Finde Permutation σ mit $||s'_{\sigma(1)}|| \geq ||s'_{\sigma(2)}|| \geq \cdots \geq ||s'_{\sigma(n)}||$;
Wende Permutation σ auf die Spalten von S an;
$A_1 \longleftarrow S^tS$, berechne Koeffizienten der durch A_1 definierten quadratischen Form $q_1(x) = x^tA_1x$;
Fincke-Pohst-Algorithmus auf Q_1 anwenden findet alle y mit $q_1(y) \leq C$;
Transformation $x = U(y_{\sigma^{-1}(1)}, \ldots, y_{\sigma^{-1}(n)})^t$;

Algorithm 9: modifizierter Fincke-Pohst-Algorithmus

$P \neq NP$) ein schwieriges Problem, für das es keine schnellen Algorithmen gibt.

8.2 Berechnung von Grundeinheiten

Aus dem Dirichletschen Einheitensatz ist die Struktur der Einheitengruppe bekannt. Die Berechnung der Einheitengruppe zerfällt dann in zwei Aufgaben: einerseits die Berechnung der Einheitswurzeln in K, andererseits die Berechnung einer Basis des freien Teils, also von Fundamentaleinheiten. Kompliziert ist hier die Berechnung von Fundamentaleinheiten. Dafür benutzt man die logarithmische Einbettung aus Definition 7.1, die schon im Beweis des Einheitensatzes eine zentrale Rolle spielte.

In diesem Abschnitt sei K ein Zahlkörper vom Grad n mit Signatur (r_1, r_2). Wir schreiben $r = r_1 + r_2 - 1$.

Für Fundamentaleinheiten $u_1, \ldots, u_r$ war der Regulator durch die folgende Determinante definiert:

$$R = |\det(\log|\sigma_i(u_j)|)_{i,j=1}^r|$$

Dieselbe Definition kann man für eine Basis einer beliebigen Untergruppe $U \subseteq \mathcal{O}_K^\times$ vom endlichen Index machen, man spricht dann vom *Regulator der Untergruppe* U. Man sieht dann

$$[\mathcal{O}_K^\times : U] = \frac{\mathrm{Reg}(U)}{\mathrm{Reg}(\mathcal{O}_K^\times)}.$$

Für eine gegebene Gruppe U von Einheiten liefert eine untere Schranke an den Regulator $R = \mathrm{Reg}(\mathcal{O}_K^\times)$ dann eine obere Schranke für den Index $[\mathcal{O}_K^\times : U]$.

Die Berechnung der Einheitengruppe erfolgt also in drei Schritten:

(i) Zuerst bestimmt man eine untere Schranke für den Regulator des Zahlkörpers, dabei erhält man alle Einheitswurzeln.

(ii) Dann bestimmt man r linear unabhängige Einheiten. Dies kann durch eine effektive Variante des Einheitensatzes erfolgen und liefert eine Untergruppe $U \subseteq \mathcal{O}_K^\times$ vom endlichen Index.

(iii) Dann vergrößert man die Untergruppe aus Schritt (ii) schrittweise, bis man eine Basis von $\mathcal{O}_K^\times$ erhält.

Man beachte die formale Analogie zur Berechnung des Ganzheitsrings: auch dort beginnt man mit einer Untergruppe vom endlichen Index, die Diskriminante liefert eine Schranke für diesen Index, und man vergrößert die Untergruppe schrittweise so lange, bis man den Ganzheitsring bestimmt hat.

Eine gute *Regulatorschranke* wurde von Fieker und Pohst[2] bewiesen. Sei K ein Zahlkörper vom Grad n, $\sigma_1, \ldots, \sigma_n$ die $\mathbb{Q}$-Einbettungen von K in einen gewählten algebraischen Abschluß $\overline{\mathbb{Q}}$. Man betrachtet dann die Funktion

$$Q : \mathcal{O}_K^\times \to \mathbb{R} : u \mapsto \sum_{j=1}^{n} (\log(|\sigma_j(u)|))^2.$$

Der Definition sieht man an, daß es eine enge Beziehung zwischen Q und der logarithmischen Einbettung gibt. Die Funktion Q ist eine quadratische Form auf $\mathcal{O}_K^\times$, und ihre Diskriminante (also die Determinante einer Matrix A mit $Q(x) = x^t Ax$) ist $\det(Q) = 2^{-r_2} n \operatorname{Reg}(\mathcal{O}_K^\times)^2$. Eine untere Schranke für den Regulator erhält man nach Satz 8.7 aus den sukzessiven Minima der logarithmischen Einbettung

$$M_1 \cdots M_r \leq \gamma_r \det(Q) = \frac{1}{2^{r_2}} n \gamma_r \operatorname{Reg}(\mathcal{O}_K^\times)^2.$$

Eine bessere untere Schranke erhält man wie folgt: für eine gewählte Konstante $C \geq (1+\sqrt{2})n$ betrachten wir

$$S_C := \{\alpha \in \mathcal{O}_K \mid T_2(\alpha) < C\} \cup \{\alpha \in K \mid \alpha^{-1} \in \mathcal{O}_K, T_2(\alpha^{-1}) < C\},$$

$$\text{wobei } T_2(\alpha) = \sum_{j=1}^{n} \sigma_j(\alpha)^2.$$

Die Menge S_C kann mit Hilfe des Fincke-Pohst-Algorithmus berechnet werden, es geht hier auch wieder um die Aufzählung von Gitterpunkten mit beschränkter Norm. Aus $C > n$ und $|\sigma(\zeta_n)| = 1$ folgt, daß die Einheitswurzeln notwendig in S_C enthalten sind.

Wir nehmen an, daß S_C schon m linear unabhängige Einheiten $u_1, \ldots, u_m$ enthält. Dann wählen wir j so, daß für jedes u_i höchstens j verschiedene Konjugierte $\sigma_l(u_i)$ Absolutbetrag 1 haben und definieren

$$C^* = \frac{n-j}{4} \operatorname{arcosh}^2\left(\frac{C-j}{n-j}\right),$$

$$M_i^* = \min\{C^* \mid \exists u_1, \ldots, u_i \in \mathcal{O}_K^\times \cap S_C \text{ lin. unabh.}, Q(u_i) \leq C\}$$

für $1 \leq i \leq m$ und $M_i^* = C^*$ für $m+1 \leq i \leq r$. Zuletzt definieren wir

$$\widetilde{M_i} = \frac{n-j}{4} \operatorname{arcosh}^2\left(\frac{M_i^*-j}{n-j}\right).$$

Dann gilt

[2] C. Fieker und M.E. Pohst. A lower regulator bound for number fields. J. Number Theory 128 (2008), no. 10, 2767–2775.

Proposition 8.11. *Sei $u \in \mathcal{O}_K^\times$ eine Einheit mit $T_2(u) \geq M_i^*$ und $T_2(u^{-1}) \geq M_i^*$. Dann gilt $Q(u) \geq \widetilde{M_i}$. Insbesondere gilt für den Regulator die folgende Abschätzung*

$$\mathrm{Reg}(\mathcal{O}_K^\times) \geq \sqrt{\frac{\widetilde{M_1} \cdots \widetilde{M_r} 2^{r_2}}{n \gamma_r^{r/2}}}.$$

Zusammen mit den Hermite-Konstanten nach Satz 8.7 für $r \leq 8$, $\gamma_9 \leq 1248$ und

$$\gamma_r \leq \left(\frac{2}{\pi}\right)^r \Gamma\left(1 + \frac{r+2}{2}\right)^2, \quad r \geq 10$$

erhält man so eine gute untere Schranke für den Regulator $\mathrm{Reg}(\mathcal{O}_K^\times)$.

Die *Konstruktion von r unabhängigen Einheiten* wird durch eine konstruktive Variante vom Beweis des Dirichletschen Einheitensatzes erreicht[3]. Sei $I = \{i_1, \ldots, i_\mu\} \subseteq \{1, \ldots, r_1 + r_2\}$ eine Teilmenge und $J = \{1, \ldots, r_1 + r_2\} \setminus I$. Wir bezeichnen

$$\tilde{I} = I \cup \{i_\nu + r_2 \mid i_\nu > r_1, 1 \leq \nu \leq \mu\}, \tilde{\mu} = \#\tilde{I}, \tilde{J} = \{1, \ldots, n\} \setminus \tilde{I}.$$

Man berechnet dann eine Sequenz von Elementen $\beta_{I,k} \in \mathcal{O}_K$ und Moduln $M_{I,k}$ mit den folgenden Eigenschaften:

$$\beta_{I,0} = 1, M_{I,0} = \mathcal{O}_K, \beta_{I,k+1} \in M_{I,k}, M_{I,k+1} = \frac{1}{\beta_{I,k+1}} M_{I,k},$$

$$|\sigma_j(\beta_{I,k+1})| < 1 \forall j \in \tilde{I},\ |\sigma_j(\beta_{I,k+1})| \geq 1 \forall j \in \tilde{J},\ \prod_{i=0}^{k+1} |N_{K/\mathbb{Q}}(\beta_{I,i})| \leq \tilde{C}.$$

Dabei ist $\tilde{C} > 0$ eine festgelegte Konstante. Man kann dann eine Sequenz von Elementen $\gamma_{I,k}$ definieren:

$$\gamma_{I,0} = 1,\ \gamma_{I,k} = \prod_{i=0}^{k} \beta_{I,i}.$$

Für Indizes μ, ν mit $M_{I,\mu} = M_{I,\nu}$ erhält man dann eine Einheit

$$\epsilon_j = \frac{\gamma_{I,\mu}}{\gamma_{I,\nu}} = \prod_{k=\nu+1}^{\mu} \beta_{I,k}.$$

Die Existenz von Indizes wie oben folgt wie im Beweis des Einheitensatzes, cf. Satz 7.2.

Die $\beta_{I,k+1}$ werden mit Hilfe des LLL-Algorithmus bestimmt. Man wählt $\delta > 0$ geeignet und setzt

$$\lambda_j = d \forall j \in \tilde{J}, \lambda_j = d^{1 - \frac{n}{\tilde{\mu}}} \forall j \in \tilde{I},\ \text{insbesondere } \prod_{j=1}^{n} \lambda_j = 1.$$

[3] J. Buchmann und A. Pethő. Computation of independent units in number fields by Dirichlet's method. Math. Comp. 52 (1989), no. 185, 149–159

Für eine Basis $x_1, \ldots, x_n$ von $M_{I,k}$ definiert man eine quadratische Form $T_{2,\lambda}(x)$

$$T_{2,\lambda}(x) = \sum_{j=1}^{n} \lambda_j^2 \left| \sum_{i=1}^{n} \mu_i \sigma_j(x_i) \right|^2, x = \mu_1 x_1 + \cdots \mu_n x_n \in \mathcal{O}_K.$$

Das Element $\beta_{I,k+1}$ wird dann als erster Vektor einer LLL-reduzierten Basis von $M_{I,k}$ mit der Form $T_{2,\lambda}$ gewählt. Die oben formulierten Forderungen an $\beta_{I,k}$ folgen dann aus der Definition von LLL-reduziert, cf. [Poh93, VI.2.D]. Wie im Beweis des Einheitensatzes Satz 7.2 erhält man dann r linear unabhängige Einheiten, wenn man die obigen Berechnungen für verschiedene Indexmengen, z.B. $I_1 = \{1\}, \ldots, I_r = \{r\}$ macht. Mehr Indexmengen bietet den Vorteil der Parallelisierbarkeit und ermöglichen es, Einheiten mit kleinen Koeffizienten (bzgl. der Ganzheitsbasis) zu finden.

Für den letzten Schritt benutzt man die folgende Proposition:

Proposition 8.12. *Sei ζ ein Erzeuger von μ_K, sei $U \subseteq \mathcal{O}_K^\times$ vom endlichen Index gegeben durch Einheiten $u_1, \ldots, u_r$ und sei $B \geq [\mathcal{O}_K^\times : U]$. Wenn für alle Primzahlen $p \leq B$ und alle ganzen Zahlen $0 \leq m_i \leq p$ die Gleichung*

$$X^p = \zeta^{m_0} u_1^{m_1} \cdots u_r^{m_r}$$

keine Lösung in $\mathcal{O}_K$ hat, dann sind die $u_1, \ldots, u_r$ Fundamentaleinheiten, bilden also eine Basis von $\mathcal{O}_K^\times$.

Beweis. Offensichtlich ist eine Lösung der obigen Gleichung eine noch nicht in U enthaltene Einheit. Wenn die Gleichung für alle Primzahlen $p \leq B$ und alle ganzen Zahlen $0 \leq m_i \leq p$ nicht lösbar ist, dann muß offensichtlich der Index $[\mathcal{O}_K^\times : U]$ größer als B sein, das ist aber nach Voraussetzung nicht möglich. □

Sei K ein Zahlkörper vom Grad n, $x_1, \ldots, x_n$ eine Ganzheitsbasis, $\sigma_1, \ldots, \sigma_n$ die verschiedenen Einbettungen. Zur Lösung der Gleichung $X^m = \alpha$ setzt man $\lambda_j = \sqrt[m]{\sigma_j(\alpha)}$ und definiert dann für $x = \mu_1 x_1 + \cdots \mu_n x_n \in \mathcal{O}_K$

$$T_{2,\lambda}(x) = \sum_{j=1}^{n} \lambda_j^2 \left| \sum_{i=1}^{n} \mu_i \sigma_j(x_i) \right|^2.$$

Damit gilt für alle Lösungen der Gleichung $X^m = \alpha$ die "Normgleichung" $T_{2,\lambda}(x) = n$.

Mit dem Fincke-Pohst-Algorithmus kann man somit alle Lösungen der Gleichungen $X^p = \zeta^{m_0} u_1^{m_1} \cdots u_r^{m_r}$ aufzählen und auf diese Weise die Gruppe U schrittweise bis $\mathcal{O}_K^\times$ vergrößern. Außerdem findet man auf diese Weise auch alle Einheitswurzeln in $\mathcal{O}_K^\times$. Mit der beschriebenen Methode muß man ungefähr p^r viele Gleichungen lösen, dies kann durch weitere Argumente auf die Größenordnug $r + 1$ reduziert werden, cf. [Poh93, VI.3].

8.3 Berechnung der Klassengruppe

Auf die Berechnung der Klassengruppe gehen wir hier nicht sehr detailliert ein. In Beispiel 6.22 hatten wir die Minkowski-Schranke berechnet, alle Primideale

unter der Minkowski-Schranke faktorisiert und dann mit Normgleichungen argumentiert, daß ein gefundenes Ideal kein Hauptideal ist. Nach dem gleichen Muster funktioniert auch der Algorithmus zur Berechnung der Klassengruppe, allerdings mit vielen technischen Verfeinerungen.

Ein wesentlicher Punkt ist die Größe der Minkowski-Schranke. Es ist sehr aufwendig, alle Ideale unterhalb der Minkowski-Schranke zu faktorisieren und Relationen zwischen diesen Idealen zu finden, wenn die Diskriminante des Zahlkörpers groß ist. Es gibt eine verbesserte Schranke von Bach[4], nach der jede Idealklasse einen Repräsentanten mit Norm $\leq 12 \log^2 |d_K|$ besitzt. Diese Schranke ist allerdings nur unter Annahme der erweiterten Riemannschen Hypothese (ERH) richtig. Sie wird in Pari/GP genutzt. Man sollte sich allerdings immer der Tatsache bewußt sein, daß Klassengruppenberechnungen, wenn sie nicht durch `bnfcertify` verifiziert wurden nur unter Annahme der erweiterten Riemannschen Hypothese gültig sind.

Die Berechnung der Klassengruppe läuft dann wie im obigen Beispiel: man faktorisiert alle Ideale (p) für $p \leq 12 \log^2 |d_K|$. Dies liefert eine Liste von Idealen, die (unter ERH) ein Erzeugendensystem für die Klassengruppe enthält.

Ein Ideal mit Norm n ist genau dann ein Hauptideal, wenn es ein Element mit Norm n enthält. Mit Hilfe des LLL-Algorithmus bzw. des Fincke-Pohst-Algorithmus kann man alle Elemente $x \in \mathcal{O}_K$ aufzählen, die Norm n haben und überprüfen, ob das jeweilige Element ein Erzeuger des Ideals ist. Auf diese Weise kann man testen, ob ein gegebenes Ideal ein Hauptideal ist.

Damit erhält man dann die Relationen der Klassengruppe: man kann alle möglichen Potenzen der endlich vielen Ideale bilden. Wegen der Endlichkeit der Klassengruppe muß eine Potenz ein Hauptideal sein, mit dem obigen Test findet man dann die Ordnung der jeweiligen Ideale in der Klassengruppe. Dann kann man alle möglichen Produkte bilden und wieder nach Hauptidealen suchen, damit findet man dann alle Relationen in der Klassengruppe.

So wie oben beschrieben ist dieses Verfahren sehr langwierig. Es gibt viele technische Verbesserungen, die es ermöglichen dieses Verfahren zu beschleunigen. Dies sind allerdings hauptsächlich Implementierungsfragen. Die Grundidee ist immer noch dieselbe wie in Beispiel 6.22.

8.4 Klassen- und Einheitengruppe in Pari/GP

Die folgende Zeile ermittelt die Klassengruppen und Regulatoren für alle reell quadratischen Körper mit Diskriminante ≤ 1000. Dabei führt die Funktion `isfundamental(n)` einen Test aus, ob n die Diskriminante eines quadratischen Zahlkörpers ist, und `quadclassunit` liefert einen Vektor dessen Komponenten die Klassenzahl, die Struktur der Klassengruppe und, Erzeuger der einzelnen zyklischen Summanden und den Regulator enthalten. Die Programmausgabe ist nur ausschnittweise angedeutet.

```
? for(n=2,1000,if(isfundamental(n),print([n,quadclassunit(n)])));
...
[665, [2, [2], [Qfb(2, 25, -5, 0.E-38)],
   10.219684191557813476134991801]]
```

[4] E. Bach. Explicit bounds for primality testing and related problems. Math. Comp. 55 (1990), no. 191, 355–380.

```
[668, [1, [], [], 5.81710230213576281762682 4543]]
[669, [1, [], [], 12.629001045503912977406896 90]]
[673, [1, [], [], 32.212174294579240650807472 81]]
[677, [1, [], [], 3.951613336082065540026529081]]
[680, [4, [2, 2],
  [Qfb(13, 2, -13, 0.E-38), Qfb(7, 20, -10, 0.E-38)],
  3.259572556262921561296584731]]
[681, [1, [], [], 30.698438128293577523350818 74]]
[685, [2, [2], [Qfb(3, 25, -5, 0.E-38)],
  6.632003513258114905870712376]]
[689, [4, [4], [Qfb(8, 23, -5, 0.E-38)],
  5.347084854209184791455226173]]
[696, [2, [2], [Qfb(10, 16, -11, 0.E-38)],
  7.973155314701886653592549634]]
[697, [6, [6], [Qfb(3, 25, -6, 0.E-38)],
  5.575963450863238908574232162]]
[701, [1, [], [], 10.067475404442529264225951 85]]
[705, [2, [2], [Qfb(10, 15, -12, 0.E-38)],
  13.069641694930572943689515 69]]
[709, [1, [], [], 17.412565799224712882340530 70]]
[712, [2, [2], [Qfb(19, 16, -6, 0.E-38)],
  8.071530796022351693010529459]]
[713, [1, [], [], 16.173788980975779541034160 37]]
[716, [1, [], [], 15.941408590534062038308136 90]]
...
```

Mit dem folgenden Programm kann man die Cohen-Lenstra-Heuristik nachvollziehen. Nach Durchlauf des Programms enthält die Variable `a` die Anzahl der quadratischen Zahlkörper mit Diskriminante ≤ 10000, und g die Anzahl der quadratischen Zahlkörper, für die der ungerade Anteil der Klassengruppe trivial ist – dies wird mit `s=s/2^valuation(s,2)` erreicht. Man kann sehen, wie notwendig die Einschränkung auf den ungeraden Anteil ist, wenn man diese Zeile im Programm wegläßt. Analog kann man durch Modifikation der Zeile `if(s==1,g++)` andere Teile der Cohen-Lenstra-Heuristik verstehen. Mit `if(valuation(s,p)==v,g++)` könnte man genau den Anteil der reellquadratischen Zahlkörper mit Diskriminante ≤ 10000 ermitteln, für die die p-Bewertung der Klassenzahl eine gegebene Zahl v ist.

```
? a=0;g=0;
  for(n=2,10000,
    if(isfundamental(n),
      a++;
      s=quadclassunit(n)[1];s=s/2^valuation(s,2);
      if(s==1,g++))); g/a+0.0
%1 = 0.884653302661846861649687 8081
? ... for(n=2,100000, ...
%2 = 0.835329341317365269461077 8443
? ... if(valuation(s,3)==1,g++) ...
%3 = 0.077883667433453828458757 80480
? ... if(s==7,g++) ....
%4 = 0.009201445941505093657574761748
```

Mit `contfrac` kann man Kettenbruchentwicklungen zum Lösen der Pellsche Gleichung berechnen lassen. Die Kettenbruchentwicklung für $\sqrt{13}$ aus Beispiel 7.5 kann man wie folgt realisieren. Mit `contfracpnqn` kann man die einzelnen Brüche in der Kettenbruchentwicklung erhalten.

```
? contfrac(sqrt(13))
%1 = [3, 1, 1, 1, 1, 6, 1, 1, 1, 1, 6, 1, 1, 1, 1, 6,
  1, 1, 1, 1, 6, 1, 1, 1, 1, 6, 1, 1, 1, 1, 6, 1, 1, 1, 1, 6,
  1, 1, 1, 1, 6, 1, 1, 1, 1, 6]
? contfracpnqn([3,1,1,1,1])
%2 = [18 11] [5 3]
? contfracpnqn([3,1,1,1,1,6,1,1,1,1,6])
%3 = [4287 649] [1189 180]

? contfrac(sqrt(103))
%4 = [10, 6, 1, 2, 1, 1, 9, 1, 1, 2, 1, 6, 20,
          6, 1, 2, 1, 1, 9, 1, 1, 2, 1, 6, 20,
          6, 1, 2, 2]
? contfracpnqn([10,6,1,2,1,1,9,1,1,2,1,6])
%5 =
[227528 33877] [22419 3338]

? 227528^2-103*22419^2
%6 = 1

? f=Pol([1,0,-103]);
? nf=bnfinit(f);
? bnfcertify(f);
? nf.fu
%10 = [Mod(22419*x + 227528, x^2 - 103)]
```

In diesem Fall finden wir wieder die Fundamentallösung der Pellschen Gleichung $(18, 5)$, die wir schon in Beispiel 7.5 ermittelt hatten. Ebenso tritt nach der nächsten Periode die erste positive Lösung auf. Wir geben auch noch ein Beispiel für etwas größere Zahlen.

Durch `bnfinit` werden automatisch Klassen- und Einheitengruppe berechnet. Hierbei wird für die Berechnung der Klassengruppe allerdings die Bach- und nicht die Minkowski-Schranke benutzt. Die Ergebnisse von `bnfinit` sind somit nur unter der Annahme der erweiterten Riemannschen Hypothese gültig. Um wirklich gültige Ergebnisse zu bekommen, muß man immer noch die Funktion `bnfcertify` aufrufen, die dann wirklich die Minkowski-Schranke benutzt. Wir betrachten den Zahlkörper $\mathbb{Q}(\zeta_{23})$, der erste zyklotomische Körper mit nichttrivialer Klassengruppe, cf. Satz 6.26.

```
? f=polcyclo(23);
? nf=bnfinit(f);
  *** bnfinit: the PARI stack overflows !
  current stack size: 4000000 (3.815 Mbytes)
  [hint] you can increase GP stack with allocatemem()

? allocatemem()
```

```
  *** allocatemem: Warning: doubling stack size;
  new stack = 8000000 (7.629 Mbytes).
? nf=bnfinit(f);
? bnfcertify(nf)
  *** bnfcertify: Warning: large Minkowski bound:
  certification will be VERY long.
  *** bnfcertify: not enough precomputed primes,
  need primelimit ~ 9324407.
? nfbasistoalg(nf,idealtwoelt(nf,nf.clgp.gen[1]))
%6 = [Mod(47, ...), Mod(x - 12, ...)]
```

Die Klassengruppe von $\mathbb{Q}(\zeta_{23})$ wird also von $(47, \zeta_{23} - 12)$ erzeugt. Bereits in diesem Beispiel haben wir nicht mehr `bnfcertify` ausgeführt und vertrauen auf die Richtigkeit der Ergebnisse.

Nach Aufruf von `bnfinit` kann man die Klassengruppe unter `clgp`, den Regulator unter `reg`, und die Fundamental- bzw. Torsionseinheiten unter `fu` und `tu` abrufen. In unserem Standardbeispiel $K = \mathbb{Q}(\theta)$ mit $\theta^3 - \theta^2 - 2\theta - 8 = 0$ haben wir also triviale Klassengruppe, Regulator $\sim 7,027$, eine Fundamentaleinheit $3\theta^2 - 13\theta + 13$ und (wegen der reellen Einbettung) nur die Einheitswurzeln ± 1.

```
? f=Pol([1,-1,-2,-8]);
? nf=bnfinit(f);
? bnfcertify(nf)
%3 = 1
? nf.clgp
%4 = [1, [], []]
? nf.reg
%5 = 7.0273467933610955236852570 95
? nf.fu
%6 = [Mod(3*x^2 - 13*x + 13, x^3 - x^2 - 2*x - 8)]
? nf.tu
%7 = [2, Mod(-1, x^3 - x^2 - 2*x - 8)]
```

Wir lassen noch die Fundamentaleinheiten für einen zyklotomischen Körper ausrechnen, die drei Punkte sind jeweils durch das zyklotomische Polynom $\Phi_{17}(x)$ zu ersetzen.

```
? f=polcyclo(17);
? nf=bnfinit(f);
? bnfcertify(nf)
%3 = 1
? nf.reg
%4 = 3640.012213375972735646592782
? nf.fu
%5 = [Mod(x^3 + x^2, ...), Mod(x^14 + x^3, ...),
  Mod(x^12 + x^11 + x^10 + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 +
    x^3 + x^2, ...),
  Mod(x^15 + x, ...), Mod(x^8 + x^3, ...), Mod(x^10 + x^8, ...),
  Mod(x^15 + x^6, ...)]
? nf.tu
%6 = [34, Mod(-x^3, ...)]
```

Erwartungsgemäß gibt es $\frac{\phi(17)}{2} - 1$ Fundamentaleinheiten, und die Einheitswurzelgruppe wird erzeugt von einer primitiven 17-ten Einheitswurzel, wenn auch nicht der offensichtlichen.

Kapitel 9

Zerlegung und Verzweigung von Primidealen

In diesem Kapitel diskutieren wir die relative Situation, also das Verhalten von Ganzheitsringen und Primidealen in Erweiterungen L/K von Zahlkörpern. Die relative Diskriminante liefert Information über die Verzweigung und die Existenz relativer Ganzheitsbasen. Im Fall von Galois-Erweiterungen gibt es einfachere Gesetzmäßigkeiten für die Zerlegung von Primidealen. Wir diskutieren eingehender das Beispiel zyklotomischer Erweiterungen.

9.1 Vorüberlegungen zur Lokalisierung von Ringen und Moduln

Definition 9.1. *Sei R ein Ring und M ein R-Modul. Eine Teilmenge $S \subseteq R \setminus \{0\}$ heißt* multiplikativ abgeschlossen*, wenn sie die 1 enthält und unter Multiplikation abgeschlossen ist. Für eine multiplikativ abgeschlossene Teilmenge $S \subseteq R \setminus \{0\}$ definieren wir die folgende Äquivalenzrelation auf $M \times S$:*

$$(m, s) \sim (m', s') \text{ genau dann, wenn } (ms' - m's)u = 0 \text{ für ein } u \in S.$$

Wir definieren den Ring $S^{-1}R = (R \times S)/\sim$.

Beispiel 9.2.

Für einen Integritätsbereich R ist $S = R \setminus \{0\}$ multiplikativ abgeschlossen. Der Ring $S^{-1}R$ ist ein Körper, der Körper der Brüche oder Quotientenkörper von R.

Für einen Integritätsbereich R und ein Primideal $\mathfrak{p} \subseteq R$ ist $S = R \setminus \mathfrak{p}$ multiplikativ abgeschlossen. Der Ring $R_\mathfrak{p} := S^{-1}R$ ist ein lokaler Ring mit maximalem Ideal $\mathfrak{p}R_\mathfrak{p}$.

Für einen Integritätsbereich R und ein Element $f \in R \setminus \{0\}$ ist $S = \{f^n \mid n \geq 0\}$ multiplikativ abgeschlossen. □

Proposition 9.3. *Sei R ein Ring, $S \subseteq R$ eine multiplikativ abgeschlossene Teilmenge. Dann existiert eine ordnungserhaltende Bijektion zwischen der Menge*

der Primideale von $S^{-1}R$ und der Menge der zu S disjunkten Primideale von R.

Proposition 9.4. *Sei R ein Ring, M ein R-Modul. Dann sind die beiden folgenden Aussagen äquivalent:*

(i) $M = 0$.

(ii) $M_\mathfrak{p} = 0$ *für alle Primideale* $\mathfrak{p} \subseteq R$.

Sei $f : M \to N$ ein R-Modulhomomorphismus. Dann sind die beiden folgenden Aussagen äquivalent:

(i) f ist injektiv bzw. surjektiv.

(ii) $f_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$ ist injektiv bzw. surjektiv.

Proposition 9.5. *Sei R ein Integritätsbereich, $A \subseteq R$ ein Teilring, $S \subseteq A$ eine multiplikativ abgeschlossene Teilmenge und B der ganze Abschluß von A in R. Dann ist $S^{-1}B$ der ganze Abschluß von $S^{-1}A$ in $S^{-1}R$.*

Beweis. Ein Element von $S^{-1}B$ hat die Form b/s mit $b \in B, s \in S$. Für b haben wir eine Ganzheitsgleichung $b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$, die man durch s^n teilt, um die Ganzheitsgleichung für b/s zu erhalten:

$$\left(\frac{b}{s}\right)^n + \frac{a_{n-1}}{s}\left(\frac{b}{s}\right)^{n-1} + \cdots + \frac{a_0}{s^n} = 0.$$

Umgekehrt hat man für ein Element $x/s \in S^{-1}R$, $x \in R, s \in S$, das ganz über $S^{-1}A$ ist, eine Ganzheitsgleichung

$$\left(\frac{x}{s}\right)^n + \frac{a_{n-1}}{t_{n-1}}\left(\frac{b}{s}\right)^{n-1} + \cdots + \frac{a_0}{t_0} = 0.$$

Durchmultiplizieren mit $(t_0 t_1 \cdots t_{n-1})^n$ zeigt, daß $xt_0 \cdots t_{n-1}/s$ ganz über A ist. Also $xt_0 \cdots t_{n-1}/s \in B$ und $x/s = (1/t_0 \cdots t_{n-1})(xt_0 \cdots t_{n-1}/s) \in S^{-1}B$. □

Korollar 9.6. *Die Lokalisierung eines Dedekind-Rings ist wieder ein Dedekind-Ring.*

Beweis. Nach Proposition 9.3 ist die Lokalisierung eines Dedekind-Rings ist wieder noethersch mit Krull-Dimension 1. Nach Proposition 9.5 ist sie auch ganz-abgeschlossen. □

Proposition 9.7. *Sei A ein Integritätsbereich, $S \subseteq A$ eine multiplikativ abgeschlossene Teilmenge und $\mathfrak{m} \subseteq A$ ein maximales Ideal mit $\mathfrak{m} \cap S = \emptyset$. Dann gilt*

$$S^{-1}A/\mathfrak{m}S^{-1}A \cong A/\mathfrak{m}.$$

Beweis. Der Ringhomomorphismus $A \to S^{-1}A \to S^{-1}A/\mathfrak{m}S^{-1}A$ hat Kern $\mathfrak{m}S^{-1}A \cap A = \mathfrak{m}$, also haben wir einen injektiven Ringhomomorphismus $\phi : A/\mathfrak{m} \to S^{-1}A/\mathfrak{m}S^{-1}A$.

Sei $x = a/s \in S^{-1}A$ und bezeichne $\overline{x}$ die Restklasse von x in $S^{-1}A/\mathfrak{m}S^{-1}A$. Nach Voraussetzung ist $s \notin \mathfrak{m}$. Da $\mathfrak{m}$ maximal ist, existiert $b \in A$ mit $bs \equiv 1 \mod \mathfrak{m}$. Damit ist

$$\frac{a}{s} - ab = \frac{a}{s}(1 - bs) \in \mathfrak{m}S^{-1}A,$$

also ist $\phi(ab) = \overline{x}$. □

9.2 Gradformel

Sei A ein Dedekind-Ring mit Quotientenkörper K und L/K eine separable Erweiterung. Sei B der ganze Abschluß von A in L. Nach Satz 2.7, Korollar 3.20 und einem Argument wie in Proposition 4.8 ist B wieder ein Dedekind-Ring.

Sei $(0) \neq \mathfrak{p} \subseteq A$ ein Primideal. Dann gibt es nach Satz 4.15 eine Faktorisierung

$$B\mathfrak{p} = \prod_{i=1}^{q} \mathfrak{P}_i^{e_i},$$

wobei die $\mathfrak{P}_i$ paarweise verschiedene Primideale von B sind und $e_i \geq 0$.

Eine direkte Konsequenz aus dem Satz über die Idealfaktorisierung Satz 4.15 ist die Tatsache, daß die Primideale $\mathfrak{P}_i$ genau die Primideale $\mathfrak{Q}$ von B mit $\mathfrak{Q} \cap A = \mathfrak{p}$ sind. Folglich ist die kanonische Abbildung $A/\mathfrak{p} \to B/\mathfrak{P}_i$ ein injektiver Homomorphismus von Körpern. Da nach Korollar 3.20 der Ring B ein endlich erzeugter A-Modul ist, ist auch $B/\mathfrak{P}_i$ ein endlich-dimensionaler $A/\mathfrak{p}$-Vektorraum.

Definition 9.8. *Die Zahl $f_i = f(\mathfrak{P}_i/\mathfrak{p}) = \dim_{A/\mathfrak{p}} B/\mathfrak{P}_i$ heißt* Restklassen- *oder* Trägheitsgrad *des Ideals $\mathfrak{P}_i$ über A. Die Zahl $e_i = e(\mathfrak{P}_i/\mathfrak{p})$ heißt Verzweigungsindex von $\mathfrak{P}_i$ über A.*

Das Primideal $\mathfrak{p}$ heißt vollständig zerlegt*, wenn in der Faktorisierung $B\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ für alle $i = 1, \ldots, r$ gilt $e_i = f_i = 1$, also $r = n = [L : K]$.*

Das Primideal $\mathfrak{P}_i$ in der Zerlegung $B\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ heißt unverzweigt*, wenn $e_i = 1$ (und die Restklassenerweiterung $A/\mathfrak{p} \to B/\mathfrak{P}_i$ separabel ist). Ansonsten heißt $\mathfrak{P}_i$* verzweigt*. Wenn $f_i = 1$ ist, heißt $\mathfrak{P}_i$* rein verzweigt*. Das Primideal $\mathfrak{p}$ heißt* unverzweigt*, wenn alle $\mathfrak{P}_i$ unverzweigt sind, ansonsten heißt $\mathfrak{p}$* verzweigt*.*

Die Erweiterung L/K heißt unverzweigt*, wenn alle Primideale $\mathfrak{p} \subseteq A$ unverzweigt sind.*

Für Trägheitsgrad und Verzweigungsindex gilt die folgende Gradformel:

Satz 9.9. *Sei A ein Dedekind-Ring mit Quotientenkörper K und L/K eine separable Erweiterung vom Grade n. Sei B der ganze Abschluß von A in L. Sei $\mathfrak{p} \subseteq A$ ein Primideal mit Faktorisierung $B\mathfrak{p} = \prod_{i=1}^{q} \mathfrak{P}_i^{e_i}$. Dann gilt*

$$\sum_{i=1}^{q} e_i f_i = [B/B\mathfrak{p} : A/\mathfrak{p}] = n.$$

Beweis. Für die erste Gleichheit betrachtet man die Idealkette

$$B \supseteq \mathfrak{P}_1 \supseteq \mathfrak{P}_1^2 \supseteq \cdots \supseteq \mathfrak{P}_1^{e_1} \supseteq \mathfrak{P}_1^{e_1}\mathfrak{P}_2 \supseteq \cdots \supseteq \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2} \supseteq \cdots \supseteq \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_q^{e_q} = B\mathfrak{p}.$$

Zwei aufeinanderfolgende Elemente der Kette sind von der Form $\mathfrak{Q} \supseteq \mathfrak{Q}\mathfrak{P}_i$, und $\mathfrak{Q}/\mathfrak{Q}\mathfrak{P}_i$ ist ein eindimensionaler $B/\mathfrak{P}_i$-Vektorraum. Damit ist $\dim_{A/\mathfrak{p}} \mathfrak{Q}/\mathfrak{Q}\mathfrak{P}_i = f_i$. Aufsummieren liefert die Behauptung.

Für die zweite Gleichheit nehmen wir zuerst an, daß B ein freier A-Modul ist. In diesem Fall kann man eine A-Basis $x_1, \ldots, x_n$ von B wählen, die dann eine $A/\mathfrak{p}$-Basis von $B/B\mathfrak{p}$ induziert.

Im allgemeinen Fall betrachten wir die multiplikativ abgeschlossene Teilmenge $S = A \setminus \mathfrak{p}$ und die dazugehörigen lokalisierten Ringe $A_\mathfrak{p} = S^{-1}A$ und

$B_\mathfrak{p} = S^{-1}B$. Nach Proposition 9.3 ist $A_\mathfrak{p}$ ein Hauptidealring mit maximalem Ideal $\mathfrak{p}A_\mathfrak{p}$. Nach Proposition 9.5 ist $B_\mathfrak{p}$ der ganze Abschluß von $A_\mathfrak{p}$ in L. Damit folgt aus der Vorüberlegung im Hauptidealringfall die Gleichheit $[B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p} : A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}] = n$.

Aus der Faktorisierung $\mathfrak{p}B = \prod_{i=1}^q \mathfrak{P}_i^{e_i}$ folgt mit Proposition 9.3 und $\mathfrak{P}_i \cap S = \emptyset$ die Faktorisierung $\mathfrak{p}B_\mathfrak{p} = \prod_{i=1}^q (\mathfrak{P}_i B_\mathfrak{p})^{e_i}$. Zusammen mit der vorigen Überlegung erhalten wir

$$[B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p} : A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}] = \sum_{i=1}^q e_i [B_\mathfrak{p}/\mathfrak{P}_i B_\mathfrak{p} : A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}].$$

Wegen Proposition 9.7 ist aber $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \cong A/\mathfrak{p}$ und $B_\mathfrak{p}/\mathfrak{P}_i B_\mathfrak{p} \cong B/\mathfrak{P}_i$. Damit folgt die Behauptung. □

Aus dem chinesischen Restsatz folgt dann außerdem der Isomorphismus

$$B/B\mathfrak{p} \cong \prod_{i=1}^q B/\mathfrak{P}_i^{e_i}.$$

Die folgende Multiplikativität ist eine direkte Konsequenz aus der Definition.

Proposition 9.10. *Sei A ein Dedekind-Ring mit Quotientenkörper K und $L_2/L_1/K$ endliche separable Erweiterungen. Sei B_i der ganze Abschluß von A in L_i. Sei $\mathfrak{P}_2 \subseteq B_2$ ein Primideal und $\mathfrak{P}_1 = \mathfrak{P}_2 \cap B_1$, $\mathfrak{p} = \mathfrak{P}_2 \cap A \neq (0)$. Dann gilt*

$$e(\mathfrak{P}_2/\mathfrak{p}) = e(\mathfrak{P}_2/\mathfrak{P}_1)e(\mathfrak{P}_1/\mathfrak{p}) \qquad f(\mathfrak{P}_2/\mathfrak{p}) = f(\mathfrak{P}_2/\mathfrak{P}_1)f(\mathfrak{P}_1/\mathfrak{p}).$$

9.3 Zerlegung von Primidealen (in Galoiserweiterungen)

Wie bereits erwähnt, kann man für fast alle Primideale eine Zerlegung durch Polynomfaktorisierung berechnen. Genauer sei L/K eine Erweiterung von Zahlkörpern und $\theta \in \mathcal{O}_L$ ein ganzes primitives Element von L/K. Dann ist $\mathcal{O}_K[\theta]$ eine Ordnung in $\mathcal{O}_L$. Man bezeichnet mit

$$\mathfrak{F} = \{\alpha \in \mathcal{O}_L \mid \alpha\mathcal{O}_L \subseteq \mathcal{O}_K[\theta]\}$$

den *Führer* des Ringes $\mathcal{O}_K[\theta]$.

Satz 9.11. *Sei L/K eine Erweiterung von Zahlkörpern und $\theta \in \mathcal{O}_L$ ein ganzes primitives Element von L/K mit Minimalpolynom $p(X) \in \mathcal{O}_K[X]$. Sei $\mathfrak{p} \subseteq \mathcal{O}_K$ ein zum Führer $\mathfrak{F}$ von $\mathcal{O}_K[\theta]$ teilerfremdes Primideal, und sei $\overline{p}(X) = \overline{p}_1(X)^{e_1} \cdots \overline{p}_r(X)^{e_r}$ die Zerlegung des Polynoms $p(X) \mod \mathfrak{p}$ in irreduzible Faktoren. Dann sind $\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + p_i(\theta)\mathcal{O}_L$ die verschiedenen über $\mathfrak{p}$ liegenden Primideale von $\mathcal{O}_L$. Der Trägheitsgrad f_i von $\mathfrak{P}_i$ ist $\deg \overline{p}_i(X)$ und es gilt $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$.*

Beweis. Wir haben (analog zu Übungsaufgabe 4.14) Isomorphismen

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \mathcal{O}_K[\theta]/\mathfrak{p}\mathcal{O}_K[\theta] \cong (\mathcal{O}_K/\mathfrak{p})[X]/(\overline{p}(X)).$$

Zum ersten Isomorphismus: Die Ideale $\mathfrak{p}$ und $\mathfrak{F}$ sind teilerfremd, also ist $\mathfrak{p}\mathcal{O}_L + \mathfrak{F} = \mathcal{O}_L$. Mit $\mathfrak{F} \subseteq \mathcal{O}_K[\theta]$ haben wir $\mathfrak{p}\mathcal{O}_L + \mathcal{O}_K[\theta] = \mathcal{O}_L$, also ist der kanonische Homomorphismus $\mathcal{O}_K[\theta] \to \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ surjektiv. Der Kern des Homomorphismus ist (wegen der Teilerfremdheit) $\mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_K[\theta] = \mathfrak{p}\mathcal{O}_K[\theta]$.

Zum zweiten Isomorphismus: Der Kern des surjektiven Homomorphismus $\mathcal{O}_K[\theta] \to (\mathcal{O}_K/\mathfrak{p})[X]/(\overline{p}(X))$ wird durch $\mathfrak{p}$ und $p(X)$ erzeugt. Außerdem ist $\mathcal{O}_K[\theta] = \mathcal{O}_K[X]/(p(X))$.

Aus der vorausgesetzten Faktorisierung $\overline{p}(X) = \overline{p}_1(X)^{e_1} \cdots \overline{p}_r(X)^{e_r}$ folgt mit dem chinesischen Restsatz eine Zerlegung

$$(\mathcal{O}_K/\mathfrak{p})[X]/(\overline{p}(X)) \cong \prod_{i=1}^{r} (\mathcal{O}_K/\mathfrak{p})[X]/(\overline{p}_i(X))^{e_i}.$$

Damit sind die Primideale dieses endlichen Rings genau die Hauptideale $(\overline{p}_i(X))$.

Die Behauptung folgt dann aus Übungsaufgabe 4.5 und dem surjektiven Homomorphismus $\mathcal{O}_L \to (\mathcal{O}_K/\mathfrak{p})[X]/(\overline{p}(X))$. □

Für Galoiserweiterungen L/K vereinfacht sich die Struktur der Zerlegung von Primidealen. Wie bereits in Kapitel 3 benutzt, ist für $x \in \mathcal{O}_L$ und $\sigma \in \mathrm{Gal}(L/K)$ auch $\sigma(x) \in \mathcal{O}_L$. Die Galoisgruppe operiert also durch $\mathcal{O}_K$-Algebrenhomomorphismen auf $\mathcal{O}_L$. Da Urbilder von Primidealen wieder Primideale sind, ist für ein Primideal $\mathfrak{P} \subseteq \mathcal{O}_L$ auch $\sigma(\mathfrak{P})$ wieder ein Primideal. Außerdem ist

$$\sigma(\mathfrak{P}) \cap \mathcal{O}_K = \sigma(\mathfrak{P} \cap \mathcal{O}_K) = \mathfrak{P} \cap \mathcal{O}_K,$$

also operiert die Galoisgruppe auch auf der Menge der Primideale über einem Primideal $\mathfrak{p} \subseteq \mathcal{O}_K$. Man bezeichnet $\sigma(\mathfrak{P})$ als zu $\mathfrak{P}$ konjugiertes Primideal.

Proposition 9.12. *Sei L/K eine Galoiserweiterung von Zahlkörpern. Für ein gegebenes Primideal $\mathfrak{p} \subseteq \mathcal{O}_K$ operiert $\mathrm{Gal}(L/K)$ transitiv auf der Menge der über $\mathfrak{p}$ gelegenen Primideale $\mathfrak{P} \subseteq \mathcal{O}_L$.*

Beweis. Seien $\mathfrak{P}, \mathfrak{P}' \subseteq \mathcal{O}_L$ zwei über $\mathfrak{p} \subseteq \mathcal{O}_K$ gelegene Primideale. Wir nehmen an, daß es kein $\sigma \in \mathrm{Gal}(L/K)$ mit $\mathfrak{P}' = \sigma(\mathfrak{P})$ gibt. Dann gibt es nach dem chinesischen Restsatz ein $x \in \mathcal{O}_L$ mit $x \equiv 0 \mod \mathfrak{P}'$ und $x \equiv 1 \mod \sigma(\mathfrak{P})$ für alle $\sigma \in \mathrm{Gal}(L/K)$. Damit ist

$$N_{L/K}(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x) \in \mathfrak{P}' \cap \mathcal{O}_K = \mathfrak{p}.$$

Aber $x \notin \sigma(\mathfrak{P})$ ist äquivalent zu $\sigma(x) \notin \mathfrak{P}$ für alle $\sigma \in \mathrm{Gal}(L/K)$, wegen der Primidealeigenschaft folgt also aus der Annahme $\prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x) \notin \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$. Dies ist ein Widerspruch. □

Durch die Transitivität der Galoisoperation vereinfacht sich die Zerlegung von Primidealen enorm:

Proposition 9.13. *Sei L/K eine Galoiserweiterung vom Grad n, und $\mathfrak{p} \subseteq \mathcal{O}_K$ ein Primideal. Dann gilt in der Zerlegung*

$$\mathcal{O}_L\mathfrak{p} = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}, \qquad [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}] = f_i$$

bereits $e = e_1 = \cdots = e_g$, $f = f_1 = \cdots = f_g$ und $n = efg$.

Beweis. Nach Proposition 9.12 gibt es für jedes $1 \leq i \leq j$ ein $\sigma_i \in \mathrm{Gal}(L/K)$ mit $\sigma(\mathfrak{P}_1) = \mathfrak{P}_i$. Aus der Eindeutigkeit der Primidealzerlegung folgt die Behauptung. □

Definition 9.14. *Sei L/K eine Galoiserweiterung von Zahlkörpern, $\mathfrak{P} \subseteq \mathcal{O}_L$ ein Primideal. Die Untergruppe*

$$G_{\mathfrak{P}} = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\} \subseteq \mathrm{Gal}(L/K)$$

heißt Zerlegungsgruppe *von $\mathfrak{P}$ über K. Der invariante Zwischenkörper*

$$Z_{\mathfrak{P}} = \{x \in L \mid \sigma(x) = x \text{ für alle } \sigma \in G_{\mathfrak{P}}\}$$

heißt Zerlegungskörper *von $\mathfrak{P}$ über K.*

Die Zerlegungsgruppe beschreibt, in wie viele verschiedene Primideale sich $\mathfrak{p}$ in der Erweiterung L/K zerlegt. Es gibt nämlich eine Bijektion zwischen der Menge dieser verschiedenen Primideale und der Menge der Nebenklassen $\mathrm{Gal}(L/K)/G_{\mathfrak{P}}$. Die Zerlegung des Primideals $\mathfrak{p}$ hat damit die einfache Form

$$\mathcal{O}_L\mathfrak{p} = \prod_{\sigma \in \mathrm{Gal}(L/K)/G_{\mathfrak{P}}} \sigma(\mathfrak{P})^e.$$

Proposition 9.15. *Sei $\mathfrak{P}_Z = \mathfrak{P} \cap Z_{\mathfrak{P}}$. Dann gilt*

(i) $\mathcal{O}_L\mathfrak{P}_Z = \mathfrak{P}^e$.

(ii) $e(\mathfrak{P}_Z/\mathfrak{p}) = f(\mathfrak{P}_Z/\mathfrak{p}) = 1$.

Beweis. (i) folgt aus $\mathrm{Gal}(L/Z_{\mathfrak{P}}) = G_{\mathfrak{P}}$. Aus $n = efg$ folgt $\#G_{\mathfrak{P}} = [L : Z_{\mathfrak{P}}] = ef$. (ii) folgt dann aus der Multiplikativität von e und f, cf. Proposition 9.10. □

Der Zerlegungskörper von L/K ist also die Zwischenerweiterung $Z_{\mathfrak{P}}/K$, in der das Primideal $\mathfrak{p}$ vollständig zerlegt wird, die Restklassenerweiterung und die Verzweigung entstehen in der Erweiterung $L/Z_{\mathfrak{P}}$.

Ein Element $\sigma \in G_{\mathfrak{P}}$ induziert wegen $\sigma(\mathcal{O}_L) = \mathcal{O}_L$ und $\sigma(\mathfrak{P}) = \mathfrak{P}$ einen Automorphismus des Restklassenkörpers $\kappa(\mathfrak{P}) = \mathcal{O}_L/\mathfrak{P}$.

Lemma 9.16. *Der Gruppenhomomorphismus*

$$G_{\mathfrak{P}} \to \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})).$$

ist surjektiv.

Beweis. Nach dem Satz vom primitiven Element ist $\kappa(\mathfrak{P}) = \kappa(\mathfrak{p})(\overline{\alpha})$ für ein $\alpha \in \mathcal{O}_L$. Sei $P \in \mathcal{O}_{Z_{\mathfrak{P}}}[X]$ das normierte Minimalpolynom von α, es hat das Minimalpolynom von $\overline{\alpha}$ über $\kappa(\mathfrak{p})$ als Faktor. Für ein $\overline{\sigma} \in \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ ist damit auch $\overline{\sigma}(\overline{\alpha})$ eine Nullstelle von P. Damit existiert $\sigma \in G_{\mathfrak{P}}$ mit $\sigma(\alpha) = \overline{\sigma}(\overline{\alpha})$. Damit ist das Bild von σ unter dem Homomorphismus wirklich $\overline{\sigma}$. □

Definition 9.17. *Die Gruppe*

$$I_{\mathfrak{P}} = \ker\left(G_{\mathfrak{P}} \to \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))\right) \subseteq G_{\mathfrak{P}}$$

heißt Trägheitsgruppe *von $\mathfrak{P}$ über K. Der invariante Zwischenkörper*

$$T_{\mathfrak{P}} = \{x \in L \mid \sigma(x) = x \text{ für alle } \sigma \in I_{\mathfrak{P}}\}$$

heißt Trägheitskörper *von $\mathfrak{P}$ über K.*

Proposition 9.18. *Die Erweiterung $T_\mathfrak{P}/Z_\mathfrak{P}$ ist galoissch mit Galoisgruppe* $\mathrm{Gal}(T_\mathfrak{P}/Z_\mathfrak{P}) \cong \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$. *Außerdem ist* $\mathrm{Gal}(L/T_\mathfrak{P}) \cong I_\mathfrak{P}$. *Für die Ordnungen der Gruppen gilt*

$$\#I_\mathfrak{P} = e, \qquad \#\,\mathrm{Gal}(T_\mathfrak{P}/Z_\mathfrak{P}) = f.$$

Beweis. Die erste Aussage folgt aus der Normalität von $I_\mathfrak{P}$, die letzte Aussage aus der Gradformel und der Tatsache $\kappa(\mathfrak{P} \cap T_\mathfrak{P}) \cong \kappa(\mathfrak{P})$. □

Korollar 9.19. *Sei L/K eine Galoiserweiterung von Zahlkörpern, $\mathfrak{p} \subseteq \mathcal{O}_K$ ein Primideal. Dann ist $\mathfrak{p}$ genau dann in L/K unverzweigt, wenn es ein $\mathfrak{P} \subseteq \mathcal{O}_L$ über $\mathfrak{p}$ gibt mit $I_\mathfrak{P} = 1$ gibt.*

Die Trägheitsgruppe bestimmt also die Verzweigung einer Erweiterung. Der Trägheitskörper ist der maximale unverzweigte Zwischenkörper von L/K, die Erweiterung $L/T_\mathfrak{P}$ vollständig verzweigt.

Übungsaufgabe 9.1. *Sei L/K eine Galoiserweiterung von Zahlkörpern, $\mathfrak{P} \subseteq \mathcal{O}_L$ ein Primideal und $\sigma \in \mathrm{Gal}(L/K)$. Zeigen Sie*

$$Z_{\sigma(\mathfrak{P})} = \sigma Z_\mathfrak{P} \sigma^{-1}, \qquad I_{\sigma(\mathfrak{P})} = \sigma I_\mathfrak{P} \sigma^{-1}.$$

Insbesondere sind in einer abelschen Erweiterung die Zerlegungs- und Trägheitsgruppen zu konjugierten Primidealen gleich.

Zum Schluß definieren wir noch den *Frobenius-Automorphismus* eines Primideals in einer Galois-Erweiterung. Sei L/K eine Galoiserweiterung von Zahlkörpern, $\mathfrak{p} \subseteq \mathcal{O}_K$ ein unverzweigtes Primideal und $\mathfrak{P} \subseteq \mathcal{O}_L$ ein Primideal über $\mathfrak{p}$. Nach dem bisher gesagten ist die Trägheitsgruppe trivial und die Zerlegungsgruppe kanonisch isomorph zur Galoisgruppe der Restklassenkörpererweiterung $\mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$. Diese Galoisgruppe ist zyklisch, und für $q = \#\kappa(\mathfrak{p})$ hat sie den kanonischen Erzeuger $x \mapsto x^q$. Der Automorphismus $x \mapsto x^q$ in $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ wird *Frobenius-Automorphismus* genannt. Über den kanonischen Isomorphismus $Z_\mathfrak{P} \cong \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ hat auch die Zerlegungsgruppe einen kanonischen Erzeuger, der ebenfalls *Frobenius-Automorphismus von* $\mathfrak{P}$ genannt wird. Der Frobenius-Automorphismus wird mit $(\mathfrak{P}, L/K)$ bezeichnet. Wenn die Erweiterung L/K abelsch ist, hängt die Zerlegungsgruppe und damit der Frobenius-Automorphismus nur von $\mathfrak{p}$ ab, und wird mit $\left(\frac{L/K}{\mathfrak{p}}\right)$ bezeichnet.

Proposition 9.20. *Sei L/K eine Galoiserweiterung mit Zwischenkörper F, sei $\mathfrak{P} \subseteq \mathcal{O}_L$ ein Primideal und f der Restklassengrad von $\mathfrak{P} \cap F$ über K. Dann gilt*

(i) $(\mathfrak{P}, L/F) = (\mathfrak{P}, L/K)^f$.

(ii) Wenn F/K auch eine Galoiserweiterung mit zugehörigem Homomorphismus $\phi : \mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$ ist, dann ist

$$\phi((\mathfrak{P}, L/K)) = (\mathfrak{P} \cap F, F/K).$$

9.4 Relative Diskriminante und Verzweigung

Nun soll es darum gehen, die Verzweigung von Primidealen besser zu verstehen. Das entscheidende Hilfsmittel dafür ist wieder die Diskriminante, diesmal in einer relativen Form.

Definition 9.21. *Sei A ein Dedekind-Ring mit Quotientenkörper K, L/K eine endliche separable Erweiterung vom Grad n und B der ganze Abschluß von A in L. Sei $I \subseteq L$ ein gebrochenes Ideal (von B).*

Die relative Spur *von I in L/K ist das gebrochene Ideal*

$$\mathrm{Tr}_{L/K}(I) = \{\mathrm{Tr}_{L/K}(x) \mid x \in I\}.$$

Für ein Primideal $\mathfrak{p} \subseteq B$ definieren wir die relative Norm *von $\mathfrak{p}$ in L/K durch $N_{L/K}(\mathfrak{p}) = (\mathfrak{p} \cap A)^f$, wobei $f = [B/\mathfrak{p} : A/(\mathfrak{p} \cap A)]$ ist. Für ein gebrochenes Ideal $I = \prod \mathfrak{p}_i^{n_i}$ definieren wir die relative Norm von I in L/K durch*

$$N_{L/K}(I) = \prod N_{L/K}(\mathfrak{p}_i)^{n_i}.$$

Man überzeugt sich leicht, daß die in der Definition angegebenen Mengen auch wirklich wieder gebrochene Ideale sind.

Für die relative Norm und Spur gilt die folgende Transitivitätseigenschaft:

Proposition 9.22. *Sei A ein Dedekind-Ring mit Quotientenkörper K. Seien $L_2/L_1/K$ endliche separable Erweiterungen und B_i der ganze Abschluß von A in L_i. Sei I ein gebrochenes Ideal in L_2. Dann gilt*

$$\mathrm{Tr}_{L_2/K}(I) = \mathrm{Tr}_{L_1/K}(\mathrm{Tr}_{L_2/L_1}(I)), \qquad N_{L_2/K}(I) = N_{L_1/K}(N_{L_2/L_1}(I))$$

Beweis. Für die relative Spur folgt das direkt aus Übungsaufgabe 3.9 und der Definition.

Für die relative Norm reicht es aufgrund der Multiplikativität, die Aussage für Primideale nachzuweisen. Sei $\mathfrak{P} \subseteq B_2$ ein Primideal. Dann ist

$$N_{L_2/K}(\mathfrak{P}) = (\mathfrak{P} \cap A)^{[B_2/\mathfrak{P} : A/\mathfrak{P}\cap A]}$$

$$N_{L_2/L_1}(\mathfrak{P}) = (\mathfrak{P} \cap B_1)^{[B_2/\mathfrak{P} : B_1/\mathfrak{P}\cap B_1]}$$

$$N_{L_1/K}(\mathfrak{P} \cap B_1) = (\mathfrak{P} \cap A)^{[B_1/\mathfrak{P}\cap B_1 : A/\mathfrak{P}\cap A]}$$

Die Behauptung folgt dann aus der Gradformel

$$[B_2/\mathfrak{P} : A/\mathfrak{P} \cap A] = [B_2/\mathfrak{P} : B_1/\mathfrak{P} \cap B_1][B_1/\mathfrak{P} \cap B_1 : A/\mathfrak{P} \cap A].$$

□

Die folgende Aussage zeigt, daß die hier definierte relative Norm die bisherigen Begriffe von Norm von Elementen und Idealnorm verallgemeinert.

Proposition 9.23. *(i) Sei K ein Zahlkörper und I ein gebrochenes Ideal. Dann ist die relative Norm $N_{K/\mathbb{Q}}(I)$ gleich dem von der Idealnorm $N(I)$ erzeugten Ideal in $\mathbb{Z}$.*

(ii) Sei L/K eine Galois-Erweiterung von Zahlkörpern mit Galoisgruppe G. Dann gilt für ein gebrochenes Ideal I in L

$$\prod_{\sigma \in G} \sigma(I) = \mathcal{O}_L N_{L/K}(I).$$

(iii) Sei L/K eine Erweiterung von Zahlkörpern, $0 \neq x \in L$. Dann gilt

$$N_{L/K}((x)) = (N_{L/K}(x)).$$

Beweis. (i) Für ein Primideal $\mathfrak{p} \subseteq \mathcal{O}_K$ ist die Idealnorm gleich $\#(\mathcal{O}_K/\mathfrak{p})$. Mit $(p) = \mathfrak{p} \cap \mathbb{Z}$ und $f = [\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_p]$ ist dann $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_{p^f}$. Damit folgt die Gleichheit.

(ii) Es reicht wieder, die Aussage für ein Primideal $\mathfrak{P} \subseteq \mathcal{O}_L$ zu beweisen. Es gilt nach Proposition 9.13

$$\mathcal{O}_L(\mathfrak{P} \cap \mathcal{O}_K) = \left(\prod_{i=1}^{g} \mathfrak{P}_i\right)^e,$$

wobei $\mathfrak{P}$ als einer der Faktoren auftaucht. Außerdem operiert nach Proposition 9.12 die Galoisgruppe $\mathrm{Gal}(L/K)$ transitiv auf den $\mathfrak{P}_i$. Also ist

$$\prod_{i=1}^{n} \sigma_i(\mathfrak{P}) = \left(\prod_{i=1}^{g} \mathfrak{P}_i\right)^{ef} = \mathcal{O}_L\mathfrak{P}^f = \mathcal{O}_L N_{L/K}(\mathfrak{P}).$$

(iii) Zuerst nehmen wir an, daß L/K Galois ist. Nach (ii) ist

$$\mathcal{O}_L N_{L/K}((x)) = \prod_{i=1}^{n} \sigma_i((x)) = \prod_{i=1}^{n} (\sigma_i(x)) = \left(\prod_{i=1}^{n} \sigma_i(x)\right) = (N_{L/K}(x)).$$

Außerdem ist aber $N_{L/K}((x)) = \mathcal{O}_L N_{L/K}((x)) \cap K = \mathcal{O}_L(N_{L/K}(x)) \cap K = (N_{L/K}(x))$. Im Allgemeinen betrachtet man die normale Hülle L' von L/K, mit $[L' : L] = m$. Dort gilt dann $N_{L/K}((x))^m = (N_{L/K}(x))^m$, woraus mit der Eindeutigkeit der Idealfaktorisierung die Behauptung folgt. □

Definition 9.24. *Sei L/K eine Erweiterung von Zahlkörpern. Die* relative Diskriminante *von L/K ist das Ideal $\mathcal{D}_{L/K} \subseteq \mathcal{O}_K$, das von den Elementen $D_{L/K}(x_1, \ldots, x_n)$ erzeugt wird, wobei $x_1, \ldots, x_n$ alle K-Basen von L mit $x_i \in \mathcal{O}_L$ durchläuft.*

Lemma 9.25. *Sei A ein Ring, $B_1, \ldots, B_n$ seien A-Algebren, die als A-Moduln frei und endlich erzeugt sind, und sei $B = \prod_{i=1}^n B_i$. Dann ist*

$$\mathcal{D}_{B/A} = \prod_{i=1}^{n} \mathcal{D}_{B_i/A}.$$

Beweis. Induktiv reicht es, den Fall $n = 2$ zu zeigen. Seien $x_1, \ldots, x_{m_1}$ und $y_1, \ldots, y_{m_2}$ Basen von B_1 bzw. B_2. Damit ist $x_1, \ldots, x_{m_1}, y_1, \ldots, y_{m_2}$ eine A-Basis für $B_1 \times B_2$. Da das Produkt in $B_1 \times B_2$ komponentenweise gebildet wird, ist $x_i y_j = 0$, also auch $\mathrm{Tr}(x_i y_j) = 0$. Damit hat die Matrix der Spurform Block-Diagonalform. Dies impliziert die Behauptung. □

Lemma 9.26. *Sei $A \hookrightarrow B$ eine Ringerweiterung und $I \subseteq A$ ein Ideal. Sei B ein freier A-Modul mit Basis $x_1, \ldots, x_n$. Dann ist $\overline{x_1}, \ldots, \overline{x_n}$ eine A/I-Basis von B/I und $D(\overline{x_1}, \ldots, \overline{x_n}) = \overline{D(x_1, \ldots, x_n)}$.*

Beweis. Die Operationen in der Definition der Diskriminante (darstellende Matrix für Multiplikation mit x, Spur, Spurform, Determinante) sind offensichtlich verträglich mit der Quotientenbildung. □

Lemma 9.27. *Sei K ein Körper, endlich oder von Charakteristik 0, sei L eine endlich-dimensionale kommutative K-Algebra. Dann ist $\mathcal{D}_{L/K} \neq (0)$ genau dann, wenn es in L keine von 0 verschiedenen nilpotenten Elemente gibt.*

Beweis. Sei x ein nilpotentes Element. Wir erweitern es zu einer K-Basis $x = x_1, x_2, \ldots, x_n$ von L. Dann ist xx_j nilpotent, also $\mathrm{Tr}(xx_j) = 0$. Damit ist $D(x_1, \ldots, x_n) = 0$, da die Matrix der Spurform eine Nullzeile hat.

Wir nehmen nun an, daß L keine nilpotenten Elemente außer 0 hat. Dann ist L ein Produkt von Erweiterungskörpern von K, es gibt endlich viele maximale Ideale $\mathfrak{p}_i$ von L mit $L \cong \prod L/\mathfrak{P}_i$. Nach Lemma 9.25 ist $\mathcal{D}_{L/K} = \prod \mathcal{D}_{(L/\mathfrak{P}_i)/K}$. Mit Übungsaufgabe 3.3 sind die Diskriminanten $\mathcal{D}_{(L/\mathfrak{P}_i)/K} \neq 0$. □

Satz 9.28. *Ein Primideal $(0) \neq \mathfrak{p} \subseteq \mathcal{O}_K$ ist in der Körpererweiterung L/K genau dann verzweigt, wenn $\mathfrak{p} \supseteq \mathcal{D}_{L/K}$. Insbesondere existieren in einer Erweiterung L/K von Zahlkörpern nur endlich viele verzweigte Primideale.*

Beweis. Wegen $\mathcal{D}_{L/K} \neq 0$ und der Idealfaktorisierung in Dedekind-Ringen folgt die zweite Behauptung aus der ersten.

Aus der Idealfaktorisierung von $\mathfrak{p}$ in $\mathcal{O}_L$ folgt

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \prod_{i=1}^{g} \mathcal{O}_L/\mathfrak{P}_i^{e_i}.$$

Damit verzweigt $\mathfrak{p}$ genau dann, wenn die $\mathcal{O}_K/\mathfrak{p}$-Algebra $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ nichttriviale nilpotente Elemente hat, also wenn $\mathcal{D}_{(\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L)/\mathcal{O}_K/\mathfrak{p}} \neq 0$.

Wir nutzen wieder die Lokalisierung. Sei $S = \mathcal{O}_K \setminus \mathfrak{p}$, $\mathcal{O}_{K,\mathfrak{p}} = S^{-1}\mathcal{O}_K$ und $\mathcal{O}_{L,\mathfrak{p}} = S^{-1}\mathcal{O}_L$. Damit ist $\mathcal{O}_{K,\mathfrak{p}}$ ein Hauptidealring, und wir können eine Basis $e_1, \ldots, e_n$ von $\mathcal{O}_{L,\mathfrak{p}}$ wählen. Damit ist die Diskriminante $\mathcal{D}_{(\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L)/\mathcal{O}_K/\mathfrak{p}} = 0$ genau dann, wenn $D(e_1, \ldots, e_n) \in \mathfrak{p}\mathcal{O}_{L,\mathfrak{p}}$ ist.

Wenn $D(e_1, \ldots, e_n) \in \mathfrak{p}\mathcal{O}_{L,\mathfrak{p}}$ und $x_1, \ldots, x_n$ eine K-Basis von L mit $x_i \in \mathcal{O}_L$ ist, dann gibt es eine Basiswechselmatrix (a_{ij}) mit $x_i = \sum a_{ij}e_j$ und $a_{ij} \in \mathcal{O}_{K,\mathfrak{p}}$. Damit ist

$$D(x_1, \ldots, x_n) = \det(a_{ij})^2 D(e_1, \ldots, e_n) \in \mathfrak{p}\mathcal{O}_{K,\mathfrak{p}} \cap \mathcal{O}_K = \mathfrak{p}.$$

Gilt umgekehrt $\mathcal{D}_{L/K} \subseteq \mathfrak{p}$, schreibt man $e_i = y_i s^{-1}$ mit $y_i \in \mathcal{O}_L$ und $s \in S$. Damit folgt dann

$$D(e_1, \ldots, e_n) = s^{-2n} D(y_1, \ldots, y_n) \in \mathcal{O}_{K,\mathfrak{p}}\mathcal{D}_{L/K} \subseteq \mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}.$$

□

Die in der Erweiterung L/K verzweigten Primideale von $\mathcal{O}_K$ sind also genau die Teiler der Diskriminante. Außerdem charakterisiert die Diskriminante, wann eine relative Ganzheitsbasis existiert:

Proposition 9.29. *Für eine Erweiterung von Zahlkörpern L/K gibt es genau dann eine relative Ganzheitsbasis, d.h. $\mathcal{O}_L$ ist ein freier $\mathcal{O}_K$-Modul, wenn die relative Diskriminante $\mathcal{D}_{L/K}$ ein Hauptideal ist.*

Wenn K ein Zahlkörper mit $\mathrm{Cl}(\mathcal{O}_K) \neq 0$ ist, dann existiert eine Körpererweiterung L/K, für die es keine relative Ganzheitsbasis gibt.

9.5 Ausblick: Differente und Verzweigung

Analog kann man ebenfalls die Verzweigung von Primidealen in $\mathcal{O}_L$ charakterisieren. Dazu dient die sogenannte Differente. Wir werden die Aussagen zur Differente hier nur formulieren und nicht beweisen.

Mit Hilfe der Spurform kann man jedem gebrochenen Ideal $I \subseteq L$ ein duales gebrochenes Ideal $I^* = \{x \in L \mid \mathrm{Tr}_{L/K}(xI) \subseteq \mathcal{O}_K\}$ zuordnen.

Definition 9.30. *Sei L/K eine Erweiterung von Zahlkörpern. Das gebrochene Ideal*

$$\mathcal{O}_L^* = \{x \in L \mid \mathrm{Tr}_{L/K}(x\mathcal{O}_L) \subseteq \mathcal{O}_K\}$$

heißt Dedekindscher Komplementärmodul. *Das dazu inverse Ideal $\Delta_{L/K}$ heißt* Differente *der Erweiterung L/K.*

Für ein Element $\alpha \in \mathcal{O}_L$ mit Minimalpolynom $f(X) \in \mathcal{O}_K[X]$ definieren wir die Differente des Elementes α *durch*

$$\delta_{L/K}(\alpha) = \begin{cases} f'(\alpha) & L = K(\alpha) \\ 0 & L \neq K(\alpha) \end{cases}$$

Proposition 9.31. *Für Erweiterungen $L/F/K$ gilt $\Delta_{L/K} = \Delta_{L/F}\Delta_{F/K}$.*

Proposition 9.32. *Für $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ ist $\Delta_{L/K} = (\delta_{L/K}(\alpha))$. Allgemeiner ist $\Delta_{L/K}$ das von den $\delta_{L/K}(\alpha), \alpha \in \mathcal{O}_L$ erzeugte Ideal.*

Satz 9.33. *Ein Primideal $\mathfrak{q} \subseteq \mathcal{O}_L$ ist genau dann in der Körpererweiterung L/K verzweigt, wenn $\mathfrak{q} \supseteq \Delta_{L/K}$.*

Die Beziehung zwischen Diskriminante und Differente verallgemeinert die Formel aus Proposition 3.13.

Proposition 9.34. $N_{L/K}(\Delta_{L/K}) = \mathcal{D}_{L/K}$

9.6 Beispiel: Zyklotomische Körper

Zuletzt wollen wir noch die Primidealzerlegung am Beispiel der zyklotomischen Körper betrachten. Sei $K = \mathbb{Q}(\zeta_n)$. In Satz 3.27 haben wir eine Ganzheitsbasis und die Diskriminante bestimmt: Der Ganzheitsring ist $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$, und eine Primzahl $p \in \mathbb{Z}$ ist genau dann verzweigt, wenn $p \mid n$.

Nach den vorigen Betrachtungen über Galoiserweiterungen hat eine unverzweigte Primzahl $p \nmid n$ in $\mathcal{O}_K$ die Faktorisierung

$$p\mathcal{O}_K = \mathfrak{P}_1 \cdots \mathfrak{P}_g,$$

wobei $f = [\kappa(\mathfrak{P}_i) : \mathbb{F}_p]$ für beliebiges i und $fg = \phi(\zeta_n)$ ist. Es reicht also, den Restklassengrad f zu bestimmen.

Übungsaufgabe 9.2. *Der Restklassengrad f ist die kleinste natürliche Zahl mit $p^f \equiv 1 \mod n$.*

Übungsaufgabe 9.3. *Wie viele Primfaktoren hat (71) in $\mathbb{Q}(\zeta_{20})$? Für welche n ist (59) in $\mathbb{Q}(\zeta_n)$ vollständig zerlegt?*

Für eine verzweigte Primzahl ist das Ergebnis komplizierter zu beweisen. Sei $n = p^{v_p(m)}n'$. Dann ist f die kleinste natürliche Zahl mit $p^f \equiv 1 \mod n'$, $e = \phi(p^{v_p(n)}) = p^{v_p(n)-1}(p-1)$ und es gilt

$$p\mathcal{O}_K = \prod_{i=1}^{\phi(n_1)/f} \mathfrak{P}_i^e.$$

Durch die Betrachtung von zyklotomischen Körpern und ihren quadratischen Zwischenkörpern erhält man einen einfachen, konzeptionellen Beweis für das quadratische Reziprozitätsgesetz.

Proposition 9.35. *Sei q eine ungerade Primzahl, $K = \mathbb{Q}(\zeta_q)$. Es gibt genau einen quadratischen Zwischenkörper von $K/\mathbb{Q}$, nämlich*

$$F = \mathbb{Q}(\sqrt{q^*}) \text{ mit } q^* = (-1)^{\frac{(q-1)}{2}} q.$$

Beweis. Es ist $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{F}_q^\times \cong \mathbb{Z}/(q-1)\mathbb{Z}$. Quadratische Teilkörper entsprechen nach dem Hauptsatz der Galoistheorie genau den Untergruppen vom Index 2. In $\mathbb{F}_q^\times$ gibt es nur eine solche Untergruppe, nämlich $(\mathbb{F}_q^\times)^2$. Also gibt es einen eindeutigen quadratischen Zwischenkörper $F \subseteq \mathbb{Q}(\zeta_q)$. Diesen bestimmen wir mit Hilfe der Verzweigung. Nach Satz 3.27 ist nur das Primideal (q) in $K/\mathbb{Q}$ verzweigt. Nach Proposition 9.10 kann die quadratische Erweiterung $F/\mathbb{Q}$ ebenfalls nur in (q) verzweigt sein. Aus Beispiel 3.24 folgt dann die Behauptung. □

Sei nun p eine von q verschiedene (insbesondere unverzweigte) Primzahl und sei $\sigma_p = \left(\frac{K/\mathbb{Q}}{p}\right)$ der Frobenius-Automorphismus von p. Wir haben eine exakte Sequenz

$$1 \to (\mathbb{F}_q^\times)^2 \to \mathbb{F}_q^\times \cong \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Gal}(F/\mathbb{Q}) \to 1.$$

Nach Proposition 9.20 ist das Bild von σ_p in $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ gleich $\left(\frac{F/\mathbb{Q}}{p}\right)$ und mit der exakten Sequenz ist das Bild genau dann nichttrivial, wenn p kein Quadrat modulo q ist. Man kann also den Frobenius-Automorphismus von p mit dem Legendre-Symbol identifizieren:

$$\left(\frac{F/\mathbb{Q}}{p}\right) = \left(\frac{p}{q}\right).$$

Mit Proposition 4.22 ist aber der Frobenius-Automorphismus von p für den Zwischenkörper $\mathbb{Q}(\sqrt{q^*})/\mathbb{Q}$ genau dann nicht-trivial, wenn p träge in $\mathbb{Q}(\sqrt{q^*})/\mathbb{Q}$ ist, also

$$\left(\frac{F/\mathbb{Q}}{p}\right) = \left(\frac{q^*}{p}\right).$$

Damit können wir jetzt also den Beweis für das quadratische Reziprozitätsgesetz nachtragen.

Proposition 9.36. *(i) Sei p eine ungerade Primzahl und $a \in \mathbb{Z}$ mit $p \nmid a$. Dann gilt*

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

(ii) Seien p, q zwei verschiedene Primzahlen. Dann gilt

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

(iii)

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

Beweis. (i) Sei $w \in \mathbb{Z} \setminus p\mathbb{Z}$ so daß $\overline{w}$ ein Erzeuger von $\mathbb{F}_p^\times$ ist. Dann ist $a \equiv w^j \mod p$ genau dann ein Quadratrest, wenn j gerade ist, also $\left(\frac{a}{p}\right) = (-1)^j$. In $\mathbb{F}_p^\times$ gibt es aber nur ein Element der Ordnung 2, nämlich die Restklasse von $-1 \equiv w^{\frac{p-1}{2}} \mod p$. Damit ist

$$\left(\frac{a}{p}\right) = (-1)^j \equiv w^{\frac{j(p-1)}{2}} \equiv a^{\frac{p-1}{2}} \mod p.$$

(ii) Aus der Identifikation mit dem Frobenius-Automorphismus und (i) folgt

$$\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right) = \left(\frac{-1}{p}\right)^{\frac{(q-1)}{2}}\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{q}{p}\right).$$

(iii) Nach Proposition 4.23 ist 2 in F verzweigt, wenn $q^* \equiv 1 \mod 8$, und träge, wenn $q^* \equiv 5 \mod 8$. Damit ist

$$\left(\frac{2}{p}\right) = \left(\frac{F/\mathbb{Q}}{2}\right) = (-1)^{\frac{q^2-1}{8}}.$$

□

Übungsaufgaben

Übungsaufgabe 9.4. *Wir betrachten den Zahlkörper $K = \mathbb{Q}(\sqrt{-5}, i)$.*

(i) Zeigen Sie, daß die folgenden Elements eine Basis des Ganzheitsrings $\mathcal{O}_K$ bilden :

$$1, i, \frac{1+\sqrt{5}}{2}, i \cdot \frac{1+\sqrt{5}}{2}.$$

Betrachten Sie dazu die Norm $N_{K/\mathbb{Q}(i)}$ eines Elements in $\mathcal{O}_K$ und gehen Sie wie im Beweis von Satz 1.3 vor.

(ii) Zeigen Sie

$$D\left(1, i, \frac{1+\sqrt{5}}{2}, i \cdot \frac{1+\sqrt{5}}{2}\right) = 400.$$

(iii) Zeigen Sie mit Hilfe der Gradformel, daß die Erweiterung $K/\mathbb{Q}(\sqrt{-5})$ unverzweigt ist. Es kann hilfreich sein, auch den Zwischenkörper $\mathbb{Q}(\sqrt{5})$ zu betrachten.

(iv) Zeigen Sie, daß

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Bestimmen Sie alle Zwischenkörper.

(v) Berechnen Sie für die Ideale (2), (3) *und* (5) *Zerlegungs- und Trägheitsgruppe in der Erweiterung* $K/\mathbb{Q}$.

Übungsaufgabe 9.5. *Zeigen Sie, daß der Ganzheitsring von* $\mathbb{Q}(\sqrt{-5}, i)$ *ein Hauptidealring ist.*

Übungsaufgabe 9.6. *Wie sehen die quadratischen Teilkörper von* $\mathbb{Q}(\zeta_n)$ *aus, wenn* n *keine Primzahl ist?*

Kapitel 10

Bewertungstheorie und lokale Körper

10.1 Bewertete Körper

Definition 10.1. *Sei K ein Körper. Ein* Absolutbetrag auf K *ist eine Abbildung $|\cdot|_v : K \to \mathbb{R} : x \mapsto |x|_v$ mit den folgenden Eigenschaften:*

(i) Für alle $x \in K$ gilt $|x|_v \geq 0$, und $|x|_v = 0$ genau dann, wenn $x = 0$.

(ii) Für alle $x, y \in K$ gilt $|xy|_v = |x|_v|y|_v$.

(iii) Für alle $x, y \in K$ gilt $|x + y|_v \leq |x|_v + |y|_v$.

Ein Absolutbetrag, der der verschärften Dreiecksungleichung

$$|x + y|_v \leq \max\{|x|_v, |y|_v\}$$

genügt, heißt nicht-archimedisch.

Definition 10.2. *Sei K ein Körper. Eine* diskrete Bewertung auf K *ist eine Abbildung $v : K \to \mathbb{R} \cup \{\infty\}$ mit den folgenden Eigenschaften:*

(i) $v(x) = \infty$ genau dann, wenn $x = 0$.

(ii) Für alle $x, y \in K$ gilt $v(xy) = v(x)v(y)$.

(iii) Für alle $x, y \in K$ gilt $v(x + y) \geq \min\{v(x), v(y)\}$.

(iv) Das Bild $v(K^\times)$ ist eine diskrete Untergruppe von $\mathbb{R}$ vom Rang 1.

Lemma 10.3. *Sei v eine diskrete Bewertung auf dem Körper K, $a > 1$ eine reelle Zahl. Dann ist $|x|_v = a^{-v(x)}$ ein Absolutbetrag.*

Beweis. Die Eigenschaften (i) und (ii) sind offensichtlich. Die Dreiecksungleichung folgt aus $a^{-v(x+y)} \leq a^{\min\{-v(x),-v(y)\}} \leq a^{-v(x)} + a^{-v(y)}$. □

Beispiel 10.4. *(i) $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ sind Körper mit einem Absolutbetrag, dem "gewöhnlichen" Absolutbetrag. Dieser kommt nicht von einer diskreten Bewertung.*

(ii) Sei R ein Dedekind-Ring mit Quotientenkörper K, $\mathfrak{p}$ ein Primideal, $x \in K^\times$ ein Element und I_x das zugehörige gebrochene Ideal mit Faktorisierung $I_x = \prod \mathfrak{q}^{v_\mathfrak{q}(x)}$. Dann ist die Abbildung

$$v_\mathfrak{p} : K \mapsto \mathbb{Z} \cup \{\infty\} : x \mapsto \begin{cases} v_\mathfrak{p}(x) & x \neq 0 \\ \infty & x = 0 \end{cases}$$

eine diskrete Bewertung. Eigenschaften (i) und (iv) sind klar, (ii) folgt aus Satz 4.15 und (iii) aus Korollar 4.17. Auf K hat man dann nach dem Lemma auch einen Absolutbetrag.

(iii) Ein Spezialfall des Beispiels (ii) ist der p-adische Betrag auf $\mathbb{Q}$, der durch $|x|_p = p^{-v_p(x)}$ gegeben ist, wobei $v_p(x)$ die Vielfachheit von x in der Primfaktorisierung von x ist.

(iv) Sei K ein Körper. Wir bezeichnen mit

$$K((X)) = \left\{ \sum_{i=-n}^{\infty} a_i X^i \mid n \in \mathbb{Z}, a_i \in K \right\}$$

den Körper der Laurentreihen über K. *Auf diesem Körper ist eine diskrete Bewertung* deg *gegeben, die jeder Laurentreihe $\sum_{i=-n}^{\infty} a_i X^i$ mit $a_{-n} \neq 0$ den Wert $-n$ zuweist.*

□

Proposition 10.5. *Sei R ein Ring. Die folgenden Aussagen sind äquivalent:*

(i) R ist ein Dedekind-Ring mit genau einem maximalen Ideal.

(ii) R ist von der Form $\{x \in K \mid v(x) \geq 0\}$ für eine diskrete Bewertung eines Körpers K.

In diesem Fall ist das maximale Ideal $\mathfrak{m} = \{x \in K \mid v(x) > 0\}$ und K der Quotientenkörper von R.

Beweis. (i) ⇒ (ii) ist Beispiel 10.4.

(ii) ⇒ (i): Sei umgekehrt K ein mit v diskret bewerteter Körper. Wir zeigen zuerst, daß $R = \{x \in K \mid v(x) \geq 0\}$ ein Ring ist. Seien $x, y \in R$. Dann ist $v(x+y) \geq \min\{v(x), v(y)\} \geq 0$ und $v(xy) = v(x)v(y) \geq 0$, also ist R unter Addition und Multiplikation abgeschlossen. Mit diesem Argument sieht man auch, daß $\mathfrak{m} = \{x \in K \mid v(x) > 0\}$ ein Ideal ist.

Für die Elemente $x \in R \setminus \mathfrak{m}$ ist $v(x) = v(x^{-1}) = 0$, diese Elemente sind also invertierbar und $\mathfrak{m}$ ist folglich maximal.

Aus $v(x) < 0$ folgt $v(x^{-1}) > 0$, also ist K der Quotientenkörper von R.

Die Bewertung v ist diskret, sei $\pi \in \mathfrak{m}$ mit $v(\pi)$ minimal. Ohne Beschränkung der Allgemeinheit ist $v(\pi) = 1$. Für $x \in K$ ist $u = x\pi^{-v(x)}$ eine Einheit, da $v(u) = v(x)v(\pi^{-v(x)}) = 0$ ist. Damit hat jedes Element von $K^\times$ die Form $u\pi^v$ mit $u \in R^\times$ und $v \in \mathbb{Z}$. Insbesondere ist R ein Hauptidealring, das Ideal $\mathfrak{m}$ wird von π erzeugt. □

Ringe wie in Proposition 10.5 heißen *diskrete Bewertungsringe*.

Beispiel 10.6. *(i) Sei $R = \mathcal{O}_K$, $\mathfrak{p}$ ein Primideal, und $S = \mathcal{O}_K \setminus \mathfrak{p}$. Dann ist $S^{-1}\mathcal{O}_K$ der diskrete Bewertungsring zur Bewertung $v_\mathfrak{p}$ aus Beispiel 10.4.*

(ii) Der zur Bewertung deg *auf dem Laurentreihenkörper $K((X))$ gehörende Bewertungsring ist der Potenzreihenring $K[[X]] = \{\sum_{i=0}^{\infty} a_i X^i \mid a_i \in K\}$.* □

Sei K ein Körper mit Absolutbetrag $|\cdot|_v$. Dann bilden die Mengen

$$B(x, \epsilon) = \{y \in K \mid |x - y|_v < \epsilon\}, x \in K, \epsilon \in \mathbb{R}$$

die Subbasis einer Topologie, der von $|\cdot|_v$ induzierten Topologie. Insbesondere kann man auch über die Konvergenz von Folgen sprechen, genau wie man das bezüglich des gewöhnlichen Absolutbetrages auf $\mathbb{R}$ in der Analysis tut.

Zwei Absolutbeträge auf K heißen *äquivalent*, wenn sie dieselbe Topologie induzieren.

Lemma 10.7. *Sei K ein Körper und $|\cdot|_1$ und $|\cdot|_2$ äquivalente Absolutbeträge auf K. Dann gibt es eine reelle Zahl $\lambda > 0$ mit $|\cdot|_1 = |\cdot|_2^{\lambda}$.*

Beweis. Da Grenzwerte nur von der Topologie abhängen gilt

$$\{x \in K \mid |x|_1 < 1\} = \{x \mid \lim_{n\to\infty} x^n = 0\} = \{x \in K \mid |x|_2 < 1\}.$$

Ebenso ist $|x|_1 > 1$ genau dann, wenn $|x|_2 > 1$. Wenn $|x|_1 = 1$ für alle $x \in K^\times$ ist, gilt die Aussage trivialerweise. Sei also $y \in K$ mit $a = |y|_1 > 1$ und $b = |y|_2$. Wir wollen $\lambda = \log_b a$ zeigen.

Für $x \in K^\times$ gilt $|x|_1 = a^\alpha$ für geeignetes $\alpha \geq 0$. Seien $m, n \in \mathbb{N}$ mit $m/n \geq \alpha$.

$$|x|_1 < |y|_1^{\frac{m}{n}} \Rightarrow \left|\frac{x^n}{y^m}\right|_1 < 1 \Rightarrow \left|\frac{x^n}{y^m}\right|_2 < 1 \Rightarrow |x|_2 < |y|_2^{\frac{m}{n}}.$$

Ebenso zeigt man $|x|_2 > b^{\frac{m}{n}}$ für $m/n < \alpha$, zusammen also $|x|_2 = b^\alpha$. Die Behauptung folgt aus

$$|x|_1 = a^\alpha = b^{\alpha \log_b a} = |x|_2^{\log_b a}.$$

□

Ein Körper K mit Absolutbetrag $|\cdot|_v$ heißt *vollständig*, wenn jede Cauchy-Folge einen Grenzwert in K besitzt.

Übungsaufgabe 10.1. *(i) Für einen beliebigen Körper mit Absolutbetrag $|\cdot|_v$ ist die Menge K_v der Cauchy-Folgen modulo Nullfolgen wieder ein Körper. Es gibt eine eindeutige Fortsetzung von $|\cdot|_v$ auf K_v, bezüglich derer K_v vollständig ist. Außerdem ist K dicht in K_v. Der Körper K_v heißt* Vervollständigung *oder* Komplettierung von K bezüglich des Absolutbetrages $|\cdot|_v$.

(ii) Formulieren Sie die universelle Eigenschaft der Komplettierung.

Proposition 10.8. *Jeder Absolutbetrag auf $\mathbb{Q}$ ist zum gewöhnlichen Absolutbetrag $|\cdot|_\infty$ oder zu einem p-adischen Betrag $|\cdot|_p$ äquivalent.*

Beweis. Sei $|\cdot|_v$ nicht-archimedisch. Dann ist $|n|_v \leq 1$ und es gibt eine Primzahl p mit $|p|_v < 1$, da sonst $|x|_v = 1$ für alle $x \in \mathbb{Q}^\times$. Die Menge $\mathfrak{a} = \{a \in \mathbb{Z} \mid |a|_v < 1\}$ ist ein Ideal mit $p \in \mathfrak{a}$ und $1 \notin \mathfrak{a}$, also $\mathfrak{a} = (p)$. Für $a \in \mathbb{Z}$ mit $a = bp^{v_p(a)}$ ist $|b|_v = 1$, also ist $|\cdot|_v$ zum p-adischen Betrag äquivalent.

Sei nun $|\cdot|_v$ archimedisch. Wir wollen für natürliche Zahlen $m, n > 1$ die Gleichung

$$|m|_v^{1/\log m} = |n|_v^{1/\log n}$$

zeigen. Wir setzen $m = a_0 + a_1 n + \cdots + a_r n_r$ mit $0 \leq a_i \leq n-1$ und $n^r \leq m$. Dann ist $r \leq \log m / \log n$ und $|a_i|_v \leq n$, und wir haben

$$|m|_v \leq \sum |a_i|_v |n|_v^i \leq \sum |a_i|_v |n|_v^r \leq \left(1 + \frac{\log m}{\log n}\right) n |n|_v^{\frac{\log m}{\log n}}.$$

Ersetzt man m durch m^k und zieht die k-te Wurzel erhält man für $k \to \infty$ die Ungleichung $|m|_v^{1/\log m} \leq |n|_v^{1/\log n}$. Ein symmetrisches Argument liefert die Gleichheit. Aus der Gleichung entnehmen wir nun die Konstante $c = |n|_v^{1/\log n}$. Dann ist $|n|_v = c^{\log n}$ und mit $s = \log c$ ist $|x|_v = |x|_\infty^s$, also ist der Absolutbetrag $|\cdot|_v$ zum gewöhnlichen Absolutbetrag äquivalent. □

Beispiel 10.9. *Die Vervollständigung von $\mathbb{Q}$ bezüglich des gewöhnlichen Absolutbetrages $|\cdot|_\infty$ ist $\mathbb{R}$. Die Vervollständigung von $\mathbb{Q}$ bezüglich des p-adischen Betrages $|x|_p$ wird mit $\mathbb{Q}_p$ bezeichnet.* □

Definition 10.10. *Sei K ein Zahlkörper. Ein Absolutbetrag auf K heißt* kanonisch*, wenn seine Einschränkung auf $\mathbb{Q}$ mit dem gewöhnlichen oder einem p-adischen Absolutbetrag übereinstimmt. Die Äquivalenzklassen kanonischer Absolutbeträge heißen* Stellen *des Zahlkörpers.*

10.2 Das Henselsche Lemma

Wir interessieren uns für das Verhalten der diskreten Bewertungsringe unter Komplettierung.

Satz 10.11. *Sei K ein durch v diskret bewerteter Körper mit Komplettierung K_v. Seien $\mathcal{O} = \{x \in K \mid v(x) \geq 0\}$ und $\mathcal{O}_v = \{x \in K_v \mid v(x) \geq 0\}$ die entsprechenden Bewertungsringe mit maximalen Idealen $\mathfrak{m}$ bzw. $\mathfrak{m}_v$.*

(i) $\mathcal{O}_v$ ist der topologische Abschluß von $\mathcal{O}$ in K_v.

(ii) Für alle $i \geq 1$ ist $\mathcal{O}/\mathfrak{m}^i \cong \mathcal{O}_v/\mathfrak{m}_v^i$.

(iii) Die kanonische Abbildung

$$\mathcal{O}_v \to \varprojlim \mathcal{O}_v/\mathfrak{m}_v^n$$

ist ein Isomorphismus und Homöomorphismus.

Beweis. (i) Sei (a_i) eine Cauchy-Folge in $\mathcal{O}$. Da für alle i gilt $v(a_i) \geq 0$ ist auch $v(\lim a_i) \geq 0$, also ist der Abschluß von $\mathcal{O}$ in K_v in $\mathcal{O}_v$ enthalten. Umgekehrt sei (a_i) eine Cauchy-Folge in K mit $\lim a_i \in \mathcal{O}_v$. Damit existiert ein $n_0 \in \mathbb{N}$ mit $v(a_n) \geq 0$ für alle $n \geq n_0$, also ist $\lim a_i$ auch Grenzwert einer Folge von Elementen aus $\mathcal{O}$.

(ii) Nach Proposition 10.5 ist jedes Element $a \in \mathcal{O}_v$ mit $v(a) = 1$ ein Erzeuger des maximalen Ideals $\mathfrak{m}_v$. Sei π ein $\mathcal{O}$-Erzeuger des maximalen Ideals $\mathfrak{m}$, wegen der Fortsetzung der Bewertung ist π damit auch ein $\mathcal{O}_v$-Erzeuger von $\mathfrak{m}_v$. Der Homomorphismus $\mathcal{O} \to \mathcal{O}_v/(\pi^i)$ hat dann den Kern (π^i) und faktorisiert damit durch einen injektiven Homomorphismus $\mathcal{O}/(\pi^i) \to \mathcal{O}_v/(\pi^i)$. Nach (i) existiert aber für jedes $a \in \mathcal{O}_v$ ein $b \in \mathcal{O}$ mit $v(a-b) \geq i$ bzw. $a \equiv b \mod (\pi^i)$. Damit ist der Homomorphismus auch surjektiv.

(iii) Der inverse Limes ist definiert durch

$$\varprojlim \mathcal{O}_v/\mathfrak{m}_v^n = \left\{ (x_n) \in \prod_{n=1}^{\infty} \mathcal{O}_v/\mathfrak{m}_v^n \mid x_n \equiv x_{n+1} \mod \mathfrak{m}_v^{n+1}. \right\}.$$

Der Kern der kanonischen Abbildung ist $\cap_{n=1}^{\infty} \mathfrak{m}_v^n = (0)$, also ist die Abbildung injektiv. Wegen (ii) hat jedes Element $a \in \mathcal{O}_v/\mathfrak{m}_v^n$ eine eindeutige Darstellung durch $a \equiv \sum a_i \pi^i \mod \mathfrak{m}_v^i$. Damit kann jedes Element des inversen Limes als Folge von Partialsummen einer Reihe $\sum_{i=0}^{\infty} a_i \pi^i$ geschrieben werden. Die Reihe konvergiert in $\mathcal{O}_v$ und ihr Grenzwert ist das Urbild von $\sum_{i=0}^{\infty} a_i \pi^i$.

Die Mengen $\prod_{i=n}^{\infty} \mathcal{O}_v/\mathfrak{m}_v^i$ bilden eine Umgebungsbasis der 0 im unendlichen Produkt, ihr Schnitt mit $\varprojlim \mathcal{O}_v/\mathfrak{m}_v^n$ eine Umgebungsbasis der 0 im inversen Limes. Die Mengen $\mathfrak{m}^i$ bilden eine Umgebungsbasis der 0 in $\mathcal{O}_v$. Diese Umgebungsbasen werden unter dem Isomorphismus ineinander abgebildet, also ist die kanonische Abbildung auch ein Homöomorphismus. □

Beispiel 10.12. *Der Bewertungsring von $\mathbb{Q}_p$ bezüglich der Fortsetzung des p-adischen Betrages wird mit $\mathbb{Z}_p$ bezeichnet. Dieser sollte nicht mit dem Bewertungsring $\mathbb{Z}_{(p)}$ des p-adischen Betrages auf $\mathbb{Q}$ verwechselt werden, $\mathbb{Z}_p$ ist die Komplettierung von $\mathbb{Z}_{(p)}$ wie im obigen Satz.* □

Proposition 10.13. *Sei K ein diskret bewerteter Körper mit Bewertungsring $\mathcal{O}$. Wir nehmen an, daß $\mathcal{O}/\mathfrak{m}$ endlich ist. Sei $F(x_1, \ldots, x_n)$ ein Polynom mit Koeffizienten aus $\mathcal{O}$. Die Kongruenz $F(x_1, \ldots, x_n) \equiv 0 \mod \mathfrak{m}^i$ ist genau dann für alle $i \geq 1$ lösbar, wenn die Gleichung $F(x_1, \ldots, x_n) = 0$ in $\mathcal{O}_v$ lösbar ist.*

Beweis. Eine Lösung der Gleichung in $\mathcal{O}_v$ liefert durch Reduktion modulo $\mathfrak{m}_v^i$ Lösungen für alle Kongruenzen.

Für die Umkehrung schränken wir uns auf $n = 1$ ein. Sei nun x_i die Lösung der Kongruenz $F(x) \equiv 0 \mod \mathfrak{m}^i$. Die x_i setzen sich zu einem Element im unendlichen Produkt $\prod_{n=1}^{\infty} \mathcal{O}_v/\mathfrak{m}_v^n$ zusammen. Wir nehmen an, daß die ersten n Glieder der Folge (x_i) bereits die Bedingung $x_i \equiv x_{i+1} \mod \mathfrak{m}^{i+1}$ erfüllen. Da es nur endlich viele Restklassen modulo $\mathfrak{p}^{n+1}$ gibt existiert eine Teilfolge (y_i) für die $F(y_i) \equiv 0 \mod \mathfrak{m}^{n+1}$ und $y_n \equiv y_{n+1} \mod \mathfrak{m}^{n+1}$ gilt. Induktiv konstruiert man so ein Element im inversen Limes, das die Gleichung $F(x) = 0$ erfüllt. □

Die Komplettierung von diskreten Bewertungsringen kodiert also die Information zur Lösung von Kongruenzen modulo Potenzen des maximalen Ideals. Gleichungen in der Komplettierung kann man dann mit analytischen Methoden lösen. Die Übertragung des Newton-Verfahrens auf nicht-archimedisch bewertete Körper wird als Lemma von Hensel bezeichnet.

Proposition 10.14 (Henselsches Lemma)**.** *Sei K ein vollständiger diskret bewerteter Körper mit Bewertungsring $\mathcal{O}$, und $f(X) \in \mathcal{O}[X]$ ein Polynom mit*

$f(X) \not\equiv 0 \mod \mathfrak{m}$. Wir nehmen an, daß $f(X)$ modulo $\mathfrak{m}$ eine Zerlegung in teilerfremde Polynome $\overline{g}(X), \overline{h}(X) \in \mathcal{O}/\mathfrak{m}[X]$ besitzt:

$$f(X) \equiv \overline{g}(X)\overline{h}(X) \mod \mathfrak{m}.$$

Dann besitzt $f(X)$ eine Zerlegung $f(X) = g(X)h(X)$ in Polynome $g(X), h(X) \in \mathcal{O}[X]$ mit

$$\deg g = \deg \overline{g}, \qquad g(X) \equiv \overline{g}(X) \mod \mathfrak{m}, \qquad h(X) \equiv \overline{h}(X) \mod \mathfrak{m}.$$

Beweis. In einer ersten Näherung betrachten wir Polynome $g_0, h_0 \in \mathcal{O}[X]$ mit $\deg g_0(X) \equiv \deg \overline{g}$, $g_0(X) \equiv \overline{g}(X) \mod \mathfrak{m}$ und $h_0(X) \equiv \overline{h}(X) \mod \mathfrak{m}$. Da $\overline{g}$ und $\overline{h}$ teilerfremd sind, existieren auch Polynome $a(X), b(X) \in \mathcal{O}[X]$ mit $ag_0 + bh_0 \equiv 1 \mod \mathfrak{m}$. Wenn $f = g_0h_0$ und $ag_0 + bh_0 = 1$ in $\mathcal{O}[X]$ gilt, sind wir fertig, sonst wählen wir in den Differenzen $f - g_0h_0$ und $ag_0 + bh_0 - 1$ den Koeffizienten mit der kleinsten Bewertung und bezeichnen ihn mit π.

Wir setzen

$$g = g_0 + \sum p_i\pi^i, \qquad h = h_0 + \sum q_i\pi^i$$

mit Polynomen $p_i, q_i \in \mathcal{O}[X]$ mit Grad $\leq \deg \overline{g}$ bzw. $\leq \deg f - \deg \overline{g}$. Rekursiv wollen wir die p_i und q_i so bestimmen, daß für $g_{n-1} = g_0 + p_1\pi + \cdots + p_{n-1}\pi^{n-1}$ und $h_{n-1} = h_0 + q_1\pi + \cdots + q_{n-1}\pi^{n-1}$ die Kongruenz $f \equiv g_{n-1}h_{n-1} \mod \pi^n$ gilt. Der Grenzüberganz zu $n \to \infty$ liefert dann die gewünschte Faktorisierung. Der Rekursionsanfang ist mit g_0 und h_0 gemacht.

Seien also g_{n-1} und h_{n-1} gegeben. Dann haben wir nach unserem Ansatz $g_n = g_{n-1} + p_n\pi^n$ und $h_n = h_{n-1} + q_n\pi^n$ und wir wollen die folgende Kongruenz lösen:

$$f - g_{n-1}h_{n-1} \equiv (g_{n-1}q_n + h_{n-1}p_n)\pi^n \equiv (g_0q_n + h_0p_n)\pi^n \mod \pi^{n+1}.$$

Wegen $g_0a + h_0b \equiv 1 \mod \pi$ ist $g_0af_n + h_0bf_n \equiv f_n \mod \pi$, also wären af_n und bf_n gute Lösungen, wir müssen aber noch die Gradbeschränkung sicherstellen.

Wir definieren p_n also durch eine Division mit Rest $bf_n = qg_0 + p_n$. Wegen $\deg g_0 = \deg \overline{g}$ ist der höchste Koeffizient von g_0 eine Einheit, und nach dem Gauß-Lemma folgt $q(X) \in \mathcal{O}[X]$. Die obige Kongruenz vereinfacht sich zu

$$g_0(af_n + h_0q) + h_0p_n \equiv f_n \mod \pi.$$

Das Polynom q_n ergibt sich aus $af_n + h_0q$ durch streichen aller durch π teilbaren Koeffizienten. □

Beispiel 10.15. *Das Polynom $x^{p-1} - 1 \in \mathbb{Z}_p[X]$ zerfällt über dem Restklassenkörper $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$ in verschiedene Linearfaktoren. Mit Proposition 10.14 zerfällt dieses Polynom also auch in $\mathbb{Z}_p$ in Linearfaktoren, d.h. $\mathbb{Q}_p$ enthält die $(p-1)$-ten Einheitswurzeln.* □

Übungsaufgabe 10.2. *Sei K vollständig bezüglich einer diskreten Bewertung und Bewertungsring $\mathcal{O}$. Jedes irreduzible normierte Polynom in $K[X]$ mit konstantem Koeffizienten in $\mathcal{O}$ liegt schon in $\mathcal{O}[X]$.*

10.3 Lokale Körper

Wir interessieren uns hier für die Vervollständigungen von Zahlkörpern an Absolutbeträgen.

Satz 10.16. *Sei K ein bewerteter Körper mit Charakteristik 0. Die folgenden Aussagen sind äquivalent.*

(i) K ist eine endliche Erweiterung von $\mathbb{Q}_p$.

(ii) K ist vollständig bezüglich einer diskreten Bewertung mit endlichem Restklassenkörper.

(iii) K ist vollständig, lokal kompakt und nicht diskret.

(iv) K ist Komplettierung eines Zahlkörpers an einem Absolutbetrag wie in Beispiel 10.4 (ii).

Es gibt auch eine Version dieses Satzes in Charakteristik p: Die endlichen Erweiterungen von $\mathbb{F}_q((t))$ sind genau die Komplettierung von Funktionenkörpern an einem Absolutbetrag. Körper mit den Eigenschaften (ii) bzw. (iii) im obigen Satz 10.16 (aber nicht notwendig Charakteristik 0) heißen *lokale Körper*. Der Beweis des Satzes ergibt sich aus den folgenden Sätzen: Die Äquivalenz $(i) \Leftrightarrow (ii)$ sind Satz 10.17 und Satz 10.18, die Implikation $(i) \Leftrightarrow (iv)$ ist Satz 10.20 und die Implikation $(iv) \Rightarrow (ii)$ ist Satz 10.11 (ii). Die Äquivalenz $(i) \Leftrightarrow (iii)$ zeigen wir hier nicht, cf. [Wei67, Kapitel I, §3].

Satz 10.17. *Sei K vollständig bezüglich einer diskreten Bewertung v. Für eine algebraische Erweiterung L/K existiert eine eindeutige Fortsetzung von v auf L. Wenn $[L : K] = n$ endlich ist, ist die Fortsetzung durch $v_L(\alpha) = \sqrt[n]{v_K(N_{L/K}(\alpha))}$ gegeben und L ist vollständig bezüglich dieser Fortsetzung.*

Beweis. Jede algebraische Erweiterung ist Vereinigung der endlichen Teilerweiterungen, wir können also $[L : K] = n$ endlich annehmen.

Sei $\mathcal{O}_K$ der Bewertungsring von K und $\mathcal{O}_L$ der ganze Abschluß von $\mathcal{O}_K$ in L. Dann gilt

$$\mathcal{O}_L = \left\{\alpha \in L \mid N_{L/K}(\alpha) \in \mathcal{O}_K\right\}.$$

Die Inklusion $\subseteq$ ist klar. Sei $\alpha \in L^\times$, $N_{L/K}(\alpha) \in \mathcal{O}_K$ und sei $f(X) = X^d + a_1X^{d-1} + \cdots + a_d \in K[X]$ das Minimalpolynom von α. Die Norm $N_{L/K}(\alpha)$ ist dann eine Potenz von a_d, also $v(a_d) \geq 0$ und mit Übungsaufgabe 10.2 folgt $f(X) \in \mathcal{O}[X]$, also $\alpha \in \mathcal{O}_L$.

Für die angegebene Fortsetzung sind wegen der Multiplikativität der Norm die Bedingungen (i) und (ii) klar. Offensichtlich folgt aus $v(\alpha) \geq 0$ auch $v(\alpha + 1) \geq 0$, dies impliziert die verschärfte Dreiecksungleichung in der Form $v(\alpha/\beta + 1) \geq \min\{v(\alpha/\beta), v(1)\}$. Damit definiert $v(\alpha) = \sqrt[n]{v(N_{L/K}(\alpha))}$ eine Bewertung auf L, die offensichtlich v fortsetzt und $\mathcal{O}_L$ als Bewertungsring hat.

Seien v_1 und v_2 Fortsetzungen von v auf L mit Bewertungsringen $\mathcal{O}_1$ und $\mathcal{O}_2$. Sei $\alpha \in \mathcal{O}_1 \setminus \mathcal{O}_2$ mit Minimalpolynom $f(X) = X^d + a_1X^{d-1} + \cdots + a_d$. Die Koeffizienten sind in $\mathcal{O}_K$ und nach Voraussetzung ist $\alpha^{-1} \in \mathfrak{m}_2$, aber $1 = -a_1\alpha^{-1} - \cdots - a_d\alpha^{-d} \in \mathfrak{m}_2$ ist ein Widerspruch zur Annahme. Also ist $\mathcal{O}_1 \subseteq \mathcal{O}_2$. Daraus folgt auch $\mathfrak{m}_1 \subseteq \mathfrak{m}_2$. Ein symmetrisches Argument liefert $v_1(\alpha) > 0$ genau dann, wenn $v_2(\alpha) > 0$, und mit dem Argument aus Lemma 10.7 folgt die

Äquivalenz von v_1 und v_2. Da v_1 und v_2 beide v fortsetzen, müssen sie sogar gleich sein.

Die Vollständigkeit folgt aus der hier nicht bewiesenen Tatsache, daß ein endlich-dimensionaler Vektorraum V über einem vollständig bewerteten Körper K immer schon zu K^n *homöomorph* ist. □

Satz 10.18. *Sei K vollständig bezüglich einer diskreten Bewertung v mit endlichem Restklassenkörper und* $\mathrm{char}(k) = 0$. *Dann ist K eine endliche Erweiterung von $\mathbb{Q}_p$.*

Beweis. Wegen $\mathrm{char}(k) = 0$ ist $\mathbb{Q} \subseteq K$ und die Einschränkung von v auf $\mathbb{Q}$ ist nach Proposition 10.8 äquivalent zu einer p-adischen Bewertung. Die universelle Eigenschaft der Komplettierung impliziert $\mathbb{Q}_p \subseteq K$. Nach dem Lemma von Riesz ist ein topologischer Vektorraum genau dann lokal-kompakt, wenn er endlich-dimensional ist. Das Ergebnis folgt dann aus der folgenden Proposition. □

Proposition 10.19. *Sei K vollständig bezüglich einer diskreten Bewertung v mit endlichem Restklassenkörper und* $\mathrm{char}(k) = 0$. *Dann ist K lokal kompakt, und sein Bewertungsring $\mathcal{O}$ ist kompakt.*

Beweis. Mit Satz 10.11 können wir $\mathcal{O}$ und den inversen Limes $\lim \mathcal{O}/\mathfrak{m}^n$ identifizieren. Die Ringe $\mathcal{O}/\mathfrak{m}^n$ sind endlich, also kompakt. Nach dem Satz von Tychonoff ist dann das unendliche Produkt $\prod \mathcal{O}/\mathfrak{m}^n$ kompakt, damit auch die abgeschlossene Teilmenge $\lim \mathcal{O}/\mathfrak{m}^n$.

Für $a \in K$ ist $a + \mathcal{O}$ eine offene und kompakte Umgebung, also ist K lokal kompakt. □

Satz 10.20. *Sei $k/\mathbb{Q}_p$ endlich. Dann gibt es einen Zahlkörper $K/\mathbb{Q}$ mit $[K : \mathbb{Q}] = [k : \mathbb{Q}_p]$ und K ist dicht in k.*

Beweis. Nach Satz 10.17 gibt es eine Bewertung auf k, die die p-adische Bewertung fortsetzt und die wir auch mit v_p bezeichnen. Wir wählen ein primitives Element α von $k/\mathbb{Q}_p$ mit Minimalpolynom $f(X) = X^d + a_1 X^{d-1} + \cdots + a_d$. Da $\mathbb{Q}$ in $\mathbb{Q}_p$ dicht liegt, können wir für gegebenes n ein Polynom $g(X) = X^d + b_1 X^{d-1} + \cdots + b_d$ wählen mit $v_p(a_i - b_i) \geq n$ für alle i.

Das Polynom f ist nach Voraussetzung irreduzibel und separabel. Dann ist für genügend großes n auch g irreduzibel und separabel. Außerdem ist nach Wahl der b_i die Bewertung

$$v_p(f(\alpha) - g(\alpha)) = v_p(-g(\alpha)) = \prod v(\alpha - \beta_i)$$

groß, wobei β_i die Nullstellen von g bezeichnet. Es gibt also eine Nullstelle β von g für die $v(\alpha - \beta)$ groß ist.

Wir wollen $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\beta)$ zeigen, wenigstens für genügend großes n. Sei dazu k' die normale Hülle von $\mathbb{Q}_p(\alpha, \beta)$. Für $\sigma \in \mathrm{Gal}(k'/\mathbb{Q}_p(\beta))$ und $a \in k'$ ist $v_p(\sigma(a)) = v_p(a)$, da $v_p(\sigma(\cdot))$ eine neue Bewertung und nach Satz 10.17 gleich $v_p(\cdot)$ ist. Für n groß genug können wir $v_p(\beta - \alpha) > v_p(\sigma(\alpha) - \alpha)$ für alle $\sigma \in \mathrm{Gal}(k'/\mathbb{Q}_p(\beta))$ mit $\sigma(\alpha) \neq \alpha$ annehmen. Damit ist

$$v_p(\beta - \sigma(\alpha)) = v_p(\sigma(\beta) - \sigma(\alpha)) > v_p(\sigma(\alpha) - \alpha).$$

Wir erhalten einen Widerspruch:

$$v_p(\sigma(\alpha) - \alpha) = v_p(\sigma(\alpha) - \beta + \beta - \alpha) > v_p(\sigma(\alpha) - \alpha).$$

Also muß $\sigma(\alpha) = \alpha$ für alle $\sigma \in \mathrm{Gal}(k'/\mathbb{Q}_p(\beta))$ sein. Wir haben dann $\mathbb{Q}_p(\alpha) \subseteq \mathbb{Q}_p(\beta)$, und mit einem symmetrischen Argument sogar Gleichheit. Der so gefundene Zahlkörper erfüllt die Behauptung. □

10.4 Ausblick: Lokal-Global-Prinzip

In diesem letzten Abschnitt wollen wir noch einen Ausblick auf eine mögliche Anwendung lokaler Körper in der Zahlentheorie geben. Wir stellen kurz die Entwicklung des Lokal-Global-Prinzips vor, das es ermöglicht, quadratische Formen über $\mathbb{Q}$ zu klassifizieren und quadratische Gleichungen über $\mathbb{Q}$ zu lösen. Die Wirkungsweise des Lokal-Global-Prinzips ist dabei, daß man die quadratische Gleichung nur über den lokalen Körpern zu lösen braucht, um auch eine Lösung über $\mathbb{Q}$ zu erhalten. Die Lösung einer quadratischen Gleichung über lokalen Körpern ist nun aber deutlich einfacher als die "globale" Lösung. Die Beweise der Aussagen dieses Abschnitts finden sich z.B. in [Ser73, Teil I], Ziel dieses Ausblicks ist eher, eine Vorstellung von der Vorgehensweise der Zahlentheorie zu liefern.

An dieser Stelle muß natürlich auch darauf hingewiesen werden, daß ein Lokal-Global-Prinzip in dieser Form nur für quadratische Gleichungen gilt. Das bekannte Beispiel $3X^3 + 4Y^3 + 5Z^3 = 0$ von Selmer zeigt, daß ab Grad 3 Gleichungen existieren, die in allen lokalen Körpern eine Lösung haben, aber keine globale Lösung. Dies ist eine der wesentlichen Schwierigkeiten, mit denen sich die modernere Zahlentheorie beschäftigt.

Definition 10.21. *Sei K ein Körper. Für Elemente $a, b \in K^\times$ definieren wir das* Hilbert-Symbol *durch*

$$(a,b) = \begin{cases} 1 & Z^2 - aX^2 - bY^2 = 0 \text{ hat eine nichttriviale Lösung} \\ -1 & \text{sonst} \end{cases}$$

Das Hilbert-Symbol ist eine Verallgemeinerung des Legendre-Symbols. Es macht eine Aussage über das Lösungsverhalten der quadratischen Form $Z^2 - aX^2 - bY^2$ im Körper K. Offensichtlich hängt das Hilbert-Symbol nur von der Quadrat-Restklasse von a und b ab, es liefert also eine Abbildung $K^\times/(K^\times)^2 \times K^\times/(K^\times)^2 \to \mathbb{Z}/2\mathbb{Z}$. Wie im Fall des Legendre-Symbols überzeugt man sich davon, daß $(a,b) = 1$ genau dann, wenn a die Norm eines Elementes aus $K(\sqrt{b})^\times$ ist.

Die folgende Proposition zeigt, daß man im Fall lokaler Körper von Charakteristik 0 das Hilbert-Symbol durch das Legendre-Symbol ausdrücken kann. Der Beweis ist eine explizite Fallunterscheidung.

Proposition 10.22. *Für $K = \mathbb{R}$ ist $(a,b) = 1$ genau dann, wenn $a > 0$ oder $b > 0$ ist.*

Für $K = \mathbb{Q}_p$ können wir $a = p^\alpha u$ und $b = p^\beta v$ mit $u, v \in \mathbb{Z}_p^\times$ schreiben und haben dann

$$(a,b) = (-1)^{\alpha\beta\epsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha \quad \text{für } p \neq 2$$

$$(a,b) = (-1)^{\epsilon(u)\epsilon(v)+\alpha\omega(v)+\beta\omega(u)} \quad \text{für } p = 2$$

wobei $\epsilon(u)$ und $\omega(u)$ jeweils die Restklassen von $\frac{u-1}{2}$ und $\frac{u^2-1}{8}$ modulo 2 bezeichnen.

Korollar 10.23. *Das Hilbert-Symbol erfüllt die folgenden Rechenregeln:*

(i) $(a,b) = (b,a)$, $(a,b^2) = 1$.

(ii) $(a,-a) = 1$, $(a,1-a) = 1$.

(iii) $(aa',b) = (a,b)(a',b)$.

(iv) $(a,b) = (a,-ab) = (a,(1-a)b)$.

Beweis. (i) und (ii) sind offensichtlich. (iii) folgt aus Proposition 10.22. (iv) folgt aus (i)-(iii). □

Die folgende Produktformel ist im Wesentlichen eine Umformulierung des quadratischen Reziprozitätsgesetzes, zusammen mit Proposition 10.22.

Proposition 10.24 (Produktformel)**.** *Seien $a,b \in \mathbb{Q}^\times$. Dann gilt $(a,b)_v = 1$ für fast alle Stellen v von $\mathbb{Q}$ und*

$$\prod_{v\in V} (a,b)_v = 1, \; V \text{ die Menge der Stellen von } \mathbb{Q}.$$

Das erste Beispiel für ein Lokal-Global-Prinzip ist die folgende Existenzaussage über rationale Zahlen mit gegebenem Hilbert-Symbol. Diesen Satz können wir hier nicht beweisen, er benutzt den Approximationssatz und Dirichlets Satz über Primzahlen in arithmetischen Progressionen.

Proposition 10.25. *Wir bezeichnen wieder mit V die Stellenmenge von $\mathbb{Q}$. Sei $(a_i)_{i\in I}$ eine endliche Menge von Elementen $a_i \in \mathbb{Q}^\times$ und $(\epsilon_{i,v})_{i\in I, v\in V}$ eine Menge von Zahlen $\epsilon_{i,v} = \pm 1$. Dann existiert eine rationale Zahl $x \in \mathbb{Q}^\times$ mit $(a_i,x)_v = \epsilon_{i,v}$ für alle $i \in I$ und $v \in V$ genau dann, wenn die folgenden Bedingungen erfüllt sind:*

(i) Fast alle $\epsilon_{i,v}$ sind 1.

(ii) Für alle $i \in I$ gilt $\prod_{v\in V} \epsilon_{i,v} = 1$.

(iii) Für alle $v \in V$ existiert $x_v \in \mathbb{Q}_v^\times$ mit $(a_i,x_v)_v = \epsilon_{i,v}$ für alle $i \in I$.

Die Bedingungen des Satzes sind die globale Bedingung der Produktformel und die lokale Existenz von p-adischen bzw. reellen Zahlen mit dem gegebenen Hilbert-Symbol. Das reicht schon aus, um die Existenz einer rationalen Zahl mit gegebenem Hilbert-Symbol zu garantieren. Die Aussagen lassen sich auf Zahlkörper verallgemeinern.

Wir betrachten nun quadratische Formen, cf. Definition 8.1. Eine quadratische Form auf einem K-Vektorraum V ist eine Abbildung $q : V \to K$ mit den beiden Eigenschaften

(i) $q(av) = a^2 q(v)$ für alle $v \in V$ und $a \in K$.

(ii) $(x,y) \mapsto q(x+y) - q(x) - q(y)$ ist eine Bilinearform.

Die Dimension von V wird auch als *Rang der quadratischen Form* q bezeichnet.

Nach Wahl einer Basis $e_1, \ldots, e_n$ von V kann man die quadratische Form durch eine Matrix darstellen:

$$q(X) = \sum_{i,j} a_{ij} x_i x_j, \qquad x = \sum x_i e_i.$$

Basiswechsel mit der Matrix X ändert die darstellende Matrix von A zu XAX^t, damit ist die Determinante von $A = (a_{ij})$ bis auf ein Quadrat wohldefiniert. Die Restklasse von $\det(a_{ij})$ in $K^\times/(K^\times)^2$ wird *Diskriminante der quadratischen Form* q genannt und mit $\operatorname{disc}(q)$ bezeichnet. Das Gram-Schmidt-Verfahren, s. Proposition 8.3, erlaubt es, für jede quadratische Form q auf einem Vektorraum V eine Orthogonalbasis zu finden, in der q die Form

$$q(x) = \sum a_i x_i^2$$

hat. In diesem Fall ist $\operatorname{disc}(q) = \prod a_i$.

Die Klassifikation von quadratischen Formen über endlichen Körpern ist sehr einfach – eine quadratische Form ist bis auf Isometrie durch Rang und Diskriminante bestimmt.

Proposition 10.26. *Sei q eine quadratische Form vom Rang n über $\mathbb{F}_q$. Dann ist q isometrisch zu einer der folgenden Formen*

$$q \cong \begin{cases} x_1^2 + \cdots + x_n^2 & \operatorname{disc}(q) \in (\mathbb{F}_q^\times)^2, \\ x_1^2 + \cdots + x_{n-1}^2 + \operatorname{disc}(q) x_n^2 & \operatorname{disc}(q) \in (\mathbb{F}_q^\times)^2 \end{cases}$$

Die Klassifikation quadratischer Formen über $\mathbb{Q}_p$ ist schon etwas komplizierter. Wir benötigen noch eine zweite Invariante:

Definition 10.27. *Sei $K = \mathbb{Q}_p$, V ein K-Vektorraum, q eine quadratische Form auf V und $e_1, \ldots, e_n$ eine Orthogonalbasis von q bezüglich derer $q(x) = \sum a_i x_i^2$ ist. Dann definieren wir*

$$\epsilon(e_1, \ldots, e_n) = \prod_{i<j} (a_i, a_j).$$

Proposition 10.28. *Die Zahl $\epsilon(e_1, \ldots, e_n)$ hängt nicht von der Wahl der Orthogonalbasis $e_1, \ldots, e_n$ ab. Die Zahl $\epsilon(q) = \epsilon(e_1, \ldots, e_n)$ ist also eine Invariante der quadratischen Form q. Sie wird die* Hasse-Witt-Invariante *von q genannt.*

Satz 10.29. *Sei $K = \mathbb{Q}_p$.*

(i) Zwei quadratische Formen über K sind isometrisch genau dann, wenn Rang, Diskriminante und Hasse-Witt-Invariante übereinstimmen.

(ii) Die Gleichung $q(x) = 0$ hat genau dann eine nicht-triviale Lösung, wenn eine der folgenden Bedingungen erfüllt ist:

- *(a)* $\operatorname{rk}(q) = 2$ *und* $\operatorname{disc}(q) = -1$,
- *(b)* $\operatorname{rk}(q) = 3$ *und* $(-1, -d) = \epsilon(q)$,
- *(c)* $\operatorname{rk}(q) = 4$ *und* $d \neq -1$ *oder* ($d = 1$ *und* $\epsilon(q) = (-1, -1)$,
- *(d)* $\operatorname{rk}(q) \geq 5$.

(iii) Sei $n \geq 1$, $d \in K^\times/(K^\times)^2$ und $\epsilon = \pm 1$. Dann existiert genau dann eine quadratische Form vom Rang n mit Diskriminante d und Hasse-Witt-Invariante ϵ, wenn eine der folgenden Bedingungen erfüllt ist:

(a) $n = 1$ und $\epsilon = 1$.

(b) $n = 2$, $d \neq -1$.

(c) $n = 2$, $\epsilon = 1$.

(d) $n \geq 3$.

Beweis. Die Spezialfälle niedrigen Ranges erhält man durch Berechnungen mit dem Hilbert-Symbol. Der allgemeine Fall ergibt sich durch Induktion aus den Spezialfällen. □

Satz 10.30 (Hasse-Minkowski)**.** *(i) Zwei über $\mathbb{Q}$ definierte quadratische Formen q_1 und q_2 sind genau dann isometrisch, wenn für alle Stellen v von $\mathbb{Q}$ die entsprechenden Formen $q_{1,v}$ und $q_{2,v}$ isometrisch über $\mathbb{Q}_p$ sind.*

(ii) Sei q eine quadratische Form über $\mathbb{Q}$. Die Gleichung $q(x) = 0$ hat genau dann eine nicht-triviale Lösung in $\mathbb{Q}$, wenn für alle Stellen v von $\mathbb{Q}$ die Gleichung $q_v(x) = 0$ eine Lösung in $\mathbb{Q}_v$ hat.

Beweis. Auch hier sind die Spezialfälle explizite Rechnungen mit der Produktformel und dem Lokal-Global-Prinzip für das Hilbert-Symbol. Der allgemeine Fall ist eine Induktion. □

Der Satz von Hasse-Minkowski liefert so eine umfassende Verallgemeinerung des Zwei-Quadrate-Satzes.

Korollar 10.31 (Gauß)**.** *Sei a eine positive ganze Zahl. Die folgenden Eigenschaften sind äquivalent:*

(i) Die Zahl a ist als Summe von drei Quadraten darstellbar.

(ii) Die Zahl a hat nicht die Form $4^x(8y - 1)$.

(iii) Die Zahl $-a$ ist kein Quadrat in $\mathbb{Q}_2$.

Übungsaufgaben

Übungsaufgabe 10.3. *Sei K ein Körper und $p(X)$ ein irreduzibles Polynom. Bestimmen Sie die Komplettierung des Funktionenkörpers $K(X)$ bezüglich des Absolutbetrages, der zum Primideal $(p(X))$ gehört.*

Übungsaufgabe 10.4. *Zeigen Sie, daß die Menge der Potenzreihen*

$$\left\{ \sum_{i=-m}^{\infty} a_i p^i \mid m \in \mathbb{Z}, 0 \leq a_i < p \right\}$$

mit $\mathbb{Q}_p$ identifiziert werden kann. Geben Sie die p-adische Entwicklung für -1 und $(1-p)^{-1}$ an.

Übungsaufgabe 10.5. *Eine Potenzreihe $f(X) = \sum_{i=0}^{\infty} a_i X^i$ ist genau dann eine Einheit im Potenzreihenring $K[[X]]$, wenn $a_0 \neq 0$ ist.*

Übungsaufgabe 10.6. *Zeigen Sie, daß die Gleichung $x^2 = 0$ eine Lösung in $\mathbb{Z}_7$ hat. Geben Sie die ersten 3 Terme der 7-adischen Entwicklung der beiden Lösungen an.*

Übungsaufgabe 10.7. *Seien p, q verschiedene Primzahlen mit $q \nmid (p-1)$. Benutzen Sie das Henselsche Lemma, um zu zeigen, daß die Gleichung $x^q + y^q = z^q$ eine Lösung in $\mathbb{Z}_p$ hat.*

Übungsaufgabe 10.8. *Sei $K = \mathbb{Q}(\theta)$ der Zahlkörper, der durch Adjunktion einer Wurzel θ von $f(x) = x^3 - 5x + 5$ entsteht. Welche Primideale von $\mathbb{Z}$ sind verzweigt in $K/\mathbb{Q}$? Berechnen Sie den Verzweigungsindex der entsprechenden Primideale. Was können Sie nach dem Berechnen des Verzweigungsindex über den Ganzheitsring $\mathcal{O}_K$ sagen?*

Hinweis: Zur Beschreibung der Verzweigung ist es nicht notwendig, den Ganzheitsring zu ermitteln, sondern die lokalen Erweiterungen zu untersuchen.

Übungsaufgabe 10.9. *Sei $K/\mathbb{Q}_p$ ein lokaler Körper, $u \in \mathcal{O}_K^*$ eine Einheit, und $e \in \mathbb{N}$ eine natürliche Zahl mit $p \nmid e$. Zeigen Sie, dass die Erweiterung $K(\alpha)/K$ unverzweigt ist, wobei $\alpha^e = u$ ist.*

Übungsaufgabe 10.10. *Zeigen Sie, dass $\mathbb{Q}_p(\zeta_p) = \mathbb{Q}_p(\sqrt[p-1]{-p})$ gilt.*

(a) Geben Sie das Minimalpolynom für $\zeta_p - 1$ an und folgern Sie daraus, dass $(\zeta_p - 1)^{p-1} \equiv -p \mod (\zeta_p - 1)^p$.

(b) Benutzen Sie das Henselsche Lemma, um zu zeigen, dass eine $(p-1)$-te Wurzel von $-p$ in $\mathbb{Q}_p(\zeta_p)$ existiert. Folgern Sie daraus die Behauptung.

Übungsaufgabe 10.11. *Sei K ein Zahlkörper.*

(i) Zeigen Sie, daß ein Element $x \in K$ genau dann ganz ist, wenn für alle endlichen Stellen v von K gilt $v(x) \geq 0$.

(ii) Zeigen Sie, daß ein ganzes Element $x \in \mathcal{O}_K$ genau dann eine Einheit ist, wenn für alle endlichen Stellen v von K das Element x_v eine Einheit in $\mathcal{O}_{K_v}$ ist, also $v(x) = 0$ ist.

Übungsaufgabe 10.12. *Sei L/K eine Erweiterung globaler Körper, v ein Absolutbetrag auf K und $w_1, \ldots, w_n$ die Beträge von L, die v fortsetzen. Wir normieren die Beträge w_i so, daß $|x|_{w_i} = |x|_v^{[L_{w_i}:K_v]}$ für alle $x \in K$. Zeigen Sie:*

$$|N_{L/K}|_v = \prod_{w_i | v} |x|_{w_i}.$$

Anhang A

Grundlagen

Konventionen: Alle Ringe sind kommutativ mit 1, Ringhomomorphismen bewahren die 1.

A.1 Moduln: Lineare Algebra über Ringen

Definition A.1. *Sei R ein Ring. Ein R-*Modul *M ist eine Menge zusammen mit zwei Operationen, der Addition $+ : M \times M \to M$ und der Skalarmultiplikation $\cdot : R \times M \to M$, so daß die folgenden Axiome gelten:*

(i) $(M, +)$ *ist eine abelsche Gruppe.*

(ii) Für alle $\lambda, \mu \in R$ und $x, y \in M$ gilt

$$\lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y, \qquad (\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x.$$

(iii) Für alle $\lambda, \mu \in R$ und $x \in M$ gilt $\lambda \cdot (\mu \cdot x) = (\lambda\mu) \cdot x$.

(iv) Für alle $x \in M$ gilt $1 \cdot x = x$.

Definition A.2. *Sei R ein Ring. Ein R-Modulhomomorphismus $f : M \to N$ ist eine Abbildung, die mit den Operationen $+$ und $\cdot$ verträglich ist, d.h. für alle $x, y \in M$ und $\lambda, \mu \in R$ gilt*

$$f(\lambda \cdot x + \mu \cdot y) = \lambda \cdot f(x) + \mu \cdot f(y).$$

Die Menge der R-Modulhomomorphismen $f : M \to N$ wird mit $\mathrm{Hom}_R(M, N)$ *bezeichnet.*

Für $R = k$ ein Körper sind k-Moduln genau die k-Vektorräume, k-Modulhomomorphismen sind genau k-lineare Abbildungen. Moduln über $\mathbb{Z}$ sind genau abelsche Gruppen.

Aussagen aus der Linearen Algebra, bei denen man nicht durch irgendwelche Elemente teilen muß, sind auch für Moduln über Ringen gültig.

Definition A.3. *Sei R ein Ring, M ein R-Modul.*

(i) Eine Familie $m_i \in M$, $i \in I$, heißt Erzeugendensystem*, wenn es für jedes $m \in M$ ein $n \in \mathbb{N}$, $i_1, \ldots, i_n \in I$, und $\lambda_1, \ldots, \lambda_n \in R$ gibt mit $m = \sum_{j=1}^{n} \lambda_j m_{i_j}$.*

(ii) Ein Modul heißt endlich erzeugt*, wenn es ein endliches Erzeugendensystem gibt.*

(iii) Eine Familie $m_i \in M$, $i \in I$ heißt linear unabhängig*, wenn aus $\lambda_1 m_{i_1} + \cdots + \lambda_n m_{i_n} = 0$ schon $\lambda_1 = \cdots = \lambda_n = 0$ folgt.*

(iv) Ein linear unabhängiges Erzeugendensystem heißt Basis.

(v) Ein Modul heißt frei*, wenn es eine Basis gibt. Die Mächtigkeit der Basis heißt* Rang des Moduls.

Definition A.4. *Sei R ein Ring, M ein R-Modul. Ein R-Untermodul $N \subseteq M$ ist eine Teilmenge, die abgeschlossen unter Addition und Skalarmultiplikation ist.*

Wenn $N \subseteq M$ ein R-Untermodul ist, dann definiert

$$x \sim y \text{ genau dann, wenn } x - y \in N$$

eine Äquivalenzrelation auf M. Auf den Äquivalenzklassen kann man wieder die Struktur eines R-Moduls definieren und zwar durch

$$[x] + [y] = [x + y], \qquad \lambda \cdot [x] = [\lambda \cdot x].$$

Der Ring M/N heißt Quotientenmodul. Wenn R ein Ring und $I \subseteq R$ ein Ideal, also ein R-Untermodul, von R ist, dann erhält man so auch wieder eine Ringstruktur auf R/I.

Definition A.5. *Sei R ein Ring, $f : M \to N$ ein R-Modulhomomorphismus. Wir definieren*

$$\ker f = \{m \in M \mid f(m) = 0\}, \qquad \operatorname{im} f = \{n \in N \mid \exists m \in M : f(m) = n\}.$$

Eine Sequenz von R-Modulhomomorphismen

$$\cdots \xrightarrow{f_{i-1}} M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \xrightarrow{f_{i+2}} \cdots$$

heißt exakt an der Stelle M_i*, wenn* $\ker f_{i+1} = \operatorname{im} f_i$*. Sie heißt* exakt*, wenn sie an allen Stellen exakt ist.*

Kern und Bild sind R-Untermoduln.

Satz A.6. *Sei R ein Ring, $f : M \to N$ ein R-Modulhomomorphismus. Dann ist die induzierte Abbildung $\overline{f} : M/\ker f \to \operatorname{im} f$ ein Isomorphismus von R-Moduln. Für Untermoduln $N_1, N_2 \subseteq M$ gibt es einen kanonischen Isomorphismus von R-Moduln*

$$(N_1 + N_2)/N_1 \cong N_2/(N_1 \cap N_2).$$

Für Untermoduln $N_1 \subseteq N_2 \subseteq M$ gibt es einen kanonischen Isomorphismus von R-Moduln

$$(M/N_1)/(N_2/N_1) \cong M/N_2.$$

Wir formulieren noch die Ring-Version der Cramerschen Regel. Dies funktioniert, da im Beweis der Cramerschen Regel keine Division auftritt.

Lemma A.7. *Sei R ein Ring, $A = (a_{ij})$ eine quadratische Matrix in $M_n(R)$. Wenn das Gleichungssystem $Ax = b$ eine nichttriviale Lösung $(x_1, \ldots, x_n)$ hat, dann gilt $x_i \det A = \det A_i$ für alle i, wobei A_i entsteht, indem in A die i-te Spalte durch b ersetzt wird.*

A.2 Matrizen und Moduln über Hauptidealringen

Wir beginnen mit einer kurzen Erinnerung zu euklidischen Ringen und dem euklidischen Algorithmus.

Definition A.8. *Sei R ein Integritätsbereich. Eine* euklidische Funktion *auf R ist eine Abbildung $f : R\setminus\{0\} \to \mathbb{N}$, so daß für $a, b \in R$ mit $b \neq 0$ Elemente $q, r \in R$ existieren mit $a = qb + r$ und $r = 0$ oder $f(r) < f(b)$. Ein Integritätsbereich heißt* euklidischer Ring*, wenn es auf R eine euklidische Funktion gibt.*

Beispiele für euklidische Ringe sind $\mathbb{Z}$ und $K[X]$. Für $\mathbb{Z}$ ist der Absolutbetrag eine euklidische Funktion. Für den Polynomring $K[X]$ ist die Gradfunktion $\deg : K[X] \to \mathbb{N}$ eine euklidische Funktion. Damit kann man über wiederholte Polynomdivision den größten gemeinsamen Teiler von zwei Polynomen berechnen.

Eingabe: zwei Polynome $f(X), g(X) \in K[X]$
Ausgabe: $ggT(f(X), g(X))$
while $g(X) \neq 0$ **do**
  Polynomdivision mit Rest $f(X) = q(X)g(X) + r(X)$ mit
  $\deg r(X) < \deg g(X)$;
  $f(X) \longleftarrow g(X), g(X) \longleftarrow r(X)$;
end
$ggT = f(X)$;

Algorithm 10: Euklidischer Algorithmus im Polynomring

Terminierung des Algorithmus folgt daraus, daß in jedem Schritt der Grad von $f(X)$ und $g(X)$ kleiner wird. Korrektheit folgt aus $ggT(f(X), g(X)) = ggT(g(X), r(X))$ für $f(X) = q(X)g(X) + r(X)$. Der Zeitbedarf für den euklidischen Algorithmus ist quadratisch im Grad der Polynome.

A.2.1 Hermite-Normalform

Definition A.9 (Hermite-Normalform)**.** *Eine $(m \times n)$-Matrix (a_{ij}) mit Einträgen in $\mathbb{Z}$ ist in* Hermite- Normalform*, wenn es ein r mit $0 \leq r \leq n$ und eine streng wachsende Abbildung $f : [r+1, n] \to [1, m]$ gibt, so daß die ersten r Spalten identisch 0 sind und für alle j mit $r+1 \leq j \leq n$ die folgenden Bedingungen erfüllt sind:*

(i) $a_{f(j),j} > 0$,

(ii) $a_{ij} = 0$ *für* $i > f(j)$,

(iii) $a_{f(j),j} > a_{f(j),k} \geq 0$ *für* $k > j$.

Satz A.10. *Sei A eine $(m \times n)$-Matrix mit Einträgen in $\mathbb{Z}$. Dann existiert eine eindeutige $(m \times n)$-Matrix B in Hermite-Normalform und eine Matrix $U \in GL_n\mathbb{Z}$ so daß gilt $B = AU$.*

Der Beweis ist eine Kombination aus dem Gauß-Verfahren zur Lösung linearer Gleichungssysteme und dem euklidischen Algorithmus zur Bestimmung größter gemeinsamer Teiler.

Eingabe: $(m \times n)$-Matrix (a_{ij}) mit Einträgen in $\mathbb{Z}$
Ausgabe: Hermite-Normalform (b_{ij}) von (a_{ij})
$i \longleftarrow m$, $k \longleftarrow n$, $l \longleftarrow \max(1, m-n+1)$;
repeat
  while $\exists j < k : a_{ij} \neq 0$ **do**
    Wähle j_0 so daß a_{i,j_0} minimalen Betrag unter den $a_{i,j}$ mit $j \leq k$ hat;
    if $j_0 < k$ **then** k-te und j_0-te Spalte vertauschen;
    if $a_{i,k} < 0$ **then** k-te Spalte mit -1 multiplizieren;
    $b \longleftarrow a_{ik}$;
    forall $j = 1, \ldots, k-1$ **do** $q \longleftarrow \lfloor a_{ij}/b + 1/2 \rfloor$, $A_j \longleftarrow A_j - qA_k$;
    `// A_j ist die j-te Spalte, also elt. Spaltenoperation`
  end
  if $a_{ik} < 0$ **then** k-te Spalte mit -1 multiplizieren;
  if $a_{ik} = 0$ **then**
    $k \longleftarrow k+1$
  else
    forall $j > k$ **do** $q \longleftarrow \lfloor a_{ij}/b + 1/2 \rfloor$, $A_j \longleftarrow A_j - qA_k$
  end
  $i \longleftarrow i-1$, $k \longleftarrow k-1$;
until $i = l - 1$;
$j + k - 1$-te Spalte von A ist j-te Spalte der Hermite-Normalform;

Algorithm 11: Hermite-Normalform

Bemerkung A.11. *Für eine Matrix $A \in M_n\mathbb{Z}$ mit $\det(A) \neq 0$ und $B \geq |a_{ij}|$ eine obere Schranke für die Beträge der Einträge in A kann die Hermite-Normalform mit $O(n^6 \log n \log B)$ arithmetischen Operationen bestimmt werden. Die Größenordnung der auftretenden Zahlen ist dabei in Binärdarstellung $O(n^4 \log n \log B)$.*

Bemerkung A.12. *Die Hermite-Normalform kann für allgemeiner für Hauptidealringe definiert werden. Wir benötigen hier aber nur den Fall $\mathbb{Z}$.*

Die Hermite-Normalform kann unter anderem zur Berechnung von Kern und Bild einer Matrix mit $\mathbb{Z}$-Koeffizienten benutzt werden.

A.2.2 Elementarteilersatz

Die folgende Form des Elementarteilersatzes sollte, wenigstens für $R = \mathbb{Z}$, aus der Linearen Algebra bekannt sein. Der Beweis ist eine Kombination aus dem Gauß-Verfahren zur Lösung linearer Gleichungssysteme und dem euklidischen Algorithmus zur Bestimmung größter gemeinsamer Teiler.

Satz A.13 (Elementarteilersatz, Erste Form)**.** *Sei R ein Hauptidealring, $A = (a_{ij})$ eine $(n \times m)$-Matrix mit Einträgen in R. Dann existieren Matrizen $S \in GL_n(R)$ und $T \in GL_m(R)$, so daß SAT eine Diagonalmatrix mit Einträgen $(d_1, \ldots, d_{\min(n,m)})$ ist, wobei $d_1 \mid d_2 \mid \cdots \mid d_{\min(n,m)}$ gilt.*

Diese Normalform von Matrizen wird als Smith-Normalform bezeichnet. Wir ersparen uns hier die explizite Angabe eines Algorithmus zur Berechnung der Smith-Normalform.

Aus diesem Satz kann man Strukturaussagen für endlich erzeugte Moduln über Hauptidealringen ableiten.

Satz A.14 (Elementarteilersatz, Zweite Form)**.** *Sei R ein Hauptidealring, M ein endlich erzeugter R-Modul. Dann gibt es Elemente $d_1, \ldots, d_k \in R$ mit $d_1 \mid d_2 \mid \cdots \mid d_k$ so daß*

$$M \cong \bigoplus_{i=1}^{k} R/(d_i).$$

Beweis. Diese Aussage folgt aus der ersten Form, in dem man für M eine freie Auflösung wählt:

$$R^m \xrightarrow{f} R^n \to M \to 0.$$

Die darstellende Matrix A von f ist eine $(n \times m)$-Matrix. Die Matrizen S und T sind Basiswechselmatrizen. Wenn f Diagonalform mit Elementarteilern d_i hat, dann ist der Quotient offensichtlich von der angegebenen Form. □

Korollar A.15. *Sei R ein Hauptidealring, M ein endlich erzeugter R-Modul.*

(i) Wenn M torsionsfrei ist, d.h. $ax = 0$, $a \in R$, $x \in M$ impliziert $a = 0$ oder $x = 0$, dann ist M frei.

(ii) Wenn M frei ist, dann ist jeder R-Untermodul von M wieder frei.

Übungsaufgabe A.1. *Ein Ring R ist genau dann ein Hauptidealring, wenn für jeden freien R-Modul M jeder R-Untermodul $N \subseteq M$ wieder frei ist.*

Anhang B

Beispiele in Pari/GP

Aufgabe 1

Geben Sie ein Pari/GP-Programm an, mit dem man für gegebenes m die kleinste Zahl n bestimmen kann, so daß das zyklotomische Polynom $\Phi_n(X)$ einen Koeffizienten $\pm m$ hat.

Das folgende Programm löst die Aufgabenstellung. Die Sequenz und das Programm findet sich auf `http://oeis.org/A013594`

```
nm=10000;
m=0;
forstep(n=1,nm,2,
if(issquarefree(n),
  p=polcyclo(n);o=poldegree(p);
  for(k=0,o,a=abs(polcoeff(p,k));
    if(a>m,m=a;print([m,n,factor(n)])))))
```

Die erste Zeile definiert die Schranke `nm` für m. Wir beginnen bei $m = 0$. Die `forstep`-Schleife geht durch alle ungeraden Zahlen n von 1 bis `nm`. In dieser Schleife ist `p` das zyklotomische Polynom $\Phi_n(X)$, `o` ist der Grad von `p` und die `for`-Schleife testet für alle Koeffizienten von `p`, ob der Absolutbetrag `a` des Koeffizienten größer als m ist. In diesem Fall wird `m`, `n` und eine Faktorisierung von `n` ausgegeben. Dieses Programm produziert nach einigem Warten die Ausgabe.

```
[1, 1, matrix(0,2)]
[2, 105, [3, 1; 5, 1; 7, 1]]
[3, 385, [5, 1; 7, 1; 11, 1]]
[4, 1365, [3, 1; 5, 1; 7, 1; 13, 1]]
[5, 1785, [3, 1; 5, 1; 7, 1; 17, 1]]
[6, 2805, [3, 1; 5, 1; 11, 1; 17, 1]]
[7, 3135, [3, 1; 5, 1; 11, 1; 19, 1]]
[8, 6545, [5, 1; 7, 1; 11, 1; 17, 1]]
[9, 6545, [5, 1; 7, 1; 11, 1; 17, 1]]
```

Mit normalen Einstellungen kommt man über $m = 11305$ nicht hinaus.

Alternativ produziert das folgende Programm die Sequenz der Grade von zyklotomischen Polynomen mit einem Koeffizienten $> b$.

```
nm=10000;
b=2;
forstep(n=1,nm,2,
if(issquarefree(n),
  p=polcyclo(n);o=poldegree(p);
  m=0;
  for(k=0,o,a=abs(polcoeff(p,k));
    if(a>b,m=1));
  if(m>0,print([o,factor(o),n,factor(n)]))))
```

Aufgabe 2

Bestimmen Sie die Faktorisierung von $4 \cdot 503$ *in* $K = \mathbb{Q}(\theta)$ *mit* $\theta^3 - \theta^2 - 2\theta - 8 = 0$. *Bestimmen Sie die Faktorisierung von* $4 \cdot 503$ *im Zerfällungskörper des Polynoms* $f(X) = X^3 - X^2 - 2X - 8$. *Geben Sie die gefundenen Ideale jeweils in der Form* $(a, b), a, b \in \mathcal{O}_K$ *als auch in Hermite-Normalform an.*

Jedem Aufruf von `nf=bnfinit(f)` sollte auch ein `bnfcertify(nf)` folgen, um zu überprüfen, ob die Ergebnisse auch richtig sind. Dies liegt daran, daß Pari/GP nicht die Minkowski-Schranke, sondern eine verbesserte Schranke zur Berechnung der Klassenzahl benutzt, die von Bach unter Annahme der erweiterten Riemann-Hypothese bewiesen wurde. Ohne Aufruf von `bnfcertify(nf)` sind die Ergebnisse also nur unter Annahme der erweiterten Riemann-Hypothese richtig. Diese Aufrufe wurden im folgenden Programmtext weggelassen.

Die folgende Pari/GP-Sitzung löst den ersten Teil von Aufgabe 8.2:

```
? f=Pol([1,-1,-2,-8]);
? nf=bnfinit(f);
? P2=idealprimedec(nf,2)
%3 = [[2, [1, 1, 0]~, 1, 1, [0, 1, 0]~],
      [2, [2, 1, 1]~, 1, 1, [1, 1, 1]~],
      [2, [3, 0, 1]~, 1, 1, [0, 0, 1]~]]
? idealhnf(nf,P2[1])
%4 = [2 1 0] [0 1 0] [0 0 1]
? idealhnf(nf,P2[2])
%5 = [2 0 0] [0 1 0] [0 0 1]
? idealhnf(nf,P2[3])
%6 = [2 0 1] [0 1 0] [0 0 1]
? nf.zk
%7 = [1, 1/2*x^2 - 1/2*x - 1, x]
? nfbasistoalg(nf,idealtwoelt(nf,P2[1])[2])
%8 = Mod(1/2*x^2 - 1/2*x, x^3 - x^2 - 2*x - 8)
? nfbasistoalg(nf,idealtwoelt(nf,P2[2])[2])
%9 = Mod(1/2*x^2 + 1/2*x + 1, x^3 - x^2 - 2*x - 8)
? nfbasistoalg(nf,idealtwoelt(nf,P2[3])[2])
%10 = Mod(x + 3, x^3 - x^2 - 2*x - 8)
? idealnorm(nf,P2[3])
%11 = 2
? P503=idealprimedec(nf,503)
%12 = [[503, [149, 0, 1]~, 2, 1, [218, 2, -149]~],
```

```
       [503, [204, 0, 1]~, 1, 1, [71, 2, -204]~]]
? idealhnf(nf,P503[1])
%13 =
[503 395 149] [0 1 0] [0 0 1]
? idealhnf(nf,P503[2])
%14 = [503 217 204] [0 1 0] [0 0 1]
? nfbasistoalg(nf,idealtwoelt(nf,P503[1])[2])
%15 = Mod(x + 149, x^3 - x^2 - 2*x - 8)
? nfbasistoalg(nf,idealtwoelt(nf,P503[2])[2])
%16 = Mod(x + 204, x^3 - x^2 - 2*x - 8)
? bnf.clgp
%17 = [1, [], []]
? bnfisprincipal(bnf,P503[1])
%18 = [[]~, [-41, -16, -22]~]
? nfbasistoalg(bnf,bnfisprincipal(bnf,P503[1])[2])
%19 = Mod(-8*x^2 - 14*x - 25, x^3 - x^2 - 2*x - 8)
? nfbasistoalg(bnf,bnfisprincipal(bnf,P503[2])[2])
%20 = Mod(-3*x^2 - 3*x - 5, x^3 - x^2 - 2*x - 8)
? nfbasistoalg(bnf,bnfisprincipal(bnf,P2[1])[2])
%21 = Mod(-3/2*x^2 - 5/2*x - 4, x^3 - x^2 - 2*x - 8)
? nfbasistoalg(bnf,bnfisprincipal(bnf,P2[2])[2])
%22 = Mod(-1/2*x^2 - 1/2*x - 1, x^3 - x^2 - 2*x - 8)
? nfbasistoalg(bnf,bnfisprincipal(bnf,P2[3])[2])
%23 = Mod(-x^2 - 2*x - 3, x^3 - x^2 - 2*x - 8)
```

Die Ausgaben des Programms sind wie folgt zu interpretieren: In Zeile 3 sieht man, daß (2) in $\mathbb{Q}(\theta)$ als Produkt von drei Idealen zerfällt. Die Zeilen 4, 5 und 6 liefern die Hermite-Normalform für die drei Primidealfaktoren. Mit `nf.zk` bekommt man die Ganzheitsbasis $1, \frac{\theta^2-\theta-2}{2}, \theta$. In Zeile 17 sieht man, daß die Klassengruppe trivial ist, daß also alle Ideale Hauptideale sind. In den Zeilen 8-10 bekommt man die Erzeuger der Primidealfaktoren von (2). In den Zeilen 21-23 erhält man zusätzlich die Erzeuger dieser Hauptideale. Das Ergebnis ist

$$\mathfrak{p}_{2,1} = \left(2, \frac{\theta^2-\theta}{2}\right) = \left(-\frac{3\theta^2+5\theta+8}{2}\right)$$

$$\mathfrak{p}_{2,2} = \left(2, \frac{\theta^2+\theta+2}{2}\right) = \left(-\frac{\theta^2+\theta+2}{2}\right)$$

$$\mathfrak{p}_{2,1} = (2, \theta+3) = \left(-\theta^2-2\theta-3\right).$$

Analog für die Primzahl 503:

$$\mathfrak{p}_{503,1} = (503, \theta+149) = \left(-8\theta^2-14\theta-25\right)$$

$$\mathfrak{p}_{503,2} = (503, \theta+204) = \left(-3\theta^2-3\theta-5\right)$$

Die Faktorisierung ist dann $4 \cdot 503 = \mathfrak{p}_{2,1}^2\mathfrak{p}_{2,2}^2\mathfrak{p}_{2,3}^2\mathfrak{p}_{503,1}^2\mathfrak{p}_{503,2}$.

Den Zerfällungskörper bzw. das Minimalpolynom eines primitiven Elements des Zerfällungskörpers erhält man, indem man `polcompositum`-Aufrufe iteriert. Es ist klar, daß der Zerfällungskörper eines Polynoms vom Grad n höchstens Grad $n!$ hat. In unserem Fall reicht damit eine Anwendung von `polcompositum`.

```
? f=Pol([1,-1,-2,-8])
%1 = x^3 - x^2 - 2*x - 8
? polcompositum(f,f)
%2 = [x^3 + x^2 - 2*x + 8,
   x^6 + 2*x^5 - 31*x^4 + 132*x^3 + 420*x^2 - 2624*x + 24832]
? polredabs(%[2])
%3 = x^6 + 11*x^4 - 32*x^3 + 156*x^2 - 176*x + 256
? nf=bnfinit(%);
? nf.clgp
%5 = [7, [7], [[4, 0, 0, 0, 0, 2; 0, 1, 0, 0, 0, 0;
   0, 0, 4, 2, 0, 2; 0, 0, 0, 1, 0, 0;
   0, 0, 0, 0, 2, 0; 0, 0, 0, 0, 0, 1]]]
? P2=idealprimedec(nf,2)
%6 = [[2, [-1, 0, 0, 0, 0, 1]~, 1, 1, [0, 0, 0, 0, 0, 1]~],
      [2, [-1, 0, 0, 1, 0, 1]~, 1, 1, [0, 0, 0, 1, 0, 1]~],
      [2, [-1, 1, 0, 1, 1, 1]~, 1, 1, [0, 1, 0, 1, 1, 1]~],
      [2, [0, 0, 1, 1, 1, 1]~, 1, 1, [1, 0, 1, 1, 1, 1]~],
      [2, [1, 0, 1, 0, 0, 1]~, 1, 1, [0, 0, 1, 0, 0, 1]~],
      [2, [1, 1, 0, 1, 0, 1]~, 1, 1, [0, 1, 0, 1, 0, 1]~]]
? P503=idealprimedec(nf,503)
%7 = [[503, [-137, 1, 0, 1, 0, 0]~, 2, 1,
            [-70, -95, -140, 83, -133, 50]~],
     [503, [41, 1, 0, 1, 0, 0]~, 2, 1,
           [24, 190, 93, 142, 71, -4]~],
     [503, [96, 1, 0, 1, 0, 0]~, 2, 1,
           [70, 15, -15, -119, -140, 98]~]]
? factor(nf.disc)
%8 = [-1 1] [503 3]
? nf.zk
%9 = [1, 1/24*x^4 + 1/12*x^3 + 11/24*x^2 - 1/4*x + 8/3,
  7/288*x^5 - 1/144*x^4 + 19/96*x^3 - 151/144*x^2 + 101/36*x - 38/9,
  -1/24*x^4 - 1/12*x^3 - 11/24*x^2 + 5/4*x - 8/3,
  -5/288*x^5 - 1/144*x^4 - 3/32*x^3 + 89/144*x^2 - 67/36*x + 10/9,
  1/144*x^5 - 1/72*x^4 + 5/48*x^3 + 5/72*x^2 + 22/9*x - 10/9]
? nfbasistoalg(nf,idealtwoelt(nf,P2[1])[2])
%10 = Mod(1/144*x^5 - 1/72*x^4 + 5/48*x^3 + 5/72*x^2 + 22/9*x - 19/9,
  x^6 + 11*x^4 - 32*x^3 + 156*x^2 - 176*x + 256)
? nfbasistoalg(nf,idealtwoelt(nf,P2[2])[2])
%11 = Mod(1/144*x^5 - 1/18*x^4 + 1/48*x^3 - 7/18*x^2 + 133/36*x - 43/9,
x^6 + 11*x^4 - 32*x^3 + 156*x^2 - 176*x + 256)
? nfbasistoalg(nf,idealtwoelt(nf,P2[3])[2])
%12 = Mod(-1/96*x^5 - 1/48*x^4 + 1/96*x^3 + 11/16*x^2 + 19/12*x - 1,
  x^6 + 11*x^4 - 32*x^3 + 156*x^2 - 176*x + 256)
? nfbasistoalg(nf,idealtwoelt(nf,P2[4])[2])
%13 = Mod(1/72*x^5 - 5/72*x^4 + 1/8*x^3 - 59/72*x^2 + 167/36*x - 62/9,
  x^6 + 11*x^4 - 32*x^3 + 156*x^2 - 176*x + 256)
? nfbasistoalg(nf,idealtwoelt(nf,P2[5])[2])
%14 = Mod(1/32*x^5 - 1/48*x^4 + 29/96*x^3 - 47/48*x^2 + 21/4*x - 13/3,
  x^6 + 11*x^4 - 32*x^3 + 156*x^2 - 176*x + 256)
? nfbasistoalg(nf,idealtwoelt(nf,P2[6])[2])
```

```
%15 = Mod(1/144*x^5 - 1/72*x^4 + 5/48*x^3 + 5/72*x^2 + 31/9*x - 1/9,
  x^6 + 11*x^4 - 32*x^3 + 156*x^2 - 176*x + 256)
? nfbasistoalg(nf,idealtwoelt(nf,P503[1])[2])
%16 = Mod(x - 137, x^6 + 11*x^4 - 32*x^3 + 156*x^2 - 176*x + 256)
? nfbasistoalg(nf,idealtwoelt(nf,P503[2])[2])
%17 = Mod(x + 41, x^6 + 11*x^4 - 32*x^3 + 156*x^2 - 176*x + 256)
? nfbasistoalg(nf,idealtwoelt(nf,P503[3])[2])
%18 = Mod(x + 96, x^6 + 11*x^4 - 32*x^3 + 156*x^2 - 176*x + 256)
? bnfisprincipal(nf,P2[1])
%19 = [[6]~, [-43/4096, -19/2048, -25/1024, 69/4096, 85/4096, 1/1024]~]
? bnfisprincipal(nf,P2[2])
%20 = [[1]~, [1/4, 0, -1, 3/4, 3/4, 1/2]~]
? bnfisprincipal(nf,P2[3])
%21 = [[1]~, [9/4, 1/2, 0, -3/4, -3/4, 0]~]
? bnfisprincipal(nf,P2[4])
%22 = [[6]~, [-57/2048, -25/512, -111/4096, -3/128, 7/1024, 23/4096]~]
? bnfisprincipal(nf,P2[5])
%23 = [[1]~, [7/4, 2, 5/4, 7/4, 7/4, -3/4]~]
? bnfisprincipal(nf,P2[6])
%24 = [[6]~, [83/4096, -117/2048, -17/1024, -173/4096, -29/4096, 25/1024]~]
? bnfisprincipal(nf,P503[1])
%25 = [[0]~, [-1, -2, -2, -2, 0, 2]~]
? bnfisprincipal(nf,P503[2])
%26 = [[0]~, [1, 2, 2, 0, 0, 2]~]
? bnfisprincipal(nf,P503[3])
%27 = [[0]~, [-1, 2, -2, 2, 2, -2]~]
? nfbasistoalg(nf,bnfisprincipal(nf,P503[1])[2])
%28 = Mod(-5/144*x^5 - 1/72*x^4 - 3/16*x^3 + 161/72*x^2 - 49/18*x + 47/9,
  x^6 + 11*x^4 - 32*x^3 + 156*x^2 - 176*x + 256)
? nfbasistoalg(nf,bnfisprincipal(nf,P503[2])[2])
%29 = Mod(1/16*x^5 + 1/24*x^4 + 37/48*x^3 - 25/24*x^2 + 10*x - 13/3,
  x^6 + 11*x^4 - 32*x^3 + 156*x^2 - 176*x + 256)
? nfbasistoalg(nf,bnfisprincipal(nf,P503[3])[2])
%30 = Mod(-7/72*x^5 + 1/36*x^4 - 19/24*x^3 + 115/36*x^2 - 110/9*x + 107/9,
  x^6 + 11*x^4 - 32*x^3 + 156*x^2 - 176*x + 256)
```

Der Ganzheitsring des Zerfällungskörpers ist kein Hauptidealring, die Klassengruppe ist $\mathbb{Z}/7\mathbb{Z}$. Die Primidealfaktoren von 2 sind keine Hauptideale. Die Primidealfaktoren von 503 sind Hauptideale, und wir haben auch ihre Erzeuger bestimmt.

Aufgabe 3

Geben Sie eine Ganzheitsbasis für den Zerfällungskörper von $f(X) = X^3 - X^2 - 2X - 8$ *an. Geben Sie für alle Zwischenkörper Erzeuger der Klassengruppe an.*

Die Ganzheitsbasis haben wir schon in Aufgabe 2 mit bestimmt:

$$1, \frac{x^4 + 2x^3 + 11x^2 - 6x + 48}{24}, \frac{7x^5 - 2x^4 + 57x^3 - 302x^2 + 808x - 1216}{288},$$

$$\frac{-x^4-2x^3-11x^2+30x-48}{24}, \frac{-5x^5-2x^4-27x^3+178x^2-536x+320}{288},$$
$$\frac{x^5-2x^4+15x^3+10x^2+352x-160}{144}$$

wobei x eine Wurzel von $X^6+11X^4-32X^3+156X^2-176X+256=0$ ist.

```
? f=Pol([1,-1,-2,-8])
%1 = x^3 - x^2 - 2*x - 8
? polcompositum(f,f)
%2 = [x^3 + x^2 - 2*x + 8,
  x^6 + 2*x^5 - 31*x^4 + 132*x^3 + 420*x^2 - 2624*x + 24832]
? polredabs(%[2])
%3 = x^6 + 11*x^4 - 32*x^3 + 156*x^2 - 176*x + 256
? nf=bnfinit(%);
? nf.clgp
%5 = [7, [7], [[4, 0, 0, 0, 0, 2; 0, 1, 0, 0, 0, 0;
   0, 0, 4, 2, 0, 2; 0, 0, 0, 1, 0, 0;
   0, 0, 0, 0, 2, 0; 0, 0, 0, 0, 0, 1]]]
? nfsubfields(nf)
%6 = [[x, 0],
[x^2 + 22*x + 624, 1/8*x^5 + 11/8*x^3 - 2*x^2 + 39/2*x - 22],
[x^3 + 29*x - 34, -5/288*x^5 + 5/144*x^4 - 1/96*x^3 +
  155/144*x^2 - 10/9*x + 34/9],
[x^3 - 13*x + 20, -1/144*x^5 + 1/72*x^4 - 5/48*x^3 +
  31/72*x^2 - 17/18*x + 28/9],
[x^3 + 17*x - 82, 7/288*x^5 - 7/144*x^4 + 11/96*x^3 -
  217/144*x^2 + 91/18*x - 62/9],
[x^6 + 11*x^4 - 32*x^3 + 156*x^2 - 176*x + 256, x]]
```

Die Ausgabe von `nfsubfields` liefert einen Vektor. Die Komponenten sind `[g,h]`, wobei `g` die absolute Gleichung des Zwischenkörpers ist und `h` eine Wurzel des Polynoms in x ausdrückt. Die interessanten Zwischenkörper werden also durch die Polynome $X^2+22X+624$, $X^3+29X-34$, $X^3-13X+20$ und $X^3+17X-82$ gegeben.

Der quadratische Zwischenkörper hat Klassenzahl 21, die kubischen Zwischenkörper haben Klassenzahl 1. Die Klassengruppe des quadratischen Zahlkörpers ist zyklisch, und der Erzeuger ist

$$\left(3, \frac{\alpha+10}{2}\right), \alpha^2+22\alpha+524=0$$

Dies erhält man mit

```
? nfbasistoalg(nf,idealtwoelt(nf,nf.clgp.gen[1])[2])
%5 = Mod(1/2*x + 5, x^2 + 22*x + 624)
```

Analog erhält man die Erzeuger der Klassengruppe des Zerfällungskörpers von X^3-X^2-2X-8:

```
? idealtwoelt(nf,nf.clgp.gen[1])
%6 = [4, [-2, -1, -2, 0, 0, -1]~]
```

```
? nfbasistoalg(nf,idealtwoelt(nf,nf.clgp.gen[1])[2])
%7 = Mod(-1/18*x^5 - 1/72*x^4 - 7/12*x^3 + 113/72*x^2 - 281/36*x + 44/9,
x^6 + 11*x^4 - 32*x^3 + 156*x^2 - 176*x + 256)
```

Die Klassengruppe wird also vom Ideal

$$\left(4, \frac{-4x^5 - x^4 - 42x^3 + 113x^2 - 562x + 352}{72}\right)$$

erzeugt, wobei x eine Wurzel von $X^6 + 11X^4 - 32X^3 + 156X^2 - 176X + 256 = 0$ ist

Aufgabe 4

Für welche $n \leq 100$ hat die Gleichung $x^2 - 13y^2 = n$ eine Lösung? Für welche $n \leq 100$ hat die Gleichung $x^2 + 13y^2 = n$ eine Lösung? Worin besteht der Unterschied?

```
? f=Pol([1,0,-13]);
? nf=bnfinit(f);
? for(i=1,100,a=bnfisintnorm(nf,i);if(a!=[],print([i, a])))
[1, [1]]
[3, [x + 4, 1/2*x + 5/2]]
[4, [2]]
[9, [-1/2*x - 7/2, 3, 5/2*x + 19/2]]
[12, [2*x + 8, x + 5]]
[13, [3/2*x + 13/2]]
[16, [4]]
[17, [1/2*x - 9/2, 1/2*x + 9/2]]
[23, [x + 6, -7/2*x - 27/2]]
[25, [5]]
[27, [1/2*x - 11/2, 3/2*x - 15/2, 3/2*x + 15/2, 1/2*x + 11/2]]
[29, [5/2*x + 21/2, -2*x - 9]]
[36, [-x - 7, 6, 5*x + 19]]
[39, [1/2*x + 13/2, -1/2*x + 13/2]]
[43, [3/2*x + 17/2, -9/2*x - 35/2]]
[48, [4*x + 16, 2*x + 10]]
[49, [7]]
[51, [-5/2*x - 23/2, 13/2*x + 49/2, -x - 8, 7/2*x + 29/2]]
[52, [3*x + 13]]
[53, [1/2*x + 15/2, 1/2*x - 15/2]]
[61, [-6*x - 23, -3/2*x - 19/2]]
[64, [8]]
[68, [x - 9, x + 9]]
[69, [-1/2*x + 17/2, -2*x - 11, -2*x + 11, -1/2*x - 17/2]]
[75, [5*x + 20, 5/2*x + 25/2]]
[79, [-3*x - 14, 9/2*x + 37/2]]
[81, [-4*x + 17, -3/2*x - 21/2, -9, 15/2*x + 57/2, 4*x + 17]]
[87, [x + 10, -1/2*x - 19/2, -1/2*x + 19/2, x - 10]]
[92, [2*x + 12, -7*x - 27]]
[100, [10]]
```

Die ganzzahligen Lösungen sind allerdings nur diejenigen, die auch ganze Koeffizienten haben.

Das selbe funktioniert auch für $x^2 + 13$.

```
? for(i=1,100,a=bnfisintnorm(nf,i);if(a!=[],print([i, a])))
[1, [1]]
[4, [2]]
[9, [3]]
[13, [x]]
[14, [x + 1, x - 1]]
[16, [4]]
[17, [x + 2, x - 2]]
[22, [x + 3, x - 3]]
[25, [5]]
[29, [x + 4, x - 4]]
[36, [6]]
[38, [x + 5, x - 5]]
[49, [x - 6, -7, x + 6]]
[52, [2*x]]
[53, [-2*x + 1, 2*x + 1]]
[56, [2*x + 2, 2*x - 2]]
[61, [-2*x + 3, 2*x + 3]]
[62, [x + 7, x - 7]]
[64, [8]]
[68, [2*x + 4, 2*x - 4]]
[77, [2*x - 5, -x - 8, x - 8, -2*x - 5]]
[81, [9]]
[88, [2*x + 6, 2*x - 6]]
[94, [x + 9, x - 9]]
[100, [10]]
```

Hier können wegen $-13 \equiv 3 \mod 4$ nur ganzzahlige Koeffizienten auftreten.

Man kann alternativ auch die folgende Methode probieren. Der Unterschied liegt in der Klassengruppe. Es reicht nicht, daß p zerlegt ist, für die Existenz eines Elements mit gegebener Norm müssen die entsprechenden Idealfaktoren auch Hauptideale sein, damit ein Element mit der richtigen Norm existiert. Zum Beispiel ist (11) in $\mathbb{Q}(\sqrt{-13})$ zerlegt, aber die Faktoren sind keine Hauptideale:

```
? idealprimedec(nf,11)
%12 = [[11, [-3, 1]~, 1, 1, [3, 1]~], [11, [3, 1]~, 1, 1, [-3, 1]~]]
? bnfisprincipal(nf,%[1])
%13 = [[1]~, [-3/2, 1/2]~]
```

Literaturverzeichnis

[Pari/GP] Bill Alombert, Christian Batut, Karim Belabas, Dominique Bernardi, Henri Cohen, Francisco Diaz y Diaz, Yves Eichenlaub, Xavier Gourdon, Louis Granboulan, Bruno Haible, Guillaume Hanrot, Pascal Letard, Gerhard Niklasch, Michel Olivier, Thomas Papanikolaou, Xavier Roblot, Denis Simon, Emmanuel Tollis, Ilya Zakharevitch, and the PARI group, PARI/GP, version `2.3.5`, specialized computer algebra system, Bordeaux, 2010, `http://pari.math.u-bordeaux.fr/`.

Lehrbücher

[AM69] M.F. Atiyah und I.G. Macdonald. Introduction to commutative algebra. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1969.

[Coh93] H. Cohen. A course in computational algebraic number theory. Graduate Texts in Mathematics, 138. Springer-Verlag, Berlin, 1993.

[Die85] J.A. Dieudonné (Hrsg.). Abrégé d'histoire des mathématiques 1700-1900. Band 1: Algébre, analyse classique, théorie des nombres. Herrmann, Paris, 1978.

[HilZB] D. Hilbert. The theory of algebraic number fields. Translated from the German and with a preface by Iain T. Adamson. With an introduction by Franz Lemmermeyer and Norbert Schappacher. Springer-Verlag, Berlin, 1998.

[Neu92] J. Neukirch. Algebraische Zahlentheorie. Springer-Verlag, 1992.

[Poh93] M. Pohst. Computational algebraic number theory. DMV Seminar, 21. Birkhuser Verlag, Basel, 1993.

[PZ89] M. Pohst und H. Zassenhaus. Algorithmic algebraic number theory. Encyclopedia of Mathematics and its Applications, 30. Cambridge University Press, Cambridge, 1989.

[Rib01] P. Ribenboim. Classical theory of algebraic numbers. Universitext. Springer-Verlag, New York, 2001.

[Sam70] P. Samuel. Algebraic theory of numbers. Translated from the French by Allan J. Silberger. Houghton Mifflin Co., 1970.

[Ser73] J.-P. Serre. A course in arithmetic. Translated from the French. Graduate Texts in Mathematics 7. Springer-Verlag, 1973.

[Was97] L.C. Washington. Introduction to cyclotomic fields. Second edition. Graduate Texts in Mathematics, 83. Springer-Verlag, New York, 1997.

[Wei67] A. Weil. Basic number theory. Die Grundlehren der mathematischen Wissenschaften, Band 144. Springer-Verlag New York, 1967.