

Protokoll zur Vorlesung Algebraische Zahlentheorie WS 25/26

W. Bley

7. Januar 2026

1 Ganzheitsringe und Diskriminanten

1.1 Motivation und grundlegende Definitionen

Für eine ungerade Primzahl p gilt:

a) Es gibt genau dann Zahlen $x, y \in \mathbb{Z}$ mit $x^2 + y^2 = p$, wenn $p \equiv 1 \pmod{4}$.

b) Es gibt genau dann Zahlen $x, y \in \mathbb{Z}$ mit $x^2 - 6y^2 = p$, wenn $p \equiv \pm 1 \pmod{8}$.

Die Diskussion der Beweise dieser beiden Resultate hat uns auf folgende Definitionen geführt.

Definition 1.1.1 Eine endliche Körpererweiterung von $\mathbb{Q}$ heißt algebraischer Zahlkörper oder kurz Zahlkörper.

Definition 1.1.2 Sei K ein Zahlkörper. Dann heißt

$$\mathcal{O}_K := \{\alpha \in K \mid \exists f \in \mathbb{Z}[X] \text{ normiert, so dass } f(\alpha) = 0\}$$

Ring der ganzen Zahlen von K .

Example 1.1.3 Sei $d \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei. Sei $K = \mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper. Dann gilt:

$$\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\omega \text{ mit } \omega = \begin{cases} \sqrt{d}, & \text{falls } d \equiv 2, 3 \pmod{4}, \\ \frac{1+\sqrt{d}}{2}, & \text{falls } d \equiv 1 \pmod{4}. \end{cases}$$

Man zeigt relativ leicht:

a) $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

b) $\mathbb{Z}[\sqrt{2}]^\times = \{\pm(1 + \sqrt{2})^k \mid k \in \mathbb{Z}\}$.

Im Allgemeinen gibt der Dirichletsche Einheitensatz Auskunft über die Struktur der Einheitsgruppe $\mathcal{O}_K^\times$.

Satz 1.1.4 (Dirichletscher Einheitensatz) Sei K ein Zahlkörper. Dann ist $\mathcal{O}_K^\times$ eine endlich erzeugte abelsche Gruppe. Insbesondere also $\mathcal{O}_K^\times \simeq (\mathcal{O}_K^\times)_{tors} \times \mathbb{Z}^r$.

Zusatz: r nennt man den Einheitenrang und es gilt: $r = s + t - 1$, wobei

$$\begin{aligned} s &= \text{Anzahl der reellen Einbettungen von } K \text{ in } \mathbb{C}, \\ t &= \text{halbe Anzahl der komplexen Einbettungen von } K \text{ in } \mathbb{C}. \end{aligned}$$

Bei der Diskussion der Gleichung $p = x^2 + 6y^2$ sind wir auf das Phänomen gestoßen, dass Ganzheitsringe im allgemeinen keine Hauptidealringe sind. Wir werden im Rahmen der Vorlesung die sogenannte Idealklassengruppe

$$\text{cl}_K := \text{Gruppe der gebrochenen Ideale / Untergruppe der Hauptideale}$$

studieren und beweisen, dass dies eine endliche Gruppe ist. Es gilt:

$$\text{cl}_K = 1 \iff \mathcal{O}_K \text{ ist ein Hauptidealring.}$$

Ein weiteres Thema des ersten Teils der Vorlesung werden Zerlegungsgesetze sein. Ganzheitsringe in Zahlkörpern sind Dedekindringe, und in Dedekindringen gilt der Satz von der eindeutigen Primidealzerlegung. Falls nun L/K eine Erweiterung von Zahlkörpern ist, so werden wir für ein Primideal $\mathfrak{p}$ von $\mathcal{O}_K$ die Primidealzerlegung von $\mathfrak{p}\mathcal{O}_L$ studieren.

Hier ein erstes Beispiel:

Sei $K = \mathbb{Q}(\sqrt{d})$ mit d wie oben ein quadratischer Zahlkörper und $p \neq 2$ eine Primzahl. Dann gilt:

$$p\mathcal{O}_K = \begin{cases} \mathfrak{p}\bar{\mathfrak{p}}, \mathfrak{p} \neq \bar{\mathfrak{p}}, & \text{falls } \left(\frac{d}{p}\right) = 1, p \nmid d, \\ \mathfrak{p}, & \text{falls } \left(\frac{d}{p}\right) = -1, p \nmid d, \\ \mathfrak{p}^2, & \text{falls } p \mid d. \end{cases}$$

Hierbei bezeichnet $\left(\frac{a}{p}\right)$ das Legendresymbol.

Satz 1.1.5 (Quadratisches Reziprozitätsgesetz) a) Seien $p \neq q$ zwei ungerade Primzahlen. Dann gilt:

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

mit

$$\varepsilon = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} = \begin{cases} +1, & \text{falls } p \equiv 1 \pmod{4} \text{ oder } q \equiv 1 \pmod{4}, \\ -1, & \text{falls } p \equiv 3 \pmod{4} \text{ und } q \equiv 3 \pmod{4}, \end{cases}$$

(1.Ergänzungssatz und 2.Ergänzungssatz) Sei $p \neq 2$ eine Primzahl. Dann gilt:

$$\begin{aligned} \text{b)} \quad \left(\frac{-1}{p}\right) &= (-1)^{(p-1)/2} = \begin{cases} +1, & \text{falls } p \equiv 1 \pmod{4}, \\ -1, & \text{falls } p \equiv 3 \pmod{4}. \end{cases} \\ \text{c)} \quad \left(\frac{2}{p}\right) &= (-1)^{(p^2-1)/8} = \begin{cases} +1, & \text{falls } p \equiv \pm 1 \pmod{8}, \\ -1, & \text{falls } p \equiv \pm 3 \pmod{8}. \end{cases} \end{aligned}$$

Mit den Methoden, die wir im Laufe der Vorlesung entwickeln, werden wir in der Lage sein, folgendes Theorem zu beweisen.

Satz 1.1.6 Sei $p \neq 2$ eine Primzahl und $d \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei. Dann gibt es genau dann $x, y \in \mathbb{Z}$ mit $p = x^2 - dy^2$, wenn $\left(\frac{d}{p}\right) = +1$ und $\mathfrak{p}$ ein Hauptideal ist. Für $d > 0$ gibt es in diesem Fall unendlich viele Lösungen, für $d < 0$ nur endlich viele.

1.2 Ganze Zahlen

Konvention: Alle unsere Ringe sind, wenn nicht ausdrücklich anders gesagt, stets kommutativ und haben eine 1.

Definition 1.2.1 Sei $A \subseteq B$ eine Ringerweiterung. Ein Element $b \in B$ heißt ganz über A , wenn b Nullstelle eines normierten Polynoms $f \in A[X]$ ist. Der Ring B heißt ganz über A , falls alle $b \in B$ ganz über A sind.

Satz 1.2.2 Sei $A \subseteq B$ eine Ringerweiterung und seien $b_1, \dots, b_n \in B$. Dann gilt:

$$b_1, \dots, b_n \text{ ganz über } A \iff A[b_1, \dots, b_n] \text{ ist endlich erzeugter } A\text{-Modul.}$$

Insbesondere sind also Summen und Produkte von ganzen Elementen wieder ganz.

Folgerung 1.2.3 Sei $K/\mathbb{Q}$ ein Zahlkörper. Dann ist $\mathcal{O}_K$ ein Ring.

Ganzheit ist gewissermaßen transitiv:

Satz 1.2.4 Seien $A \subseteq B \subseteq C$ Ringerweiterungen. Sei B ganz über A und $c \in C$ ganz über B . Dann ist c ganz über A .

Definition 1.2.5 Sei $A \subseteq B$ eine Ringerweiterung.

a) Der Ring

$$\mathcal{O}_{A,B} := \{b \in B \mid b \text{ ist ganz über } A\}$$

heißt ganzer Abschluss von A in B .

b) Falls $\mathcal{O}_{A,B} = A$ gilt, so heißt A ganz abgeschlossen in B .

Als Beispiel haben wir eingesehen, dass faktorielle Ringe ganz abgeschlossen in ihrem Quotientenkörper sind.

Wir betrachten nun die folgende Situation: A sei ein nullteilerfreier Ring, der ganz abgeschlossen in seinem Quotientenkörper K ist. L/K sei eine endliche separable Körpererweiterung und B der ganze Abschluss von A in L , also $B = \mathcal{O}_{A,L}$.

Lemma 1.2.6 In dieser Situation gilt: $L = \text{Quot}(B)$. Genauer gilt sogar, dass jedes $\beta \in L$ in der Form

$$\beta = \frac{b}{a} \text{ mit } b \in B \text{ und } a \in A$$

geschrieben werden kann.

Lemma 1.2.7 In obiger Situation gilt für $\beta \in L$:

$$\beta \in B \iff \text{Mipo}_{K,\beta} \in A[X].$$

Remark 1.2.8 Für den Beweis von Lemma 1.2.6 braucht man die Voraussetzung “ A ganz abgeschlossen” noch nicht.

Sei nun L/K eine endliche Körpererweiterung. Sei $\alpha \in L$ und

$$T_\alpha: L \longrightarrow L, \quad \beta \mapsto \alpha\beta$$

die lineare Abbildung Multiplikation mit α .

Definition 1.2.9 a) $\text{Tr}_{L/K}(\alpha) := \text{Spur}(T_\alpha)$ heißt (körpertheoretische) Spur von α .

b) $N_{L/K}(\alpha) := \det(T_\alpha)$ heißt Norm von α .

Aus der linearen Algebra ist der folgende Zusammenhang zwischen charakteristischem Polynom und Norm und Spur bekannt.

Lemma 1.2.10 Sei L/K eine endliche Körpererweiterung und $\alpha \in L$.

a) Sei $\chi_\alpha(t) = \det(tE - T_\alpha) \in K[t]$ das charakteristische Polynom von T_α . Sei explizit

$$\chi_\alpha(t) = t^n - a_1 t^{n-1} + \dots + (-1)^n a_n.$$

Dann gilt: $\text{Tr}_{L/K}(\alpha) = a_1, N_{L/K}(\alpha) = a_n$.

b) $\text{Tr}_{L/K}$ ist K -linear.

c) $N_{L/K}$ ist multiplikativ.

Satz 1.2.11 Sei L/K eine endliche separable Körpererweiterung. Sei $\bar{K}$ ein algebraischer Abschluss von K und $G = G(L/K, \bar{K}/K)$ die Menge der K -Automorphismen von L . Dann gilt:

- a) $\chi_\alpha(t) = \prod_{\sigma \in G} (t - \sigma(\alpha))$.
- b) $\text{Tr}_{L/K}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha)$.
- c) $N_{L/K}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha)$.

Folgerung 1.2.12 Sei $K \subseteq L \subseteq M$ ein Turm von endlichen separablen Körpererweiterungen. Dann gilt:

- a) $\text{Tr}_{M/K}(\alpha) = \text{Tr}_{L/K}(\text{Tr}_{M/L}(\alpha))$.
- b) $N_{M/K}(\alpha) = N_{L/K}(N_{M/L}(\alpha))$.

Definition 1.2.13 Sei L/K eine endliche separable Körpererweiterung vom Grad n . Seien $\alpha_1, \dots, \alpha_n$ Elemente aus L . Ferner sei $G(L/K, \bar{K}/K) = \{\sigma_1, \dots, \sigma_n\}$. Dann heißt

$$d(\alpha_1, \dots, \alpha_n) := \left(\det (\sigma_i(\alpha_j))_{1 \leq i, j \leq n} \right)^2$$

Diskriminante von $\alpha_1, \dots, \alpha_n$.

Lemma 1.2.14 Es gilt:

a)

$$d(\alpha_1, \dots, \alpha_n) = \det (\text{Tr}_{L/K}(\alpha_i \alpha_j))_{1 \leq i, j \leq n}.$$

b) Für $\theta \in L$ gilt:

$$d(1, \theta, \dots, \theta^{n-1}) = \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)^2,$$

wobei $\theta_i := \sigma_i(\theta)$.

Satz 1.2.15 Sei L/K eine endliche separable Körpererweiterung und seien $\alpha_1, \dots, \alpha_n \in L$. Dann gilt:

- a) $\alpha_1, \dots, \alpha_n$ ist K -Basis von $L \iff d(\alpha_1, \dots, \alpha_n) \neq 0$.
- b) Die Abbildung $L \times L \longrightarrow K, (x, y) \mapsto \text{Tr}_{L/K}(xy)$, definiert eine nicht-ausgeartete Bilinearform auf L .

Wir betrachten nun wieder die Situation wie oben: A sei ein nullteilerfreier Ring, der ganz abgeschlossen in seinem Quotientenkörper K ist. L/K sei eine endliche separable Körpererweiterung und B der ganze Abschluss von A in L , also $B = \mathcal{O}_{A,L}$.

Lemma 1.2.16 In dieser Situation gilt:

- a) Für alle $b \in B$ gilt: $\text{Tr}_{L/K}(b), N_{L/K}(b) \in A$.
- b) Für $b \in B$ gilt:

$$b \in B^\times \iff N_{L/K}(b) \in A^\times.$$

Lemma 1.2.17 In obiger Situation gilt für jede in B gelegene K -Basis $\alpha_1, \dots, \alpha_n$ von L mit $d := d(\alpha_1, \dots, \alpha_n)$

$$dB \subseteq A\alpha_1 \oplus \dots \oplus A\alpha_n.$$

Aus der Theorie der Moduln über Hauptidealringen erhalten wir das nächste Resultat.

Satz 1.2.18 In obiger Situation sei A ein Hauptidealring. Dann ist jeder endlich-erzeugte B -Untermodul $M \neq 0$ von L ein freier A -Modul vom Rang $n = [L : K]$. Insbesondere gibt es $\alpha_1, \dots, \alpha_n \in B$, so dass

$$B = A\alpha_1 \oplus \dots \oplus A\alpha_n.$$

Definition 1.2.19 Eine A -Basis von B wie im Satz nennt man Ganzheitsbasis von L/K (bezüglich des Grundrings A). Speziell sprechen wir von einer Ganzheitsbasis des Zahlkörpers L , falls $A = \mathbb{Z}$ und $B = \mathcal{O}_L$.

Definition 1.2.20 Sei $L/\mathbb{Q}$ ein Zahlkörper und $\alpha_1, \dots, \alpha_n \in \mathcal{O}_L$ eine Ganzheitsbasis. Dann nennt man

$$d_L := d(\alpha_1, \dots, \alpha_n)$$

die Diskriminante von L/K .

Man beachte, dass diese Bildung unabhängig von der Wahl der Ganzheitsbasis ist.

Definition 1.2.21 Sei $L/\mathbb{Q}$ ein Zahlkörper und $M \neq 0$ ein endlich erzeugter $\mathcal{O}_L$ -Teilmodul von L . Sei $\alpha_1, \dots, \alpha_n$ eine $\mathbb{Z}$ -Basis von M . Dann nennt man

$$d(M) = d_{L/K}(M) := d(\alpha_1, \dots, \alpha_n)$$

die Diskriminante von M .

Es gilt dann:

Satz 1.2.22 Seien $L/\mathbb{Q}$ ein Zahlkörper und $0 \neq M \subseteq M'$ zwei endlich erzeugte $\mathcal{O}_L$ -Teilmoduln von L . Dann ist $[M' : M] < \infty$ und es gilt

$$d(M) = [M' : M]^2 d(M').$$

Folgerung 1.2.23 Sei $\alpha_1, \dots, \alpha_n \in \mathcal{O}_L$ eine $\mathbb{Q}$ -Basis von L und $d(\alpha_1, \dots, \alpha_n)$ sei quadratfrei. Dann ist $\alpha_1, \dots, \alpha_n$ eine Ganzheitsbasis.

1.3 Ideale

Wir erinnern zunächst an die Definition und grundlegende Eigenschaften noetherscher Ringe und Moduln. Im Folgenden ist R stets ein kommutativer Ring mit Eins.

Definition 1.3.1 Ein R -Modul M heißt noethersch, falls alle seine R -Teilmoduln endlich erzeugt sind.

Insbesondere können wir R als R -Modul betrachten. R ist genau dann noethersch, wenn jedes Ideal in R endlich erzeugt ist.

Für einen noetherschen Ring R und einen R -Modul M gilt:

$$M \text{ ist noethersch} \iff M \text{ ist endlich erzeugt.}$$

Satz 1.3.2 Sei M ein R -Modul. Dann sind folgende Aussagen äquivalent:

- a) M ist noethersch.
- b) Jede aufsteigende Kette

$$M_1 \subseteq M_2 \subseteq \dots$$

von R -Teilmoduln von M wird stationär.

- c) Jede nicht-leere Familie von R -Teilmoduln von M enthält maximale Elemente (bez. der Inklusion).

Wir kommen nun zu einem ersten zentralen Resultat der Vorlesung.

Satz 1.3.3 Sei K ein Zahlkörper. Dann ist $\mathcal{O}_K$ noethersch, ganz abgeschlossen und jedes Primideal $\mathfrak{p} \neq 0$ ist ein maximales Ideal.

Definition 1.3.4 Ein nullteilerfreier Ring R heißt Dedekindring, falls folgende Eigenschaften erfüllt sind:

- a) R ist noethersch.
- b) R ist ganz abgeschlossen.
- c) Jedes Primideal $\mathfrak{p} \neq 0$ ist ein maximales Ideal.

Nach dieser Definition ist auch jeder Körper ein Dedekindring. Wir interessieren uns aber vor allem für Dedekindringe, die keine Körper sind. Satz 1.3.3 besagt also, dass der Ring $\mathcal{O}_L$ der ganzen Zahlen in einem Zahlkörper L stets ein Dedekindring ist.

Im Weiteren sei $\mathcal{O}$ stets ein Dedekindring mit Quotientenkörper K .

Satz 1.3.5 Sei $\mathfrak{a}$ ein nicht-triviales Ideal, d.h. $\mathfrak{a} \neq (0), \mathcal{O}$. Dann gibt es eine bis auf Reihenfolge eindeutige Darstellung

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r \quad (1)$$

von $\mathfrak{a}$ als Produkt von Primidealen $\mathfrak{p}_i$. Schreibt man (1) in der Form

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}$$

mit paarweise verschiedenen Primidealen $\mathfrak{p}_1, \dots, \mathfrak{p}_s$, $s \leq r$, $e_i \in \mathbb{Z}_{>0}$, so gilt auch

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cap \dots \cap \mathfrak{p}_s^{e_s}.$$

Mit der Notation aus dem Satz erhalten wir aus dem Chinesischen Restsatz

$$\mathcal{O}/\mathfrak{a} \simeq \mathcal{O}/\mathfrak{p}_1^{e_1} \times \dots \times \mathcal{O}/\mathfrak{p}_s^{e_s}.$$

Wie üblich in der Ringtheorie werden wir folgende Konventionen, Sprech- und Schreibweisen übernehmen. Seien dazu $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}$ Ideale.

- a) $\mathfrak{a} \mid \mathfrak{b} \iff \mathfrak{b} \subseteq \mathfrak{a}$.
- b) $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$ nennen wir den ggT von $\mathfrak{a}$ und $\mathfrak{b}$. Fall $\mathfrak{a} + \mathfrak{b} = \mathcal{O}$ gilt, so sagen wir, dass $\mathfrak{a}$ und $\mathfrak{b}$ teilerfremd sind.
- c) $\mathfrak{a} \cap \mathfrak{b}$ nennen wir auch das kgV von $\mathfrak{a}$ und $\mathfrak{b}$.

Lemma 1.3.6 Sei $\mathfrak{a}$ ein nicht-triviales Ideal von $\mathcal{O}$ und $\mathfrak{p} \neq 0$ ein Primideal. Dann gilt:

$$\mathfrak{a} = \mathfrak{p}^n \mathfrak{b} \text{ mit } n \in \mathbb{Z}_{\geq 0} \text{ and } (\mathfrak{b}, \mathfrak{p}) = \mathcal{O} \iff \mathfrak{a} \subseteq \mathfrak{p}^n \text{ und } \mathfrak{a} \not\subseteq \mathfrak{p}^{n+1}.$$

Im Weiteren wollen wir den Idealbegriff erweitern, so dass die sogenannten gebrochenen Ideale eine Gruppe bezüglich der Modulmultiplikation bilden.

Definition 1.3.7 Ein gebrochenes Ideal in K ist ein endlich erzeugter $\mathcal{O}$ -Teilmodul $\mathfrak{a} \neq 0$ von K .

Lemma 1.3.8 Sei $0 \neq \mathfrak{a} \subseteq K$ ein $\mathcal{O}$ -Teilmodul. Dann gilt:

$$\mathfrak{a} \text{ ist ein gebrochenes Ideal} \iff \exists c \in \mathcal{O}, c \neq 0 \text{ mit } c\mathfrak{a} \subseteq \mathcal{O}.$$

Satz 1.3.9 Die Gruppe der gebrochenen Ideale bildet eine Gruppe $J_{\mathcal{O}}$ bez. der Multiplikation von Idealen. Das Einselement ist gegeben durch $\mathcal{O}$ und für ein gebrochenes Ideal $\mathfrak{a}$ gilt

$$\mathfrak{a}^{-1} = (\mathcal{O} : \mathfrak{a})$$

mit

$$(\mathcal{O} : \mathfrak{a}) := \{x \in K \mid x\mathfrak{a} \subseteq \mathcal{O}\}.$$

Folgerung 1.3.10 Jedes gebrochene Ideal $\mathfrak{a}$ von K besitzt eine eindeutige Produktdarstellung

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}}, \quad \nu_{\mathfrak{p}} \in \mathbb{Z}, \nu_{\mathfrak{p}} = 0 \text{ für fast alle } \mathfrak{p}.$$

Hierbei durchläuft $\mathfrak{p}$ alle Primideale ungleich 0 von $\mathcal{O}$.

Folgerung 1.3.11 Jedes gebrochene Ideal $\mathfrak{a}$ von K kann man eindeutig in der Form

$$\mathfrak{a} = \mathfrak{b}/\mathfrak{c}$$

mit ganzen, zueinander teilerfremden Ideal $\mathfrak{b}, \mathfrak{c}$ schreiben.

Definition 1.3.12 a) $P_{\mathcal{O}} := \{\alpha \mathcal{O} \mid \alpha \in K^{\times}\}$ heißt Gruppe der (gebrochenen) Hauptideale.

b) $\text{cl}_{\mathcal{O}} := J_{\mathcal{O}}/P_{\mathcal{O}}$ heißt Idealklassengruppe oder kurz Klassengruppe von $\mathcal{O}$.

c) Für $\mathfrak{a} \in J_{\mathcal{O}}$ bezeichne $[\mathfrak{a}] := \mathfrak{a}P_{\mathcal{O}}$ die Klasse von $\mathfrak{a}$.

Ein nächstes Ziel der Vorlesung wird sein, die Endlichkeit von $\text{cl}_K := \text{cl}_{\mathcal{O}_K}$ zu beweisen, falls K ein Zahlkörper ist.

Satz 1.3.13 Sei $\mathcal{O}$ ein Dedekindring mit nur endlich vielen Primidealen. Dann ist $\mathcal{O}$ ein Hauptidealring.

Satz 1.3.14 Sei $0 \neq \mathfrak{m} \subseteq \mathcal{O}$ ein ganzes Ideal. Dann gibt es in jeder Idealklasse $c \in \text{cl}_{\mathcal{O}}$ ganze, zu $\mathfrak{m}$ teilerfremde Ideale. Mit anderen Worten: es gibt ganze Ideal $\mathfrak{a}$ mit $[\mathfrak{a}] = c$ und $(\mathfrak{a}, \mathfrak{m}) = \mathcal{O}$.

Satz 1.3.15 Jedes Ideal eines Dedekindrings $\mathcal{O}$ läßt sich durch zwei Elemente erzeugen. Stärker gilt sogar: Sei $0 \neq \mathfrak{a}$ ein Ideal in $\mathcal{O}$ und $0 \neq \alpha \in \mathfrak{a}$ ein beliebiges Element. Dann gibt es $\beta \in \mathfrak{a}$, abhängig von der Wahl von α , so dass $\mathfrak{a} = (\alpha, \beta)$.

Zum Beweis haben wir folgendes Resultat gezeigt.

Satz 1.3.16 Sei $\mathcal{O}$ ein Dedekindring und $0 \neq \mathfrak{b} \subseteq \mathcal{O}$ ein ganzes Ideal. Dann ist $\mathcal{O}/\mathfrak{b}$ ein HIR.

1.4 Nachtrag zu Ganzheitsbasen und Diskriminanten

Satz 1.4.1 Seien $K/\mathbb{Q}$ und $L/\mathbb{Q}$ zwei Zahlkörper und sei $n := [K : \mathbb{Q}]$, $m := [L : \mathbb{Q}]$. Sei $N := KL$ und es gelte $[N : \mathbb{Q}] = nm$. Sei $d := \gcd(d_K, d_L)$. Dann gilt:

$$(a) \quad \mathcal{O}_N = \mathcal{O}_K \cdot \mathcal{O}_L,$$

$$(b) \quad d_N = d_K^m d_L^n.$$

2 Die Endlichkeit der Klassenzahl

2.1 Gitter und der Minkowskische Gitterpunktsatz

Definition 2.1.1 Sei V ein $\mathbb{R}$ -Vektorraum der Dimension $n < \infty$. Ein Gitter ist eine Untergruppe Γ von V von der Form

$$\Gamma = \mathbb{Z}v_1 \oplus \dots \oplus \mathbb{Z}v_m$$

mit linear unabhängigen Vektoren $v_1, \dots, v_m$ aus V . Die Menge

$$\Phi := \{x_1v_1 + \dots + x_mv_m \mid x_i \in \mathbb{R}, 0 \leq x_i < 1\}$$

heißt Grundmasche von Γ bezüglich der Basis $v_1, \dots, v_m$. Ein Gitter heißt voll, falls $n = m$.

Diese Definition ist anschaulich, aber basisabhängig. Im Folgenden wollen wir Gitter und ihre Eigenschaften durch topologische Eigenschaften beschreiben. Es sei im weiteren V stets ein $\mathbb{R}$ -Vektorraum der Dimension $n < \infty$.

Definition 2.1.2 Eine Untergruppe Γ von V heißt diskret, falls jedes $\gamma \in \Gamma$ eine Umgebung U besitzt, so dass $\Gamma \cap U = \{\gamma\}$.

Man kann zeigen, dass diskrete Untergruppen stets abgeschlossen in V sind.

Lemma 2.1.3 Sei Γ eine Untergruppe von V . Dann ist Γ genau dann diskret, wenn für alle beschränkten Teilmengen $C \subseteq V$ der Durchschnitt $C \cap \Gamma$ endlich ist.

Satz 2.1.4 Eine Untergruppe Γ von V ist genau dann ein Gitter, wenn sie diskret ist.

Lemma 2.1.5 Ein Gitter Γ in V ist genau dann voll, wenn es eine beschränkte Teilmenge $M \subseteq V$ gibt, so dass

$$\bigcup_{\gamma \in \Gamma} (\gamma + M) = V.$$

Sei nun V ein euklidischer Vektorraum der Dimension $n < \infty$ mit Skalarprodukt

$$\langle \cdot, \cdot \rangle: V \times V \longrightarrow \mathbb{R}.$$

Sei $e_1, \dots, e_n$ eine Orthonormalbasis von V . Dann setzt man

$$\text{Vol} \left(\left\{ \sum_{i=1}^n x_i e_i \mid 0 \leq x_i \leq 1 \right\} \right) := 1$$

und erhält hierdurch einen Volumenbegriff auf V . Sei

$$\Phi := \left\{ \sum_{i=1}^n x_i v_i \mid 0 \leq x_i \leq 1 \right\}$$

das von einer Basis $v_1, \dots, v_n$ aufgespannte Parallelepiped. Sei T die Übergangsmatrix, d.h.

$$v_i = \sum_{j=1}^n t_{ji} e_j, \quad i = 1, \dots, n.$$

Lemma 2.1.6 In dieser Situation gilt:

$$\text{Vol}(\Phi) = |\det(T)| = \sqrt{\det(\langle v_i, v_j \rangle)_{1 \leq i, j \leq n}}.$$

Definition 2.1.7 Für ein volles Gitter Γ in V mit Grundmasche Φ setzt man $\text{Vol}(\Gamma) := \text{Vol}(\Phi)$.

Diese Definition ist unabhängig von der Wahl der Grundmasche.

Definition 2.1.8 a) Eine Teilmenge $X \subseteq V$ heißt zentral-symmetrisch, falls für alle $x \in X$ auch $-x \in X$ gilt.

b) Eine Teilmenge $X \subseteq V$ heißt konvex, falls für alle $x, y \in X$ gilt

$$\{\lambda x + (1 - \lambda)y \mid 0 \leq \lambda \leq 1\} \subseteq X.$$

Der folgende Satz, der sogenannte Minkowskische Gitterpunktsatz, ist die Quelle für den Beweis der Endlichkeit der Klassenzahl.

Satz 2.1.9 Sei Γ ein volles Gitter im euklidischen Vektorraum V , $n = \dim_{\mathbb{R}}(V)$. Sei $X \subseteq V$ zentral-symmetrisch, konvex und es gelte

$$\text{Vol}(X) > 2^n \text{Vol}(\Gamma).$$

Dann enthält X einen nicht-trivialen Gitterpunkt, d.h. es gibt $0 \neq \gamma \in X \cap \Gamma$.

2.2 Minkowski-Theorie

Sei $K/\mathbb{Q}$ ein Zahlkörper. Seien

$$\rho_1, \dots, \rho_r: K \hookrightarrow \mathbb{R}$$

die reellen Einbettungen und

$$\sigma_1, \bar{\sigma}_1, \dots, \sigma_s, \bar{\sigma}_s: K \hookrightarrow \mathbb{C}$$

die Paare komplexer Einbettungen.

Im Folgenden bezeichne τ stets eine beliebige Einbettung, ρ ist stets reell und σ stets komplex.

Definition 2.2.1 Der $\mathbb{R}$ -Vektorraum

$$K_{\mathbb{R}} := \left\{ (z_{\tau})_{\tau} \in \prod_{\tau} \mathbb{C} \mid z_{\rho} \in \mathbb{R}, z_{\bar{\sigma}} = \bar{z}_{\sigma} \right\}$$

heißt Minkowski-Raum.

Offensichtlich ist $\dim_{\mathbb{R}}(K_{\mathbb{R}}) = r + 2s = n$.

Auf $K_{\mathbb{R}}$ definieren wir ein Skalarprodukt durch

$$\langle x, y \rangle := \sum_{\tau} x_{\tau} \bar{y}_{\tau}.$$

Der nächste Satz stellt den Zusammenhang zum Standardskalarprodukt auf dem $\mathbb{R}^n$ her.

Satz 2.2.2 Die Abbildung

$$\begin{aligned} f: K_{\mathbb{R}} &\longrightarrow \prod_{\tau} \mathbb{R} = \mathbb{R}^{s+2s}, \\ (z_{\tau})_{\tau} &\longmapsto (z_{\rho_1}, \dots, z_{\rho_1}, \operatorname{Re}(z_{\sigma_1}), \operatorname{Im}(z_{\sigma_1}), \dots, \operatorname{Re}(z_{\sigma_s}), \operatorname{Im}(z_{\sigma_s})), \end{aligned}$$

ist eine Isomorphismus von $\mathbb{R}$ -Vektorräumen. Für das Skalarprodukt

$$(\cdot, \cdot): \mathbb{R}^{r+2s} \times \mathbb{R}^{r+2s} \longrightarrow \mathbb{R}, \quad (x, y) = \sum_{\rho} x_{\rho} y_{\rho} + \sum_{\sigma} 2x_{\sigma} y_{\sigma},$$

gilt für alle $x, y \in K_{\mathbb{R}}$

$$\langle x, y \rangle = (f(x), f(y)).$$

Hieraus folgt unmittelbar der Zusammenhang $\operatorname{Vol}(\cdot, \cdot) = 2^s \operatorname{Vol}_{\mathcal{L}}$, wobei letzteres das Lebesgue-Volumen bezeichnet.

Wir betrachten nun die sogenannte Minkowski-Abbildung

$$j: K \longrightarrow K_{\mathbb{R}}, \quad \alpha \mapsto (\tau(\alpha))_{\tau}.$$

Die Abbildung j ist injektiv und $\mathbb{Q}$ -linear.

Satz 2.2.3 Sei $0 \neq \mathfrak{a} \triangleleft \mathcal{O}_K$ ein ganzes Ideal. Dann ist $\Gamma := j(\mathfrak{a})$ ein volles Gitter in $K_{\mathbb{R}}$ und es gilt

$$\operatorname{Vol}(\Gamma) = \sqrt{|d_K|} [\mathcal{O}_K : \mathfrak{a}].$$

Satz 2.2.4 Sei $0 \neq \mathfrak{a} \triangleleft \mathcal{O}_K$ ein ganzes Ideal und sei für alle Einbettungen τ eine Zahl $c_{\tau} \in \mathbb{R}_{>0}$ gegeben mit $c_{\bar{\tau}} = c_{\tau}$. Es gelte:

$$\prod_{\tau} c_{\tau} > \left(\frac{2}{\pi} \right)^s \sqrt{|d_K|} [\mathcal{O}_K : \mathfrak{a}].$$

Dann gibt es ein $0 \neq a \in \mathfrak{a}$, so dass für alle Einbettungen τ gilt:

$$|\tau(a)| < c_{\tau}.$$

Wir setzen $N(\mathfrak{a}) := [\mathcal{O}_K : \mathfrak{a}]$ und erhalten das folgende

Lemma 2.2.5 *Zu jedem ganzen Ideal $0 \neq \mathfrak{a} \triangleleft \mathcal{O}_K$ gibt es ein $0 \neq a \in \mathfrak{a}$ mit der Eigenschaft*

$$|N_{K/\mathbb{Q}}(a)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|} N(\mathfrak{a}).$$

Hieraus folgt die Endlichkeit der Klassenzahl. Zuvor brauchen wir noch das folgende Resultat.

Lemma 2.2.6 *Sei $N \in \mathbb{R}_{>1}$. Dann gibt es nur endlich viele ganze Ideale $\mathfrak{a}$ mit $N(\mathfrak{a}) \leq N$.*

Satz 2.2.7 *Sei K ein Zahlkörper. Dann ist cl_K eine endliche abelsche Gruppe.*

Die Schranke aus Lemma 2.2.5 kann man verbessern. Es gilt:

Lemma 2.2.8 *Sei*

$$M := \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}$$

die sogenannte Minkowski-Schranke. Dann gibt es zu jedem ganzen Ideal $0 \neq \mathfrak{a} \triangleleft \mathcal{O}_K$ ein $0 \neq a \in \mathfrak{a}$ mit der Eigenschaft

$$|N_{K/\mathbb{Q}}(a)| \leq M \cdot N(\mathfrak{a}).$$

Remark 2.2.9 Die Klassengruppe wird erzeugt von den Klassen ganzer Ideale mit Norm kleiner gleich der Minkowski-Schranke M . Explizit:

$$\text{cl}_K = \langle [\mathfrak{a}] : N(\mathfrak{a}) \leq M \rangle.$$

Remark 2.2.10 Sei $\mathfrak{a}$ ein ganzes Ideal. Dann gilt:

$$\mathfrak{a} \text{ ist ein Hauptideal} \iff \exists \alpha \in \mathfrak{a} : |N_{K/\mathbb{Q}}(\alpha)| = N(\mathfrak{a}).$$

Sei L/K eine Erweiterung von Zahlkörpern. Ein Primideal $\mathfrak{p}$ in $\mathcal{O}_K$ heißt unverzweigt in L/K , falls in der Primidealzerlegung $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ alle Exponenten e_i gleich 1 sind. Die Erweiterung L/K heißt unverzweigt, falls alle Primideale $\mathfrak{p}$ in $\mathcal{O}_K$ unverzweigt sind.

Es gilt: L/K ist unverzweigt $\iff d_{L/K} = \mathcal{O}_K$. Hierbei bezeichnete $d_{L/K}$ das Diskriminantenideal, das wir in dieser Allgemeinheit noch gar nicht definiert haben.

Im Rahmen der Übungen werden Sie zeigen:

Satz 2.2.11 *Jede nicht-triviale Zahlkörpererweiterung $L/\mathbb{Q}$ ist verzweigt, oder mit anderen Worten: $d_L > 1$.*

3 Der Dirichletsche Einheitsatz

3.1 Der Dirichletsche Einheitsatz und sein Beweis

Wir behalten die Bezeichnungen des letzten Abschnitts bei und betrachten die Abbildung

$$\begin{aligned} l : K_{\mathbb{R}}^{\times} &\longrightarrow \mathbb{R}^{r+s}, \\ x = (x_{\tau}) &\mapsto (\log |x_{\rho_1}|, \dots, \log |x_{\rho_r}|, 2 \log |x_{\sigma_1}|, \dots, 2 \log |x_{\sigma_s}|). \end{aligned}$$

Wenn wir $K_{\mathbb{R}}^{\times}$ mit komponentenweiser Multiplikation versehen, so ist l ein Gruppenhomomorphismus, d.h. $l(xy) = l(x) + l(y)$.

Sei

$$N: K_{\mathbb{R}}^{\times} \longrightarrow \mathbb{R}^{\times}, \quad N(x) = \prod_{\tau: K \hookrightarrow \mathbb{C}} x_{\tau},$$

$$T: \mathbb{R}^{r+s} \longrightarrow \mathbb{R}, \quad T((x_{\tau})) = \sum_{\tau} x_{\tau}.$$

Man beachte, dass sich in der Definition von T die Summe über alle $\tau \in \{\rho_1, \dots, \rho_r, \sigma_1, \dots, \sigma_s\}$ erstreckt.

Dann kommutiert das folgende Diagramm

$$\begin{array}{ccccc} K^{\times} & \xrightarrow{j} & K_{\mathbb{R}}^{\times} & \xrightarrow{l} & \mathbb{R}^{r+s} \\ \downarrow N_{K/\mathbb{Q}} & & \downarrow N & & \downarrow T \\ \mathbb{Q}^{\times} & \xrightarrow{\subseteq} & \mathbb{R}^{\times} & \xrightarrow{\log|\cdot|} & \mathbb{R} \end{array}$$

Man beachte, dass alle involvierten Abbildungen Gruppenhomomorphismen sind. Betrachte nun

$$\begin{aligned} \mathcal{O}_K^{\times} &= \{\varepsilon \in \mathcal{O}_K \mid N_{K/\mathbb{Q}}(\varepsilon) = \pm 1\}, \\ S &:= \{y \in K_{\mathbb{R}}^{\times} \mid N(y) = \pm 1\} \\ H &:= \{x \in \mathbb{R}^{r+s} \mid T(x) = 0\}. \end{aligned}$$

Es sei nun $\lambda := l \circ j$ und $\Gamma := \lambda(\mathcal{O}_K^{\times})$. Offenbar gilt: $\Gamma \leq H$ und $\dim_{\mathbb{R}}(H) = r + s - 1$.

Satz 3.1.1 Die Gruppe der Einheitswurzeln μ_K ist endlich und die Sequenz

$$1 \longrightarrow \mu_K \longrightarrow \mathcal{O}_K^{\times} \xrightarrow{\lambda} \Gamma \longrightarrow 0$$

ist exakt.

Wir werden zeigen, dass Γ ein volles Gitter in H ist. Dazu benötigen wir das

Lemma 3.1.2 Sei a eine natürliche Zahl. Dann gibt es bis auf Assoziiertheit nur endlich viele $\alpha \in \mathcal{O}_K$ mit $|N_{K/\mathbb{Q}}(\alpha)| = a$.

Satz 3.1.3 Die Untergruppe Γ von H ist ein volles Gitter. Insbesondere ist also $\Gamma \simeq \mathbb{Z}^{r+s-1}$.

Als direkte Folgerung hieraus erhalten wir den Dirichletschen Einheitensatz.

Satz 3.1.4 Sei K ein Zahlkörper. Dann sind die Einheiten $\mathcal{O}_K^{\times}$ eine endlich erzeugte abelsche Gruppe vom $\mathbb{Z}$ -Rang $t := r + s - 1$. Es gibt also Einheiten $\varepsilon_1, \dots, \varepsilon_t$, so dass

$$\mathcal{O}_K^{\times} = \mu_K \times \varepsilon_1^{\mathbb{Z}} \times \dots \times \varepsilon_t^{\mathbb{Z}} \simeq \mu_K \times \mathbb{Z}^t.$$

Man nennt dann $\varepsilon_1, \dots, \varepsilon_t$ ein System von Fundamenteleinheiten.

3.2 Berechnung der Fundamenteleinheit in reell-quadratischen Zahlkörpern

Sei stets $d > 1$ quadratfrei und $K = \mathbb{Q}(\sqrt{d})$.

Satz 3.2.1 Die Einheiten in $\mathcal{O}_K$ korrespondieren 1-1 mit den Lösungen $(x, y) \in \mathbb{Z}^2$ der sogenannten Pellischen Gleichung $x^2 - dy^2 = \pm 4$. Explizit:

$$\alpha = \frac{1}{2}(x + y\sqrt{d}) \mapsto (x, y)$$

Definition 3.2.2 Die Fundamenteinheit ε mit $\varepsilon > 1$ nennen wir die normalisierte Fundamenteinheit.

Falls ε die normalisierte Fundamenteinheit ist, so ist $\{\pm\varepsilon, \pm\varepsilon^{-1}\}$ genau die Menge aller Fundamenteinheiten. Jede beliebige Einheit η ist von der Form $\eta = \pm\varepsilon^m$ mit einem eindeutig bestimmten $m \in \mathbb{Z}$. Die Einheiten $\eta > 1$ sind von der Form $\eta = \varepsilon^m$ mit $m \in \mathbb{N}$.

Satz 3.2.3 $\varepsilon = a + b\sqrt{d}$ mit $a, b \in \frac{1}{2}\mathbb{Z}_{>0}$ ist genau dann die normalisierte Fundamenteinheit, wenn für alle anderen Einheiten $\eta = c + e\sqrt{d} > 1$ die Ungleichung $a < c$ gilt.

In der Korrespondenz von Satz 3.2.1 entspricht also die Fundamenteinheit derjenigen Lösung (x, y) der Pellischen Gleichung mit minimalem $x > 1$.

3.3 Der Regulator

Es sei $t = r + s - 1$ der Einheitenrang und $\varepsilon_1, \dots, \varepsilon_t$ ein System von Fundamenteinheiten. Dann ist $\lambda(\varepsilon_1), \dots, \lambda(\varepsilon_t)$ eine $\mathbb{Z}$ -Basis von $\Gamma = \lambda(\mathcal{O}_K^\times)$. Der Vektor

$$\lambda_0 := \frac{1}{\sqrt{r+s}}(1, \dots, 1)^{\text{trans}} \in \mathbb{R}^{r+s}$$

hat Länge 1 und steht senkrecht auf allen $\lambda(\varepsilon_i)$. Also ist

$$\text{Vol}_{\mathcal{L}}(\Gamma) = \pm \det(\lambda_0, \lambda(\varepsilon_1), \dots, \lambda(\varepsilon_t)).$$

Satz 3.3.1 Das Volumen von $\Gamma = \lambda(\mathcal{O}_K^\times)$ ist gegeben durch

$$\text{Vol}(\Gamma) = \sqrt{r+s} R_K,$$

wobei R_K der Absolutbetrag eines beliebigen $t \times t$ -Minors der $(t+1) \times t$ -Matrix $(\lambda(\varepsilon_1), \dots, \lambda(\varepsilon_t))$ ist.

Definition 3.3.2 R_K nennt man den Regulator von K .

Sei nun $\eta_1, \dots, \eta_t$ ein beliebiges System von Einheiten. Wir definieren den zugehörigen Regulator durch

$$R_K(\eta_1, \dots, \eta_t) := \text{Absolutbetrag eines } t \times t\text{-Minors von } (\lambda(\eta_1), \dots, \lambda(\eta_t)).$$

Dann gilt also $R_K = R_K(\varepsilon_1, \dots, \varepsilon_t)$. Wir sagen, dass $\eta_1, \dots, \eta_t$ ein unabhängiges Einheitensystem ist, wenn $\langle \eta_1, \dots, \eta_t \rangle$ endlichen Index in $\mathcal{O}_K^\times$ hat.

Satz 3.3.3 Sei $\eta_1, \dots, \eta_t \in \mathcal{O}_K^\times$ ein beliebiges System von Einheiten. Dann gilt:

$$\eta_1, \dots, \eta_t \text{ ist unabhängiges Einheitensystem} \iff R_K(\eta_1, \dots, \eta_t) \neq 0.$$

Falls $R_K(\eta_1, \dots, \eta_t) \neq 0$, so gilt

$$[\mathcal{O}_K^\times / \mu_K : \langle \eta_1, \dots, \eta_t \rangle \mu_K / \mu_K] = \frac{R_K(\eta_1, \dots, \eta_t)}{R_K}.$$

Diese Aussagen werden im Rahmen der Übungen bewiesen.

4 Erweiterungen von Dedekindringen

4.1 Das Polynomzerlegungsgesetz

Sei nun L/K eine Erweiterung von Zahlkörpern und $\mathfrak{p} \triangleleft \mathcal{O}_K$ ein Primideal ungleich 0. Wir wollen die Primidealzerlegung von $\mathfrak{p}\mathcal{O}_L$ studieren.

Sei

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

mit $e_i \geq 1$ die gesuchte Zerlegung. Dann sind die $\mathfrak{P}_i$ genau die Primideale $\mathfrak{P}$ von $\mathcal{O}_L$ mit der Eigenschaft $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$. Wir schreiben dann $\mathfrak{P} \mid \mathfrak{p}$ und sagen, $\mathfrak{P}$ liegt über $\mathfrak{p}$. Die Zahl e_i heißt Verzeigungsindex und die Zahl

$$f_i := [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$$

nennen wir den Trägheitsgrad von $\mathfrak{P}_i$.

Satz 4.1.1 *In dieser Situation gilt: $\sum_{i=1}^r e_i f_i = [L : K]$.*

Im Weiteren wollen wir für fast alle Primideale $\mathfrak{p} \neq (0)$ von $\mathcal{O}_K$ die Primidealzerlegung von $\mathfrak{p}\mathcal{O}_K$ explizit angeben. Dies geschieht durch das sogenannte Polynomzerlegungsgesetz.

Sei dazu $L = K(\theta)$ mit einem ganzen Element θ . Sei $f \in \mathcal{O}_K[x]$ das Minimalpolynom von θ .

Definition 4.1.2 Das Ideal $\mathfrak{f} := \{\alpha \in \mathcal{O}_K \mid \alpha\mathcal{O}_L \subseteq \mathcal{O}_K[\theta]\}$ nennen wir den Führer oder Konduktor von $\mathcal{O}_K[\theta]$ bezüglich $\mathcal{O}_L$.

Der Konduktor ist das größte in $\mathcal{O}_K[\theta]$ gelegene $\mathcal{O}_L$ -Ideal. Es gilt:

$$\mathfrak{f} = \mathcal{O}_L \iff \mathcal{O}_K[\theta] = \mathcal{O}_K.$$

Satz 4.1.3 *Sei $\mathfrak{p}$ ein zu $\mathfrak{f}$ teilerfremdes Ideal, d.h. $\mathfrak{p}\mathcal{O}_L + \mathfrak{f} = \mathcal{O}_L$. Sei $k := \mathcal{O}_K/\mathfrak{p}$ der Restklassenkörper und sei $\bar{f}$ das Bild von f in $k[x]$. Es sei*

$$\bar{f}(x) = \bar{f}_1(x)^{e_1} \cdots \bar{f}_r(x)^{e_r}$$

die Zerlegung von $\bar{f}$ in $k[x]$ mit paarweise verschiedenen irreduziblen Polynomen $\bar{f}_i$. Dann sind die über $\mathfrak{p}$ liegenden Primideale von $\mathcal{O}_L$ gegeben durch

$$\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + f_i(\theta)\mathcal{O}_L, \quad i = 1, \dots, r.$$

Der Trägheitsgrad von $\mathfrak{P}_i$ ist gegeben durch $\deg(\bar{f}_i)$ und es gilt

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}.$$

Wir benutzen folgende Sprechweisen. Sei $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$. Dann sagen wir, $\mathfrak{p}$ ist voll zerlegt, falls $r = [L : K]$, und wir nennen $\mathfrak{p}$ unverzweigt, wenn $e_i = 1$ für $i = 1, \dots, r$.

4.2 Verzweigung und Diskriminante

Verzweigte Primideale sind in gewissem Sinne schwieriger als die unverzweigten. Tatsächlich gibt es aber nur endlich viele verzweigte.

Satz 4.2.1 *Sei L/K eine Erweiterung von Zahlkörpern. Dann gibt es nur endlich viele verzweigte Primideale $\mathfrak{p}$ von $\mathcal{O}_K$.*

Remark 4.2.2 Für eine Zahlkörpererweiterung L/K haben wir bislang noch keine Diskriminante definiert. Unsere Definition funktioniert im Prinzip für alle Erweiterungen L/K , wo $\mathcal{O}_K$ ein Hauptidealbereich ist. Allgemeiner kann man $d_{L/K}$ mit Hilfe der Lokalisierungen nach Primidealen $\mathfrak{p}$ von $\mathcal{O}_K$ definieren. Oder alternativ: Die Diskriminante ist dasjenige Ideal von $\mathcal{O}_K$, das erzeugt wird von allen $d(\omega_1, \dots, \omega_n)$, wobei $\omega_1, \dots, \omega_n$ alle in $\mathcal{O}_L$ gelegenen Basen von L/K durchläuft.

Es gilt der folgende

Satz 4.2.3 Sei L/K eine Erweiterung von Zahlkörpern. Dann gilt:

$$\mathfrak{p} \text{ verzweigt in } L/K \iff \mathfrak{p} \mid d_{L/K}.$$

Den Satz haben wir nicht bewiesen. Wir haben gezeigt:

Satz 4.2.4 Sei K ein Zahlkörper und p eine Primzahl. Dann gilt:

$$p \text{ verzweigt in } K/\mathbb{Q} \implies p \mid d_K.$$

4.3 Hilbertsche Verzeigungstheorie

In diesem Abschnitt ist nun L/K stets eine Galoiserweiterung von Zahlkörpern mit Gruppe $G := \text{Gal}(L/K)$. In dieser Situation wirkt G in natürlicher Weise auf den arithmetischen Objekten, die wir bislang untersucht haben, wie zum Beispiel $\mathcal{O}_L, I_L, \mu_L, \mathcal{O}_L^\times, \text{cl}_L$.

Wir untersuchen hier die Wirkung von G auf I_L . Da I_L als abelsche Gruppe von den Primidealen erzeugt ist, reicht es die Wirkung auf Primideale $\mathfrak{P}$ zu studieren.

Satz 4.3.1 Sei $\mathfrak{p}$ ein Primideal von $\mathcal{O}_K$. Dann wirkt G transitiv auf der Menge der Primideale von $\mathcal{O}_L$ über $\mathfrak{p}$.

Definition 4.3.2 Sei $\mathfrak{P}$ ein Primideal von $\mathcal{O}_L$. Dann nennt man

$$G_{\mathfrak{P}} := \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

die Zerlegungsgruppe von $\mathfrak{P}$. Der Fixkörper $Z_{\mathfrak{P}} := L^{G_{\mathfrak{P}}}$ heißt Zerlegungskörper von $\mathfrak{P}$.

Wir werden nächstes Mal zeigen:

Lemma 4.3.3 Für ein festes Primideal $\mathfrak{P}$ von $\mathcal{O}_L$ über $\mathfrak{p}$ gilt:

- a) $\#\{\mathfrak{Q} \mid \mathfrak{Q} \text{ liegt über } \mathfrak{p}\} = [G : G_{\mathfrak{P}}]$.
- b) $G_{\mathfrak{P}} = 1 \iff Z_{\mathfrak{P}} = L \iff \mathfrak{p} \text{ ist voll zerlegt.}$
- c) $G_{\mathfrak{P}} = G \iff Z_{\mathfrak{P}} = K \iff \mathfrak{p} \text{ ist unzerlegt.}$
- d) Für $\sigma \in G$ ist $G_{\sigma(\mathfrak{P})} = \sigma G_{\mathfrak{P}} \sigma^{-1}$.

Satz 4.3.4 Sei L/K eine Galoiserweiterung von Zahlkörpern und es sei $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$. Dann gilt

$$f_1 = \dots = f_r =: f, \quad e_1 = \dots = e_r =: e,$$

und daher auch

$$efr = [L : K]$$

und

$$\mathfrak{p}\mathcal{O}_L = \left(\prod_{\sigma \in G/G_{\mathfrak{P}}} \sigma(\mathfrak{P}) \right)^e$$

für alle Primideale $\mathfrak{P} \mid \mathfrak{p}$.

Im Weiteren schreiben wir $Z := Z_{\mathfrak{P}}$ für den Zerlegungskörper von $\mathfrak{P}$. Wir setzen $\mathfrak{P}_Z := \mathfrak{P} \cap Z$.

Satz 4.3.5 Dann gilt:

- a) $\mathfrak{P}_Z$ ist unzerlegt in L/Z .
- b) $\mathfrak{P}$ hat über Z den Verzweigungsindex e und den Trägheitsgrad f .
- c) Verzweigungsindex und Trägheitsgrad von $\mathfrak{P}_Z$ in Z/K sind beide gleich 1.

Im Weiteren wollen wir auch den Verzweigungsindex e gruppentheoretisch interpretieren. Sei $\sigma \in G_{\mathfrak{P}}$. Dann induziert σ eine Galoisautomorphismus

$$\bar{\sigma}: \mathcal{O}_L/\mathfrak{P} \longrightarrow \mathcal{O}_L/\mathfrak{P}, \quad \bar{\alpha} \mapsto \overline{\sigma(\alpha)}, \alpha \in \mathcal{O}_L.$$

Im Folgenden schreiben wir $\kappa(\mathfrak{P}) := \mathcal{O}_L/\mathfrak{P}$ und $\kappa(\mathfrak{p}) := \mathcal{O}_K/\mathfrak{p}$ für die Restklassenkörper.

Satz 4.3.6 *Der natürliche Homomorphismus $G_{\mathfrak{P}} \longrightarrow \text{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})), \sigma \mapsto \bar{\sigma}$, ist surjektiv.*

Definition 4.3.7 Der Kern des surjektiven Homomorphismus $\text{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})), \sigma \mapsto \bar{\sigma}$, heißt Trägheitsgruppe oder Verzweigungsgruppe von $\mathfrak{P}$ über K . Bezeichnung: $I_{\mathfrak{P}}$. Den Fixkörper $T = T_{\mathfrak{P}} := L^{I_{\mathfrak{P}}}$ nennt man den Trägheitskörper.

Die Trägheitsgruppe hat die folgende explizite Beschreibung:

$$I_{\mathfrak{P}} = \{\sigma \in G_{\mathfrak{P}} \mid \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}}, \forall \alpha \in \mathcal{O}_L\}.$$

Satz 4.3.8 *Es sei $\mathfrak{P}/\mathfrak{p}$ mit Verzweigungsindex $e = e(\mathfrak{P}/\mathfrak{p})$ und Restklassenkörpergrad $f = f(\mathfrak{P}/\mathfrak{p})$.*

- a) *Die Erweiterung $T_{\mathfrak{P}}/Z_{\mathfrak{P}}$ ist galoissch.*
- b) *Es gilt: $|I_{\mathfrak{P}}| = e$ und $|G_{\mathfrak{P}}/I_{\mathfrak{P}}| = f$.*
- c) *Es gilt:*

$$\begin{aligned} e(\mathfrak{P}_Z/\mathfrak{p}) &= e(\mathfrak{P}_T/\mathfrak{P}_Z) = 1, & e(\mathfrak{P}/\mathfrak{P}_T) &= e, \\ f(\mathfrak{P}_Z/\mathfrak{p}) &= f(\mathfrak{P}/\mathfrak{P}_T) = 1, & f(\mathfrak{P}_T/\mathfrak{P}_Z) &= f. \end{aligned}$$

Für unverzweigte Primideale $\mathfrak{P}$ ist $G_{\mathfrak{P}}$ isomorph zur Galoisgruppe $\text{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ der Restklassenkörpererweiterung. Als Erweiterung von endlichen Körpern ist $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ zyklisch, die Galoisgruppe wird erzeugt vom sogenannten Frobeniuselement φ . Explizit:

$$\text{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})) = \langle \varphi \rangle \text{ mit } \varphi(\alpha) = \alpha^q,$$

wobei $q := |\kappa(\mathfrak{p})|$. Dies definiert ein eindeutig bestimmtes Element $\varphi_{\mathfrak{P}} \in G_{\mathfrak{P}} \leq G$.

Satz 4.3.9 *Sei L/K galoissch und $\mathfrak{P}$ unverzweigt in L/K . Dann gibt es genau einen Automorphismus $\varphi_{\mathfrak{P}} \in G_{\mathfrak{P}} \leq G$ mit*

$$\varphi(\alpha) \equiv \alpha^q \pmod{\mathfrak{P}}, \quad \forall \alpha \in \mathcal{O}_L,$$

Hierbei ist $q := |\kappa(\mathfrak{p})|$.

Folgerung 4.3.10 *Falls L/K galoissch, aber nicht zyklisch ist, so gibt es höchstens endlich viele unzerlegte Primideale. Genauer: Nur die verzweigten Primideale $\mathfrak{P}$ können unzerlegt sein.*

4.4 Beispiel: Kreisteilungskörper

Es sei stets $K = K_n = \mathbb{Q}(\zeta_n)$.

Lemma 4.4.1 *Sei $n = p^\nu$ eine Primzahlpotenz und $\pi = 1 - \zeta_{p^\nu}$. Dann ist $\pi\mathcal{O}_K$ ein Primideal vom Grad $f = 1$ und es gilt*

$$p\mathcal{O}_K = (\pi\mathcal{O}_K)^e \text{ mit } e = \varphi(p^\nu) = (p-1)p^{\nu-1} = [K : \mathbb{Q}].$$

Die Primzahl p ist also voll verzweigt in $\mathbb{Q}(\zeta_{p^\nu})/\mathbb{Q}$.

Ferner gilt:

$$d(\zeta_{p^\nu}) = \pm p^s \text{ mit } s = p^{\nu-1}(\nu p - \nu - 1).$$

Satz 4.4.2 Sei $n \in \mathbb{N}$ und $K = \mathbb{Q}(\zeta_n)$. Dann gilt: $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$. Falls

$$n = p_1^{\nu_1} \cdots p_m^{\nu_m}$$

die Primzahlzerlegung von n ist, so ist die Diskriminante d_K ein Produkt von Potenzen der p_i .

Das Polynomzerlegungsgesetz liefert uns den folgenden Sachverhalt.

Satz 4.4.3 Sei $n = \prod_p p^{\nu_p}$ die Primidealzerlegung von n . Für eine Primzahl p sei $f_p \in \mathbb{Z}_{>0}$ minimal mit der Eigenschaft

$$p^{f_p} \equiv 1 \pmod{n/p^{\nu_p}}.$$

Dann gilt

$$p\mathcal{O}_K = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^{e_p} \text{ mit } e_p = \varphi(p^{\nu_p}),$$

wobei die Primideale $\mathfrak{p}_i$ jeweils den Restklassengrad f_p haben und die Zahl r durch die Gleichung $\varphi(n) = r f_p e_p$ eindeutig festgelegt ist.

Folgerung 4.4.4 Eine Primzahl p ist genau dann verzweigt in $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, wenn p ein Teiler von n ist, es sei denn $p = 2 = (n, 4)$. Eine Primzahl p ist genau dann voll zerlegt in $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, wenn $p \equiv 1 \pmod{n}$ gilt. Insbesondere ist $p = 2$ nicht voll zerlegt für alle $n \in \mathbb{N}$.

5 Bewertungstheorie

5.1 Bewertungen

Sei $\mathcal{O}$ ein Dedekindring mit Quotientenkörper K und $\mathfrak{p} \neq (0)$ ein Primideal in $\mathcal{O}$. Für $\alpha \in \mathcal{O}$ schreiben wir $\alpha\mathcal{O} = \mathfrak{p}^{v_{\mathfrak{p}}(\alpha)}\mathfrak{a}$ mit einem ganzen zu $\mathfrak{p}$ teilerfremden Ideal $\mathfrak{a}$. Dann ist $v_{\mathfrak{p}}$ multiplikativ, d.h. $v_{\mathfrak{p}}(\alpha\beta) = v_{\mathfrak{p}}(\alpha) + v_{\mathfrak{p}}(\beta)$ für alle $\alpha, \beta \in \mathcal{O}$. Also kann man $v_{\mathfrak{p}}$ auf $K^\times$ fortsetzen und wir erhalten einen Homomorphismus von Gruppen

$$v_{\mathfrak{p}}: K^\times \longrightarrow \mathbb{Z}.$$

Zusätzlich definieren wir $v_{\mathfrak{p}}(0) := \infty$.

Lemma 5.1.1 Für alle $\alpha, \beta \in K$ gilt:

$$v_{\mathfrak{p}}(\alpha + \beta) \geq \min(v_{\mathfrak{p}}(\alpha), v_{\mathfrak{p}}(\beta)).$$

Falls $v_{\mathfrak{p}}(\alpha) \neq v_{\mathfrak{p}}(\beta)$ gilt, so gilt in der Ungleichung die Gleichheit.

$v_{\mathfrak{p}}$ nennt man die $\mathfrak{p}$ -adische Bewertung auf K . Die Bewertung $v_{\mathfrak{p}}$ gibt Anlass zu einem $\mathfrak{p}$ -adischen Betrag auf K . Für jedes $b \in \mathbb{R}_{>1}$ wird nämlich durch $|\alpha| := b^{-v_{\mathfrak{p}}(\alpha)}$ ein Betrag auf K definiert. Unabhängig von der Wahl von b definieren diese Beträge alle dieselbe Topologie auf K . In der folgenden Definition wird dieser Betrag geeignet normiert.

Definition 5.1.2 Sei K ein Zahlkörper und $\mathcal{O} = \mathcal{O}_K$. Für $\alpha \in K$ setzen wir $|\alpha|_{\mathfrak{p}} := (N\mathfrak{p})^{-v_{\mathfrak{p}}(\alpha)}$. Dann heißt $|\alpha|_{\mathfrak{p}}$ der $\mathfrak{p}$ -adische Betrag von α .

Der $\mathfrak{p}$ -adische Betrag erfüllt eine verschärfte Dreiecksungleichung.

Lemma 5.1.3 Für $\alpha, \beta \in K$ gilt:

- (a) $|\alpha|_{\mathfrak{p}} \geq 0$.
- (b) $|\alpha|_{\mathfrak{p}} = 0 \iff \alpha = 0$.
- (c) $|\alpha + \beta|_{\mathfrak{p}} \leq \max(|\alpha|_{\mathfrak{p}}, |\beta|_{\mathfrak{p}}) \leq |\alpha|_{\mathfrak{p}} + |\beta|_{\mathfrak{p}}$.

5.2 Die p -adischen Zahlen

In diesem Abschnitt werden wir die p -adischen Zahlen $\mathbb{Z}_p$ sowie den Quotientenkörper $\mathbb{Q}_p$ konstruieren. Es sei p stets eine Primzahl. Dann besitzt jede natürliche Zahl f eine p -adische Entwicklung

$$f = a_0 + a_1p + a_2p^2 + \dots + a_{n-1}p^{n-1}$$

mit eindeutig bestimmten Zahlen $0 \leq a_i \leq p-1$.

Definition 5.2.1 Eine ganze p -adische Zahl ist eine formale Potenzreihe

$$\sum_{i=0}^{\infty} a_i p^i$$

mit ganzen Zahlen $0 \leq a_i \leq p-1$. Die Gesamtheit der ganzen p -adischen Zahlen bezeichnen wir mit $\mathbb{Z}_p$.

Das folgende Resultat ist elementar.

Satz 5.2.2 Die Restklassen $a \bmod p^n$ sind in eindeutiger Weise durch

$$a \equiv a_0 + a_1p + a_2p^2 + \dots + a_{n-1}p^{n-1} \pmod{p^n}$$

mit ganzen Zahlen $0 \leq a_i \leq p-1$ gegeben.

Jede ganze Zahl f liefert also eine p -adische Entwicklung $\sum_{i=0}^{\infty} a_i p^i$, derart dass für alle $n \geq 1$ gilt:

$$f \equiv \sum_{i=0}^{n-1} a_i p^i \pmod{p^n}.$$

Definition 5.2.3 Die formalen Laurantreihen

$$\sum_{i=-m}^{\infty} a_i p^i$$

mit ganzen Zahlen $0 \leq a_i \leq p-1$ und $m \in \mathbb{Z}$ nennt man p -adische Zahlen. Die Gesamtheit der p -adischen Zahlen bezeichnen wir mit $\mathbb{Q}_p$.

Im Weiteren wollen wir eine Ringstruktur auf $\mathbb{Z}_p$ definieren. Die p -adischen Zahlen $\mathbb{Q}_p$ sind dann der Quotientenkörper von $\mathbb{Z}_p$.

Dazu betrachten wir den projektiven Limes $\varprojlim_n \mathbb{Z}/p^n \mathbb{Z}$. Explizit ist der projektive Limes gegeben durch

$$\varprojlim_n \mathbb{Z}/p^n \mathbb{Z} = \{(x_n) \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n \mathbb{Z} \mid x_{n+1} \equiv x_n \pmod{p^n} \text{ für alle } n \geq 1\}.$$

Satz 5.2.4 Die Zuordnung

$$\mathbb{Z}_p \longrightarrow \varprojlim_n \mathbb{Z}/p^n \mathbb{Z}, \quad \sum_{i=0}^{\infty} a_i p^i \mapsto \left(\sum_{i=0}^{n-1} a_i p^i \right)_{n=1}^{\infty}$$

ist eine Bijektion.

Der projektive Limes ist mittels komponentenweiser Addition und Multiplikation in natürlicher Weise ein kommutativer Ring. Durch die obige Bijektion übertragen wir diese Ringstruktur auf $\mathbb{Z}_p$. Jede Laurantreihe g kann man in der Form $p^m h$ mit $m \in \mathbb{Z}$ und einer Potenzreihe $h \in \mathbb{Z}_p$ schreiben. Daher setzt sich diese Ringstruktur auf $\mathbb{Q}_p$ fort.

Satz 5.2.5

- a) $\mathbb{Z}_p^\times = \{\sum_{\nu=0}^{\infty} a_\nu p^\nu \mid a_0 \neq 0\}$.
- b) $\mathbb{Z}_p$ ist nullteilerfrei.
- c) $\text{Quot}(\mathbb{Z}_p) = \mathbb{Q}_p$.

5.3 p -adische Kompletzierung

In diesem Abschnitt wollen wir eine weitere Art der Konstruktion von $\mathbb{Q}_p$ kennen lernen. Sei dazu R der Ring der Cauchy-Folgen rationaler Zahlen und $\mathfrak{m} \triangleleft R$ das Ideal der Nullfolgen. Dann ist $\mathfrak{m}$ ein maximales Ideal in R .

Definition 5.3.1 $\mathbb{Q}_p := R/\mathfrak{m}$.

Wir benutzen hier dasselbe Symbol, müssen uns aber später klar machen, dass dieses $\mathbb{Q}_p$ bis auf eine natürliche Isomorphie mit dem $\mathbb{Q}_p$ aus dem letzten Abschnitt übereinstimmt.

Man setzt nun den p -adischen Betrag $|\cdot|_p$ auf $\mathbb{Q}_p$ fort. Sei dazu $x = (x_n)_{n=1}^\infty + \mathfrak{m}$ ein Element in $\mathbb{Q}_p$ repräsentiert durch die Cauchyfolge rationaler Zahlen $(x_n)_{n=1}^\infty$. Dann definiert man

$$|x|_p := \lim_{n \rightarrow \infty} |x_n|_p.$$

Satz 5.3.2 $\mathbb{Q}_p$ ist bezüglich $|\cdot|_p$ ein vollständiger Körper.

Literatur hierzu: Gerhard Frey, Elementare Zahlentheorie, vieweg

Beobachtung: Sei $0 \neq x = (x_n)_{n=1}^\infty + \mathfrak{m}$ ein Element in $\mathbb{Q}_p$ repräsentiert durch die Cauchyfolge rationaler Zahlen $(x_n)_{n=1}^\infty$. Dann wird die Folge $(|x_n|_p)_{n=1}^\infty$ stationär. D.h. es gibt ein n_0 , so dass für alle $n \geq n_0$ gilt:

$$|x|_p = |x_n|_p \text{ bzw. } v_p(x) = v_p(x_n).$$

Definition 5.3.3 $\mathbb{Z}_p := \{\alpha \in \mathbb{Q}_p \mid |\alpha|_p \leq 1\} = \{\alpha \in \mathbb{Q}_p \mid v_p(\alpha) \geq 0\}$ heißt Ring der ganzen p -adischen Zahlen.

Satz 5.3.4 a) $\mathbb{Z}_p$ ist ein Ring.

b) $\mathbb{Z}_p$ ist der topologische Abschluss von $\mathbb{Z}$ in $\mathbb{Q}_p$.

c) Jedes $\alpha \in \mathbb{Z}_p$ wird repräsentiert durch eine Cauchyfolge $(y_n)_{n=1}^\infty$ mit $y_n \in \mathbb{Z}$.

Lemma 5.3.5 a) Es gilt: $\mathbb{Z}_p^\times = \{\alpha \in \mathbb{Q}_p \mid |\alpha|_p = 1\} = \{\alpha \in \mathbb{Q}_p \mid v_p(\alpha) = 0\}$.

b) Jedes $\alpha \in \mathbb{Q}_p$ hat eine eindeutige Darstellung $\alpha = p^m \eta$ mit $m \in \mathbb{Z}$ und $\eta \in \mathbb{Z}_p^\times$.

Satz 5.3.6 Die von Null verschiedenen Ideale von $\mathbb{Z}_p$ sind die Hauptideale

$$p^n \mathbb{Z}_p = \{\alpha \in \mathbb{Q}_p \mid v_p(\alpha) \geq n\}$$

und es gilt

$$\mathbb{Z}/p^n \mathbb{Z} \simeq \mathbb{Z}_p/p^n \mathbb{Z}_p.$$

Satz 5.3.7 Der kanonische Homomorphismus

$$\mathbb{Z}_p \longrightarrow \varprojlim_n \mathbb{Z}_p/p^n \mathbb{Z}_p \simeq \varprojlim_n \mathbb{Z}/p^n \mathbb{Z}$$

ist ein Isomorphismus.

6 Bewertete Körper

6.1 Grundlegendes

Ein Betrag eines Körpers K ist eine Funktion $|\cdot|: K \longrightarrow \mathbb{R}$, so dass für alle $x, y \in K$ gilt

- (i) $|x| \geq 0$ und $|x| = 0 \iff x = 0$,
- (ii) $|xy| = |x||y|$,
- (iii) $|x + y| \leq |x| + |y|$.

Zwei Beträge auf K nennen wir äquivalent, wenn sie die gleiche Topologie erzeugen.

Satz 6.1.1 Seien $|\cdot|_1$ und $|\cdot|_2$ zwei Beträge auf dem Körper K . Dann sind folgende Aussagen äquivalent:

- (a) $|\cdot|_1$ und $|\cdot|_2$ sind äquivalent.
- (b) Für alle $x \in K$ gilt: $|x|_1 < 1 \implies |x|_2 < 1$.
- (c) Für alle $x \in K$ gilt: $|x|_2 < 1 \implies |x|_1 < 1$.
- (d) Es gibt ein $s \in \mathbb{R}_{>0}$, so dass für alle $x \in K$ gilt: $|x|_1 = |x|_2^s$.

Der folgende, sogenannte Approximationssatz, ist eine Verallgemeinerung des Chinesischen Restsatzes.

Satz 6.1.2 Seien $|\cdot|_1, \dots, |\cdot|_n$ paarweise inäquivalente Beträge von K und $a_1, \dots, a_n \in K$. Dann gibt es zu jedem $\varepsilon > 0$ ein $x \in K$, so dass für alle $i = 1, \dots, n$ gilt:

$$|x - a_i|_i < \varepsilon.$$

Wir erinnern an die folgende Definition.

Definition 6.1.3 Ein Betrag $|\cdot|$ auf dem Körper K heißt nicht-archimedisch oder endlich, falls $|n|$ für $n \in \mathbb{N}$ beschränkt ist. Andernfalls nennen wir den Betrag archimedisch oder unendlich.

Satz 6.1.4 Sei $|\cdot|$ ein Betrag auf dem Körper K . Dann gilt:

$$|\cdot| \text{ ist nicht-archimedisch} \iff |x + y| \leq \max(|x|, |y|), \forall x, y \in K$$

Über die Beträge von $\mathbb{Q}$ beziehungsweise allgemeiner die Beträge eines Zahlkörpers K gibt der Satz von Ostrowski Auskunft.

Satz 6.1.5 Sei K ein Zahlkörper. Dann ist jeder Betrag $|\cdot|$ auf K äquivalent zu $|\cdot|_{\mathfrak{p}}$ für ein Primideal $\mathfrak{p} \neq 0$ oder zu $|\cdot|_{\tau}$ für eine Einbettung $\tau: K \hookrightarrow \mathbb{C}$.

Für einen nicht-archimedischen Betrag auf einem Körper K definieren wir eine Bewertung

$$v: K \longrightarrow \mathbb{R} \cup \{\infty\}$$

mittels

$$v(\alpha) := -\log |\alpha| \text{ für alle } \alpha \neq 0 \text{ und } v(0) := \infty.$$

Dann hat man offensichtlich

$$\begin{aligned} v(\alpha) = \infty &\iff \alpha = 0, \\ v(\alpha\beta) &= v(\alpha) + v(\beta), \\ v(\alpha + \beta) &\geq \min(v(\alpha), v(\beta)). \end{aligned}$$

Jede solche Funktion mit diesen Eigenschaften nennen wir eine Bewertung. Zwei Bewertungen v_1 und v_2 heißen äquivalent, wenn es eine $s \in \mathbb{R}_{>0}$ gibt mit der Eigenschaft $v_1 = sv_2$. Jede Bewertung auf K liefert uns umgekehrt durch die Setzung $|\alpha| := B^{-v(\alpha)}$ mit $B \in \mathbb{R}_{>1}$ einen nicht-archimedischen Betrag. Nicht-archimedische Beträge und Bewertungen entsprechen sich also (jeweils modulo Äquivalenz).

Satz 6.1.6 Sei $|\cdot|$ ein nicht-archimedischer Betrag auf dem Körper K und v die entsprechende Bewertung. Dann ist

$$\mathcal{O} := \{\alpha \in K \mid v(\alpha) \geq 0\} = \{\alpha \in K \mid |\alpha| \leq 1\}$$

ein lokaler Ring mit maximalem Ideal

$$\mathfrak{p} = \{\alpha \in K \mid v(\alpha) > 0\} = \{\alpha \in K \mid |\alpha| < 1\}.$$

Ferner gilt:

$$\mathcal{O}^\times := \{\alpha \in K \mid v(\alpha) = 0\} = \{\alpha \in K \mid |\alpha| = 1\}$$

Remark 6.1.7 a) Äquivalente Bewertungen bzw. Beträge führen zu denselben Ringen.
b) Für alle $\alpha \in K^\times$ gilt: $\alpha \in \mathcal{O}$ oder $\alpha^{-1} \in \mathcal{O}$. Der Ring $\mathcal{O}$ ist also ein Bewertungsring im Sinne der kommutativen Algebra.

Definition 6.1.8 Eine Bewertung v auf dem Körper K heißt diskret, falls sie einen kleinsten positiven Wert s hat. Wir nennen dann v normiert, falls $s = 1$ gilt. Falls v normiert ist, so nennen wir jedes Element $\pi \in K$ mit $v(\pi) = 1$ ein Primelement oder auch Uniformisierendes.

Remark 6.1.9 Sei v eine diskrete Bewertung auf K und $s := \min\{v(\alpha) \mid \alpha \in K\}$. Dann gilt:

$$v(K^\times) = s\mathbb{Z}.$$

Lemma 6.1.10 Sei v eine diskrete, normierte Bewertung auf dem Körper K und π ein Primelement. Dann hat jedes $\alpha \in K^\times$ eine eindeutige Darstellung

$$\alpha = \pi^m u$$

mit $m \in \mathbb{Z}$ und einer Einheit $u \in \mathcal{O}^\times$.

Satz 6.1.11 Sei v eine diskrete Bewertung auf K . Dann ist $\mathcal{O} = \{\alpha \in K \mid v(\alpha) > 0\}$ ein Hauptidealring. Sei v zusätzlich normiert und π ein Primelement. Dann sind die von 0 verschiedenen Ideale gegeben durch

$$\mathfrak{p}^n = \pi^n \mathcal{O} = \{\alpha \in K \mid v(\alpha) > n\}, \quad n \in \mathbb{Z}_{\geq 0}.$$

Für alle $n \in \mathbb{Z}_{\geq 0}$ gilt:

$$\mathfrak{p}^n / \mathfrak{p}^{n+1} \simeq \mathcal{O} / \mathfrak{p}.$$