Protokoll zur Vorlesung Algebraische Zahlentheorie WS 23/24

W. Bley

5. Februar 2024

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 Einheitengruppe $\mathcal{O}_K^\times$.

Satz 1.1.4 *(Dirichletscher Einheitensatz) Sei K ein Zahlkörper. Dann ist $\mathcal{O}_K^\times$ eine endlich erzeugte abelsche Gruppe. Insbesondere also $\mathcal{O}_K^\times \simeq \left(\mathcal{O}_K^\times\right)_{tors} \times \mathbb{Z}^r$.*
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 Geleichung $p = x^2 + 6y^2$ sind wir auf das Phänomen gestoßen, dass Ganzheitsringe im allgemeinen keine Hauptidealringe sind. Wir werden im Rahmen der Vorlesung die sogenannte Idealklassengruppe

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

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

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

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:

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

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

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 $b_1, \ldots, b_n \in B$. Dann gilt:*

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

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: $L = \mathrm{Quot}(B)$. 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 $\beta \in L$:*

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

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

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

die lineare Abbildung Multiplikation mit α.

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

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

Dann gilt: $\mathrm{Tr}_{L/K}(\alpha) = a_1, \mathrm{N}_{L/K}(\alpha) = a_n$.
b) $\mathrm{Tr}_{L/K}$ ist K-linear.
c) $\mathrm{N}_{\mathrm{L/K}}$ 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) $\mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha)$.
c) $\mathrm{N}_{L/K}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha)$.

Folgerung 1.2.12 *Sei $K \subseteq L \subseteq M$ ein Turm von endlichen separablen Körpererweiterungen. Dann gilt:*
a) $\mathrm{Tr}_{M/K}(\alpha) = \mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(\alpha))$.
b) $\mathrm{N}_{M/K}(\alpha) = \mathrm{N}_{L/K}(\mathrm{N}_{M/L}(\alpha))$.

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

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

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

Lemma 1.2.14 *Es gilt:*
a)

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

b) Für $\theta \in L$ gilt:

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

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

Satz 1.2.15 *Sei L/K eine endliche separable Körpererweiterung und seien $\alpha_1, \ldots, \alpha_n \in L$. Dann gilt:*
a) $\alpha_1, \ldots, \alpha_n$ ist K-Basis von $L \iff d(\alpha_1, \ldots, \alpha_n) \neq 0$.
b) Die Abbildung $L \times L \longrightarrow K, (x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$, 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: $\mathrm{Tr}_{L/K}(b), \mathrm{N}_{L/K}(b) \in A$.
b) Für $b \in B$ gilt:

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

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

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

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 $\alpha_1, \ldots, \alpha_n \in B$, so dass*

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

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 $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_L$ eine Ganzheitsbasis. Dann nennt man

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

die Diskriminante von L/K.

Man beachte, dass diese Bildung unabhängig von der Wahl der Ganzheitsbasis ist.
Allgemeiner definieren wir eine Diskriminante für beliebige endliche erzeugte $\mathcal{O}_L$-Teilmoduln $M \neq 0$ von L.

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

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

die Diskriminante von M.

Satz 1.2.22 *Sei $L/\mathbb{Q}$ 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 $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_L$ eine $\mathbb{Q}$-Basis von L und $d(\alpha_1, \ldots, \alpha_n)$ sei quadratfrei. Dann ist $\alpha_1, \ldots, \alpha_n$ 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

$$M_1 \subseteq M_2 \subseteq \ldots$$

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 Definiton 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*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r \tag{1}$$

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 $\mathfrak{p}_1, \ldots \mathfrak{p}_s$, $s \leq r$, $e_i \in \mathbb{Z}_{>0}$, so gilt auch

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

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

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

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:*

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

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) $\mathrm{cl}_{\mathcal{O}} := J_{\mathcal{O}}/P_{\mathcal{O}}$ 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 $\mathrm{cl}_K := \mathrm{cl}_{\mathcal{O}_K}$ zu beweisen, falls K ein Zahlkörper ist.

Satz 1.3.13 *Sei $0 \neq \mathfrak{m} \subseteq \mathcal{O}$ ein ganzes Ideal. Dann gibt es in jeder Idealklasse $c \in \mathrm{cl}_{\mathcal{O}}$ 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 1.3.14 *Jedes Ideal eines Dedekindrings $\mathcal{O}$ läßt sich durch zwei Elemente erzeugen.*

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

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

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

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

heißt Grundmasche von Γ bezüglich der Basis $v_1, \ldots, v_m$. 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

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

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

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

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:*

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

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

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 Vekrorraum V, $n = \dim_{\mathbb{R}}(V)$. Sei $X \subseteq V$ zentral-symmetrisch, konvex und es gelte*

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

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

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

die reellen Einbettungen und

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

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*

$$\begin{aligned} f\colon K_{\mathbb{R}} &\longrightarrow \prod_{\tau} \mathbb{R} = \mathbb{R}^{s+2s}, \\ (z_\tau)_\tau &\mapsto (z_{\rho_1}, \ldots, z_{\rho_1}, \mathrm{Re}(z_{\sigma_1}), \mathrm{Im}(z_{\sigma_1}), \ldots, \mathrm{Re}(z_{\sigma_s}), \mathrm{Im}(z_{\sigma_s})), \end{aligned}$$

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

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

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

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

Hieraus folgt unmittelbar der Zusammenhang $\mathrm{Vol}_{(\ ,\ )} = 2^s \mathrm{Vol}_{\mathcal{L}}$, wobei letzteres das Lebesgue-Volumen bezeichnet.
Wir betrachten nun die sogenannte Minkowsi-Abbildung

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

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

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

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

Satz 2.2.4 *Sei $0 \neq \mathfrak{a} \lhd \mathcal{O}_K$ 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:*

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

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

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

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

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

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

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 $0 \neq \mathfrak{a} \lhd \mathcal{O}_K$ ein $0 \neq a \in \mathfrak{a}$ mit der Eigenschaft

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

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

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

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

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

3 Der Dirichletsche Einheitensatz

3.1 Der Dirichletsche Einheitensatz und sein Beweis

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

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

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

$$\begin{aligned} N\colon K_{\mathbb{R}}^{\times} &\longrightarrow \mathbb{R}^{\times}, \quad N(x) = \prod_{\tau\colon K \hookrightarrow \mathbf{C}} x_\tau, \\ T\colon \mathbb{R}^{r+s} &\longrightarrow \mathbb{R}, \quad T((x_\tau)) = \sum_{\tau} x_\tau. \end{aligned}$$

Man beachte, dass sich in der Definition von T die Summe über alle $\tau \in \{\rho_1, \ldots, \rho_r, \sigma_1, \ldots, \sigma_s\}$ erstreckt.
Dann kommutiert das folgende Diagramm

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

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 $\dim_{\mathbb{R}}(H) = r + s$.

Satz 3.1.1 *Die Gruppe der Einheitswuzeln 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 $\Gamma \simeq \mathbb{Z}^{r+s-1}$.*

Also 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 $\varepsilon_1, \ldots, \varepsilon_t$, so dass*

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

Man nennt dann $\varepsilon_1, \ldots, \varepsilon_t$ ein System von Fundamentaleinheiten.

3.2 Berechnung der Fundamentaleinheit 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 Pellschen Gleichung $x^2 - dy^2 = \pm 4$. Explizit:*

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

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

Falls ε die normalisierte Fundamentaleinheit ist, so ist $\{\pm\varepsilon, \pm\varepsilon^{-1}\}$ genau die Menge aller Fundamentaleinheiten. 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 Fundamentaleinheit, 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 Fundamentaleinheit derjenigen Lösung (x, y) der Pellschen Gleichung mit minimalem $x > 1$.

3.3 Der Regulator

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

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

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

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

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 $(\lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_t))$ ist.

Definition 3.3.2 R_K nennt man den Regulator von K.

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

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

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

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

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

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

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

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 $\mathfrak{p} \lhd \mathcal{O}_K$ 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

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

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

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

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 $i = 1, \ldots, r$.

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 Zahlkörperweiterung 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 $d(\omega_1, \ldots, \omega_n)$, wobei $\omega_1, \ldots, \omega_n$ alle in $\mathcal{O}_L$ gelegenenen 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 $G := \mathrm{Gal}(L/K)$. In dieser Situation wirkt G in natürlicher Weise auf die arithmetischen Objekte, die wir bislang untersucht haben, wie zum Beispiel $\mathcal{O}_L, I_L, \mu_L, \mathcal{O}_L^\times, \mathrm{cl}_L$.
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 $\mathfrak{P}$.

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) $G_{\mathfrak{P}} = 1 \iff Z_{\mathfrak{P}} = L \iff \mathfrak{p}$ *ist voll zerlegt.*
c) $G_{\mathfrak{P}} = G \iff Z_{\mathfrak{P}} = K \iff \mathfrak{p}$ *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*

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

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

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

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

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

Definition 4.3.7 Der Kern des surjektiven Homomorphismus $\mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})), \sigma \mapsto \bar{\sigma}$, 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 Verweigungsindex $e = e(\mathfrak{P}/\mathfrak{p})$ 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:

$$e(\mathfrak{P}_Z/\mathfrak{p}) = e(\mathfrak{P}_T/\mathfrak{P}_Z) = 1, \quad e(\mathfrak{P}/\mathfrak{P}_T) = e,$$
$$f(\mathfrak{P}_Z/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{P}_T) = 1, \quad f(\mathfrak{P}_T/\mathfrak{P}_Z) = f.$$

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

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

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 $p \neq 2$ ist genau dann voll zerlegt in $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, wenn $p \equiv 1 \pmod{n}$ gilt.*

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

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

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

$$f = a_0 + a_1 p + a_2 p^2 + \ldots + a_{n-1} p^{n-1}$$

mit eindeutg 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*

$$a \equiv a_0 + a_1 p + a_2 p^2 + \ldots + a_{n-1} p^{n-1} \pmod{p^n}$$

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 projecktive 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) $\mathrm{Quot}(\mathbb{Z}_p) = \mathbb{Q}_p$.

5.3 p-adische Komplettierung

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 $\mathfrak{m} \lhd R$ 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 $|\ |_p$ 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 definert man

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

Satz 5.3.2 *$\mathbb{Q}_p$ ist bezüglich $|\ |_p$ 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: $\mathbb{Z}_p^{\times} = \{\alpha \in \mathbb{Q}_p \mid |x|_p = 1\} = \{\alpha \in \mathbb{Q}_p \mid v_p(x) = 0\}$.*
b) Jedes $\alpha \in \mathbb{Q}_p$ hat eine eindeutige Dartstellung $\alpha = p^m\eta$ 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 $|\ |: K \longrightarrow \mathbb{R}$, so dass für alle $x, y \in K$ gilt

$$\begin{aligned}
&(i) && |x| \geq 0 \text{ und } |x| = 0 \iff x = 0,\\
&(ii) && |xy| = |x||y|,\\
&(iii) && |x + y| \leq |x| + |y|.
\end{aligned}$$

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

Satz 6.1.1 *Seien* $|\ |_1$ *und* $|\ |_2$ *zwei Beträge auf dem Körper* K*. Dann sind folgende Aussagen äquivalent:*
(a) $|\ |_1$ *und* $|\ |_2$ *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* $|\ |_1, \ldots, |\ |_n$ *paarweise inäquivalente Beträge von* K *und* $a_1, \ldots, a_n \in K$*. Dann gibt es zu jedem* $\varepsilon > 0$ *ein* $x \in K$*, so dass für alle* $i = 1, \ldots, n$ *gilt:*

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

Wir erinnern an die folgende Definition.

Definition 6.1.3 Ein Betrag $|\ |$ 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* $|\ |$ *ein Betrag auf dem Körper* K*. Dann gilt:*

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

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* $|\ |$ *auf* K *äquivalent zu* $|\ |_{\mathfrak{p}}$ *für ein Primideal* $\mathfrak{p} \neq 0$ *oder zu* $|\ |_\tau$ *für eine Einbettung* $\tau \colon K \hookrightarrow \mathbb{C}$*.*

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

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

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* $|\ |$ *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 eine 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:

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

6.2 Komplettierungen

Sei $(K, |\ |)$ ein Körper zusammen mit einem Betrag. Wie beim Übergang von $\mathbb{Q}$ nach $\mathbb{R}$ oder von $\mathbb{Q}$ nach $\mathbb{Q}_p$ kann man auch zu $(K, |\ |)$ die Komplettierung definieren. Wir bezeichnen die Komplettierung im Folgenden mit $\hat{K}$.
Wir konzentrieren uns im Weiteren auf den nicht-archimedischen Fall, und setzen daher ab jetzt voraus, dass $|\ |$ ein endlicher Betrag ist. Sei $0 \neq a \in \hat{K}$ repräsentiert durch die Cauchyfolge $(a_n)_n$ mit $a_n \in K$. Dann konvergiert $(|a_n|)_n$ und wir erhalten eine Fortsetzung von $|\ |$ auf $\hat{K}$ mittels

$$|a| := \lim_{n\to\infty} |a_n|.$$

Entsprechend erhalten wir eine zugehörige Bewertung $\hat{v}$ auf $K^\times$ durch

$$\hat{v}(a) := -\log|a| = \lim_{n\to\infty} v(a_n).$$

Sowohl $(|a_n|)_n$ als auch $(v(a_n))_n$ werden stationär. Die Wertebereiche von v und $\hat{v}$ stimmen daher überein. Falls also v diskret ist, so ist auch $\hat{v}$ diskret. Ebenso: Falls v diskret und normiert ist, so ist auch $\hat{v}$ diskret und normiert.

Satz 6.2.1 *Sei v eine normierte diskrete Bewertung auf K. Sei $\hat{K}$ die Komplettierung von K bezüglich v und $\hat{v}$ die Fortsetzung von v auf $\hat{K}$. Seien*

$$\mathcal{O} = \{x \in K \mid v(x) \geq 0\} \supseteq \mathfrak{p} = \{x \in K \mid v(x) > 0\},$$
$$\hat{\mathcal{O}} = \{x \in \hat{K} \mid \hat{v}(x) \geq 0\} \supseteq \hat{\mathfrak{p}} = \{x \in \hat{K} \mid \hat{v}(x) > 0\}$$

die zugehörigen Bewertungsringe mit ihren maximalen Idealen. Dann gilt für alle $n \geq 1$:

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

Im folgenden Satz bleiben wir in der Situation des letzten Satzes und verwenden die darin eingeführte Notation.

Satz 6.2.2 *Sei $R \subseteq \mathcal{O}$ ein Vertretersystem von $\mathcal{O}/\mathfrak{p}$ mit $0 \in R$. Sei $\pi \in \mathcal{O}$ ein Primelement. Dann hat jedes $\alpha \in \hat{K}^\times$ eine eindeutige Darstellung als konvergente Reihe*

$$\alpha = \pi^m \left(a_0 + a_1\pi + a_2\pi^2 + \ldots\right)$$

mit $m = \hat{v}(\alpha) \in \mathbb{Z}$, $a_i \in R$ und $a_0 \neq 0$.

6.3 Hensels Lemma

In diesem Abschnitt sei stets K ein bewerteter Körper, der bez. dem nicht-archimendischen Betrag $|\ |$ vollständig ist. Es sei $\mathcal{O}$ der zugehörige Bewertungsring und $\mathfrak{p}$ sein maximales Ideal. Es sei $k := \mathcal{O}/\mathfrak{p}$ der Restklassenkörper.
Unsere Standardbeispiele sind $\mathbb{Z}_p$ mit maximalem Ideal $p\mathbb{Z}_p$ und $k = \mathbb{F}_p$, oder allgemeiner, $\mathcal{O} = \mathcal{O}_{K_\mathfrak{p}}$, wobei hier K ein algebraischer Zahlkörper und $K_\mathfrak{p}$ seine Vervollständigung bezüglich dem $\mathfrak{p}$-adischen Betrag $|\ |_\mathfrak{p}$ ist. Hier gilt: $k = \mathcal{O}_K/\mathfrak{p}$ (bis auf kanonische Isomorphie).

Definition 6.3.1 Ein Polynom $f \in \mathcal{O}[x]$ heißt primitiv, falls $f \not\equiv 0 \pmod{\mathfrak{p}}$.

Satz 6.3.2 *(Hensels Lemma) Sei $f \in \mathcal{O}[x]$ primitiv. Falls f modulo $\mathfrak{p}$ eine Zerlegung*

$$f \equiv \bar{g}\bar{h} \pmod{\mathfrak{p}}$$

in teilerfremde Polynome $\bar{g}, \bar{h} \in k[x]$ hat, so hat f auch eine Zerlegung $f = gh$ mit Polynomen $f, g \in \mathcal{O}[x]$, so dass $\deg(g) = \deg(\bar{g})$ und

$$g \equiv \bar{g} \pmod{\mathfrak{p}}, \quad h \equiv \bar{h} \pmod{\mathfrak{p}}.$$

Folgerung 6.3.3 *Sei $f \in \mathcal{O}[x]$ primitiv und es gelte $(\bar{f}, \bar{f}') = 1$. Sei $a \in \mathcal{O}$ und es gelte $f(a) \equiv 0 \pmod{\mathfrak{p}}$. Dann gibt es ein $\alpha \in \mathcal{O}$ mit $f(\alpha) = 0$ und $\alpha \equiv a \pmod{\mathfrak{p}}$.*

Als direkte Konsequenz aus der Folgerung erhält man, dass die $(p-1)$-ten Einheitswurzeln μ_{p-1} in $\mathbb{Z}_p$ enthalten sind.

Sei nun K vollständig bezüglich des nicht-archimedischen Betrags $|\ |$. Sei

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0, \quad a_n \neq 0,$$

ein Polynom in $K[x]$. Dann definiert man: $|f| := \max\{|a_0|, \ldots, |a_n|\}$.

Folgerung 6.3.4 *Sei K vollständig bezüglich des nicht-archimedischen Betrags $|\ |$. Sei*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0, \quad a_n a_0 \neq 0,$$

ein irreduzibles Polynom in $K[x]$. Dann gilt: $|f| = \max\{|a_0|, |a_n|\}$.

Satz 6.3.5 *Sei K vollständig bezüglich des nicht-archimedischen Betrags $|\ |$ und L/K eine endliche Körpererweiterung vom Grad n. Dann besitzt $|\ |$ eine eindeutige Fortsetzung auf L. Diese ist für $\alpha \in L$ gegeben durch*

$$|\alpha| := \sqrt[n]{|\mathrm{N}_{L/K}(\alpha)|}.$$

Der Körper L ist mit diesem Betrag wieder vollständig.

Remark 6.3.6 In dieser Situation ist der Bewertungsring $\mathcal{O} := \{\alpha \in L \mid |\alpha| \leq 1\}$ der ganze Abschluss von $\{\alpha \in K \mid |\alpha| \leq 1\}$.

Satz 6.3.5 erlaubt es nun, den p-adischen Betrag auf den algebraischen Abschluss $\mathbb{Q}_p^c$ von $\mathbb{Q}_p$ fortzusetzen. Explizit wählt man für $\alpha \in \mathbb{Q}_p^c$ eine endliche Körpererweiterung $L/\mathbb{Q}_p$ mit $\alpha \in L$ und definiert

$$|\alpha|_p := \sqrt[[L:\mathbb{Q}_p]]{|\mathrm{N}_{L/\mathbb{Q}_p}(\alpha)|_p}.$$

Satz 6.3.7 *$(\mathbb{Q}_p^c, |\ |_p)$ ist nicht vollständig.*

Es sei nun $\mathbb{C}_p$ die Vervollständigung von $\mathbb{Q}_p^c$ bezüglich $|\ |_p$. Dann ist $\mathbb{C}_p$ algebraisch abgeschlossen. Wir wollen zeigen, dass $\mathbb{C}_p$ algebraisch abgeschlossen ist. Dazu benötigen wir zunächst Krasners Lemma.

Satz 6.3.8 *(Krasners Lemma) Sei K vollständig und nicht-archimedisch bezüglich dem Betrag $|\ |$. Seien $a, b \in K^c$ und sei a separabel über $K(b)$. Sei $P(x) \in K(b)[x]$ das Minimalpolynom von a. Für alle Nullstellen $a' \neq a$ von $P(x)$ gelte*

$$|b - a| < |a' - a|.$$

Dann gilt: $a \in K(b)$

Satz 6.3.9 *$\mathbb{C}_p$ ist algebraisch abgeschlossen.*

7 Lokale Körper

7.1 Grundlegendes

Definition 7.1.1 Ein lokaler (Zahl-)Körper ist eine endliche Erweiterung von $\mathbb{Q}_p$ für eine Primzahl p.

In der Literatur sind in der Regel lokale Körper die endlichen Erweiterungen von $\mathbb{Q}_p$ oder von $\mathbb{F}_q((t))$. Wir beschränken uns hier auf die Betrachtung endlicher Erweiterungen von $\mathbb{Q}_p$.

Satz 7.1.2 *Der Bewertungsring $\mathcal{O}$ eines lokalen Körpers K ist kompakt. Insbesondere ist K lokal kompakt.*

7.2 Die Struktur der multiplikativen Gruppe eines lokalen Körpers

Sei im Weiteren K stets ein lokaler Körper mit Bewertungsring $\mathcal{O} = \mathcal{O}_K$, maximalem Ideal $\mathfrak{p} = \mathfrak{p}_K$ und Primelement π. Es gilt also $\mathfrak{p} = \pi\mathcal{O}_K$. Weiter sei $q := |\mathcal{O}_K/\mathfrak{p}|$ die Ordnung des Restklassenkörpers. Mit $U_K^{(1)} := 1 + \mathfrak{p}_K \subseteq \mathcal{O}_K^\times$ bezeichnet man die Gruppe der Einseinheiten.
Wir wollen im Folgenden die Struktur der abelschen Gruppe $K^\times$ bestimmen. Ein erster Schritt hierzu ist folgendes Resultat.

Satz 7.2.1

$$K^\times = \pi^{\mathbb{Z}} \times \mu_{q-1} \times U_K^{(1)}.$$

Im Folgenden wollen wir die $\mathbb{Z}_p$-Modulstruktur der Einseinheiten $U_K^{(1)}$ studieren. Dazu definieren wir den p-adischen Logarithmus.

Satz 7.2.2 *Für einen p-adischen Zahlkörper K gibt es einen eindeutigen stetigen Homomorphismus*

$$\log\colon K^\times \longrightarrow K$$

mit $\log(p) = 0$ und

$$\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \ldots = -\sum_{\nu=1}^{\infty} (-1)^\nu \frac{x^\nu}{\nu}$$

für alle $x \in \mathfrak{p}_K$.

Remark 7.2.3 a) Für alle Einheitswurzeln ζ gilt $\log(\zeta) = 0$.
b) Schreibt man $\alpha = \pi^m \cdot \omega(\alpha) \cdot \langle\alpha\rangle$ mit $m = v_{\mathfrak{p}}(\alpha), \omega(\alpha) \in \mu_{q-1}$ und $\langle\alpha\rangle \in U_K^{(1)}$, so gilt

$$\log(\alpha) = m\log(\pi) + \log(\langle\alpha\rangle) \text{ mit } \log(\pi) = -\frac{1}{e}\log(\langle p\rangle).$$

Hierbei ist e der Verzweigungsindex, d.h. $p\mathcal{O}_K = \mathfrak{p}_K^e$.

Die Reihenentwicklung der Exponentialfunktion liefert formal eine Umkehrfunktion zum Logarithmus. Um die Konvergenz zu analysieren brauchen wir folgendes Lemma.

Lemma 7.2.4 *Sei ν eine natürliche Zahl und $\nu = \sum_{i=0}^{r} a_i p^i$ mit $0 \leq a_i < p$ ihre p-adische Entwicklung. Dann gilt:*

$$v_p(\nu!) = \frac{1}{p-1}\sum_{i=0}^{r} a_i(p^i - 1).$$

Satz 7.2.5 *Für einen p-adischen Zahlkörper K liefern die Potenzreihen*

$$\exp(x) = 1 + x + \frac{x^2}{2} + \frac{x^3}{3!} + \ldots = \sum_{\nu=0}^{\infty}\frac{x^\nu}{\nu!}$$

und

$$\log(1+z) = z - \frac{z^2}{2} + \frac{z^3}{3} - \ldots = -\sum_{\nu=1}^{\infty}(-1)^\nu\frac{z^\nu}{\nu}$$

für $n > \frac{e}{p-1}$ zueinander inverse Isomorphismen $U_K^{(n)} \simeq \mathfrak{p}_K^n$.

Satz 7.2.6 *Sei K ein p-adischer Zahlkörper und $q = \#\mathcal{O}_K/\mathfrak{p}_K$. Dann gilt:*

$$K^\times \simeq \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^d$$

mit $a \in \mathbb{Z}_{\geq 0}$ und $d = [K : \mathbb{Q}_p]$.

7.3 Erweiterungen p-adischer Zahlkörper

Sei L/K eine Erweiterung p-adischer Zahlkörper mit Restklassenkörpergrad f und Verzweigungsindex e. Dann gilt $ef = [L : K]$.

Definition 7.3.1 Wir nennen L/K voll verzweigt, falls $e = [L : K]$. Die Erweiterung heißt unverzweigt, falls $e = 1$,

Wir studieren zunächst die voll verzweigten Erweiterungen.
Ein Polynom

$$g(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0 \in \mathcal{O}_K[x]$$

ist ein Eisensteinpolynom, falls $a_0, \ldots, a_{m-1} \in \mathfrak{p}_K$ und $a_0 \notin \mathfrak{p}_K^2$. Eisensteinpolynome sind irreduzibel in $\mathcal{O}_K[x]$ und $K[x]$.

Satz 7.3.2
(1) Folgende Aussagen sind äquivalent:
(i) $L = K(\lambda)$, wobei λ Nullstelle eines Eisensteinpolynoms ist.
(ii) L/K ist voll verzweigt.
(iii) $\mathcal{O}_L = \mathcal{O}_K[\lambda]$ für jede (eine) Uniformisierende λ von L.
(2) Falls (i) erfüllt ist, so ist λ eine Uniformisierende und $\deg(g) = [L : K]$.
(3) Sei L/K voll verzweigt und π_L eine Uniformisierende in L. Dann ist das Minimalpolynom von π_L ein Eisensteinpolynom.

Wir kommen nun zum Studium der unverzweigten Erweiterungen.
Ab jetzt bezeichnen wir für einen p-adischer Zahlkörper M den Restklassenkörper $\mathcal{O}_M/\mathfrak{p}_M$ mit k_M.

Lemma 7.3.3 *Sei M/K eine Erweiterung p-adischer Zahlkörper. Sei m eine zu p teilerfremde natürliche Zahl. Dann sind die irreduziblen Faktoren $\bar{g}(x)$ von $x^m - 1$ in $k_M[x]$ genau die Reduktionen der irreduziblen Faktoren $g(x)$ von $x^m - 1$ in $M[x]$*

Als Konsequenz erhalten wir für $k = k_K$ die Gleichheit

$$[K(\mu_m) : K] = [k(\mu_m) : k].$$

Satz 7.3.4 *Sei K ein p-adischer Zahlkörper.*
(a) Zu jeder natürlichen Zahl f gibt es eine eindeutig bestimmte unverzweigte Erweiterung K_f/K mit $[K_f : K] = f$. Genauer gilt:

$$K_f = K(\mu_m) \text{ mit } m = q^f - 1,$$

wobei $q := |k|$.
(b) Sei L/K eine Erweiterung von p-adischen Zahlkörpern und $f = f(L/K)$. Dann gilt:
(i) $K \subseteq K_f \subseteq L$
(ii) L/K_f ist voll verzweigt.
(iii) K_f/K ist die maximal unverzweigte Teilerweiterung von L/K.

Im Rahmen des Beweises haben wir gezeigt:

Remark 7.3.5 (a) Sei L/K unverzweigt und K'/K beliebig (jedoch alles p-adische Zahlkörper). Dann ist auch LK'/K' unverzweigt.
(b) Das Kompositum von unverzweigten Erweiterungen ist wieder unverzweigt.

Zum Abschluss dieses Abschnittes studieren wir zahm verzweigte Erweiterungen.

Definition 7.3.6 Sei L/K eine Erweiterung p-adischer Zahlkörper. Dann heißt L/K zahm verzweigt, falls $p \nmid e = e(L/K)$.

Satz 7.3.7 *Sei L/K eine Erweiterung p-adischer Zahlkörper mit maximal unverzweigter Teilerweiterung T. Dann gilt:*

$$L/K \text{ ist zahm} \iff L = T(\sqrt[m_1]{a_1}, \ldots, (\sqrt[m_r]{a_r}),$$

mit $a_i \in T^\times$ und $p \nmid m_i$.

Zahm verzweigte Erweiterungen sind also Radikalerweiterungen von T, bzw. sogar von K, da ja $T = K(\mu_m)$ ebenfalls eine Radikalerweiterung ist.

Lemma 7.3.8 *Sei K ein p-adischer Zahlkörper, $u \in \mathcal{O}_K^\times$ und d eine natürliche Zahl mit $p \nmid d$. Dann ist $K(\sqrt[d]{u})/K$ unverzweigt.*

Folgerung 7.3.9 *Sei L/K eine zahm verzweigte Erweiterung p-adischer Zahlkörper und sei K'/K eine beliebige Erweiterung p-adischer Zahlkörper. Dann ist auch LK'/K' zahm verzweigt.*

Folgerung 7.3.10 *Seien L_1/K und L_2/K zahm verzweigte Erweiterungen p-adischer Zahlkörper. Dann ist auch L_1L_2/K zahm verzweigt.*

Den obigen Satz können wir verfeinern.

Satz 7.3.11 *Sei L/K eine zahm und voll verzweigte Erweiterung p-adischer Zahlkörper mit Verzweigungsindex e, d.h. $p \nmid e = [L : K]$. Dann gibt es ein Primelement π von K und ein Primelement π_L von L, so dass π_L Nullstelle von $x^e - \pi$ ist.*

Quelle des Beweises ist das folgende Lemma, das wiederum mit Krasners Lemma bewiesen wird.

Lemma 7.3.12 *Sei E/K eine voll verzweigte Erweiterung p-adischer Zahlkörper und $m \in \mathbb{N}$ teilerfremd zu p. Sei π_0 ein Primelement in K und $\beta \in E$ erfülle $|\beta|^m = |\pi_0|$. Dann gibt es ein Primelement π in K, so dass eine Nullstelle von $x^m - \pi$ in $K(\beta)$ enthalten ist.*

7.4 Ein Beispiel

Die Erweiterungen $\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p$ sind voll verzweigt vom Grad $p^{m-1}(p-1)$ mit Primelement $1-\zeta_{p^n}$, siehe Aufgabe 4, Blatt 12. Die Erweiterung ist genau dann zahm verzweigt, wenn $m = 1$ gilt.
Im Gegensatz hierzu sind die Erweiterungen $\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p$ für $p \nmid n$ unverzweigt. Hier gilt allgemeiner:

Satz 7.4.1 *Sei K ein p-adischer Zahlkörper und $L = K(\zeta_n)$ mit $p \nmid n$. Es sei $q = |k| = |\mathcal{O}_K/\mathfrak{p}_K|$ die Ordnung des Restklassenkörpers von K. Dann gilt:*
(i) L/K ist unverzweigt vom Grad f, wobei f die kleinste natürliche Zahl ist mit der Eigenschaft $q^f \equiv 1 \pmod{n}$.
(ii) $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(k_L/k)$, *insbesondere ist L/K also zyklisch.*
(iii) $\mathrm{Gal}(L/K)$ *wird erzeugt von $\varphi\colon \zeta_n \mapsto \zeta_n^q$.*
(iv) $\mathcal{O}_L = \mathcal{O}_K[\zeta_n]$.

8 Kummertheorie

8.1 Grundlegende Definitionen und Resultate

Sei F ein beliebiger Körper und n eine natürliche Zahl. Die Kummertheorie verfolgt das Ziel, alle abelschen Erweiterungen K/F vom Exponenten n durch Daten im Grundkörper F zu beschreiben. Dies gelingt in elementarer Art und Weise, falls eine primitive n-te Einheitswurzel in F enthalten ist.
Die Verallgemeinerung der Kummertheorie ist die sogenannte Klassenkörpertheorie, die die abelschen Erweiterungen von F durch Daten in F beschreibt und ohne die einschränkenden Bedingungen

- F enthält eine primitive n-te Einheitswurzel,
- $\exp(Gal(K/F))$ teilt n

auskommt. Die Klassenkörpertheorie ist Inhalt der Zahlentheorie II im kommenden Sommersemester.

Proposition 8.1.1 *Sei F ein Körper, der eine primitive n-te Einheitswurzel ω enthält. Insbesondere ist also $(n, \mathrm{char}(F)) = 1$.*
a) Sei $a \in F^\times$ und $K = F(\sqrt[n]{a})$. Dann ist K/F zyklisch, wobei $m := [K : F]$ die Ordnung von a in $F^\times/F^{\times n}$ ist. Insbesondere gilt also $m \mid n$.
b) Sei K/F zyklisch vom Grad n. Dann gibt es ein Element $a \in F^\times$ der Ordnung n in $F^\times/F^{\times n}$, so dass $K = F(\sqrt[n]{a})$ gilt.

Die Quelle des Beweises zu b) ist Hilberts Satz 90.

Definition 8.1.2 Eine endliche Galoiserweiterung K/F heißt n-Kummererweiterung, falls F eine primitive n-te Einheitswurzel enthält und $\mathrm{Gal}(K/F)$ abelsch mit $\exp(\mathrm{Gal}(K/F)) \mid n$ ist.

Proposition 8.1.3 *Der Körper F enthalte eine primitive n-te Einheitswurzel. Dann sind folgende Aussagen äquivalent:*
1) K/F ist n-kummersch.
2) Es gibt $a_1, \ldots, a_r \in F^\times$, so dass $K = F(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_r})$.

8.2 Die Kummerpaarung

Definition 8.2.1 Sei G eine endliche abelsche Gruppe. Dann nennt man $\hat{G} := \mathrm{Hom}(G, \mathbb{C}^\times)$ die Gruppe der (linearen) Charaktere von G.

Lemma 8.2.2 *(a) Es gibt einen (nicht-kanonischen) Isomorphismus $G \simeq \hat{G}$.*
(b) G und $\hat{\hat{G}}$ sind kanonisch isomorph.

Definition 8.2.3 Seien G_1, G_2 und C abelsche Gruppen. Sei $B\colon G_1 \times G_2 \longrightarrow C$ eine bilineare Abbildung. Dann nennt man B eine nicht-ausgeartete oder perfekte Paarung, wenn B in jedem Argument nicht ausgeartet ist, d.h.

$$B(g_1, g_2) = 1, \forall g_2 \in G_2 \implies g_1 = 1,$$
$$B(g_1, g_2) = 1, \forall g_1 \in G_1 \implies g_2 = 1.$$

Lemma 8.2.4 *Seien G_1 und G_2 abelsche Gruppen von endlichem Exponenten und C endlich zyklisch mit $\exp(G_i) \mid |C|$, $i = 1, 2$. Sei $B\colon G_1 \times G_2 \longrightarrow C$ eine perfekte Paarung. Sei G_1 oder G_2 endlich. Dann sind G_1 und G_2 endlich und B induziert Isomorphismen $G_1 \simeq Hom(G_2, C)$ und $G_2 \simeq Hom(G_1, C)$. Ferner ist $G_1 \simeq G_2$ (nicht-kanonisch).*

Wir wenden diese allgemeinen Sachverhalte nun im Rahmen der Kummertheorie an. Im Folgenden sei K/F eine n-Kummererweiterung.

Definition 8.2.5 Die Abbildung

$$\begin{aligned} B\colon \mathrm{Gal}(F/K) \times (F^\times \cap K^{\times,n})/F^{\times n} &\longrightarrow \mu_n, \\ (\sigma, a \bmod F^{\times n}) &\mapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}, \end{aligned}$$

heißt Kummerpaarung.

Satz 8.2.6 *Die Kummerpaarung ist wohldefiniert, bilinear und perfekt. Falls $K = F(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_r})$, so gilt*

$$(F^\times \cap K^{\times n})/F^{\times n} = \langle a_1 \bmod F^{\times n}, \ldots, a_r \bmod F^{\times n} \rangle.$$

Insbesondere hat man einen (nicht-kanonischen) Isomorphismus

$$\mathrm{Gal}(K/F) \simeq \langle a_1 \bmod F^{\times n}, \ldots, a_r \bmod F^{\times n} \rangle.$$

Zusammenfassend formulieren wir den Hauptsatz der Kummertheorie.

Satz 8.2.7 *Sei F ein Körper, der eine primitive n-te Einheitswurzel enthält. Sei F^c ein algebraischer Abschluss von F. Dann hat man eine ordnungerhaltende $1-1$-Korrespondenz*

$$\begin{aligned} n - \text{Kummererweiterungen } K/F \text{ mit } K \subseteq F^c &\longrightarrow \text{endliche Untergruppen } W \text{ von } F^\times/F^{\times n}, \\ K &\mapsto (F^\times \cap K^{\times n})/F^{\times n}, \\ F(\sqrt[n]{W}) &\leftarrow W \end{aligned}$$

Wenn K zu W korrespondiert, so ist die Kummerpaarung

$$\mathrm{Gal}(K/F) \times W \longrightarrow \mu_n$$

perfekt, insbesondere $\mathrm{Gal}(K/F) \simeq W$ (nicht-kanonisch).

Anwendung: Wenn nun F ein p-adischer Zahlkörper mit $\mu_n \subseteq F$ ist, so folgt aus der Endlichkeit von $F^\times/F^{\times n}$, dass es zu F nur endlich viele endliche abelsche Erweiterungen K/F gibt mit $exp(\mathrm{Gal}(K/F)) \mid n$.

8.3 Höhere Verzweigungsgruppen

In diesem Abschnitt ist K/F stets eine galoissche Erweiterung von p-adischen Zahlkörpern mit $G := \mathrm{Gal}(K/F)$.

Definition 8.3.1 Sei $s \geq 1$ eine ganze Zahl. Dann heißt

$$G_s = G_s(K/F) := \{\sigma \in G \mid \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{p}_K^{s+1}}, \forall \alpha \in \mathcal{O}_K\}$$

s-te (höhere) Verzweigungsgruppe.

Remark 8.3.2
(a) Es ist $G_{-1} = G$ und $G_0 = I(K/F)$ die bereits bekannte Verzweigungsgruppe.
(b) Für $s \geq 0$ gilt $G_s(F/K) = G_s(F/K_0)$, wobei $K_0 := K^{G_0}$. Daher kann man bei der Betrachtung der höheren Verzweigungsgruppen meist oE voraussetzten, dass F/K voll verzweigt ist.

Lemma 8.3.3
(a) Für alle $s \geq -1$ ist G_s ein Normalteiler in G.
(b) Für alle $s \geq 0$ gilt $G_s \leq G_{s-1}$.

Lemma 8.3.4 *Sei π_K ein Primelement in K. Dann gilt für alle ganzen Zahlen $s \geq -1$*

$$G_s(K/F) = \{\sigma \in G \mid \sigma(\pi_K) \equiv \pi_K \pmod{\mathfrak{p}_K^{s+1}}\}$$

Insbesondere ist $G_s(K/F) = 1$ für alle s mit $s + 1 > \max\limits_{\sigma \neq 1}\{\sigma(\pi_K) - \pi_K\}$.

Wir wollem im Folgenden zeigen, dass die Kompositionsreihe

$$G = G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \ldots \supseteq G_t = 1$$

abelsche Faktoren hat.

Lemma 8.3.5 *Sei K ein p-adischer Zahlkörper und $U_K^{(n)}$ für $n \in \mathbb{Z}_{\geq 0}$ die Gruppe der Einseinheiten n-ter Stufe. Dann gilt:*

$$\begin{aligned} U_K^{(0)}/U_K^{(1)} &\simeq k_K^\times, \\ U_K^{(n)}/U_K^{(n+1)} &\simeq k_K \text{ for } n \geq 0. \end{aligned}$$

Der nächste Satz zeigt, dass die Faktoren der obigen Kompositionsreihe abelsch sind.

Satz 8.3.6 *Sei K/F eine Galoiserweiterung von p-adischen Zahlkörpern mit Gruppe G. Sei π_K ein Primelement in K und $s \geq 0$. Dann induziert die Abbildung*

$$\varphi\colon G_s \longrightarrow U_K^{(s)}/U_K^{(s+1)}, \quad \sigma \mapsto \frac{\sigma(\pi_K)}{\pi_K} \cdot U_K^{(s+1)}$$

einen wohldefinierten, injektiven Gruppenhomomorphismus

$$G_s/G_{s+1} \hookrightarrow U_K^{(s)}/U_K^{(s+1)}.$$

Hieraus liest man ab:

Satz 8.3.7 *Sei K/F eine Galoiserweiterung von p-adischen Zahlkörpern mit Gruppe G. Dann gilt:*
(a) G ist auflösbar.
(b) Die eindeutig bestimmte p-Sylowuntergruppe von G_0 ist gegeben durch G_1.
(c) G_0/G_1 ist abelsch von zu p teilerfremder Ordnung. Genauer: $|G_0/G_1|$ teilt $|k_K| - 1$.
(d) Für $s \geq 1$ ist jeder der Faktoren G_s/G_{s+1} eine p-elementar-abelsche Gruppe.

8.4 Endlichkeit der Anzahl der Erweiterungen von F von beschränktem Grad

Satz 8.4.1 *Sei $F/\mathbb{Q}_p$ ein p-adischer Zahlkörper, $n \geq 1$ eine ganze Zahl und F^c ein algebraischer Abschluss von F. Dann gibt es in F^c/F nur endlich viele Galoiserweiterungen K/F, so dass $[K : F]$ ein Teiler von n ist.*

Folgerung 8.4.2 *Sei $F/\mathbb{Q}_p$ ein p-adischer Zahlkörper, $m \geq 1$ eine ganze Zahl und F^c ein algebraischer Abschluss von F. Dann gibt es in F^c/F nur endlich viele Erweiterungen K/F mit $[K : F] \leq m$.*

ENDE