Zahlentheorie

Manuel Kauers
nach einer Vorlesung von
Prof. Dr. C.-G. Schmidt

16. August 2002

Inhaltsverzeichnis

1 Einführende Beispiele

Bsp. Diophantische Probleme: Suche zu vorgegebenen Gleichungen ganzzahlige Lösungen.

- PELLsche Gleichung

$$X^2 - aY^2 = \pm 1$$

($a \in \mathbb{N}$ kein Quadrat), auch behandelt von BRAHMEGUPTA. Eine Lösung stammt von BHASCAVA. Demnach existiert eine kleinste Lösung $(x_0, y_0) \in \mathbb{Z}^2$, aus der sich systematisch alle weiteren ableiten lassen.

Für $a = 2$ ist etwa $x_0 = y_0 = 1$ und die Menge aller Lösungen ist gegeben durch

$$\{(x, y) \in \mathbb{Z}^2 : \exists\, n \in \mathbb{Z} : x + y\sqrt{2} = (1 + \sqrt{2})^n\}.$$

Für $a = 109$ ist nach FERMAT die kleinste Lösung des Problems gegeben durch

$$(x_0, y_0) = (158\,070\,671\,986\,249, 15\,140\,424\,455\,100).$$

- Pythagoräische Zahlentrippel: Finde Lösungen $(x, y, z) \in \mathbb{Z}^3$ der Gleichung $x^2 + y^2 = z^2$. EUKLID und DIOPHANTOS charakterisieren durch

$$\{(m(s^2 - r^2), 2mrs, m(s^2 + r^2)) : m, r, s \in \mathbb{Z}\}$$

alle Lösungen.

- FERMAT-Gleichung: Finde Lösungen $(x, y, z) \in \mathbb{Z}^3$ der Gleichung

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

FERMATS Vermutung von 1637, daß diese Gleichung für $n \geq 3$ keine nichttrivialen Lösungen hat, wurde 1994 von WILES bestätigt.

- Kongruenzzahlen: Welche natürlichen Zahlen n treten als Flächeninhalt von rechtwinkligen Dreiecken mit rationalen Seitenlängen auf? Besitzt für $n \in \mathbb{N}$ die Gleichung

$$E_n : y^2 = x^3 - n^2 x$$

eine Lösung in $\mathbb{Q}$ mit $y \neq 0$?. Die reellen Lösungen von E_n definieren eine *elliptische Kurve*, deren rationale Punkte nach MORELL eine endliche erzeugte ABELsche Gruppe bilden.

2 Algebraische Zahlen

Def. 1 Der Ring

$$\mathbb{Z}[\mathrm{i}] := \{a \cdot 1 + b \cdot \mathrm{i} \in \mathbb{C} : a, b \in \mathbb{Z}\}$$

heißt Ring der GAUSSschen Zahlen.

Satz 1 $\mathbb{Z}[\mathrm{i}]$ ist euklidisch und faktoriell. Es gilt $\mathbb{Z}[\mathrm{i}]^\times = \{\pm 1, \pm \mathrm{i}\} = \langle i \rangle$.

Satz 2 Sei $p \in \mathbb{N}$ prim, $p \neq 2$. Dann gilt:

$$\Big(\exists\, a, b \in \mathbb{N} : \quad p = a^2 + b^2\Big) \quad \Longleftrightarrow \quad p \equiv 1 \bmod 4$$

Satz 3

1. Ein Vertretersystem $\mathbb{P}$ der Primelemente von $\mathbb{Z}[\mathrm{i}]$ is durch folgende Elemente gegeben:

   (a) $\pi = 1 + \mathrm{i}$,

   (b) $\pi = a + b\mathrm{i}$ mit $a^2 + b^2$ prim und $a > |b| > 0$,

   (c) $\pi = p$ mit p prim in $\mathbb{Z}$ und $p \equiv 3(4)$.

2. (Zerlegungsgesetz für Primzahlen) Für $p \in \mathbb{Z}$ prim gilt in $\mathbb{Z}[i]$: $2 \sim \pi_2^2$ oder $p \sim \pi_p \bar{\pi}_p$ $(p \equiv 1(4))$ oder $p \sim \pi_p$ $(p \equiv 3(4))$.

Bem. Die GAUSSschen Zahlen spielen in $\mathbb{Q}(\mathrm{i})$ die Rolle der ganzen Zahlen, ähnlich der Rolle von $\mathbb{Z}$ in $\mathbb{Q}$. Sie besitzen eine koordinatenfreie Charakterisierung innerhalb des Körpers $\mathbb{Q}(\mathrm{i})$.

Satz 4 Für $x \in \mathbb{Q}(\mathrm{i})$ gilt

$$x \in \mathbb{Z}[\mathrm{i}] \qquad \Longleftrightarrow \qquad \exists\, a, b \in \mathbb{Z} : \quad x^2 + ax + b = 0.$$

Def. 2 Ein Körper $K \supseteq \mathbb{Q}$ heißt (*algebraischer*) *Zahlkörper*, falls die Erweiterung $K/\mathbb{Q}$ endlich ist, d.h. $\dim_{\mathbb{Q}} K < \infty$. Die Elemente eines algebraischen Zahlkörpers heißen *algebraische Zahlen*.

Def. 3 Sei $A \leq B$ Ringerweiterung und $b \in B$. b heißt *ganz* über A, falls b Nullstelle eines normierten Polynoms

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-1} \in A[X]$$

ist. B heißt *ganze* Ringerweiterung von A, falls alle $b \in B$ ganz über A sind.

Satz 5 Seien $b_1, \ldots, b_n \in B$. Dann gilt: $b_1, \ldots, b_n$ sind genau dann ganz über A, wenn $A[b_1, \ldots, b_n]$ endlich erzeugter A-Modul ist.

Bem.

- Sind $b_1, \ldots, b_n$ ganz über A, dann ist jedes $b \in A[b_1, \ldots, b_n]$ ganz über A, insbesondere sind $b_1 + b_2$ und $b_1 \cdot b_2$ ganz über A.
- Seien $A \leq B \leq C$ Ringerweiterungen. Dan gilt: Ist B ganz über A und C ganz über B, dann ist C auch ganz über A.

Def. 4 Der Teilring

$$\overline{A} = \{b \in B : b \text{ ist ganz über } A\} \subseteq B$$

heißt der *ganze Abschluß* von A. A heißt *ganzabgeschlossen* in B im Fall $A = \overline{A}$. Ist A ein Integritätsbereich mit Quotientenkörper $K = \mathrm{Quot}(A)$, so heißt der ganze Abschluß $\overline{A}$ von A in K die *Normalisierung* von A.

Bem.

- Faktorielle Ringe sind stets ganzabgeschlossen.

- Sei A ganzabgeschlossener Integritätsbereich, $K = \mathrm{Quot}(A)$. Ferner sei L/K eine endliche Körpererweiterung, d. h. $\dim_K L < \infty$, und B der ganze Abschluß von A in L. Dann ist B ganzabgeschlossen, jedes Element $\beta \in L$ hat die Form $\beta = \frac{b}{a}$ mit $b \in B$ und $a \in A$, und für $\beta \in L$ gilt: β ist genau dann ganz über A, wenn das Minimalpolynom von β in $A[X]$ liegt.

Def. 5 Zu $x \in L$ sei $T_x : L \to L : \alpha \mapsto x \cdot \alpha$. Dann heißt

$$\mathrm{Tr}_{L/K} : L \to K, \qquad \mathrm{Tr}_{L/K}(x) := \mathrm{Tr}(T_x)$$

die *Spur* und

$$\mathcal{N}_{L/K} : L \to K, \qquad \mathcal{N}_{L/K}(x) := \mathcal{N}(T_x) = \det T_x$$

die *Norm* von L über K. Dabei seien $\mathrm{Tr}(T_x)$ und $\mathcal{N}(T_x)$ die Koeffizienten a_1 bzw. a_n des charakteristischen Polynoms $g_x(t) = \det(t\,\mathrm{id} - T_x)$.

Bem. Wegen $T_{x+y} = T_x + T_y$ und $T_{xy} = T_x \circ T_y$ sind Spur und Norm Homomorphismen der additiven Gruppe L und der multiplikativen Gruppe $L^\times$.

Satz 6 L/K sei separabel. Durchläuft $\sigma : L \hookrightarrow \bar{K}$ die verschiedenen K-Einbettungen von L im algebraischen Abschluß $\bar{K}$ von K, so gelten:

1. $g_x(t) = \prod_\sigma (t - \sigma(x))$,
2. $\mathrm{Tr}_{L/K}(x) = \sum_\sigma \sigma(x)$,
3. $\mathcal{N}_{L/K}(x) = \prod_\sigma \sigma(x)$.

Bem. Für einen Körperturm $M/L/K$ von endlichen Erweiterungen gilt

$$\mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L} = \mathrm{Tr}_{M/K}, \qquad \mathcal{N}_{L/K} \circ \mathcal{N}_{M/L} = \mathcal{N}_{M/K}.$$

Def. 6 Sei $\alpha_1, \ldots, \alpha_n$ die Basis einer separablen Körpererweiterung L/K. Dann heißt

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

die *Diskriminante* dieser Basis.

Satz 7 Sei L/K separabel.

1. Durch
$$\langle \cdot, \cdot \rangle : L \times L \to K, \qquad \langle x, y \rangle := \mathrm{Tr}_{L/K}(xy)$$
wird eine nichttriviale K-Bilinearform auf L erklärt.
2. Ist $\alpha_1, \ldots, \alpha_n$ eine K-Basis von L, so ist $d(\alpha_1, \ldots, \alpha_n) \neq 0$.

Bem. Sei A ein ganzabgeschlossener integrer Ring, $K = \mathrm{Quot}(A)$, L/K eine separable Körpererweiterung und B der ganze Abschluß von A in L. Dann gilt für $x \in B$:

- $\mathrm{Tr}_{L/K}(x), \mathcal{N}_{L/K}(x) \in A$,
- $x \in B^\times \iff \mathcal{N}_{L/K}(x) \in A^\times$.

Satz 8 Seien $\alpha_1, \ldots, \alpha_n \in B$ eine K-Basis von L und $d = d(\alpha_1, \ldots, \alpha_n)$. Dann gilt

$$dB \subseteq A\alpha_1 + \cdots + A\alpha_n.$$

Def. 7 Ein System $\omega_1, \ldots, \omega_n \in B$ heißt Ganzheitsbasis von L über A, wenn jedes $b \in B$ eindeutig als A-Linearkombination von $\omega_1, \ldots, \omega_n$ darstellbar ist.

Satz 9 Sei L/K separabel, A ein Hauptidealring. Dann ist jeder endlich erzeugte B-Untermodul $0 \neq M \subseteq L$ ein freier A-Modul vom Rang $(L : K)$. Insbesondere hat L eine Ganzheitsbasis.

Satz 10 Seien L/K und L'/K Galois-Erweiterungen mit den Graden $n = (L : K)$ und $n' = (L' : K)$, und es gelte $L \cap L' = K$. Weiter seien $\omega_1, \ldots, \omega_n$ und $\omega'_1, \ldots, \omega'_{n'}$ Ganzheitsbasen von L bzw. L' über A mit den Diskriminanten d bzw. d'. Falls dann $x, x' \in A$ existieren mit

$$xd + x'd' = 1,$$

so ist $\omega_i \cdot \omega'_j$ $(i = 1, \ldots, n; j = 1, \ldots, n')$ eine Ganzheitsbasis von LL' mit Diskriminante $d^{n'} \cdot d'^{n}$.

Bem. Zum Körper $K/\mathbb{Q}$ bezeichne im Folgenden $\mathfrak{O} = \mathfrak{O}_K$ den ganzen Abschluß von $\mathbb{Z}$ in K. $\mathfrak{O}$ heißt Ring der *ganzen Elemente* von K.

Satz 11 Jeder endlich erzeugte $\mathfrak{O}$-Teilmodul $\mathfrak{a}$ besitzt eine $\mathbb{Z}$-Basis $\alpha_1, \ldots, \alpha_n$, und die Diskriminante

$$d(\alpha_1, \ldots, \alpha_n) = \det(\sigma_i(\alpha_j))^2$$

ist unabhängig von der gewählten $\mathbb{Z}$-Basis. Insbesondere existiert eine Ganzheitsbasis von K über $\mathbb{Z}$.

Bem. Die von der speziellen Basis $\alpha_1, \ldots, \alpha_n$ unabhängige Diskriminante einer $\mathbb{Z}$-Basis von $\mathfrak{a}$ wird in der Form

$$d(\mathfrak{a}) := d(\alpha_1, \ldots, \alpha_n)$$

notiert.

Satz 12 Seien $0 \neq \mathfrak{a} \subseteq a'$ endlich erzeugte $\mathfrak{O}$-Teilmoduln von K. Dann ist der Index $(\mathfrak{a}' : \mathfrak{a})$ endlich und es gilt

$$d(\mathfrak{a}) = (\mathfrak{a}' : \mathfrak{a})^2 \cdot d(\mathfrak{a}').$$

3 Idealtheorie

In diesem Abschnitt sei K ein Zahlkörper, $\mathfrak{O} = \mathfrak{O}_K$ der Ring der ganzen Elemente von K und $\mathfrak{O}^\times$ die Einheitengruppe von $\mathfrak{O}$.

Bem. Jedes Element $\alpha \in \mathfrak{O} \setminus \mathfrak{O}^\times$, $\alpha \neq 0$ läßt sich in $\mathfrak{O}$ in ein Produkt irreduzibler Elemente zerlegen, jedoch ist diese Zerlegung i. A. nicht mehr eindeutig. Im Fall $K = \mathbb{Q}(\sqrt{5})$ und $\mathfrak{O} = \mathbb{Z} + \mathbb{Z}\sqrt{5}$ gilt etwa

$$3 \cdot 7 = 21 = (1 + 2\sqrt{-5}) \cdot (1 - 2\sqrt{-5}).$$

Statt ganzer Zahlen α betrachtet man daher die von ihnen erzeugten Ideale $(\alpha) = \mathfrak{O}\alpha$, oder allgemeiner alle Ideale $\mathfrak{a} \trianglelefteq \mathfrak{O}$.

Def. 8 Seien $\mathfrak{a}, \mathfrak{b} \trianglelefteq \mathfrak{O}$. *Teilbarkeit* von Idealen ist definiert durch

$$\mathfrak{a} \mid \mathfrak{b} \qquad :\Longleftrightarrow \qquad \mathfrak{b} \subseteq \mathfrak{a}.$$

Bem. Für $\alpha, \beta \in \mathfrak{O} \setminus \{0\}$ gilt

$$\alpha \mid \beta \text{ in } \mathfrak{O} \qquad \Longleftrightarrow \qquad (\alpha) \mid (\beta).$$

Def. 9 Ein Ring R heißt DEDEKIND-*Ring*, falls R noethersch und ganzabgeschlossen ist und jedes Primideal $\mathfrak{p} \neq (0)$ maximal ist.

Satz 13 $\mathfrak{O}$ ist ein DEDEKIND-Ring.

Satz 14 Jedes Ideal $\mathfrak{a} \neq (0)$ in $\mathfrak{O}$ besitzt eine bis auf die Reihenfolge eindeutige Zerlegung

$$\mathfrak{a} = \mathfrak{p}_1 \cdot \dots \cdot \mathfrak{p}_r$$

in ein Produkt von Primidealen $\mathfrak{p}_i$ in $\mathfrak{O}$.

Satz 15 Zu jedem Ideal $\mathfrak{a} \neq (0)$ in $\mathfrak{O}$ existieren Primideale $\mathfrak{p}_1, \dots, \mathfrak{p}_r \neq (0)$ mit

$$\mathfrak{p}_1, \dots, \mathfrak{p}_r \subseteq \mathfrak{a}.$$

Def. 10 Seien $\mathfrak{a}, \mathfrak{p} \trianglelefteq \mathfrak{O}$, $\mathfrak{p}$ prim. Dann sind $\mathfrak{p}^{-1}$ und $\mathfrak{a}\mathfrak{p}^{-1}$ definiert durch

$$\begin{aligned} \mathfrak{p}^{-1} &= \{x \in K : x \cdot \mathfrak{p} \subseteq \mathfrak{O}\}, \\ \mathfrak{a}\mathfrak{p}^{-1} &= \{\textstyle\sum a_i x_j : a_i \in \mathfrak{a}, x_j \in \mathfrak{p}^{-1}\}. \end{aligned}$$

Satz 16 Für jedes Ideal $\mathfrak{a} \neq (0)$ in $\mathfrak{O}$ und jedes Primideal $\mathfrak{p}$ in $\mathfrak{O}$ gilt $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathfrak{a}$.

Satz 17 (Hauptsatz über simultane Kongruenzen, Chinesischer Restsatz) Sei R ein Ring, $\mathfrak{a}_i \trianglelefteq R$ $(i = 1, \dots, n)$ mit $\mathfrak{a}_i + \mathfrak{a}_j = R$ $(i \neq j)$ und

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{a}_i.$$

Dann ist die Abbildung

$$R/\mathfrak{a} \xrightarrow{\sim} \prod_{i=1}^{n} R/\mathfrak{a}_i\,, \qquad a + \mathfrak{a} \mapsto (a + \mathfrak{a}_1, \dots, a + \mathfrak{a}_n)$$

ein Isomorphismus.

Def. 11 Ein endlich erzeugter $\mathfrak{O}$-Teilmodul $\mathfrak{a} \leq K$, $\mathfrak{a} \neq (0)$ heißt *gebrochenes* Ideal.

Bem.

- Für jedes $a \in K^\times$ ist $(a) = \mathfrak{O} \cdot a$ ein gebrochenes Ideal.
- Die gebrochenen Ideale $\mathfrak{a} \subseteq \mathfrak{O}$ sind gerade die Ideale von $\mathfrak{O}$ und heißen in Abgrenzung zu den gebrochenen Idealen auch *ganze* Ideale.
- Ein beliebiger $\mathfrak{O}$-Teilmodul $\mathfrak{a} \leq K$ ist genau dann ein gebrochenes Ideal, wenn ein $c \in \mathfrak{O} \setminus \{0\}$ esistiert, so daß $c \cdot \mathfrak{a}$ ein (ganzes) Ideal ist, also $c \cdot \mathfrak{a} \subseteq \mathfrak{O}$ oder $\mathfrak{a} \subseteq \frac{1}{c}\mathfrak{O}$.

Satz 18 Die Menge aller gebrochenen Ideale bildet eine abelsche Gruppe bezüglich der Verknüpfung

$$\mathfrak{a} \cdot \mathfrak{b} := \{\sum_{<\infty} a_i b_j : a_i \in \mathfrak{a}, b_j \in \mathfrak{b}\},$$

die sogenannte *Idealgruppe* J_K von K. Ihr Einselement ist $\mathfrak{O} = (1)$ und das Inverse zu $\mathfrak{a}$ ist

$$\mathfrak{a}^{-1} = \{x \in K : x \cdot \mathfrak{a} \subseteq \mathfrak{O}\}.$$

Satz 19 J_K ist freie abelsche Gruppe über der Menge aller Primideale $\mathfrak{p} \neq (0)$ von $\mathfrak{O}$. Das heißt jedes gebrochene Ideal $\mathfrak{a}$ besitzt eine eindeutige Produktdarstellung

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_\mathfrak{p}}$$

mit $\nu_\mathfrak{p} \in \mathbb{Z}$, $\nu_\mathfrak{p} = 0$ für fast alle $\mathfrak{p}$.

Bem.

- Die Menge

  $$P_K := \{(a) = a \cdot \mathfrak{O} : a \in K^\times\}$$

  ist eine ausgezeichnete Untergruppe von J_K. Die Faktorgruppe $\mathfrak{A}_K := J_K/P_K$ heißt die (*Ideal*)-*Klassengruppe* von K. Es gilt die exakte Sequenz

  $$1 \to \mathfrak{O}^\times \to K^\times \to J_K \to \mathfrak{A}_K \to 1.$$

- Diese Sequenz beschreibt den „Informationsverlust“ beim Übergang von Zahlen in $K^\times$ zu Idealen einerseits und andererseits die Abweichung eines beliebigen Ideals davon, Hauptideal zu sein.
- Als $\mathfrak{O}^\times$ und $\mathfrak{A}_K$ können beliebige abelsche Gruppen auftreten, wenn $\mathfrak{O}$ alle Dedekind-Ringe durchläuft.

4 Gitter

Def. 12 Sei V ein reeller Vektorraum mit $\dim V = n < \infty$. Ein *Gitter* $\Gamma \subseteq V$ ist eine Untergruppe von der Form

$$\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$$

mit linear unabhängigen $v_1, \dots, v_m \in V$. Die Menge $\{v_1, \dots, v_m\}$ heißt *Basis* des Gitters Γ und

$$\Phi = \{\sum_i x_i v_i : x_i \in \mathbb{R}, 0 \leq x_i < 1\}$$

heißt *Grundmasche* von Γ. Γ heißt *vollständig* oder *$\mathbb{Z}$-Struktur* auf V, falls $m = n$ ist.

Bem. Γ ist genau dann vollständig, wenn gilt

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

Def. 13 eine Teilmenge $D \subseteq T$ eines topologischen Raums T heißt *diskret*, falls jeder Punkt aus D isoliert in T ist, d. h. wenn es zu jedem $d \in D$ eine Umgebung U von d gibt mit $U \cap D = \{d\}$.

Satz 20 Eine Untergruppe $\Gamma \subseteq V$ ist genau dann ein Gitter, wenn Γ diskret in der Standardtopologie des $\mathbb{R}^n$ ist.

Satz 21 Ein Gitter Γ ist genau dann vollständig, wenn es eine beschränkte Menge $M \subseteq V$ gibt mit

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

Bem. Nun sei V ein euklidischer Vektorraum, $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{R}$ sein Skalarprodukt und $e_1, \dots, e_n$ eine Orthonormalbasis von V. Die Integralrechnung im $\mathbb{R}^n$ definiert ein Volumen vol mit

$$\mathrm{vol}(\Phi(e_1, \dots, e_n)) = 1.$$

Für linear unabhängige $v_1, \dots, v_n$ gilt allgemeiner

$$\mathrm{vol}(\Phi(v_1, \dots, v_n)) = |\det A|$$

mit $A = ((a_{ij}))$ und $v_i = \sum_{k=1}^{n} a_{ik} e_k$. Ferner gilt

$$\mathrm{vol}(\Phi(v_1, \dots, v_n)) = \sqrt{|\det((\langle v_i, v_j \rangle))|}.$$

$\mathrm{vol}(\Phi)$ ist unabhängig von der Wahl der $\mathbb{Z}$-Basis des Gitters

$$\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n,$$

so daß man $\mathrm{vol}(\Gamma) := \mathrm{vol}(\Phi)$ definieren kann.

Def. 14 Sei $X \subseteq V$.

1. X heißt *zentralsymmetrisch*, wenn gilt:

$$\forall \quad x \in X : \qquad -x \in X.$$

2. X heißt *konvex*, falls mit $x, y \in X$ auch $tx + (1-t)y \in X$ gilt ($t \in [0, 1]$).

Satz 22 (Gitterpunktsatz von Minkowski) Sei Γ ein vollständiges Gitter im euklidischen Vektorraum V, $X \subseteq V$ konvex und zentralsymmetrisch mit

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

Dann enthält $\Gamma \cap X$ einen Punkt $\gamma \neq 0$.

5 Minkowski-Theorie

In diesem Abschnitt sei $K/\mathbb{Q}$ eine Zahlkörpererweiterung vom Grad n. Es geht um die Einbettungen $K \hookrightarrow \mathbb{R}^n$ und die geometrischen Eigenschaften der als Punkte interpretierten algebraischen Zahlen. Es sei

$$j : K \to K_{\mathbb{C}} := \prod_{\tau : K \hookrightarrow \mathbb{C}} \mathbb{C} = \mathbb{C}^n, \qquad \alpha \mapsto (\dots, \tau(\alpha), \dots).$$

Der Raum $K_{\mathbb{C}}$ sei versehen mit dem Skalarprodukt

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

Def. 15 Sei $F : \mathbb{C} \to \mathbb{C}, F(z) := \bar{z}$. Der reelle Vektorraum $K_{\mathbb{R}} = K_{\mathbb{C}}^{+}$ der F-invarianten Punkte von $K_{\mathbb{C}}$ zusammen mit dem durch Einschränkung von $\langle \cdot, \cdot \rangle$ definierten rellen Skalarprodukt $\langle \cdot, \cdot \rangle : K_{\mathbb{R}} \times K_{\mathbb{R}} \to \mathbb{R}$ heißt Minkowski-*Raum*.

Bem. Sei

$$\{\varrho_1, \dots, \varrho_r\} := \{\tau : K \hookrightarrow \mathbb{C} : \tau(K) \subseteq \mathbb{R}\}$$

die Menge der reellen Einbettungen. Die nicht-reellen, komplexen Einbettungen kommen stets als Paare $\tau, \bar{\tau} \neq \tau$ vor und seien durch

$$\sigma_1, \dots, \sigma_s, \quad \bar{\sigma}_1, \dots, \bar{\sigma}_s$$

bezeichnet. Insgesamt gibt es also $2s + r = n$ Einbettungen. Daraus folgt

$$K_{\mathbb{R}} = \{(z_\tau) \in \prod_{\tau} \mathbb{C} : z_{\varrho_i} \in \mathbb{R} \ (i = 1, \dots, r), z_{\bar{\sigma}_i} = \bar{z}_{\sigma_i} \ (i = 1, \dots, s)\}$$

und $j(K) \subseteq K_{\mathbb{R}}$.

Satz 23 Die Zuordnung

$$f : K_{\mathbb{R}} \to \prod_{\tau} \mathbb{R} = \mathbb{R}^{r+2s}, \qquad (z_\tau) \mapsto (x_\tau)$$

mit $x_{\varrho_i} := z_\varrho \ (i = 1, \dots, r)$ und $x_{\sigma_i} = \operatorname{Re} z_{\sigma_i}$, $x_{\bar{\sigma}_i} = \operatorname{Im} z_{\sigma_i} \ (i = 1, \dots, s)$ ist ein Isomorphismus metrischer Räume, der das Skalarprodukt $\langle \cdot, \cdot \rangle$ überführt in das Skalarprodukt

$$(x, y) := \sum_{\tau} \alpha_\tau x_\tau \cdot y_\tau$$

mit $\alpha_\tau = 1 \ (\tau \in \{\varrho_1, \dots, \varrho_r\})$ und $\alpha_\tau = 2$ sonst.

Satz 24 Für jedes Ideal $\mathfrak{a} \neq (0)$ von $\mathfrak{O}$ bildet $\Gamma := j(\mathfrak{a})$ ein vollständiges Gitter in $K_{\mathbb{R}}$ mit dem Grundmaschenvolumen

$$\operatorname{vol}(\Gamma) = \sqrt{|d_K|} \cdot (\mathfrak{O} : \mathfrak{a}).$$

Satz 25 Seien $\mathfrak{a} \trianglelefteq \mathfrak{O}$, $\mathfrak{a} \neq (0)$ und $(c_\tau) \in \mathbb{R}^{r+2s}$ mit $c_\tau > 0$, $c_{\bar{\tau}} = c_\tau$ und

$$\prod_{\tau} c_\tau > A \cdot (\mathfrak{O} : \mathfrak{a})$$

für $A := \sqrt{|d_k|} \cdot (\frac{2}{\pi})^s$. Dann existiert ein $a \in \mathfrak{a} \setminus \{0\}$ mit

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

für alle $\tau : K \hookrightarrow \mathbb{C}$.

6 Die Klassenzahl eines Zahlkörpers

Def. 16 Der Index $(\mathfrak{O} : \mathfrak{a})$ eines Ideals $\mathfrak{a} \trianglelefteq \mathfrak{O}$, $\mathfrak{a} \neq (0)$ heißt die *Absolutnorm* von $\mathfrak{a}$. Schreibweise: $\mathcal{N}\mathfrak{a} := (\mathfrak{O} : \mathfrak{a})$.

Bem. Für $\mathfrak{a} = (a)$ gilt $\mathcal{N}\mathfrak{a} = |\mathcal{N}_{K/\mathbb{Q}}(a)|$.

Satz 26 Die Idealnorm ist multiplikativ, d. h. es gilt

$$\mathcal{N}(\mathfrak{a}\mathfrak{b}) = (\mathcal{N}\mathfrak{a})(\mathcal{N}\mathfrak{b}) \qquad (\mathfrak{a}, \mathfrak{b} \trianglelefteq \mathfrak{O}),$$

und sie setzt sich fort zu einem Gruppenhomomorphismus $\mathcal{N} : J_K \to \mathbb{Q}^\times_{>0}$.

Satz 27 In jedem Ideal $\mathfrak{a} \neq (0)$ von $\mathfrak{O}$ existiert ein $a \neq 0$ mit

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

Satz 28 Die Idealklassengruppe $\mathfrak{A}_K = {}^{J_K}\!/_{P_K}$ ist endlich.

Bem.

- Die Ordnung $h_K := \mathfrak{A}_K$ von ${}^{J_K}\!/_{P_K}$ heißt *Klassenzahl* von K.
- Im Fall $h_k = 1$ ist $\mathfrak{O}$ ein Hauptidealring, insbesondere gibt es eine eindeutige Primzerlegung.
- Die Endlichkeit von h_K besagt, daß die Abweichung von einer eindeutigen Primzerlegung nicht allzu groß ist. $\mathfrak{A}_K$ ist ein Maß für die Abweichung.
- In der Regel ist $h_K > 1$. Es ist nicht bekannt, ob es unendlich viele Zahlkörper mit $h_K = 1$ gibt. Es gibt genau 9 imaginärquadratische Zahlkörper mit $h_K = 1$. Dies sind genau die Körper $K = \mathbb{Q}(\sqrt{d})$ mit

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

  Es wird vermutet, daß es unendlich viele reellquadratische Zahlkörper mit Klassenzahl $h_K = 1$ gibt.
- Es bezeichne h_n die Klassenzahl des Einheitswurzelkörpers

  $$\mathbb{Q}^{(n)} := \mathbb{Q}(\mathrm{e}^{2\pi\mathrm{i}/n}) \qquad (n \in \mathbb{N}).$$

Satz 29 (Satz von Kummer) Für Primzahlen $p \geq 3$ folgt aus $p \nmid h_p$, daß $X^p + Y^p = Z^p$ nur die triviale Lösung hat, die Fermatsche Vermutung für diese p also richtig ist.

Bem.

- Die Primzahlen p mit $p \nmid h_p$ heißen *regulär*, die anderen *irregulär*. Es ist unbekannt, ob es unendlich viele reguläre p gibt.
- Die Iwasawa-Theorie beschreibt die Assymptotik von $\mathrm{ord}_p(h_{p^m})$ für wachsendes m. Es gilt:

  $$\mathrm{ord}_p(h_{p^m}) = \lambda_p p^m + \mu_p \cdot m + \nu_p$$

  für Konstanten λ_p, μ_p, ν_p.

7 Der DIRICHLETsche Einheitensatz

Sei K ein Zahlkörper vom Index $(K : \mathbb{Q}) = n = r + 2s$, $E := E_K := \mathfrak{O}_K^\times$ und $\mu(K)$ die Gruppe der Einheitswurzeln in K. Es gilt das folgende kommutative Diagramm:

$$\begin{tikzcd}
K^\times \arrow[r, "j"] \arrow[d, "\mathcal{N}_{K/\mathbb{Q}}"'] & K_{\mathbb{C}}^\times \arrow[r, "l"] \arrow[d, "N"] & \prod_\tau \mathbb{R} \arrow[d, "\mathrm{Tr}"] \\
\mathbb{Q}^\times \arrow[r, "\subseteq"'] & \mathbb{C}^\times \arrow[r, "\log|\cdot|"'] & \mathbb{R}
\end{tikzcd}$$

wobei j wie auf Seite 9 definiert ist und

$$\begin{aligned}
N &: \prod_\tau \mathbb{C}^\times \to \mathbb{C}^\times, \qquad N(\dots, z_\tau, \dots) = \prod_\tau z_\tau, \\
l &: \prod_\tau \mathbb{C}^\times \to \prod_\tau \mathbb{R}, \qquad l(\dots, z_\tau, \dots) = (\dots, \log|z_\tau|, \dots)
\end{aligned}$$

seien. Beim Übergang zu $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$-Fixmoduln erhält man

$$\begin{tikzcd}
K^\times \arrow[r, "j"] \arrow[d, "\mathcal{N}_{K/\mathbb{Q}}"'] & K_{\mathbb{R}}^\times \arrow[r, "l"] \arrow[d, "N"] & \left(\prod_\tau \mathbb{R}\right)^+ \arrow[d, "\mathrm{Tr}"] \\
\mathbb{Q}^\times \arrow[r, "\subseteq"'] & \mathbb{R}^\times \arrow[r, "\log|\cdot|"'] & \mathbb{R}
\end{tikzcd}$$

Dabei sei

$$\left(\prod_\tau \mathbb{R}\right)^+ := \prod_\varrho \mathbb{R} \times \prod_{\sigma_1, \dots, \sigma_s} \underbrace{(\mathbb{R} \times \mathbb{R})^+}_{\substack{=\{(x,x):x\in\mathbb{R}\}\cong\mathbb{R} \\ \text{via } (x,x)\mapsto 2x}} \xrightarrow[\alpha]{\sim} \mathbb{R}^{r+s}$$

mit

$$\alpha(e(j(x))) = (\log|\varrho_1(x)|, \dots, \log|\varrho_r(x)|, \log|\sigma_1(x)|^2, \dots \log|\sigma_s(x)|^2).$$

Satz 30 Es seien

$$\begin{aligned}
E &:= \{\varepsilon \in \mathfrak{O}_K : \mathcal{N}_{K/\mathbb{Q}}(\varepsilon) = \pm 1\}, \\
S &:= \{y \in K_{\mathbb{R}}^\times : N(y) = \pm 1\}, \\
H &:= \{x \in \left(\prod_\tau \mathbb{R}\right)^+ : \mathrm{Tr}(x) = 0\}.
\end{aligned}$$

Mit $\lambda : E \to H$ sei die Komposition von j und l bezeichnet, Γ sei das Bild von E unter λ. Dann ist

$$1 \to \mu(K) \xrightarrow{\subseteq} E_k \xrightarrow{\lambda} \Gamma \to 0$$

eine exakte Sequenz.

Satz 31 Γ ist ein vollständiges Gitter in $H \cong \mathbb{R}^{r+s-1}$.

Satz 32 Zu gegebenem $a \in \mathbb{N}$ existieren höchstens endlich viele nicht assoziierte $\alpha \in \mathfrak{O}_K$ mit $\mathcal{N}_{K/\mathbb{Q}}(\alpha) = a$.

Satz 33 (DIRICHLETscher Einheitensatz) Die Einheitengruppe E_K ist das direkte Produkt der endlichen zyklischen Gruppen $\mu(K)$ und einer freien abelschen Gruppe vom Rang $r + s - 1$, also

$$E_K \cong \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{r+1-s} \times \left(\mathbb{Z}/M\mathbb{Z} \right).$$

Bem. Es gibt $\varepsilon_1, \ldots, \varepsilon_t \in E_K$ $(t = r + s - 1)$, so daß jedes $\varepsilon \in E_K$ eindeutig darstellbar ist als Produkt der Form

$$\varepsilon = \zeta \cdot \varepsilon_1^{\nu_1} \cdot \cdots \cdot \varepsilon_t^{\nu_t}$$

mit eindeutigen $\nu_i \in \mathbb{Z}, \zeta \in \mu(K)$. Diese ε_i heißen *Grundeinheiten* von K.

Def. 17 Seien $\lambda_1, \ldots, \lambda_{r+s}$ die Komponenten der Abbildung

$$\lambda : E \to H \hookrightarrow \mathbb{R}^{r+s}$$

von oben und $\varepsilon_1, \ldots, \varepsilon_t$ Grundeinheiten von K. M sei eine Minore vom Rang t in

$$\begin{pmatrix} \lambda_1(\varepsilon_1) & \ldots & \lambda_1(\varepsilon_t) \\ \vdots & \ddots & \vdots \\ \lambda_{t+1}(\varepsilon_1) & \ldots & \lambda_{t+1}(\varepsilon_t) \end{pmatrix}.$$

Dann heißt $R := R_K := |\det(M)|$ der *Regulator* von K.

Bem. Der Regulator ist wohldefiniert, weil $|\det(M)|$ unabhängig von der Wahl von M ist: Für $x \in H$ gilt nämlich $\sum\limits_\tau x_\tau = 0$, d.h. $0 = \sum\limits_{j=1}^{r+s} \lambda_i(\epsilon)$, so daß sich die Minoren durch elementare Zeilenumformungen ineinander überführen lassen.

Satz 34 Die Grundmasche des Einheitengitters $\Gamma = \lambda(E)$ in dem euklidischen Raum Bild $H \subseteq \mathbb{R}^{r+s}$ hat den Inhalt

$$\mathrm{vol}(\Gamma) = \sqrt{r+s} \cdot R$$

8 Erweiterungen von DEDEKIND-Ringen

Satz 35 Sei $\mathfrak{o}$ ein DEDEKIND-Ring, $K = \mathrm{Quot}(\mathfrak{o})$, L/K eine endliche Körpererweiterung und $\mathfrak{O}$ der ganze Abschluß von $\mathfrak{o}$ in L. Dann ist auch $\mathfrak{O}$ ein DEDEKIND-Ring.

Bem.

- Wenn $\mathfrak{p} \trianglelefteq \mathfrak{o}$ ein Primideal ist, dann ist $\mathfrak{p}\mathfrak{O} \neq \mathfrak{O}$.

- Jedes Primideal $\mathfrak{p} \neq (0)$ in $\mathfrak{o}$ zerfällt in $\mathfrak{O}$ eindeutig in ein Produkt

$$\mathfrak{p}\mathfrak{O} = \mathfrak{P}^{e_1} \cdot \dots \cdot \mathfrak{P}^{e_r},$$

kurz

$$\mathfrak{p} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_\mathfrak{P}}.$$

Die Primideale $\mathfrak{P}_i$ sind genau die $\mathfrak{P}$ mit $\mathfrak{P} \cap \mathfrak{o} = \mathfrak{p}$.

Def. 18 Der Exponent $e_\mathfrak{P} = e(\mathfrak{P}, \mathfrak{p})$ in der obigen Darstellung von $\mathfrak{p}$ heißt *Verzweigungsindex* von $\mathfrak{P}$ über $\mathfrak{p}$. Der Körpergrad

$$f_\mathfrak{P} = f(\mathfrak{P}, \mathfrak{p}) = \left({}^{\mathfrak{O}}\!/_{\mathfrak{P}} : {}^{\mathfrak{o}}\!/_{\mathfrak{p}} \right)$$

heißt der *Trägheitsgrad* von $\mathfrak{P}$ über $\mathfrak{p}$.

Satz 36 Ist L/K separabel und vom Grad $n = (L : K)$, so gilt für jedes Primideal $\mathfrak{p} \neq 0$ von $\mathfrak{o}$

$$\sum_{\mathfrak{P}|\mathfrak{p}} e(\mathfrak{P}, \mathfrak{p}) \cdot f(\mathfrak{P}, \mathfrak{p}) = n,$$

kurz $\sum\limits_i e_i f_i = n$.

Def. 19 Sei $L = K(\theta), \theta \in \mathfrak{O}$ und $p(X) \in \mathfrak{o}[X]$ das Minimalpolynom von θ, $\partial p = n$. Dann heißt das Ideal $\mathcal{F} := \{\alpha \in \mathfrak{O} : \alpha\mathfrak{O} \subseteq \mathfrak{o}[\theta]\}$ *Führer* des Rings $\mathfrak{o}[\theta]$.

Bem. $\mathcal{F}$ ist das größte $\mathfrak{O}$-Ideal, daß als Menge im Ring $\mathfrak{o}[\theta]$ liegt.

Satz 37 Sei $\mathfrak{p} \trianglelefteq \mathfrak{o}$ ein Primideal, das teilerfremd zum Führer $\mathcal{F}$ von $\mathfrak{o}[\theta]$ ist. Ferner sei über dem Restklassenkörper ${}^{\mathfrak{o}}\!/_{\mathfrak{p}} =: k$

$$\bar{p}(X) = \prod_{i=1}^{r} \bar{p}_i(X_i)^{e_i}$$

mit $p_i(X) \in \mathfrak{o}[X]$ normiert. Dann sind die Ideale

$$\mathfrak{P}_i := \mathfrak{p}\mathfrak{O} + p_i(\theta) \cdot \mathfrak{O} \qquad (i = 1, \dots, r)$$

prim, es gilt

$$\mathfrak{p} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$$

und

$$f(\mathfrak{P}_i, \mathfrak{p}) = \partial(\bar{p}_i(X)).$$

Def. 20 Ein Primideal $\mathfrak{p} = \prod\limits_{i=1}^{r} \mathfrak{P}_i^{e_i}$ heißt

1. *voll verzweigt* in L, falls $r = n$ gilt, also alle $e_i = f_i = 1$ sind.
2. *unverzweigt* im Fall $r = 1$.

Ein $\mathfrak{P}_i$ heißt *unverzweigt* über $\mathfrak{o}$, falls $e_i = 1$ ist und die Restklassenerweiterung ${}^{\mathfrak{O}}/_{\mathfrak{P}_i}$ über ${}^{\mathfrak{o}}/_{\mathfrak{p}}$ separabel ist. Falls $f_i = 1$ und $e_i > 1$, heißt $\mathfrak{P}_i$ *rein verzweigt*. $\mathfrak{p}$ heißt *unverzweigt*, falls alle $\mathfrak{P}_i$ unverzweigt sind. L/K heißt *unverzweigt*, wenn alle Primideale $\mathfrak{p} \trianglelefteq \mathfrak{o}$ in $\mathfrak{O}$ unverzweigt sind.

Satz 38 Wenn L/K separabel ist, sind nur endlich viele $\mathfrak{p}$ verzweigt.

Def. 21 Das Ideal $\vartheta \trianglelefteq \mathfrak{o}$ erzeugt von allen Diskriminanten $d(\omega_1, \ldots, \omega_n)$ für K-Basen $\omega_1, \ldots, \omega_n \in \mathfrak{o}$ von L heißt *Diskriminante* von ${}^{\mathfrak{O}}/_{\mathfrak{o}}$.

9 Hilbertsche Verzweigungstheorie

In diesem Abschnitt sei L/K galoissch und $G := \mathrm{Gal}(L/K)$.

Bem.

- G operiert auf $\mathfrak{O}$, da für $a \in \mathfrak{O}, \sigma \in G$ auch $\sigma(a) \in \mathfrak{O}$ ist
- Ist $\mathfrak{P}$ ein Primideal in $\mathfrak{O}$, $\mathfrak{P} \mid \mathfrak{p}$, so gilt $\sigma(\mathfrak{P}) \mid \mathfrak{p}$. G operiert auf der Menge aller $\mathfrak{P} \mid \mathfrak{p}$ für festes $\mathfrak{p}$, denn
$$\sigma(\mathfrak{P}) \cap \mathfrak{o} = \sigma(\underbrace{\mathfrak{P} \cap \mathfrak{o}}_{=\mathfrak{p}}) = \mathfrak{p}.$$
Schreibe $\mathfrak{P}^\sigma = \sigma(\mathfrak{P})$. Die $\sigma(P)$ heißen die zu $\mathfrak{P}$ *konjugierten* Primideale.

Satz 39 G operiert transitiv auf der Menge der $\mathfrak{P} \mid \mathfrak{p}$ für festes $\mathfrak{p}$.

Def. 22 Sei $\mathfrak{P}$ ein Primideal von $\mathfrak{O}$. Die Fixgruppe
$$G_{\mathfrak{P}} := \{\sigma \in G : \mathfrak{P}^\sigma = \mathfrak{P}\}$$
heißt *Zerlegungsgruppe* von $\mathfrak{P}$ über K. Der Fixkörper $Z_{\mathfrak{P}} := L^{G_{\mathfrak{P}}}$ heißt *Zerlegungskörper* von $\mathfrak{P}$ über K.

Bem.

- Für festes $\mathfrak{P} \mid \mathfrak{p}$ ist die Abbildung
$${}^{G}/_{G_{\mathfrak{P}}} \to \{\mathfrak{P}' : \mathfrak{P}' \mid \mathfrak{p}\}, \qquad \sigma \mapsto \mathfrak{P}^\sigma$$
bijektiv
- $G_{\mathfrak{P}} = 1 \iff Z_{\mathfrak{P}} = L \iff \mathfrak{p}$ ist voll verzweigt.
$G_{\mathfrak{P}} = G \iff Z_{\mathfrak{P}} = K \iff \mathfrak{p}$ ist unverzweigt.
- $G_{\mathfrak{P}^\sigma} = \sigma(G_{\mathfrak{P}})\sigma^{-1}$.
$$\tau \in G_{\mathfrak{P}^\sigma} \iff \tau(\sigma(\mathfrak{P})) = \sigma(\mathfrak{P}) \iff \sigma^{-1}\tau\sigma(\mathfrak{P}) = \mathfrak{P} \iff \sigma^{-1}\tau\sigma \in G_{\mathfrak{P}}.$$

- In der Zerlegung $\mathfrak{p} = \prod_{i=1}^{r} \mathfrak{P}^{e_i}$ gilt: Alle e_i sind gleich, etwa $e_i = e$ ($i = 1, \ldots, r$), und alle f_i sind gleich, etwa $f_i = f$ ($i = 1, \ldots, r$), d. h. es gilt

$$\mathfrak{p} = \prod_{\sigma \bmod G_{\mathfrak{P}}} (\sigma\mathfrak{P})^e \quad \text{und} \quad n = r \cdot e \cdot f.$$

Satz 40 Sei $\mathfrak{P}_Z := \mathfrak{P} \cap Z_{\mathfrak{P}}$ das Primideal von $Z_{\mathfrak{P}}$ unter $\mathfrak{P}$. Dann gilt:

1. $\mathfrak{P}_Z$ ist unzerlegt in L, d. h. $\mathfrak{P}$ ist das einzige über Z liegende Primideal in L
2. $e(\mathfrak{P} : \mathfrak{P}_Z) = e(\mathfrak{P} : \mathfrak{p}) = e$, $f(\mathfrak{P} : \mathfrak{P}_Z) = f(\mathfrak{P} : \mathfrak{p}) = f$.
3. $e(\mathfrak{P}_Z : \mathfrak{p}) = f(\mathfrak{P}_Z : \mathfrak{p}) = 1$.

Satz 41 Seien $\varkappa(\mathfrak{P}) = {}^{\mathfrak{O}}\!/_{\mathfrak{P}}$, $\varkappa(\mathfrak{p}) = {}^{\mathfrak{o}}\!/_{\mathfrak{p}}$. Dann ist die Erweiterung $\varkappa(\mathfrak{P})/\varkappa(\mathfrak{p})$ normal und $\sigma \mapsto \bar{\sigma}$ definiert einen surjektiven Homomorphismus

$$G_{\mathfrak{P}} \to \operatorname{Aut}(\varkappa(\mathfrak{P})/\varkappa(\mathfrak{p})).$$

Def. 23 Der Kern $I_{\mathfrak{P}}$ des Homomorphismus aus obigem Satz heißt *Trägheitsgruppe* von $\mathfrak{P}$ über K. Der zugehörige Fixkörper $T_{\mathfrak{P}} := L^{I_{\mathfrak{P}}}$ heißt *Trägheitskörper*.

Satz 42 Die Erweiterung T_p/Z_p ist galoissch mit

$$\operatorname{Gal}(T_{\mathfrak{P}}/Z_{\mathfrak{P}}) \cong \operatorname{Aut}(\varkappa(\mathfrak{P})/\varkappa(\mathfrak{p})), \qquad \operatorname{Gal}(L/T_{\mathfrak{P}}) = I_{\mathfrak{P}}$$

Falls $\varkappa(\mathfrak{P})/\varkappa(\mathfrak{p})$ separabel (also galoissch) ist, gilt $|I_{\mathfrak{P}}| = e$ und

$$(G_{\mathfrak{P}} : I_{\mathfrak{P}}) = (T_{\mathfrak{P}} : Z_{\mathfrak{P}}) = f$$

und für das Primideal $\mathfrak{P}_T := \mathfrak{P} \cap T_{\mathfrak{P}}$ gilt

1. $e({}^{\mathfrak{P}}\!/_{\mathfrak{P}_T}) = e$, $f({}^{\mathfrak{P}}\!/_{\mathfrak{P}_T}) = 1$,
2. $e({}^{\mathfrak{P}_T}\!/_{\mathfrak{P}_Z}) = 1$, $f({}^{\mathfrak{P}_T}\!/_{\mathfrak{P}_Z}) = f$

Bem. Falls $\varkappa(\mathfrak{P})/\varkappa(\mathfrak{p})$ separabel ist, gilt

$$I_{\mathfrak{P}} = 1 \iff T_{\mathfrak{P}} = L \iff \mathfrak{p} \text{ ist unverzweigt in } L.$$

In diesem Fall ist $\operatorname{Gal}(\varkappa(\mathfrak{P})/\varkappa(\mathfrak{p})) \cong \operatorname{Gal}(L/K)$.

10 Kreisteilungskörper

Sei $\zeta \in \mathbb{C}$ eine primitive n-te Einheitswurzel, etwa $\zeta = \mathrm{e}^{2\pi\mathrm{i}/n}$ für ein $n \in \mathbb{N}$, und $\mathfrak{O}$ der Ring der ganzen Zahlen in $\mathbb{Q}(\zeta)$.

Satz 43 Sei $n = l^v$ eine Primzahlpotenz, $\lambda := 1 - \zeta$. Dann ist das Hauptideal (λ) in $\mathfrak{O}$ ein Primideal vom Grad 1 und es gilt $(l) = (\lambda)^d$ mit

$$d := \varphi(l^v) = (\mathbb{Q}(\zeta) : \mathbb{Q}).$$

Ferner hat die Basis $\{1, \zeta, \ldots, \zeta^{d-1}\}$ von $\mathbb{Q}(\zeta)/\mathbb{Q}$ die Diskriminante

$$d(1, \zeta, \ldots, \zeta^{d-1}) = \pm l^s$$

mit

$$s := l^{v-1} \cdot (v(l-1) - 1).$$

Satz 44 Eine Ganzheitsbasis von $\mathfrak{O}$ ist gegeben durch

$$1, \zeta, \zeta^2, \ldots, \zeta^{d-1}$$

für $d = \varphi(n) = (\mathbb{Q}(\zeta) : \mathbb{Q})$, d. h. $\mathfrak{O} = \mathbb{Z}[\zeta]$.

Satz 45 (Zerlegungssatz) Sei $n = \prod_{p \text{ prim}} p^{\nu_p}$ und f_p sei die kleinste natürliche Zahl mit

$$p^{f_p} \equiv 1 \bmod \frac{n}{p^{\nu_p}}.$$

Dann zerfällt p in $\mathbb{Q}(\zeta)$ in der Form

$$(p) = (\mathfrak{p}_1, \ldots, \mathfrak{p}_r)^{\varphi(p^{\nu_p})}$$

mit $r := \frac{\varphi(n/p^{\nu_p})}{f_p}$ verschiedenen Primidealen $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ vom gleichen Grad f_p.

Satz 46 Falls $p = 2 = (4, n)$ ist $p = 2$ unverzweigt, sonst gilt: p ist genau dann verzweigt, wenn $n = 0 \bmod p$. Für $p \neq 2$ ist p genau dann vollzerlegt, wenn $p = 1 \bmod n$. $\varphi(n) = r, e = f = 1$. (?)

Satz 47 Seien $l, p > 2$ prim, $l \neq p$, $l^* := (-1)^{\frac{p-1}{2}} \cdot l$ und ζ primitive l-te Einheitswurzel. Dann gilt: p ist genau dann vollzerlegt in $\mathbb{Q}(\sqrt{l^*})$, wenn

$$(p) = (\mathfrak{p}_1 \cdot \cdots \cdot \mathfrak{p}_r)^e$$

in $\mathbb{Q}(\zeta)$ mit $r \equiv 0 \bmod 2$.

Bem. Folgerung: $(\frac{l^*}{p}) = (\frac{p}{l})$.

11 Bewertungen

Def. 24 Eine *Bewertung* oder ein *Betrag* eines Körpers K ist eine Funktion $|\cdot| : K \to \mathbb{R}$ mit folgenden Eigenschaften:

1. $|x| \geq 0$, $|x| = 0 \iff x = 0$ $(x \in K)$ (Positiv-Definitheit)
2. $|x \cdot y| = |x| \cdot |y|$ $(x, y \in K)$ (Multiplikativität)
3. $|x + y| \leq |x| + |y|$ $(x, y \in K)$ (Dreiecksungleichung)

Bem.

- Die triviale Bewertung

$$|\cdot| : K \to \mathbb{R}, \qquad |x| := \begin{cases} 0 & (x = 0) \\ 1 & (x \neq 0) \end{cases}$$

  sei im folgenden ausgeschlossen.

- Eine Bewertung $|\cdot|$ macht den Körper K zu einem metrischen Raum mit der Metrik

$$d : K \times K \to \mathbb{R}, \qquad d(x, y) := |x - y|,$$

  also insbesondere auch zu einem topologischem Raum.

Def. 25 Zwei Bewertungen $|\cdot|_1, |\cdot|_2$ heißen *äquivalent*, $|\cdot|_1 \sim |\cdot|_2$, wenn sie die gleiche Topologie erzeugen.

Satz 48 Zwei Bewertungen $|\cdot|_1, |\cdot|_2$ sind genau dann äquivalent, wenn gilt

$$\exists \quad s > 0 \quad \forall \quad x \in K : \qquad |x|_1 = |x_2|^s.$$

Bem. Folgerung: Zwei Bewertungen $|\cdot|_1, |\cdot|_2$ sind genau dann äquivalent, wenn gilt

$$\forall \quad x \in K : \qquad |x|_1 < 1 \quad \Longrightarrow \quad |x|_2 < 1.$$

Satz 49 (Approximationssatz, verallgemeinerter Chinesischer Restsatz) Seien $|\cdot|_1, \ldots, |\cdot|_n$ paarweise nicht äquivalente Bewertungen von K und $a_1, \ldots, a_n \in K$. Dann existiert zu jedem $\varepsilon > 0$ ein $x \in K$ mit

$$|x - a_i|_i < \varepsilon \qquad (i = 1, \ldots, n).$$

Def. 26 Eine Bewertung $|\cdot|$ heißt *nicht-archimedisch* oder *ultrametrisch*, falls $\{|n| : n \in \mathbb{N}\}$ beschränkt ist, sonst *archimedisch*.

Satz 50 Eine Bewertung $|\cdot|$ ist genau dann nicht-archimedisch, wenn die verschärfte Dreiecksungleichung

$$|x + y| \leq \max\{|x|, |y|\} \qquad (x, y \in K)$$

gilt.

Bem.

- Die verschärfte Dreiecksungleichung liefert sogar Gleichheit

$$|x + y| = \max\{|x|, |y|\},$$

  falls $|x| \neq |y|$.

- Jede nicht-archimedische Bewertung $|\cdot|$ läßt sich natürlich fortsetzen auf den rationalen Funktionenkörper $K(t) = \mathrm{Quot}(K[t])$ vermöge

$$|a_0 + a_1 t + \cdots + a_n t^n| := \max\{|a_0|, \cdots, |a_n|\}.$$

Bsp.

- Der gewöhnliche Absolutbetrag $|\cdot|_\infty$ von $\mathbb{Q}$ ist archimedisch.
- Für jede Primzahl p ist die p-adische Bewertung $|\cdot|_p$ von $\mathbb{Q}$ nicht-archimedisch. Hier gilt
$$|\prod_{e \text{ prim}} e^{\nu_e}|_p := p^{-\nu_p}.$$

Satz 51 Jede nichttriviale Bewertung von $\mathbb{Q}$ ist äquivalent zu $|\cdot|_\infty$ oder $|\cdot|_p$ für ein geeignetes p.

Bem. Jeder nichtarchimedische Betrag $|\cdot|$ induziert eine Funktion

$$v : K \to \mathbb{R} \,\dot{\cup}\, \{\infty\}, \qquad v(x) := \begin{cases} -\log|x| & (x \neq 0) \\ \infty & (x = 0) \end{cases}$$

Die Eigenschaften der Bewertung liefern dann:

- $v(x) = \infty \quad \Longleftrightarrow \quad x = 0,$
- $v(x \cdot y) = v(x) + v(y),$
- $v(x + y) \geq \min\{v(x), v(y)\}.$

Def. 27 Eine Funktion $v : K \times K \to \mathbb{R} \,\dot{\cup}\, \{\infty\}$ mit

1. $v(x) = \infty \quad \Longleftrightarrow \quad x = 0,$
2. $v(x \cdot y) = v(x) + v(y),$
3. $v(x + y) \geq \min\{v(x), v(y)\}.$

heißt *Exponentialbewertung* von K. Zwei Exponentialbewertungen v_1, v_2 heißen *äquivalent*, falls eine reelle Zahl $s > 0$ existiert mit $v_1 = s \cdot v_2$.

Bem.

- Die triviale Exponentialbewertung
$$v(x) := \begin{cases} 0 & (x \neq 0) \\ \infty & (x = 0) \end{cases}$$
sei im folgenden ausgeschlossen.
- Jede Exponentialbewertung v definiert bei Vorgabe eines festen $q > 1$ eine nichtarchimedische Betragsbewertung $|x|_q$ von K durch
$$|x|_q := q^{-v(x)}.$$
Die Äquivalenzbegriffe von Betragsbewertung und Exponentialbewertung entsprechen sich.

Satz 52 Sei v eine Exponentialbewertung. Dann gilt: Die Einheitskugel

$$\mathfrak{O} = \mathfrak{O}_v := \{x \in K : |x| \leq 1\} = \{x \in K : v(x) \geq 0\}$$

ist ein Ring mit der Einheitengruppe

$$\mathfrak{O}_v^\times = \{x \in K : |x| = 1\} = \{x \in K : v(x) = 0\}$$

und dem einzigen maximalen Ideal

$$\mathfrak{p} = \mathfrak{p}_v := \{x \in K : |x| < 1\} = \{x \in K : v(x) > 0\} = \mathfrak{O}_v \setminus \mathfrak{O}_v^\times.$$

Def. 28 Ein Integritätsbereich $\mathfrak{O}$ mit $\mathrm{Quot}(\mathfrak{O}) = K$ heißt *Bewertungsring*, falls gilt

$$\forall \quad x \in K: \qquad x \in \mathfrak{O} \quad \vee \quad x^{-1} \in \mathfrak{O}.$$

Bem.

- Ein Bewertungsring hat immer ein einziges maximales Ideal, nämlich

  $$\mathfrak{p} = \{x \in \mathfrak{O} : x^{-1} \notin \mathfrak{O}\} = \mathfrak{O} \setminus \mathfrak{O}^\times.$$

  $K := \mathfrak{O}/\mathfrak{p}$ heißt *Restklassenkörper* von $\mathfrak{O}$.

- Bewertungsringe sind ganzabgeschlossen, denn ist $x \in K$ ganz über $\mathfrak{O}$, dann existieren $a_i \in \mathfrak{O}$ mit

  $$x^n + a_1 x^{n-1} + \cdots + a_n = 0.$$

  Multiplikation mit $x^{-(n-1)}$ liefert

  $$x = -a_1 - a_2 x^{-1} - \cdots - a_n x^{-(n-1)}.$$

  Falls $x \notin \mathfrak{O}$, dann ist $x^{-1} \in \mathfrak{O}$ und damit die rechte Seite in $\mathfrak{O}$. Widerspruch.

Def. 29 Die Exponentialbewertung v heißt *diskret*, falls $v(\mathfrak{p}_v) \subseteq \mathbb{R}$ ein Minimum besitzt.

Bem. Für diskrete Bewertungen v existiert ein s mit $v(K^\times) = s \cdot \mathbb{Z}$. Im Fall $s = 1$ heißt v *normiert*. Ein Element $\pi \in \mathfrak{O}$ mit $v(\pi) = 1$ für normiertes v heißt *Primelement*. Für jedes $x \in K^\times$ existiert eine eindeutige Darstellung $x = u\pi^n$ mit $u \in \mathfrak{O}^\times$ und $n \in \mathbb{Z}$.

Satz 53 Sei v eine diskrete Exponentialbewertung von K. Dann gilt:

1. $\mathfrak{O}_v$ ist ein Hauptidealring

2. Ist v normiert und π ein Primelement, so sind alle Ideale $\mathfrak{a} \neq (0)$ von der Form

   $$\mathfrak{a} = \mathfrak{p}^n = \pi^n \mathfrak{O}_v = \{x \in K : v(x) \geq n\} \qquad (n \geq 0).$$

   Ferner gilt $\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong \mathfrak{O}/\mathfrak{p}$.

Bem.

- Im folgenden sei v diskret, normiert, $q > 1$ fest und $|x| = q^{-v(x)}$.
- Die Idealkette
$$\mathfrak{O} \supseteq \mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \mathfrak{p}^3 \supseteq \dots$$
ist eine Umgebungsbasis der Null, denn
$$\mathfrak{p}^n = \{x \in K : |x| < \frac{1}{q^{n-1}}\}.$$
- Die Kette
$$\mathfrak{O}^x := U^{(0)} \supseteq U^{(1)} \supseteq U^{(2)} \supseteq \dots$$
der Einseinheitengruppen
$$U^{(n)} = 1 + \mathfrak{p}^n = \{x \in K^\times : |1 - x| < \frac{1}{q^{n-1}}\} \qquad (n > 0)$$
ist eine Umgebungsbasis der Eins.

Satz 54 Es existiert ein natürlicher Isomorpismus
$$\mathfrak{O}^\times / U^{(n)} \xrightarrow{\sim} \left(\mathfrak{O}/\mathfrak{p}^n \right)^\times \qquad (n \in \mathbb{N})$$
und ein von der Wahl des Primelements π unabhängiger Isomorpismus
$$U^{(n)}/U^{(n+1)} \xrightarrow{\sim} \mathfrak{O}/\mathfrak{p} \qquad (n \in \mathbb{N}).$$

12 Komplettierung

Bem.

- Ein Körper K mit einer Bewertung $|\cdot|$ heißt *vollständig*, wenn in ihm jede Cauchy-Folge (a_n) bezüglich $|\cdot|$ gegen ein Element $a \in K$ konvergiert.
- Jeder bewertete Körper K läßt sich isometrisch einbetten in einen vollständigen Körper $\hat{K}$, in dem K dicht liegt. $\hat{K}$ heißt *Komplettierung* von K und ist bis auf isometrische Isomorphie eindeutig bestimmt.
- Bezeichnet R den Ring aller Cauchy-Folgen in K und $\mathfrak{m}$ das maximale Ideal aller Nullfolgen in R, so ist
$$\hat{K} = R/\mathfrak{m}.$$
K läßt sich in $\hat{K}$ einbetten via
$$a \mapsto (a, a, a, \dots) + \mathfrak{m}.$$
Die Bewertung von K läßt sich auf $\hat{K}$ fortsetzen durch die Definition
$$|(a_n)_{n=1}^\infty + \mathfrak{m}| := \lim_{n \to \infty} |a_n|.$$

Bsp. $\mathbb{R}$ und $\mathbb{C}$ sind vollständig bezüglich des archimedischen Betrags.

Satz 55 (Satz von OSTROWSKI) Sei K vollständig bezüglich des archimedischen Betrags $|\cdot|$. Dann gibt es einen Isomorphismus $\sigma : K \xrightarrow{\sim} \mathbb{R}$ oder $\sigma : K \xrightarrow{\sim} \mathbb{C}$ und ein $s > 0$, so daß

$$\forall \quad a \in K : \qquad |a| = |\sigma(a)|_\infty^s .$$

Bem. Nun sei v nicht-archimedische Exponentialbewertung eines Körpers K. $\hat{K}$ sei die Komplettierung von K bezüglich v, und für jede CAUCHY-Folge $(a_n)_{n=1}^\infty$ sei

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

$\mathfrak{O} \subseteq K$ und $\hat{\mathfrak{O}} \subseteq \hat{K}$ seien die Bewertungsringe von v bzw. $\hat{v}$ und $\mathfrak{p}, \hat{\mathfrak{p}}$ die zugehörigen maximalen Ideale.

Satz 56 Restklassenkörper und Wertegruppe ändern sich nicht beim Übergang zur Komplettierung. Genauer gilt:

$$\hat{\mathfrak{O}}/\hat{\mathfrak{p}} \cong \mathfrak{O}/\mathfrak{p}, \qquad v(K^\times) = \hat{v}(\hat{K}^\times).$$

Ist v diskret, so gilt

$$\hat{\mathfrak{O}}/\hat{\mathfrak{p}}^n \cong \mathfrak{O}/\mathfrak{p}^n \qquad (n \in \mathbb{N}).$$

Bem. Sei $\mathcal{R}$ ein Restsystem, d. h. ein Vertretersystem des Restklassenkörpers $K = \mathfrak{O}/\mathfrak{p}$ mit $0 \in \mathcal{R}$. Weiter sei $\pi \in \mathfrak{O}$ prim.

Satz 57 Jedes $x \neq 0$ in $\hat{K}$ ist eindeutig darstellbar als konvergente Reihe

$$x = \pi^m (a_0 + a_1 \pi + a_2 \pi^2 + \dots)$$

mit $a_i \in \mathcal{R}, a_0 \neq 0, m \in \mathbb{Z}$.

Bsp.

- Seien $K = \mathbb{Q}$, $v_p = \mathrm{ord}_p$, $\mathcal{R} = \{0, 1, 2, \dots, p-1\}$ und $\pi = p$. Dann ist in $\hat{K} = \mathbb{Q}_p$ jedes Element von der Form

  $$x = p^m (a_0 + a_1 p + a_2 p^2 + \dots)$$

  mit $0 \leq a_i < p$.

- Sei k ein beliebiger Körper und $K = k(t)$ der Körper der rationalen Funktionen über k. Ferner seien $a \in K$ fest und $\mathfrak{p} = (t - a) \trianglelefteq k[t]$ maximal. $v_\mathfrak{p}$ sei die zugehörige Exponentialbewertung, $\mathcal{R} = k, \pi = t - a$. Dann ist $\hat{K} = k((t - a))$ der Körper der formalen Potenzreihen.

Def. 30 Sei K vollständig bezüglich der diskreten Bewertung v, $\mathfrak{p} \subseteq \mathfrak{O} \subseteq K$. Ferner sei

$$\lambda_\nu : \mathfrak{O}/\mathfrak{p}^{\nu+1} \to \mathfrak{O}/\mathfrak{p}^\nu, \quad x + \mathfrak{p}^{\nu+1} \mapsto x + \mathfrak{p}^\nu \qquad (\nu \in \mathbb{N}).$$

Dann heißt

$$\varprojlim_n \mathfrak{O}/\mathfrak{p}^n := \{(x_n)_{n=1}^\infty \in \prod_{n=1}^\infty \mathfrak{O}/\mathfrak{p}^n : \lambda_n(x_{n+1}) = x_n\} \subseteq \prod_{n=1}^\infty \mathfrak{O}/\mathfrak{p}^n$$

der *Projektive Limes* der Kette

$$\mathfrak{O}/\mathfrak{p} \xleftarrow{\lambda_1} \mathfrak{O}/\mathfrak{p}^2 \xleftarrow{\lambda_2} \mathfrak{O}/\mathfrak{p}^3 \xleftarrow{\lambda_3} \ldots.$$

$\mathfrak{O}/\mathfrak{p}^n$ sei versehen mit der diskreten Topologie, d. h. jede Teilmenge wird als offen betrachtet, $\prod_{n=1}^\infty \mathfrak{O}/\mathfrak{p}^n$ sei versehen mit der Produkttopologie.

Bem. Der Projektive Limes ist ein Teilring des Produkts $\prod_{n=1}^\infty \mathfrak{O}/\mathfrak{p}^n$.

Satz 58 Die natürlichen Abbildungen

$$\alpha : \mathfrak{O} \to \varprojlim_n \mathfrak{O}/\mathfrak{p}^n, \qquad \alpha(x) := (x + \mathfrak{p}^n)_{n=1}^\infty$$

$$\beta : \mathfrak{O}^\times \to \varprojlim_n \mathfrak{O}^\times/U^{(n)}, \qquad \beta(x) := (x + U^{(n)})_{n=1}^\infty.$$

sind Isomorphismen und Homöomorphismen.

Def. 31 K sei vollständig bezüglich der nicht-archimedischen Bewertung v. Zu $f(X) = \sum_{\nu=0}^n a_\nu X^\nu$ sei

$$|f| := \max_{\nu=0}^n |a_\nu|.$$

Ein Polynom $f(X) \in \mathfrak{O}[X]$ heißt *primitiv*, wenn nicht alle Koeffizienten in $\mathfrak{p}$ liegen.

Satz 59 (Henselsches Lemma) Sei $f \in \mathfrak{O}[X]$ primitiv und f besitze modulo $\mathfrak{p}$ eine Produktzerlegung

$$\bar{f}(X) = \bar{g}(X) \cdot \bar{h}(X)$$

mit teilerfremden Polynomen $\bar{g}, \bar{h} \in k[X]$. Dann zerfällt f als $f = g \cdot h$ mit $g, h \in \mathfrak{O}[X]$, $\partial g = \partial \bar{g}$ und $g \bmod \mathfrak{p} = \bar{g}$, $h \bmod \mathfrak{p} = \bar{h}$.

Bsp. Sei $K = \mathbb{Q}_p$, $\mathfrak{O} = \mathbb{Z}_p$, $f = X^{p-1} - 1$ und

$$K = \mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p.$$

Dann gilt $\bar{f} = \prod_{i=1}^{p-1} (X - \bar{i})$ und aus Hensels Lemma folgt

$$\exists \quad \zeta_i \in \mathfrak{O} : \qquad f = \prod_{i=1}^{p-1} (X - \zeta_i).$$

Wegen

$$f(\zeta_i) = 0 \iff \zeta_i^{p-1} = 1 \iff \zeta_i \text{ ist } (p-1)\text{-te Einheitswurzel}$$

folgt daraus die Existenz von $(p-1)$-ten Einheitswurzeln in $\mathbb{Z}_p$.

Bem. Diese Einheitswurzeln bilden mit 0 ein vollständiges Restsystem, sogar ein bezüglich Multiplikation abgeschlossenes.

Satz 60 Ist $f = a_0 + a_1X + \cdots + a_nX^n \in K[X]$ irreduzibel, so gilt

$$|f| = \max\{|a_0|, |a_n|\}.$$

Insbesondere folgt für $a_n = 1, a_0 \in \mathfrak{O}$, daß $f \in \mathfrak{O}[X]$.

Satz 61 (Fortsetzungssatz) Sei K vollständig bezüglich $|\cdot|$ (archimedisch oder nicht-archimedisch), und sei L/K eine algebraische Erweiterung. Dann gilt:

1. $|\cdot|$ besitzt eine eindeutige Fortsetzung zu einer Bewertung von L.
2. Falls $(L : K) = n$ endlich ist, ist die Fortsetzung gegeben durch

$$|\alpha| := \sqrt[n]{|\mathcal{N}_{L/K}(\alpha)|} \geq 0$$

   und L ist auch vollständig.

Satz 62 Sei K vollständig bezüglich $|\cdot|$, V ein n-dimensionaler K-Vektorraum. Dann sind alle Normen auf V äquivalent, d. h. zu je zwei Normen $||\cdot||_1$, $||\cdot||_2$ auf V existeren Konstanten $\varrho, \varrho' > 0$ mit

$$\forall \quad x \in V: \qquad \varrho||x||_1 \leq ||x||_2 \leq \varrho'||x||_1.$$

Insbesondere ist V homöomorph zu K^n versehen mit der Maximumsnorm

$$||(x_1, \ldots, x_n)||_{\max} = \max_i |x_i|$$

und somit vollständig.

13 Lokale Körper

Def. 32 Ein Körper K mit nicht-archimedischer Bewertung v heißt *lokaler* Körper, falls gilt:

1. K ist vollständig bezüglich v,
2. v ist diskret,
3. Der Restklassenkörper $k = {}^{\mathfrak{O}}\!/_{\mathfrak{p}}$ ist endlich.

$v_\mathfrak{p}$ bezeichnet die durch $v_\mathfrak{p}(K^\times) = \mathbb{Z}$ normierte Bewertung, der zugehörige Betrag $|\cdot|_\mathfrak{p}$ mit $|x|_\mathfrak{p} := |k|^{-v_\mathfrak{p}(x)}$.

Satz 63 Jeder lokale Körper ist lokal kompakt. Der Bewertungsring $\mathfrak{O}$ eines lokalen Körpers ist kompakt.

Satz 64 K ist genau dann ein lokaler Körper, wenn K endliche Erweiterung eines $\mathbb{Q}_p$ oder $\mathbb{F}_p((t)) = \mathrm{Quot}(\mathbb{F}_p[[t]])$ ist.

Def. 33 Die lokalen Körper der Charakteristik $p \neq 0$ heißen *Potenzreihenkörper* $\mathbb{F}_q((t))$ mit $q = pf$. Die lokalen Körper der Charakteristik 0 sind die $\mathfrak{p}$-adischen Zahlkörper $K/\mathbb{Q}_p$.

Satz 65 Die multiplikative Gruppe eines lokalen Körpers K besitzt die Zerlegung

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

Dabei sind $\pi^{\mathbb{Z}}$ die zyklische Gruppe erzeugt vom Primelement π, μ_{q-1} die Gruppe der $(q-1)$-ten Einheitswurzeln ($q = |k|$) und $U^{(1)} = 1 + \mathfrak{p}$ die Einseinheitengruppe in $\mathfrak{O}^\times$.

Satz 66 Sei K ein $\mathfrak{p}$-adischer Zahlkörper. Dann existiert ein eindeutig bestimmter stetiger Homomorphismus $\log : K^\times \to K$ mit $\log(p) = 0$, der für $1+x \in U^{(1)}$ durch die übliche Reihe

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

gegeben ist.

Satz 67 Sei $K/\mathbb{Q}_p$ ein $\mathfrak{p}$-adischer Zahlkörper mit $p \cdot \mathfrak{O} = \mathfrak{p}^e$. Dann konvergiert die Potenzreihe

$$\exp(x) = \sum_{\nu=0}^{\infty} \frac{x^\nu}{\nu!}$$

für alle $x \in \mathfrak{p}^n$ ($n \geq \frac{e}{p-1}$) und definiert den Isomorphismus und Homöomorphismus

$$\exp : \mathfrak{p}^n \to U^{(n)} = 1 + \mathfrak{p}^n$$

mit der Inversen $\exp^{-1} = \log$.

Satz 68 Sei $\nu \in \mathbb{N}$ mit der p-adischen Entwicklung

$$\nu = \sum_{i=0}^{r} a_i p^i, \qquad 0 \leq a_i < p$$

und $s_\nu = \sum_{i=0}^{r} a_i$. Dann gilt:

$$\mathrm{ord}_p(\nu!) = \frac{\nu - s_\nu}{p-1}.$$

Bem. Für eine p-adisch konvergente Folge $(z_n)_{n=1}^{\infty}$ in $\mathbb{Z}$ mit

$$z = \lim_{n\to\infty} z_n \in \mathbb{Z}_p$$

existiert auch der Limes

$$\lim_{n\to\infty} (1+x)^{z_i} =: (1+x)^z \qquad (1+x \in U^{(1)}).$$

Damit wird $U^{(1)}$ zum $\mathbb{Z}$-Modul.

Satz 69 Sei K ein lokaler Körper und $q = p^f = |\mathfrak{O}/\mathfrak{p}|$. Dann existiert ein algebraischer und topologischer Isomorphismus

1. im Fall $\operatorname{char} K = 0$:
$$K^\times \cong \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^d$$

2. im Fall $\operatorname{char} K = p$:
$$K^\times \cong \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}_p^{\mathbb{N}}$$

Bem. Sei $\operatorname{char} K \nmid n \in \mathbb{N}$. Dann gilt
$$(K^\times : K^{\times n}) = n(U : U^n) = \frac{n}{|n|_\mathfrak{p}} \cdot |\mu_n(K)|.$$
Dabei seien $K^{\times n} = \{k^n : k \in K^\times\}$, $U = \mathfrak{O}^\times$ und $U^n = \{u^n : u \in U\}$.

14 Zahm verzweigte Erweiterungen

In diesem Abschnitt sei K vollständig bezüglich v, $|\cdot|$ nicht-archimedisch $\mathfrak{o}$ der ganze Abschluß von $\mathbb{Z}$, $\mathfrak{p} \trianglelefteq \mathfrak{o}$ maximal prim, $k = \mathfrak{o}/\mathfrak{p}$ und L/K algebraisch. w sei die Fortsetzung von v auf L, $\mathfrak{O}, \mathfrak{P}, l$ seien die Entsprechungen von $\mathfrak{o}, \mathfrak{p}, k$ in L.

Def. 34 Eine endliche Erweiterung L/K heißt *unverzweigt*, wenn die Erweiterung der Restklassenkörper l/k sparabel ist und gilt
$$(L : K) = (l : k).$$
Eine beliebige algebraische Erweiterung L/K heißt *unverzweigt*, falls L Vereiningung endlicher unverzweigter Teilerweiterung ist.

Satz 70 Seien $L/K, K'/K$ mit $L, K' \subseteq \bar{K}$, $\bar{K}$ der algebraische Abschluß von K. Weiter sei $L' = LK'$. Dann gilt:

1. Ist L/K unverzweigt, dann auch L'/K'.
2. Jede Teilerweiterung einer unverzweigten Erweiterung ist unverzweigt.

Bem. Das Kompositum zweier unverzweigter Erweiterungen von K ist unverzweigt.

Def. 35 Sei L/K algebraische Erweiterung, T mit $K \subseteq T \subseteq L$ Komposition aller unverzweigten Teilerweiterungen von K. Dann heißt T die *maximale* unverzweigte Teilerweiterung von L/K. L/K heißt *reinverzweigt*, falls $T = K$.

Satz 71 Der Restklassenkörper von T ist der separable Abschluß l_{sep} von k in l/k. Die Wertegruppe von T ist gleich der von K.

Def. 36 L/K heißt *zahm* verzweigt, falls die Restklassenkörpererweiterung L/K separabel ist und gilt $p \nmid (L : T)$, d. h. der Grad jeder endlichen Teilerweiterung ist nicht durch p teilbar.

Satz 72 Eine endliche Erweiterung L/K ist genau dann zahm verzweigt, wenn L/T eine Radikalerweiterung der Form

$$L = T(\sqrt[m_1]{a_1}, \ldots, \sqrt[m_r]{a_r})$$

ist mit $p \nmid m_i$. In diesem Fall gilt die fundamentale Gleichung

$$(L : K) = e(L/K) \cdot f(L/K)$$

mit der Verzweigungsordnung

$$e := e(L/K) := (w(L^\times) : v(K^\times))$$

und dem Restklassengrad

$$f := f(L/K) := (l : k).$$

Satz 73 Seien L/K, K'/K algebraische Erweiterungen, $L, K' \subseteq \bar{K}$, $L' = LK'$. Dann gilt:

1. Wenn L/K zahm ist, dann auch L'/K'.
2. Jede Teilerweiterung einer zahm verzweigten Erweiterung ist zahm.

Bem. Das Kompositum zahm verzweigter Erweiterungen ist zahm verzweigt.

Def. 37 Sei L/K eine algebraische Erweiterung. Das Kompositum V/K aller zahm verzweigten Teilerweiterungen von L/K ist die maximale zahm verzweigte Teilerweiterung von L/K:

$$w(L^\times)^{(p)} = \{w \in w(L^\times) : \exists\, m \in \mathbb{N} : p \nmid m, m \cdot w \in v(K^\times)\}.$$

Satz 74 Die maximale zahm verzweigte Teilerweiterung V/K von L/K hat die Wertegruppe

$$w(V^\times) = w(L^\times)^{(p)}$$

und als Restklasssenkörper den separablen Abschluß l_{sep} von k in l.

15 Fortsetzungen von Bewertungen

Sei K ein beliebiger Körper, v eine Bewertung von K, K_v die Komplettierung von K bezüglich v, $\bar{K}_v$ der algebraische Abschluß von v, $\bar{v}$ sei die eindeutig bestimmte Fortsetzung von v auf $\bar{K}_v$. Weiter sei L/K eine algebraische Erweiterung, $\tau : L \to \bar{K}_v$ eine Injektion und $w = \bar{v} \circ \tau$, so daß also $|x|_w = |\tau(x)|_{\bar{v}}$ $(x \in L)$.

Def. 38 Die *Lokalisierung* L_w von L bezüglich w ist definiert als:

1. die Komplettierung von L bezüglich w, falls L/K endlich ist, bzw.
2. $\bigcup_i (L_i)_{w_i}$ wobei L_i/K über alle endlichen Teilerweiterungen von L/K läuft, sonst.

Satz 75 (Fortsetzungssatz) Sei L/K algebraische Körpererweiterung und v Bewertung von K. Dann gilt:

1. Zu jeder Bewertungsfortsetzung w existiert eine K-Einbettung $\tau : L \to \bar{K}_v$, so daß $w = \bar{v} \circ \tau$.
2. Für $w' = \bar{v} \circ \tau'$ gilt:
$$w = w' \quad \Longleftrightarrow \quad \tau, \tau' \text{ sind über } K_v \text{ konjugiert.}$$

Satz 76 Sei $f(X) \in K[X]$ irreduzibel und $L = K(\alpha)$ mit $f(\alpha) = 0$. Ferner sei

$$f(X) = \prod_{i=1}^{r} f_\varrho(X)^{m_\varrho}$$

in $K_v[X]$ mit f_ϱ in $K_v[X]$ irreduzibel. Dann entsprechen die $f_1, \ldots, f_r$ umkehrbar eindeutig den Fortsetzungen $w_1, \ldots, w_r$ von v auf L.

Def. 39 Sei L/K endlich, v Bewertung von K, w Bewertung von L. *Teilbarkeit* von Bewertungen ist definiert als

$$w \mid v \quad :\Longleftrightarrow \quad w|_K = v.$$

Bem. Für jede Bewertung w mit $w \mid v$ sei der Homomorphismus

$$\varphi_w : L \otimes_K K_v \to L_w, \qquad a \otimes b \mapsto a \cdot b$$

definiert. Mit diesen werde

$$\varphi := \prod_{w|v} \varphi_w : L \otimes_K K_v \to \prod_{w|v} L_w$$

definiert. $L \otimes_K K_v$ ist K_v-Vektorraum vermöge

$$K_v \times L \otimes_K K_v \to L \otimes_K K_v, \qquad (\lambda, a \otimes b) \mapsto a \otimes \lambda b$$

und ferner mit der Multiplikation

$$(a \oplus b) \cdot (a' \oplus b') := a \cdot a' \oplus b \cdot b'$$

eine K_v-Algebra. Damit ist φ Homomorphismus von K_v-Algebren.

Satz 77 Ist L/K separabel, so definiert φ einen Isomorphismus

$$L \otimes_K K_v \xrightarrow{\sim} \prod_{w|v} L_w.$$

Bem. Ist L/K separabel, so ist

$$(L : K) = \sum_{w|v} (L_w : K_v)$$

und für $\alpha \in L$ gilt

$$\mathcal{N}_{L/K}(\alpha) = \prod_{w|v} \mathcal{N}_{L_w/K_v}(\alpha), \mathrm{Tr}_{L/K}(\alpha) = \sum_{w|v} \mathrm{Tr}_{L_w/K_v}(\alpha).$$

Satz 78 Ist v diskret und L/K endlich separabel, so gilt

$$\sum_{w|v} e_w f_w = (L : K).$$

Bem. Obiger Satz ist die bewertungstheoretische Variante der fundamentalen Gleichung für Quotientenkörper von DEDEKIND-Ringen (vgl. S. 26).

16 GALOIS-Theorie von Bewertungen

Sei L/K eine GALOIS-Erweiterung beliebiger Körper, v eine Bewertung von K, $w \mid v$ eine Fortsetzung von v auf L und $G = \mathrm{Gal}(L/K)$.

Bem. Für alle $\sigma \in G$ ist $w^\sigma := w \circ \sigma$ ebenfalls eine Fortsetzung von v ($|x|_{w^\sigma} = |\sigma(x)|_w$). G operiert auf der Menge der Fortsetzungen $w \mid v$.

Satz 79 G operiert transitiv auf $\{w : w \mid v\}$.

Def. 40 Die Fixgruppe einer Fortsetzung $w \mid v$,

$$G_w := G_w(L/K) := \{\sigma \in G : w^\sigma = w\}$$

heißt die *Zerlegungsgruppe* von w. Für nicht-archimedisches v seien $\mathfrak{o}, \mathfrak{p}, k = {}^{\mathfrak{o}}/_{\mathfrak{p}}$ zu v und $\mathfrak{O}, \mathfrak{P}, l = {}^{\mathfrak{O}}/_{\mathfrak{P}}$ zu w.

Def. 41 Für nichtarchimedische v und $w \mid v$ heißt

$$I_w := I_w(L/K) = \{\sigma \in G_w : \sigma(x) \equiv x(\mathfrak{P})\ (x \in \mathfrak{O})\}$$

die *Trägheitsgruppe* von w und

$$R_w := R_w(L/K) = \{\sigma \in G_w : \frac{\sigma(x)}{x} \equiv 1(\mathfrak{P})\ (x \in L^\times)\}$$

heißt die *Verzweigungsgruppe* von w.

Bem.

- Für $\sigma \in G_w$ ist $\mathfrak{O} = \sigma\mathfrak{O}$ und $\frac{\sigma(x)}{x} \in \mathfrak{O}^\times$ $(x \in L^\times)$, denn $|\sigma(x)|_w = |x|_w$.
- G_w, I_w und R_w sind abgeschlossene Untergruppen von G bezüglich der KRULL-Topologie.
- Gegeben sei ein kommutatives Diagramm zweier GALOIS-Erweiterungen L/K und L'/K':

$$\begin{tikzcd} L \arrow[r, "\tau"] & L' \\ K \arrow[u, "\subseteq"] \arrow[r, "\tau"'] & K' \arrow[u, "\subseteq"'] \end{tikzcd}$$

  Dies definiert Homomorphismen der GALOIS-Gruppen

$$\tau^* : \mathrm{Gal}(L'/K') \to \mathrm{Gal}(L/K), \qquad \sigma' \mapsto \tau^{-1}\sigma'\tau.$$

  Mit L/K ist auch $L/\tau K$ normal, also gilt $\sigma'\tau L \subseteq \tau L$, so daß τ^* wohldefiniert ist.

- Es sei w' eine Bewertung von L', $v' := w|_{K'}, w := w' \circ \tau$ und $v := w|_K$.

Satz 80 Die Einschränkung von τ^* definiert Homomorphismen zwischen

$$G_{w'}(L'/K') \to G_w(L/K)$$

und bei nicht archimedischem v ferner zwischen

$$I_{w'}(L'/K') \to I_w(L/K) \qquad \text{sowie} \qquad R_{w'}(L'/K') \to R_w(L/K).$$

Bem. Falls $K = K', L = L'$ und $\tau \in \mathrm{Gal}(L/K)$, so gilt

$$G_{w^\tau} = \tau^{-1} G_w \tau, \qquad I_{w^\tau} = \tau^{-1} I_w \tau, \qquad R_{w^\tau} = \tau^{-1} R_w \tau.$$

Falls $L = L'$, $K \subseteq K' =: M$, $\tau = \mathrm{id}_L$, so ist

$$\tau^* : \mathrm{Gal}(L/M) \xrightarrow{\subseteq} \mathrm{Gal}(L/K)$$

die Inklusion.

Satz 81 Für jeden Zwischenkörper M $(K \subseteq M \subseteq L)$ gilt:

$$\begin{aligned} G_w(L/M) &= G_w(L/K) \cap G(L/M) \\ I_w(L/M) &= I_w(L/K) \cap G(L/M) \\ R_w(L/M) &= R_w(L/K) \cap G(L/M). \end{aligned}$$

Satz 82 Es gilt:

$$G_w(L/K) \cong G(L_w/K_v),\ I_w(L/K) = I(L_w/K_v),\ R_w(L/K) = R(L_w/K_v).$$

Def. 42 Der Fixkörper

$$Z = Z_w(L/K) = \{x \in L : \sigma(x) = x \ (\sigma \in G_w)\}$$

von G_w heißt *Zerlegungskörper* von w über K.

Satz 83

1. Die Einschränkung w_Z von w auf Z besitzt genau eine Fortsetzung auf L, nämlich w.
2. w_z und v besitzen den gleichen Restklassenkörper und die gleiche Wertgruppe.
3. $Z = L \cap K_v \subseteq L_w$.

Bem. Sei w nicht-archimedisch, $\sigma \in G_w$. Dann ist $\sigma\mathfrak{O} = \mathfrak{O}$ und $\sigma\mathfrak{P} = \mathfrak{P}$. Also definiert σ einen k-Automorphismus von $l = {}^{\mathfrak{O}}/_{\mathfrak{P}}$. Sei

$$\bar{\sigma} : l \to l, \quad x \bmod \mathfrak{P} \mapsto \sigma x \bmod \mathfrak{P}.$$

Dies liefert einen Homomorphismus

$$r : G_w \to \mathrm{Aut}(l/k), \qquad r(\sigma) = \bar{\sigma}$$

mit

$$\mathrm{Kern}\, r = \{\sigma \in G_w : \sigma x = x \bmod \mathfrak{P} \ (x \in \mathfrak{O})\} = I_w.$$

Satz 84 l/k ist normal und die Sequenz

$$1 \to I_w \xrightarrow{\subseteq} G_w \xrightarrow{r} \mathrm{Aut}(l/k) \to 1$$

ist exakt.

Def. 43 Der Fixkörper $T = T_w(L/K) = L^{I_w}$ heißt *Trägheitskörper* von w über K.

Bem. Es gilt

$$G_w/I_w = \mathrm{Gal}(T/Z) \cong \mathrm{Aut}(l/K).$$

Satz 85 T/Z ist die bei w_z maximale unverzweigte Teilerweiterung von L/Z.

Bem. Die Verzweigungsgruppe R_w ist der Kern des natürlichen Homomorphismus

$$\chi : I_w \to \mathrm{Hom}(w(L^\times)/v(K^\times), l^\times), \qquad \sigma \mapsto \chi_\sigma,$$

wobei für $\delta = \omega(x)$ gilt

$$\chi_\sigma(\delta \cdot v(K^\times)) := \frac{\sigma(x)}{x} \bmod \mathfrak{P}.$$

Satz 86 Sei $p = \mathrm{char}(k) > 0$. Dann gilt: R_w ist die einzige (pro-)p-Sylow-Gruppe von I_w.

Def. 44 $V = V_w(L/K) = L^{R_w}$ heißt der *Verzweigungskörper* von w über K.

Satz 87 V/Z ist die maximale zahm verzweigte Teilerweiterung von L/Z.

Bem. Es gilt die exakte Sequenz

$$1 \to R_w \to I_w \to \mathrm{Hom}(w(L^\times)/v(K^\times), l^\times) \to 1.$$

Index