Die Sätze von Hermite und Minkowski im Zahl- und Funktionenkörperfall

Andrin Schmidt

8. Juni 2009

Betreut durch:

Prof. Richard Pink Thomas Huber

Einleitung

Diese Bachelor-Arbeit besteht nebst einer kurzen Repetition, beziehungsweise Einführung, der benötigten Begriffe, grundsätzlich aus zwei Teilen.
Im ersten Teil soll der Satz von Hermite (welcher besagt, dass über einem beliebigen Zahlkörper nur endlich viele Zahlkörper mit einer festen Diskriminante existieren), sowie der Satz von Minkowski (welcher besagt, dass die Diskriminante jedes von $\mathbb{Q}$ verschiedenen Zahlkörpers betragsmässig grösser als Eins ist) bewiesen werden. Dieser Teil folgt Neukirch, Kap. I §2 – 5, 8 sowie Kap. III §1, 2.
Im zweiten Teil sollte als Analogon des Satzes von Hermite der folgende Satz bewiesen werden:

Theorem: Sei $K = \mathbb{F}(t)$ und seien $d, d' \in \mathcal{O}_K, n \in \mathbb{N}$. Es existieren nur endlich viele separable endliche Erweiterungen L von K mit $d_L = d$, $[L : K] = n$ und $(d_L)_\infty = d'$.

Dabei sollte Wert darauf gelegt werden im Beweis die Analogie der beiden Sätze deutlich zu machen (im Funktionenkörperfall wird der Satz üblicherweise mithilfe des Satzes von Riemann-Roch bewiesen, siehe Rosen, Chap. 5, 6). Der vollständige Beweis ist allerdings nicht gelungen, weshalb nur eine deutlich schwächere Fassung des Satzes (in welcher zusätzlich gefordert wird, dass die Erweiterung voll zerlegt ist, wodurch die Bedingung an die lokale Diskriminante redundant wird) bewiesen wird. Dieser Teil folgt Neukirch, Kap. I §2, 3 sowie Kap. II §2 – 5, 7, 8 und Weil[1], Chap. I und Chap. II, §1, 2 und zur Einführung von Funktionenkörpern Rosen, Chap. 5.
Vorausgesetzt wird zudem der Inhalt einer zwei-semestrigen Algebra Vorlesung, sowie Grundwissen in Topologie und Masstheorie.

Inhaltsverzeichnis

1 Vorkenntnisse

§1 Zahl- und Funktionenkörper

Dieser Abschnitt folgt NEUKIRCH, Kap. I, §2, 3 in Bezug auf Zahlkörper, separable Körpererweiterungen und Dedekindringe, sowie ROSEN, Chap. 5 in Bezug auf Funktionenkörper. Insbesondere sind alle nicht bewiesenen Aussagen dort nachzulesen.

(1.1) **Definition:** Eine endliche Körpererweiterung von $\mathbb{Q}$ heisst *Zahlkörper*.

(1.2) **Bemerkung:** Wegen $\operatorname{char}\mathbb{Q} = 0$ ist jede Körpererweiterung über $\mathbb{Q}$ separabel. Also ist nach dem Satz vom primitiven Element jeder Zahlkörper von der Form $\mathbb{Q}(\alpha)$ für ein algebraisches Element α. Ist umgekehrt $\overline{\mathbb{Q}}$ der algebraische Abschluss von $\mathbb{Q}$ (in $\mathbb{C}$), so ist $\mathbb{Q}(\alpha)$ für jedes $\alpha \in \overline{\mathbb{Q}}$ ein Zahlkörper.

(1.3) **Definition:** Sei $\mathbb{F}$ ein Körper. Eine endlich erzeugte Körpererweiterung vom Transzendenzgrad 1 von $\mathbb{F}$ heisst *Funktionenkörper* über $\mathbb{F}$.

(1.4) **Bemerkung:** Offensichtlich ist $\mathbb{F}(t)$ ein Funktionenkörper über $\mathbb{F}$, und durch Wahl einer Transzendenzbasis $\{t\}$ lässt sich jeder Funktionenkörper über $\mathbb{F}$ als endliche Erweiterung von $\mathbb{F}(t)$ auffassen.

(1.5) **Bemerkung:** Funktionenkörper brauchen im Allgemeinen keine separable Erweiterungen von $\mathbb{F}(t)$ zu sein; beispielsweise ist $X^p - r \in \big(\mathbb{F}_p(t)\big)[X]$ für jedes irreduzible Polynom $r \in \mathbb{F}_p[t]$ inseparabel (da $(X^p - r)' = 0$ ist) und irreduzibel (nach dem Eisensteinkriterium).

Sei im Folgenden $L|K$ eine separable Körpererweiterung vom Grad n.

(1.6) **Bemerkung:** Es existieren genau n verschiedene K-Einbettungen

$$\sigma_1, \ldots, \sigma_n : L \to \overline{K}.$$

(1.7) **Satz:** Es existieren nur endlich viele Zwischenkörper von K und L.

Beweis: Sei L^{Gal} der Galois-Abschluss von L in einem algebraischen Abschluss $\overline{L}$. Nach der Galois-Korrespondenz

$$\{\text{Zwischenkörper von } K \text{ und } L^{\mathrm{Gal}}\} \leftrightarrow \{\text{Untergruppen von } \mathrm{Gal}(L^{\mathrm{Gal}}|K)\}$$

existieren sogar nur endlich viele Zwischenkörper von K und L^{Gal}. □

(1.8) **Lemma:** Seien $\alpha \in L$ und $1 \leq i \leq n$, sodass $\sigma_i(\alpha) \neq \sigma_j(\alpha)$, falls $i \neq j$. Dann gilt $L = K(\alpha)$.

Beweis: Man nehme an, es sei $K(\alpha) \subsetneq L$. Dann besitzt $\sigma_i|_{K(\alpha)} : K(\alpha) \to \overline{K}$ eine von σ_i verschiedene Fortsetzung σ auf L. Da diese aber offensichtlich eine K-Einbettung von L in $\overline{K}$ ist, muss sie eine der Einbettungen $\sigma_1, \ldots, \sigma_n$ sein, was im Widerspruch steht zu $\sigma \neq \sigma_i$ und $\sigma(\alpha) \neq \sigma_j(\alpha)$ für $i \neq j$. □

(1.9) **Definition:** Sei $x \in L$ und es bezeichne $T_x : L \to L$ die K-lineare Abbildung $\alpha \mapsto x\alpha$. Dann heissen $\mathrm{N}_{L|K}(x) := \det_K(T_x)$ *Norm* und $\mathrm{Tr}_{L|K}(x) := \mathrm{Tr}_K(T_x)$ *Spur* von x.

(1.10) **Bemerkung:** Wegen $T_{x+y} = T_x + T_y$ und $T_{xy} = T_x \circ T_y$ gilt:

i. Die Abbildung $\mathrm{Tr}_{L|K} : L \to K$ ist ein Homomorphismus zwischen den additiven Gruppen von L und K.

ii. Die Abbildung $\mathrm{N}_{L|K} : L^* \to K^*$ ist ein Homomorphismus zwischen den multiplikativen Gruppen von L und K.

(1.11) **Lemma:** Es gilt

i. $\mathrm{Tr}_{L|K}(x) = \sum_{i=1}^{n} \sigma_i(x)$ und

ii. $\mathrm{N}_{L|K}(x) = \prod_{i=1}^{n} \sigma_i(x)$.

(1.12) **Korollar:** Sei $M|L$ eine weitere endliche separable Körpererweiterung. Dann gilt $\mathrm{Tr}_{L|K} \circ \mathrm{Tr}_{M|L} = \mathrm{Tr}_{M|K}$ und $\mathrm{N}_{L|K} \circ \mathrm{N}_{M|L} = \mathrm{N}_{M|K}$.

(1.13) **Definition:** Seien $x_1, \ldots, x_n \in L$.

$$d(x_1, \ldots, x_n) := \det\left((\sigma_i(x_j))_{i,j=1}^{n}\right)^2$$

heisst *Diskriminante* von $x_1, \ldots, x_n$.

(1.14) **Lemma:** Es gilt $d(x_1, \ldots, x_n) \neq 0$ genau dann, wenn $\{x_1, \ldots, x_n\}$ eine Basis von L über K ist.

(1.15) **Lemma:** Seien $\{x_1, \ldots, x_n\}$, $\{y_1, \ldots, y_n\}$ zwei Basen von L über K und sei $A = (a_{ij})_{i,j=1}^{n}$ die Transformationsmatrix der Basen, das heisst $y_i = \sum_{j=1}^{n} a_{ij} x_j$. Dann gilt:

$$d(y_1, \ldots, y_n) = \det(A)^2 d(x_1, \ldots, x_n).$$

Seien nun $K \subset L$ zudem Zahl- oder Funktionenkörper, $[K : \mathbb{Q}] = m$, beziehungsweise $[K : \mathbb{F}(t)] = m$, wobei $\{t\}$ eine feste Transzendenzbasis von K bezeichne, und sei $A = \mathbb{Z}$, beziehungsweise $A = \mathbb{F}[t]$.

(1.16) **Definition:** Der ganze Abschluss von A in K heisst *Ganzheitsring* von K und wird mit $\mathcal{O}_K$ bezeichnet.

(1.17) **Bemerkung:** Der ganze Abschluss von $\mathcal{O}_K$ in L ist $\mathcal{O}_L$ und der Quotientenkörper von $\mathcal{O}_K$ ist K.

(1.18) **Satz:** Sei $N \subset L$ ein endlich erzeugter nicht verschwindender $\mathcal{O}_L$-Untermodul. Ist $\mathcal{O}_K$ ein Hauptidealring, so ist N ein freier $\mathcal{O}_K$-Modul der Dimension n.

(1.19) **Lemma:** Seien $\{x_1, \ldots, x_n\}$, $\{y_1, \ldots, y_n\}$ zwei $\mathcal{O}_K$-Basen von N. Dann gilt $d(x_1, \ldots, x_n) = \varepsilon^2 d(y_1, \ldots, y_n)$, wobei ε eine Einheit von $\mathcal{O}_K$ ist.

(1.20) **Definition:** Sei $N \subset K$ ein endlich erzeugter nicht verschwindender $\mathcal{O}_K$-Untermodul und sei $\{x_1, \ldots, x_m\}$ eine A-Basis von N. Das nach (1.19) bis auf Multiplikation mit dem Quadrat einer Einheit von A nicht von $\{x_1, \ldots, x_m\}$ abhängige Element

$$d(N) := d(x_1, \ldots, x_m) \in A$$

heisst *Diskriminante* von N.

(1.21) **Definition:** Die Diskriminante des Ganzheitsrings $d_K := d(\mathcal{O}_K)$ heisst *Diskriminante* von K.

(1.22) **Bemerkung:** Der Ganzheitsring $\mathcal{O}_K$ eines beliebigen Zahl- oder Funktionenkörpers K ist im Allgemeinen nicht faktoriell.

(1.23) **Definition:** Sei R ein kommutativer Integritätsring mit Einselement, in welchem sich jedes nicht-triviale Ideal $\mathfrak{a} \subset R$ in bis auf Reihenfolge eindeutige Weise als

$$\mathfrak{a} = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_k$$

schreiben lässt, wobei $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ Primideale von R sind. Dann heisst R *Dedekindring*.

(1.24) **Satz:** Sei R ein kommutativer Integritätsring mit Einselement. Äquivalent sind:

i. Der Ring R ist ein Dedekindring.

ii. Der Ring R ist noethersch, ganzabgeschlossen und jedes Primideal $\mathfrak{p} \neq 0$ von R ist maximal.

iii. Für jedes Primideal $\mathfrak{p} \subset R$ ist die Lokalisierung $R_\mathfrak{p}$ von R bei $\mathfrak{p}$ ein faktorieller Ring.

Beweis: Zariski, Chap. V, §6

(1.25) **Satz:** Sei $B \subset K$ eine A-Unteralgebra. Äquivalent sind:

i. $B = \mathcal{O}_K$.

ii. Als A-Untermodul von K ist $B \cong A^m$, und B ist ein Dedekindring.

§2 Bewertungen, diskrete Bewertungsringe

Dieser Abschnitt folgt Neukirch, Kap. II, §3 – 5.

(1.26) **Definition:** Sei K ein Körper. Eine Abbildung $|\cdot| : K \to \mathbb{R}$ heisst *Norm* oder *Bewertung* von K, falls für alle $x, y \in K$ gilt

1. $|x| \geq 0$ und $|x| = 0 \iff x = 0$,
2. $|xy| = |x| \cdot |y|$ und
3. $|x + y| \leq |x| + |y|$.

(1.27) **Bemerkung:** Eine Bewertung $|\cdot|$ induziert die Metrik $d(x, y) = |x - y|$ und somit eine Topologie auf K.

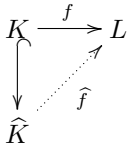
(1.28) **Definition:** Sei K ein Körper. Eine Bewertung $|\cdot|$ von K heisst *nicht-archimedisch* oder *ultrametrisch*, falls die verschärfte Dreiecksungleichung

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

gilt, das heisst, wenn die durch $|\cdot|$ induzierte Metrik eine *Ultrametrik* ist.

(1.29) **Bemerkung:** Eine Bewertung $|\cdot|$ ist genau dann nicht-archimedisch, wenn $\operatorname{char} K \neq 0$ oder $\sup_{n \in \mathbb{N}} |n| < \infty$.

(1.30) **Definition:** Seien K ein Körper und $|\cdot|$ eine Bewertung von K. Eine Körpererweiterung $\widehat{K}$ mit einer Fortsetzung $\widehat{|\cdot|}$ von $|\cdot|$ auf $\widehat{K}$ heisst *Komplettierung* von K, falls $\widehat{K}$ bezüglich $\widehat{|\cdot|}$ vollständig ist und folgende universelle Eigenschaft erfüllt ist: Ist L/K eine Körpererweiterung und L vollständig bezüglich einer Fortsetzung $|\cdot|'$ von $|\cdot|$ auf L und $f : K \to L$ ein isometrischer Homomorphismus, so existiert genau ein isometrischer K-Homomorphismus $\widehat{f} : \widehat{K} \to L$, sodass das folgende Diagramm kommutiert:



(1.31) **Bemerkung:** Die Menge C aller Cauchy-Folgen in K ist ein Ring, die Menge $\mathfrak{n}$ aller Nullfolgen ist ein maximales Ideal in C und $\widehat{K} := C/\mathfrak{n}$ ist eine Komplettierung von K bezüglich $|\cdot|$, denn $\widehat{K}$ ist vollständig bezüglich der eindeutigen Fortsetzung $|a| = \lim_{n\to\infty} |a_n|$, wobei $a = [(a_n)_{n\in\mathbb{N}}]$, von $|\cdot|$ auf $\widehat{K}$, und K lässt sich dicht in $\widehat{K}$ einbetten durch $x \mapsto (x, x, \ldots)$.
Allgemein folgt aus der universellen Eigenschaft der Komplettierung, dass die Einbettung von K in $\widehat{K}$ dicht ist, und falls $\widehat{K}, \widehat{K}'$ zwei Komplettierungen von K sind, so existiert ein eindeutiger isometrischer K-Isomorphismus $\widehat{K} \to \widehat{K}'$.

(1.32) **Satz:** Sei K vollständig bezüglich $|\cdot|$ und sei $L|K$ eine algebraische Erweiterung. Dann existiert eine eindeutige Fortsetzung von $|\cdot|$ auf L.
Falls $L|K$ endlich und separabel ist, so ist die Fortsetzung gegeben durch

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

und L ist vollständig bezüglich dieser Bewertung.

(1.33) **Definition:** Sei K ein Körper. Eine Abbildung $v : K \to \mathbb{R} \cup \{\infty\}$ heisst *Exponentialbewertung* von K, falls für alle x, y in K gilt

i. $v(x) = \infty \iff x = 0$,

ii. $v(xy) = v(x) + v(y)$ und

iii. $v(x + y) \geq \min\{v(x), v(y)\}$.

(1.34) **Bemerkung:** Ist v eine Exponentialbewertung von K, so ist $|\cdot| = \exp\circ(-v)$ eine nicht-archimedische Bewertung von K, und umgekehrt ist für jede nicht-archimedische Bewertung $|\cdot|$ die Abbildung $v = -\log\circ|\cdot|$ eine Exponentialbewertung von K.

(1.35) **Definition:** Sei v eine Exponentialbewertung von K. Die additive Untergruppe $v(K^*) \subset \mathbb{R}$ heisst *Wertegruppe* von v.

(1.36) **Definition:** Eine Exponentialbewertung v von K heisst *normierte diskrete Bewertung*, falls $v(K^*) = \mathbb{Z}$ ist.

(1.37) **Definition:** Sei R ein kommutativer Integritätsring mit Einselement, sodass eine normierte diskrete Bewertung v des Quotientenkörpers K von R existiert, mit

$$R = \{x \in K \mid v(x) \geq 0\}.$$

Dann heisst R *diskreter Bewertungsring.*

(1.38) **Satz:** Ein kommutativer Integritätsring mit Einselement ist genau dann ein diskreter Bewertungsring, wenn er ein lokaler Hauptidealring ist.

(1.39) **Korollar:** Sei R ein kommutativer Integritätsring mit Einselement. Äquivalent sind:

i. R ist ein Dedekindring.

ii. Für jedes Primideal $\mathfrak{p} \subset R$ ist die Lokalisierung $R_\mathfrak{p}$ von R bei $\mathfrak{p}$ ein diskreter Bewertungsring.

(1.40) **Bemerkung:** Diese Aussage ist eine deutliche Verschärfung von (1.24) iii.

(1.41) **Bemerkung:** Sei R ein diskreter Bewertungsring. Wegen $\mathrm{Spec}(R) = \{(0), \mathfrak{m}\}$ und $\mathfrak{m} = (\alpha)$ und da R insbesondere ein Dedekindring ist, lässt sich jedes Ideal $\mathfrak{a} \subset R$ schreiben als $\mathfrak{a} = \mathfrak{m}^k$. Da R sogar ein Hauptidealring ist, folgt daraus, dass sich sogar jedes $y \in R$ als $\varepsilon \cdot \alpha^k$ schreiben lässt, wobei ε eine Einheit ist.
Umgekehrt liefert jede solche Darstellung eine Bewertung, die auf $R \setminus \{0\}$ durch $v(\varepsilon \cdot \alpha^k) := k$ definiert ist und sich durch $v(y^{-1}) := -v(y)$ und $v(ab) = v(a) + v(b)$ auf ganz K^* fortsetzen lässt.
Ausserdem ist die Einheitengruppe $R^* = \{x \in K \mid v(x) = 0\}$.

§3 Gitter in $\mathbb{R}^n$

Dieser Abschnitt folgt Neukirch, Kap. I, §4, 5.

(1.42) **Definition:** Seien V ein n-dimensionaler $\mathbb{R}$-Vektorraum und $v_1, \ldots, v_n \in V$ linear unabhängig. Die Menge

$$\Gamma = \mathbb{Z}v_1 + \ldots + \mathbb{Z}v_n$$

heisst *vollständiges Gitter* in V.
Die Elemente $v_1, \ldots, v_n$ heissen *Basis* und

$$\Phi = \{x_1 v_1 + \ldots + x_n v_n \mid 0 \leq x_i < 1\}$$

heisst *Grundmasche* von Γ.

(1.43) **Bemerkung:** Sei V euklidisch. Dann induziert $\langle ., . \rangle$ in analoger Konstruktion zum Lebesgue-Mass ein eindeutiges Haar-Mass (siehe (1.49)) Vol auf allen Borelmessbaren Teilmengen von V.

(1.44) **Bemerkung:** Das Co-Volumen $\mathrm{CoVol}(\Gamma) := \mathrm{Vol}(\Phi)$ von Γ ist unabhängig von der Wahl der Grundmasche (also der Basis) von Γ, und es gilt $\mathrm{CoVol}(\Gamma) \neq 0$ für jedes vollständige Gitter Γ.

(1.45) **Minkowskischer Gitterpunktsatz:** Sei Γ ein vollständiges Gitter und sei $X \subset V$ eine zentralsymmetrische konvexe Menge mit $\mathrm{Vol}(X) > 2^n \mathrm{CoVol}(\Gamma)$. Dann enthält X einen von Null verschiedenen Punkt $\gamma \in \Gamma$.

Beweis: Man nehme an, für alle $\gamma_1, \gamma_2 \in \Gamma$ sei

$$(\gamma_1 + \frac{1}{2}X) \cap (\gamma_2 + \frac{1}{2}X) = \varnothing,$$

falls $\gamma_1 \neq \gamma_2$. Dann gilt offensichtlich auch

$$\big((\gamma_1 + \frac{1}{2}X) \cap \Phi\big) \cap \big((\gamma_2 + \frac{1}{2}X) \cap \Phi\big) = \varnothing,$$

wobei Φ die Grundmasche von Γ bezeichne. Folglich gilt

$$\begin{aligned}\mathrm{Vol}(\Phi) &\geq \sum_{\gamma\in\Gamma}\mathrm{Vol}\big((\frac{1}{2}X+\gamma)\cap\Phi\big) = \sum_{\gamma\in\Gamma}\mathrm{Vol}\big(\frac{1}{2}X\cap(\Phi-\gamma)\big) = \mathrm{Vol}(\frac{1}{2}X)\\ &= \frac{1}{2^n}\mathrm{Vol}(X);\end{aligned}$$

Widerspruch. Also existieren $\gamma_1,\gamma_2\in\Gamma$ mit $\gamma_1\neq\gamma_2$, und ein $v\in V$, mit $v\in(\gamma_1+\frac{1}{2}X)\cap(\gamma_2+\frac{1}{2}X)$. Das heisst, es existieren Elemente $x_1,x_2\in X$ mit $v=\gamma_1+\frac{1}{2}x_1=\gamma_2+\frac{1}{2}x_2$, und somit liegt $\gamma_1-\gamma_2=\frac{1}{2}x_2-\frac{1}{2}x_1$ als Mittelpunkt der Strecke von x_2 nach $-x_1$ in $\Gamma\cap X$. □

(1.46) **Bemerkung:** Sei K ein Zahlkörper von Grad n. Die verschiedenen Einbettungen $\sigma_1,\ldots,\sigma_n$ von K in $\overline{\mathbb{Q}}$ sind offensichtlich auch Einbettungen in $\mathbb{C}$. Ausserdem ist die komplex konjugierte Abbildung $\overline{\sigma}:K\to\mathbb{C}$ jeder Einbettung σ ebenfalls eine K-Einbettung. Die n Einbettungen von K lassen sich also unterteilen in r reelle Einbettungen

$$\rho_1,\ldots,\rho_r : K\to\mathbb{R}$$

und s Paare von komplex konjugierten Einbettungen

$$\tau_1,\overline{\tau_1},\ldots,\tau_s,\overline{\tau_s} : K\to\mathbb{C},$$

wobei $n=r+2s$ ist.

(1.47) **Definition:** Die Abbildung $\sigma:K\to\mathbb{R}^n$,

$$x\mapsto\big(\rho_1(x),\ldots,\rho_r(x),\mathrm{Re}(\tau_1(x)),\mathrm{Im}(\tau_1(x)),\ldots,\mathrm{Re}(\tau_s(x)),\mathrm{Im}(\tau_s(x))\big)$$

heisst *kanonische Einbettung* von K.

(1.48) **Satz:** Sei $\Gamma:=\sigma(\mathcal{O}_K)$. Dann ist Γ ein vollständiges Gitter in $\mathbb{R}^n$ mit

$$\mathrm{CoVol}(\Gamma)=2^{-s}\sqrt{|d_K|}.$$

Beweis: Sei $\{\alpha_1,\ldots,\alpha_n\}$ eine $\mathbb{Z}$-Basis von $\mathcal{O}_K$, also $\Gamma=\mathbb{Z}\sigma(\alpha_1)+\ldots+\mathbb{Z}\sigma(\alpha_n)$. Sei $A:=(\sigma_i(\alpha_j))_{i,j=1}^n$. Nach Definition ist $d_K=\det(A)^2$, und ausserdem ist

$$\begin{aligned}\mathrm{Vol}(\Phi) &= |\det(\langle\sigma(\alpha_i),\sigma(\alpha_j)\rangle)_{i,j=1}^n|^{\frac{1}{2}}\\ &= \Big|\det\Big(\big(\sum_{k=1}^n\sigma_k(\alpha_i)\overline{\sigma_k}(\alpha_j)\big)_{i,j=1}^n\Big)\Big|^{\frac{1}{2}}\\ &= |\det(A\overline{A}^t)|^{\frac{1}{2}}=|\det(A)|.\end{aligned}$$

□

§4 Haar-Masse

Dieser Abschnitt folgt und Weil[1], Chap. 1, §2. Die Existenz von Haar-Massen wird in Weil[2] bewiesen.

(1.49) **Definition:** Sei G eine lokal-kompakte topologische abelsche Gruppe. Ein reguläres Borel-Mass $\mu:\mathcal{B}(G)\to[0,\infty]$ heisst *Haar-Mass*, falls μ translationsinvariant ist, das heisst, falls für alle offenen Teilmengen $U\subset G$ und alle $g\in G$ gilt, dass $\mu(g+U)=\mu(U)$.

(1.50) **Satz:** Sei G eine lokal-kompakte topologische abelsche Gruppe. Dann existiert ein Haar-Mass auf G, und dieses ist bis auf einen konstanten positiven Faktor eindeutig bestimmt.

(1.51) **Satz:** Seien G eine abelsche lokal-kompakte topologische abelsche Gruppe und $H < G$ eine abgeschlossene Untergruppe. Dann gilt für geeignet normierte Haar-Masse μ_G, μ_H, $\mu_{G/H}$ und für jede messbare Funktion $f : G \to \mathbb{R}$:

$$\int_G f(x)\mathrm{d}\mu_G(x) = \int_{G/H} \int_H f(\overline{x} + y)\mathrm{d}\mu_H(y)\mathrm{d}\mu_{G/H}(\overline{x}).$$

(1.52) **Korollar:** Sind V, V' zwei messbare Repräsentantensysteme von G modulo H, so gilt $\mu(V) = \mu(V')$.

(1.53) **Bemerkung:** Seien G eine lokal-kompakte topologische abelsche Gruppe, μ ein Haar-Mass auf G und $\varphi : G \to G$ ein Automorphismus. Dann existiert eine (von μ unabhängige) Zahl $\mathrm{mod}_G(\varphi) \in \mathbb{R}^+$, sodass $\mu(\varphi(A)) = \mathrm{mod}_G(\varphi) \cdot \mu(A)$ für alle messbaren Mengen $A \subset G$ gilt. Die Konstante $\mathrm{mod}_G(\varphi)$ heisst *Modulus* von φ.
Die Abbildung $\mathrm{mod}_G : \mathrm{Aut}(G) \to \mathbb{R}^+$ ist ein Gruppenhomomorphismus.

2 Dedekindringe

Dieser Abschnitt folgt NEUKIRCH, Kap. I, §3, 8 und Kap. III, §1, 2.

Sei im Folgenden $L|K$ eine separable Körpererweiterung vom Grad n, sei $\mathfrak{o} \subset K$ ein Dedekindring mit Quotientenkörper K und $\mathcal{O} \subset L$ der ganze Abschluss von $\mathfrak{o}$ in L (in unserem Fall werden K und L Zahl- oder Funktionenkörper und $\mathfrak{o}, \mathcal{O}$ ihre Ganzheitsringe sein).

(2.1) **Satz:** $\mathcal{O}$ ist ein Dedekindring.

Beweis: Siehe NEUKIRCH, Kap. I, §8, Satz (8.1).

(2.2) **Definition:** Das von den Diskriminanten aller n-Tupel $(x_1, \dots x_n) \in \mathcal{O}^n$ erzeugte Ideal $\mathfrak{d}_{L|K} \subset \mathfrak{o}$ heisst *Diskriminante* von L über K.

(2.3) **Bemerkung:** Tatsächlich genügt es Diskriminanten von K-Basen $\{x_1, \dots, x_n\}$ von L zu betrachten, da $d(x_1, \dots, x_n) = 0$ gilt, wenn $x_1, \dots, x_n$ linear abhängig sind.

(2.4) **Bemerkung:** Falls $\mathcal{O}$ ein freier $\mathfrak{o}$-Modul ist, ist $\mathfrak{d}_{L|K}$ nach (1.19) ein Hauptideal. Insbesondere gilt stets $\mathfrak{d}_{L|\mathbb{Q}} = (d_L)$, beziehungsweise $\mathfrak{d}_{L|\mathbb{F}(t)} = (d_L)$.

(2.5) **Definition:** Sei $\mathfrak{a} \subset K$ ein endlich erzeugter $\mathfrak{o}$-Untermodul. Dann heisst $\mathfrak{a}$ *gebrochenes Ideal* von K. Ist $\mathfrak{a}$ ein Ideal von $\mathfrak{o}$, so heisst $\mathfrak{a}$ *ganzes Ideal* von K. Ein gebrochenes Ideal, das von einem Element erzeugt wird, heisst *gebrochenes Hauptideal*.

(2.6) **Bemerkung:** Die gebrochenen Ideale bilden bezüglich Multiplikation eine Gruppe, genannt Idealgruppe J_K von K. Dabei ist $\mathfrak{o}$ das Neutralelement und zu einem gebrochenen Ideal $\mathfrak{a}$ ist

$$\mathfrak{a}^{-1} := \{x \in K \mid x\mathfrak{a} \subset \mathfrak{o}\}$$

das inverse Element.
Die Gruppe J_K ist isomorph zur freien abelschen Gruppe, welche von den Primidealen von $\mathfrak{o}$ erzeugt wird.

(2.7) **Definition:** Sei $\mathfrak{A} \subset L$ ein gebrochenes Ideal. Das von den Normen $\mathrm{N}_{L|K}(\alpha)$ aller Elemente $\alpha \in \mathfrak{A}$ erzeugte gebrochene Ideal $\mathrm{N}_{L|K}(\mathfrak{A}) \subset K$ heisst *Norm* des Ideals $\mathfrak{A}$.

(2.8) **Satz:**

i. Die Abbildung $\mathrm{N}_{L|K} : J_L \to J_K$ ist ein Homomorphismus von der Idealgruppe von L in jene von K.

ii. Es gilt $\mathrm{N}_{M|K} = \mathrm{N}_{L|K} \circ \mathrm{N}_{M|L}$, wenn $M|L$ eine endliche separable Körpererweiterung ist.

Beweis: Siehe NEUKIRCH, Kap. III, §1, Satz (1.6).

(2.9) **Bemerkung:** Ist $\mathfrak{A} \subset L$ ein ganzes Ideal, so ist auch $\mathrm{N}_{L|K}(\mathfrak{A})$ ein ganzes Ideal, da $\mathrm{N}_{L|K}(\alpha) \in \mathcal{O}$ ist für jedes $\alpha \in \mathfrak{o}$.

(2.10) **Bemerkung:** Falls $(\alpha) = \mathfrak{A} \subset L$ ein gebrochenes Hauptideal ist, so ist wegen $\mathrm{N}_{L|K}(\alpha x) = \mathrm{N}_{L|K}(\alpha)\mathrm{N}_{L|K}(x)$ auch $\mathrm{N}_{L|K}(\mathfrak{A}) = (\mathrm{N}_{L|K}(\alpha))$ ein gebrochenes Hauptideal.

(2.11) **Bemerkung:** Sei $\mathfrak{a} \subset K$ ein gebrochenes Ideal. Dann gilt

$$\mathrm{N}_{L|K}(\mathfrak{a}\mathcal{O}) = \mathfrak{a}^n,$$

denn $\mathrm{N}_{L|K}(\alpha\xi) = \mathrm{N}_{L|K}(\alpha)\mathrm{N}_{L|K}(\xi) = \alpha^n \mathrm{N}_{L|K}(\xi)$.

(2.12) **Definition:** Sei $\mathfrak{A} \subset L$ ein gebrochenes Ideal. Das gebrochene Ideal

$$^*\mathfrak{A} := \{x \in L \mid \mathrm{Tr}_{L|K}(x\mathfrak{A}) \subset \mathcal{o}\}$$

heisst zu $\mathfrak{A}$ *duales gebrochenes Ideal*.

(2.13) **Bemerkung:** Die Menge $^*\mathfrak{A}$ ist tatsächlich ein gebrochenes Ideal von L, da sie offensichtlich ein $\mathcal{O}$-Modul und als solcher endlich erzeugt ist.

(2.14) **Definition:** Das gebrochene Ideal

$$\mathfrak{C}_{L|K} := \mathfrak{C}_{\mathcal{O}|\mathcal{o}} := {}^*\mathcal{O} = \{x \in L \mid \mathrm{Tr}_{L|K}(x\mathcal{O}) \subset \mathcal{o}\}$$

heisst *Dedekindscher Komplementärmodul*.
Das dazu inverse Ideal

$$\mathfrak{D}_{L|K} := \mathfrak{D}_{\mathcal{O}|\mathcal{o}} := \mathfrak{C}_{\mathcal{O}|\mathcal{o}}^{-1}$$

heisst *Differente* von L über K.

(2.15) **Bemerkung:** Wegen $\mathcal{O} \subset \mathfrak{C}_{\mathcal{O}|\mathcal{o}}$ gilt $\mathfrak{D}_{\mathcal{O}|\mathcal{o}} \subset \mathcal{O}$, also ist die Differente ein ganzes Ideal in L.

(2.16) **Bemerkung:** Der Name Differente erklärt sich folgendermassen: Sei $\alpha \in \mathcal{O}$, $f_\alpha \in \mathcal{o}[X]$ das Minimalpolynom von α und f'_α die formale Ableitung von f_α. Das Element

$$\delta_{L|K}(\alpha) := \begin{cases} f'_\alpha(\alpha) & , \text{ falls } L = K(\alpha) \\ 0 & , \text{ sonst} \end{cases}$$

von $\mathcal{O}$ heisst *Differente* von α.
Die Differente $\mathfrak{D}_{L|K}$ ist nun gerade das Ideal, welches von den Differenten $\delta_{L|K}$ aller Elemente $\alpha \in \mathcal{O}$ erzeugt wird (für einen Beweis hiervon siehe Neukirch, Kap. III, §2, Satz (2.5)).

(2.17) **Lemma:** Sei $M|L$ eine endliche separable Körpererweiterung. Dann gilt

$$\mathfrak{D}_{M|K} = \mathfrak{D}_{M|L}\mathfrak{D}_{L|K}.$$

Beweis: Es genügt zu zeigen, dass

$$\mathfrak{C}_{M|K} = \mathfrak{C}_{M|L}\mathfrak{C}_{L|K}$$

gilt; die Aussage für die Differente ergibt sich dann duch Invertieren.
Es bezeichne $\mathscr{O}$ den ganzen Abschluss von $\mathcal{o}$ in M.

$$\begin{aligned} \mathrm{Tr}_{M|K}(\mathfrak{C}_{M|L}\mathfrak{C}_{L|K}\mathscr{O}) &= (\mathrm{Tr}_{L|K} \circ \mathrm{Tr}_{M|L})(\mathfrak{C}_{M|L}\mathfrak{C}_{L|K}\mathscr{O}) \\ &= \mathrm{Tr}_{L|K}\big(\mathfrak{C}_{L|K}\mathrm{Tr}_{M|L}(\mathfrak{C}_{M|L}\mathscr{O})\big) \\ &\subset \mathrm{Tr}_{L|K}(\mathfrak{C}_{L|K}\mathcal{O}) \\ &\subset \mathcal{o} \end{aligned}$$

Also ist $\mathfrak{C}_{M|K} \supset \mathfrak{C}_{M|L}\mathfrak{C}_{L|K}$.
Wegen

$$\begin{aligned} \mathrm{Tr}_{L|K}\big(\mathrm{Tr}_{M|L}(\mathfrak{C}_{M|L}\mathscr{O})\big) &= \mathrm{Tr}_{L|K}\big(\mathrm{Tr}_{M|L}(\mathfrak{C}_{M|L}\mathscr{O}\mathcal{O})\big) \\ &= \mathrm{Tr}_{L|K}\big(\mathrm{Tr}_{M|L}(\mathfrak{C}_{M|L}\mathscr{O})\mathcal{O}\big) \\ &\subset \mathrm{Tr}_{L|K}(\mathcal{O}) \\ &\subset \mathcal{o} \end{aligned}$$

gilt $\mathrm{Tr}_{M|L}(\mathfrak{C}_{M|L}\mathscr{O}) \subset \mathfrak{C}_{L|K}$, also

$$\mathrm{Tr}_{M|L}(\mathfrak{C}_{L|K}^{-1}\mathfrak{C}_{M|K}\mathscr{O}) = \mathfrak{C}_{L|K}^{-1}\mathrm{Tr}_{M|L}(\mathfrak{C}_{M|K}\mathscr{O}) \subset \mathcal{O}.$$

Somit gilt $\mathfrak{C}_{L|K}^{-1}\mathfrak{C}_{M|K} \subset \mathfrak{C}_{M|L}$, woraus $\mathfrak{C}_{M|K} \subset \mathfrak{C}_{M|L}\mathfrak{C}_{L|K}$ folgt. □

(2.18) **Bemerkung:** Sei S eine multiplikative Teilmenge von $\mathcal{o}$. Dann gilt

$$\mathfrak{D}_{S^{-1}\mathcal{O}|S^{-1}\mathcal{o}} = S^{-1}\mathfrak{D}_{\mathcal{O}|\mathcal{o}}.$$

(2.19) **Lemma:** Ein Dedekindring mit nur endlich vielen Primidealen ist ein Hauptidealring.

Beweis: Es seien $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ die Primideale des Dedekindringes R und sei $\mathfrak{a} \subset R$ ein nicht-triviales Ideal. Weil R ein Dedekindring ist, besitzt $\mathfrak{a}$ eine Faktorisierung

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}.$$

Wähle $p_i \in \mathfrak{p}_i \setminus \mathfrak{p}_i^2$. Nach dem Chinesischen Restsatz existiert ein $\alpha \in R$, sodass für alle i

$$\alpha \equiv p_i^{r_i} \pmod{\mathfrak{p}_i^{r_i+1}}$$

gilt. Sei $(\alpha) = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_k^{s_k}$. Für alle i gilt offensichtlich $r_i = s_i$ und somit ist $\mathfrak{a} = (\alpha)$. □

(2.20) **Satz:** Zwischen der Diskriminante und der Differente besteht die Beziehung

$$\mathfrak{d}_{L|K} = \mathrm{N}_{L|K}(\mathfrak{D}_{L|K}).$$

Beweis: Wegen (2.18) und nach (1.39) genügt es die Behauptung in dem Fall zu zeigen, dass $\mathcal{o}$ ein diskreter Bewertungsring ist. Dann besitzt $\mathcal{O}$ eine Ganzheitsbasis $\{\alpha_1, \ldots, \alpha_n\}$, und nach (2.4) ist $\mathfrak{d}_{L|K} = (d(\alpha_1, \ldots, \alpha_n))$.
Ausserdem gilt $\mathfrak{C}_{L|K} = (\alpha_1', \ldots, \alpha_n')$, wobei $\{\alpha_1', \ldots, \alpha_n'\}$ die zu $\{\alpha_1, \ldots, \alpha_n\}$ duale Basis ist, also $\mathrm{Tr}_{L|K}(\alpha_i\alpha_j') = \delta_{ij}$. Da $\mathcal{o}$ ein diskreter Bewertungsring ist, besitzt auch $\mathcal{O}$ nur endlich viele Primideale und ist wegen (2.19) ein Hauptidealring. Somit existiert ein β mit $\mathfrak{C}_{L|K} = (\beta)$. Also besitzt $\mathfrak{C}_{L|K}$ über $\mathcal{o}$ die Ganzheitsbasis $\{\beta\alpha_1, \ldots, \beta\alpha_n\}$ mit der Diskriminante

$$d(\beta\alpha_1, \ldots, \beta\alpha_n) = \mathrm{N}_{L|K}(\beta)^2 d(\alpha_1, \ldots, \alpha_n).$$

Weiter gilt $(\mathrm{N}_{L|K}(\beta)) = \mathrm{N}_{L|K}(\mathfrak{C}_{L|K}) = \mathrm{N}_{L|K}(\mathfrak{D}_{L|K}^{-1}) = \mathrm{N}_{L|K}(\mathfrak{D}_{L|K})^{-1}$.
Sind ausserdem $\sigma_1, \ldots, \sigma_n : L \to \overline{K}$ die K-Einbettungen von L, so gilt

$$\begin{aligned} d(\alpha_1, \ldots, \alpha_n) &= \det\left((\sigma_i(\alpha_j))_{i,j=1}^n\right)^2 \text{ und} \\ d(\alpha_1', \ldots, \alpha_n') &= \det\left((\sigma_i(\alpha_j'))_{i,j=1}^n\right)^2 \end{aligned}$$

und somit

$$d(\alpha_1, \ldots, \alpha_n) \cdot d(\alpha_1', \ldots, \alpha_n') = 1,$$

da $\{\alpha_1, \ldots, \alpha_n\}$ und $\{\alpha_1', \ldots, \alpha_n'\}$ zueinander dual sind. Also gilt

$$\begin{aligned} \mathfrak{d}_{L|K}^{-1} &= (d(\alpha_1, \ldots, \alpha_n)^{-1}) = (d(\alpha_1', \ldots, \alpha_n')) \\ &= \mathfrak{C}_{L|K} = (d(\beta\alpha_1, \ldots, \beta\alpha_n)) \\ &= \mathrm{N}_{L|K}(\beta)^2 d(\alpha_1, \ldots, \alpha_n) \\ &= \mathrm{N}_{L|K}(\mathfrak{D}_{L|K})^{-2}\mathfrak{d}_{L|K}, \end{aligned}$$

woraus die Behauptung folgt. □

(2.21) **Satz:** Sei $M|L$ endlich und separabel. Dann gilt

$$\mathfrak{d}_{M|K} = \mathfrak{d}_{L|K}^{[M:L]} \mathrm{N}_{L|K}(\mathfrak{d}_{M|L}).$$

Beweis: Nach (2.17) gilt $\mathfrak{D}_{M|K} = \mathfrak{D}_{M|L}\mathfrak{D}_{L|K}$; mit $\mathrm{N}_{M|K} = \mathrm{N}_{L|K} \circ \mathrm{N}_{M|L}$ erhält man daraus mit (2.20)

$$\begin{aligned} \mathfrak{d}_{M|K} &= \mathrm{N}_{M|K}(\mathfrak{D}_{M|L})\mathrm{N}_{M|K}(\mathfrak{D}_{L|K}) \\ &= \mathrm{N}_{L|K}(\mathfrak{d}_{M|L})\mathrm{N}_{L|K}\big(\mathrm{N}_{M|L}(\mathfrak{D}_{L|K}\mathscr{O})\big), \end{aligned}$$

wobei $\mathscr{O}$ den Ganzheitsabschluss von $\mathcal{O}$ in M bezeichne. Mit (2.11) erhält man daraus

$$\begin{aligned} \mathfrak{d}_{M|K} &= \mathrm{N}_{L|K}(\mathfrak{d}_{M|L})\mathrm{N}_{L|K}(\mathfrak{D}_{L|K}^{[M:L]}) \\ &= \mathrm{N}_{L|K}(\mathfrak{d}_{M|L})\mathfrak{d}_{L|K}^{[M:L]}. \end{aligned}$$

□

3 Zahlkörperfall

Die Beweise von (3.1) und (3.2) folgen NEUKIRCH, Kap. III, §2, Theorem (2.13) und Satz (2.14).

(3.1) **Satz:** Seien $d \in \mathbb{Z}$ und $n \in \mathbb{N}$. Dann existieren nur endlich viele Zahlkörper vom Grad n mit der Diskriminante $d_K = d$.

Beweis: Zunächst soll gezeigt werden, dass es genügt zu beweisen, dass zu jedem $n \in \mathbb{N}$ und jedem $d \in \mathbb{Z}$ nur endlich viele Zahlkörper vom Grad n mit der Diskriminante d existieren, die das Element $\sqrt{-1}$ enthalten.
Nach (2.21) gilt für jeden Zahlkörper K mit $\sqrt{-1} \notin K$

$$\mathfrak{d}_{K(\sqrt{-1})|\mathbb{Q}} = \mathfrak{d}_{K|\mathbb{Q}}^2 \mathrm{N}_{K|\mathbb{Q}}(\mathfrak{d}_{K(\sqrt{-1})|K}),$$

also $(d_{K(\sqrt{-1})}) = (d_K)^2 \mathrm{N}_{K|\mathbb{Q}}(\mathfrak{d}_{K(\sqrt{-1})|K})$, und somit, weil $\mathrm{N}_{K|\mathbb{Q}}(\mathfrak{d}_{K(\sqrt{-1})|K})$ ein Hauptideal ist, für jedes $\alpha \in \mathfrak{d}_{K(\sqrt{-1})|K}$

$$|d_{K(\sqrt{-1})}| \leq |d_K|^2 \cdot |\mathrm{N}_{K|\mathbb{Q}}(\alpha)|.$$

Für $\alpha = -4 = d(1, \sqrt{-1})$ erhält man also

$$|d_{K(\sqrt{-1})}| \leq 4^{[K:\mathbb{Q}]} |d_K|^2.$$

Man nehme nun an, es gäbe zu einem $n \in \mathbb{N}$ und $d \in \mathbb{Z}$ unendlich viele Zahlkörper $\{K_i\}_{i \in I}$. Wegen (1.7) wäre dann auch die Menge $\{K_i(\sqrt{-1})\}_{i \in I}$ unendlich. Gemäss obiger Abschätzung der Diskriminante und da für jeden Zahlkörper $[K(\sqrt{-1}) : K] \leq 2$ gilt, würden in $\{K_i(\sqrt{-1})\}_{i \in I}$ nur endlich viele verschiedene Werte für Grad und Diskriminante angenommen, und folglich müssten zu bestimmten n', d' unendlich viele Zahlkörper, die $\sqrt{-1}$ enthalten, existieren.

Sei von nun an also K ein Zahlkörper mit $\sqrt{-1} \in K$, Diskriminante $d_K = d$ und Grad $[K : \mathbb{Q}] = n$.
Die Einbettungen $\tau_1, \ldots \tau_n$ von K in $\mathbb{C}$ sind alle komplex, da $\tau_i(\sqrt{-1}) = \pm\sqrt{-1}$ gelten muss. Sei ohne Beschränkung der Allgemeinheit $\tau_{2i-1} = \overline{\tau_{2i}}$ für $1 \leq i \leq \frac{n}{2}$.
Für jedes $C > 0$ betrachte man die Menge

$$X_C := \left\{ x \in \mathbb{R}^n \;\middle|\; |x_1| < 1, |x_2| < C\sqrt{|d|}, x_{2i-1}^2 + x_{2i}^2 < 1 \text{ für } 2 \leq i \leq \frac{n}{2} \right\}.$$

Offensichtlich ist X_C konvex und zentralsymmetrisch, und nach dem Satz von Fubini gilt $\lim_{C \to \infty} \mathrm{Vol}(X_C) = \infty$.
Sei nun Γ das Bild von $\mathcal{O}_K$ unter der kanonischen Einbettung von K in $\mathbb{R}^n$. Man wähle C so gross, dass $\mathrm{Vol}(X_C) > 2^{\frac{n}{2}} \sqrt{|d|}$ ist. Nach (1.48) ist dann $\mathrm{Vol}(X_C) > 2^n \mathrm{CoVol}(\Gamma)$, also enthält X_C nach (1.45) einen von Null verschiedenen Gitterpunkt. Das heisst $\exists \alpha \in \mathcal{O}_K \setminus \{0\}$, sodass gilt

- $|\mathrm{Im}(\tau_1(\alpha))| < C\sqrt{|d|}$,
- $|\mathrm{Re}(\tau_1(\alpha))| < 1$ und
- $|\tau_i(\alpha)| < 1$ für $i > 2$.

Wegen $\alpha \in \mathcal{O}_K$ gilt $\prod_{i=1}^n |\tau_i(\alpha)| = |\mathrm{N}_{K|\mathbb{Q}}(\alpha)| \geq 1$, also $|\tau_1(\alpha)| > 1$ und somit $\mathrm{Im}(\tau_1(\alpha)) \neq 0$. Also ist $\tau_1(\alpha) \neq \tau_2(\alpha)$, und wegen $|\tau_i(\alpha)| < 1$ für alle anderen i gilt $\tau_1(\alpha) \neq \tau_i(\alpha)$ überhaupt für alle $i > 1$. Nach (1.8) gilt somit $K = \mathbb{Q}(\alpha)$.
Die Konjugierten $\tau_i(\alpha)$ von α sind nach Konstruktion für $2 \leq i \leq n$ durch $|\tau_i(\alpha)| < 1$, sowie durch $|\mathrm{Im}(\tau_1(\alpha))| < C\sqrt{|d|}$ und $|\mathrm{Re}(\tau_1(\alpha))| < 1$ beschränkt, und somit sind (nach dem Satz von Vieta) auch die Koeffizienten des Minimalpolynoms m_α von α beschränkt. Wegen $\alpha \in \mathcal{O}_K$ hat m_α Koeffizienten in $\mathbb{Z}$, und somit gibt es für $m_\alpha \in \mathbb{Z}[X]$ und deshalb auch für $\alpha \in \overline{\mathbb{Q}}$ nur endlich viele Möglichkeiten.
Also existieren nur endlich viele Zahlkörper K mit $\sqrt{-1} \in K$ vom Grad n mit Diskriminante $d_K = d$. □

(3.2) **Satz (Minkowski Schranke):** Sei K ein Zahlkörper von Grad n. Dann gilt

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

Beweis: Seien $\rho_1, \ldots, \rho_r : K \to \mathbb{R}$ die reellen und $\tau_1, \overline{\tau_1}, \ldots, \tau_s, \overline{\tau_s} : K \to \mathbb{C}$ die komplexen Einbettungen von K. Für jedes $C > 0$ betrachte man die konvexe zentralsymmetrische Menge

$$X_C := \Big\{ x \in \mathbb{R}^n \;\Big|\; \sum_{i=1}^{r} |x_i| + 2\sum_{j=1}^{s} \sqrt{x_{r+2j-1}^2 + x_{r+2j}^2} \leq C \Big\}.$$

Nach Einführen der Polarkoordinaten $x_{r+2j-1} = u_j \cos(\theta_j)$, $x_{r+2j} = u_j \sin(\theta_j)$ mit $u_j \geq 0$ und $0 \leq \theta_j < 2\pi$ lässt sich X_C schreiben als

$$X_C = \big\{ x \in \mathbb{R}^n \;\big|\; |x_1| + \ldots + |x_r| + 2u_1 + \ldots + 2u_s \leq C \big\}$$

und man erhält

$$\begin{aligned} \mathrm{Vol}(X_C) &= \int u_1 \cdots u_s dx_1 \cdots dx_r du_1 \cdots du_s d\theta_1 \cdots d\theta_s \\ &= (2\pi)^s \int u_1 \cdots u_s dx_1 \cdots dx_r du_1 \cdots du_s \end{aligned}$$

über dem Bereich $|x_1| + \ldots + |x_r| + 2u_1 + \ldots + 2u_s \leq C$.
Durch Einschränken auf $x_i \geq 0$ und die Substitution $w_j = 2u_j$ ergibt sich

$$\mathrm{Vol}(X_C) = 2^r 4^{-s} (2\pi)^s \int w_1 \cdots w_s dx_1 \cdots dx_r dw_1 \cdots dw_s$$

über dem Bereich $x_1 + \ldots + x_r + w_1 + \ldots w_s \leq C$.
Offensichtlich ist $\mathrm{Vol}(X_C) = C^{r+2s}\mathrm{Vol}(X_1) = C^n \mathrm{Vol}(X_1)$, also ist

$$\mathrm{Vol}(X_C) = 2^r 4^{-s} (2\pi)^s C^n \int w_1 \cdots w_s dx_1 \cdots dx_r dw_1 \cdots dw_s$$

über dem Bereich $x_1 + \ldots + x_r + w_1 + \ldots w_s \leq 1$.
Es bezeichne nun

$$\begin{aligned} A_{r,s} := \quad & \{x = (x_1, \ldots, x_r, w_1, \ldots, w_s) \in \mathbb{R}^{r+s} \mid \\ & x_i \geq 0, w_j \geq 0, x_1 + \ldots + x_r + w_1 + \ldots + w_s \leq 1\}. \end{aligned}$$

und

$$I_{r,s} := \int_{A_{r,s}} w_1 \cdots w_s dx_1 \cdots dx_r dw_1 \cdots dw_s.$$

Für jedes $(x_1, \ldots, w_s) \in A_{r,s}$ gilt $x_2 + \ldots + x_r + w_1 + \ldots + w_s \leq 1 - x_1$, also gilt nach dem Satz von Fubini

$$\begin{aligned} I_{r,s} &= \int_0^1 I_{r-1,s}(1 - x_1) dx_1 \\ &= \left(\int_0^1 (1 - x_1)^{n-1} dx_1 \right) \cdot I_{r-1,s} \\ &= \frac{1}{n} I_{r-1,s}. \end{aligned}$$

Also ist nach Induktion $I_{r,s} = \frac{1}{n(n-1)\cdots(n-r+1)} I_{0,s}$.
Analog ist

$$\begin{aligned} I_{0,s} &= \left(\int_0^1 w_1 (1 - w_1)^{2s-2} dw_1 \right) \cdot I_{0,s-1} \\ &= \frac{1}{s(s-1)} I_{0,s-1}, \end{aligned}$$

also ist wieder nach Induktion $I_{0,s} = \frac{1}{(2s)!} I_{0,0}$, und somit mit $I_{0,0} = 1$

$$I_{r,s} = \frac{1}{n!}.$$

Insgesamt erhält man also

$$\mathrm{Vol}(X_C) = 2^r \left(\frac{\pi}{2}\right)^s \frac{C^n}{n!}.$$

Sei nun Γ das Bild von $\mathcal{O}_K$ unter der kanonischen Einbettung σ von K in $\mathbb{R}^n$ und sei

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

Nach (1.48) gilt $\mathrm{Vol}\,(X_{B+\varepsilon}) > 2^n \mathrm{CoVol}(\Gamma)$ für alle $\varepsilon > 0$. Also gibt es nach (1.45) für jedes $\varepsilon > 0$ ein von Null verschiedenes $\alpha \in \mathcal{O}_K$, sodass $\sigma(\alpha) \in X_{B+\varepsilon}$, und da es von diesen offensichtlich jeweils nur endlich viele gibt, existiert ein von Null verschiedenes $\alpha \in \mathcal{O}_K$, dessen Einbettung für alle $\varepsilon > 0$ in $X_{B+\varepsilon}$ enthalten ist. Somit gilt $\sigma(\alpha) \in \bigcap_{\varepsilon>0} X_{B+\varepsilon} = X_B$.
Also gilt

$$\begin{aligned}
1 &\leq |\mathrm{N}_{K|\mathbb{Q}}(\alpha)| = \prod_{i=1}^{r} |\rho_i(\alpha)| \prod_{j=1}^{s} |\tau_j(\alpha)\overline{\tau_j}(\alpha)| \\
&\leq \frac{1}{n^n} \left(\sum_{i=1}^{r} |\rho_i(\alpha)| + \sum_{j=1}^{s} \left(|\tau_j(\alpha)| + |\overline{\tau_j}(\alpha)| \right) \right)^n \\
&\leq \frac{1}{n^n} \left(\sum_{i=1}^{r} |\rho_i(\alpha)| + 2 \sum_{j=1}^{s} \sqrt{\tau_j(\alpha)^2 + \overline{\tau_j}(\alpha)^2} \right)^n \\
&\leq \frac{B^n}{n^n} = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|d_K|} \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{\frac{n}{2}} \sqrt{|d_K|}.
\end{aligned}$$

□

(3.3) **Korollar (Minkowski):** Sei $K \neq \mathbb{Q}$ ein Zahlkörper. Dann gilt $|d_K| > 1$.

(3.4) **Korollar:** Sei $d \in \mathbb{Z}$. Dann existieren nur endlich viele Zahlkörper mit der Diskriminante $d_K = d$.

Beweis: Nach (3.2) gibt es nur zu endlich vielen $n \in \mathbb{N}$ überhaupt Zahlkörper vom Grad n mit der Diskriminante $d_K = d$ und von diesen nach (3.1) jeweils nur endlich viele. □

(3.5) **Satz (Hermite):** Seien K ein Zahlkörper, $n \in \mathbb{N}$ und $\mathfrak{d} \subset \mathcal{O}_K$ ein Ideal. Dann existieren nur endlich viele Erweiterungskörper L vom Grad $[L : K] = n$ mit $\mathfrak{d}_{L|K} = \mathfrak{d}$.

Beweis: Für jeden solchen Körper L gilt wegen (2.21)

$$(d_L) = (d_K)^n \mathrm{N}_{K|\mathbb{Q}}(\mathfrak{d}).$$

Also ist d_L bis auf Vorzeichen durch $\mathfrak{d}$ bestimmt und nach (3.1) existieren nur endlich viele Erweiterungen L vom Grad n mit der Diskriminante d_L. □

4 Funktionenkörperfall

§1 Verzweigung von Bewertungen

Dieser Abschnitt folgt NEUKIRCH, Kap. II, §3 – 8.

Es bezeichnen (K, v) einen nicht-archimedisch diskret bewerteten Körper, K_v eine Vervollständigung von K und $\widehat{K_v}$ einen algebraischen Abschluss von K_v. Sei zudem L eine separable Erweiterung vom Grad n von K.

(4.1) **Bemerkung:** Gemäss (1.32) lässt v sich eindeutig zu einer Bewertung $\widehat{v}$ von $\widehat{K_v}$ fortsetzen.

(4.2) **Bemerkung:** Offensichtlich ist der algebraische Abschluss $\widehat{K}$ von K in $\widehat{K_v}$ algebraisch abgeschlossen.

(4.3) **Bemerkung:** Sei $\sigma : L \to \widehat{K_v}$ eine K-Einbettung. Dann ist $w := \widehat{v} \circ \sigma$ eine Fortsetzung der Bewertung v auf L.

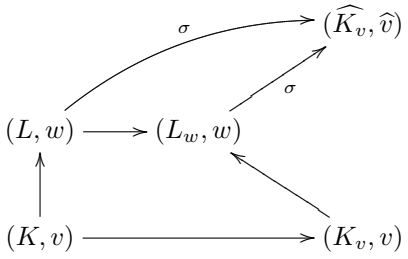
(4.4) **Satz:**

i. Sei w eine Fortsetzung der Bewertung v auf L. Dann existiert eine K-Einbettung $\sigma : L \to \widehat{K_v}$, sodass $w = \widehat{v} \circ \sigma$ gilt.

ii. Zwei Fortsetzungen $\widehat{v} \circ \sigma$, $\widehat{v} \circ \sigma'$ von v auf L sind genau dann gleich, wenn σ, σ' über K_v Galois-konjugiert sind.

Beweis: Siehe NEUKIRCH, Kap. II, §8, Satz (8.1).

(4.5) **Bemerkung:** Die Fortsetzungen w von v auf L werden also durch das folgende Diagramm charakterisiert:



(4.6) **Definition:** Sei $\mathcal{O}_v = \{x \in K_v \mid v(x) \geq 0\} \subset K_v$ der Bewertungsring von v und sei $\mathfrak{m} = \{x \in K_v \mid v(x) > 0\} \subset \mathcal{O}_v$ das maximale Ideal von $\mathcal{O}_v$. Dann heisst $\kappa := \mathcal{O}_v/\mathfrak{m}$ *Restklassenkörper* von (K_v, v).

(4.7) **Definition:** Sei w eine Fortsetzung von v auf L.
Der Index $e := [w(L_w^*) : v(K_v^*)]$ heisst *Verzweigungsindex* der Erweiterung $L_w|K_v$, beziehungsweise der Bewertungsfortsetzung w.
Der Grad $f := [\lambda : \kappa]$, wobei λ den Restklassenkörper von (L_w, w) bezeichne, heisst *Trägheitsgrad* der Erweiterung $L_w|K_v$, beziehungsweise der Bewertungsfortsetzung w.

(4.8) **Satz:** Es gilt

$$e \cdot f = [L_w : K_v].$$

Beweis: Siehe NEUKIRCH, Kap. II, §6, Satz (6.8).

(4.9) **Definition:** Die Erweiterung (L_w, w) von (K_v, v), beziehungsweise die Bewertungsfortsetzung w, heisst *unverzweigt*, falls $e = 1$ (und somit $f = [L_w : K_v]$) gilt.

(4.10) **Satz:** Jede Teilerweiterung einer unverzweigten Erweiterung ist unverzweigt und jedes Kompositum von unverzweigten Erweiterungen ist unverzweigt.

Beweis: Siehe NEUKIRCH, Kap. II, §7, Satz (7.2) und Korollar (7.3).

(4.11) **Definition:** Die Erweiterung (L_w, w) von (K_v, v), beziehungsweise die Bewertungsfortsetzung w, heisst *rein verzweigt*, falls keine unverzweigte Teilerweiterung von $L_w|K_v$ existiert (falls also $e = [L_w : K_v]$ und $f = 1$ gelten).

(4.12) **Bemerkung:** Die Verzweigung von Primidealen lässt sich folgendermassen als Spezialfall von Verzweigung von Bewertungen auffassen:
Sei $\mathcal{O}|\mathcal{o}$ eine Erweiterung von Dedekindringen mit Quotientenkörpern $L|K$ und sei $\alpha \in K^*$ beliebig. Das gebrochene Hauptideal (α) besitzt die eindeutige Zerlegung

$$(\alpha) = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha)},$$

und die Funktion $v_{\mathfrak{p}}$ definiert eine diskrete Exponentialbewertung auf K. Der zu $v_{\mathfrak{p}}$ gehörende Bewertungsring ist gerade die Lokalisierung $\mathcal{o}_{\mathfrak{p}}$ von $\mathcal{o}$ bei $\mathfrak{p}$. Ausserdem hat $\mathfrak{p}$ in $\mathcal{O}$ die Faktorisierung

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_d^{e_d},$$

und die Exponentialbewertung $v_{\mathfrak{p}}$ besitzt also auf L die verschiedenen Fortsetzungen $w_{\mathfrak{P}_1}, \ldots, w_{\mathfrak{P}_d}$. Diese Bewertungsfortsetzungen sind genau dann unverzweigt, beziehungsweise rein verzweigt, wenn die dazugehörigen Primideale $\mathfrak{P}_i$ unverzweigt, beziehungsweise rein verzweigt, über $\mathfrak{p}$ sind.

(4.13) **Satz:** Seien $w_1, \ldots, w_d$ die verschiedenen Fortsetzungen von v auf L. Dann gilt

$$K_v \otimes_K L \cong \prod_{i=1}^{d} L_{w_i}.$$

Beweis: Siehe NEUKIRCH, Kap. II, §8, Satz (8.3).

(4.14) **Korollar:** Es gilt $[L : K] = \sum_{i=1}^{d} [L_{w_i} : K_v]$.

(4.15) **Definition:** Die zum Tensor-Produkt aus (4.13) gehörende Einbettung

$$\sigma : L \to \prod_{i=1}^{d} L_{w_i}$$

heisst *kanonische Einbettung.*

(4.16) **Bemerkung:** Die Aufteilung der $\mathbb{Q}$-Einbettungen eines Zahlkörpers K in r reelle und $2s$ komplexe Einbettungen in (1.46), sowie die kanonische Einbettung $\sigma : K \to \mathbb{R}^n \cong \mathbb{R}^r \oplus \mathbb{C}^s$ sind nichts anderes als die explizite Beschreibung des Tensor-Produkts $\mathbb{R} \otimes_{\mathbb{Q}} K$ mit der dazu gehörenden kanonischen Einbettung.

(4.17) **Definition:** Der Körper L heisst voll zerlegt über K an der Stelle v, falls v genau $n = [L : K]$ verschiedene Fortsetzungen auf L besitzt.

(4.18) **Bemerkung:** Nach (4.5) ist L genau dann voll zerlegt über K an der Stelle v, wenn die K-Einbettungen $\sigma_1, \ldots, \sigma_n : L \to \widehat{K_v}$ paarweise verschiedene Fortsetzungen von v auf L induzieren. Nach dem vorherigen Korollar gilt dann ausserdem $L_{w_i} \cong K_v$ für $1 \leq i \leq n$. In diesem Fall lässt sich die kanonische Einbettung $\sigma : L \to \prod_{i=1}^{d} L_{w_i}$ nach (4.13) beschreiben durch $\sigma = (\sigma_1, \ldots, \sigma_n) : L \to K_v^n$.

(4.19) **Bemerkung:** In der Situation von (4.12) ist L gerade dann voll zerlegt über K an der Stelle $v_\mathfrak{p}$, wenn das Primideal $\mathfrak{p}$ in L voll zerlegt ist.

§2 Gitter im ultrametrischen Fall

Von nun an sei $\mathbb{F}$ ein endlicher Körper mit $q = p^r$ Elementen, und sei $K = \mathbb{F}(t)$ der rationale Funktionenkörper über $\mathbb{F}$. Dann ist $\left|\frac{f}{g}\right|_\infty := q^{\deg(f)-\deg(g)}$ eine Bewertung von K. Die Komplettierung von K bezüglich $|\cdot|_\infty$ ist der Körper der formalen Laurent-Reihen mit endlichem Hauptteil $K_\infty = \mathbb{F}((t^{-1}))$ mit der der Bewertung $\left|\sum_{i=-\infty}^{m} a_i t^i\right|_\infty := q^m$, falls $a_m \neq 0$.

(4.20) **Bemerkung:** Die Bewertung $|\cdot|_\infty$ ist nicht-archimedisch; also gilt die verschärfte Dreiecksungleichung.

Sei im Folgenden V ein n-dimensionaler K_∞-Vektorraum.

(4.21) **Satz:** Der Körper K_∞ ist lokal-kompakt. Es existiert genau eine Topologie auf V, bezüglich der V ein topologischer K-Vektorraum ist, und V ist homöomorph zu K_∞^n, also insbesondere auch lokal-kompakt. Ausserdem operiert GL_V auf V durch Homöomorphismen.

Beweis: Siehe Weil[1], Chap. 1, §2, Theorem 3 und Chap. 2, §1.

Sei im Folgenden weiter μ ein Haar-Mass auf V.

(4.22) **Satz:** Sei $\varphi : V \to V$ ein Automorphismus. Dann gilt

$$\mathrm{mod}_V(\varphi) = \mathrm{mod}_K(\det(\varphi)) = |\det(\varphi)|_\infty.$$

Beweis: Siehe Weil[1], Chap. 1, §2, Corollary 3 und Chap. 1, §4, Theorem 6.

(4.23) **Definition:** Ein diskreter $\mathbb{F}[t]$-Untermodul $\Gamma \subset V$ vom Rang n heisst *vollständiges Gitter* in V.

(4.24) **Satz:** Sei $\Gamma \subset V$ ein $\mathbb{F}[t]$-Untermodul vom Rang n. Äquivalent sind:

i. Γ ist diskret.

ii. $\Gamma = \bigoplus_{i=1}^{n} \mathbb{F}[t] b_i$, wobei $\{b_1, \ldots, b_n\}$ eine Basis von V ist.

Beweis: Siehe Weil[1], Chap. 2, §2, Theorem 1.

(4.25) **Definition:** Sei $\Gamma \subset V$ ein vollständiges Gitter. Ein Repräsentantensystem Φ von V modulo Γ heisst *Fundamentalbereich* von Γ.

(4.26) **Bemerkung:** Als additive Gruppe ist $K_\infty = \mathbb{F}[t] \oplus t^{-1}\mathbb{F}[[t^{-1}]]$. Ist $\{b_1, \ldots b_n\}$ eine Basis von V und $\Gamma = \bigoplus_{i=1}^{n} \mathbb{F}[t] b_i$ das zugehörige vollständige Gitter, so ist

$$\Phi := \prod_{i=1}^{n} t^{-1}\mathbb{F}[[t^{-1}]] b_i$$

ein kompakter, also insbesondere messbarer, Fundamentalbereich von Γ.

(4.27) **Korollar:** Seien $\Gamma \subset V$ ein vollständiges Gitter, Φ ein messbarer Fundamentalbereich von Γ und μ ein Haar-Mass auf Γ. Dann ist $\mathrm{CoVol}(\Gamma) := \mu(\Phi) < \infty$ (und ausserdem ist $\mathrm{CoVol}(\Gamma)$ nach (1.52) unabhängig von der Wahl von Φ).

(4.28) **Gitterpunktsatz:** Sei $\Gamma \subset V$ ein vollständiges Gitter und $X \subset V$ eine messbare Untergruppe mit $\mu(X) > \mathrm{CoVol}(\Gamma)$. Dann gilt $X \cap \Gamma \neq \{0\}$.

Beweis: Man nehme an, für alle $\gamma_1, \gamma_2 \in \Gamma$ sei

$$(\gamma_1 + X) \cap (\gamma_2 + X) = \varnothing,$$

falls $\gamma_1 \neq \gamma_2$. Dann gilt auch für jeden messbaren Fundamentalbereich Φ

$$\big((\gamma_1 + X) \cap \Phi\big) \cap \big((\gamma_2 + X) \cap \Phi\big) = \varnothing$$

und somit

$$\mu(\Phi) \geq \sum_{\gamma \in \Gamma} \mu\big((\gamma + X) \cap \Phi\big) = \sum_{\gamma \in \Gamma} \mu\big(X \cap (\Phi - \gamma)\big) = \mu(X);$$

Widerspruch. Also existieren $\gamma_1, \gamma_2 \in \Gamma$ mit $\gamma_1 \neq \gamma_2$, und ein $v \in V$, mit $v \in (\gamma_1 + X) \cap (\gamma_2 + X)$. Das heisst, es existieren Elemente $x_1, x_2 \in X$ mit $v = \gamma_1 + x_1 = \gamma_2 + x_2$, und somit ist $\gamma_1 - \gamma_2 = x_2 - x_1 \in X \cap \Gamma \setminus \{0\}$. □

(4.29) **Bemerkung:** Man beachte die Analogie dieses Satzes zum Minkowskischen Gitterpunktsatz (1.45); an die Stelle der zentralsymmetrischen konvexen Menge tritt die messbare Gruppe; in gewisser Weise entspricht dabei die Abgeschlossenheit der Gruppe der Konvexität und die Invertierbarkeit der Elemente der Zentralsymmetrie. Die Tatsache, dass im archimedischen Fall ein Faktor 2^n auftritt, und die Menge X also grösser sein muss, kommt daher, dass die Bedingung, dass X konvex und zentralsymmetrisch sein muss, tatsächlich weniger stark ist als die Entsprechung im nicht-archimedischen Fall. Natürlich wäre es unsinnig in Charakteristik 0 zu verlangen, dass X eine Untergruppe sein soll, da jede messbare Untergruppe von $\mathbb{R}^n$ Mass 0 oder ∞ hat.

Von nun an bezeichne μ das durch $\mathrm{CoVol}\big(\bigoplus_{i=1}^n \mathbb{F}[t]e_i\big) = 1$ normierte Haar-Mass auf K_∞^n.

(4.30) **Satz:** Sei L ein Funktionenkörper vom Grad n über K, der bezüglich der Bewertung $|\cdot|_\infty$ voll zerlegt ist. Dann ist das Bild Γ von $\mathcal{O}_L$ unter der kanonischen Einbettung σ ein vollständiges Gitter in K_∞^n, und es gilt $\mathrm{CoVol}(\Gamma) = \sqrt{|d_L|_\infty}$.

Beweis: Offensichtlich ist σ injektiv und Γ ein $\mathbb{F}[t]$-Untermodul vom Rang n von K_∞^n. Sei $\{\alpha_1, \ldots, \alpha_n\}$ eine $\mathbb{F}[t]$-Basis von $\mathcal{O}_L$ und sei $A := (\sigma_i(\alpha_j))_{i,j=1}^n$. Nach Definition ist $d_L = \det(A)^2$, also ist A ein Homöomorphismus. Ausserdem ist $\Gamma = A\big(\bigoplus_{i=1}^n \mathbb{F}[t]e_i\big)$, und somit ist Γ diskret (also ein Gitter) und nach (4.22) ist $\mathrm{CoVol}(\Gamma) = |\det A|_\infty$. □

(4.31) **Bemerkung:** Falls L nicht vollzerlegt ist über K, so existieren zwar eine kanonische Einbettung

$$\mathcal{O}_L \to K_v \otimes_K L,$$

nämlich die Einschränkung der kanonischen Einbettung von L, sowie ein kanonischer Isomorphismus

$$K_v \otimes_K L \cong \prod_{i=1}^d L_{w_i},$$

aber $\prod_{i=1}^d L_{w_i}$ besitzt als K_v-Vektorraum keine natürliche Basis. Um das Argument wie oben führen zu können müsste man eine solche Basis also unabhängig

von der Gestalt von L in einer Weise wählen, die es erlaubt die Normen in diesem Vektorraum zu kontrollieren. Gewisse Schwierigkeiten ergeben sich dabei bereits bei der Erweiterung der Restklassenkörper, erst recht aber beim verzweigten Teil der Erweiterung. Um diese Probleme im Allgemeinen zu lösen muss die Verzweigung an allen, und nicht nur an den endlichen, Stellen beachtet werden, wie (4.34) zeigt. Dazu muss neben der Diskriminante d_L auch die lokale Diskriminante d_{L_∞} in die Argumentation eingehen.
Man beachte ausserdem die Analogie dieses Satzes zu Satz (1.48). Das oben beschriebene Problem ergibt sich aber nicht, wenn K ein Zahlkörper ist, da dann die Komplettierungen an allen Stellen isomorph zu $\mathbb{R}$ oder $\mathbb{C}$ (mit der natürlichen Basis $\{1, \sqrt{-1}\}$) sind, während es im Funktionenkörperfall für die Körper L_{w_i} unendlich viele Möglichkeiten gibt.

§3 Der Satz von Hermite

(4.32) **Satz:** Seien $n \in \mathbb{N}$ und $d \in \mathbb{F}[t]$. Es existieren nur endlich viele Funktionenkörper L vom Grad $[L : K] = n$ mit Diskriminante $d_L = d$, die bezüglich der Bewertung $|\cdot|_\infty$ voll zerlegt sind.

Beweis: Für eine positive Konstante C betrachte man die Menge

$$X_C := \{x = (x_1, \dots x_n) \in K_\infty^n \mid |x_1|_\infty < C\sqrt{|d|_\infty}, |x_i|_\infty < 1 \text{ für } 2 \le i \le n\}.$$

Offensichtlich ist X_C eine offene Untergruppe von K_∞^n, und da μ das Produkt-Mass der durch $\mathrm{CoVol}(\mathbb{F}[t]) = 1$ normierten Haar-Masse auf K_∞ ist, gilt ausserdem $\lim_{C\to\infty} \mu(X_C) = \infty$
Sei Γ das Bild von $\mathcal{O}_L$ unter der kanonischen Einbettung von L in K_∞^n. Man wähle C so gross, dass $\mu(X_C) > \sqrt{|d|_\infty}$ ist. Nach (4.30) ist dann $\mu(X_C) > \mathrm{CoVol}(\Gamma)$, also enthält X_C nach (4.28) einen von Null verschiedenen Gitterpunkt, das heisst $\exists f \in \mathcal{O}_L \setminus \{0\}$, sodass gilt

- $|\sigma_1(f)|_\infty < C\sqrt{|d|_\infty}$ und
- $|\sigma_i(f)|_\infty < 1$ für $i > 2$.

Wegen $f \in \mathcal{O}_L$ ist $\mathrm{N}_{L|K}(f) \in \mathbb{F}[t]$, also gilt $\prod_{i=1}^n |\sigma_i(f)|_\infty = |\mathrm{N}_{L|K}(f)|_\infty \ge 1$ und folglich ist $|\sigma_1(f)|_\infty \ge 1$. Somit ist $\sigma_1(f) \ne \sigma_i(f)$ für alle $i \ge 2$. Nach (1.8) ist also $L = K(f)$.
Die Konjugierten $\sigma_i(f)$ von f sind nach Konstruktion für $2 \le i \le n$ durch $|\sigma_i(f)|_\infty < 1$, sowie durch $|\sigma_1(f)|_\infty < C\sqrt{|d|}$ beschränkt, und somit sind (nach Vieta) auch die Koeffizienten des Minimalpolynoms m_f von f beschränkt. Wegen $f \in \mathcal{O}_L$ hat m_f Koeffizienten in $\mathbb{F}[t]$, und somit gibt es für $m_f \in \big(\mathbb{F}[t]\big)[X]$ und deshalb auch für $f \in \overline{K}$ nur endlich viele Möglichkeiten. □

(4.33) **Bemerkung:** Wieder beachte man, dass Aussage und Beweis analog zu jenen von (3.1) sind. Die Aussage von (3.1) ist allerding etwas allgemeiner, da man dort nicht gefordert hat, dass die Erweiterungen voll zerlegt sein müssen. Diesem Umstand wird im Beweis Rechnung getragen, indem durch das Adjungieren des Elements $\sqrt{-1}$ im ersten Beweisschritt die Verzweigung fixiert wird.

(4.34) **Bemerkung:** Im Funktionenkörperfall muss jeweils mehr gefordert werden als für die entsprechenden Aussagen im Zahlkörperfall:

- Die Forderung von Separabilität im Satz von Hermite ist notwendig; (1.5) liefert eine unendliche Familie von Körpererweiterungen vom Grad p und Diskriminante 0.
- Sei $n \in \mathbb{N}$ nicht durch p teilbar, und sei $L = \big(\mathbb{F}_p(t)\big)[X]/(X^p - X - t^n)$. Offensichtlich ist dann $[L : K] = p$ und

$$d_L = \mathrm{Res}(X^p - X - t^n, -1) = 1,$$

wobei Res die Resultante bezeichnet.
Dies zeigt, dass das direkte Analogon des Satzes von Minkowski im Funktionenkörperfall nicht gilt, und dass es ausserdem für den Satz von Hermite im Funktionenkörperfall nicht genügt den Grad und die Diskriminante zu fixieren, wenn die Erweiterung bei ∞ verzweigt ist.

Literaturverzeichnis

Neukirch	J. Neukirch: Algebraische Zahlentheorie. Springer Verlag, Berlin 2007
Rosen	M. Rosen: Number Theory in Function Fields. Springer Verlag, New York 2002
Weil[1]	A. Weil: Basic Number Theory. Springer Verlag, Berlin 1967
Weil[2]	A. Weil: L'intégration dans les groupes topologiques. Hermann, Paris 1965
Zariski	O. Zariski & P. Samuel: Commutative Algebra, Vol. 1. Springer Verlag, Berlin, 1975