Arithmetische Geometrie I:

Grundlagen der algebraischen Zahlentheorie und das Grothendieck-Riemann-Roch Theorem für arithmetische Kurven

Ulf Kühn

Version vom 7. Januar 2005

Inhaltsverzeichnis

Einleitung

0.1. Vorbemerkungen. Das vorliegende Skript entspricht im wesentlichen der im Wintersemester 2003/04 an der Humboldt Universität zu Berlin gehaltenen 4-stündigen Vorlesung mit dem Titel Arithmetische Geometrie I.

Im ersten Teil werden die Grundlagen der algebraischen Zahlentheorie behandelt. Darauf aufbauend wird im zweiten Teil die Arakelov Theorie für arithmetische Kurven entwickelt. Diese Theorie ermöglicht einen konzeptionellen Zugang zu den klassischen Hauptsätzen der algebraische Zahlentheorie.

Im Gegensatz zu anderen Einführungen in die eindimensionale Arakelov Theorie wird hier die Kenntniss der Theorie algebraischer Kurven, bzw. kompakter Riemannscher Flächen nicht vorausgesetzt. Dieses Konzept entspricht den Voraussetzungen, die die Studenten am Anfang des Hauptstudiums haben, und hat sich in der Vorlesung bewährt.

Die Darstellung des Stoffes orientiert sich an dem Buch von J. Neukirch [Ne], der Diplomarbeit von D. Roessler [Ro] und dem im Internet erhältlichen Vorlesungsskript von J. Milne [Mi]. Im Ausblick auf die geplante Fortsetzung der Vorlesung sind die Notationen jedoch wie in der höherdimensionalen Arakelov Theorie (cf. [SABK], [BKK]) gewählt.

Die arithmetische K-Theorie kohärenter hermitescher Moduln wird hier nicht betrachtet, denn aufgrund der neuen Beweismethode von Satz 15.8 können wir das Grothendieck-Riemann-Roch Theorem für arithmetische Kurven, d.h., die Kommutativität des folgenden Diagramms

$$\begin{array}{ccc} \widehat{K}_0(\mathcal{O}_L) & \xrightarrow{\widehat{Td}(\Omega^1_{\mathcal{O}_L|\mathcal{O}_K})\cdot\widehat{ch}(\,\cdot\,)} & \widehat{\mathrm{CH}}(\mathcal{O}_L)_{\mathbb{Q}} \\ \downarrow{\scriptstyle i_*} & & \downarrow{\scriptstyle i_*} \\ \widehat{K}_0(\mathcal{O}_K) & \xrightarrow{\widehat{ch}(\,\cdot\,)} & \widehat{\mathrm{CH}}(\mathcal{O}_K)_{\mathbb{Q}}, \end{array}$$

auch ohne letztgenannte Theorie beweisen. Die Arakelov Theorie auf singulären arithmetischen Kurven wurde aus Zeitmangel ebenfalls nicht behandelt.

0.2. Erste Einblicke in die algebraische Zahlentheorie. Ein Körper K heißt algebraischer Zahlkörper genau dann wenn K endliche Erweiterung von $\mathbb{Q}$ ist. Der Ring der ganzen Zahlen $\mathcal{O}_K$ ist der Teilring von K für den gilt:

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

Zum Beispiel, sei $K = \mathbb{Q}[\sqrt{d}]$, d quadratfrei, $d \in \mathbb{Z}$, dann gilt für alle $\alpha = a + b\sqrt{d} \in K$

$$f(\alpha) = X^2 - 2aX + \left(a^2 - b^2 d\right) = \left(X - (a + b\sqrt{d})\right)\left(X - (a - b\sqrt{d})\right) = 0.$$

Es folgt $\alpha \in \mathcal{O}_K$ genau dann, wenn $2a \in \mathbb{Z}$ und $a^2 - b^2 d \in \mathbb{Z}$. Man zeigt:

$$\mathcal{O}_K = \mathbb{Z}[\sqrt{d}] = \{m + n\sqrt{d} \mid m, n \in \mathbb{Z}\}, \text{ falls } d \equiv 2, 3 \pmod 4$$
$$\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{m + n\frac{1+\sqrt{d}}{2}\Big| \, m, n \in \mathbb{Z}\right\}, \text{ falls } d \equiv 1 \pmod 4$$

(im letzten Fall ist $\alpha = a + b\sqrt{d} \in \mathcal{O}_k$ genau dann wenn a und b ganz oder a und b beide halbganz sind).

Der Fundamentalsatz der Arithmetik besagt, daß jede ganze Zahl $m \in \mathbb{Z}$ eine eindeutige Primfaktorzerlegung hat, d.h. m besitzt eine bis auf Permutation der einzelnen Faktoren eindeutige Darstellung $m = u \cdot p_1^{r_1} \cdot \ldots \cdot p_n^{r_n}$ wobei $u = \pm 1$, p_i eine Primzahl und die Exponenten r_i sowie n natürliche Zahlen sind.

Sei nun R ein Integritätsbereich, dann heißt ein Element p von R irreduzibel, falls p weder 0 noch Einheit ist und nicht Produkt zweier Nicht-Einheiten ist. In $\mathcal{O}_K$ kann jedes Element als Produkt von irreduziblen Elementen dargestellt werden, allerdings nicht eindeutig. Zum Beispiel gilt in $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}). \tag{0.2.1}$$

Wir zeigen jetzt mit Hilfe der Normabbildung

$$\begin{aligned} \mathrm{Nm} : \mathbb{Q}[\sqrt{-5}] &\to \mathbb{Q} \\ a + b\sqrt{5} &\mapsto a^2 + 5b^2 = (a + b\sqrt{-5})(a - b\sqrt{-5}), \end{aligned}$$

daß 2 , 3, $1+\sqrt{-5}$ und $(1-\sqrt{-5})$ irreduzibel sind. Wir beachten, daß für die Normabbildung mit $\alpha \in \mathcal{O}_K$ gilt

$$\mathrm{Nm}(\alpha) = 1 \Leftrightarrow \alpha\overline{\alpha} = 1 \Leftrightarrow \alpha \text{ ist Einheit.}$$

Angenommen $1 + \sqrt{-5} = \alpha \cdot \beta$, dann ist wegen $\mathrm{Nm}(1 + \sqrt{-5}) = \mathrm{Nm}(\alpha) \cdot \mathrm{Nm}(\beta) = 6$, $\mathrm{Nm}(\alpha) = 1$, 2 , 3 oder 6. Falls $\mathrm{Nm}(\alpha) = 1$ oder $\mathrm{Nm}(\alpha) = 6$, dann ist α bzw. β eine Einheit. $\mathrm{Nm}(\alpha) = 2$, 3 ist nicht möglich, weil 2 bzw. 3 keine Quadrate sind. Es folgt $1 + \sqrt{-5}$ ist irreduzibel. Analog zeigt man 2, 3, $1 - \sqrt{-5}$ ist irreduzibel. Beachte: $1 + \sqrt{-5} \mid 2 \cdot 3$, aber $1 + \sqrt{-5} \nmid 2$ und $1 + \sqrt{-5} \nmid 3$, d.h. irreduzible Elemente sind nicht unbedingt primär ($\alpha \in \mathcal{O}_K$ primär genau dann wenn $\alpha \mid \beta\gamma \Rightarrow \alpha \mid \beta$ oder $\alpha \mid \gamma$).

Die Idee von Kummer und Dedekind dieses Defizit zu beheben besteht darin, die Menge der Primzahlen von $\mathcal{O}_K$ zu vergrößern. Ein Ideal $\mathfrak{a}$ ist eine Teilmenge von $\mathcal{O}_K$ für die gilt: $0 \in \mathfrak{a}$, aus a, $b \in \mathfrak{a}$ folgt $a + b \in \mathfrak{a}$ und falls $a \in \mathfrak{a}$ dann ist $b \cdot a \in \mathfrak{a}$ für alle $b \in \mathcal{O}_K$. Ein Ideal $\mathfrak{a}$ heißt Primideal, falls zusätzlich gilt: aus $a \cdot b \in \mathfrak{a}$ folgt $a \in \mathfrak{a}$ oder $b \in \mathfrak{a}$. Man hat folgende Multiplikation von Idealen

$$\mathfrak{a} \cdot \mathfrak{b} = \left\{\sum a_i b_i \mid \; a_i \in \mathfrak{a}, \; b_i \in \mathfrak{b}\right\}.$$

Man zeigt (siehe Satz 2.7): in $\mathcal{O}_K$ existiert eine bis auf Permutation eindeutige Primidealzerlegung von Idealen

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdot \ldots \cdot \mathfrak{p}_n^{r_n}.$$

Beachte: Jedes $\alpha \in \mathcal{O}_K$ bestimmt ein Ideal, nämlich $(\alpha) = \{\alpha \cdot \mathcal{O}_K\}$. Ideale der Form (α) heißen Hauptideale. In unserem Beispiel 0.2.1 gilt dann:

$$(6) = (\mathfrak{p}_1 \cdot \mathfrak{p}_2) \cdot (\mathfrak{p}_3 \cdot \mathfrak{p}_4) = (\mathfrak{p}_1 \cdot \mathfrak{p}_3)\,(\mathfrak{p}_2 \cdot \mathfrak{p}_4)\,,$$

wobei $\mathfrak{p}_j,\ j = 1, \ldots, 4$ die folgenden Primideale sind:

$$\mathfrak{p}_1 = (2, 1 + \sqrt{-5}) = \{2\mathcal{O}_K + (1 + \sqrt{-5}) \cdot \mathcal{O}_K\},$$
$$\mathfrak{p}_2 = (2, 1 - \sqrt{-5}),\ \ \mathfrak{p}_3 = (3, 1 + \sqrt{-5}),\ \ \mathfrak{p}_4 = (3, 1 - \sqrt{-5}).$$

Indem man die Halbgruppe der Ideale mit gebrochenen Hauptidealen $(\alpha) = \{\alpha\mathcal{O}_K\}$, wobei $\alpha \in K^*$ ist, erweitert, erhält man eine Gruppenstruktur auf der Menge der Ideale. Die Idealklassengruppe Cl_K ist der Quotient dieser Gruppe modulo der gebrochenen Hauptideale. Wir werden zeigen, daß Cl_K eine endliche Gruppe ist (siehe Satz 3.3 und Satz 12.2). Ihre Ordnung h_K heißt die Klassenzahl von K und ist eine wichtige Invariante des Zahlkörpers K.

Ist $L|K$ eine endliche Körpererweiterung und $\mathfrak{p} \in \mathcal{O}_K$ ein Primideal, dann interessiert man sich für die Primidealzerlegung des Ideals $\mathfrak{p}\mathcal{O}_L \subset \mathcal{O}_L$. Zum Beispiel erhält man in $\mathbb{Z}[i]$ das folgende Zerlegungsverhalten von Primidealen: Sei p eine ungerade Primzahl, dann sind äquivalent:

(a) $p \equiv 1 \pmod 4$,

(b) (p) ist zerlegt in $\mathbb{Z}[i]$,

(c) es existieren $a, b \in \mathbb{Z}$ mit $p = a^2 + b^2$

Das sieht man wie folgt: Wir wissen, daß $\mathbb{Z}[i]$ ein Hauptidealring ist. Das Polynom $p_i = X^2 + 1$ ist das Minimalpolynom von i, deshalb ist $p \in \mathbb{Z}$ in $\mathbb{Z}[i]$ genau dann zerlegt, falls X^2+1 modulo p in Linearfaktoren zerfällt. Dies ist der Fall, wenn -1 ein Quadrat modulo p ist, was genau dann passiert, wenn $\mathbb{F}_p$ eine 4-te Einheitswurzel enthält. Da $\mathbb{F}_p^*$ zyklisch von Ordnung $p-1$ ist, folgt $4|p-1$, also $p \equiv 1 \pmod 4$. Deshalb gilt (a) $\Leftrightarrow$ (b). Sei (p) zerlegt in $\mathbb{Z}[i]$. Dann ist $(p) = \mathfrak{p}_1\mathfrak{p}_2$ mit Hauptidealen $\mathfrak{p}_1, \mathfrak{p}_2$ Aus $\mathfrak{p}_1 = (a + bi)$ folgt $\mathfrak{p}_2 = (a - bi)$. Deshalb ist $p = [a^2 + b^2] \cdot \mu$, wobei μ eine Einheit in $\mathbb{Z}[i]$, d.h. $\mu = \pm 1, \pm i$. Sei umgekehrt $p = a^2 + b^2$, dann gilt in $\mathbb{Z}[i]$, $p = [a + bi] \cdot [a - bi]$ und somit auch $(p) = (a + bi) \cdot (a - bi)$. $\square$

Wir weisen an dieser Stelle darauf hin, daß die Äquivalenz (a) $\Leftrightarrow$ (c) das erste Mal in einem Brief von Fermat im Jahr 1654 erwähnt wurde. Unabhängig davon, hat jedoch vermutlich Euler diese zuerst bewiesen.

0.3. Plan der Vorlesung. Im ersten Teil der Vorlesung werden obige und weitere Eigenschaften des Ringes der ganzen Zahlen eines algebraischen Zahlkörpers untersucht. Nachdem dann die Grundlagen der algebraischen Zahlentheorie bereitgestellt sind, öffnen sich viele Möglichkeiten die erworbenen Kenntnisse zu vertiefen. Der interessierte Leser kann sich anhand folgender, unvollständiger Liste selbst davon überzeugen:

- Zetafunktionen und L-Reihen

- Klassenkörpertheorie
- algorithmische Zahlentheorie
- p-adische Körper, Adele
- Kreisteilungskörper und der Satz von Fermat

Wir werden uns mit der eindimensionalen Arakelovtheorie beschäftigen. Ein wichtiger Bestandteil dieser Theorie ist die erste arithmetische Chowgruppe $\widehat{\mathrm{CH}}^1(\mathcal{O}_K)$. Sie wird durch folgende exakte Sequenz beschrieben:

$$1 \longrightarrow \mu(K) \longrightarrow \mathcal{O}_K^* \longrightarrow \mathbb{R}^{r_1+r_2} \longrightarrow \widehat{CH}^1(\mathcal{O}_K) \longrightarrow Cl_K \longrightarrow 1,$$

hierbei sind $\mu(K)$ die Einheitswurzeln von K, $\mathcal{O}_K^*$ die Einheiten von $\mathcal{O}_K$ und K habe r_1 reelle und $2r_2$ Einbettungen in den Körper $\mathbb{C}$. Man zeigt leicht, daß $\widehat{\mathrm{CH}}(\mathcal{O}_K) = \mathbb{Z} \oplus \widehat{\mathrm{CH}}^1(\mathcal{O}_K)$ eine Ringstruktur trägt. Wir werden die Eigenschaften dieser Ringe studieren. Ist zum Beispiel $i : K \hookrightarrow L$ eine endliche Körpererweiterung, dann erhält man Abbildungen i_*, i^* zwischen den zu K und L assozierten arithmetischen Chowringen.

1 Ganzheit, Norm und Spur ganzer Elemente

Der Begriff der Ganzheit ist Gegenstand der allgemeinen Theorie von Ringen (bei uns sind Ringe immer kommutativ und unitär, d.h. sie haben eine Eins), Ferner sind alle Erweiterungen als endlich und algebraisch zu betrachten.

1.1. Definition. Sei $A \subset B$ eine Ringerweiterung. Ein Element $b \in B$ heißt *ganz* (engl.: integral) über A, wenn es der normierten Gleichung

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0 \ \ (n \geq 1)$$

mit Koeffizienten $a_i \in A$ genügt. Der Ring B heißt *ganz* über A, falls jedes Element $b \in B$ ganz über A ist.
Es ist a priori ist nicht klar, ob aus $b_1, b_2 \in B$ ganz über A auch $b_1 + b_2$ und $b_1 \cdot b_2$ ganz über A folgt.

1.2. Satz. *Endlich viele Elemente $b_1, \ldots, b_n \in B$ sind genau dann ganz über A, wenn der Ring $A[b_1, \ldots, b_n]$, aufgefaßt als A-Modul endlich erzeugt ist.*
Beweis. "$\Rightarrow$ " Sei $b \in B$ ganz über A und $f \in A[x]$ ein normiertes Polynom mit $f(b) = 0$. Für alle $g(x) \in A[x]$ gilt dann

$$g(x) = q(x) \cdot f(x) + r(x)$$

mit $q(x), r(x) \in A[x]$ und $\deg\ r(x) < \deg f = d$ und somit dann $g(b) = r(b) = a_0 + \ldots + a_{d-1} b^{d-1}$. Also ist $A[b]$ als A-Modul von $1, b, \ldots b^{d-1}$ erzeugt. Der allgemeine Fall $b_1, \ldots, b_n \in$

B ganz über A folgt durch Induktion nach n. Ist nämlich b_n ganz über $A\,[b_1, \ldots, b_{n-1}]$, dann ist mit obiger Argumentation auch $A[b_1, \ldots, b_n]$ als A-Modul endlich erzeugt.

"$\Leftarrow$ " Sei $A[b_1, \ldots, b_n]$ endlich erzeut und $w_1, \ldots w_r$ ein Erzeugendensystem. Setzt man $b \in A[b_1, \ldots, b_n]$, dann existiert eine Matrix (a_{ij}) so daß für $i = 1, \ldots, r$ gilt

$$b \cdot w_i = \sum_{j=1}^{r} a_{ij} w_j, \quad a_{ij} \in A. \tag{1.2.1}$$

Sei B die Matrix $b \cdot \mathbb{E}_r - (a_{ij})$ und $d = \det(B)$. Sei B^* die adjungierte Matrix zu B (d.h. $B^* = (b^*_{ij})$, $b^*_{ij} = (-1)^{i+j} \det(B_{ij})$, wobei B_{ij} diejenige Matrix beschreibt, die man durch das streichen der i-te Spalte und j-te Zeile erhält), dann ist $B^t B^* = d \cdot \mathbb{E}_r$.

Wegen (1.2.1) ist $wBB^{*t} = 0$ für $w = (w_1, \ldots, w_r)$. Also ist $d \cdot w_i = 0$ für alle i. Da aber $1 \in A[b_1, \ldots, b_n]$ und $1 = \sum a_i w_i$ gilt, muß $d = 0$ sein. Also ist b Wurzel des normierten Polynoms $\det(B)$. □

1.3. Korollar. *Seien $b, c \in A[b_1, \ldots, b_n]$, also ganze Elemente, dann sind auch $b + c$ und $b \cdot c$ ganz über A.*

Beweis. Es ist klar, daß $b + c$, $b \cdot c \in A[b_1, \ldots, b_n]$. Da jedes Element aus $A[b_1, \ldots, b_n]$ ganz über A ist, gilt dies auch für $b + c$ und $b \cdot c$. □

1.4. Bemerkung. Seien $A \subseteq B \subseteq C$ zwei Ringerweiterungen. Ist C ganz über B und B ganz über A, dann ist auch C ganz über A. (Übung)

1.5. Definition. Die Menge

$$\overline{A} = \{b \in B \mid b \text{ ganz über } A\}$$

in einer Ringerweiterung B über A ist somit ein Ring. Man nennt $\overline{A}$ den *ganzen Abschluß* von A in B. Der Ring A heißt *ganzabgeschlossen* in B, falls $A = \overline{A}$. Beachte $\overline{A}$ ist *ganzabgeschlossen* in B. Ist A ein Integritätsring mit Quotientenkörper K, dann heißt der ganze Abschluß $\overline{A}$ von A in K die *Normalisierung* von A.

1.6. Bemerkung. Jeder faktorielle Ring A ($\widehat{=}$ ZPE-Ring) ist ganzabgeschlossen in seinem Quotientenkörper: Sei nämlich $\frac{a}{b} \in K$ ganz über A, $a, b \in A$ und $\left(\frac{a}{b}\right)^n + a_1 \left(\frac{a}{b}\right)^{n-1} + \ldots + a_n = 0$, $a_i \in A$, dann ist

$$a^n + a_1 b a^{n-1} + \ldots + a_n b^n = 0.$$

Deshalb gilt $b \mid a$ und somit $\frac{a}{b} \in A$.

1.7. Satz. *Sei A ein ganzabgeschlossener Integritätsbereich mit Quotientenkörper K. Sei $L|K$ eine endliche Erweiterung und B der ganze Abschluß von A in L.*

(i) *Jedes Element $\beta \in L$ hat eine Darstellung der Form $\beta = \frac{b}{a}$ mit $b \in B$ und $a \in A$;*

(ii) *$\beta \in L$ ist ganz über A genau dann, wenn das Minimalpolynom $p_\beta(x) \in K[x]$ von β Koeffizienten in A hat.*

Beweis: (i) Sei $\beta \in L$ und $a_n\beta^n + \ldots + a_0 = 0,\ a_i \in A$ das zugehörige Minimalpolynom. Dann ist $b = a_n\beta$ ganz über A und offensichtlich ist $\beta = \frac{b}{a_n}$. (ii) Sei β ganz über A und sei $g(x) \in A[x]$ ein normiertes Polynom mit $g(\beta) = 0$. Dann ist das Minimalpolynom $p_\beta(x)$ ein Teiler von $g(x)$ in $K[x]$, da $K[x]$ ein ZPE-Ring ist. Es sei L der Zerfällungskörper von p_β. Alle Nullstellen $\beta_1, \ldots, \beta_n \in L$ von $p_\beta(x)$ sind ebenfalls Nullstellen von g, also ganz über A. Ausmultiplizieren der rechten Seite von $p_\beta(x) = (x - \beta_i) \cdots (x - \beta_n)$ zeigt, daß die Koeffizienten von p_β ganz über A sind. Weil $K \cap B = A$ ist, ist schließlich $p_\beta \in A[x]$. $\square$

1.8. Definition. Ein *algebraischer Zahlkörper* ist eine endliche Körpererweiterung K von $\mathbb{Q}$. Die Elemente von K heißen algebraische Zahlen. Eine algebraische Zahl heißt ganz über $\mathbb{Z}$, wenn sie Nullstelle eines normierten Polynoms $f(x) \in \mathbb{Z}[x]$ ist. Man nennt die Normalisierung $\mathcal{O}_K$ von $\mathbb{Z}$ in K den *Ring der ganzen Zahlen* von K.

Für das weitere Verständnis benötigen wir einige Grundlagen aus der Körpertheorie die wir im Appendix bereitgestellt haben (siehe A.1 – A.8).

1.9. Definition. Sei $L|K$ eine endliche Erweiterung. Sei $x \in L$ und $T_x : L \to L$ sei der Endomorphismus des K-Vektorraums L gegeben durch $T_x(\alpha) = x \cdot \alpha$. Dann ist die *relative Spur* und die *relative Norm* von x über K definiert durch $\mathrm{Tr}_{L|K}(x) = \mathrm{Tr}(T_x)$ und $\mathrm{Nm}_{L|K}(x) = \det(T_x)$.

1.10. Satz. *Sei $L|K$ separabel, dann gilt für $x \in L$:*

(i) $\mathrm{Tr}_{L|K}(x) = \sum_{\sigma \in \mathrm{Hom}_K(L,\overline{K})} \sigma(x).$

(ii) $\mathrm{Nm}_{L|K}(x) = \prod_{\sigma \in \mathrm{Hom}_K(L,\overline{K})} \sigma(x).$

Beweis. Sei $T_x : L \to L$ gegeben durch $T_x(\alpha) = x \cdot \alpha$ und sei $f_x(t) = \det(t\mathbb{E}_n - T_x) = t^n - a_1t^{n-1} + \ldots + (-1)^n a_n \in K[t]$ das charakteristische Polynom von T_x. Dann gilt $f_x(t) = p_x(t)^d$, wobei $p_x(t)$ das Minimalpolynom von x und $d = [L : K(x)]$ sind. Denn mit $p_x(t) = t^n + c_1t^{m-1} + \ldots + c_m,\ \ m = [K(x) : K]$, mit $1, x, \ldots, x^{m-1}$ als Basis von $K(x) \mid K$ und mit $\alpha_1, \ldots, \alpha_d$ als eine Basis von $L|K(x)$ ist $\alpha_1, \alpha_1x, \ldots, \alpha_1x^{m-1}, \ldots, \alpha_dx^{m-1}$ eine Basis von $L|K$. Bezüglich dieser Basis gilt

$$T_x = \underbrace{\begin{pmatrix} P & & & \\ & P & & \\ & & \ddots & \\ & & & P \end{pmatrix}}_{d \cdot m} \quad \text{mit} \quad P = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \ldots & \ldots & 0 & 1 \\ -c_m & \ldots & \ldots & \ldots & -c_1 \end{pmatrix},$$

also $T_x(y) = y^T T_x$, und weil $\mathrm{char}(P)(t) = p_x(t)$, gilt $f_x(t) = p_x(t)^d$. Die Menge $\mathrm{Hom}_K(L, \overline{K})$ zerfällt unter der Relation

$$\sigma \sim \tau \Leftrightarrow \sigma(x) = \tau(x)$$

in m Äquivalenzklassen der Mächtigkeit d.
Weil $L|K$ separabel ist, ist auch $L|K(x)$ und $K(x) \mid K$ separabel. Es gelten sowohl $m = \#\operatorname{Hom}_K(K(x), \overline{K})$, als auch $d = \#\operatorname{Hom}_{K(x)}(L, \overline{K})$, also läßt sich jede Einbettung von $K(x)$ auf m verschiedene Arten fortsetzen. Wenn nun $\sigma_1, \ldots, \sigma_m$ eine Repräsentantensystem obiger Äquivalenzklassen ist, so ist

$$p_x(t) = \prod_{i=1}^{m}(t - \sigma_i x)$$

und damit $f_x(t) = \prod_{i=1}^{m}(t - \sigma_i x)^d = \prod_{i=1}^{m}\prod_{\sigma\sim\sigma_i}(t - \sigma x) = \prod_{\sigma}(t - \sigma x)$. Die Behauptung folgt nun leicht. □

1.11. Satz. *Für einen Turm $K \subseteq L \subseteq M$ endlicher separabler Erweiterungen gilt:*

(i) $\operatorname{Tr}_{L|K} \circ \operatorname{Tr}_{M|L} = \operatorname{Tr}_{M|K}$;

(ii) $\operatorname{Nm}_{L|K} \circ \operatorname{Nm}_{M|L} = \operatorname{Nm}_{M|K}$.

Beweis. Die Menge der K-Einbettungen $\operatorname{Hom}_K(M, \overline{K})$ zerfällt unter der Relation

$$\sigma \sim \tau \Leftrightarrow \sigma \mid_L = \tau \mid_L$$

in $m = [L : K]$ Äquivalenzklassen. Ist $\sigma_1, \ldots, \sigma_m$ ein Repräsentantensystem, so ist

$$\operatorname{Hom}_K(L, \overline{K}) = \{\sigma_i \mid_L,\ \ i = 1, \ldots, m\}$$

und

$$\begin{aligned}\operatorname{Tr}_{M|K}(x) &= \sum_{i=1}^{m}\sum_{\sigma\sim\sigma_i}\sigma x = \sum_{i=1}^{m}\operatorname{Tr}_{\sigma_i(M)|\sigma_i(L)}(\sigma_i(x)) \\ &= \sum_{i=1}^{m}\sigma_i \operatorname{Tr}_{M|L}(x) = \operatorname{Tr}_{L|K}(Tr_{M|L}(x)).\end{aligned}$$

Auf analoge Art zeigt man die Aussage für die Norm. □

1.12. Bemerkung. (i) Sei A ganz abgeschlossener Integritätsbereich mit Quotientenkörper K und sei B der ganze Abschluß von A in einer endlichen Erweiterung $L|K$. Ist $x \in B$, dann ist auch σx ganz für alle $\sigma \in \operatorname{Hom}_K(L, \overline{K})$.Aus $\Sigma\sigma_i(x) = c_1$, $\Pi\sigma(x) = c_n$, wobei c_i für die Koeffizienten des Minimalpolynoms vom x stehen, folgt

$$Tr_{L|K}(x),\ \ Nm_{L|K}(x) \in A.$$

(ii) Für die Einheitengruppe B^* gilt

$$x \in B^* \Leftrightarrow Nm_{L|K}(x) \in A^*. \tag{1.12.1}$$

Denn wenn $a \cdot Nm_{L|K}(x) = 1$, für ein $a \in A$, dann ist $1 = a \cdot \prod_\sigma \sigma(x) = \left(a \cdot \prod_{\sigma \neq id} \sigma(x)\right) \cdot x$ mit $\left(a \prod_{\sigma \neq id} \sigma(x)\right) = x^{-1} \in L \cap B = B$.

1.13. Satz. *Ist $L|K$ separabel und A ein Hauptidealring, so ist jeder endlich erzeugte B-Untermodul $M \neq 0$ von L ein freier A-Modul vom Rang $[L : K]$. Insbesondere besitzt B eine Ganzheitsbasis.*

Für das folgende benötigen wir den Begriff der Diskriminante, den wir zuerst bereitstellen werden.

1.14. Definition. Die *Diskriminante* der Basis $\alpha_1, \ldots, \alpha_n$ einer separablen Erweiterung $L \mid K$ ist definiert vermöge

$$\operatorname{discr}(\alpha_1, \ldots, \alpha_n) = \det((\sigma_i \alpha_j)_{ij})^2 \ ,$$

wobei $\sigma_i,\ i = 1, \ldots, n$, die K-Einbettungen $L \to \overline{K}$ durchläuft.

1.15. Satz. *Sei $L|K$ separabel mit Basis $\alpha_1, \ldots, \alpha_d$ dann gilt:*

(i) $\operatorname{discr}(\alpha_1, \ldots, \alpha_n) = \det(Tr_{L|K}(\alpha_i \alpha_j))$.

(ii) $\operatorname{discr}(\alpha_1, \ldots, \alpha_n) \neq 0$.

(iii) *Die durch $(x, y) = Tr_{L|K}(xy)$ gegebene Bilinearform auf dem K-Vektorraum L ist nicht ausgeartet.*

Beweis. (i) Wegen $\operatorname{Tr}_{L|K}(\alpha_i \alpha_j) = \sum_{\operatorname{Hom}(L, \overline{K})} (\sigma_k \alpha_i)(\sigma_k \alpha_j)$ ist

$$\begin{aligned} \det(Tr_{L|K}(\alpha_i \alpha_j)_{ij}) &= \det((\sigma_k \alpha_i)^t_{ik} \cdot (\sigma_k \alpha_j)_{kj}) \\ &= \det((\sigma_k \alpha_i)_{ik})^2 \\ &= \operatorname{discr}(\alpha_1, \ldots, \alpha_n). \end{aligned}$$

(ii) und (iii) Sei $L = K[\theta]$ mit Basis $1, \theta, \theta^2, \ldots, \theta^{n-1}$. Dann ist $(x, y) = \operatorname{Tr}_{L|K}$ die Bilinearform bezüglich der Matrix $M = (\operatorname{Tr}_{L|K}(\theta^{i-1} \cdot \theta^{j-1}))_{ij}$. Mit $\theta_i = \sigma_i \theta$ gilt

$$\det(M) = \operatorname{discr}(1, \theta, \ldots \theta^{n-1}) = \prod_{i<j} (\theta_i - \theta_j)^2 \neq 0,$$

hierbei haben wir ausgenutzt, daß M eine Vandermondsche Matrix ist. Die Bilinearform (x, y) ist somit nicht ausgeartet. Ist nun $\alpha_1, \ldots, \alpha_n$ eine beliebige Basis von L, dann ist (x, y) bezüglich dieser Basis durch die Matrix $M_\alpha = (\operatorname{Tr}_{L|K}(\alpha_i \alpha_j))_{ij}$ gegeben. Wegen obiger Betrachtung ist M_α nicht singulär. □

1.16. Lemma. *Sei $\alpha_1, \ldots, \alpha_n \in B$ eine Basis von $L|K$ und $d = \operatorname{discr}(\alpha_1, \ldots, \alpha_n)$ die Diskriminante. Dann gilt:*

$$d \cdot B \subseteq A\alpha_1 + \ldots + A\alpha_n.$$

Beweis. Ist $\alpha = a_1\alpha_1 + \ldots + a_n\alpha_n \in B$, $a_j \in A$, so bilden die a_j eine Lösung des linearen Gleichungssystems

$$\mathrm{Tr}_{L|K}(\alpha_i\alpha) = \sum_j (\mathrm{Tr}_{L|K}(\alpha_i\alpha_j))_{ij} a_j.$$

$$\Leftrightarrow \quad A^* \begin{pmatrix} \mathrm{Tr}_{L|K}(\alpha_1\alpha) \\ \vdots \\ \mathrm{Tr}_{L|K}(\alpha_n\alpha) \end{pmatrix} = d \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \quad ,$$

wobei A^* die adjungierte Matrix zu $A = (\mathrm{Tr}_{L|K}(\alpha_i\alpha_j))_{ij}$ ist. Es gilt somit $da_j \in A$ für alle $j = 1, \ldots, n$ und somit

$$d\alpha \in A\alpha_1 + \ldots + A\alpha_n.$$

□

1.17. Definition. Seien A, B, K, L wie in obiger Bemerkung. Eine *Ganzheitsbasis* von B über A ist ein System von Elementen $\omega_1, \ldots, \omega_n \in B$, so daß jedes $b \in B$ sich eindeutig vermöge

$$b = a_1\omega_1 + \ldots + b_n\omega_n$$

als Linearkombination mit Koeffizienten $a_i \in A$ darstellen läßt.

Aus Satz 1.7 folgt, daß eine Ganzheitsbasis $\omega_1, \ldots, \omega_n$ stets eine K-Basis von $L|K$ ist. Deshalb ist $n = [L : K]$. Mit anderen Worten: Die Existenz einer Ganzheitsbasis bedeutet, daß B ein freier A-Modul ist. Im allgemeinen gibt es keine Ganzheitsbasis.

Beweis von Satz 1.13. (Existenz einer Ganzheitsbasis) Sei $M \neq 0$ ein endlich erzeugter B-Untermodul von L und $\alpha_1, \ldots, \alpha_n$ eine Basis von $L|K$. Nach Multiplikation mit einem geeigneten Element aus A liegt diese Basis sogar in B (weil $L = \frac{B}{A}$ ist). Wegen dem obigen Lemma gilt dann:

$$d \cdot B \subseteq A\alpha_1 + \ldots + A\alpha_n \quad .$$

Sei $\mu_1, \ldots, \mu_r \in M$ ein Erzeugendensystem des B-Moduls M. Da alle $\mu \in L$, gibt es ebenfalls ein $a \in A$ mit $a\mu_i \in B$, $i = 1, \ldots r$, also gilt: $aM \subseteq B$.
Damit ist

$$adM \subseteq dB \subseteq A\alpha_1 + \ldots + A\alpha_n = M_0 \quad .$$

Weil A ein Hauptidealring ist, und weil M_0 freier A-Modul, ist auch adM und somit auch M freie A-Moduln. Wegen

$$\mathrm{Rang}(M) = \mathrm{Rang}(dM) \leq \mathrm{Rang}(M_0) \leq \mathrm{Rang}(M)$$

ist Rang $(M) = \mathrm{Rang}(M_0) = [L : K]$. Die letzte Ungleichung gilt weil $M = B\cdot\mu_1 + \ldots + B\mu_r$ ein endlich erzeugter B-Modul und $B = A\alpha_1 + \ldots + A\alpha_n$ ist. Daraus folgt $\mathrm{Rang}_A M \geq n$ da bereits schon $\mu_i\alpha_1, \ldots, \mu_i\alpha_n$ für ein μ_i linear unabhängig über A sind. □

1.18. Definition. Sei $\mathcal{O}_K$ der Ring der ganzen Zahlen in einer endlichen Erweiterung K von $\mathbb{Q}$, d.h. $\mathcal{O}_K$ ist der ganze Abschluß von $\mathbb{Z}$ in K. Wir haben für jeden endlich erzeugten $\mathcal{O}_K$-Untermodul $\mathfrak{a}$ von K eine $\mathbb{Z}$-Basis $\alpha_1, \ldots, \alpha_n$

$$\mathfrak{a} = \mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_n \quad .$$

Die absolute Diskriminante $\mathrm{discr}(\mathfrak{a}) = \mathrm{discr}(\alpha_1, \ldots, \alpha_n)$ von $\mathfrak{a}$ ist unabhängig von der Wahl der Basis, da die Übergangsmatrizen zu einer anderen Basis die Determinante ± 1 haben. Man definiert die *(absolute) Diskriminante* D_K von K über $\mathbb{Q}$ vermöge

$$D_K = \mathrm{discr}(\mathcal{O}_K) = \mathrm{discr}(\mathfrak{a}).$$

2 Idealtheorie von Dedekindringen

2.1. Sei A ein Ring. Eine Teilmenge $\mathfrak{a} \subset R$ heißt *Ideal*, falls $\mathfrak{a}$ additiv abgeschlossen ist und $A\mathfrak{a} \subset \mathfrak{a}$ gilt. Mit anderen Worten ein Ideal $\mathfrak{a}$ ist ein A-Untermodul des A-Moduls A. A ist ein *Noetherscher Ring*, falls jedes Ideal von A endlich erzeugt ist. Ideale der Form $(a) = \{a \cdot A\} \subseteq A$ heißen *Hauptideale*. Ist jedes Ideal von A ein Hauptideal, dann heißt A ein *Hauptidealring*. Ein Ideal $\mathfrak{p}$ von A heißt *Primideal*, wenn $\mathfrak{p} \neq A$ ist und wenn gilt: Sind $a, b \in A \setminus \mathfrak{p}$, so ist auch $a \cdot b \in A \setminus \mathfrak{p}$, d.h., die Menge $A \setminus \mathfrak{p}$ ist multiplikativ abgeschlossen. Ein Ideal $\mathfrak{m}$ von A heißt *maximales Ideal*, wenn $\mathfrak{m} \neq A$ ist und für jedes Ideal $\mathfrak{a}$ mit $\mathfrak{m} \subsetneq \mathfrak{a} \subset A$, folgt, daß $\mathfrak{a} = A$ ist. Folgender Satz ist wohlbekannt:

2.2. Satz.

(i) *Ein Ideal $\mathfrak{p} \neq (0)$ von A ist genau dann ein Primideal, falls $A/\mathfrak{p}$ ein Integritätsring ist.*

(ii) *Ein Ideal $\mathfrak{m}$ von A ist genau dann maximal, wenn $A/\mathfrak{m}$ ein Körper ist.* □

2.3. Seien $\mathfrak{a}, \mathfrak{b}$ zwei Ideale von A. Man sagt: $\mathfrak{a}$ teilt $\mathfrak{b}$ und schreibt dafür auch $\mathfrak{a} \mid \mathfrak{b}$, falls $\mathfrak{b} \subseteq \mathfrak{a}$. Die Summe von $\mathfrak{a}$ und $\mathfrak{b}$ wird durch

$$\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a}, \quad b \in \mathfrak{b}\}$$

definiert. Sind $a, b \in A$, dann schreibt man auch (a, b) anstelle von $(a) + (b)$. Das Produkt von $\mathfrak{a}$ und $\mathfrak{b}$ ist definiert durch

$$\mathfrak{a} \cdot \mathfrak{b} = \{\sum_i a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\} \quad .$$

2.4. Satz. (Chinesischer Restsatz) *Sei A ein Integritätsbereich. Seien $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ Ideale mit $\mathfrak{a}_i + \mathfrak{a}_j = A$, also paarweise teilerfremd. Ist dann $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{a}_i$, so ist $A/\mathfrak{a} \cong \bigoplus_{i=1}^n A/\mathfrak{a}_i$.* □

2.5. Definition: Ein noetherscher, ganz abgeschlossener Integritätsbereich, in dem jedes von Null verschiedene Primideal ein maximales Ideal ist, heißt *Dedekindring*.

Eine wichtige Klasse von Dedekindringen liefert der folgende

2.6. Satz. *Sei K ein algebraischer Zahlkörper und $\mathcal{O}_K$ sein Ring der ganzen Zahlen. Dann ist $\mathcal{O}_K$ ein Dedekindring.*

Beweis. O_K ist endlich erzeugt: Sei $\beta_1, \ldots, \beta_n$ eine $\mathbb{Q}$-Basis von K. Mit Satz 1.7 kann angenommen werden, daß die β_i in $\mathcal{O}_K$ liegen. Da die Bilinearform $(x, y) \mapsto \mathrm{Tr}(xy)$ nicht ausgeartet ist, existiert eine zu $\beta_1, \ldots, \beta_n$ duale Basis $\beta_1', \ldots, \beta_n'$, so daß $\mathrm{Tr}(\beta_i \beta_j') = \delta_{ij}$. Es gilt dann $A\beta_1 + \ldots + A\beta_n \subset B \subset A\beta_1' + \ldots + A\beta_n'$.

Beweis der zweiten Inklusion: Sei $\beta \in B$, $\beta = \Sigma b_i \beta_i'$. Zz.: $b_i \in A$. Die β, β_i sind ganz, also ist auch $\mathrm{Tr}(\beta\beta_i)$ ganz für alle i. Es ist $\mathrm{Tr}(\beta\beta_i') = \mathrm{Tr}\left((\Sigma b_j \beta_j)\beta_i'\right) = \Sigma b_j \,\mathrm{Tr}(\beta_j \beta_i) = \Sigma b_j \delta_{ij} = b_i$. Also ist $b_i \in A$. Mit Satz 1.13 folgt, daß $\mathcal{O}_K$ als $\mathbb{Z}$-Modul endlich erzeugt ist.

Weil $\mathcal{O}_K$ der ganze Abschluß von $\mathbb{Z}$ in K ist, ist $\mathcal{O}_K$ ganz abgeschlossen in K. Sei nun $\mathfrak{p} \neq 0$ ein Primideal und $(p) = \mathfrak{p} \cap \mathbb{Z}$. Das Ideal (p) von $\mathbb{Z}$ ist ein von Null verschiedenes Primideal: Sei $y \in \mathfrak{p},\ y \neq 0$, und $y^n + a_1 y^{n-1} + \ldots + a_n = 0$, mit $a_i \in \mathbb{Z}$ und $a_n \neq 0$. Dann ist $a_n \in \mathfrak{p} \cap \mathbb{Z} = (p)$. Der Integritätsbereich $\mathcal{O}_K/\mathfrak{p}$ ist somit ein endlich erzeugter $\mathbb{F}_p = \mathbb{Z}/(p)$-Modul, in dem alle Elemente über $\mathbb{F}_p$ algebraisch sind, d.h. $\mathcal{O}_K/\mathfrak{p}$ ist ein Körper, also ist $\mathfrak{p}$ ein maximales Ideal. □

Eine weitere Klasse von Dedekindringen sind die Koordinatenringe von glatten, ebenen Kurven über $\mathbb{C}$ (siehe 9.4).

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

2.7. Satz.(Primidealzerlegung in Dedekindringen) *Jedes von* (0) *und* (1) *verschiedene Ideal $\mathfrak{a}$ von $\mathcal{O}$ besitzt eine bis auf die Reihenfolge eindeutige Zerlegung*

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

in Primideale $\mathfrak{p}_i$ von $\mathcal{O}$.

Faßt man die gleichen Primideale zusammen, so erhält man die Produktdarstellung

$$\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \cdot \ldots \cdot \mathfrak{p}_r^{\nu_r}\ ,\quad \nu_i > 0\ .$$

2.8. Definition. Ein *gebrochenes Ideal* von K ist ein endlich erzeugter $\mathcal{O}$-Untermodul $\mathfrak{a} \neq 0$ von K.

Für jedes $a \in K^*$ ist $(a) = a \cdot \mathcal{O}$ ein gebrochenes Hauptideal. Beachte: Ein $\mathcal{O}$-Untermodul $\mathfrak{a} \neq 0$ von K ist genau dann ein gebrochenes Ideal, falls es ein $c \in \mathcal{O}$ gibt mit $c\mathfrak{a} \subset \mathcal{O}$. Das gilt, weil $\mathcal{O}$ ein noetherscher Ring ist. Die Ideale von $\mathcal{O}$ werden auch als die *ganzen Ideale* von K bezeichnet. Wir setzen die Multiplikation von Idealen auf die gebrochenen Ideale fort.

2.9. Satz. *Die gebrochenen Ideale von K bilden ein abelsche Gruppe, die Idealgruppe J_K von K. Das Einselement ist $(1) = \mathcal{O}$, und das Inverse zu $\mathfrak{a}$ ist*

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

Beweis. Assoziativität, Kommutativität und Existenz der Eins sind offensichtlich. Zum Beweis der Existenz des Inversen benötigen wir folgendes Lemma, das wir später beweisen werden (vgl. Lemma 2.14):

Ist $\mathfrak{p}$ *ein Primideal von* $\mathcal{O}$ *so ist* $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathfrak{a}$ *für jedes Ideal* $\mathfrak{a} \neq 0$.

Sei nun $\mathfrak{p}$ ein Primideal, dann folgt aus dem Lemma $\mathfrak{p} \subsetneqq \mathfrak{p}\mathfrak{p}^{-1}$, und deshalb aus der Maximalität von $\mathfrak{p}$, daß $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$. Ist $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \cdot \ldots \cdot \mathfrak{p}_r^{\nu_r}$ ein ganzes Ideal, dann ist $\mathfrak{b} = \mathfrak{p}_1^{-\nu_1} \cdot \ldots \cdot \mathfrak{p}_r^{-\nu_r}$ mit $\mathfrak{p}_i^{-\nu_i} = \mathfrak{p}_i^{-1} \cdot \ldots \cdot \mathfrak{p}_i^{-1}$ (ν_i-Faktoren) ein Inverses. Denn aus $\mathfrak{b}\mathfrak{a} \subseteq \mathcal{O}$ folgt $\mathfrak{b} \subseteq \mathfrak{a}^{-1}$ und ist umgekehrt $x\mathfrak{a} \subseteq \mathcal{O}$, so ist $x\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{b}$ und weil $\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathcal{O}$, gilt dann $x \in \mathfrak{b}$. Es gilt deshalb $\mathfrak{b} = \mathfrak{a}^{-1}$. Sei nun $\mathfrak{a}$ ein beliebiges gebrochenes Ideal. Wähle $c \in \mathcal{O}$ mit $c \cdot \mathfrak{a} \subset \mathcal{O}$, dann ist $(c\mathfrak{a})^{-1} = c^{-1}\mathfrak{a}^{-1}$ das Inverse von $c\mathfrak{a}$. Aus der Assoziativität und Kommutativität des Produktes folgt $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}$. □

2.10. Als Anwendung erhalten wir, daß jedes gebrochene Ideal $\mathfrak{a}$ eine eindeutige Produktdarstellung

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

mit $\nu_\mathfrak{p} \in \mathbb{Z}$ und $\nu_\mathfrak{p} = 0$ für fast alle Primideale $\mathfrak{p}$ besitzt. Mit anderen Worten: J_K ist die durch die Primideale $\mathfrak{p} \neq 0$ erzeugte freie abelsche Gruppe.

2.11. Definition. Die gebrochenen Ideale $(a) = a\mathcal{O}$ mit $a \in K^*$ bilden eine Untergruppe von J_K, die Gruppe der *gebrochenen Hauptideale* P_K. Die Faktorgruppe

$$Cl_K = J_K/P_K$$

heißt die *Idealklassengruppe* .

2.12. Proposition. *Folgende Sequenz ist exakt*

$$1 \to \mathcal{O}^* \to K^* \to J_K \to Cl_K \to 1.$$

Hierbei sind die beiden ersten Morphismen die natürliche Inklusion, der dritte Morphismus ist gegeben durch die Abbildung $a \mapsto (a)$ *und die beiden letzten Morphismen sind die natürliche Projektion.*

Beweis: Übung. □

2.13. Lemma: *Zu jedem Ideal* $\mathfrak{a} \neq 0$ *von* $\mathcal{O}$ *existieren es von Null verschiedene Primideale* $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ *mit*

$$\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \subseteq \mathfrak{a}.$$

Beweis: Wir nehmen an, die Menge $\mathfrak{M}$ der Ideale, die dieser Bedingung widerspricht, sei nicht leer. Weil $\mathcal{O}$ noethersch ist, gibt es ein Ideal $\mathfrak{a} \in \mathfrak{M}$, das bezüglich der Inklusion maximal ist. Dieses Ideal $\mathfrak{a}$ ist kein Primideal, d.h. es gibt Elemente $b_1, b_2 \in \mathcal{O} \setminus \mathfrak{a}$, so daß $b_1 \cdot b_2 \in \mathfrak{a}$. Setze $\mathfrak{a}_1 = \mathfrak{a} + (b_1)$ und $\mathfrak{a}_2 = \mathfrak{a} + (b_2)$, dann ist $\mathfrak{a} \subsetneq \mathfrak{a}_1$, $\mathfrak{a} \subsetneq \mathfrak{a}_2$ und $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}$. Wegen der Maximalität von $\mathfrak{a}$ enthalten $\mathfrak{a}_1, \mathfrak{a}_2$ Primidealprodukte, deren Produkt in $\mathfrak{a}$ liegt. Es folgt ein Widerspruch. □

2.14. Lemma: *Sei $\mathfrak{p}$ ein Primideal von $\mathcal{O}$, so ist $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathfrak{a}$ für jedes Ideal $\mathfrak{a} \neq 0$.*

Beweis: Sei $a \in \mathfrak{p},\ a \neq 0$ und $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \subseteq (a) \subseteq \mathfrak{p}$ mit minimalem r. Weil $\mathfrak{p}$ ein Primideal ist, ist eines der $\mathfrak{p}_i$ gleich $\mathfrak{p}$, denn sonst gäbe es für jedes $i = 1, \ldots, r$ ein $a_i \in \mathfrak{p}_i \setminus \mathfrak{p}$ mit $a_1 \cdot \ldots \cdot a_r \in \mathfrak{p}$. O.B.d.A. sei $\mathfrak{p}_1 = \mathfrak{p}$. Wegen $\mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r \not\subseteq (a)$, gibt es ein $b \in \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r$ mit $b \notin a \cdot \mathcal{O}$, also auch $a^{-1}b \notin \mathcal{O}$. Andererseits ist $b \cdot \mathfrak{p} \subseteq (a)$, also $a^{-1}b\mathfrak{p} \subseteq \mathcal{O}$, und somit $a^{-1}b \in \mathfrak{p}^{-1}$. Wir folgern: $\mathfrak{p}^{-1} = \mathcal{O} \cdot \mathfrak{p}^{-1} \not\subseteq \mathcal{O}$.

Sei nun $\mathfrak{a} \neq 0$ ein Ideal von $\mathcal{O}$ und $\alpha_1, \ldots, \alpha_n$ ein Erzeugendensystem. Wir führen die Annahme $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$ zum Widerspruch. Aus unserer Annahme folgt, daß für jedes $\beta \in \mathfrak{p}^{-1}$ ein Gleichungssystem der Form

$$x\alpha_i = \sum_j a_{ij}\alpha_j\ , \qquad a_{ij} \in \mathcal{O}\ .$$

existiert. Somit ist β Nullstelle des normierten Polynoms $\det(x \cdot \mathbb{E}_n - (a_{ij})_{ij}) \in \mathcal{O}[x]$. Weil $\mathcal{O}$ ganz abgeschlossen ist, folgt $\beta \in \mathcal{O}$, wegen $\mathfrak{p}^{-1} \not\subseteq \mathcal{O}$ erhalten wir den Widerspruch. □

Wir haben somit Satz 2.9 gezeigt.

Beweis von Satz 2.7. Existenz der Primzerlegung: Sei $\mathfrak{M}$ die Menge aller Ideale $\mathfrak{a} \neq (0), (1)$, die keine Primzerlegung besitzen. Sei $\mathfrak{a} \in \mathfrak{M}$ maximal bezüglich der Inklusion. Es gibt ein maximales Ideal $\mathfrak{p}$, so daß

$$\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}.$$

Es ist $\mathfrak{a} \neq \mathfrak{a}\mathfrak{p}^{-1}$ und $\mathfrak{p} \neq \mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$. Wegen der Maximalität von $\mathfrak{a}$ in $\mathfrak{M}$ besitzt $\mathfrak{a}\mathfrak{p}^{-1}$ eine Primzerlegung $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$, also auch $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p} \cdot \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$, also $\mathfrak{a} \notin \mathfrak{M}$.

Eindeutigkeit: Seien nun

$$\mathfrak{a} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r = \mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_s \tag{2.14.1}$$

zwei Primzerlegungen von $\mathfrak{a}$. Dann teilt $\mathfrak{p}_1$ einen Faktor $\mathfrak{q}_i$ der rechten Seite, da $\mathfrak{p}_1 \supset \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r = \mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_s$ (Wdh.: $\mathfrak{p}$ ist ein Primideal g.d.w. aus $\mathfrak{p} \supseteq \mathfrak{a}\mathfrak{b}$ folgt $\mathfrak{p} \supseteq \mathfrak{a}$ oder $\mathfrak{p} \supseteq \mathfrak{b}$, d.h. $\mathfrak{p} \mid \mathfrak{a}\mathfrak{b} \Rightarrow \mathfrak{p} \mid \mathfrak{a}$ oder $\mathfrak{p} \mid \mathfrak{b}$.). Ist etwa $\mathfrak{p}_1$ ein Teiler von $\mathfrak{q}_1$, dann folgt aus der Maximalität der Primideale sogar $\mathfrak{p}_1 = \mathfrak{q}_1$. Wir multiplizieren die Gleichung (2.14.1) mit $\mathfrak{p}_1^{-1}$ und weil $\mathfrak{p}_1\mathfrak{p}_1^{-1} = \mathcal{O}$ ist, erhalten wir

$$\mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r = \mathfrak{q}_2 \cdot \ldots \cdot \mathfrak{q}_s\ .$$

So fortfahrend erhalten wir $r = s$ und nach Vertauschen der Indizes $\mathfrak{p}_i = \mathfrak{q}_i$, $i = 1, \ldots, r$. □

Mit ein bißchen mehr Mühe hätten wir folgenden Satz beweisen können:

2.15. Satz. *Sei $\mathcal{O}$ ein Integritätsbereich mit Quotientenkörper K. Dann ist äquivalent:*

(a) *$\mathcal{O}$ ist Dedekindring.*

(b) *Jedes von Null verschiedene Ideal von $\mathcal{O}$ besitzt eine eindeutige Zerlegung als Produkt von Primidealen.*

(c) *Jedes von Null verschiedene Ideal ist das Produkt von Primidealen.*

(d) *Die Menge der von Null verschiedenen gebrochenen Ideale von K ist eine multiplikative Gruppe.*

Beweis. siehe P. Ribenboim, Classical theory of algebraic numbers. □

2.16. Proposition. *Sei $\mathcal{O}$ ein Dedekindring dann gilt:*

(i) Sei $\mathfrak{a} \subseteq \mathcal{O}$ ein Ideal und $\alpha \in \mathfrak{a}$. Dann existiert ein $\alpha' \in \mathfrak{a}$, sodaß gilt: $\mathfrak{a} = (\alpha, \alpha') = (\alpha) + (\alpha')$.

(ii) Sei $0 \neq \mathfrak{a} \subset \mathcal{O}$, dann gibt es in jeder Idealklasse von Cl_K ein ganzes zu $\mathfrak{a}$ teilerfremdes Ideal.

(iii) Besitzt $\mathcal{O}$ nur endlich viele Primideale, dann ist $\mathcal{O}$ ein Hauptidealring.

Beweis. Übung. (Tip: Swinnerton-Dyer, Ribenboim) □

Im Folgenden werden wir einen Beweis zur Endlichkeit der Klassenzahl von algebraischen Zahlkörpern vorstellen.

3 die Endlichkeit der Klassenzahl

Wir geben hier einen elementaren Beweis zur Endlichkeit der Klassenzahl. In Kapitel 12 werden wir einen kurzen ßtrukturellen"Beweis geben. **3.1.** Sei K algebraischer Zahlkörper mit $[K : \mathbb{Q}] = n$. Weiter sei $\mathfrak{B} = \{\beta_1, \ldots, \beta_n\}$ eine $\mathbb{Z}$-Basis für $\mathcal{O}_K$. Eine Norm $\|\cdot\|_{\mathfrak{B}} : K \to \mathbb{Q}_{\geq 0}$ ist bezüglich dieser Basis dann gegeben durch

$$\|\alpha\|_{\mathfrak{B}} = \sum_{j=1}^{n} |a_j|,$$

wobei $\alpha = a_1\beta_1 + \ldots + a_n\beta_n \in K$ mit $\alpha_n \in \mathbb{Q}$. Sind α, $\gamma = c_1\beta_1 + \ldots + c_n\beta_n \in \mathcal{O}_K$, dann gilt

$$\|\alpha\gamma\|_{\mathfrak{B}} = \Big\| \sum\sum a_i c_j \beta_i \beta_j \Big\|_{\mathfrak{B}} \leq \sum\sum |a_i c_j| \|\beta_i\beta_j\|_{\mathfrak{B}} \leq C_{\mathfrak{B}} \cdot \|\alpha\|_{\mathfrak{B}} \|\gamma\|_{\mathfrak{B}},$$

mit $C_{\mathfrak{B}} = \max_{i,j} \|\beta_i\beta_j\|_{\mathfrak{B}}$. Wir bemerken, daß $\|\cdot\|_{\mathfrak{B}} : \mathcal{O}_K \to \mathbb{N}$ eine *Höhenfunktion* auf $\mathcal{O}_K$ ist, d.h. es gibt nur endlich viele $\alpha \in \mathcal{O}_K$ mit $\|\alpha\|_{\mathfrak{B}} < \kappa$ für jede positive reelle Zahl κ.

3.2. Lemma. *Sei $\mathfrak{a} \subset K$ ein gebrochenes Ideal und $\alpha \in \mathfrak{a}$, $\alpha \neq 0$, ein Element mit minimaler Norm. Dann gilt: Zu jedem $\beta \in \mathfrak{a}$ existieren $\gamma \in \mathcal{O}_K$ und $m \in \mathbb{Z}$ derart, daß*

$$\left\| \frac{m\beta}{\alpha} - \gamma \right\|_{\mathfrak{B}} \leq (C_{\mathfrak{B}} + 1)^{-1} \text{ und } 0 < m \leq M_{\mathfrak{B}},$$

wobei $M_{\mathfrak{B}} = (n(C_{\mathfrak{B}} + 1))^n + 1$ ist.

Beweis. O.B.d.A. ist $\mathfrak{a}$ ein ganzes Ideal, denn die Multiplikation von $\mathfrak{a}$, und somit auch β mit einer ganzen Zahl läßt die Aussage des Lemmas invariant. Ebenfalls ist die Existenz eines Elements α mit minimaler Norm gesichert. Zu gegebenen $m \in \mathbb{N}$ finden wir $\gamma_m \in \mathcal{O}_K$, so daß

$$\frac{m\beta}{\alpha} - \gamma_m = c_1^{(m)}\beta_1 + \ldots + c_n^{(m)}\beta_n$$

mit $0 \leq c_j^{(m)} < 1$ für alle $c_j^{(m)}$. Somit bestimmt γ_m einen Punkt $P_m = (c_1^{(m)}, \ldots, c_n^{(n)})$ im Einheitswürfel bezüglich $\|\cdot\|_{\mathfrak{B}}$. Vermöge der Ungleichungen

$$\frac{r_j}{n(c+1)} \leq c_j < \frac{r_j+1}{n\cdot(c+1)}, \quad \begin{array}{l} 0 \leq r_j < n(c+1) \\ j = 1, \ldots, n \end{array},$$

zerlegen wir den Einheitswürfel in $(n\cdot(C_{\mathfrak{B}}+1))^n = M_{\mathfrak{B}} - 1$ Unterwürfel. Es müssen mindestens zwei der Punkte $P_1, \ldots, P_m$ im gleichen Unterwürfel liegen ("Dirichlet'sches Schubfachprinzip"). Seien P_{m_1} und P_{m_2} mit $m_1 < m_2$ zwei solcher Punkte. Wir setzen $m = m_2 - m_1$ und $\gamma = \gamma_{m_2} - \gamma_{m_1}$ und erhalten

$$\begin{aligned} \left\| \frac{m\beta}{\alpha} - \gamma \right\|_{\mathfrak{B}} &= \left\| \frac{m_2\beta}{\alpha} - \gamma_{m_2} - \left(\frac{m_1\beta}{\alpha} - \gamma_{m_1} \right) \right\|_{\mathfrak{B}} \\ &= \|P_{m_2} - P_{m_1}\|_{\mathfrak{B}} = \sum_{j=1}^{n} \mid c_j^{(m_2)} - c_j^{(m_1)} \mid \\ &\leq n \cdot \frac{1}{n\cdot(C_{\mathfrak{B}}+1)} = \frac{1}{(C_{\mathfrak{B}}+1)}. \end{aligned}$$

□

3.3. Satz. *Sei K ein algebraischer Zahlkörper, dann ist seine Idealklassengruppe Cl_K eine endliche Gruppe.*

Beweis: Seien $\mathfrak{a}, \alpha, \beta, \gamma, m$ wie in Lemma 3.2 gewählt. Dann ist

$$\|m\beta - \alpha\gamma\|_{\mathfrak{B}} \overset{2.17}{\leq} C_{\mathfrak{B}}\|\alpha\|_{\mathfrak{B}} \left\| \frac{m\beta}{\alpha} - \gamma \right\|_{\mathfrak{B}} \overset{2.18}{\leq} \frac{C_{\mathfrak{B}}}{C_{\mathfrak{B}}+1}\|\alpha\|_{\mathfrak{B}} < \|\alpha\|_{\mathfrak{B}}.$$

Da $m\beta - \gamma \in \mathfrak{a}$, folgt aus der Minimalität von α, daß $m\beta$ für jedes $\beta \in \mathfrak{a}$ ein Vielfaches von α ist. Insbesondere gilt dann auch $(M_{\mathfrak{B}}!\beta) \subset (\alpha)$. Setze $\mathfrak{a}_1 = (M_{\mathfrak{B}}!)\cdot\mathfrak{a}\cdot(\alpha^{-1})$. Beachte: $\mathfrak{a}_1$ ist ein ganzes Ideal in der Klasse von $\mathfrak{a}$. Da $\alpha \in \mathfrak{a}$, enthält $\mathfrak{a}_1$ das Ideal $(M_{\mathfrak{B}}!)$. Deswegen muß $\mathfrak{a}_1$ die Vereinigung endllich vieler Nebenklassen von $(M_{\mathfrak{B}}!)$ in $\mathcal{O}_K$ sein. Insbesondere gibt es nur endlich viele Möglichkeiten für $\mathfrak{a}_1$. □

Bemerkung. Für praktische Untersuchungen ist die im Beweis verwendete Abschätzung viel zu grob.

4 Lokalisierung, diskrete Bewertungsringe

4.1. Sei A ein Integritätsbereich und K sein Quotientenkörper, d.h.,

$$K = \left\{ \frac{a}{b} \,\middle|\, a \in A,\, b \in A \setminus \{0\} \right\}.$$

Wenn wir anstelle von $A\setminus\{0\}$, eine andere multiplikativ abgeschlossene Menge $S\subset A\setminus\{0\}$ wählen, dann stellt man leicht fest, daß

$$AS^{-1}=\left\{\frac{a}{b}\,\middle|\,a\in A,\,b\in S\right\}$$

ebenfalls ein Integritätsbereich ist.

4.2. Satz. *Die Zuordnungen $\mathfrak{q}\mapsto\mathfrak{q}S^{-1}$, für Primideale $\mathfrak{q}\subseteq A\setminus S$, und $\mathfrak{Q}\mapsto\mathfrak{Q}\cap A$, für Primideale $\mathfrak{Q}$ von AS^{-1}, sind zueinander inverse $1:1$-Korrespondenzen.*

Beweis. Ist $\mathfrak{q}\subset A\setminus S$ ein Primideal von A, so ist $\mathfrak{Q}=\mathfrak{q}S^{-1}=\left\{\frac{q}{s}|\,q\in\mathfrak{q},\,s\in S\right\}$ ein Primideal von AS^{-1}: Seien $\frac{a}{s},\frac{a'}{s'}\in AS^{-1}$ und $\frac{a}{s}\cdot\frac{a'}{s'}\in\mathfrak{Q}$, d.h. $\frac{aa'}{ss'}=\frac{q}{s''}$ für ein $q\in\mathfrak{q}$ und $s''\in S$. Somit ist $s''aa'=qss'\in\mathfrak{q}$. Weil nun $s''\notin\mathfrak{q}$ folgt $aa'\in\mathfrak{q}$ und somit, weil $ss'\notin\mathfrak{q}$, auch $\frac{a}{s}\in\mathfrak{Q}$ oder $\frac{a'}{s'}\in\mathfrak{Q}$. Es ist $\mathfrak{q}=\mathfrak{Q}\cap A$, weil aus $\frac{q}{s}=a\in\mathfrak{Q}\cap A$ folgt, daß $q=as\in\mathfrak{q}$. Also gilt wegen $s\notin\mathfrak{q}$ schließlich $a\in\mathfrak{q}$.

Ist nun umgekehrt $\mathfrak{Q}$ ein Primideal von AS^{-1}, dann ist offensichtlich $\mathfrak{q}=\mathfrak{Q}\cap A$ ein Primideal von A. Es gilt dann auch $\mathfrak{q}\subset A\setminus S$, denn gäbe es ein $s\in S$ mit $s\in\mathfrak{q}$, dann wäre $\frac{1}{1}=s\cdot\frac{1}{s}\in\mathfrak{Q}$ und somit wäre $\mathfrak{Q}=AS^{-1}$, also insbesondere kein Primideal. Es ist $\mathfrak{Q}=\mathfrak{q}S^{-1}$: Denn wenn $\frac{a}{s}\in\mathfrak{Q}$, so ist $a=\frac{a}{s}\cdot s\in\mathfrak{Q}\cap A=\mathfrak{q}$ und deshalb auch $\frac{a}{s}=a\cdot\frac{1}{s}\in\mathfrak{q}S^{-1}$. Die Zuordnungen $\mathfrak{q}\mapsto\mathfrak{q}S^{-1}$ und $\mathfrak{Q}\mapsto\mathfrak{Q}\cap A$ sind zueinander invers, womit der Satz bewiesen ist. □

4.3. Definition. Ist nun $S=A\setminus\mathfrak{p}$ für ein Primideal $\mathfrak{p}$, dann schreibt man $A_\mathfrak{p}$ anstelle von AS^{-1} und nennt $A_\mathfrak{p}$ die *Lokalisierung von A bei $\mathfrak{p}$*.

Anschaulich gesehen vergißt $A_\mathfrak{p}$ alle bis auf die auf $\mathfrak{p}$ bezogenen Eigenschaften von A. Es erweist sich oft als günstig, die Eigenschaften von A zuerst in den "einfacheren" Ringen $A_\mathfrak{p}$ zu untersuchen.

4.4. Korollar. *(i) Ist $\mathfrak{p}$ ein Primideal von A, so ist $A_\mathfrak{p}$ ein lokaler Ring, d.h. $A_\mathfrak{p}$ besitzt ein einziges maximales Ideal, nämlich $\mathfrak{m}_\mathfrak{p}=\mathfrak{p}A_\mathfrak{p}$.*

(ii) *Man hat eine kanonische Einbettung $A/\mathfrak{p}\hookrightarrow A_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$ durch die $A_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$ zum Quotientenkörper von $A/\mathfrak{p}$ wird.*

(iii) *Ist $\mathfrak{p}$ sogar ein maximales Ideal von A, so gilt $A/\mathfrak{p}^n\cong A_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}^n$ für alle $n\in\mathbb{N}$.*

Beweis. (i) Aufgrund von Satz 4.2 entsprechen die Ideale von $A_\mathfrak{p}$ umkehrbar eindeutig den in $\mathfrak{p}$ enthaltenen Idealen von A. Daher ist $\mathfrak{m}_\mathfrak{p}=\mathfrak{p}A_\mathfrak{p}$ das einzige maximale Ideal in $A_\mathfrak{p}$.

(ii) Es sei f der Homomorphismus

$$f:A/\mathfrak{p}^n\longrightarrow A_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}^n$$

gegeben durch $a\pmod{\mathfrak{p}^n}\mapsto\frac{a}{1}\pmod{\mathfrak{m}_\mathfrak{p}^n}$. Für $n=1$ ist f injektiv, wegen $\mathfrak{p}=\mathfrak{m}_\mathfrak{p}\cap A$. Deswegen ist $A_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$ der Quotientenkörper von $A/\mathfrak{p}$.

(iii) Es sei nun $\mathfrak{p}$ maximal und $n\geq 1$. Wir zeigen zuerst, daß für jedes $s\in A\setminus\mathfrak{p}$ gilt $\mathfrak{p}^n+sA=A$, d.h. $\overline{s}\equiv s\pmod{\mathfrak{p}^n}$ ist eine Einheit in $A/\mathfrak{p}^n$. Für $n=1$ ist die wegen der Maximalität von $\mathfrak{p}$ klar, denn $A/\mathfrak{p}$ ist ein Körper. Mittels Induktion zeigt man dann diese Behauptung für $n\geq 1$. Denn aus $\mathfrak{p}^n+sA=A$ folgt

$$\mathfrak{p}=\mathfrak{p}A=\mathfrak{p}\left(\mathfrak{p}^n+sA\right)\subsetneq\mathfrak{p}^{n+1}+sA,$$

woraus aufgrund der Maximalität von $\mathfrak{p}$ dann $\mathfrak{p}^{n+1} + sA = A$ folgt.

Der Homomorphismus f ist injektiv. Sei $a \in A$ mit $a \in \mathfrak{m}_\mathfrak{p}^n$, d.h. $a = \frac{b}{s}$ mit $b \in \mathfrak{p}^n$ und $s \notin \mathfrak{p}$. Somit ist $as = b \in \mathfrak{p}^n$ und deshalb $\overline{as} = 0$ in $A/\mathfrak{p}^n$. Weil aber $\overline{s} \neq 0$ folgt $\overline{a} = 0 \in A/\mathfrak{p}^n$.

Der Homomorphismus f ist surjektiv. Sei $\frac{a}{s} \in A_\mathfrak{p}$, wobei $a \in A$ und $s \notin \mathfrak{p}$. Dann gibt es nach Behauptung (ii) ein $a' \in A$ mit $a \equiv a's \pmod{\mathfrak{p}^n}$, so daß $\frac{a}{s} \equiv \frac{a'}{1} \pmod{\mathfrak{p}^n A_\mathfrak{p}}$, d.h. $\frac{a}{s} \pmod{\mathfrak{m}_\mathfrak{p}^n}$ liegt im Bild von f. □

4.5. In einem lokalen Ring mit maximalen Ideal $\mathfrak{m}$ gilt immer $A^* = A \setminus \mathfrak{m}$. Dies gilt weil für jedes $a \in A \setminus \mathfrak{m}$ das Hauptideal (a) in keinem anderen maximalen Ideal enthalten sein kann, also $(a) = A$ gelten muß.

4.6. Definition. Ein *diskreter Bewertungsring* ist ein Hauptidealring $\mathcal{O}$ mit einem einzigen maximalen Ideal $\mathfrak{p} \neq 0$.

Es folgt $\mathfrak{p} = (\pi) = \pi\mathcal{O}$ und $\pi \in \mathcal{O}$ ist aufgrund obiger Bemerkung 4.5 eindeutig bis auf eine Einheit. Jedes von Null verschiedene Element a aus $\mathcal{O}$ hat deshalb die Gestalt $a = u \cdot \pi^n$ wobei $u \in \mathcal{O}^*$ und $n \in \mathbb{N}$. Für die Elemente $a \in K^* = (\mathrm{Quot}(\mathcal{O}))^*$ gilt dann

$$a = u \cdot \pi^n$$

mit $u \in \mathcal{O}^*$ und $n \in \mathbb{Z}$. Der Exponent n obiger Darstellung von $a \in K^* = Quot(\mathcal{O})$ heißt die *Bewertung* von a und wird mit $v_\mathfrak{p}(a)$ bezeichnet. Man hat also $(a) = \mathfrak{p}^{v_\mathfrak{p}(a)}$ für alle $0 \neq a \in K$.

Man betrachtet die Bewertung als eine Funktion

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

die man üblicherweise vermöge $\nu_\mathfrak{p}(0) = \infty$ auf ganz K fortsetzt. Sie erfüllt dann folgende Identitäten:

$$v_\mathfrak{p}(ab) = v_\mathfrak{p}(a) + v_\mathfrak{p}(b), \quad v_\mathfrak{p}(a+b) \geq \min(v_\mathfrak{p}(a), v_\mathfrak{p}(b)).$$

4.7. Proposition. *Ist $\mathcal{O}$ ein Integritätsbereich, dann gilt*

$$\mathcal{O} = \bigcap_{\mathfrak{p} \in \operatorname{Spec}\mathcal{O}} \mathcal{O}_\mathfrak{p},$$

wobei $\operatorname{Spec}\mathcal{O}$ *die Menge aller Primideale von $\mathcal{O}$ bezeichnet.*

Beweis. Sei $\frac{a}{b} \in \bigcap_{\mathfrak{p} \in \operatorname{Spec}\mathcal{O}} \mathcal{O}_\mathfrak{p}$ mit a, $b \in \mathcal{O}$, dann ist $\mathfrak{a} = \{x \in \mathcal{O} \mid xa \in b\mathcal{O}\}$ ein Ideal, das in keinem Primideal von $\mathcal{O}$ enthalten sein kann: Für alle $\frac{a}{b}$ und alle Primideale $\mathfrak{p}$ gibt es eine Darstellung der Gestalt $\frac{a}{b} = \frac{c}{s}$ mit $c \in \mathcal{O}$ und $s \in \mathcal{O} \setminus \mathfrak{p}$. Es ist $sa = bc$ und daher gilt sogar $s \in \mathfrak{a} \setminus \mathfrak{p}$. Da $\mathfrak{a}$ in keinem maximalen Ideal liegt, folgt $\mathfrak{a} = \mathcal{O}$, also auch $a = 1 \cdot a \in b\mathcal{O}$, d.h. $\frac{a}{b} \in \mathcal{O}$. □

4.8. Satz. *Ist $\mathcal{O}$ ein Dedekindring und $S \subseteq \mathcal{O} \setminus \{0\}$ eine multiplikativ abgeschlossene Teilmenge, so ist auch $\mathcal{O}S^{-1}$ ein Dedekindring.*

Beweis. Wir zeigen zuerst, daß $\mathcal{O}S^{-1}$ noethersch ist. Sei $\mathfrak{A}$ ein Ideal von $\mathcal{O}S^{-1}$ und setze $\mathfrak{a} = \mathfrak{A} \cap \mathcal{O}$. Dann ist $\mathfrak{A} = \mathfrak{a}S^{-1}$, denn falls $\frac{a}{s} \in \mathfrak{A}$ mit $a \in \mathcal{O}$ und $s \in S$, so ist $a = s \cdot \frac{a}{s} \in \mathfrak{A} \cap \mathcal{O} = \mathfrak{a}$, also $\frac{a}{s} = a \cdot \frac{1}{s} \in \mathfrak{a}S^{-1}$. Mit $\mathfrak{a}$ ist daher auch $\mathfrak{A}$ endlich erzeugt.

Analog dem Beweis von Satz 4.2 zeigt man, daß jedes Primideal von $\mathcal{O}S^{-1}$ maximal ist, weil dies auch für jedes Primideal von $\mathcal{O}$ gilt.

Der Ring $\mathcal{O}S^{-1}$ ist ganzabgeschlossen. Denn wenn $x \in K = \mathrm{Quot}(\mathcal{O})$ der Gleichung

$$x^n + \frac{a_1}{s_1}x^{n-1} + \ldots + \frac{a_n}{s_n} = 0$$

mit Koeffizienten $\frac{a_i}{s_i} \in \mathcal{O}S^{-1}$ genügt, dann ist mit $s = s_1 \cdot \ldots \cdot s_n$ das Element $sx \in K$ ganz über $\mathcal{O}$. Weil $\mathcal{O}$ ganzabgeschlossen ist, ist $xs \in \mathcal{O}$, somit $x = xss^{-1} \in \mathcal{O}S^{-1}$. Also ist $\mathcal{O}S^{-1}$ ganzabgeschlossen. □

4.9. Satz. *Sei $\mathcal{O}$ ein noetherscher Integritätsbereich. $\mathcal{O}$ ist ein Dedekindring genau dann wenn die Lokalisierungen $\mathcal{O}_\mathfrak{p}$ für alle Primideale $\mathfrak{p} \neq 0$ diskrete Bewertungsringe sind.*

Beweis. Ist $\mathcal{O}$ ein Dedekindring, so sind es auch die Lokalisierungen $\mathcal{O}_\mathfrak{p}$ für alle Primideale $\mathfrak{p} \neq 0$. Das maximale Ideal $\mathfrak{m}_\mathfrak{p} = \mathfrak{p}\mathcal{O}_\mathfrak{p}$ ist das einzige Primideal von $\mathcal{O}_\mathfrak{p}$. Wählt man ein $\pi \in \mathfrak{m}_\mathfrak{p} \setminus \mathfrak{m}_\mathfrak{p}^2$, so muß daher $(\pi) = \mathfrak{m}_\mathfrak{p}$ und ferner auch $(\pi^n) = \mathfrak{m}_\mathfrak{p}^n$ gelten. Daher ist $\mathcal{O}_\mathfrak{p}$ ein Hauptidealring, also ein diskreter Bewertungsring.

Sind nun umgekehrt alle $\mathcal{O}_\mathfrak{p}$ diskrete Bewertungsringe, so sind sie als Hauptidealringe ganzabgeschlossen (faktorielle Ringe sind ganzabgeschlossen). Somit ist auch $\mathcal{O} = \bigcap_{\mathfrak{p} \in \mathrm{Spec}\,\mathcal{O}} \mathcal{O}_\mathfrak{p}$ ganzabgeschlossen. Wegen $\mathfrak{p} = \mathfrak{m}_\mathfrak{p} \cap \mathcal{O}_\mathfrak{p}$ ist jedes Primideal $\mathfrak{p}$ von $\mathcal{O}$ maximal, weil dies für $\mathcal{O}_\mathfrak{p}$ gilt. Laut Voraussetzung ist $\mathcal{O}$ noethersch, deswegen ist $\mathcal{O}$ sogar ein Dedekindring. □

4.10. Sei $\mathfrak{a} \subseteq \mathcal{O}$ ein Ideal in einem Integritätsbereich, dann nennt man $\mathfrak{a}_\mathfrak{p} = \mathfrak{a}\mathcal{O}_\mathfrak{p}$ die $\mathfrak{p}$-Komponente von $\mathfrak{a}$. Falls $\mathfrak{b} \subseteq \mathcal{O}$ ein weiteres Ideal ist, dann gilt $(\mathfrak{ab})_\mathfrak{p} = \mathfrak{a}_\mathfrak{p}\mathfrak{b}_\mathfrak{p}$. Es ist $\mathfrak{a} \subseteq \mathfrak{b}$ genau dann wenn $\mathfrak{a}_\mathfrak{p} \subseteq \mathfrak{b}_\mathfrak{p}$ für alle $\mathfrak{p}$. Ferner ist $\mathfrak{a} = \mathfrak{b}$ falls $\mathfrak{a}_\mathfrak{p} = \mathfrak{b}_\mathfrak{p}$ für alle $\mathfrak{p}$.

4.11. Satz. *Ist $\mathcal{O}$ ein Dedekindring, dann gilt:*

(i) $(\mathfrak{a}^{-1})_\mathfrak{p} = (\mathfrak{a}_\mathfrak{p})^{-1}$.

(ii) Für fast alle $\mathfrak{p}$ gilt $\mathfrak{a}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$.

(iii) Jedes Ideal ist der Durchschnitt seiner $\mathfrak{p}$-Komponenten, d.h. $\mathfrak{a} = \bigcap_{\mathfrak{p} \in \mathrm{Spec}\,\mathcal{O}} \mathfrak{a}_\mathfrak{p}$.

(iv) Ist für alle $\mathfrak{p}$ ein Ideal $\mathfrak{a}_\mathfrak{p} \subseteq \mathcal{O}_\mathfrak{p}$ so gegeben, daß fast alle $\mathfrak{a}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$, dann ist $\mathfrak{a} = \bigcap_{\mathfrak{p} \in \mathrm{Spec}\,\mathcal{O}} \mathfrak{a}_\mathfrak{p}$ ein Ideal von $\mathcal{O}$ und $\left(\bigcap_{\mathfrak{p} \in \mathrm{Spec}\,\mathcal{O}} \mathfrak{a}_\mathfrak{p}\right)_\mathfrak{p} = \mathfrak{a}_\mathfrak{p}$.

Beweis. (i) klar.

(ii) Seien $a_1, \ldots, a_r \in K$ ein Erzeugendensystem von $\mathfrak{a}$. Es genügt zu zeigen für $a \in K^*$ gilt $(a)_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$ für fast alle $\mathfrak{p}$. Mittels der Primidealzerlegung von (a) erhalten wir $(a)_\mathfrak{p} = (\mathfrak{q}_1^{e_1} \cdot \ldots \cdot \mathfrak{q}_r^{e_r})_\mathfrak{p} = (\mathfrak{q}_1^{e_1})_\mathfrak{p} \cdot \ldots \cdot (\mathfrak{q}_r^{e_r})_\mathfrak{p}$. Da aber für jedes $\mathfrak{q}_i \neq \mathfrak{p}$ und $S = \mathcal{O} \setminus \mathfrak{p}$ gilt, daß $(\mathfrak{q}_1^{e_1})_\mathfrak{p} = \mathfrak{q}_1^{e_1}S^{-1} = \mathcal{O}_\mathfrak{p}$ ist, folgt die Behauptung.

(iii) Für zwei Ideale $\mathfrak{a}$, $\mathfrak{b}$ gilt

$$\mathfrak{a} \bigcap_{\mathfrak{p}\in\operatorname{Spec}\mathcal{O}} \mathfrak{b}_\mathfrak{p} \subseteq \bigcap_{\mathfrak{p}\in\operatorname{Spec}\mathcal{O}} \mathfrak{a}\mathfrak{b}_\mathfrak{p} = \bigcap_{\mathfrak{p}\in\operatorname{Spec}\mathcal{O}} \mathfrak{a}_\mathfrak{p}\mathfrak{b}_\mathfrak{p}. \tag{4.11.1}$$

Ersetzt man in dieser Formel $\mathfrak{a}$ durch $\mathfrak{a}^{-1}$ und $\mathfrak{b}$ durch $\mathfrak{a}\mathfrak{b}$ so wird mit (i)

$$\bigcap_{\mathfrak{p}\in\operatorname{Spec}\mathcal{O}} \mathfrak{b}_\mathfrak{p} = \bigcap_{\mathfrak{p}\in\operatorname{Spec}\mathcal{O}} \mathfrak{a}_\mathfrak{p}^{-1}\mathfrak{a}_\mathfrak{p}\mathfrak{b}_\mathfrak{p} = \bigcap_{\mathfrak{p}\in\operatorname{Spec}\mathcal{O}} \mathfrak{a}^{-1}\mathfrak{a}_\mathfrak{p}\mathfrak{b}_\mathfrak{p} \supseteq \mathfrak{a}^{-1} \bigcap_{\mathfrak{p}\in\operatorname{Spec}\mathcal{O}} \mathfrak{a}_\mathfrak{p}\mathfrak{b}_\mathfrak{p} = \mathfrak{a}^{-1} \bigcap_{\mathfrak{p}\in\operatorname{Spec}\mathcal{O}} \mathfrak{a}\mathfrak{b}_\mathfrak{p}.$$

Multiplikation mit $\mathfrak{a}$ liefert wegen (4.11.1)

$$\mathfrak{a}\left(\bigcap_{\mathfrak{p}\in\operatorname{Spec}\mathcal{O}} \mathfrak{b}_\mathfrak{p}\right) = \bigcap_{\mathfrak{p}\in\operatorname{Spec}\mathcal{O}} \mathfrak{a}\mathfrak{b}_\mathfrak{p} = \bigcap_{\mathfrak{p}\in\operatorname{Spec}\mathcal{O}} \mathfrak{a}_\mathfrak{p}\mathfrak{b}_\mathfrak{p}.$$

Setzt man in der letzten Formel $\mathfrak{b} = \mathcal{O}$, so folgt $\mathfrak{a} = \bigcap_{\mathfrak{p}\in\operatorname{Spec}\mathcal{O}} \mathfrak{a}_\mathfrak{p}$.
(iv) Es ist $\mathfrak{a} = \bigcap_{\mathfrak{p}\in\operatorname{Spec}\mathcal{O}} \mathfrak{a}_\mathfrak{p} \in K$ ein gebrochenes Ideal, da $\mathcal{O}\cdot\bigcap_{\mathfrak{p}\in\operatorname{Spec}\mathcal{O}} \mathfrak{a}_\mathfrak{p} = \bigcap_{\mathfrak{p}\in\operatorname{Spec}\mathcal{O}} \mathfrak{a}_\mathfrak{p} = \mathfrak{a}$. Da $\mathfrak{a} = \bigcap_{\mathfrak{p}\in\operatorname{Spec}\mathcal{O}} \mathfrak{a}_\mathfrak{p} \subseteq \bigcap_{\mathfrak{p}\in\operatorname{Spec}\mathcal{O}} \mathcal{O}_\mathfrak{p} = \mathcal{O}$ ist $\mathfrak{a}$ sogar ein ganzes Ideal. Weil $\mathfrak{a}_\mathfrak{q}\mathcal{O}_\mathfrak{p} = K$ für $\mathfrak{q} \neq \mathfrak{p}$ ist, folgt $\mathfrak{a}\mathcal{O}_\mathfrak{p} = \mathfrak{a}_\mathfrak{p} \cap K = \mathfrak{a}_\mathfrak{p}$ wie behauptet war. □

5 Erweiterungen von Dedekindringen, Verzweigungstheorie

5.1. Motivation. Sei K ein algebraischer Zahlkörper $\mathcal{O}_K$ sein Ring der ganzen Zahlen. Dann war für jedes Primideal $\mathfrak{p} \in \mathcal{O}_K$ die Menge $\mathfrak{p}\cap\mathbb{Z} = (p)$ ein Primideal in $\mathbb{Z}$, d.h., $p\mathcal{O}_K \subseteq \mathfrak{p}$. Was ist die Primidealzerlegung von (p) in $\mathcal{O}_K$? Die Verzweigungstheorie untersucht die Primidealzerlegung von Primidealen von Erweiterungen von Dedekindringen.

5.2. Satz. *Sei o ein Dedekindring mit Quotientenkörper $K, L|K$ eine endliche separable Erweiterung und $\mathcal{O}$ der ganze Abschluß von o in L. Dann ist $\mathcal{O}$ ebenfalls ein Dedekindring.*

Beweis. Als ganzer Abschluß von o ist $\mathcal{O}$ auch ganz abgeschlossen.

Die Maximalität der Primideale $\mathfrak{P} \neq 0$ beweist man analog zum Beweis dafür, daß der Ring der ganzen Zahlen ein Dedekindring ist. Man sieht daß $\mathfrak{p} = \mathfrak{P} \cap o$ ein von Null verschiedenes Primideal ist. Deswegen ist der Integritätsbereich $\mathcal{O}/\mathfrak{P}$ eine Erweiterung des Körpers $o/\mathfrak{p}$ und damit selbst ein Körper.

Es bleibt zu zeigen, daß $\mathcal{O}$ noethersch ist. Dazu sei $\alpha_1, \ldots, \alpha_n$ eine in $\mathcal{O}$ gelegene Basis von $L|K$ mit Diskriminante $d = \operatorname{discr}(\alpha_1, \ldots, \alpha_n)$. Es gilt $d \neq 0$ und $\mathcal{O} \subseteq o\frac{\alpha_1}{d} + \ldots + o\frac{\alpha_n}{d}$. Jedes Ideal von $\mathcal{O}$ ist ebenfalls in diesem endlich erzeugten o-Modul enthalten, ist also erst recht ein endlich erzeugter o-Modul. □

5.3. Bemerkung. Satz 5.2 gilt auch ohne die Annahme der Separabilität (siehe [Ne], I.12.8). Im folgenden seien o, K, $\mathcal{O}$ und L wie im Satz 5.2 gewählt.

5.4. Lemma. *Für ein Primideal $0 \neq \mathfrak{p} \subset \mathfrak{o}$ gilt stets $\mathfrak{p}\mathcal{O} \neq \mathcal{O}$.*

Beweis. Sei $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$, so daß $\pi\mathfrak{o} = \mathfrak{p} \cdot \mathfrak{a}$ mit $\mathfrak{p} \nmid \mathfrak{a}$, d.h. $\mathfrak{p} + \mathfrak{a} = \mathfrak{o}$. Es gibt also ein $s \in \mathfrak{a}$ mit $s \notin \mathfrak{p}$, so daß $s\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{a} = \pi\mathfrak{o}$. Gälte nun $\mathfrak{p}\mathcal{O} = \mathcal{O}$, dann folgte $s\mathcal{O} = s\mathfrak{p}\mathcal{O} \subseteq \pi\mathcal{O}$, also $s = \pi x$ mit $x \in \mathcal{O} \cap K = \mathfrak{o}$, d.h. $s \in \mathfrak{p}$. □

5.5. Bemerkung. Es gilt sogar $\mathfrak{a}\mathcal{O} \cap K = \mathfrak{a}$, für alle Ideale $\mathfrak{a}$ von $\mathfrak{o}$ (siehe 5.18).

5.6. Definition. Sei $\mathfrak{p}$ ein Primideal aus $\mathfrak{o}$. Weil $\mathcal{O}$ ein Dedekindring ist, zerfällt $\mathfrak{p}\mathcal{O}$ eindeutig in Primideale, d.h. es gibt Primideale $\mathfrak{P}_i \subset \mathcal{O}$ so daß

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_r^{e_r}. \tag{5.6.1}$$

Man nennt e_i den *Verzweigungsindex* (engl.: ramification index) und der Körpergrad $f_i = [\mathcal{O}/\mathfrak{P}_i : \mathfrak{o}/\mathfrak{p}]$ heißt der *Trägheitsgrad* (engl.: inertia degree) von $\mathfrak{P}_i$ über $\mathfrak{p}$.

5.7. Satz. *Ist $L|K$ separabel mit $n = [L : K]$, dann erfüllen die Exponenten in der Zerlegung* (5.6.1) *die fundamentale Gleichung*

$$\sum_{i=1}^{r} e_i f_i = n.$$

Beweis. Wir haben $\mathcal{O}/\mathfrak{p}\mathcal{O} \cong \bigoplus_{i=1}^{r} \mathcal{O}/\mathfrak{P}_i^{e_i}$ (chinesischer Restsatz). Da $\mathcal{O}/\mathfrak{p}\mathcal{O}$ und alle $\mathcal{O}/\mathfrak{P}_i^{e_i}$ Vektorräume über dem Körper $\mathbb{F}_\mathfrak{p} = \mathfrak{o}/\mathfrak{p}$ sind, folgt die Behauptung aus den Formeln

$$\begin{aligned} \dim_{\mathbb{F}_\mathfrak{p}}(\mathcal{O}/\mathfrak{p}\mathcal{O}) &= n, && (*) \\ \dim_{\mathbb{F}_\mathfrak{p}}(\mathcal{O}/\mathfrak{P}_i^{e_i}) &= e_i f_i. && (**) \end{aligned}$$

Zum Beweis der Gleichung $(*)$, seien $\omega_1, \ldots, \omega_m \in \mathcal{O}$ Repräsentanten einer Basis $\overline{\omega}_1, \ldots, \overline{\omega}_m$ von $\mathcal{O}/\mathfrak{p}\mathcal{O}$. Es ist $m < \infty$, da $\mathcal{O}$ ein endlich erzeugter $\mathfrak{o}$-Modul ist. Wir zeigen, daß $\omega_1, \ldots, \omega_m$ eine Basis von $L|K$ ist. Angenommen die $\omega_1, \ldots, \omega_m$ sind linear abhängig über K. Dann gäbe es $a_1, \ldots, a_m \in K$ mit

$$a_1 w_1 + \ldots + a_m w_m = 0.$$

Sei $\mathfrak{a} = (a_1, \ldots, a_m) \subseteq K$ und wähle $a \in \mathfrak{a}^{-1}$ mit $a \notin \mathfrak{a}^{-1}\mathfrak{p}$, d.h. $a\mathfrak{a} \not\subseteq \mathfrak{p}$. Dann liegen alle $aa_1, \ldots, aa_m$ in $\mathfrak{o}$, aber nicht alle in $\mathfrak{p}$. Aus

$$aa_1 w_1 + \ldots + aa_m w_m \equiv 0 \pmod{\mathfrak{p}}$$

folgt eine lineare Abhängigkeit der $\overline{\omega}_i$ über $\mathbb{F}_\mathfrak{p}$, somit ein Widerspruch. Also sind $\omega_1, \ldots, \omega_m$ linear unabhängig. Wir betrachten nun $\mathfrak{o}$-Moduln $M = \mathfrak{o}\omega_1 + \ldots + \mathfrak{o}\omega_m$ und $N = \mathcal{O}/M$. Wegen $\mathcal{O} = M + \mathfrak{p}\mathcal{O}$ gilt $\mathfrak{p}N = N$. Da $L|K$ separabel ist, so ist $\mathcal{O}$ und damit auch N ein endlich erzeugter $\mathfrak{o}$-Modul. Für ein Erzeugendensystem $\alpha_1, \ldots, \alpha_s$ von N gilt dann

$$\alpha_j = \sum_i a_{ij}\alpha_i \quad \text{mit } a_{ij} \in \mathfrak{p}.$$

Setze $A = (a_{ij}) - \mathbb{E}_s$ und $B = A^*$, d.h. $B \cdot A = d \cdot \mathbb{E}_s$ mit $d = \det(A)$. Da $A \cdot (\alpha_1, \ldots, \alpha_s)^t = 0$ folgt

$$0 = B \cdot A(\alpha_1, \ldots, \alpha_s)^t = (d\alpha_1, \ldots, d\alpha_s)^t$$

und somit $dN = 0$, d.h. $d\mathcal{O} \subseteq M = \mathfrak{o}\omega_1, + \ldots + \mathfrak{o}\omega_m$. Es ist $d = 0$, da $\det(A) \equiv \det(-\mathbb{E}_s) \equiv (-1)^s \mod \mathfrak{p}$. Weil $L = dL$ ergibt sich $L = K\omega_1 + \ldots + K\omega_m$. Also ist $\omega_1, \ldots, \omega_m$ eine Basis von L/K, d.h. $m = n$.

Zum Beweis der Gleichung $(**)$ betrachten wir die absteigende Kette

$$\mathcal{O}/\mathfrak{P}_i^{e_i} \supseteq \mathfrak{P}_i/\mathfrak{P}_i^{e_i} \supseteq \ldots \supseteq \mathfrak{P}_i^{e_i-1}/\mathfrak{P}_i^{e_i} \supseteq (0)$$

von $\mathbb{F}_\mathfrak{p}$-Vektorräumen. Die Quotienten $\mathfrak{P}_i^\nu/\mathfrak{P}_i^{\nu+1}$ dieser Kette sind isomorph zu $\mathcal{O}/\mathfrak{P}_i$. Denn falls $\alpha \in \mathfrak{P}_i^\nu \setminus \mathfrak{P}_i^{\nu+1}$ ist, hat der Homomorphismus $\mathcal{O} \to \mathfrak{P}_i^\nu/\mathfrak{P}_i^{\nu+1}$ gegeben durch $a \mapsto a\alpha$ den Kern $\mathfrak{P}_i^{\nu+1}$. Er ist surjektiv, weil $\mathfrak{P}_i^\nu = \mathrm{ggT}\left(\mathfrak{P}_i^{\nu+1}, (\alpha)\right)$, d.h. $\mathfrak{P}_i^\nu = \alpha\mathcal{O} + \mathfrak{P}_i^{\nu+1}$. Weil $f_i = [\mathcal{O}/\mathfrak{P}_i : \mathbb{F}_\mathfrak{p}]$ gilt $\dim_{\mathbb{F}_\mathfrak{p}}\left(\mathfrak{P}_i^\nu/\mathfrak{P}_i^{\nu+1}\right) = f_i$ und weil obige Kette die Länge e_i hat folgt:

$$\dim_{\mathbb{F}_\mathfrak{p}}(\mathcal{O}/\mathfrak{P}_i^{e_i}) = \sum_{\nu=0}^{e_i-1} \dim_{\mathbb{F}_\mathfrak{p}}\left(\mathfrak{P}_i^\nu/\mathfrak{P}_i^{\nu+1}\right) = e_i f_i.$$

□

5.8. Definition. (Es gelten die Bezeichnungen von Definition 5.6) Das Primideal $\mathfrak{p}$ heißt *voll zerlegt*, falls alle $e_i = f_i = 1$. $\mathfrak{p}$ heißt *unzerlegt*, falls gleichzeitig $r = 1$. Das Primideal $\mathfrak{P}_i$ in der Zerlegung $\mathfrak{p} = \prod \mathfrak{P}_i^{e_i}$ heißt unverzweigt über $\mathfrak{o}$, wenn $e_i = 1$ und $\mathcal{O}/\mathfrak{P}_i \mid \mathfrak{o}/\mathfrak{p}$ ein separable Erweiterung ist. Sonst heißt es *verzweigt*. Man sagt es sei *rein verzweigt*, falls zusätzlich noch $f_i = 1$ ist. Das Primideal $\mathfrak{p}$ heißt *unverzweigt*, falls alle $\mathfrak{P}_i$ unverzweigt sind, sonst verzweigt. Die Erweiterung $L|K$ heißt *unverzweigte Erweiterung*, falls alle Primideale $\mathfrak{p}$ von K in L unverzweigt sind.

5.9. Übung. Zeige, daß für ein quadratfreies a und für Primzahlen p mit $(p, 2a) = 1$ gilt:

$$(p) \text{ ist voll zerlegt in } \mathbb{Q}(\sqrt{a}) \Leftrightarrow \left(\frac{a}{p}\right) = 1,$$

wobei $\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{falls } x^2 = a \pmod p \text{ eine Lösung hat,} \\ -1, & \text{falls } x^2 = a \pmod p \text{ keine Lösung hat.} \end{cases}$.

5.10. Sei $\theta \in L$ ein ganzes primitives Element von L, d.h. $L = K[\theta]$, und sei $p(x) = p_\theta(x) \in K[x]$ sein Minimalpolynom. Man definiert den *Führer* $\mathfrak{F}$ des Ringes $\mathfrak{o}[\theta]$ als das größte in $\mathfrak{o}[\theta]$ gelegene Ideal $\mathfrak{F}$ von $\mathcal{O}$, d.h.

$$\mathfrak{F} = \{\alpha \in \mathcal{O} \mid \alpha\mathcal{O} \subseteq \mathfrak{o}[\theta]\}.$$

Beachte: $\mathfrak{F} \neq 0$.

5.11. Satz.(Kummer-Dedekind) *Sei* $\mathfrak{p}$ *ein zum Führer* $\mathfrak{F}$ *von* $\mathfrak{o}[\theta]$ *teilerfremdes Primideal von* $\mathfrak{o}$ *und für das Minimalpolynom von* θ *gelte:*

$$p(x) \equiv \overline{p}_1(x)^{e_1} \cdot \ldots \cdot \overline{p}_r(x)^{e_r} \qquad (\mathrm{mod}\ \mathfrak{p})$$

mit irreduziblen Faktoren $\overline{p}_i(x) \in \mathbb{F}_\mathfrak{p}[x]$. Sei $p_i(x) \in \mathfrak{o}[x]$ ein Repräsentant von $\overline{p}_i$. Dann sind

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

die verschiedenen über $\mathfrak{p}$ liegenden Primideale von $\mathcal{O}$. Der Trägheitsgrad f_i von $\mathfrak{P}_i$ ist der Grad von $\overline{p}_i(x)$ und es gilt:

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_r^{e_r}.$$

□

Beweis. Setze $\mathcal{O}' = \mathfrak{o}[\theta]$ und $\overline{\mathfrak{o}} = \mathfrak{o}/\mathfrak{p}$. Dann erhalten wir kanonische Isomorphismen

$$\mathcal{O}/\mathfrak{p}\mathcal{O} \cong \mathcal{O}'/\mathfrak{p}\mathcal{O}' \cong \overline{\mathfrak{o}}[x]/(\overline{p}(x)).$$

Der erste Isomorphismus beruht auf der Teilerfremdheit $\mathfrak{p}\mathcal{O} + \mathfrak{F} = \mathcal{O}$. Wegen $\mathfrak{F} \subseteq \mathcal{O}'$ folgt $\mathcal{O} = \mathfrak{p}\mathcal{O} + \mathcal{O}'$ und deswegen ist $\mathcal{O}' \to \mathcal{O}/\mathfrak{p}\mathcal{O}$ surjektiv mit Kern $\mathfrak{P}\mathcal{O} \cap \mathcal{O}'$. Letzterer ist gleich $\mathfrak{p}\mathcal{O}'$, denn wegen $(\mathfrak{p}, \mathfrak{F} \cap \mathfrak{o}) = 1$ ist $\mathfrak{p}\mathcal{O} \cap \mathcal{O}' = \mathfrak{p} + \mathfrak{F}(\mathfrak{p}\mathcal{O} \cap \mathcal{O}') \subseteq \mathfrak{p}\mathcal{O}'$.
Der zweite Isomorphismus ergibt sich duch den surjektiven Homomorphismus

$$\mathfrak{o}[x] \longrightarrow \overline{\mathfrak{o}}[x]/(\overline{p}(x)).$$

Der Kern ist durch $\mathfrak{p}$ und $p(x)$ erzeugte Ideal. Weil $\mathcal{O}' = \mathfrak{o}[\theta] = \mathfrak{o}[x]/(p(x))$ wird $\mathcal{O}'/\mathfrak{p}\mathcal{O}' \cong \overline{\mathfrak{o}}[x]/(\overline{\mathfrak{o}}(x))$. Wegen $\overline{p}(x) = \prod_{i=1}^{r} \overline{p}_i(x)^{e_i}$ besteht der Isomorphismus

$$\overline{\mathfrak{o}}[x]/(\overline{p}(x)) \cong \bigoplus_{i=1}^{r} \overline{\mathfrak{o}}[x]/(\overline{p}_i(x))^{e_i} \quad .$$

Deshalb sind die Primideale des Ringes $R = \overline{o}[x]/(\overline{p}(x))$, die durch $\overline{p}_i(x) \pmod{\overline{p}(x)}$ gegebenen Hauptideale $\overline{p}_i,\ i = 1, \ldots, r$. Es gilt $[R/(\overline{p}_i(x)) : \mathfrak{o}] = \deg \overline{p}_i(x)$ und $(0) = (\overline{p}) = \bigcap_{i=1}^{r} (\overline{p}_i)^{e_i}$. Es gilt nun diese Erkenntnisse auf den Ring $\mathcal{O}/\mathfrak{p}\mathcal{O}$ zu übertragen, denn weil $\overline{\mathfrak{o}}[x]/(\overline{p}(x)) \cong \mathcal{O}/\mathfrak{p}\mathcal{O}, f(x) \to f(\theta)$, gelten dort die gleichen Verhältnisse. Die Primideale $\overline{\mathfrak{P}}_i$ von $\mathcal{O}/\mathfrak{p}\mathcal{O}$ entsprechen den $\overline{p}_i$ und werden von $p_i(\theta) \bmod \mathfrak{p}\mathcal{O}$ erzeugt. Weiter ist $[(\mathcal{O}/\mathfrak{p}\mathcal{O})/\overline{\mathfrak{P}_i} : \overline{\mathfrak{o}}] = \deg p_i$ und $(0) = \bigcap_{i=1}^{r} \overline{\mathfrak{P}}_i^{e_i}$. Sei nun $\mathfrak{P}_i = \mathfrak{p}\mathcal{O} + p_i(\theta)\mathcal{O}$ das Urbild von $\overline{\mathfrak{P}}_i$ unter dem kanonischen Homomorphismus

$$\mathcal{O} \longrightarrow \mathcal{O}/\mathfrak{p}\mathcal{O}.$$

Dann durchläuft $\mathfrak{P}_i$, wobei $i = 1, \ldots, r$ ist, die über $\mathfrak{p}$ gelegenen Primideale von $\mathcal{O}$, es ist $f_i = [\mathcal{O}/\mathfrak{P}_i : \mathfrak{o}/\mathfrak{p}] = \deg p_i$. Es ist $\mathfrak{P}_i^{e_i}$ das Urbild von $\overline{\mathfrak{P}}_i^{e_i}$ und $\mathfrak{p}\mathcal{O} \supseteq \bigcap_{i=1}^{r} \mathfrak{P}_i^{e_i}$, also $\mathfrak{p}\mathcal{O} \mid \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$ und damit $\mathfrak{p}\mathcal{O} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$, weil $\sum_i e_i f_i = n$. □

5.12. Bemerkung. Die Aussage von Satz 5.11 gilt sogar für alle Primideale von $\mathfrak{o}[\theta]$, nicht nur für die zum Führer $\mathfrak{F}$ teilerfremden (siehe zB. [St])

5.13. Satz. *Ist $L|K$ separabel, so gibt es nur endlich viele in L verzweigte Primideale.*

Beweis. Sei $L = K[\theta]$ und $p \in K[x]$ das Minimalpolynom von θ. Weiter sei

$$d = \operatorname{discr}(1, \theta, \theta^2, \ldots, \theta^{n-1}) = \prod_{i<j} (\theta_i - \theta_j)^2 \in \mathfrak{o}$$

die Diskriminante. Dann sind alle zu d und zum Führer $\mathfrak{F}$ von $\mathfrak{o}[\theta]$ teilerfremden Primideale unverzweigt. Denn $p \pmod{\mathfrak{p}}$ hat nur dann mehrfache Nullstellen, falls $d \equiv 0 \bmod \mathfrak{p}$. Aufgrund des letzten Satzes beschreibt die Reduktion von p das Verzweigungsverhalten der Primideale über $\mathfrak{p}$. Die Restkörpererweiterungen $\mathcal{O}/\mathfrak{P}_i \mid \mathfrak{o}/\mathfrak{p}$ werden durch $\overline{\theta} \equiv \theta \pmod{\mathfrak{P}_i}$ erzeugt, sind also separabel. Deshalb ist $\mathfrak{p}$ unverzweigt. Da es nur endlich viele Primideale gibt, die $d \cdot \mathfrak{F}$ teilen, folgt die Aussage. □

5.14. Bemerkung. Man kann die Menge der verzweigten Primideale noch genauer beschreiben. Falls $K = \mathbb{Q}$, $\mathfrak{o} = \mathbb{Z}$ und $L|K$ algebraischer Zahlkörper ist, dann ist $\mathcal{O} = \mathcal{O}_L$ und $\operatorname{discr}(\mathcal{O}_K) \subseteq \mathfrak{F}$. Man zeigt, daß genau die Primideale $\mathfrak{P}$ verzweigen, die $\partial_{L|K} := \operatorname{discr}(\mathcal{O}_K)$ (vgl. Definition 7.1) teilen.

5.15. Satz. *Sei K ein algebraischer Zahlkörper, dann existiert eine endliche Erweiterung $L|K$ mit der Eigenschaft, daß für alle Ideale $\mathfrak{a} \subseteq \mathcal{O}_K$ das Ideal $\mathfrak{a} \cdot \mathcal{O}_L$ ein Hauptideal ist.*

Beweis. Seien $\mathfrak{a}_1, \mathfrak{a}_2$ Ideale von K mit der gleichen Idealklasse, d.h. es gibt $\beta_1, \beta_2 \in K$, so daß $(\beta_1)\mathfrak{a}_1 = (\beta_2)\mathfrak{a}_2$. Es gilt somit auch $(\beta_1)\mathfrak{a}_1\mathcal{O}_L = (\beta_2)\mathfrak{a}_2\mathcal{O}_L$ für alle Erweiterungen $L|K$. Deshalb genügt es die Aussage für einen Repräsentanten jeder Idealklasse zu zeigen. Seien nun $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ die Repräsentanten von Cl_K. Da $|Cl_K| = h$ ist, sind alle $\mathfrak{a}_i^h$, $i = 1, \ldots, n$ Hauptideale, d.h. $\mathfrak{a}_i^h = (\alpha_i)$ für ein $\alpha_i \in K$. Der Körper $L = K[\sqrt[h]{\alpha_1}, \ldots \sqrt[h]{\alpha_n}]$ erfüllt die Behauptung des Satzes, denn aus $\mathfrak{a}_i^h\mathcal{O}_L = (\mathfrak{a}_i\mathcal{O}_L)^h = (\alpha_i)$ folgt $\mathfrak{a}_i\mathcal{O}_L = \left(\sqrt[h]{\alpha_i}\right)$. □

5.16. Bemerkung. Beachte: Aus Satz 5.15 folgt, daß $\mathcal{O}_L$ selbst im Allgemeinen kein Hauptidealring ist. Wiederholtes Anwenden der Konstruktion des Satzes führt zu einer Kette von algebraischer Zahlkörper

$$K \subseteq L_1 \subseteq L_2 \subseteq \cdots \quad ,$$

in denen Ideale von L_i in L_j für $j > i$ Hauptideale sind. Man zeigt, daß es sowohl endliche als auch undendliche Ketten gibt (schwieriger Satz von Golod und Shavarevich!). Das Studium von Körpererweiterungen mit vorgegebenem Verzweigungsverhalten wird in der Klassenkörpertheorie untersucht.

Für das weitere Verständnis benötigen wir einige Grundlagen über Galoiserweiterungen (siehe A.9 – A.15).

5.17. Lemma. *Ein Primideal $\mathfrak{P}$ aus $\mathcal{O}$ teilt $\mathfrak{p} \cdot \mathcal{O}$, wobei $\mathfrak{p}$ aus $\mathfrak{o}$ ist, genau dann, wenn $\mathfrak{p} = \mathfrak{P} \cap K$.*

Beweis. "⇒" Offensichtlich gilt $\mathfrak{p} \subseteq \mathfrak{P} \cap K$, da außerdem $\mathfrak{P} \cap K$ ein Primideal ist, folgt aus der Maximalität der Primideale $\mathfrak{p} = \mathfrak{P} \cap K$.

"⇐"Falls $\mathfrak{p} \subset \mathfrak{P}$ (als Menge!), dann ist auch $\mathfrak{p}\mathcal{O} \subset \mathfrak{P}$, also $\mathfrak{P}$ teilt $\mathfrak{p}\mathcal{O}$. □

5.18. Lemma. *Sei $\mathfrak{a}$ ein gebrochenes Ideal von K. Dann gilt $\mathfrak{a}\mathcal{O} \cap K = \mathfrak{a}$.*

Beweis. Als Mengen besteht die Inklusion $\mathfrak{a} \subset \mathfrak{a}\mathcal{O}$. Es ist deshalb zu zeigen, daß wenn $\beta \in \mathfrak{a} \cup \mathcal{O}$, so ist β bereits in $\mathfrak{a}$: Sei also $\beta = \sum \alpha_i w_i$ mit $\alpha_i \in \mathfrak{a}$, $w_i \in \mathcal{O}$. Es reicht, den Fall $L|K$ galoissch zu betrachten. Seien $\sigma_1, \ldots, \sigma_n$ die Elemente der Galoisgruppe $\mathrm{Gal}(L|K)$. Da β gleichzeitig in K ist, gilt somit:

$$\beta^n = \prod_j (\sigma_j \beta) = \prod_j (\sum_i \alpha_i \sigma_j w_i).$$

Wenn wir die rechte Seite als Polynom in den α_i betrachten, dann sind die Koeffizienten symmetrische Funktionen in den $\sigma_j w_i$, somit also aus o. Es folgt $\beta^n \in \mathfrak{a}^n$ und da die Idealgruppe J_K torsionsfrei ist, folgt $\beta \in \mathfrak{a}$. □

5.19. Satz. *Sei $L|K$ galoissch vom Grad n und $\mathfrak{P}_1, \ldots, \mathfrak{P}_k$ die Primidealteiler von $\mathfrak{p}\mathcal{O}$ für ein Primideal $\mathfrak{p} \in o$. Dann sind die Verzweigungsindizes e_i und die Trägheitsgrade f_i der $\mathfrak{P}_i$, $i = 1, \ldots, 2$ gleich und somit gilt $efk = n$.*

Beweis. Der Körper K und somit auch o ist $\mathrm{Gal}(L|K)$ invariant. Ist nun $\sigma \in \mathrm{Gal}(L|K)$ und $\mathfrak{P}$ ein Primideal von $\mathcal{O}$, dann ist auch $\sigma\mathfrak{P}$ ein Primideal. Weil $\mathfrak{P}$ teilt $\mathfrak{p}\mathcal{O}$ genau dann, wenn $\mathfrak{p} = \mathfrak{P} \cap K$, folgt, daß mit $\mathfrak{P}$ auch alle $\sigma\mathfrak{P}$ Teiler von $\mathfrak{p}\mathcal{O}$ sind. Es ist klar, daß $e = e(\mathfrak{P}/\mathfrak{p}) = e(\sigma\mathfrak{P}/\mathfrak{p})$ und $f = f(\mathfrak{P}/\mathfrak{p}) = f(\sigma\mathfrak{P}/\mathfrak{p})$.

Seien nun $\mathfrak{P}$ und $\mathfrak{Q}$ nicht konjugierte Teiler von $\mathfrak{p}\mathcal{O}$, d.h. $\sigma\mathfrak{P} \neq \mathfrak{Q}$ für alle $\sigma \in \mathrm{Gal}(L|K)$. Es existiert dann ein $\beta \in \mathfrak{Q}$ mit $\beta \notin \sigma\mathfrak{P}$ für alle $\sigma \in \mathrm{Gal}(L|K)$. Setze $b = \mathrm{Nm}_{L|K}(\beta) = \prod_{\sigma \in \mathrm{Gal}(L|K)} \sigma\beta$. Als Norm eines ganzen Elements von $\mathcal{O}$ ist $b \in o$ und weil $\beta \in \mathfrak{Q}$ ist auch $b \in \mathfrak{Q}$ und somit ist $b \in \mathfrak{Q} \cap o = \mathfrak{p}$. Andererseits ist $\beta \notin \sigma^{-1}\mathfrak{P}$ und deshalb auch $\sigma\beta \notin \mathfrak{P}$ für alle $\sigma \in \mathrm{Gal}(L|K)$. Da aber $\prod \sigma\beta \in \mathfrak{p} \subset \mathfrak{P}$, erhalten wir einen Widerspruch zur Primeigenschaft von $\mathfrak{P}$. Deshalb sind alle Teiler von $\mathfrak{p}\mathcal{O}$ zueinander konjugiert. Somit sind die Verzweigungsindizes bzw. Trägheitsgrade bzgl. $\mathfrak{p}$ der Faktoren der Primfaktorzerlegung von $\mathfrak{p}$ in $\mathcal{O}$ gleich. □

6 Norm von Idealen, Produktformel

Seien o, K, $\mathcal{O}$ und L wie gehabt. Zusätzlich sei $L|K$ separabel.

6.1. Definition. Die *relative Norm* $\mathrm{Nm}_{L|K}(\mathfrak{P})$ eines Primideals $\mathfrak{P} \subset \mathcal{O}$ von L wird definiert als das Ideal

$$\mathrm{Nm}_{L|K}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})},$$

wobei $\mathfrak{p} = \mathfrak{P} \cap o$ und $f(\mathfrak{P}/\mathfrak{p}) = [\mathcal{O}/\mathfrak{P} : o/\mathfrak{p}]$. Damit wird die relative Norm eines beliebigen Ideals $\mathfrak{A} \subset \mathcal{O}$ von L mit Primidealzerlegung $\mathfrak{A} = \prod_{i=1}^n \mathfrak{P}_i^{r_i}$ definiert als

$$\mathrm{Nm}_{L|K}(\mathfrak{A}) = \prod_{i=1}^n \mathrm{Nm}_{L|K}(\mathfrak{P}_i)^{r_i}.$$

6.2. Proposition. *Für einen Körperturm $L_2|L_1|K$ gilt für alle Ideale $\mathfrak{A}$ von L_2, daß* $\mathrm{Nm}_{L_1|K}\big(\mathrm{Nm}_{L_2|L_1}(\mathfrak{A})\big) = \mathrm{Nm}_{L_2|K}(\mathfrak{A})$.

Beweis. Es genügt die Aussage für $\mathfrak{A} = \mathfrak{P}_2$ mit einem Primideal $\mathfrak{P}_2$ zu beweisen. Sei nun $\mathrm{Nm}_{L_2|L_1}(\mathfrak{P}_2) = \mathfrak{P}_1^{f(\mathfrak{P}_2/\mathfrak{P}_1)}$ und $\mathrm{Nm}_{L_1|K}(\mathfrak{P}_1) = \mathfrak{p}^{f(\mathfrak{P}_1/\mathfrak{p})}$. Die Behauptung folgt aus der Identität $f(\mathfrak{P}_2/\mathfrak{P}_1)\cdot f(\mathfrak{P}_1/\mathfrak{p}) = f(\mathfrak{P}_2/\mathfrak{p})$, die wegen $[\mathcal{O}_{L_2}/\mathfrak{P}_2 : \mathcal{O}_{L_1}/\mathfrak{P}_1]\cdot[\mathcal{O}_{L_1}/\mathfrak{P}_1 : \mathcal{O}/\mathfrak{p}] = [\mathcal{O}_{L_2}/\mathfrak{P}_2 : \mathcal{O}/\mathfrak{p}]$ gilt. □

6.3. Definition. In dem Spezialfall $\mathcal{O} = \mathbb{Z}$, $K = \mathbb{Q}$ und $L|K$ eine algebraische Körpererweiterung mit Ring der ganzen Zahlen $\mathcal{O} = \mathcal{O}_L$ wird die Komposition

$$\mathrm{Nm} : J_L \overset{\mathrm{Nm}_{L|\mathbb{Q}}}{\longrightarrow} J_{\mathbb{Q}} \overset{\sim}{\longrightarrow} \mathbb{Q}_{>0}$$

die *absolute Norm* genannt. Man identifiziert hierbei das Hauptideal mit seinem Erzeuger und wegen der exakten Sequenz $1 \to \{\pm 1\} \to \mathbb{Q}^* \to J_{\mathbb{Q}} \to 1$ ist die zweite Abbildung in der Tat ein Isomorphismus. Mittels des Chinesischen Restsatzes überzeugt man sich leicht, daß

$$\mathrm{Nm}(\mathfrak{A}) = [\mathcal{O}_L : \mathfrak{A}] = \#\mathcal{O}_L/\mathfrak{A}.$$

6.4. Satz. *Für jedes $\gamma \in L$ erfüllt die absolute Norm die Gleichheit* $\mathrm{Nm}\big((\gamma)\big) = \big|\,\mathrm{Nm}_{L|\mathbb{Q}}(\gamma)\big|$. *In anderen Worten, folgendes Diagramm kommutiert:*

$$\begin{array}{ccc} L^* & \longrightarrow & J_L \\ {\scriptstyle |\mathrm{Nm}_{L|\mathbb{Q}}(\cdot)|}\downarrow & \swarrow^{\mathrm{Nm}} & \downarrow{\scriptstyle \mathrm{Nm}_{L|\mathbb{Q}}} \\ \mathbb{Q}_{>0} & \xrightarrow{\sim} & J_{\mathbb{Q}} \end{array}$$

Beweis. Zum Beweis der Verträglichkeit der Normabbildungen aus den Definitionen 6.1 und 6.3 wählen wir eine Ganzheitsbasis $\beta_1, \ldots, \beta_n$ von $\mathcal{O}_L$ über $\mathbb{Z}$. Damit ist $\gamma\beta_1, \ldots, \gamma\beta_n$ eine Basis des Hauptideals (γ). Wir erhalten

$$\gamma\beta_j = \sum_{k=1}^{n} a_{jk}\beta_k,$$

mit $a_{jk} \in \mathbb{Z}$ und setzen $A = (a_{jk})$. Man folgert nun

$$\mathrm{Nm}\big((\gamma)\big) = [\mathcal{O}_L : \gamma\mathcal{O}_L] = |\det(A)| = \big|\,\mathrm{Nm}_{L|\mathbb{Q}}(\gamma)\big|,$$

hierbei ist die letzte Gleicheit gerade die Definition der Norm von $\gamma \in L$. □

6.5. Bemerkung. Mit Hilfe der absoluten Norm ergibt sich ein schneller Beweis der fundamentalen Gleichung für die Zerlegung einer Primzahl p in $\mathcal{O}_L$: Sei $p\mathcal{O}_L = \mathfrak{P}_1^{e_1}\cdot\ldots\cdot\mathfrak{P}_r^{e_r}$, dann gilt

$$p^{[L:\mathbb{Q}]} = \mathrm{Nm}_{L|\mathbb{Q}}(p) = \mathrm{Nm}(p\mathcal{O}_L) = \mathrm{Nm}(\mathfrak{P}_1)^{e_1}\cdot\ldots\cdot\mathrm{Nm}(\mathfrak{P}_r)^{e_r} = p_1^{f_1e_1}\cdot\ldots\cdot p_r^{f_re_r}$$

und deshalb auch $[L : \mathbb{Q}] = \sum e_i f_i$ wobei $f_i = [\mathcal{O}_L/\mathfrak{P}_i : \mathbb{Z}/(p)]$.

6.6. Definition. Sei $\gamma \in L$ mit Primidealzerlegung $(\gamma) = \mathfrak{P}_1^{v_{\mathfrak{P}_1}(\gamma)} \cdot \ldots \cdot \mathfrak{P}_r^{v_{\mathfrak{P}_r}(\gamma)}$. Sei $\mathfrak{P} \in \operatorname{Spec} \mathcal{O}_L$ ein Primideal von L, dann ist der $\mathfrak{P}$-*adische Absolutbetrag* von γ gegeben durch

$$|\gamma|_{\mathfrak{P}} = \operatorname{Nm}(\mathfrak{P})^{-v_{\mathfrak{P}}(\gamma)} = p^{-f_{\mathfrak{P}} v_{\mathfrak{P}}(\gamma)},$$

wobei $(p) = \mathfrak{P} \cap \mathbb{Z}$ und $f_{\mathfrak{P}} = [\mathcal{O}_L/\mathfrak{P} : \mathbb{Z}/(p)]$.
Wir fixieren nun ein und für alle Mal eine Einbettung von $\overline{\mathbb{Q}}$ in $\mathbb{C}$. Damit setzen wir für $\sigma \in \operatorname{Hom}_{\mathbb{Q}}(L, \overline{\mathbb{Q}}) = \operatorname{Hom}_{\mathbb{Q}}(L, \mathbb{C})$

$$|\gamma|_{\sigma} = |\sigma(\gamma)|,$$

wobei $|\sigma(\gamma)|$ der gewöhnliche Absolutbetrag einer komplexen Zahl ist.

6.7. Satz. (Produktformel) *Sei $\gamma \in L$, dann gilt mit $\widehat{\operatorname{Spec}}\, \mathcal{O}_L := \operatorname{Spec} \mathcal{O}_L \cup \operatorname{Hom}_{\mathbb{Q}}(L, \overline{\mathbb{Q}})$*

$$\prod_{\mathfrak{P} \in \widehat{\operatorname{Spec}}\, \mathcal{O}_L} |\gamma|_{\mathfrak{P}} = 1.$$

Beweis. Aufgrund von Satz 6.4 gilt

$$\prod_{\mathfrak{P} \in \operatorname{Spec} \mathcal{O}_L} |\gamma|_{\mathfrak{P}} = \frac{1}{\operatorname{Nm}\big((\gamma)\big)} = \frac{1}{\big|\operatorname{Nm}_{L|\mathbb{Q}}(\gamma)\big|}.$$

Weil $L|\mathbb{Q}$ separabel ist folgt aus Satz 1.10 die Gleichheit

$$\big|\operatorname{Nm}_{L|\mathbb{Q}}(\gamma)\big| = \Big|\prod_{\sigma \in \operatorname{Hom}_{\mathbb{Q}}(L,\overline{\mathbb{Q}})} \sigma\gamma\Big| = \prod_{\sigma \in \operatorname{Hom}_{\mathbb{Q}}(L,\overline{\mathbb{Q}})} |\sigma\gamma| = \prod_{\sigma \in \operatorname{Hom}_{\mathbb{Q}}(L,\overline{\mathbb{Q}})} |\gamma|_{\sigma}.$$

Daraus folgt dann die Behauptung. □

6.8. Satz. *Sei $L|K$ eine separable algebraische Erweiterung.*

(i) *Es gilt $\operatorname{Nm}_{L|K}(\mathfrak{a}\mathcal{O}_L) = \mathfrak{a}^{[L:K]}$ für alle Ideale $\mathfrak{a} \neq 0$ von K.*

(ii) *Zusätzlich sei $L|K$ galoissch. Sei $\mathfrak{P}$ ein Primideal von L, $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}$ und $\mathfrak{p}\mathcal{O} = (\mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_r)^e$. Dann gilt*

$$\operatorname{Nm}_{L|K}(\mathfrak{P}) \cdot \mathcal{O} = (\mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_r)^{ef} = \prod_{\sigma \in \operatorname{Gal}(L|K)} \sigma\mathfrak{P}.$$

(iii) *Die relative Norm von Idealen ist mit der relativen Normabbildung von Körpern verträglich, i.a.W. folgendes Diagramm kommutiert*

$$\begin{array}{ccc} L^* & \longrightarrow & J_L \\ {\scriptstyle \operatorname{Nm}_{L|K}}\downarrow & & \downarrow{\scriptstyle \operatorname{Nm}_{L|K}} \\ K^* & \longrightarrow & J_K \end{array}$$

(iv) *Für jedes Ideal* $\mathfrak{A}$ *von* L *ist* $\mathrm{Nm}_{L|K}(\mathfrak{A})$ *das von den Normen* $\mathrm{Nm}_{L|K}(a)$ *der Elemente* $a \in \mathfrak{A}$ *erzeugte Ideal von* K*.*

Beweis. (i) Es genügt die Aussage für ein Primideal $\mathfrak{p}$ von K zu betrachten, dann gilt jedoch

$$\mathrm{Nm}_{L|K}(\mathfrak{p}\mathcal{O}) = \mathrm{Nm}_{L|K}\big(\prod_{i=1}^{r}\mathfrak{P}_i^{e_i}\big) = \prod_{i=1}^{r}\mathrm{Nm}_{L|K}(\mathfrak{P}_i)^{e_i} = \mathfrak{p}^{\sum e_i f_i} = \mathfrak{p}^{[L:K]}.$$

(ii) Aus $\mathrm{Nm}_{L|K}(\mathfrak{P}) = \mathfrak{p}^f$ folgt die erste Gleichheit. Da die Galoisgruppe $\mathrm{Gal}(L|K)$ transitiv auf der Menge $\{\mathfrak{P}_1, \dots \mathfrak{P}_r\}$ operiert und weil $efr = [L:K]$ ist, gilt die zweite Gleicheit.
(iii) Wir untersuchen zuerst den Fall, daß $L|K$ galoisch ist. Die Abbildung $J_K \to J_L$ gegeben durch $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_L$ ist injektiv, da beide Gruppen freie Gruppen sind, deshalb genügt es für beliebiges $\beta \in L$ die folgende Gleichheit zu zeigen

$$\mathrm{Nm}_{L|K}\big((\beta)\big)\mathcal{O} = \prod\sigma(\beta) = \prod(\sigma\beta\mathcal{O}) = \big(\prod\sigma\beta\big)\mathcal{O} = \mathrm{Nm}_{L|K}(\beta)\cdot\mathcal{O}.$$

Im allgemeinen Fall betrachten wir eine Galoiserweiterung $E|K$ die L als Teilkörper enthält. Es sei $d = [E:L]$ und es bezeichne $\mathcal{O}_E$ den ganze Abschluß von $\mathcal{O}$ in E. Dann gilt mit dem bereits bewiesenen

$$\mathrm{Nm}_{L|K}\big((\beta)\big)^d = \mathrm{Nm}_{E|K}\big(\beta\mathcal{O}_E\big) = \big(\mathrm{Nm}_{E|K}(\beta)\big) = \big(\mathrm{Nm}_{L|K}(\beta)^d\big) = \big(\mathrm{Nm}_{L|K}(\beta)\big)^d.$$

Weil J_K torsionsfreie Gruppe ist, folgt daraus $\mathrm{Nm}_{L|K}\big((\beta)\big) = \big(\mathrm{Nm}_{L|K}(\beta)\big)$.
(iv) Wegen (iii) ist die Aussage klar für Hauptideale. Sei nun $\mathfrak{p}$ ein Primideal von K, dann ist der ganze Abschluß $\mathcal{O}_\mathfrak{p}$ von $\mathcal{o}_\mathfrak{p}$ in L ein Hauptidealring. Dies gilt weil $\mathcal{O}_\mathfrak{p}$ ein Dedekindring mit endlich vielen Primidealen (nämlich genau einem!) ist. Sei nun $\mathfrak{a}$ das von den relativen Normen $\mathrm{Nm}_{L|K}(a)$ mit $a \in \mathfrak{A}$ erzeugte Ideal. Dann ist $\mathfrak{A}_\mathfrak{p} = \mathfrak{A}\mathcal{O}_\mathfrak{p}$ ein Hauptideal und $\mathfrak{a}_\mathfrak{p} = \mathrm{Nm}_{L|K}(\mathfrak{A}_\mathfrak{p}) = \mathrm{Nm}_{L|K}(\mathfrak{A})_\mathfrak{p}$. Da dies jedoch für alle $\mathfrak{p}$ gilt folgt die Behauptung. □

7 Diskriminante und Differente

7.1. Definition. Das Ideal $\partial_{L|K} \in \mathcal{O}_K$, welches von den Diskriminanten aller in $\mathcal{O}_L$ gelegenen Basen von $L|K$ erzeugt wird, heißt das *Diskriminantenideal* von $L|K$.
Man überzeugt sich leicht, daß

$$\partial_{L|K} = \bigcap_{\mathfrak{p}\in\mathrm{Spec}\,\mathcal{O}_K}(\partial_{L|K})_\mathfrak{p},$$

wobei $(\partial_{L|K})_\mathfrak{p} = \mathrm{discr}((\mathcal{O}_L)_\mathfrak{p} \mid (\mathcal{O}_K)_\mathfrak{p})$ die Diskriminante der Ganzheitsbasis von $(\mathcal{O}_L)_\mathfrak{p}$ über dem Hauptidealring $(\mathcal{O}_K)_\mathfrak{p}$ ist.

7.2. Proposition. *Es gilt* $\mathfrak{p} \in \mathcal{O}_K$ *ist verzweigt in* $\mathcal{O}_L$ *genau dann, wenn* $\mathfrak{p} \supset \partial_{L|K}$

Beweis. `Beweis aus ??? Milne einarbeiten` □

7.3. Definition. Das gebrochene Ideal

$$\mathcal{O}_L^\vee = \{x \in L \mid \mathrm{Tr}_{L|K}(x\mathcal{O}_L) \subseteq \mathcal{O}_K\}$$

heißt der Dedekindsche Komplementärmodul. Das dazu inverse Ideal $\mathcal{D}_{L|K} = (\mathcal{O}_L^\vee)^{-1}$ heißt die *Differente* von $\mathcal{O}_L$ über $\mathcal{O}_K$.

7.4. Satz. *Zwischen der Diskriminante und der Differente besteht die Beziehung*

$$\partial_{L|K} = \mathrm{Nm}(\mathcal{D}_{L|K}). \tag{7.4.1}$$

Beweis. Ist S eine multiplikative Teilmenge von $\mathcal{O}_K$, dann gilt

$$\partial_{S^{-1}\mathcal{O}_L|S^{-1}\mathcal{O}_K} = S^{-1}\partial_{\mathcal{O}_L|\mathcal{O}_K} \text{ und } \mathcal{D}_{S^{-1}\mathcal{O}_L|S^{-1}\mathcal{O}_K} = S^{-1}\mathcal{D}_{\mathcal{O}_L|\mathcal{O}_K}.$$

Darum genügt es (7.4.1) lokal zu beweisen. Dann sind jedoch wegen Proposition 2.16 $\mathcal{O}_{K,\mathfrak{p}}$ und $\mathcal{O}_{L,\mathfrak{p}} = (\mathcal{O}_K \setminus \mathfrak{p})^{-1}\mathcal{O}_L$ Hauptidealringe. Weiter gibt es eine Ganzheitsbasis $\{\alpha_1, \ldots, \alpha_n\}$ von $\mathcal{O}_{L,\mathfrak{p}}$ über $\mathcal{O}_{K,\mathfrak{p}}$ und deshalb ist $\partial_{\mathcal{O}_{L,\mathfrak{p}}|\mathcal{O}_{K,\mathfrak{p}}} = \mathrm{discr}(\alpha_1, \ldots, \alpha_n)$. Der Komplementärmodul wird durch die duale Basis $\alpha_1', \ldots, \alpha_n'$ aufgespannt, für die $\mathrm{Tr}_{L|K}(\alpha_i\alpha_j') = \delta_{ij}$ gilt. Es sei (β) ein Erzeuger des Hauptideals $\partial_{\mathcal{O}_{L,\mathfrak{p}}|\mathcal{O}_{K,\mathfrak{p}}}$ und $\mathrm{discr}(\beta\alpha_1, \ldots, \beta\alpha_n) = (\mathrm{Nm}_{L|K}(\beta))^2 \,\mathrm{discr}(\alpha_1, \ldots, \alpha_n)$. Damit ist dann

$$(\mathrm{Nm}_{L|K}(\beta)) = (\mathrm{Nm}_{L|K}(\mathcal{O}_{L,\mathfrak{p}})) = \mathrm{Nm}_{L|K}(\mathcal{D}_{\mathcal{O}_{L,\mathfrak{p}}\mathcal{O}_{K,\mathfrak{p}}})^{-1}$$

und $(\mathrm{discr}(\alpha_1, \ldots, \alpha_n)) = \partial_{\mathcal{O}_{L,\mathfrak{p}}|\mathcal{O}_{K,\mathfrak{p}}}$. Mit den Gleichheiten $\mathrm{discr}(\alpha_1, \ldots, \alpha_n) = \det((\sigma_i\alpha_j))^2$, $\mathrm{discr}(\alpha_1', \ldots \alpha_n') = \det((\sigma_i\alpha_j'))^2$ und $\mathrm{Tr}_{L|K}\,\alpha_i\alpha_j' = \delta_{ij}$ folgt

$$\mathrm{discr}(\alpha_1, \ldots, \alpha_n) \cdot \mathrm{discr}(\alpha_1', \ldots, \alpha_n') = 1.$$

Wir erhalten damit

$$\begin{aligned}\partial^{-1}_{\mathcal{O}_{L,\mathfrak{p}}|\mathcal{O}_{K,\mathfrak{p}}} &= (\mathrm{discr}(\alpha_1, \ldots, \alpha_n)^{-1} = (\mathrm{discr}(\alpha_1', \ldots, \alpha_n')) \\ &= (\mathrm{discr}(\beta\alpha_1, \ldots, \beta\alpha_n)) \\ &= \mathrm{Nm}_{L|K}(\mathcal{D}_{\mathcal{O}_{L,\mathfrak{p}}|\mathcal{O}_{K,\mathfrak{p}}})^{-2}\partial_{\mathcal{O}_{K,\mathfrak{p}}|\mathcal{O}_{L,\mathfrak{p}}},\end{aligned}$$

also auch $\partial_{\mathcal{O}_{L,\mathfrak{p}}|\mathcal{O}_{K,\mathfrak{p}}} = Nm_{L|K}(\mathcal{D}_{\mathcal{O}_{L,\mathfrak{p}}|\mathcal{O}_{K,\mathfrak{p}}})$. □

Literatur: Koch, Algebraische Zahlentheorie

8 Gitter und Minkowski-Räume

8.1. Definition. Sei V ein n-dimensionaler $\mathbb{R}$-Vektorraum. Ein *Gitter* in V ist eine Untergruppe der Form

$$\Lambda = \mathbb{Z}v_1 + \ldots + \mathbb{Z}v_m$$

mit linear unabhängigen Vektoren $v_1, \ldots, v_m$ aus V. In anderen Worten: Ein Gitter ist eine freie Abelsche Untergruppe von V die von linear unabhängigen Vektoren erzeugt wird. Das Gitter Λ heißt *vollständig* falls $m = n$ ist. Ist Λ ein vollständiges Gitter, dann ist $\Lambda \otimes \mathbb{R} = V$.

8.2. Beispiel. a) Die Untergruppe $\mathbb{Z}+\mathbb{Z}\sqrt{2}$ von $\mathbb{R}$ ist zwar eine freie abelsche Gruppe vom Rang 2, aber kein Gitter in $\mathbb{R}$.

b) Die Untergruppe $\{(a + b\sqrt{2}, a - b\sqrt{2}) \mid a, b \in \mathbb{Z}\} \subset \mathbb{R}^2$ ist ein Gitter, da $(1, 1)$ und $(\sqrt{2}, -\sqrt{2})$ linear unabhängige Vektoren sind.

8.3. Definition Sei $\Lambda = \mathbb{Z}v_1 + \ldots + \mathbb{Z}v_m$ ein Gitter, dann heißt $\{v_1, \ldots, v_m\}$ eine Basis und die Menge

$$\mathcal{F}_\Lambda = \{x_1v_1 + \ldots + x_mv_m \mid x_i \in \mathbb{R},\ \ 0 \leq x_i < 1\}$$

ein Grundmasche (oder auch Fundamentalbereich) von Λ.

Wir versehen nun V mit einer Topologie. Die Wahl einer Basis von V bestimmt einen Isomorphismus $V \to \mathbb{R}^n$ und somit eine Topologie auf V, (durch zurückziehen der üblichen Topologie von $\mathbb{R}^n$). Diese ist von der Wahl der Basis unabhängig, da lineare Abbildungen Homöomorphismen sind. Eine Untergruppe von V heißt diskret, falls sie in der induzierten Topologie diskret ist. (Ein topologischer Raum heißt diskret, wenn seine Punkte offene Menge sind.) In anderen Worten Λ ist diskret, falls jeder Punkt $\alpha \in \Lambda$ eine Umgebung $U \subset V$ besitzt, so daß $U \cap \Lambda = \{\alpha\}$.

8.4. Lemma. *Es sei Λ eine Untergruppe von einem endlich dimensionalen reellen Vektorraum V. Dann ist äquivalent:*

(i) *Λ ist eine diskrete Untergruppe;*

(ii) *es gibt eine offene Teilmenge U von V sodaß $U \cap \Lambda = \{0\}$;*

(iii) *jede kompakte Teilmenge von V schneidet Λ in einer endlichen Menge;*

(iv) *jede beschränkte Teilmenge von V schneidet Λ in einer endlichen Menge.*

Beweis. (i) $\Leftrightarrow$ (ii): Die Richtung (i) $\Rightarrow$ (ii) ist klar und es bleibt zu zeigen (ii) $\Rightarrow$ (i). Die Translation $x \mapsto \alpha + x$ auf V ist ein Homöomorphismus. Ist nun U eine Umgebung von 0 mit $U \cap \Lambda = \{0\}$, so ist $\alpha + U$ eine Umgebung von α mit $(\alpha + U) \cap \Lambda = \{\alpha\}$.

(i) $\Rightarrow$ (iii). Λ ist diskret, deshalb ist $C \cap \Lambda$ für jedes Kompaktum C eine kompakte, diskrete Menge, also endlich.

(ii) $\Rightarrow$ (iv). Dies ist klar, weil in $\mathbb{R}^n$ der Abschluß von beschränkten Mengen kompakt ist.

(iv) $\Rightarrow$ (ii). Sei K eine beschränkte Umgebung von 0. Dann ist $S = U \cap \Lambda \setminus \{0\}$ eine endliche Menge, also abgeschlossen. Deshalb ist $U \setminus S$ eine offene Umgebung von 0 mit der gewünschten Eigenschaft.

(iv) $\Rightarrow$ (iii). Ist klar. □

8.5. Satz. *Eine Untergruppe $\Lambda \subseteq V$ ist genau dann ein Gitter, wenn sie diskret ist.*

Beweis. Sei Λ eine diskrete Untergruppe von V. Sei V_0 der lineare Unterraum, der durch die Menge Λ aufgespannt wird, und m seine Dimension. Sei $u_1, \ldots, u_m$ eine in Λ gelegene Basis von V_0 und

$$\Lambda_0 = \mathbb{Z}u_1 + \cdots + \mathbb{Z}u_m \subset \Lambda.$$

Λ_0 ist ein vollständiges Gitter von V_0. Wir wollen zuerst zeigen, daß der Index $[\Lambda : \Lambda_0]$ endlich ist. Dazu durchlaufe $\gamma_i \in \Lambda$ ein Repräsentantensystem für die Nebenklassen in Λ/Λ_0. Da Λ vollständig ist in V_0, überdecken die Translate $\gamma + \mathcal{F}_{\Lambda_0}$, mit $\gamma \in \Lambda$ und der Grundmasche $\mathcal{F}_{\Lambda_0}$ für Λ_0, ganz V_0. Deshalb ist jedes γ_i von der Gestalt $\gamma_i = \mu_i + \gamma_{0i}$, wobei $\mu_i \in \mathcal{F}_{\Lambda_0}$ und $\gamma_{0i} \in \Lambda_0 \subseteq V_0$. Da die $\mu_i = \gamma_i - \gamma_{0i} \in \Lambda$ diskret in der beschränkten Menge $\mathcal{F}_{\Lambda_0}$ liegen, kann es nur endlich viele Nebenklassen γ_i geben.

Ist nun $q = [\Lambda : \Lambda_0]$, so ist $q\Lambda \subseteq \Lambda$ also auch

$$\Lambda \subseteq \frac{1}{q}\Lambda_0 = \mathbb{Z}\left(\frac{1}{q}u_1\right) + \cdots + \mathbb{Z}\left(\frac{1}{q}u_m\right).$$

Weil Λ eine abelsche Untergruppe der freien abelschen Gruppe $\frac{1}{q}\Lambda_0$ ist, besitzt Λ ein $\mathbb{Z}$-Basis $v_1, \ldots, v_m$, mit $r \leq m$. Da Λ jedoch V_0 aufspannt sind die Vektoren $v_1, \ldots, v_r$ linear unabhängig und es gilt $r = m$. Darum ist Λ ein Gitter. □

8.6. Satz. (Minkowski'scher Gitterpunksatz) *Sei X eine zentralsymmetrische und konvexe Teilmenge des n-dimensionalen Vektorraumes V und Λ ein vollständiges Gitter.*

(i) *Dann gilt* $\#\{\Lambda \cap X\} \geq 2^{-n}\frac{\mathrm{vol}(X)}{\mathrm{vol}(\Lambda)}$, *wobei* $\mathrm{vol}(\Lambda) = \mathrm{vol}(\mathcal{F}_\Lambda)$ *ist.*

(ii) *Ist* $\mathrm{vol}(X) > 2^n \mathrm{vol}(\Lambda)$, *so enthält X mindestens einen von Null verschiedenen Gitterpunkt $\gamma \in \Lambda$.*

8.7. Beweis. Wir fixieren ein kleines $\varepsilon > 0$ und setzen

$$\frac{1}{2}X = \{v \in V \mid 2v \in X\} \text{ und } (1/2+\varepsilon)X = \{v \in V \mid \left(\frac{2}{1+2\varepsilon}\right) \cdot v \in X\}.$$

Weiter sei $N \in \mathbb{N}$ und $\Lambda_N = \frac{1}{N} \cdot \Lambda = \{v \in V \mid N \cdot v \in \Lambda\}$. Die Grundmasche $\mathcal{F}_N$ von Λ_N ist ein Parallelepiped mit $\mathrm{vol}(\mathcal{F}_N) = N^{-n} \mathrm{vol}\,\Lambda$. Die Anzahlen

$$b_N(1/2X) = \#\{\gamma \in \Lambda_N \mid \gamma\mathcal{F}_N \subseteq 1/2X\}, \text{ resp.}$$
$$b_N((1/2+\varepsilon) \cdot X) = \#\{\gamma \in \Lambda_N \mid \gamma\mathcal{F}_N \subseteq (1/2+\varepsilon)X\},$$

multipliziert mit $\mathrm{vol}(\mathcal{F}_N)$ ergeben im wesentlichen das Volumen von $1/2X$, resp. $(1/2+\varepsilon)X$, also

$$N^{-n}b_N(1/2X) = \left(\frac{1}{2}\right)^n \frac{\mathrm{vol}(X)}{\mathrm{vol}(\Lambda)} + \delta_N, \text{ resp.}$$
$$N^{-n}b_N((1/2+\varepsilon)X) = (1/2+\varepsilon)^n \frac{\mathrm{vol}(X)}{\mathrm{vol}(\Lambda)} + \delta'_N,$$

wobei δ_N, resp. δ'_N mit wachsendem N gegen 0 streben. Die Grundmasche $\mathcal{F}_N$ hat 2^n Ecken, die jeweils auch Ecken von 2^n Translate $\gamma\mathcal{F}_N$ sind, deshalb geben die Anzahlen $b_N(1/2X)$ und $b_N(1/2+\varepsilon)X)$ obere Schranken für die Anzahl $a_N = \#\{\Lambda \cup 1/2X\}$, d.h.

$$b_N(1/2X) \leq a_N \leq b_N((1/2+\varepsilon)X).$$

Beachte: Für N hinreichend groß gewählt, und ε_1 beliebig klein gilt, dann

$$2^{-n}\frac{\mathrm{Vol}(X)}{\mathrm{Vol}(\Lambda)} - \varepsilon_1 \leq N^{-n}a_N \leq 2^{-n}\frac{\mathrm{Vol}(X)}{\mathrm{Vol}(\Lambda)} + \varepsilon_1.$$

Weil

$$a_N = \{\Lambda_N \cup 1/2X\} = \sum_{\gamma\in\Lambda_N/\Lambda} \#\{\gamma + \Lambda \cup 1/2X\}$$

und $\#\{\Lambda_n/\Lambda\} = N^n$ gilt, gibt es ein $\gamma_i \in \Lambda_N/\Lambda$, so daß $\#\{\gamma_i + \Lambda \cup 1/2x\} \geq \frac{a_N}{N^n}$. Seien nun $a_1, a_2, ..., a_m \in \{\gamma_i + \Lambda \cup 1/2X\}$, dann sind, weil X zentralsymmetrisch ist, auch $-a_1, -a_2, \ldots, -a_m \in 1/2X$ und weil X konvex ist, sind alle $1/2(a_1 - a_i) \in 1/2X$. Es folgt $a_1 - a_i \in X$ für $i = 1, \ldots, m$, mit $m \geq N^{-n}a_N$, weil alle a_i in der gleichen Nebenklasse von Λ in Λ_N liegen, ist auch $a_1 - a_i \in \Lambda$. Es folgt

$$\#\{\Lambda \cup X\} \geq \#\{a_1 - a_i\} \geq N^{-n}a_N \geq 2^{-n}\frac{\mathrm{Vol}(X)}{\mathrm{Vol}(\Lambda)} - \varepsilon_1,$$

weil ε_1 beliebig klein gewählt werden kann, folgt die Behauptung (i).
(i) $\Rightarrow$ (ii) ist trivial. □

8.8. Sei K ein algebraischer Zahlkörper. Wegen $K = \mathbb{Q}[\beta] \cong \mathbb{Q}[x]/(g(x))$ folgt aus der abstrakten Algebra

$$K \otimes_{\mathbb{Q}} \mathbb{C} \cong \mathbb{C}[x]/(g(x)) \cong \prod_{\sigma\in\Sigma} \mathbb{C}[x]/(x - \sigma\beta) \cong \prod_{\sigma\in\Sigma} \mathbb{C}$$

Man setzt $K_{\mathbb{C}} := \prod_{\sigma\in\Sigma} \mathbb{C}$. Als Menge ist $K_{\mathbb{C}} \cong \mathbb{C}^{[K:\mathbb{Q}]}$ und seine Ringstruktur ist durch die komponentenweise Multiplikation gegeben. Zusätzlich haben wir einen Ringhomomorphismus $\iota : K \to K_{\mathbb{C}}$ gegeben durch $f \mapsto (\sigma f)_{\sigma\in\Sigma}$.
Die Galoisgruppe $\mathrm{Gal}(\mathbb{C}|\mathbb{R})$ wird von der komplexen Konjugation F_∞, wobei $F_\infty(z) = \overline{z}$ ist, erzeugt. Man nennt F_∞ den *Frobenius* in Unendlich. Die Operation von F_∞ auf $K_{\mathbb{C}}$ ist gegeben durch $F_\infty(z_\sigma) = \overline{z}_{\overline{\sigma}}$, wobei $\overline{\sigma}$ die zu σ konjugierte Einbettung ist.

8.9. Definition. Der F_∞-invariante Fixmodul $K_{\mathbb{C}}^{F_\infty}$ von $K_{\mathbb{C}}$ heißt *Minkowski-Raum* und wird mit $K_{\mathbb{R}}$ bezeichnet. Wie oben bestehen Isomorphismen $K_{\mathbb{R}} \cong K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Beachte dabei daß als K-Modul $K_{\mathbb{R}} \ncong \prod_{\sigma\in\Sigma} \mathbb{R}$.

8.10. Proposition. *(i) Die Einbettung $\iota : K \to K_{\mathbb{C}}$ ist F_∞-invariant, d.h. $\iota(K) \in K_{\mathbb{R}}$.*
(ii) Für ganze Ideale $\mathfrak{a}$ von K ist $\iota(\mathfrak{a}) \subset K_{\mathbb{R}}$ ein Gitter.

Beweis. Es seien $\sigma_1, \dots, \sigma_{r_1}$ die reellen Einbettungen und $\sigma_{r_1+1}, \overline{\sigma}_{r_1+1}, \dots, \sigma_{r_1+r_2}, \overline{\sigma}_{r_1+r_2}$ die komplexen Einbettungen von K mit $n = r_1 + 2r_2$. Damit erhalten wir dann

$$\begin{aligned} F_\infty(\iota(f)) &= F_\infty\left(\sigma_1(f), \dots, \sigma_{r_1}(f), \sigma_{r_1+1}(f), \overline{\sigma}_{r_1+1}(f), \dots, \sigma_{r_1+r_2}(f), \overline{\sigma}_{r_1+r_2}(f)\right) \\ &= \left(\overline{\sigma}_1(f), \dots, \overline{\sigma}_{r_1}(f), \overline{\sigma_{r_1+1}(f)}, \overline{\sigma_{r_1+1}(f)}, \dots, \overline{\sigma_{r_1+r_2}(f)}, \overline{\sigma_{r_1+r_2}(f)}\right) \\ &= \left(\sigma_1(f), \dots, \sigma_{r_1}(f), \sigma_{r_1+1}(f), \overline{\sigma}_{r_1+1}(f), \dots, \sigma_{r_1+r_2}(f), \overline{\sigma}_{r_1+r_2}(f)\right) = \iota(f). \end{aligned}$$

Weil $\mathfrak{a}$ ein freier $\mathbb{Z}$-Modul vom Rang n und weil $\mathfrak{a} \otimes_{\mathbb{Z}} \mathbb{Q} = K \cong \mathbb{Q}^n$ ist, ist $\iota(\mathfrak{a})$ ein Gitter in $K_{\mathbb{R}} \cong \mathbb{R}^n$. □

8.11. Definition. Auf $\prod_\sigma \mathbb{R} \subseteq \prod_\sigma \mathbb{C}$ operiert F_∞ vermöge $x_\sigma \mapsto x_{\overline{\sigma}}$. Es bezeichne $\widehat{H}(K)$ den F_∞-invarianten Fixmodul $\left(\prod_\sigma \mathbb{R}\right)^{F_\infty}$. Die Elemente $\mathfrak{g} \in \widehat{H}(K)$ werden *Greenobjekte* genannt.

8.12. Auf dem $\mathbb{C}$-Vektorraum $K_{\mathbb{C}}$ haben wir eine Spurabbildung $\mathrm{Tr} : K_{\mathbb{C}} \to \mathbb{C}$ die durch die Summe der Koordinaten gegeben ist. Für die Spur gilt $\mathrm{Tr}_{K|\mathbb{Q}}(a) = \mathrm{Tr}(\iota(a))$ für alle $a \in K$.

Auf den Einheiten $K_{\mathbb{C}}^* = \{(x_\sigma)_{\sigma\in\Sigma} \in K_{\mathbb{C}} \,|\, x_\sigma \in \mathbb{C}^* \forall \sigma \in \Sigma\} = \prod_\sigma \mathbb{C}^*$ von $K_{\mathbb{C}}$ haben wir eine Normabbildung $\mathrm{Nm} : K_{\mathbb{C}}^* \to \mathbb{C}^*$ die durch das Produkt der Koordinaten gegeben ist. Für die Norm gilt $\mathrm{Nm}_{L|\mathbb{Q}}(f) = \mathrm{Nm}(\iota(f))$ für alle $f \in K^*$ und $\mathrm{Nm}(F_\infty(z)) = F_\infty(\mathrm{Nm}(z))$ für alle $z \in K_{\mathbb{C}}^*$.

Der Logarithmus $\log \mathbb{C}^* \to \mathbb{R}$ gegeben durch $z \mapsto \log|z|$ induziert einen Homomorphismus $\log : K_{\mathbb{C}}^* \to \prod_\sigma \mathbb{R}$. Wegen $\log(F_\infty(z)) = F_\infty(\log(z))$ für alle $z \in K_{\mathbb{C}}^*$ gilt $\log(K_{\mathbb{R}}^*) \subseteq \widehat{H}(K)$. Wir erhalten darum das folgende kommutative Diagramm:

$$\begin{array}{ccccc} & & \overset{\rho}{\frown} & & \\ K^* & \xrightarrow{\iota} & K_{\mathbb{R}}^* & \xrightarrow{\log} & \widehat{H}(K) \\ \downarrow{\scriptstyle \mathrm{Nm}_{K|\mathbb{Q}}} & & \downarrow{\scriptstyle \mathrm{Nm}} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ \mathbb{Q}^* & \xrightarrow{\iota} & \mathbb{R}^* & \xrightarrow{\log} & \mathbb{R}. \end{array}$$

Im folgenden bezeichne ρ immer die Komoposition $\iota \circ \log$.

Obige Betrachtungen lassen sich auf eine Körpererweiterung $L|K$ kanonisch fortsetzen und man erhält das analoge kommutative Diagramm:

$$\begin{array}{ccccc} & & \overset{\rho}{\frown} & & \\ L^* & \xrightarrow{\iota} & L_{\mathbb{R}}^* & \xrightarrow{\log} & \widehat{H}(L) \\ \downarrow{\scriptstyle \mathrm{Nm}_{L|K}} & & \downarrow{\scriptstyle \mathrm{Nm}_{L|K}} & & \downarrow{\scriptstyle \mathrm{Tr}_{L|K}} \\ K^* & \xrightarrow{\iota} & K_{\mathbb{R}}^* & \xrightarrow{\log} & \widehat{H}(K). \end{array}$$

8.13. Proposition. *(i) Der Raum der Greenobjekte $\widehat{H}(K)$ ist isomorph zu $\mathbb{R}^{r_1+r_2}$.*

(ii) Das Bild $\Gamma_K = \rho(\mathcal{O}_K^*)$ der Einheiten von $\mathcal{O}_K$ ist eine diskrete Untergruppe und liegt in der Hyperfläche $\widehat{H}(K)_0 = \{\mathfrak{g} \in \widehat{H}(K) \mid \mathrm{Tr}(\mathfrak{g}) = 0\} \subset \widehat{H}(K)$.
(iii) Es bezeichne $\mu(K)$ die Einheitswurzeln von K, dann ist die folgende Sequenz ist exakt

$$1 \longrightarrow \mu(K) \longrightarrow \mathcal{O}_K^* \longrightarrow \Gamma_K \longrightarrow 0.$$

Beweis. (i). Sei $x = (x_\sigma)_{\sigma\in\Sigma} \in \widehat{H}(K)$, dann gilt

$$F_\infty(x) = (x_{\sigma_1}, \ldots, x_{\overline{\sigma_{r_1+1}}}, x_{\sigma_{r_1+1}}, \ldots) = (x_{\sigma_1}, \ldots, x_{\sigma_{r_1+1}}, x_{\overline{\sigma_{r_1+1}}}, \ldots) = x.$$

Darum ist $x_{\sigma_r} = x_{\overline{\sigma_r}}$ für $r \geq r_1 + 1$ und da alle $x_\sigma \in \mathbb{R}$ sind, folgt somit $\widehat{H}(K) \cong \mathbb{R}^{r_1+r_2}$.
(ii) Sei $\varepsilon \in \mathcal{O}_K^*$, dann ist $\mathrm{Nm}(\varepsilon) = \pm 1$ wegen (1.12.1) und darum ist

$$\mathrm{Tr}(\rho(\varepsilon)) = \log(|\,\mathrm{Nm}(\varepsilon)|) = 0.$$

Wir betrachten die kompakte Menge $C = \{x \in \widehat{H}(K)_0 \,|\, |x_\sigma| \leq M\}$. Die Menge $\log^{-1}(C) = \{x \in K_\mathbb{R} \,|\, |x| \leq e^M\} \subset K_\mathbb{R}$ ist ebenfalls kompakt. Weil $\iota(\mathcal{O}_K)$ ein Gitter in $K_\mathbb{R}$ ist, kann es deshalb nur endlich viele $f \in \mathcal{O}_K$ geben mit $\rho(f) \in C$ und davon sind ebenfalls nur endlich viele von der Gestalt $\varepsilon \in \mathcal{O}_K^*$. Deshalb ist $\rho(\mathcal{O}_K^*)$ eine diskrete Untergruppe.
(iii). Der Kern der Abbildung $\mathcal{O}_K^* \to \Gamma_K$ ist gegeben durch die ε mit $|\sigma(\varepsilon)| = 1$ für alle $\sigma \in \Sigma$, also durch die Einheitswurzeln $\mu(K)$ in K. □
In Kapitel 12 werden wir den Dirichlet'schen Einheitensatz beweisen. Dieser besagt, daß $\mathrm{rk}(\mathcal{O}_K^*) = r_1 + r_2 - 1$ oder in anderen Worten:

$$\mathcal{O}_K^* \cong \mu(K) \times \mathbb{Z}^{r_1+r_2-1}.$$

9 Arithmetische Kurven

Wir wollen jetzt die Theorie der algebraischen Zahlkörper, die wir bislang mit Methoden der Algebra und Arithmetik untersucht haben auch aus geometrischer Sicht behandeln.

Die richtige Sprache dazu ist die Theorie der Schemata, wie sie von Grothendieck et. al. ($\sim$ 1960) entwickelt wurde. Wir wollen jetzt illustrieren, daß der Ring der ganzen Zahlen eines Zahlkörpers sich wie der Koordinatenring einer glatten affine Kurve verhält.

9.1. Definition. Eine *affine, ebene Kurve* C (definiert über $\mathbb{C}$) ist gegeben als die Nullstellenmenge eines irreduziblen Polynoms $f(x, y) \in \mathbb{C}[x, y]$. Der Ring $R_C = \mathbb{C}[x, y]/(f(x, y))$ wird der *Koordinatenring* von C genannt.

In der algebraischen Geometrie wird gezeigt, wie sich geometrische Eigenschaften von C in algebraische Eigenschaften von R_C übersetzen. (e.g. Fulton; Miranda; Forster)

9.2. Beispiele. Eine besonders gut untersuchte Klasse von Kurven sind die elliptische Kurven (e.g. Silverman: Elliptic curves; Knapp: Elliptic curves). Diese Kurven sind gegeben durch Gleichungen der Form $y^2 = p(x)$, für ein Polynom $p(x)$ mit $\deg(p(x)) = 3$.

Mit dem Befehl

```
plots[implicitplot]( f(x,y), x=a..b, y=c..d);
```

des Computerprogramms MAPLE lassen sich schnell reelle Bilder zeichnen.

9.3. Sei C affine, ebene Kurve, d.h. die Nullstellenmenge eines irreduziblen Polynomen $f \in \mathbb{C}[X,Y]$ und sei $R_C = \mathbb{C}[X,Y]/(f)$ der Koordinatenring von C. Die Punkte $P \in C$ entsprechen den maximalen Idealen $\mathfrak{m}_P = \{g \in R_C \mid g(P) = 0\}$ von R_C. Darum ist der Raum $\mathrm{Max}(R_C) = \{\text{maximale Ideale von } R_C\}$ von zentraler Bedeutung. Weil $R_C/\mathfrak{m}_P \cong \mathbb{C}$ ist, können wir jedes Element $g \in R_C$ vermöge der Zuordnung $g(\mathfrak{m}_P) := g \mod \mathfrak{m}_P$ als Funktion auf $\mathrm{Max}(R_C)$ betrachten; beachte: $g(\mathfrak{m}_P)$ entspricht gerade $g(P)$. Die abgeschlossenen Mengen auf $\mathrm{Max}(R_C)$ sind gegeben durch Nullstellenmengen der Elemente $g \in R_C$:

$$\begin{aligned} V(g) &= \{\mathfrak{m} \in \mathrm{Max}(R_C) \,|\, g(\mathfrak{m}) = 0\} \\ &= \{\mathfrak{m} \in \mathrm{Max}(R_C) \,|\, \mathfrak{m} \supseteq (g)\}. \end{aligned}$$

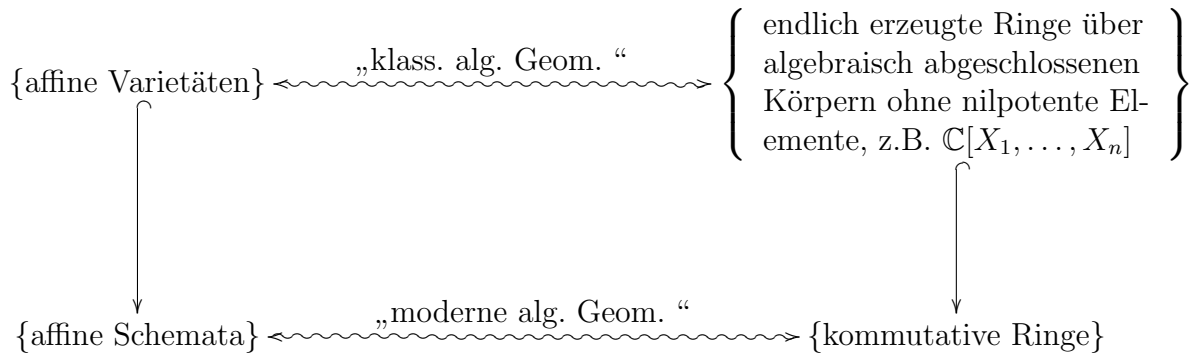
Beachte: entweder ist $\#V(g) < \infty$ oder $V(g) = \mathrm{Max}(R_C)$. Die somit erhaltene Topologie heißt Zariski Topologie. Die offenen Mengen sind dann von der Gestalt $U(g) = \mathrm{Max}(R_C) \setminus V(g)$.
Ein Punkt $P \in C$ heißt singulär, falls $\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0$, andernfalls heißt P regulär. Die Tangente an einem Punkt $P = (a,b) \in C$ ist gegeben durch die Gleichung

$$\frac{\partial f}{\partial x}(a,b) \cdot (X-a) + \frac{\partial f}{\partial y}(a,b) \cdot (Y-b) = 0.$$

Deshalb sind die singulären Punkte genau die Punkte deren Tangente nicht eindeutig ist. Ist P regulär, dann ist der lokale Ring $(R_C)_{\mathfrak{m}_p}$ ein diskreter Bewertungsring. Die Bewertung einer Funktion $g \in R_C$ auf $\mathrm{Max}(R_C)$ ist gerade die Verschwindungsordnung von g in P. Ein Kurve heißt glatt, bzw. $\mathrm{Max}(R_C)$ heißt regulär, falls kein Punkt singulär ist, bzw. alle $(R_C)_{\mathfrak{m}_P}$ diskrete Bewertungsringe sind. Wir fassen unsere Betrachtungen im folgenden Satz zusammen.

9.4. Satz. *Sei C eine glatte, ebene, affine Kurve über $\mathbb{C}$, dann ist der Koordinatenring R_C ein Dedekindring.*

9.5. Bemerkung. Auf ähnliche Art und Weise erhält man Bijektionen



9.6. Schemata. Die exakte Definition eines Schemas ist etwas technisch (siehe z.B. Kunz: Algebraische Geometrie; Eisenbud-Harris: The Geometry of Schemes; Hartshorne: Algebraic Geometry). Für unser Verständnis reicht folgende „grobe“ Beschreibung aus.

Was ist das Schema zu einen kommutativen Ring R:

Als Menge ist das Schema $\operatorname{Spec} R$ eines Ringes R gegeben durch $\operatorname{Spec} R = \{\text{Primideale } \mathfrak{p} \subseteq R\}$. Zum Beispiel ist $\operatorname{Spec} \mathbb{Z} = \{0, 2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots\}$. Die regulären Funktionen auf $\operatorname{Spec} R$ sind gegeben durch die $f \in R$ mit „Werten“ $f(\mathfrak{p}) = f \mod \mathfrak{p} \in R/\mathfrak{p}$ in dem Punkt $\mathfrak{p}$.

Die Topologie auf $\operatorname{Spec} R$ ist die Zariskitopologie, d.h. jede Teilmenge $S \subset R$ bestimmt eine abgeschlossene Menge

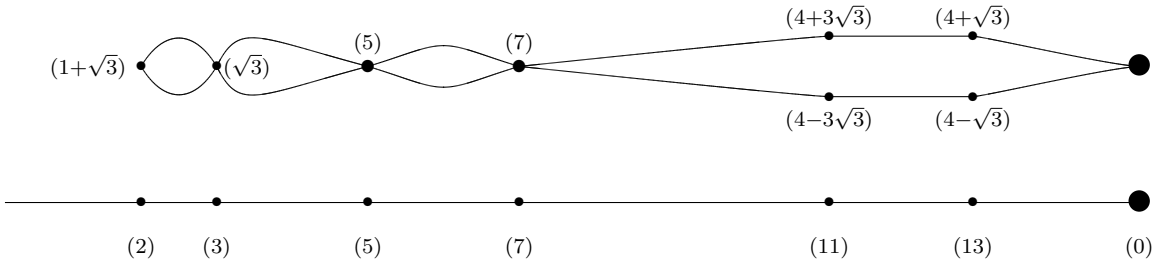
$$\begin{aligned} V(S) &= \{\mathfrak{p} \in \operatorname{Spec} R \mid f(\mathfrak{p}) = 0 \text{ für alle } f \in S\} \\ &= \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \supset S\}. \end{aligned}$$

Falls $0 \neq f \in R$, dann ist $X_f \subset X = \operatorname{Spec} R$ mit $X_f = \operatorname{Spec} R \setminus V(f) = \operatorname{Spec} R_f = \operatorname{Spec} R[1/f]$, eine ausgezeichnete offene Umgebung von X. Man kann zeigen, dass die X_f eine Basis der Topologie auf X bilden. Beachte: X_f ist wiederum selbst ein Schema. Man zeigt, daß sich die X_f in einem geeigneten Sinn verkleben lassen („die regulären Funktionen auf offene Mengen bilden eine Garbe“).

9.7. Definition. In Analogie zu den ebenen, affinen Kurven über $\mathbb{C}$, bezeichnet man deshalb $\operatorname{Spec} R$ für Teilringe R eines algebraischen Zahlkörpers K, deren Quotientenkörper gleich K ist, als *arithmetische Kurven.*

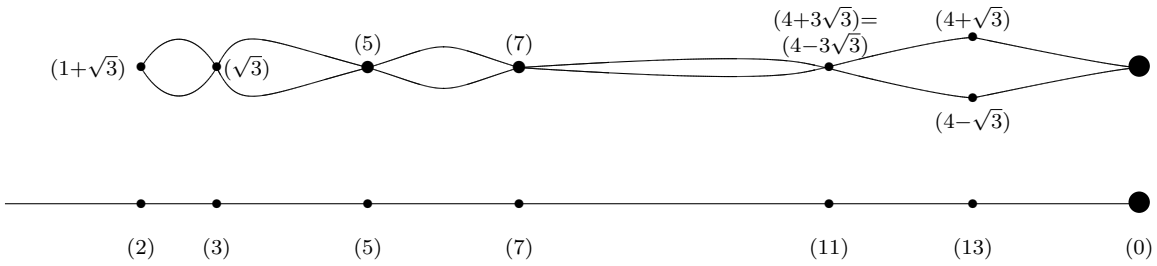
Ringerweiterungen solcher Ringe entsprechen dann Überlagerungen von arithmetischen Kurven.

Als Beispiel betrachten wir die zweifache Überlagerung $\operatorname{Spec} \mathbb{Z}[\sqrt{3}]$ von $\operatorname{Spec} \mathbb{Z}$, also die Fasern der Projektion $\pi : \operatorname{Spec} \mathbb{Z}[\sqrt{3}] \longrightarrow \operatorname{Spec} \mathbb{Z}$:



Die Punkte, die die Ideale (5) bzw. (7) $\in \operatorname{Spec} \mathbb{Z}[\sqrt{3}]$ darstellen, sind dicker, weil im Gegensatz zu den anderen dargestellten Primidealen von $\operatorname{Spec} \mathbb{Z}[\sqrt{3}]$ die jeweiligen Restklassenkörper $\mathbb{Z}[\sqrt{3}]/(\sqrt{5})$ bzw. $\mathbb{Z}[\sqrt{3}]/(\sqrt{7})$ quadratische Erweiterungen der Restklassenkörper $\mathbb{F}_5$ bzw. $\mathbb{F}_7$ sind.

Im Vergleich dazu ist für die zweifache Überlagerung $\operatorname{Spec} \mathbb{Z}[11\sqrt{3}]$ von $\operatorname{Spec} \mathbb{Z}$ die Primstelle (11) nicht mehr unverzweigt, da die Ideale $(4 + 3\sqrt{3})$ und $(4 - 3\sqrt{3})$ in $\operatorname{Spec} \mathbb{Z}[11\sqrt{3}]$ zusammenfallen:



In der letzten Abbildung ist z.B. mit $(1+\sqrt{3})$ natürlich der Durchschnitt $(1+\sqrt{3})\cap\mathbb{Z}[11\sqrt{3}]$, also die Faser $\pi^{-1}(2)$ der Projektion $\pi : \operatorname{Spec}\mathbb{Z}[11\sqrt{3}] \longrightarrow \operatorname{Spec}\mathbb{Z}$ gemeint.

9.8. Übung. (i) Zeichne weitere Beispiele und untersuche dabei die Singularitäten. Nimm z.B. $\mathbb{Z}[27\sqrt{3}]$ anstelle von $\mathbb{Z}[11\sqrt{3}]$.

(ii) Zeige: eine arithmetische Kurve ist glatt genau dann, wenn R der Ring der ganzen Zahlen von K ist.

9.9. Chowgruppen. Sei R ein noetherscher Integritätsbereich mit Quotientenkörper K. Ein *Divisor* auf $\operatorname{Spec} R$ ist eine formale Summe

$$D = \sum_{\mathfrak{p}\in\operatorname{Max}(R)} a_{\mathfrak{p}}\mathfrak{p}$$

von abgeschlossenen Punkten $\mathfrak{p}$, d.h. $\mathfrak{p}$ ist ein maximales Ideal, auf $\operatorname{Spec} R$, wobei fast alle $a_{\mathfrak{p}} = 0$ sind. Die Gruppe der Divisoren auf $\operatorname{Spec} R$ ist

$$Z^1(R) = \left\{ \sum_{\mathfrak{p}\in\operatorname{Max}(R)} a_{\mathfrak{p}}\mathfrak{p} \mid \text{ fast alle } a_{\mathfrak{p}} = 0 \right\}$$

versehen mit der offensichtlichen Addition. Jede reguläre Funktion $f \in K^*$ auf $\operatorname{Spec} R$ bestimmt einen Divisor

$$\operatorname{div}(f) = \sum \operatorname{ord}_{\mathfrak{p}}(f)\mathfrak{p}$$

und Divisoren der Form $\operatorname{div}(f)$ heißen *Hauptdivisoren* . Hierbei ist, falls $f = \frac{a}{b}$ mit $a, b \in R$,

$$\operatorname{ord}_{\mathfrak{p}}(f) = \ell_{R_{\mathfrak{p}}}(R_{\mathfrak{p}}/aR_{\mathfrak{p}}) - \ell_{R_{\mathfrak{p}}}(R_{\mathfrak{p}}/bR_{\mathfrak{p}}),$$

wobei $\ell_{R_{\mathfrak{p}}}(M)$ die Länge eines $R_{\mathfrak{p}}$-Moduls M bezeichnet, das ist die maximale Länge einer echt absteigenden Kette

$$M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_\ell = 0$$

von $R_{\mathfrak{p}}$-Untermoduln. Weil die Längenfunktion auf kurzen exakten Sequenzen additiv ist, d.h. da aus

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

$\ell(M') + \ell(M'') = \ell(M)$ folgt, erhalten wir einen Homomorphismus $\operatorname{div} : K^* \to Z^1(R)$. Divisoren der Form $\operatorname{div}(f)$ heißen Hauptdivisoren und

$$Rat^1(R) = \{\operatorname{div}(f) \mid f \in K^*\} \subset Z^1(R)$$

bezeichnet die Untergruppe der Hauptdivisoren. Zwei Divisoren $D_1, D_2 \in Z^1(R)$, die sich um einen Hauptdivisor unterscheiden, heißen rational äquivalent. Die Quotientengruppe

$$CH^1(R) = Z^1(R)/Rat^1(R)$$

heißt die *erste Chowgruppe* von R.

9.10. Satz. *Sei R ein Dedekindring, dann besteht ein kanonischer Isomorphismus*

$$\begin{aligned} CH^1(R) &\cong Cl_K \\ D &\mapsto \Pi \mathfrak{p}^{a_\mathfrak{p}}. \end{aligned}$$

Beweis. In R ist jedes Primideal $\mathfrak{p} \neq 0$ maximal und jedes Ideal $\mathfrak{a}$ hat eine eindeutige Primidealzerlegung $\mathfrak{a} = \prod_{\mathfrak{p}\in\operatorname{Max}(R)} \mathfrak{p}^{a_\mathfrak{p}}$, wobei fast alle $a_\mathfrak{p} = 0$ sind. Wir haben bereits gezeigt, daß $\mathfrak{a}$ durch die Angabe der $a_\mathfrak{p}$ eindeutig bestimmt ist. Die Abbildung $J_K \to Z^1(R)$ gegeben durch $\mathfrak{a} = \prod_{\mathfrak{p}\in\operatorname{Max}(R)} \mathfrak{p}^{a_\mathfrak{p}} \mapsto \sum_{\mathfrak{p}\in\operatorname{Max}(R)} a_\mathfrak{p}\mathfrak{p}$ ist somit ein Isomorphismus. Es genügt somit zu zeigen, daß das folgende Diagram kommutiert

$$\begin{array}{ccc} K^* & & \\ {\scriptstyle ()}\downarrow & \searrow^{\operatorname{div}} & \\ J_K & \xrightarrow{\sim} & Z^1(R), \end{array}$$

d.h. die Bewertung $\nu_\mathfrak{p} \colon K^* \to \mathbb{Z}$ stimmt mit $\operatorname{ord}_\mathfrak{p} : K^* \to \mathbb{Z}$ überein. Per Definition ist $\nu_\mathfrak{p}(a)$ für ein $a \in R \setminus \{0\}$ der Exponent ν gegeben durch $a\mathcal{O}_\mathfrak{p} = \mathfrak{m}_\mathfrak{p}^\nu$, wobei $\mathfrak{m}_\mathfrak{p}$ das maximale Ideal des diskreten Bewertungsring $\mathcal{O}_\mathfrak{p}$ ist. Da

$$\mathcal{O}_\mathfrak{p}/a\mathcal{O}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}/\mathfrak{m}^\nu \supset \underbrace{\mathfrak{m}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}^\nu \supsetneq \cdots \supsetneq \mathfrak{m}_\mathfrak{p}^\nu/\mathfrak{m}_\mathfrak{p}^\nu = 0}_{v-\text{mal}},$$

ist somit $\nu = \operatorname{ord}_\mathfrak{p}(a)$. Der allgemeine Fall $f = \frac{a}{b} \in K^*$ folgt nun offensichtlich. □

??? `projektive Kurven, Residuenformel etc.`

10 Arithmetische Chowringe

10.1. Definition. Sei K ein algebraischer Zahlkörper und $\mathcal{O}_K$ sein Ring der ganzen Zahlen. Es sei $Z^1(\mathcal{O}_K)$ die Menge der Divisoren auf Spec $\mathcal{O}_K$. Die Elemente der Menge

$$\widehat{Z}^1(\mathcal{O}_K) = \{(Z, \mathfrak{g}) \mid Z \in Z^1(\mathcal{O}_K),\ \mathfrak{g} =\in \widehat{H}(K)\}$$

heißen *arithmetische Divisoren*. Die komponentenweise Addition macht $\widehat{Z}^1(\mathcal{O}_K)$ zu einer abelschen Gruppe. Die Abbildung $K^* \to \widehat{Z}^1(\mathcal{O}_K)$ gegeben durch

$$f \mapsto \widehat{\operatorname{div}}(f) = (\operatorname{div}(f), (-\log|\sigma(f)|)_{\sigma\in\Sigma})$$

ist ein Homomorphismus von Gruppen dessen Bild die mit $\widehat{Rat}^1(\mathcal{O}_K)$ bezeichnete Untergruppe von $\widehat{Z}^1(\mathcal{O}_K)$ ist. Die Elemente von $\widehat{Rat}^1(\mathcal{O}_K)$ heißen *arithmetische Hauptdivisoren* (oder auch rationale arithmetische Zykel).
Die Quotientengruppe

$$\widehat{\mathrm{CH}}^1(\mathcal{O}_K) := \widehat{Z}^1(\mathcal{O}_K)/\widehat{Rat}^1(\mathcal{O}_K)$$

heißt *erste arithmetische Chowgruppe* von $\mathcal{O}_K$.

10.2. Bemerkung. Für beliebige arithmetische Zykel $(Z, \mathfrak{g})$ besteht keine Relation zwischen dem Zykel und dem Greenobjekt. Wir halten jedoch fest, daß bei der analogen Konstruktion arithmetischer Chowgruppen von höherdimensionalen arithmetischen Varietäten sehr wohl eine nichttriviale Beziehung bestehen muß.

10.3. Satz. *Folgende Sequenz ist exakt:*

$$1 \longrightarrow \mu(K) \xrightarrow{i} \mathcal{O}_K^* \xrightarrow{\rho} \widehat{H}(K) \xrightarrow{a} \widehat{\mathrm{CH}}^1(\mathcal{O}_K) \xrightarrow{\zeta} Cl_K \longrightarrow 1\,,$$

hierbei sind i die Identität, $a([\mathfrak{g}]) = [0, -\mathfrak{g}]$ und $\zeta([\sum_{\mathfrak{p}\in\mathrm{Max}(\mathcal{O}_K)} a_\mathfrak{p}\mathfrak{p}, \mathfrak{g}]) = [\prod_{\mathfrak{p}\in\mathrm{Max}(\mathcal{O}_K)} \mathfrak{p}^{-a_\mathfrak{p}}]$.

Beweis: $\ker(i) = 1$ klar.
$\mathrm{Im}(i) = \ker(\rho)$. „$\subset$“: Da $\log|\sigma\zeta| = 0$ für alle $\sigma \in \Sigma$, ist diese Richtung klar. „$\supset$“: Ist $|\sigma(\epsilon)| = 1$ dann folgt $\sigma(\epsilon) = e^{2\pi i r}$ mit $r \in \mathbb{R}$. Weil jedoch $\rho(\mathcal{O}_K^*)$ diskret in $\widehat{H}(K)$ ist, ist $r \in \mathbb{Q}$, also $\epsilon \in \mu(K)$.
$\mathrm{Im}(\rho) = \ker(a)$. „$\subset$“: Sei $\epsilon \in \mathcal{O}_K^*$, dann ist $\operatorname{div}\epsilon = 0$ und deshalb ist $(\operatorname{div}(\epsilon), \mathfrak{g}(\epsilon)) = (0, -\rho(\epsilon)) = a(\rho(\epsilon)) \in \widehat{\mathrm{Rat}}^1(\mathcal{O}_K)$. „$\supset$“ klar, weil $\rho(1) = 0$.
$\mathrm{Im}(a) = \ker(\zeta)$ klar.
$\mathrm{Im}(\zeta) = Cl_K$ klar. □

10.4. Bemerkung. (i) Mittels des „5-er Lemmas“ erhalten wir einen nicht kanonischen Isomorphismus

$$\widehat{\mathrm{CH}}^1(\mathcal{O}_K) \cong \widehat{H}(K)/\Gamma_K \oplus Cl_K.$$

(ii) Mittels obiger exakter Sequenz überzeugt man sich leicht, daß $\widehat{\mathrm{CH}}^1(\mathbb{Z}) \cong \mathbb{R}$ ist.

10.5. Definition. Die *arithmetische Gradabbildung*

$$\widehat{\deg} : \widehat{Z}^1(\mathcal{O}_K) \longrightarrow \mathbb{R}$$

ist definiert durch

$$\widehat{\deg}\Big(\sum_{\mathfrak{p}\in\mathrm{Max}(\mathcal{O}_K)} a_\mathfrak{p}\mathfrak{p}, (g_\sigma)_{\sigma\in\Sigma}\Big) = \sum_{\mathfrak{p}\in\mathrm{Max}(\mathcal{O}_K)} a_\mathfrak{p} \log\big(\#\mathcal{O}_K/\mathfrak{p}\big) + \sum_\sigma g_\sigma.$$

10.6. Proposition. *Die arithmetische Gradabbildung induziert einen Gruppenhomomorphismus* $\widehat{\deg} : \widehat{\mathrm{CH}}^1(\mathcal{O}_K) \longrightarrow \mathbb{R}$.

Beweis: Wir müssen zeigen $\widehat{\deg}(\widehat{Rat}^1(\mathcal{O}_K)) = 0$. Mit Hilfe der Produktformel erhalten wir

$$\begin{aligned}
\widehat{\deg}(\widehat{\mathrm{div}}(f)) &= \sum_{\mathfrak{p}} \nu_{\mathfrak{p}}(f) \log(\#(\mathcal{O}_k/\mathfrak{p})) + \sum_{\sigma} -\log|\sigma(f)| \\
&= \sum_{\mathfrak{p}} \nu_{\mathfrak{p}}(f) \log(\mathrm{Nm}(\mathfrak{p})) + \sum_{\sigma} -\log|\sigma(f)| \\
&= \log\left(\prod_{\mathfrak{p}} \mathrm{Nm}(\mathfrak{p})^{\nu_{\mathfrak{p}}(f)} \prod_{\sigma} |\sigma(f)|^{-1}\right) \\
&= \log\left(\prod_{\mathfrak{p}} |f|_{\mathfrak{p}}^{-1} \prod_{\sigma} |\sigma(f)|^{-1}\right) \\
&= \log(1) = 0.
\end{aligned}$$

□

10.7. Definition. Der *arithmetische Chowring* $\widehat{\mathrm{CH}}(\mathcal{O}_K)$ ist definiert als die additive Gruppe

$$\widehat{\mathrm{CH}}(\mathcal{O}_K) = \mathbb{Z} \oplus \widehat{\mathrm{CH}}^1(\mathcal{O}_K)$$

versehen mit der Multiplikation $\widehat{\mathrm{CH}}(\mathcal{O}_K) \times \widehat{\mathrm{CH}}(\mathcal{O}_K) \to \widehat{\mathrm{CH}}(\mathcal{O}_K)$

$$(r_1, d_1) \cdot (r_1, d_2) = (r_1 r_2, r_1 d_2 + r_2 d_1).$$

Man nennt die Multiplikation auch *arithmetische Schnittpaarung.*

10.8. Bemerkung. Die erste Komponente von $\widehat{\mathrm{CH}}(\mathcal{O}_K)$ wird von der Klasse des Ideals (0) erzeugt. Für „gewisse“ höher-dimensionale Ringe R, d.h. Ringe für die Primidealketten $\mathfrak{p}_1 \supset \mathfrak{p}_2 \supset \ldots$ der Länge ≥ 1 existieren, wie z.B. $\mathbb{Z}[X]$ und $(\zeta, x) \supset (\zeta)$, gibt es höhere arithmetische Chowgruppen $\widehat{CH}^*(R)$ und $\widehat{CH}(R) = \oplus_p \widehat{\mathrm{CH}}^p(R)$ besitzt eine nicht triviale arithmetische Schnittpaarung.

10.9. Definition. Sei $L|K \hookrightarrow L$ eine Erweiterung von Zahlkörpern. Dann wird eine *Pullback Abbildung*

$$i^* : \widehat{\mathrm{CH}}(\mathcal{O}_K) \longrightarrow \widehat{\mathrm{CH}}(\mathcal{O}_L)$$

definiert vermöge der folgenden Zuordnung von arithmetischen Zykeln

$$i^*(r, (D, \mathfrak{g})) = (r, (i^*D, i^*\mathfrak{g})) \in \mathbb{Z} \oplus \widehat{Z}^1(\mathcal{O}_L).$$

Hierbei ist

$$i^*D = \sum_{\mathfrak{p} \in \mathrm{Max}(\mathcal{O}_K)} a_{\mathfrak{p}} i^*\mathfrak{p} = \sum_{\mathfrak{P} \in \mathrm{Max}(\mathcal{O}_L)} a_{\mathfrak{p}} \cdot \sum_{\mathfrak{P}|\mathfrak{p}\mathcal{O}_L} e_{\mathfrak{P}}\mathfrak{P},$$

in der Summe ist $e_{\mathfrak{P}}$ der Verzweigungsindex von $\mathfrak{P}$ über $\mathfrak{p}$, d.h. $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^{e_{\mathfrak{P}}} \cdot \mathfrak{a}$ mit $(\mathfrak{P}, \mathfrak{a}) = \mathcal{O}_L$. Weiter ist

$$i^*\mathfrak{g} = (i^*\mathfrak{g}_\sigma)_{\sigma\in\Sigma_K} = (\mathfrak{g}_{\tau|_K})_{\tau\in\Sigma_L},$$

bei der letzten Gleichheit erinnern wir an die Tatsache, daß $\tau|_K \in \Sigma_K$ für alle $\tau \in \Sigma_L$.

10.10. Proposition. *Das Pull-back i^* ist wohldefiniert.*

Beweis. Da i^* linear ist, genügt es zu zeigen, daß $i^*\widehat{Rat}^1(\mathcal{O}_K) \subseteq \widehat{Rat}^1(\mathcal{O}_L)$. Sei $f \in K^*$, dann ist

$$\begin{aligned}
i^*\widehat{\operatorname{div}}_{\mathcal{O}_K}(f) &= (i^*\operatorname{div}_{\mathcal{O}_K}(f), i^*\mathfrak{g}(f)) \\
&= \left(\sum_{\mathfrak{p}} \nu_{\mathfrak{p}}(f) i^*\mathfrak{p}, (i^*(-\log|\sigma(f)|))_{\sigma\in\Sigma_K}\right) \\
&= \left(\sum_{\mathfrak{p}} \nu_{\mathfrak{p}}(f) \sum_{\mathfrak{P}|\mathfrak{p}\mathcal{O}_L} e_{\mathfrak{P}}\mathfrak{P}, \left((-\log|\sigma(f)|)_{\tau|_K=\sigma}\right)_{\tau\in\Sigma_L}\right) \\
&= \left(\sum_{\mathfrak{P}} \nu_{\mathfrak{P}}(f)\mathfrak{P}, (-\log|\tau(f)|)_{\tau\in\Sigma_L}\right) \\
&= (\operatorname{div}_{\mathcal{O}_L}(f), \mathfrak{g}_{\mathcal{O}_L}(f)) = \widehat{\operatorname{div}}_{\mathcal{O}_L}(f).
\end{aligned}$$

□

10.11. Bemerkung. Gegeben sei folgendes kommutatives Diagram von Inklusionen von Zahlkörpern

$$\begin{array}{ccc} K & \xhookrightarrow{\ i\ } & L \\ & {\scriptstyle h}\searrow & \downarrow{\scriptstyle j} \\ & & M \end{array},$$

dann gilt für die Pullbackabbildungen $h^* = j^*\circ i^*$. Dies folgt aus den leicht zu überprüfenden Identitäten $j^*(i^*D) = h^*D$ und $j^*(i^*\mathfrak{g}) = h^*\mathfrak{g}$.

10.12. Definition. Sei $L|K$ eine Erweiterung von Zahlkörpern. Dann wird eine *Push-forward Abbildung*

$$i_*\colon \widehat{\mathrm{CH}}(\mathcal{O}_L) \longrightarrow \widehat{\mathrm{CH}}(\mathcal{O}_K)$$

definiert vermöge der Zuordnung von arithmetischen Zykeln

$$i_*(r, (D, \mathfrak{g})) = (r[L:K], (i_*D, i_*\mathfrak{g})),$$

wobei

$$\begin{aligned}
i_*D &= \sum_{\mathfrak{P}} a_{\mathfrak{P}} i_*\mathfrak{P} = \sum_{\mathfrak{P}} a_{\mathfrak{P}} \operatorname{Nm}_{L|K}(\mathfrak{P}) \\
&= \sum_{\mathfrak{p}} a_{\mathfrak{P}}[\mathfrak{P}:\mathfrak{p}]\mathfrak{p}
\end{aligned}$$

und

$$i_*\mathfrak{g} = \left(\sum_{\substack{\tau\in\sigma_L \\ \tau|_K=\sigma}} g_\tau \right)_{\sigma\in\Sigma_K} .$$

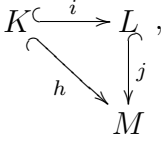
10.13. Proposition. *Das Push-forward i_* ist wohldefiniert.*

Beweis. Man sieht leicht, daß i_* linear ist. Es genügt zu zeigen $i_*\widehat{Rat}^1(\mathcal{O}_L) \subset \widehat{Rat}^1(\mathcal{O}_K)$. Dazu sei $f \in L^*$, dann ist

$$\begin{aligned} i_*\widehat{\operatorname{div}}_{\mathcal{O}_L}(f) &= (i_* \operatorname{div}_{\mathcal{O}_L}(f),\ i_*\mathfrak{g}(f)) \\ &= \left(\sum_{\mathfrak{P}} \nu_{\mathfrak{P}} i_*\mathfrak{P},\ i_*\mathfrak{g}(f) \right) \\ &= \left(\sum_{\mathfrak{P}} \nu_{\mathfrak{p}} \operatorname{Nm}_{L|K} \mathfrak{P},\ \left(\sum_{\tau|_K=\sigma} -\log|\tau(f)| \right)_{\sigma\in\Sigma_K} \right) \\ &= \big(\operatorname{div}(\operatorname{Nm}_{L|K}(f)),\ \mathfrak{g}(\operatorname{Nm}_{L|K}(f))\big) \\ &= \widehat{\operatorname{div}}(\operatorname{Nm}_{L|K}(f)). \end{aligned}$$

□

10.14. Bemerkung. Gegeben sei folgendes ein kommutatives diagram von Inklusionen von Zahlkörpern



dann gilt: $h_*i_* \circ j_*$.

10.15. Satz.

(i) Sei $L|K$ eine Erweiterung von Zahlkörpern, dann ist $i^* : \widehat{\mathrm{CH}}(\mathcal{O}_K) \longrightarrow \widehat{\mathrm{CH}}(\mathcal{O}_L)$ ein Ringhomomorphismus.

(ii) Es gilt $i_* \circ i^* = [L : K]$ und es besteht die Projektionsformel

$$i_*(i^*(\kappa) \cdot \lambda) = \kappa \cdot i_*(\lambda),$$

für alle $\kappa \in \widehat{\mathrm{CH}}(\mathcal{O}_K)$ und $\lambda \in \widehat{\mathrm{CH}}(\mathcal{O}_L)$.

Beweis. (i) Wegen

$$\begin{aligned} i^*(r_1,(D_1,\mathfrak{g}_1)) \cdot i^*(r_2,(D_2,\mathfrak{g}_2)) &= (r_1r_2, r_1(i^*D_2, i^*\mathfrak{g}_2) + r_2(i^*D_1, i^*\mathfrak{g}_1)) \\ &= i^*(r_1r_2, r_1(D_2,\mathfrak{g}_2) + r_2(D_1,\mathfrak{g}_1)) \\ &= i^*((r_1,(D_1,\mathfrak{g}_1)) \cdot (r_2,(D_2,\mathfrak{g}_2)) \end{aligned}$$

ist i^* ein Ringhomomorphismus.
(ii) Sei $(r,(D,\mathfrak{g}))\in\widehat{\mathrm{CH}}(\mathcal{O}_K)$. Wir zeigen die Gleichheit $i_*i^*(r,(D,\mathfrak{g}))=[L:K](r,(D,\mathfrak{g}))$ komponentenweise. Man sieht sofort $i_*i^*r=[L:K]\cdot r$. Sei $\mathfrak{a}=\prod_{\mathfrak{p}}\mathfrak{p}^{a_\mathfrak{p}}$ das Ideal zu $D=\sum_{\mathfrak{p}}a_\mathfrak{p}\cdot\mathfrak{p}$. Dann ist $\mathrm{Nm}_{L|K}(\mathfrak{a}\mathcal{O}_L)$ das Ideal zu i_*i^*D. Da $\mathrm{Nm}_{L|K}(\mathfrak{a}\mathcal{O}_L)=\mathfrak{a}^{[L:K]}$ ist, gilt somit $i_*i^*D=[L:K]D$. Die Identität $i_*i^*\mathfrak{g}=[L:K]\mathfrak{g}$ folgt aus einer leichten Rechnung. Sei $\kappa=(r_1,(D_1,\mathfrak{g}_1))\in\widehat{\mathrm{CH}}(\mathcal{O}_K)$ und $\lambda=(r_2,(D_2,\mathfrak{g}_2))\in\widehat{\mathrm{CH}}(\mathcal{O}_L)$, dann gilt wegen $i_*i^*=[L:K]$, daß

$$\begin{aligned}i_*(i^*\kappa\cdot\lambda)&=i_*\left(r_1r_2,r_1(D_2,\mathfrak{g}_2)+r_2(i^*D_1,i^*\mathfrak{g}_1)\right)\\&=\left([L:K]r_1r_2,r_1(i_*D_2,i_*\mathfrak{g}_2)+r_2(i_*i^*D_1,i_*i^*\mathfrak{g}_1)\right)\\&=\left([L:K]r_1r_2,r_1(i_*D_2,i_*\mathfrak{g}_2)+[L:K]r_2(D_1,\mathfrak{g}_1)\right)\\&=(r_1,(D_1,\mathfrak{g}_1))\cdot i_*\left(r_2,(D_2,\mathfrak{g}_2)\right).\end{aligned}$$

□

10.16. Bemerkung. Beachte i_* ist kein Ringhomomorphismus!

10.17. Funktorialität der arithmetischen Chowgruppen: Als einen Beitrag zur mathematischen Allgemeinbildung weisen wir darauf hin, daß die arithmetischen Chowgruppen funktoriell sind.

10.18. Proposition. *Sei ZK die Kategorie der Zahlkörper.*

(i) *Der arithmetische Chowring $\widehat{\mathrm{CH}}$ ist ein kovarianter Funktor von der Kategorie ZK in die Kategorie der Ringe, wenn einem Morphismus $i:K\hookrightarrow L$ der Morphismus $i^*:(\widehat{\mathrm{CH}}(\mathcal{O}_K))\to\widehat{\mathrm{CH}}(\mathcal{O}_L)$ zugeordnet wird.*

(ii) *Die arithmetische Chowgruppe $\widehat{\mathrm{CH}}$ ist ein kontravarianter Funktor von der Kategorie der Zahlkörper in die Kategorie der abelschen Gruppen, wenn einem Morphismus $i:K\hookrightarrow L$ der Morphismus $i_*\colon\widehat{\mathrm{CH}}(\mathcal{O}_L)\to\widehat{\mathrm{CH}}(\mathcal{O}_K)$ zugeordnet wird.*

Beweis. Übung (Tip: Überprüfe die Definitionen aus Appendix B). □

11 Vollständige Idealklassengruppen

11.1. Definition. Sei K ein Zahlkörper und $\mathcal{O}_K$ sein Ring der ganzen Zahlen. Ein Paar $\overline{\mathfrak{a}}=(\mathfrak{a},(r_\sigma)_{\sigma\in\sum})$, wobei $r_\sigma\in\mathbb{R}^+$ für alle Einbettungen $\sigma\in\Sigma$ und $(r_\sigma)_{\sigma\in\Sigma}\in K_\mathbb{R}$, heißt *vollständiges Ideal*. Vermöge der Multiplikation

$$\begin{aligned}\overline{\mathfrak{a}}\cdot\overline{\mathfrak{b}}&=(\mathfrak{a},(r_\sigma)_{\sigma\in\Sigma})\cdot(\mathfrak{b},(s_\sigma)_{\sigma\in\Sigma})\\&=(\mathfrak{a}\cdot\mathfrak{b},(r_\sigma\cdot s_\sigma)_{\sigma\in\Sigma}),\end{aligned}$$

wobei die Multiplikation auf $K_{\mathbb{R}}$ komponentenweise gegeben ist, erhalten wir die *vollständige Idealgruppe* $\widehat{J}(\mathcal{O}_K)$. Für ein vollständiges Ideal $\overline{\mathfrak{a}} = (\mathfrak{a}, (r_\sigma)_{\sigma\in\Sigma})$ definieren wir $\mathfrak{a}_f = (\mathfrak{a}, (1)_{\sigma\in\Sigma})$ für den „endlichen Anteil“ und $\mathfrak{a}_\infty = ((1), (r_\sigma)_{\sigma\in\Sigma})$ für den „archimedischen Anteil“, damit gilt dann

$$\overline{\mathfrak{a}} = \mathfrak{a}_f \cdot \mathfrak{a}_\infty.$$

Wir werden gelegentlich auch $\mathfrak{a}_f$ mit $\mathfrak{a}$ und $\mathfrak{a}_\infty$ mit $(r_\sigma)_{\sigma\in\Sigma}$ identifizieren.
Einem Element $a \in K^*$ ordnen wir das *vollständige Hauptideal*

$$\overline{(a)} = \big((a), (|\sigma(a)|^{-1})_{\sigma\in\Sigma}\big)$$

zu und wir bezeichnen die Untergruppe der vollständigen Hauptideale mit $\widehat{P}(\mathcal{O}_K)$.

11.2. Definition. Die *vollständige Idealklassengruppe* $\widehat{Cl}(\mathcal{O}_K)$ ist definiert als der Quotient

$$\widehat{Cl}(\mathcal{O}_K) = \widehat{J}(\mathcal{O}_K)/\widehat{P}(\mathcal{O}_K).$$

11.3. Satz. *Die Abbildung* $\widehat{c}_1 : \widehat{J}(\mathcal{O}_K) \to \widehat{Z}^1(\mathcal{O}_K)$ *gegeben durch*

$$\overline{\mathfrak{a}} = (\mathfrak{a}, (r_\sigma)_{\sigma\in\Sigma}) \mapsto \widehat{c}_1(\overline{\mathfrak{a}}) = \left(\sum_{\mathfrak{p}\in \operatorname{Spec}\mathcal{O}_K} -\nu_{\mathfrak{p}}(\mathfrak{a})\mathfrak{p}, (-\log(r_\sigma))_{\sigma\in\Sigma} \right)$$

induziert einen Isomorphismus

$$\widehat{Cl}(\mathcal{O}_K) \cong \widehat{CH}^1(\mathcal{O}_K).$$

Man nennt $\widehat{c}_1(\overline{\mathfrak{a}})$ die *erste arithmetische Chernklasse* von $\overline{\mathfrak{a}}$.
Beweis. Die Abbildung

$$\begin{aligned} \widehat{Z}^1(\mathcal{O}_K) &\to \widehat{J}(\mathcal{O}_K) \\ D = (\Sigma a_{\mathfrak{p}}\mathfrak{p}, (r_\sigma)_{\sigma\in\Sigma}) &\mapsto \overline{\mathcal{O}(D)} = \left(\prod_{\mathfrak{p}\in\operatorname{Spec}\mathcal{O}_K} \mathfrak{p}^{-a_{\mathfrak{p}}}, (e^{-r_\sigma})_{\sigma\in\Sigma} \right) \end{aligned}$$

ist offensichtlich invers zu $\widehat{c}_1$. Es folgt $\widehat{Z}^1(\mathcal{O}_K) \cong \widehat{J}(\mathcal{O}_K)$. Man sieht leicht, daß auch $\widehat{Rat}^1(\mathcal{O}_K) \cong \widehat{P}(\mathcal{O}_K)$ gilt, woraus die Behauptung folgt. □

11.4. Sei $\overline{\mathfrak{a}} = \mathfrak{a}_f \cdot \mathfrak{a}_\infty$ ein vollständiges Ideal, dann bestimmt $\mathfrak{a}_f$ vermöge der kanonischen Einbettung $\iota\colon K \to K_{\mathbb{R}}$ ein Gitter $\iota(\mathfrak{a}_f)$. Des weiteren bestimmt $\mathfrak{a}_\infty$ eine lineare Abbildung auf $K_{\mathbb{R}}$, nämlich

$$\begin{aligned} &\mathfrak{a}_\infty\colon K_{\mathbb{R}} \to K_{\mathbb{R}} \\ &(k_\sigma)_{\sigma\in\Sigma} \mapsto (r_\sigma k_\sigma)_{\sigma\in\Sigma}. \end{aligned}$$

11.5. Definition Die *arithmetische Euler-Minkowski Charakteristik* $\widehat{\chi}$ eines vollständigen Ideals $\overline{\mathfrak{a}}$ ist gegeben durch die Abbildung

$$\begin{aligned}\widehat{Cl(\mathcal{O}_K)} &\to \mathbb{R}, \text{ mit}\\ \widehat{\chi}(\overline{\mathfrak{a}}) &= -\log(\mathrm{vol}(\mathfrak{a}_\infty(\iota(\mathfrak{a}_f)))),\end{aligned}$$

wobei $\mathrm{vol}(\mathfrak{a}_\infty(\iota(\mathfrak{a}_f)))$ das Volumen der Grundmasche bezüglich des kanonischen Maßes auf $K_\mathbb{R}$ ist (d.h. bezüglich dem Maß, das die Einschränkung des kanonischen Maßes von $K_\mathbb{C} = \mathbb{C}^n$ auf $K_\mathbb{R} = K_\mathbb{C}^{\mathrm{F}_\infty}$ ist.

11.6. Satz. *Die arithmetische Euler-Minkowski-Charakteristik hängt nur von der Klasse von $\overline{\mathfrak{a}}$ in $\widehat{Cl}(\mathcal{O}_K)$ ab.*

Beweis. Sei $\overline{(a)} = (a) \cdot a_\infty$ ein vollständiges Hauptideal. Dann ist

$$\overline{(\mathfrak{a})} \cdot \overline{\mathfrak{a}} = a\mathfrak{a}_f \cdot a_\infty \mathfrak{a}_\infty.$$

Das Gitter $\iota(a \cdot \mathfrak{a}_f)$ ist das Bild des Gitters $\iota(\mathfrak{a}_f)$ unter der linearen Abbildung $m_a \colon K_\mathbb{R} \to K_\mathbb{R}$ gegeben durch $(k_\sigma)_{\sigma\in\Sigma} \mapsto (\sigma(a)k_\sigma)_{\sigma\in\Sigma}$. Es gilt $\det(m_a) = \mathrm{Nm}_{K|\mathbb{Q}}(a)$. Wegen $a_\infty = (|\sigma(a)|^{-1})_{\sigma\in\Sigma}$ gilt für die induzierte lineare Abbildung $a_\infty : K_\mathbb{R} \to K_\mathbb{R}$, daß $\det(a_\infty) = 1/\mathrm{Nm}_{K|\mathbb{Q}}(a)$. Es folgt

$$\begin{aligned}\widehat{\chi}(\overline{(a)} \cdot \overline{\mathfrak{a}}) &= -\log(\mathrm{vol}(a_\infty(\mathfrak{a}_\infty(m_a(\iota(\mathfrak{a}_f))))))\\ &= -\log(\det(a_\infty)\cdot\det(m_a)\,\mathrm{vol}(\mathfrak{a}_\infty \cdot \iota(\mathfrak{a}_f)))\\ &= \widehat{\chi}(\overline{\mathfrak{a}}).\end{aligned}$$

□

11.7. Proposition. *Setze $\overline{\mathcal{O}_K} = \overline{(1)} = \big((1), ((1)_{\sigma\in\Sigma})\big)$. Dann gilt $\widehat{\chi}(\overline{\mathcal{O}_K}) = -\log\sqrt{|D_K|}$, wobei D_K die absolute Diskriminante von K bezeichnet.*

Beweis. Sei $\alpha_1, \ldots, \alpha_n$ eine Ganzheitsbasis von $\mathcal{O}_K$ über $\mathbb{Z}$. Das Gitter $\iota(\mathcal{O}_K) \subset K_\mathbb{R}$ wird somit durch die Vektoren $(\sigma_1(\alpha_j), \ldots, \sigma_n(\alpha_j))$ erzeugt, wobei $\sigma_1, \ldots, \sigma_n \in \Sigma$ und $j = 1, \ldots, n$. Das Volumen von $\iota(\mathcal{O}_K)$ ist somit gegeben durch

$$|\det(\sigma_i(\alpha_j)_{ij})| = \mathrm{vol}(\iota\mathcal{O}_K).$$

Aufgrund von Definition 1.14 der Diskriminante

$$D_k = \mathrm{discr}(\alpha_1, \ldots, \alpha_n) = \det((\sigma_i(\alpha_j)_{ij})^2$$

erhalten wir die Behauptung. □

11.8. Satz. (Arithmetischer Riemann-Roch für vollständige Ideale) *Sei $\overline{\mathfrak{a}} \in \widehat{Cl}(\mathcal{O}_K)$, dann gilt*

$$\widehat{\chi}(\overline{\mathfrak{a}}) = \widehat{\deg}(\widehat{c_1}(\overline{\mathfrak{a}})) + \widehat{\chi}(\overline{\mathcal{O}_K}).$$

Beweis. Sei $\overline{\mathfrak{a}} = \mathfrak{a}_f \cdot \mathfrak{a}_\infty$ mit $\mathfrak{a}_f = \prod \mathfrak{p}^{-a_\mathfrak{p}}$ und $\mathfrak{a}_\infty = \big((e^{-g_\sigma})_{\sigma\in\Sigma}\big)$. Dann ist $\widehat{\deg}(\widehat{c}_1(\overline{\mathfrak{a}})) = \sum_\mathfrak{p} a_\mathfrak{p} \log \operatorname{Nm}\mathfrak{p} + \sum_{\sigma\in\Sigma} g_\sigma$. Das Gitter $\iota(\mathfrak{a}_f)$ ist ein Untergitter von $\iota(\mathcal{O}_K)$, darum gibt es eine lineare Abbildung $m_\mathfrak{a} : K_\mathbb{R} \to K_\mathbb{R}$, so daß gilt $m_\mathfrak{a}\iota(\mathcal{O}_K) = \iota(\mathfrak{a})$. Es gilt

$$|\det(m_\mathfrak{a})| = [\iota(\mathcal{O}_K) : i(\mathfrak{a})] = [\mathcal{O}_K : \mathfrak{a}] = \operatorname{Nm}(\mathfrak{a}) = \prod_\mathfrak{p} \operatorname{Nm}(\mathfrak{p})^{-a_\mathfrak{p}}.$$

Wir erhalten damit für die linke Seite

$$\begin{aligned}
\widehat{\chi}(\overline{\mathfrak{a}}) &= -\log \operatorname{vol}(\mathfrak{a}_\infty \cdot \iota(\mathfrak{a}_f)) \\
&= -\log \operatorname{vol}(\mathfrak{a}_\infty \cdot m_\mathfrak{a} \cdot \iota(\mathcal{O}_k)) \\
&= -\log(\det(\mathfrak{a}_\infty) \cdot \det(m_\mathfrak{a}) \cdot \operatorname{vol}(\iota(\mathcal{O}_K)) \\
&= -\log(\det(\mathfrak{a}_\infty)) - \log(\det(m_\mathfrak{a})) - \log(\operatorname{vol}\iota(\mathcal{O}_K)) \\
&= \sum_{\sigma\in\Sigma} g_\sigma + \sum_\mathfrak{p} a_\mathfrak{p} \log \operatorname{Nm}\mathfrak{p} + \widehat{\chi}(\overline{\mathcal{O}_K}).
\end{aligned}$$

□

11.9. Definition. Sei $\overline{\mathfrak{a}}$ ein vollständiges Ideal und X eine beschränkte Teilmenge von $K_\mathbb{R}$. Damit definieren wir die folgende Menge

$$H^0(\overline{\mathfrak{a}}, X) = \{a \in K \mid a \in \mathfrak{a}_f \text{ und } \iota((a)) \in \mathfrak{a}_\infty(X)\}.$$

Diese Menge wird die *Menge der Schnitte von* $\overline{\mathfrak{a}}$ *in* X genannt. Sei $D \in \widehat{Z}^1(\mathcal{O}_K)$ ein arithmetischer Divisor und $\overline{\mathcal{O}(D)} = \mathcal{O}(D) \cdot \mathcal{O}(D)_\infty$ das zugehörige vollständige Ideal. Dann definieren wir die *Menge der kleinen Schnitte von* D als

$$H^0(D) = \{f \in K^* \mid \widehat{\operatorname{div}} f \geq -D\} \cup \{0\}.$$

Hierbei ist, falls $D = \sum_{\mathfrak{p}\in\operatorname{Spec}\mathcal{O}_K} \nu_\mathfrak{p}\mathfrak{p} + (g_\sigma)_{\sigma\in\sum}$, die Ungleichung $\widehat{\operatorname{div}} f \geq -D$ genau dann erfüllt, wenn $\nu_\mathfrak{p}(f) \geq -\nu_\mathfrak{p}$ für alle $\mathfrak{p} \in \operatorname{Spec}\mathcal{O}_K$ und $-\log|\sigma(f)| \geq -g_\sigma$ für alle $\sigma \in \Sigma$.

11.10. Proposition

(i) Die Mächtigkeit von $H^0(\overline{\mathfrak{a}}, X)$ *ist endlich und hängt nur von der Klasse von* $\mathfrak{a}$ *in* $\widehat{Cl}(\mathcal{O}_K)$ *ab.*

(ii) Die Mächtigkeit von $H^0(D)$ *ist endlich und hängt nur von der Klasse von* D *in* $\widehat{\mathrm{CH}}^1(\mathcal{O}_K)$ *ab.*

Beweis. (i) Übung.
(ii) Aus den Definitionen folgt sofort

$$H^0(D) = \{f \in \mathcal{O}(D) \mid |\sigma(f)| \leq e^{g_\sigma}\}.$$

Da $i(\mathcal{O}(D)) \subseteq K_{\mathbb{R}}$ ein Gitter ist und weil die zentralsymmetrische konvexe Menge

$$X_{\mathfrak{g}} = \{z \in K_{\mathbb{R}} \mid |z_\sigma| \leq e^{g_\sigma}\}$$

kompakt ist, folgt wegen $H^0(D) = i(\mathcal{O}(D)) \cap X_g$ die Endlichkeit dieser Menge. Sei $D' = D + \widehat{\mathrm{div}}(g)$. Dann induziert der Morphismus $m_g \colon K^* \to K^*$ gegeben durch $f \mapsto f \cdot g$ einen Isomorphismus von $H^0(D)$ nach $H^0(D')$. Denn

$$\begin{aligned} H^0(D') &= \{f \in K^* \mid \widehat{\mathrm{div}} f \geq D + \widehat{\mathrm{div}} g\} \\ &= \{f \in K^* \mid \widehat{\mathrm{div}} f - \widehat{\mathrm{div}} g \geq D\} \\ &= \{g \cdot h \in K^* \mid \widehat{\mathrm{div}} h \geq D\} \\ &= \{g \cdot h \mid h \in H^0(D)\}. \end{aligned}$$

□

11.11. Proposition. *Sei* $\mathbb{E} = \{z \in K_{\mathbb{R}} \,|\, |z_\sigma| \leq 1$ *für alle* $\sigma \in \Sigma\}$ *der Einheitsquader in* $K_{\mathbb{R}}$.

(i) Ist $0 \neq a \in H^0(\overline{\mathfrak{a}}, \mathbb{E})$, *dann ist das Ideal* $a \cdot \mathfrak{a}^{-1}$ *ganz und* $\mathrm{Nm}(a\mathfrak{a}^{-1}) \leq \det(\mathfrak{a}_\infty)$.

(ii) Es gilt $H^0(D) = H^0(\overline{\mathcal{O}(D)}, \mathbb{E})$.

Beweis. (i): Übung
zu ii: Es gilt

$$H^0(D) = \{f \in \mathcal{O}(D) \mid |\sigma(f)| \leq e^{g_\sigma}\} = \{f \in \mathcal{O}(D) \mid \iota(f) \in \mathcal{O}(D)_\infty(\mathbb{E})\}$$

□

11.12. Satz

(i) Falls $\widehat{\deg} D < 0$ *ist, dann ist* $H^0(D) = \{0\}$.

(ii) Falls $\widehat{\deg} D \leq 0$ *und* $H^0(D) \neq \{0\}$ *sind, dann bestehen in* $\widehat{Cl}(\mathcal{O}_K)$ *die Gleichheiten* $\overline{\mathcal{O}} = \overline{\mathcal{O}(D)}$ *und* $\#H^0(D) = \#(\mu(K)) + 1$.

(iii) Falls $\widehat{\deg}(D) \geq -\widehat{\chi}(\mathcal{O}_K) - r_2 \log(\pi/2)$ *ist, dann ist* $H^0(D) \neq \{0\}$.

Beweis. (i) Sei $\widehat{\deg}(D) < 0$. Angenommen es existiert ein $0 \neq f \in H^0(D)$. Dann ist wegen $\widehat{\mathrm{div}}(f) \geq -D$ auch $\widehat{\deg}(\widehat{\mathrm{div}}(f)) \geq -\widehat{\deg}(D)$. Weil $\widehat{\deg}$ auf $\widehat{Rat}^1(\mathcal{O}_K)$ verschwindet, folgt aus der Annahme der Widerspruch zu Proposition 10.6, da sonst gilt:

$$0 = \widehat{\deg}(\widehat{\mathrm{div}}(f)) \geq -\widehat{\deg}(D) > 0.$$

(ii) Wegen (i) genügt es D mit $\widehat{\deg}(D) = 0$ zu betrachten. Sei $0 \neq f \in H^0(D)$, dann ist $\widehat{\operatorname{div}}(f) + D \geq 0$. Aufgrund der Linearität von $\widehat{\deg}$ gilt:

$$\begin{aligned} 0 &= \widehat{\deg}(\widehat{\operatorname{div}}(f)) + \widehat{\deg}(D) \\ &= \widehat{\deg}(\widehat{\operatorname{div}}(f) + D) \\ &= \sum_{\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K} (\nu_{\mathfrak{p}}(f) + \nu_{\mathfrak{p}}) \log \operatorname{Nm} \mathfrak{p} + \sum_{\sigma} (\log |\sigma(f)| + g_\sigma). \end{aligned}$$

In beiden Summen ist jeder Summand positiv, also muß gelten

$$\nu_{\mathfrak{p}}(f) = -\nu_{\mathfrak{p}} \qquad \forall \mathfrak{p} \in \operatorname{Spec} \mathcal{O} \tag{11.12.1}$$

und

$$\log |\sigma(f)| = -g_\sigma \qquad \forall \sigma \in \Sigma. \tag{11.12.2}$$

Aus (11.12.1) folgt $(f) = \mathcal{O}(D)$, d.h. f ist bis auf Einheiten bestimmt und aus (11.12.2) folgt f ist bis auf Einheitswurzeln definiert. Es folgt $D = \widehat{\operatorname{div}}(f)$ und $\#\left(H^0(D)\right) = \#(\mu(K)) + 1$.

(iii) Wir setzen

$$X_{\mathfrak{g}} = \{z \in K_{\mathbb{R}} \mid |z_\sigma| \leq e^{g_\sigma} \text{ für } \quad \text{alle } \sigma \in \Sigma\}.$$

Beachte $X_{\mathfrak{g}}$ ist eine zentralsymmetrische, konvexe Teilmenge von $K_{\mathbb{R}}$ und $H^0(D) \cap X_{\mathfrak{g}} \neq \emptyset$. Aus dem Satz von Minkowski folgt.

$$\begin{aligned} \# H^0(D) &= \#\{i(\mathcal{O}(D)) \cap X_{\mathfrak{g}}\} \\ &\geq 2^{\dim K_{\mathbb{R}}} \frac{\operatorname{vol} X_{\mathfrak{g}}}{\operatorname{vol} i(\mathcal{O}(D))} \\ &= 2^{-(r_1+r_2)} \frac{2^{r_1} \pi^{r_2} e^{\sum_\sigma \mathfrak{g}_\sigma}}{\operatorname{Nm}(\mathcal{O}(D)) \cdot \operatorname{vol}(i(\mathcal{O}_K))} \\ &= e^{\widehat{\deg}(D)} \cdot (\pi/2)^{r_2} \cdot \operatorname{vol}(i(\mathcal{O}_K))^{-1}. \end{aligned}$$

Daraus folgt $\# H^0(D) \geq 1$ genau dann, wenn $e^{\widehat{\deg} D} \geq \operatorname{vol}(i(\mathcal{O}_K)) \cdot (\pi/2)^{-r_2}$. Wegen $\widehat{\chi}(\mathcal{O}_K) = -\log(\operatorname{vol}(i(\mathcal{O}_K)))$ folgt die Behauptung. □

12 Hauptsätze der algebraischen Zahlentheorie

Eine erste Anwendung der bisher entwickelten Theorie sind neue Beweise der Hauptsätze der algebraischen Zahlentheorie.

12.1. Satz (Hermite-Minkowski) *Sei $K \neq \mathbb{Q}$ ein Zahlkörper, dann gilt für seine Diskriminante $D_K \geq 2$.*

Beweis. Sei $\mathfrak{g} = (g_\sigma)_{\sigma\in\Sigma} \in \widehat{H}(K)$ und $D_\mathfrak{g} = (0, \mathfrak{g})$. Wähle $\mathfrak{g}$, so daß $\widehat{\deg}(D) = \sum_{\sigma\in\Sigma} \mathfrak{g}_\sigma \geq -\widehat{\chi}(\mathcal{O}_K) - r_2 \log(\pi/2)$, dann ist $H^0(D_\mathfrak{g}) \neq 0$. Aufgrund von 11.12.(i) ist $\widehat{\deg}(D_\mathfrak{g}) \geq 0$ und somit

$$\begin{aligned} -\widehat{\chi}(\mathcal{O}_K) - r_2 \log(\pi/2) \geq 0 &\Leftrightarrow \frac{1}{2} \log D_K \geq r_2 \log(\pi/2) > 0 \\ &\Leftrightarrow D_K \geq (\pi/2)^{2r_2} > 1,57^{2r_2}. \end{aligned}$$

Ist $r_2 > 0$, dann sind wir fertig.
Sei nun $D_K = 1$ und $r_2 = 0$, dann gilt für alle $D \in \widehat{Z}^1(\mathcal{O}_K)$ mit $\widehat{\deg}(D) = 0$, daß $H^0(D) \neq \{0\}$. Wegen 11.12.(ii) folgt somit $D = \widehat{\operatorname{div}}(f)$ für ein $f \in K^*$. Für jedes $\mathfrak{g} \in \widehat{H}(K)$ mit $\operatorname{Tr}\mathfrak{g} = 0$ ist $D_\mathfrak{g}$ ein arithmetischer Divisor mit $\widehat{\deg} D = 0$. Da es allerdings nur abzählbar viele $u \in \mathcal{O}_K^*$ gibt, existiert ein $D_\mathfrak{g} \neq \widehat{\operatorname{div}}(u)$. Also ist $D_K > 1$. □

12.2. Satz *Die Idealklassengruppe $\mathcal{O}_K$ von K ist endlich.*
Beweis. Sei $\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}^{-a_\mathfrak{p}} \subseteq K$ ein Ideal. Wir wählen $\overline{\mathfrak{a}} = \mathfrak{a}_f \cdot \mathfrak{a}_\infty$ mit $\mathfrak{a}_f = \mathfrak{a}$ ein vollständiges Ideal, so daß

$$\widehat{\deg}(\widehat{c_1}(\overline{\mathfrak{a}})) = -\widehat{\chi}(\mathcal{O}_K) - r_2 \log(\pi/2) = C_K.$$

Aufgrund des 11.12.(iii) folgt $H^0(\overline{\mathfrak{a}}, \mathbb{E}) \neq \{0\}$. Sei $0 \neq a \in H^0(\overline{\mathfrak{a}}, \mathbb{E})$, dann ist $a \cdot \overline{\mathfrak{a}} = a\mathfrak{a}$ ein ganzes Ideal in der Klasse von $\mathfrak{a}$ mit $\operatorname{Nm}(a\mathfrak{a}) \leq e^{C_K}$. Wir wissen, daß ganze Ideale $\mathfrak{a} \subseteq \mathcal{O}_K$ Untergitter $\iota(\mathfrak{a}) \subset \iota(\mathcal{O}_K)$ von Index $\operatorname{Nm}(\mathfrak{a})$ entsprechen. Da es nur endlich viele Untergitter mit vorgegebenen Index gibt, folgt die Behauptung. □

12.3. Satz (Dirichlet'scher Einheitensatz) *Sei K ein algebraischer Zahlkörper vom Grad $n = r_1 + r_2$ über $\mathbb{Q}$. Dann ist $\mathcal{O}_K^*$ eine endlich erzeugte abelsche Gruppe vom Rang $r_1 + r_2 - 1$, i.a.w.*

$$\mathcal{O}_K^* \simeq \mu(K) \times \mathbb{Z}^{r_1+r_1-1},$$

wobei $\mu(K)$ die endliche Gruppe der Einheitswurzeln bezeichnet.
Beweis. Wir erinnern an die exakte Sequenz

$$1 \to \mu(K) \to \mathcal{O}_K^* \xrightarrow{\rho} \widehat{H}(K) \xrightarrow{a} \widehat{\mathrm{CH}}^1(\mathcal{O}_K) \to CH^1 \to 1,$$

wobei $a(\mathfrak{g}) = [0, \mathfrak{g}]$ und an den arithmetischen Grad

$$\widehat{\deg}\colon \widehat{\mathrm{CH}}^1(\mathcal{O}_K) \to \mathbb{R}.$$

Wir wissen außerdem, daß $\Gamma_K = \rho(\mathcal{O}_K)$ eine diskrete Untergruppe ist, die in der Hyperebene $H_0 = \{g \in \widehat{H}(K) \mid \operatorname{Tr}(\mathfrak{g}) = 0\}$ enthalten ist. Wir wollen zeigen, daß Γ_K ein vollständiges Gitter in H_0 ist. Äquivalent ist es zu zeigen, daß H_0/Γ_K kompakt ist. Dazu betrachten wir den Homomorphismus

$$\begin{aligned} \overline{a} : \widehat{H}(K)/\Gamma_K &= \widehat{\mathrm{CH}}^1(\mathcal{O}_K) \\ \mathfrak{g} \mod \Gamma_K &\mapsto (0, \mathfrak{g}). \end{aligned}$$

Durch Komposition mit $\widehat{\deg}$ erhalten wir eine Surjektion

$$\begin{aligned}\widehat{\deg}\circ\overline{a}\colon \widehat{H}(K)/\Gamma_K &\to \mathbb{R},\\ \mathfrak{g} &\to \mathrm{Tr}(\mathfrak{g}),\end{aligned}$$

deren Kern gerade H_0/Γ_K ist.

Setze $H_{-\widehat{\chi}(\mathcal{O}_K)} = \{\mathfrak{g} \in \widehat{H}(K) \mid \widehat{\deg}\circ\overline{a}(\mathfrak{g}) = -\widehat{\chi}(\mathcal{O}_K)\} \subseteq \widehat{H}(K)$. Da die Menge $H_{-\widehat{\chi}(\mathcal{O}_K)}/\Gamma_K$ als Nebenklasse von H_0/Γ_K in der topologischen Gruppe $\widehat{H}(K)/\Gamma_K$ zu H_0/Γ_K homöomorph ist, genügt es die Kompaktheit dieser Menge zu zeigen.

Wir werden zeigen, daß eine beliebige Folge $(\mathfrak{g}_n)_{n\in\mathbb{N}} \in H_{-\widehat{\chi}(\mathcal{O}_K)}$ eine modulo Γ_K konvergente Teilfolge besitzt. Für jedes Folgenglied $\mathfrak{g}_n$ existiert ein $0 \neq s_n \in H^0(\overline{\mathcal{O}(D_{\mathfrak{g}n})})$. Wegen $\mathcal{O}(D_{\mathfrak{g}}) = \mathcal{O}$ ist $s_n\mathcal{O}_K^{-1} = (s_n)$ ein ganzes Hauptideal mit $\mathrm{Nm}(s_n) \leq e^{-\widehat{\chi}(\mathcal{O}_K)}$.

Wir wissen, daß es nur endlich viele ganze Ideale mit beschränkter Norm gibt. Deshalb können wir nach Wahl einer geeigneten Teilfolge anmelden, daß $s_n \cdot \mathcal{O}_K = s_0 \cdot \mathcal{O}_K$ für alle $n \in \mathbb{N}$. Es folgt $s_n = u_n \cdot s_0$ für ein $u_n \in \mathcal{O}_K^*$. Da $s_n \in H^0(\overline{\mathcal{O}(D_{\mathfrak{g}})})$ ist, existiert eine Konstante A sodaß für alle $\mathfrak{g} = (g_\sigma)_{\sigma\in\Sigma} \in (\mathfrak{g}_n)_{n\in\mathbb{N}}$ und alle $\sigma \in \Sigma$ gilt:

$$\begin{aligned}-\log|\sigma(s_n)| = -\log|\sigma(u_n)\cdot\sigma(s_0)| &\geq -g_\sigma\\ \Leftrightarrow A \leq \log|\sigma(s_0)| &\leq -\log|\sigma(u_n)| + g_\sigma.\end{aligned}$$

Da $\sum\limits_{\sigma\in\Sigma}(-\log(\sigma(u_n)) + g_\sigma) = -\widehat{\chi}(\mathcal{O}_K)$ ist, erhalten wir eine weitere Schranke

$$-\log|\sigma(u_n)| + g_\sigma \leq -\widehat{\chi}(\mathcal{O}_K) - (n-1)A =: B.$$

Es folgt $A \leq g_\sigma - \log|\sigma(u_n)| \leq B$. Da der von A und B bestimmte abgeschlossene Quader kompakt ist, besitzt die beschränkte Folge $(\mathfrak{g}_n + \rho(u_n))_{n\in\mathbb{N}}$ die zur ursprünglichen Folge $(\mathfrak{g}_n)_{n\in\mathbb{N}}$ modulo Γ_K kongruent ist, wegen dem Satz von Bolzano-Weierstraß eine konvergente Teilfolge. □

12.4. Satz (Minkowski) *Es gibt nur endlich viele Zahlkörper K, deren Grad $n = [K:\mathbb{Q}]$ und Diskriminante D_K beschränkt sind.*

Beweis. Es reicht zu zeigen, daß jeder solcher Zahlkörper ein über $\mathbb{Z}$ ganzes, primitives Element α besitzt, dessen Absolutbeträge $|\sigma(\alpha)|$ für alle $\sigma \in \Sigma$ durch eine nur von D_K und n bestimmte Konstante beschränkt sind. Sei also α so ein primitives Element. Dann sind die Koeffizienten des Minimalpolynoms $p_\alpha(x) = \prod\limits_{\sigma\in\Sigma}(x - \sigma(\alpha))$ beschränkte ganze Zahlen. Da es nur endlich viele Polynome mit beschränktem Grad und Koeffizienten gibt, sind wir fertig, weil $K \cong \mathbb{Q}[x]/(P_\alpha(x))$. Sei nun K ein Zahlkörper mit $n = [K:Q]$ und Diskriminante D_K.

Fall 1: K besitzt eine reelle Einbettung $\sigma_0\colon K \to \mathbb{Q}$ (dies ist z.B. immer der Fall, wenn n ungerade ist). Es sei $D_{\mathfrak{g}}$ der arithmetische Divisor $(0,\mathfrak{g})$, wobei $\mathfrak{g} = (g_\sigma)_{\sigma\in\sum} \in \widehat{H}(K)$ mit

$$g_\sigma = \begin{cases} -\widehat{\chi}(\mathcal{O}_K) + (1-n)\log(2) & \sigma = \sigma_0\\ \log(2) & \sigma \neq \sigma_0.\end{cases}$$

Man stellt sofort fest, daß $\widehat{\deg} D_{\mathfrak{g}} = -\widehat{\chi}(\mathcal{O}_K)$. Sei nun $0 \neq \alpha \in H^0((D_{\mathfrak{g}})$, dann ist (α) ein ganzes Ideal mit positiver Norm und

$$|\sigma(\alpha)| \leq \begin{cases} D_K^{1/2} \cdot 2^{n-1} & \sigma = \sigma_0 \\ 1/2 & \sigma \neq \sigma_0. \end{cases}$$

Insbesondere ist $D_K^{1/2} \cdot 2^{n-1} \geq 1$. Die Einschränkung von σ_0 auf $\mathbb{Q}(\alpha)$, liefert eine Einbettung $\sigma_0 \colon \mathbb{Q}(\alpha) \to \mathbb{C}$. Wir haben bereits gezeigt, daß

$$[K \colon \mathbb{Q}(\alpha)] = \# \left\{ \sigma \in \Sigma \mid \sigma|_{\mathbb{Q}(\alpha)} = \sigma_0|_{\mathbb{Q}(\alpha)} \right\}.$$

Da $\sigma_0(\alpha) \geq 1$ und $\sigma(\alpha) < 1$ für alle $\sigma \neq \sigma_0$ ist, folgt daraus $K = \mathbb{Q}(\alpha)$.

Fall 2: K besitzt keine reelle Einbettung. Wegen der F_∞-Invarianz von $\mathfrak{g}$ erzeugt die Methode vom Fall 1 nur Elemente α mit $[K \colon \mathbb{Q}(\alpha)] \geq 2$. Wir werden deshalb anstelle von

$$H^0(D_{\mathfrak{g}}) = \{ f \in \mathcal{O}(D_{\mathfrak{g}}) \mid i(f) \in X_{\mathfrak{g}} \}$$

Mengen der Form

$$H^0(\overline{\mathcal{O}(D_{\mathfrak{g}})}, X) = \{ f \in \mathcal{O}(D_{\mathfrak{g}}) \mid \iota(f) \in X \} \subseteq K_{\mathbb{R}} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

mit X einer kompakten, zentralsymmetrischen Menge, die für alle komplexen Einbettungen symmetrisch zur reellen Achse ist.

Wir wählen

$$X = \left\{ z \in K_{\mathbb{R}} \;\middle|\; \begin{array}{l} |\Re(z_{\sigma_0})| \leq 1/2,\ \Im(z_{\sigma_0}) \leq 2^{\dim K_{\mathbb{R}} - 1} \cdot |D_K|^{1/2} \\ |z_\sigma| \leq 1/2 \text{ falls } \sigma \neq \sigma_0, \overline{\sigma_0} \end{array} \right\}.$$

Man berechnet leicht

$$\operatorname{vol}(X) = 2^{\dim K_{\mathbb{R}}} (D_K)^{1/2} \pi^{r_2 - 1}.$$

Aus dem Satz von Minkowski (Satz 8.6) folgt

$$H^0(\overline{\mathcal{O}}, X) \geq 2^{-\dim K_{\mathbb{R}}} \cdot \frac{\operatorname{vol}(X)}{\operatorname{vol}(i(\mathcal{O}(D)))} \geq 1.$$

Sei $\alpha \in H^0(\overline{\mathcal{O}}, X)$, dann ist wegen $\alpha \in \mathcal{O}_K$, $\operatorname{Nm}((\alpha)) \geq 1$, also insbesondere auch $|\Im(\sigma_0(\alpha))| > 1/2$. Deshalb ist $\sigma_0(\alpha) \neq \sigma(\alpha)$ für alle $\sigma \neq \sigma_0$ und wie im Fall 1 folgern wir $\mathbb{Q}(\alpha) = K$. □

13 Modultheorie über Dedekindringen

Für das Folgende benötigen wir aus der Algebra den folgenden Struktursatz über projektive Moduln über Dedekindringen. Desweiteren setzen wir die Kenntnis der multilinearen Algebra voraus (siehe z.B. C.1 – C.10).

13.1. Definition Ein R-Modul M heißt *projektiv* falls $\mathrm{Hom}_R(M,\cdot)$ ein exakter Funktor ist, also daß für jede exakte Sequenz $0 \to F' \to F \to F'' \to 0$ von R-Moduln auch die Sequenz $0 \to \mathrm{Hom}_R(M,F') \to \mathrm{Hom}_R(M,F) \to \mathrm{Hom}_R(M,F'') \to 0$ exakt ist.

13.2. Definition. Der *Rang* eines projektiven $\mathcal{O}_K$-Moduls ist die Dimension

$$\mathrm{rg}(M) = \dim_K(M \otimes_{\mathcal{O}} K).$$

Projektive Moduln L vom Rang 1 werden *invertierbare $\mathcal{O}_K$-Moduln*, oder auch *Geradenbündel* genannt.

13.3. Lemma. *Sei L ein invertierbarer Modul, dann ist L als $\mathcal{O}_K$-Modul isomorph zu einem gebrochenen Ideal.*

Beweis. Der Morphismus $L \otimes_{\mathcal{O}_K} L^\vee \to \mathcal{O}_K$, gegeben durch $a \otimes a^\vee \mapsto a^\vee(a)$, ist ein Isomorphismus. Denn für $0 \neq \alpha \in L$ ist die Abbildung

$$\begin{aligned} &L \to L \otimes_\sigma K = K(\alpha \otimes 1) \\ &x \mapsto f(x) \cdot (\alpha \otimes 1), \end{aligned} \tag{13.3.1}$$

wobei $x = s\alpha \mapsto f(x) = s$, $s \in \mathcal{O}_K$, injektiv, weil L ein projektive Modul ist. Also ist das Bild des $\mathcal{O}_K$-Modulhomomorphismus $L \to K, x \mapsto f(x)$ ein gebrochenes Ideal. □

13.4. Lemma. *Seien $\mathfrak{a}, \mathfrak{b} \subseteq K$ gebrochene Ideale, dann gilt*

$$\mathfrak{a} \oplus \mathfrak{b} \cong \mathcal{O} \oplus \mathfrak{ab}.$$

Beweis. Wähle $a \in \mathfrak{a}$, so daß $J = a \cdot \mathfrak{a}^{-1} \subseteq \mathcal{O}_K$ ein ganzes Ideal ist. Es sei $J = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_r^{e_r}$ die Primidealzerlegung (mit möglicherweise mehrfachen Faktoren!). Für $i = 1, \ldots, r$ wähle $b_i \in \mathfrak{b}\mathfrak{p}_i^{-1} \cdot \ldots \cdot \mathfrak{p}_r^{-1}$ mit $b_i \notin \mathfrak{p}_1, \ldots, \mathfrak{p}_r$ und setze $b = \sum_{i=1}^{r} b_i$. Dann folgt $\mathfrak{b}^{-1}b \not\subset \mathfrak{p}_i$ für alle i und somit ist $\mathfrak{b}^{-1}b$ teilerfremd zu J. Es gilt also:

$$a\mathfrak{a}^{-1} + b\mathfrak{b}^{-1} = \mathcal{O}_K.$$

Wähle nun $c \in \mathfrak{a}^{-1}, d \in \mathfrak{b}^{-1}$, so daß $ac + bd = 1$ und bilde damit die invertierbare Matrix

$$A = \begin{pmatrix} c & b \\ -d & a \end{pmatrix}, \quad A^{-1} = \begin{pmatrix} a & -b \\ d & c \end{pmatrix}.$$

Durch nachrechnen ergibt sich

$$(\mathfrak{a} \oplus \mathfrak{b})A \subseteq \mathcal{O}_K \oplus \mathfrak{ab}$$

und

$$(\mathcal{O}_K \oplus \mathfrak{ab})A^{-1} \subseteq \mathfrak{a} \oplus \mathfrak{b},$$

woraus die Behauptung folgt. □

13.5. Satz. *Sei $\mathcal{O}$ ein Dedekindring und M ein endlich erzeugter $\mathcal{O}$-Modul. Dann sind äquivalent:*

(i) *M ist projektiv,*

(ii) *M ist direkter Summand eines freien, endlich erzeugten $\mathcal{O}$-Moduls,*

(iii) *M ist lokal frei, d.h. $M \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$ ist für jedes Primideal $\mathfrak{p}$ ein freier $\mathcal{O}_{\mathfrak{p}}$-Modul,*

(iv) *M ist torsionfrei, d.h. die Abbildung $M \to M, x \mapsto ax$, ist für jedes $a \in \mathcal{O},\ a \neq 0$, injektiv,*

(v) *$M \cong \mathcal{O}^n \oplus \mathfrak{a}$ mit einem Ideal $\mathfrak{a}$ von $\mathcal{O}$ und einer ganzen Zahl $n \geq 0$.*

Beweis. siehe z.B. [La1] □

Definition. Sei $\mathcal{O}$ ein Dedekindring und P ein projektiver $\mathcal{O}$-Modul. Dann ist $P \simeq \mathcal{O}^n \oplus \mathfrak{a}$ und wir definieren die Determinante von P vermöge

$$\det(P) = \underbrace{\mathcal{O} \otimes_{\mathcal{O}} \ldots \otimes_{\mathcal{O}} \mathcal{O} \otimes_{\mathcal{O}}}_{\text{n-mal}} \mathfrak{a} = \mathfrak{a}.$$

Übung. Zeige $\det(P) = \bigcap_{\mathfrak{p} \in \operatorname{Spec} \mathcal{O}} \det(P_{\mathfrak{p}})$, hierbei ist $\det(P_{\mathfrak{p}})$ wie in Definition C.8 gegeben.

13.6. Satz. *Sei $\mathcal{O}$ ein Dedekindring, mit Quotientenkörper $Quot(\mathcal{O})$, dann besteht für sein Grothendieckring der Isomorphismus $K_0(\mathcal{O}) \simeq \mathbb{Z} \oplus Cl_K$.* (siehe z.B. Appendix C.4).

Beweis. Übung (Tip: Benutze Lemma 13.4 und Satz 13.5. □

13.7. Definition. Sei $B|A$ eine Erweiterung von kommutativen Ringen und I sei der Kern des Homomorphismus

$$\mu : B \otimes_A B \to B, \qquad x \otimes y \mapsto x \cdot y.$$

Damit ist der *Differentialmodul* $\Omega^1_{B|A}$ von B über A gegeben durch

$$\Omega^1_{B|A} = I/I^2.$$

Vermöge der Einbettung $B \hookrightarrow B \otimes B$, $b \mapsto b \otimes 1$, fassen wir $\Omega^1_{B|A}$ als B-Modul auf. Mittels

$$x \mapsto dx := x \otimes 1 - 1 \otimes x \qquad \mod I^2,$$

erhalten wir eine Derivation

$$d : B \longrightarrow \Omega^1_{B|A},$$

d.h. d erfüllt die Gleichungen

$$\begin{aligned} d(xy) &= xdy + ydx \qquad \forall x, y \in B \\ da &= 0 \qquad \forall a \in A \end{aligned}$$

Beachte: Das Ideal I wird von $dx, x \in B$ erzeugt. Denn falls $\sum x_i \otimes y_i \in I$, so ist $\sum x_i y_i = 0$ und somit

$$\begin{aligned} \sum x_i \otimes y_i &= \sum x_i \otimes y_i - (\sum x_i y_i) \otimes 1 \\ &= \sum x_i (1 \otimes y_i - y_i \otimes 1). \end{aligned}$$

13.8. Satz. *Sei $L|K$ eine algebraische Erweiterung von Zahlkörpern. Dann ist folgende Sequenz exakt*

$$0 \to \mathcal{D}_{L|K} \to \mathcal{O}_L \to \Omega^1_{\mathcal{O}_L|\mathcal{O}_K} \to 0. \tag{13.8.1}$$

Hierbei bezeichnet $\mathcal{D}$ die Differente, siehe Definition 7.3.

Beweis. Wir werden (13.8.1) nur für den Spezialfall $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ zeigen.

13.9. Lemma. *Sei $\mathcal{O}_L = \mathcal{O}_K[\alpha]$, dann wird $\Omega^1_{\mathcal{O}_L|\mathcal{O}_K}$ von $d\alpha$ erzeugt und die Sequenz*

$$0 \to (f'(\alpha)) \xrightarrow{i} \mathcal{O}_L \xrightarrow{m} \Omega^1_{\mathcal{O}_L|\mathcal{O}_K} \to 0,$$

wobei $f(x) \in \mathcal{O}_K[x]$ das Minimalpolynom von α ist, ist exakt.

Beweis. Aus $d(b_1 + b_2) = db_1 + db_2$ und $d\alpha^n = (n-1)\alpha^{n-1}d\alpha$ folgt, daß für beliebiges $b = \sum a_i \alpha^i \in \mathcal{O}_L$ gilt $\alpha b = (\sum i a_i \alpha^{i-1}) d\alpha$. Es gilt $0 = d(f(\alpha)) = f'(\alpha) \cdot d\alpha$ und somit $b \cdot d\alpha = 0$ für alle $b \in (f'(\alpha))$. Es gilt $\ker m \subset \mathrm{Im} i$: Sei $b \in \mathcal{O}_L$ mit $bd\alpha = 0$, dann gilt wegen $b = \sum a_i \alpha^i$ und $d\mathcal{O}_K = 0$, daß

$$nb \cdot d\alpha = (\sum_{i=0} a_i \alpha^i) d\alpha = d\left(\sum_{i=0} \frac{a_i}{i+1} \alpha^{i+1} \right) = 0.$$

Es gibt also ein $a_0 \in \mathcal{O}_K$, sodaß α eine Nullstelle des Polynoms $p(x) = \sum\limits_{i=0} \frac{a_i}{i+1} x^i + a_0$ ist. Da f das Minimalpolynom von α ist, folgt $p(x) = r(x) \cdot f(x)$ und deswegen ist

$$b = p'(\alpha) = f'(\alpha) \cdot r(\alpha) + f(\alpha) \cdot r'(\alpha) = f'(\alpha) \cdot r(\alpha) \in (f'(\alpha)).$$

□

13.10. Lemma. *Sei $\mathcal{O}_L = \mathcal{O}_K[\alpha]$, dann ist $\mathcal{D}_{\mathcal{O}_L|\mathcal{O}_K} = (f'(\alpha))$.*

Beweis. Sei $f(x) = a_0 + a_1 X + \ldots + a_n X^n$ das Minimalpolynom von α und

$$\frac{f(x)}{x - \alpha} = b_0 + b_1 X + \ldots + b_{n-1} X^{n-1}.$$

Damit ergibt sich die zu $1, \alpha, \alpha^2, \ldots, \alpha$ duale Basis zu

$$\frac{b_0}{f'(\alpha)}, \frac{b_1}{f'(\alpha)}, \cdots, \frac{b_{n-1}}{f'(\alpha)}$$

und nämlich $\alpha_1, \ldots, \alpha_n$ die Nullstellen von $f(x)$, so gilt

$$\sum_{i=1}^{n} \frac{f(x)}{x-\alpha_1} \frac{\alpha_i^r}{f'(\alpha_i)} = x^r, \qquad 0 \leq r \leq n-1 \tag{13.10.1}$$

denn die Differenz beider Seiten ist ein Polynom vom Grad $\leq n-1$, mit n-verschiedenen Nullstellen $\alpha_1, \ldots, \alpha_n$, woraus die Gleichheit folgt ($f(\alpha+\varepsilon) = \varepsilon \cdot f'(\alpha) + \mathcal{O}(\varepsilon^2)$).
Wir schreiben als (13.10.1) als

$$\mathrm{Tr}_{L|K}\left(\frac{f(x)}{x-\alpha}\frac{\alpha^r}{f'(\alpha)}\right) = x^r$$

und Koeffizientenvergleich ergibt

$$\mathrm{Tr}_{L|K}\left(\alpha^i \cdot \frac{b_j}{f'(\alpha)}\right) = \delta_{ij}.$$

Aus den rekurrenten Formeln

$$b_{n-1} = 1, \qquad b_{n-2} - \alpha b_{n-1} = a_{n-1}$$

ergibt sich

$$b_{n-i} = \alpha^{i-1} + a_{n-1}\alpha^{i-2} + \ldots + a_{n-i+1},$$

sodaß $\mathcal{O}_K \cdot b_0 + \ldots + \mathcal{O}_K b_{n-1} = \mathcal{O}_K[\alpha]$ und deswegen $\mathcal{O}_L^\nu = \left(\frac{1}{f'}\right)$. Es folgt wegen $\mathcal{D}_{\mathcal{O}_L|\mathcal{O}_K} = (\mathcal{O}_L^\nu)^{-1}$ die Behauptung. □

13.11. Bemerkung. (i) Der allgemeine Fall im Beweis des Satzes 13.8 wird mit Hilfe der Theorie der Komplettierungen auf den Spezial zurückgeführt (siehe z.B. [Ne], Lemma 10.4, [Ko] Proposition 4.6.6). mittels der Technik der Komplementierungen (was wir nicht gelernt haben!) bewiesen. ??? `literatur dazu?`
$\Omega^1_{\mathcal{O}_L|\mathcal{O}_K}$ ist immer ein Torsionsmodul.

14 Metrisierte $\mathcal{O}_K$-Moduln

Sei K ein algebraischer Zahlkörper und $\mathcal{O}_K$ sein Ring der ganzen Zahlen. Zuerst betrachten wir nochmals den Ring $K_{\mathbb{C}} = K \otimes_{\mathbb{Q}} \mathbb{C}$ und die Involution F_∞. Danach untersuchen wir metrisierte Moduln. Wir treffen hierbei die Verabredung, daß alle von uns betrachteten $\mathcal{O}_K$-Moduln endlich erzeugt sind.

14.1. Mittels $X(\mathbb{C}) = \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C}) = \Sigma$ erhalten wir eine kanonische Zerlegung

$$K_{\mathbb{C}} \cong \bigoplus_{\sigma \in X(\mathbb{C})} \mathbb{C} \tag{14.1.1}$$

gegegeben durch

$$a \otimes z \mapsto \bigoplus_{\sigma \in X(\mathbb{C})} z \cdot \sigma(a) \qquad (a \in K,\, z \in \mathbb{C}).$$

Die rechte Seite läßt sich als die Menge $\mathbb{C}^{X(\mathbb{C})} = \mathrm{Hom}(X(\mathbb{C}), \mathbb{C})$, also die Menge aller Funktionen $x \colon X(\mathbb{C}) \to \mathbb{C}$ auffassen, d.h.

$$K_{\mathbb{C}} \simeq \mathrm{Hom}_{\mathbb{Q}}(X(\mathbb{C}), \mathbb{C}). \tag{14.1.2}$$

Der Körper K ist vermöge $K \to K \otimes_{\mathbb{Q}} \mathbb{C}$, $a \mapsto a \otimes 1$, kanonisch in $K_{\mathbb{C}}$ eingebettet. Wenn wir nun K mit seinem Bild identifizieren, dann ist in der Betrachtung (14.1.1) ein Element $a \in K$ ein Tupel $\bigoplus_{\sigma \in X(\mathbb{C})} \sigma(a)$ und in der Betrachtung (14.1.2) ist a die Funktion bestimmt durch $a(\sigma) := \sigma(a)$.

Es bezeichne F_∞ das erzeugende Element der Galoisgruppe $\mathrm{Gal}(\mathbb{C}|\mathbb{R})$. F_∞ induziert dann auf $K_{\mathbb{C}}$ eine Involution F_∞, die in der Darstellung (14.1.2) für $X \colon X(\mathbb{C}) \to \mathbb{C}$ durch

$$(F_\infty(x))(\sigma) = \overline{x(\overline{\sigma})}$$

gegeben ist. F_∞ heißt die Frobenius-Korrespondenz an der Stelle Unendlich oder auch kürzer nur Frobenius in Unendlich.

14.2. Definition. Die Konjugation auf $K_{\mathbb{C}}$ ist die Involution, gegeben durch

$$\overline{x}(\sigma) := \overline{x(\sigma)}.$$

Wir nennen ein $x \in K_{\mathbb{C}}$, also eine Funktion $x \colon X(\mathbb{C}) \to \mathbb{C}$ positiv und schreiben $x > 0$, wenn sie reelle Werte hat und wenn $x(\sigma) > 0$ für alle $\sigma \in X(\mathbb{C})$.

14.3. Sei M ein $\mathcal{O}_K$-Modul, dann setzen wir

$$M_{\mathbb{C}} = M \otimes_{\mathbb{Z}} \mathbb{C}.$$

$M_{\mathbb{C}}$ ist ein Modul über dem Ring $K_{\mathbb{C}} = \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{C}$, denn wenn wir $\mathcal{O}_K$ als Teilring von $K_{\mathbb{C}}$ auffassen, dann gilt:

$$M_{\mathbb{C}} = M \otimes_{\mathbb{Z}} \mathbb{C} = M \otimes_{\mathcal{O}_K} (\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{C}) = M \otimes_{\mathcal{O}_K} K_{\mathbb{C}}.$$

Die Involution F_∞ auf $K_{\mathbb{C}}$ induziert die Involution auf $M_{\mathbb{C}}$, sie ist gegeben durch

$$F_\infty(a \otimes x) = a \otimes F_\infty(x) \qquad \forall a \otimes x \in M \otimes_{\mathcal{O}_K} K_{\mathbb{C}}$$

bzw.

$$F_\infty(a \otimes x) = a \otimes \overline{x} \qquad \forall a \otimes x \in M \otimes_{\mathbb{Z}} \mathbb{C}.$$

14.4. Definition. Eine *hermitesche Metrik* auf dem $K_{\mathbb{C}}$-Modul $M_{\mathbb{C}}$ ist eine sesquilineare Abbildung

$$\langle\ ,\ \rangle_M \colon M_{\mathbb{C}} \times M_{\mathbb{C}} \longrightarrow K_{\mathbb{C}},$$

(d.h. $\langle\ ,\ \rangle$ ist im ersten Argument $K_{\mathbb{C}}$-linear und $\overline{\langle x, y\rangle}_M = \langle y, x\rangle_M$) derart, daß $\langle x, x\rangle_M > 0$ für $x \neq 0$. Die Metrik $\langle\ ,\ \rangle_M$ heißt F_∞-*invariant*, wenn überdies gilt:

$$\langle x, y\rangle_M = F_\infty\langle x, y\rangle_M = \langle F_\infty x, F_\infty y\rangle_M.$$

14.5. Bemerkung. Wegen $K_{\mathbb{C}} = \bigoplus_{\sigma\in\Sigma(\mathbb{C})} \mathbb{C}$ haben wir eine Zerlegung

$$M_{\mathbb{C}} = M \otimes_{\mathcal{O}_K} K_{\mathbb{C}} = \bigoplus_{\sigma\in X(\mathbb{C})} M_\sigma,$$

mit $M_\sigma = M \otimes_{\mathcal{O}_K,\sigma} \mathbb{C}$, (d.h. $\mathcal{O}_K$ wird vermöge $\sigma\colon K \hookrightarrow \mathbb{C}$, als Teilring von $\mathbb{C}$ aufgefaßt). Eine hermitesche Metrik $\langle\ ,\ \rangle_M$ zerlegt sich in eine direkte Summe

$$\langle x, y\rangle_M = \bigoplus_{\sigma\in X(\mathbb{C})} \langle x_\sigma, y_\sigma\rangle_{M_\sigma}$$

hermitescher Skalarprodukte $\langle\ ,\ \rangle_{M_\sigma}$ auf die $\mathbb{C}$-Vektorräume M_σ. Die F_∞-Invarianz von $\langle\ ,\ \rangle_M$ bedeutet dann die Kommutativität der Diagramme

$$\begin{array}{ccc} M_\sigma \times M_\sigma & \xrightarrow{\langle\,,\rangle_{M_\sigma}} & \mathbb{C} \\ {\scriptstyle F_\infty\times F_\infty}\downarrow & & \downarrow{\scriptstyle F_\infty} \\ M_{\overline{\sigma}} \times M_{\overline{\sigma}} & \xrightarrow{\langle\,,\rangle_{M_{\overline{\sigma}}}} & \mathbb{C} \end{array}$$

für alle $\sigma \in X(\mathbb{C})$.

14.6. Definition. Ein *metrisierter $\mathcal{O}_K$-Modul* $\overline{M}$ ist ein Paar $(M, \langle,\rangle)$, bestehend aus einem endlich erzeugten $\mathcal{O}_K$-Modul M und einer F_∞-invarianten, hermiteschen Metrik auf $M_{\mathbb{C}}$.

14.7. Beispiele. (i) Jedes gebrochene Ideal $\mathfrak{a} \subseteq K$, ist als $\mathcal{O}_K$-Modul M mit der *trivialen Metrik*

$$\langle x, y\rangle = x\overline{y} = \bigoplus_{\sigma\in X(\mathbb{C})} x_\sigma\overline{y}_\sigma$$

auf $\mathfrak{a} \otimes_{\mathbb{Z}} \mathbb{C} = K \otimes_{\mathbb{Q}} \mathbb{C} = K_{\mathbb{C}}$ ausgestattet. Es folgt $\overline{M} = (\mathfrak{a}, \langle\ ,\ \rangle)$ ist ein metrisierter $\mathcal{O}_K$-Modul. Man erhält daraus alle F_∞-invarianten, hermiteschen Metriken auf $\mathfrak{a}$ durch

$$\alpha(x, y) = \alpha x\overline{y} = \bigoplus_\sigma \alpha(\sigma)x_\sigma\overline{y}_\sigma,$$

wobei $\alpha \in K_{\mathbb{C}}$ eine Funktion $\alpha\colon X(\mathbb{C}) \to \mathbb{R}_+^*$ mit $\alpha(\overline{\sigma}) = \alpha(\sigma)$ ist.

(ii) Sei $L|K$ eine endliche Erweiterung und $\mathfrak{A}$ ein gebrochenes Ideal von L, das wir als $\mathcal{O}_K$-Modul M betrachten. Sei $Y(\mathbb{C}) = \mathrm{Hom}(L, \mathbb{C})$ und $|_K\colon Y(\mathbb{C}) \to X(\mathbb{C}), \tau \mapsto \tau|_K$, die

Restriktion. Wir schreiben $\tau|\sigma$, falls $\tau|_K = \sigma$. Dann besteht folgende Zerlegung für den komplexifizierten Modul $\mathfrak{A} \otimes_{\mathbb{Z}} \mathbb{C} = L_{\mathbb{C}}$, den wir mit $M_{\mathbb{C}}$ bezeichnen wollen

$$M_{\mathbb{C}} = \bigoplus_{\tau \in Y(\mathbb{C})} \mathbb{C} = \bigoplus_{\sigma \in X(\mathbb{C})} \left(\bigoplus_{\tau|\sigma} \mathbb{C} \right) = \bigoplus_{\sigma \in X(\mathbb{C})} M_\sigma.$$

M wird zu einem metrisierten $\mathcal{O}_K$-Modul $\overline{M}$, in dem wir jeden der $[L:K]$-dimensionalen $\mathbb{C}$-Vektorräume M_σ mit der Standardmetrik

$$\langle x, y \rangle_{M_\sigma} = \sum_{\tau|\sigma} x_\tau \overline{y}_\tau$$

versehen.

14.8. Sei $\overline{\mathfrak{a}} = \mathfrak{a}_f \mathfrak{a}_\infty$ ein vollständiges Ideal, dann bestimmt $\overline{\mathfrak{a}}$ wie folgt einen invertierbaren, metrisierten $\mathcal{O}_K$-Modul $L(\overline{\mathfrak{a}})$: Nach voriger Bemerkung ist $\mathfrak{a}_f$ ein invertierbarer $\mathcal{O}_K$-Modul und mit $\mathfrak{a}_\infty = (r_\sigma)_{\sigma \in X(\mathbb{C})}$ erhalten wir auf $(\mathfrak{a}_f)_{\mathbb{C}} = \mathfrak{a}_f \otimes_{\mathbb{Z}} \mathbb{C} = K_{\mathbb{C}}$ die Metrik

$$\langle x, y \rangle_{\mathfrak{a}} = \bigoplus_{\sigma \in X(\mathbb{C})} r_\sigma^2 x_\sigma \overline{y_\sigma}$$

Falls $\overline{\mathfrak{a}} = \mathfrak{a}_f = \mathfrak{a}$, d.h. wenn $\mathfrak{a}_\infty = (1, (1)_{\sigma \in x(\mathbb{C})})$ ist, dann erhalten wir die triviale Metrik und schreiben $\overline{L}(\mathfrak{a})$ anstelle von $L(\overline{\mathfrak{a}})$.

14.9. Proposition. *(i) Sind $\overline{M}, \overline{M}'$ metrisierte $\mathcal{O}_K$-Moduln, so sind auch*
die direkte Summe $M \oplus M'$ mit der Metrik $\langle x \oplus x', y + y' \rangle_{M+M'} = \langle x, y \rangle_M + \langle x', y' \rangle_{M'}$,
das Dual $M^\vee = \mathrm{Hom}_{\mathcal{O}_K}(M, \mathcal{O}_K)$ mit der Metrik $\langle x^\vee, y^\vee \rangle_{M^\vee} = \overline{\langle x, y \rangle}_M$, wobei $x^\vee = \langle ., x \rangle_M : M_{\mathbb{C}} \to K_{\mathbb{C}}$,
das Tensorprodukt $M \otimes M'$ mit der Metrik $\langle x \otimes x', y \otimes y' \rangle_{M \otimes M'} = \langle x, y \rangle_M \cdot \langle x', y' \rangle_{M'}$ und die n-te äußere Potenz $\wedge^n M$ mit der Metrik $\langle x_1 \wedge \ldots \wedge x_n, y_1 \wedge \ldots \wedge y_n \rangle_{\Lambda^n M} = \det(\langle x_i, y_j \rangle_M)$ auf natürliche Art und Weise metrisierte $\mathcal{O}_K$-Moduln, die wir mit $\overline{M} \oplus \overline{M}'$, $\overline{M}^\vee$, $\overline{M} \otimes \overline{M}'$ und $\wedge^n \overline{M}$ bezeichnen.
(ii) Es bestehen die Identitäten $\overline{M} \otimes \overline{N} \cong \overline{N} \otimes \overline{M}$, $(\overline{M} \otimes \overline{N}) \otimes \overline{L} \cong \overline{M} \otimes (\overline{N} \otimes \overline{L})$ und $\overline{M} \otimes (\overline{N} \oplus \overline{L}) \cong (\overline{M} \otimes \overline{N}) \oplus (\overline{M} \otimes \overline{L})$
Beweis. Übung. □

14.10. Definition. Wir nennen zwei metrisierte $\mathcal{O}_K$-Moduln M und M' *isometrisch*, falls es einen Isomorphismus $M \to M'$ von $\mathcal{O}_K$-Moduln gibt, der eine Isometrie $f_{\mathbb{C}} : M_{\mathbb{C}} \to M'_{\mathbb{C}}$, d.h., $\langle x, y \rangle_M = \langle f(x), f(y) \rangle_{M'}$, induziert.

14.11. Definition. Die *arithmetische Picardgruppe* $\widehat{\mathrm{Pic}}(\mathcal{O}_K)$ ist definiert als die Menge der Isometrieklassen invertierbarer, metrisierter $\mathcal{O}_K$-Moduln, d.h.,

$$\widehat{\mathrm{Pic}}(\mathcal{O}_K) = \{\text{invertierbare, metrisierte } \mathcal{O}_K\text{-Moduln}\} \Big/ \text{Isometrie}.$$

14.12. Satz

(i) *Zwei vollständige Ideale* $\overline{\mathfrak{a}}$ *und* $\overline{\mathfrak{b}}$ *liefern genau dann isometrische metrisierte* $\mathcal{O}$*-Moduln* $\overline{L}(\overline{\mathfrak{a}})$ *und* $\overline{L}(\mathfrak{b})$*, wenn sie sich um ein vollständiges Hauptideal* $(\overline{a})$ *unterscheiden, d.h. falls* $\overline{\mathfrak{a}} = \overline{(a)}\overline{\mathfrak{b}}$.

(ii) *Jeder invertierbare metrisierte* $\mathcal{O}_K$*-Modul ist isometrisch zu einem metrisierten* $\mathcal{O}_K$*-Modul der Gestalt* $L(\overline{\mathfrak{a}})$.

(iii) *Es gilt:* $L(\overline{\mathfrak{ab}}) \cong L(\overline{\mathfrak{a}}) \otimes L(\overline{\mathfrak{b}})$ *und* $L\left(\overline{(\mathfrak{a})^{-1}}\right) \cong L(\mathfrak{a})^\vee$.

Beweis. Seien $\overline{\mathfrak{a}} = \big(\mathfrak{a}_f, (r_\sigma)_{\sigma\in X(\mathbb{C})}\big)$, $\overline{\mathfrak{b}} = \big(\mathfrak{b}_f, (s_\sigma)_{\sigma\in X(\mathbb{C})}\big)$ und $(\overline{a}) = \big((a), (|\sigma(a)^{-1}|)_{\sigma\in X(\mathbb{C})}\big)$. Angenommen $\overline{\mathfrak{a}} = \overline{(a)} \cdot \overline{\mathfrak{b}}$, dann ist $\mathfrak{a}_f = (a)\cdot\mathfrak{b}_f$ und $r_\sigma = |\sigma(a)|^{-1}s_\sigma$ für alle $\sigma \in X(\mathbb{C})$. Der $\mathcal{O}_K$-Modulisomorphismus $m_a : \mathfrak{b}_f \to \mathfrak{a}_f$ sei gegeben durch $x \mapsto ax$. Dann gilt:

$$\begin{aligned}\langle x, y\rangle_{\mathfrak{b}} &= \sum_{\sigma\in X(\mathbb{C})} s_\sigma^2 x_\sigma \overline{y_\sigma} = \sum_{\sigma\in X(\mathbb{C})} s_\sigma^2 |\sigma(a)|^{-2}\, \sigma(a) x_\sigma \overline{\sigma(a) y_\sigma} = \sum_{\sigma\in X(\mathbb{C})} r_\sigma^2 (ax)_\sigma \overline{(ay)_\sigma} \\ &= \langle ax, ay\rangle_{\mathfrak{a}},\end{aligned}$$

wobei die Gleichheit wegen $\sigma(a)\overline{\sigma(a)} = |\sigma(a)|^2$ gilt. Daher sind $L(\overline{\mathfrak{a}})$ und $L(\overline{\mathfrak{b}})$ isometrisch. Sei nun $g\colon L(\overline{\mathfrak{a}}) \to L(\overline{\mathfrak{b}})$ eine Isometrie. Dann ist g als $\mathcal{O}_K$-Modulisomorphismus gegeben durch die Multiplikation

$$m_a\colon \mathfrak{b}_f \to \mathfrak{a}_f,$$

mit $a \in \mathfrak{b}_f^{-1}\mathfrak{a}_f \cong \mathrm{Hom}_{\mathcal{O}_K}(\mathfrak{b}_f, \mathfrak{a}_f)$. Aus der zweiten Bedingung an g folgt:

$$\sum s_\sigma^2 x_\sigma \overline{y}_\sigma = \langle x, y\rangle_{\mathfrak{b}} = \langle m_a x, m_a y\rangle_{\mathfrak{a}} = a\overline{a}\langle x, y\rangle_{\mathfrak{a}} = \sum |a_\sigma|^2 r_\sigma^2 x_\sigma \overline{y}_\sigma$$

und daraus $|\sigma(a)|^{-1}s_\sigma = r_\sigma$, weil alle $r_\sigma, s_\sigma \in \mathbb{R}^+$ sind. Es folgt: $\overline{\mathfrak{a}} = (\overline{a})\overline{\mathfrak{b}}$.

(ii) Sei L ein invertierbarer metrisierter $\mathcal{O}_K$-Modul. Es bezeichne f den obigen Isomorphismus (13.3.1)

$$f\colon L \to \mathfrak{a}_f, \quad x \mapsto f(x)$$

auf ein gebrochenes Ideal. Durch den Isomorphismus $f_{\mathbb{C}}\colon L_{\mathbb{C}} \to (\mathfrak{a}_f)_{\mathbb{C}} = K_{\mathbb{C}}$, d.h. durch die die Fortsetzung von f auf $L_{\mathbb{C}}$, erhalten wir auf $K_{\mathbb{C}}$ die F_∞-invariante, hermitesche Metrik

$$h(x, y) = \langle f_{\mathbb{C}}^{-1}(x),\ f_{\mathbb{C}}^{-1}(y)\rangle_L.$$

Diese ist von der Form

$$h(x, y) = \sum_{\sigma\in X(\mathbb{C})} r_\sigma^2 x_\sigma \overline{y}_\sigma.$$

mit $r_\sigma \in \mathbb{R}^+$ und $r_\sigma = r_{\overline{\sigma}}$. Also ist $\overline{\mathfrak{a}} = \big(\mathfrak{a}_f, (r_\sigma)_{\sigma\in X(\mathbb{C})}\big)$ ein vollständiges Ideal, so daß L isometrisch zu $L(\overline{\mathfrak{a}})$ ist.

(iii) Sei $\overline{\mathfrak{a}} = \mathfrak{a}_f \cdot \mathfrak{a}_\infty$ und $\overline{\mathfrak{b}} = \mathfrak{b}_f \cdot \mathfrak{b}_\infty$. Der Abbildung $\mathfrak{a}_f \otimes \mathfrak{b}_f \to \mathfrak{a}_f\mathfrak{b}_f$, gegeben durch $a \otimes b \mapsto ab$, ist ein Isomorphismus zwischen $L(\mathfrak{a}) \otimes_{\mathcal{O}_K} L(\mathfrak{b})$ und $L(\mathfrak{ab})$. Wegen

$$\langle ab, a'b'\rangle_{\mathfrak{ab}} = \sum_{\sigma\in X(\mathbb{C})} r_\sigma^2 s_\sigma^2 a_\sigma b_\sigma \overline{a'_\sigma b'_\sigma} = \sum_{\sigma\in X(\mathbb{C})} r_\sigma^2 a_\sigma \overline{a}'_\sigma \cdot s_\sigma^2 b_\sigma \overline{b'_\sigma} = \langle a, a'\rangle_{\mathfrak{a}} \cdot \langle b, b'\rangle_{\mathfrak{b}}$$

ist dies sogar eine Isometrie.
Der $L(\overline{\mathfrak{a}})^\vee$ unterliegende $\mathcal{O}_K$-Modul $\mathrm{Hom}_{\mathcal{O}_K}(\mathfrak{a}_f, \mathcal{O}_K)$ wird vermöge der Abbildung

$$\begin{aligned} g : \mathfrak{a}_f^{-1} &\to \mathrm{Hom}_{\mathcal{O}_K}(\mathfrak{a}_f, \mathcal{O}_K) \\ a &\mapsto (g(a) : x \mapsto ax) \end{aligned}$$

isomorph zu $\mathfrak{a}_f^{-1}$. Für den induzierten $K_\mathbb{C}$-Isomorphismus gilt:

$$g_\mathbb{C}(x)(y) = xy = \sum_{\sigma \in X(\mathbb{C})} r_\sigma^{-2} r_\sigma^2 x_\sigma \overline{y}_\sigma = \left(r_\sigma^{-2}\right)_{\sigma \in X(\mathbb{C})} \cdot \langle x, y \rangle_{L(\overline{\mathfrak{a}})} = \left(r_\sigma^{-2}\right)_{\sigma \in X(\mathbb{C})} \cdot x^\vee(y).$$

Es folgt

$$\begin{aligned} \langle g_\mathbb{C}(x), g_\mathbb{C}(y) \rangle_{L(\overline{\mathfrak{a}})^\vee} &= \left(r_\sigma^{-4}\right)_{\sigma \in X(\mathbb{C})} \langle x^\vee, y^\vee \rangle_{L(\overline{\mathfrak{a}})^\vee} = \left(r_\sigma^{-4}\right)_{\sigma \in X(\mathbb{C})} \overline{\langle \overline{x}, \overline{y} \rangle}_{L(\overline{\mathfrak{a}})} = \left(r_\sigma^{-2}\right)_{\sigma \in X(\mathbb{C})} x\overline{y} \\ &= \langle x, y \rangle_{L((\overline{\mathfrak{a}})^{-1})} \end{aligned}$$

Deshalb besteht die Isometrie $L(\overline{\mathfrak{a}})^\vee \cong L((\overline{\mathfrak{a}})^{-1})$. □

14.13. Korollar. *Es bestehen Gruppenisomorphismen*

$$\widehat{\mathrm{Pic}}(\mathcal{O}_K) \cong \widehat{Cl}(\mathcal{O}_K) \cong \widehat{\mathrm{CH}}^1(\mathcal{O}_K).$$

Beweis. Wir wissen bereits $\widehat{Cl}(\mathcal{O}_K) \cong \widehat{\mathrm{CH}}^1(\mathcal{O}_K)$. Es sei $[\overline{\mathfrak{a}}]$ die Klasse von $\overline{\mathfrak{a}}$ in $\widehat{Cl}(\mathcal{O}_K)$ und $[L(\overline{\mathfrak{a}})]$ die Isometrieklasse von $L(\overline{\mathfrak{a}})$. Die Zuordnung $[\overline{\mathfrak{a}}] \mapsto [L(\overline{\mathfrak{a}})]$ ist nicht von der Wahl der Repräsentanten abhängig, denn ist $\overline{\mathfrak{b}}$ ein anderer Repräsentant, so ist $\overline{\mathfrak{a}} = (\overline{a})\overline{\mathfrak{b}}$ und $L(\overline{\mathfrak{a}})$ ist aufgrund obigen Satzes isometrisch zu $L(\overline{\mathfrak{b}})$. Diese Zuordnung ist wegen

$$[L(\overline{\mathfrak{a}}\overline{\mathfrak{b}})] = [L(\overline{\mathfrak{a}}) \otimes_{\mathcal{O}_K} L(\overline{\mathfrak{b}})] = [L(\overline{\mathfrak{a}})][L(\overline{\mathfrak{b}})]$$

ein muliplikativer Homomorphismus. □

15 Arithmetische K-Gruppen

15.1. Definition. Eine *kurze exakte Sequenz metrisierter $\mathcal{O}_K$-Moduln*

$$0 \longrightarrow \overline{M}' \xrightarrow{\alpha} \overline{M} \xrightarrow{\beta} \overline{M}'' \longrightarrow 0$$

ist eine kurze exakte Sequenz der unterliegenden $\mathcal{O}_K$-Moduln

$$0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0,$$

so daß die induzierte kurze exakte Sequenz von hermiteschen Räumen

$$0 \longrightarrow (M'_\mathbb{C}, \langle\ ,\ \rangle_{M'}) \xrightarrow{\alpha_\mathbb{C}} (M, \langle\ ,\ \rangle_M) \xrightarrow{\beta_\mathbb{C}} (M'', \langle\ ,\ \rangle_{M''}) \longrightarrow 0$$

isometrisch spaltet, d.h. $\langle x', y'\rangle_{M'} = \langle \alpha_{\mathbb{C}}(x'), \alpha_{\mathbb{C}}(y')\rangle_M$ und für alle $x, y \in \alpha_{\mathbb{C}}(M'_{\mathbb{C}})^{\perp} \subseteq M$ gilt $\langle x, y\rangle_M = \langle \beta_{\mathbb{C}}(x), \beta_{\mathbb{C}}(y))_{M''}$.

15.2. Definition. Sei $\overline{M}$ ein metrisierter, projektiver $\mathcal{O}_K$-Modul und es bezeichne $\{\overline{M}\}$ seine Isometrieklasse. Dann setzen wir $\widehat{F}_0(\mathcal{O}_K) = \bigoplus_{\{\overline{M}\}} \mathbb{Z}\{\overline{M}\}$ und $\widehat{R}_0(\mathcal{O}_K)$ sei die Untergruppe von $\widehat{F}_0(\mathcal{O}_K)$, die durch alle Elemente der Gestalt $\{\overline{M'}\} - \{\overline{M}\} - \{\overline{M''}\}$ erzeugt wird, welche aus einer kurzen exakten Sequenz metrisierter $\mathcal{O}_K$-Moduln

$$0 \to \overline{M'} \to \overline{M} \to \overline{M''} \to 0 \tag{15.2.1}$$

entstehen.

15.3. Definition. Die *arithmetische K-Gruppe* $\widehat{K}_0(\mathcal{O}_K)$ *von* $\mathcal{O}_K$ (oder auch vollständige Grothendieckgruppe) ist definiert als der Quotient

$$\widehat{K}_0(\mathcal{O}_K) = \widehat{F}_0(\mathcal{O}_K)/\widehat{R}_0(\mathcal{O}_K).$$

Die Klasse eines metrisierten $\mathcal{O}_K$-Moduls $\overline{M}$ wird mit $[\overline{M}]$ bezeichnet (präziser wäre zu sagen, daß $[\overline{M}]$ die Klasse der Isometrieklasse $\{\overline{M}\}$ ist). Beachte, aus (15.2.1) folgt:

$$[\overline{M}] = [\overline{M'}] + [\overline{M''}] = [\overline{M'} \oplus \overline{M''}].$$

Für zwei metrisierte $\mathcal{O}_K$-Moduln $\overline{M}, \overline{M'}$ setzen wir

$$\{\overline{M}\}\{M'\} = \{\overline{M} \otimes \overline{M'}\}. \tag{15.3.1}$$

Proposition. *Lineare Fortsetzung von* (15.3.1) *induziert eine Ringstruktur auf* $\widehat{K}_0(\mathcal{O}_K)$. *Das neutrale Element der Multiplikation ist* $[L(\mathcal{O})] = [1]$.

Beweis. Die Behauptung folgt aus den Identitäten von Proposition 14.9(ii) und der Tatsache, daß alle betrachteten Moduln projektiv sind. □

15.4. Proposition. *Sei* $\overline{\mathfrak{a}}$ *ein vollständiges Ideal und* $L(\overline{\mathfrak{a}})$ *der zugehörige metrisierte invertierbare Modul. Die Abbildung* $\widehat{Cl}(\mathcal{O}_K) \to \widehat{K}_0(\mathcal{O}_K)$ *gegeben durch* $[\overline{\mathfrak{a}}] \mapsto [L(\overline{\mathfrak{a}})]$, *ist ein Homomorphismus, dessen Bild die Einheitengruppe* $\widehat{K}_0(\mathcal{O}_K)^*$ *von* $\widehat{K}_0(\mathcal{O}_K)$ *ist.*

Beweis. Dies wurde schon gezeigt. □

15.5. Satz. *Als additive Gruppe wird* $\widehat{K}_0(\mathcal{O}_K)$ *durch Elemente der Form* $[L(\overline{\mathfrak{a}})]$ *erzeugt.*

15.6. Beweis. Sei $\overline{M}$ ein metrisierter $\mathcal{O}_K$-Modul. Aus dem Struktursatz für projektive Moduln folgt $M \simeq \mathcal{O}_K^n \oplus \mathfrak{a}$. Indem wir die Metrik von M auf $\mathcal{O}^n$ einschränken und auf $\mathfrak{a}$ die Metrik wählen, die durch den Isomorphismus $(\mathcal{O}_u^n)_{\mathbb{C}}^{\perp} \cong \mathfrak{a}_{\mathbb{C}}$ induziert werden, erhalten wir die kurze exakte Sequenz metrisierter $\mathcal{O}_K$-Moduln

$$0 \to \overline{\mathcal{O}^n} \to \overline{M} \to L(\overline{\mathfrak{a}}) \to 0.$$

Auf analoge Art und Weise erhalten wir für jedes $m \in \mathbb{N}$ eine kurze exakte Sequenz metrisierter $\mathcal{O}_K$-Moduln

$$0 \to \overline{\mathcal{O}}^{m-1} \to \overline{\mathcal{O}}^m \to L(\overline{\mathcal{O}}) \to 0.$$

Mit vollständiger Induktion über dem Rang erhalten wir die Behauptung. □

15.7. Lemma. *Sei* $A = \left(\begin{smallmatrix} \alpha & \gamma \\ \overline{\gamma} & \beta \end{smallmatrix}\right) \in M_2(K_{\mathbb{C}})$, *so daß*

$$\langle x \oplus y, x' \oplus y' \rangle_A = \alpha x\overline{x}' + \gamma x\overline{y}' + \delta y\overline{x}' + \beta y\overline{y}'$$

eine hermitesche, F_∞*-invariante Metrik auf* $K_{\mathbb{C}} \oplus K_{\mathbb{C}}$ *bestimmt. Es seien* L_1 *und* L_2 *invertierbare Moduln. Wir schreiben* $A \sim A'$, *falls* $[(L_1 \oplus L_2, \langle\ ,\ \rangle_A)] = [(L_1 + L_2, \langle\ ,\ \rangle_{A'})] \in \widehat{K}_0(\mathcal{O}_K)$. *Dann gilt für alle* L, L'

$$\left(\begin{smallmatrix} \alpha & \gamma \\ \overline{\gamma} & \beta \end{smallmatrix}\right) \sim \left(\begin{smallmatrix} \alpha & 0 \\ 0 & \beta - \frac{\gamma\overline{\gamma}}{\alpha} \end{smallmatrix}\right)$$

und für jedes $\delta \in K_{\mathbb{C}},\ \delta > 0$, *gilt*

$$\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \sim \begin{pmatrix} \frac{\alpha\beta}{\gamma} & 0 \\ 0 & \delta \end{pmatrix}.$$

Beweis. Wir betrachten zuerst die kurze exakte Sequenz

$$0 \to L_1 \to L_1 \oplus L_2 \to L_2 \to 0.$$

Wenn wir $\overline{L}_1 = (L_1, \alpha\langle\ ,\ \rangle)$, wobei mit $\alpha\langle\ ,\ \rangle$ die Metrik gemeint ist, die durch $\alpha\langle\ ,\ \rangle \mapsto \Sigma\alpha x_\sigma \overline{y\sigma}$ induziert wird, und $\overline{L_1 \oplus L_2} = (L_1 \oplus L_2, \langle\ ,\ \rangle_A)$ wählen, dann ist das orthogonale Komplement von $(L_1)_{\mathbb{C}}$ in $(L_1 \oplus L_2)_{\mathbb{C}}$ gegeben durch

$$\begin{aligned}(L_1)_{\mathbb{C}}^{\perp} &= \{a \oplus b \in K_{\mathbb{C}} \oplus K_{\mathbb{C}} \mid \langle x \oplus 0, a \oplus b\rangle_A = \alpha x\overline{a} + \gamma x\overline{b} = 0\ \forall x \in (L_1)_{\mathbb{C}}\} \\ &= \{(-\overline{\gamma}/\alpha)b \oplus b \mid b \in K_{\mathbb{C}}\}.\end{aligned}$$

Sei $\pi : (L_1)_{\mathbb{C}}^{\perp} \to (L_2)_{\mathbb{C}}$ der Isomorphismus gegeben durch $(-\gamma/\alpha)b \oplus b \mapsto b$. Die von π induzierte Metrik ist eindeutig bestimmt durch

$$\begin{aligned}\delta &= \langle \pi^{-1}(1), \pi^{-1}(1)\rangle_A = \langle(-\overline{\gamma}/\alpha)1 \oplus 1, -\overline{\gamma}/\alpha 1 \oplus 1\rangle_A \\ &= \alpha\frac{\gamma\overline{\gamma}}{\alpha^2} - \gamma\frac{\overline{\gamma}}{\alpha} + \overline{\gamma}\frac{\gamma}{\alpha} + \beta = \beta - \frac{\gamma\overline{\gamma}}{\alpha}.\end{aligned}$$

Es folgt die kurze exakte Sequenz metrisierter $\mathcal{O}_K$-Moduln

$$0 \to (L_1, \alpha\langle\ ,\ \rangle) \to (L_1 \oplus L_2, \langle\ ,\ \rangle_A) \to (L_2, \beta - \frac{\gamma\overline{\gamma}}{\alpha}\langle\ ,\ \rangle) \to 0,$$

d.h. $(L_1, \alpha\langle\ ,\ \rangle) + (L_2, \beta - \frac{\gamma\overline{\gamma}}{\alpha}\langle\ ,\ \rangle) - (L_1 \oplus L_2, \langle\ ,\ \rangle_A) \in \hat{R}_0(\mathcal{O}_K)$. Also gilt

$$\begin{aligned}&[L_1 \oplus L_2, \alpha\langle\ ,\ \rangle \oplus \beta - \frac{\gamma\overline{\gamma}}{\alpha}\langle\ ,\ \rangle] = [L_1 \oplus L_2, \langle\ ,\ \rangle_A] \\ &\Leftrightarrow \begin{pmatrix} \alpha & 0 \\ 0 & \beta - \frac{\gamma\overline{\gamma}}{\alpha} \end{pmatrix} \sim \begin{pmatrix} \alpha & \gamma \\ \overline{\gamma} & \beta \end{pmatrix} \\ &\Leftrightarrow \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \sim \begin{pmatrix} \alpha & \gamma \\ \overline{\gamma} & \beta + \frac{\gamma\overline{\gamma}}{\alpha} \end{pmatrix}. \qquad (15.7.1)\end{aligned}$$

Verfahren wir analog mit der kurzen exakten Sequenz

$$0 \to L_2 \to L_1 \oplus L_2 \to L_1 \to 0,$$

so erhalten wir

$$\begin{pmatrix} \alpha' & 0 \\ 0 & \beta' \end{pmatrix} \sim \begin{pmatrix} \alpha' + \frac{\gamma'\overline{\gamma}'}{\beta'} & \gamma' \\ \overline{\gamma}' & \beta' \end{pmatrix} \tag{15.7.2}$$

Setzen wir in (15.7.2) $\beta' = \beta + \frac{\gamma\overline{\gamma}}{\alpha}$ und $\alpha' = \frac{\alpha\beta}{\beta+\frac{\gamma\overline{\gamma}}{\alpha}}$, so sind die rechten Seiten von (15.7.1) und (15.7.2) gleich und wir erhalten

$$\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \sim \begin{pmatrix} \frac{\alpha\beta}{\beta+\frac{\gamma\overline{\gamma}}{\alpha}} & 0 \\ 0 & \beta + \frac{\gamma\overline{\gamma}}{\alpha} \end{pmatrix},$$

wenn wir noch $\delta = \beta + \frac{\gamma\overline{\gamma}}{\alpha}$ setzen, folgt schließlich, daß für alle $\delta \geq \beta$ gilt:

$$\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \sim \begin{pmatrix} \frac{\alpha\beta}{\delta} & 0 \\ 0 & \delta \end{pmatrix}. \tag{15.7.3}$$

Ersetzen wir α durch $\alpha\beta/\varepsilon$ und β durch ε, dann folgt aus (15.7.3), daß für alle $\kappa \geq \varepsilon > 0$ gilt:

$$\begin{pmatrix} \frac{\alpha\beta}{\varepsilon} & 0 \\ 0 & \varepsilon \end{pmatrix} \sim \begin{pmatrix} \frac{\alpha\beta}{\kappa} & 0 \\ 0 & \kappa \end{pmatrix}.$$

Dies gilt insbesondere auch für $\kappa > \max(\delta, \varepsilon)$, woraus dann folgt daß für alle $\varepsilon > 0$ gilt:

$$\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \sim \begin{pmatrix} \frac{\alpha\beta}{\varepsilon} & 0 \\ 0 & \varepsilon \end{pmatrix}.$$

□

15.8. Satz. *Für alle vollständigen Ideale $\overline{\mathfrak{a}}, \overline{\mathfrak{b}}$ besteht in $\widehat{K}_0(\mathcal{O}_K)$ die Formel*

$$[L(\overline{\mathfrak{a}})] + [L(\overline{\mathfrak{b}})] = [L(\overline{\mathfrak{a}\mathfrak{b}})] + [L(\mathcal{O}_K)] \tag{15.8.1}$$

Beweis. Sei $\overline{\mathfrak{a}} = (\mathfrak{a}, (r_\sigma)_{\sigma\in X(\mathbb{C})}), \overline{\mathfrak{b}} = (\mathfrak{b}, (b_\sigma)_{\sigma\in X(\mathbb{C})})$. Sei $A \in \mathrm{M}_2(K)$ wie im Beweis von Lemma 13.4. Wir betrachten zuerst den metrisierten $\mathcal{O}_K$-Modul

$$\overline{\mathfrak{a} \oplus \mathfrak{b}} = (\mathfrak{a} \oplus \mathfrak{b}, \langle\ ,\ \rangle_{\widetilde{A}}).$$

wobei

$$\begin{aligned} \langle (x_1, y_1)(x_2, y_2) \rangle &= \langle (x_1, y_1)A, (x_2, y_2)A \rangle_{\overline{\mathcal{O}}_K \oplus \overline{\mathfrak{a}\mathfrak{b}}} \\ &= \langle cx_1 + dy_1, cx_2 + dy_2 \rangle + \langle -bx_1 + ay_1, -bx_2 + ay_2 \rangle_{\overline{\mathfrak{a}\mathfrak{b}}}. \end{aligned}$$

Wir schreiben

$$\widetilde{A} = \begin{pmatrix} |c|^2 & c\overline{d} \\ \overline{c}d & |d|^2 \end{pmatrix} + rs \begin{pmatrix} |b|^2 & b\overline{a} \\ \overline{b}a & |a|^2 \end{pmatrix}$$

und $\widetilde{A}$ erfüllt die Voraussetzungen von Lemma 15.7 Mit etwas Mühe berechnet man

$$\begin{aligned} \widetilde{A} &\sim \begin{pmatrix} |c|^2 + rs|b|^2 & 0 \\ 0 & \frac{rs((b\cdot\overline{d}+a\overline{c})(\overline{b}d+\overline{a}c))}{|c|^2+rs|b|^2} \end{pmatrix} \\ &\sim \begin{pmatrix} r & 0 \\ 0 & s\cdot|b\overline{d}+a\overline{c}|^2 \end{pmatrix} \end{aligned}$$

Wir erhalten somit die Behauptung $[L(\overline{\mathfrak{a}})] + [L(\overline{\mathfrak{b}})] = [\overline{\mathfrak{a}\oplus\mathfrak{b}}] = [\mathcal{O}_K] + [L(\overline{\mathfrak{a}\mathfrak{b}})]$ □

15.9. Satz. *Sei $\Gamma_K = \rho(\mathcal{O}_K^*) \subseteq \widehat{H}(K) \simeq \mathbb{R}^{r_1+r_2}$. Dann ist die folgende Sequenz exakt*

$$0 \to \widehat{H}(K)/\Gamma_K \xrightarrow{c} \widehat{K}_0(\mathcal{O}_K) \xrightarrow{\pi} K_0(\mathcal{O}_K) \to 0,$$

hierbei ist $\pi([\overline{M}]) = [M]$ und

$$c(\mathfrak{g}) := [(\mathcal{O}_K, (e^{2g_\sigma})_{\sigma\in X(\mathbb{C})})] - [L(\mathcal{O}_K)].$$

Beweis. Zuerst zeigen wir, daß c ein Homomorphismus ist:

$$\begin{aligned} c(\mathfrak{g}+\mathfrak{h}) &= [(\mathcal{O}_K, (e^{2(g_\sigma+h_\sigma)})_{\sigma\in X(\mathbb{C})})] - [L(\mathcal{O}_K)] \\ &= [(\mathcal{O}_K, (e^{R(g_\sigma)R(h_\sigma)})_{\sigma\in X(\mathbb{C})})]] + [L(\mathcal{O}_K)] - 2[L(\mathcal{O}_K)] \\ &= [(\mathcal{O}_K, (e^{2g_\sigma})_{\sigma\in X(\mathbb{C})})] + [(\mathcal{O}_K, (e^{2h_\sigma})_{\sigma\in X(\mathcal{O})})] - 2[L(\mathcal{O}_K)] \\ &= c(\mathfrak{g}) + c(\mathfrak{h}). \end{aligned}$$

Bei der vorletzten Gleichheit haben wir 15.8 mit $\delta = 1$ verwendet.
Der Homomorphismus π ist offensichtlich surjektiv.
Sei $0 \neq [\overline{M}] \in \widehat{K}_0(\mathcal{O}_K)$ mit $\pi[\overline{M}] = [M] = 0$. Dann gilt wegen $[M] = [N]$ genau dann, wenn $M \cong N$ und weil $[\overline{M}] = \sum_{i=1}^{r} m_i[L(\overline{\mathfrak{a}}_i)]$ ist, sogar

$$\begin{aligned} [\overline{M}] &= \sum n_i[L(\mathfrak{a}_i, (r_\sigma^{(i)})_{\sigma\in X(\mathbb{C})})] - [L(\mathfrak{a}_i, (s_\sigma^{(i)})_{\sigma\in X(\mathbb{C})})] \\ &= \sum n_i[L(\mathcal{O}_K, (r_\sigma^{(i)})_{\sigma\in X(\mathbb{C})})] - [L(\mathcal{O}_K, (s_\sigma^{(i)})_{\sigma\in X(\mathbb{C})})] \\ &= \sum n_i[L(\mathcal{O}_K, (s_\sigma^{(i)} r_\sigma^{(i)})_{\sigma\in X(\mathbb{C})})] - [L(\mathcal{O}_K)]. \end{aligned}$$

Also ist $\mathrm{Im}(c) = \ker(\pi)$. Es bleibt zu zeigen (c) ist injektiv.
Wir müssen zeigen $[L(\mathcal{O}_K, e^{2\mathfrak{g}})] = [L(\mathcal{O}_K)]$ genau dann, wenn $\mathfrak{g} = \rho(a)$ mit $a \in \mathcal{O}_K^*$. Da die Automorphismen des $\mathcal{O}_K$-Moduls $\mathcal{O}_K$ gerade die Morphismen der Form $\mathrm{Im}_a \colon \mathcal{O}_K \to \mathcal{O}_K$, $x \mapsto ax$, sind und weil $e^{2\rho(a)} = (1/|\sigma(a)|^2)_{\sigma\in X(\mathbb{C})}$ ist, folgt die Injektivität. □

15.10. Bemerkung. Aus allgemeinen Prinzipien heraus („5er-Lemma“) erhalten wir somit eine nicht-kanonische Isomorphie

$$\widehat{K}_0(\mathcal{O}_K) \simeq \widehat{H}(K)/\Gamma_K \oplus K_0(\mathcal{O}_K).$$

15.11. Proposition. *Die Rangabbildung* $\overline{M} \mapsto \mathrm{rg}(\overline{M})$ *induziert einen Homomorphismus* $\widehat{K}_0(\mathcal{O}_K) \to \mathbb{Z}$.

Beweis. Klar, weil für kurze exakte Sequenzen $0 \to M' \to M \to M'' \to 0$ gilt, daß $\mathrm{rg}(M) = \mathrm{rg}(M') + \mathrm{rg}(M'')$. □

15.12. Satz. *Die Determinante* $\overline{M} \mapsto \Lambda^{\mathrm{rg}\, M}\overline{M} =: \det(\overline{M})$ *von metrisierten* $\mathcal{O}_K$*-Moduln induziert einen Homomorphismus*

$$\widehat{K}_0(\mathcal{O}_K) \longrightarrow \widehat{\mathrm{Pic}}(\mathcal{O}_K).$$

Beweis. Sei $\overline{M}$ ein metrisierter $\mathcal{O}_K$-Modul, dann ist $\det(\overline{M})$ ein metrisierter invertierbarer $\mathcal{O}_K$-Modul, dieser entspricht bis auf Isometrie einem metrisierten Modul der Gestalt $L(\overline{\mathfrak{a}})$ für ein vollständiges Ideal $\overline{\mathfrak{a}}$. Wir erhalten somit einen Homomorphismus

$$\begin{aligned} \det : \widehat{F}_0(\mathcal{O}_K) &\to \widehat{\mathrm{Pic}}(\mathcal{O}_K) \\ \{\overline{M}\} &\mapsto [\overline{\mathfrak{a}}]. \end{aligned}$$

Wir müssen zeigen, daß $\det(\widehat{R}_0(\mathcal{O}_K)) = [\mathcal{O}_K]$. Dies ist jedoch unmittelbare Konsequenz des folgenden Lemmas. □

15.13. Lemma. *Sei* $0 \to \overline{M}' \to \overline{M} \to \overline{M}'' \to 0$ *eine kurze exakte Sequenz metrisierter* $\mathcal{O}_K$*-Moduln, dann gilt*

$$\det(\overline{M}') \otimes \det(\overline{M}'') \cong \det(\overline{M}).$$

Beweis. Man sieht leicht, daß für jede Wahl eines Schnittes s in der kurzen, exakten Sequenz

$$0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$$

die Abbildung

$$\begin{aligned} \kappa : \quad \det(M') \otimes \det(M'') &\to \det(M) \\ (m'_1 \wedge \ldots \wedge m'_r) \otimes (m''_1 \wedge \ldots \wedge m''_r) &\mapsto (\alpha(m'_1) \wedge \ldots \wedge \alpha(m'_r) \wedge s(m''_1) \wedge \ldots \wedge s(m''_s)) \end{aligned}$$

ein Isomorphismus ist. Die induzierten komplexen Isomorphismen

$$\det(M'_\sigma) \otimes \det(M''_\sigma) \to \det(M_\sigma)$$

bestehen auch, wenn wir anstelle von s_σ durch eine orthogonale Spaltung $s_\sigma^\perp$ ersetzen, d.h. $s_\sigma^\perp M''_\sigma = (\alpha(M'))^\perp$. Wir wählen nun orthogonale Basen $\{v'_1, \ldots, v'_r\}$ von M'_σ und

$\{v_1'', \ldots, v_s''\}$ von M_σ'' und setzen $v' = v_1' \wedge \ldots \wedge v_r'$ und $v'' = v_1'' \wedge \ldots \wedge v_s''$. Dann ist $\langle v', v' \rangle_{\det M_\sigma'} = \det(\langle v_i', v_j \rangle_{ij}) = 1$, ebenso ist $\langle v'', v'' \rangle_{\det M_\sigma''} = 1$ und

$$\begin{aligned}\langle \kappa(v' \otimes v''), \kappa(v' \otimes v'') \rangle_{\det M_\sigma} &= \langle \alpha v' \wedge s_\sigma^\perp v'', \alpha v' \wedge s_\sigma^\perp v'' \rangle_{\det M_\sigma} \\ &= \det \left(\begin{array}{c|c} \langle v_i', v_j' \rangle_{M_\sigma'} & 0 \\ \hline 0 & \langle v_i'', v_j'' \rangle_{M_\sigma''} \end{array} \right) = 1.\end{aligned}$$

Woraus die Behauptung folgt, da v', v'' und $\kappa(v' \otimes v'')$ die jeweiligen Basen sind. □

15.14. Definition. Die Abbildung $\widehat{\mathrm{ch}} : \widehat{K}_0(\mathcal{O}_K) \to \widehat{\mathrm{CH}}(\mathcal{O}_K)$, gegeben durch $\widehat{\mathrm{ch}}(\alpha) = \mathrm{rg}(\alpha) \oplus \widehat{c}_1(\det(\alpha))$, heißt der *arithmetische Cherncharakter*. Sowie hier als auch im folgenden wird $\det \alpha = \mathrm{L}(\mathfrak{a})$ mit $\mathfrak{a}$ identifiziert, wobei $\mathrm{L}(\mathfrak{a})$ den zum Ideal $\mathfrak{a}$ zugehö rigen invertierbaren Modul beschreibt.

15.15. Satz. *Der arithmetische Cherncharakter* $\widehat{\mathrm{ch}} : \widehat{K}_0(\mathcal{O}_K) \longrightarrow \widehat{\mathrm{CH}}(\mathcal{O}_K)$ *ist ein Ringisomorphismus.*

Beweis. Wir zeigen zuerst, daß $\widehat{\mathrm{ch}}$ ein Ringhomomorphismus ist. Additivität besteht, weil

$$\begin{aligned}\widehat{\mathrm{ch}}(\alpha + \beta) &= \mathrm{rg}(\alpha + \beta) \oplus \widehat{c}_1(\det(\alpha + \beta)) \\ &= \mathrm{rg}(\alpha) + \mathrm{rg}(\beta) \oplus \widehat{c}_1(\det(\alpha) \otimes \det(\beta)) \\ &= \mathrm{rg}(\alpha) \oplus \widehat{c}_1(\det(\alpha)) + \mathrm{rg}(\beta) \oplus \det(\beta) \\ &= \widehat{\mathrm{ch}}(\alpha) + \widehat{\mathrm{ch}}(\beta).\end{aligned}$$

Beachte: wie zuvor definiert, steht in $\widehat{K}_0(\mathcal{O}_K)$ $''\cdot''$ für $''\otimes''$, sowie $''+''$ für $\oplus$. Da $\widehat{K}_0(\mathcal{O}_K)$ von invertierbaren metrisierten Moduln erzeugt wird, und $\widehat{\mathrm{ch}}$ additiv ist, genügt es, den Beweis der Multiplikativität für den Fall $\mathrm{rg}(\alpha) = \mathrm{rg}(\beta) = 1$ zu betrachten.

$$\begin{aligned}\widehat{\mathrm{ch}}(\alpha \cdot \beta) &= \mathrm{rg}(\alpha \cdot \beta) \oplus \widehat{c}_1(\det(\alpha \cdot \beta)) \\ &= 1 \oplus (\widehat{c}_1(\det(\alpha)) + \widehat{c}_1(\det(\beta))) \\ &= (1 \oplus \widehat{c}_1(\det(\alpha))) \cdot (1 \oplus \widehat{c}_1(\det(\beta))) \\ &\overset{\text{Def.}}{=} \widehat{\mathrm{ch}}(\alpha) \cdot \widehat{\mathrm{ch}}(\beta)\end{aligned}$$

Die vorletzte Gleichung besteht, weil $xy = 0$ in $\widehat{\mathrm{CH}}(\mathcal{O}_K)$ für alle $x, y \in \widehat{\mathrm{CH}}^1(\mathcal{O}_K)$. Die Behauptung folgt aus der Angabe des inversen Homomorphismus

$$\begin{aligned}\widehat{\mathrm{ch}}^{-1} : \widehat{\mathrm{CH}}(\mathcal{O}_K) &\to \widehat{K}_0(\mathcal{O}_K) \\ r \oplus D &\mapsto (r-1)[1] + [L(\widehat{c}_1^{-1}(D))].\end{aligned}$$

Es gilt:

$$\begin{aligned}\widehat{\mathrm{ch}}(\widehat{\mathrm{ch}}^{-1}(r \oplus D)) &= \widehat{\mathrm{ch}}((r-1)[1] + [L(\widehat{c}_1^{-1}(D))] \\ &= r \oplus \widehat{c}_1(\overline{\mathcal{O}(D)}) = r \oplus D\end{aligned}$$

und für α mit $\mathrm{rg}(\alpha) = 0$ gilt:

$$\begin{aligned}\widehat{\mathrm{ch}}^{-1}(\widehat{\mathrm{ch}}(\alpha)) &= \widehat{\mathrm{ch}}^{-1}(\mathrm{rg}(\alpha) \oplus \widehat{c}_1(\det(\alpha))) \\ &= (\mathrm{rg}(\alpha) - 1)[1] + [\det(\alpha)] \\ &= [\alpha].\end{aligned}$$

Additivität:

$$\begin{aligned}\widehat{\mathrm{ch}}^{-1}(r_1 + r_2 \oplus D_1 + D_2) &= (r_1 + r_2 - 1)[1] + [L(\widehat{c}_1^{-1}(D_1 + D_2))] \\ &= (r_1 + r_2 - 1)[1] + [L(\widehat{c}_1^{-1}(D_1)) \cdot L(\widehat{c}_1^{-1}(D_2))] \\ &= (r_1 + r_2 - 1)[1] - [1] + [L(\widehat{c}_1^{-1}(D_1))] + [L(\widehat{c}_1^{-1}(D_2))] \\ &= \widehat{\mathrm{ch}}^{-1}(r_1 \oplus D_1) + \widehat{\mathrm{ch}}^{-1}(r_2 \oplus D_2)\end{aligned}$$

Multiplikativität:

$$\widehat{\mathrm{ch}}^{-1}(r_1 r_2 \oplus r_1 D_2 + r_2 D_1) = (r_1 r_2 - 1)[1] + r_1[L(\widehat{c}_1^{-1}(D_2))] + r_2[L(\widehat{c}_1^{-1}(D_1))]$$

□

15.16. Definition. Sei $L|K$ eine endliche Erweiterung und es bezeichne $i : K \hookrightarrow L$ die natürliche Inklusion. Dann definieren wir wie folgt eine *Pull-back*-Abbildung

$$i^* \colon \widehat{K}_0(\mathcal{O}_K) \longrightarrow \widehat{K}_0(\mathcal{O}_L). \tag{15.16.1}$$

Ist M ein projektiver $\mathcal{O}_K$-Modul, dann ist $M \otimes_{\mathcal{O}_K} \mathcal{O}_L$ ein projektiver $\mathcal{O}_L$-Modul. Eine hermitesche, F_∞-invariante Metrik $\langle\ ,\ \rangle_M$ auf dem $K_\mathbb{C}$-Modul $M_\mathbb{C} = M \otimes_\mathbb{Z} \mathbb{C} = M \otimes_{\mathcal{O}_K} K_\mathbb{C}$ setzt sich wegen

$$(M \otimes_{\mathcal{O}_K} \mathcal{O}_L)_\mathbb{C} = M \otimes_{\mathcal{O}_K} \mathcal{O}_L \otimes_\mathbb{Z} \mathbb{C} = M \otimes_{\mathcal{O}_K} L_\mathbb{C}$$

zu einer hermiteschen, F_∞-invarianten Metrik auf $(M \otimes_{\mathcal{O}_K} \mathcal{O}_L)_\mathbb{C}$ fort. Wir bezeichnen den so aus $\overline{M} = (M, \langle\ ,\ \rangle_M)$ erhaltenen metrisierten Modul mit $i^*\overline{M}$. Der Morphismus (15.16.1) sei nun durch die Zuordnung $\overline{M} \mapsto [i^*\overline{M}]$ induziert.

15.17. Lemma. *Das Pull-back i^* ist ein wohldefinierter Gruppenhomomorphismus $i^* : \widehat{K}_0(\mathcal{O}_K) \longrightarrow \widehat{K}_0(\mathcal{O}_L)$.*

Beweis. Es genügt zu zeigen, daß $i^*(\widehat{R}_0(\mathcal{O}_K)) \subseteq \widehat{R}_0(\mathcal{O}_L)$. Sei $0 \to M' \to M \to M'' \to 0$ eine kurze exakte Sequenz von $\mathcal{O}_L$-Moduln. Weil $\mathcal{O}_L$ ein projektiver $\mathcal{O}_K$-Modul ist, folgt dann

$$0 \to M' \otimes_{\mathcal{O}_K} \mathcal{O}_L \to M \otimes_{\mathcal{O}_K} \mathcal{O}_L \to M'' \otimes_{\mathcal{O}_K} \mathcal{O}_L \to 0.$$

Ist nun $0 \to \overline{M}' \to \overline{M} \to \overline{M}'' \to 0$ eine kurze exakte Sequenz metrisierter $\mathcal{O}_K$-Moduln, dann ist

$$0 \to i^*\overline{M}' \to i^*\overline{M} \to i^*\overline{M}'' \to 0$$

eine kurze exakte Sequenz von metrisierten $\mathcal{O}_L$-Moduln, da die Metriken auf den komplexifizierten Moduln $i^*M'_\mathbb{C}, i^*M_\mathbb{C}, i^*M''_\mathbb{C}$ durch $L_\mathbb{C}$-lineare Fortsetzung entstanden sind. □

15.18. Proposition. *Die arithmetische K-Gruppe $\widehat{K}_0(\mathcal{O}_.)$ ist ein kovarianter Funktor von der Kategorie der Zahlkörper in die Kategorie der Ringe, wenn einem Morphismus $i\colon K \hookrightarrow L$ der Morphismus $i^*\colon \widehat{K}_0(\mathcal{O}_K) \to \widehat{K}_0(\mathcal{O}_L)$ zugeordnet wird.*

Beweis. Es bleibt zu zeigen: Ist $\begin{array}{ccc} K & \xhookrightarrow{i} & L \\ & \searrow^{h} & \downarrow{\scriptstyle j} \\ & & M \end{array}$ ein kommutatives Diagramm von Inklusionen von Zahlkörpern, dann besteht für die Pull-back Abbildungen h^*, j^*, i^* die Identität $h^* = j^* \circ c^*$. Diese Identität folgt jedoch leicht aus obigen Betrachtungen. □

15.19. Definition. Sei $L|K$ eine endliche Erweiterung und $i : K \hookrightarrow L$ die natürliche Inklusion. Dann definieren wir wie folgt eine Push-forward Abbildung

$$i_*\colon \widehat{K}_0(\mathcal{O}_L) \longrightarrow \widehat{K}_0(\mathcal{O}_K). \tag{15.19.1}$$

Sei $\overline{M} = (M\langle\ ,\ \rangle_M)$ ein metrisierter $\mathcal{O}_K$-Modul. Ist M ein projektiver $\mathcal{O}_L$-Modul, dann ist M auch ein projektiver $\mathcal{O}_K$-Modul, da $\mathcal{O}_L$ ein endlich erzeugter $\mathcal{O}_K$-Modul ist. Für die Komplexifizierung $M_{\mathbb{C}} = M \otimes_{\mathbb{Z}} \mathbb{C}$ haben wir bekanntermaßen die Zerlegung

$$M_{\mathbb{C}} = \bigoplus_{\tau\in X(\mathbb{C})} M_\tau = \bigoplus_{\sigma\in X(\mathbb{C})} \Big(\bigoplus_{\tau|\sigma} M_\tau\Big) =: \bigoplus_{\sigma\in Y(\mathbb{C})} M_\sigma.$$

Damit definieren wir dann die F_∞-invariante Metrik $\langle x, y\rangle_{M_\sigma} = \sum_{\tau|\sigma} \langle x_\tau, y_\tau\rangle_{M_\tau}$. Wir bezeichnen den so erhaltenen metrisierten $\mathcal{O}_K$-Modul mit $i_*\overline{M}$. Der Morphismus (15.19.1) sei von der Zuordnung $\overline{M} \mapsto [i_*\overline{M}]_{i_*}$.

15.20. Lemma. *Das Push-forward ist ein wohldefinierter Gruppenhomomorphismus.*

Beweis. Es genügt zu zeigen $i_*\widehat{R}_0(\mathcal{O}_L) \subseteq \widehat{R}_0(\mathcal{O}_K)$. Weil für jede kurze Sequenz metrisierter $\mathcal{O}_L$-Moduln $0 \to \overline{M}' \to \overline{M} \to \overline{M}'' \to 0$ auch ihr Push-forward

$$0 \to i_*\overline{M}' \to i_*\overline{M} \to i_*\overline{M}'' \to 0$$

eine solche ist, folgt die Behauptung. □

15.21. Proposition. *Die arithmetische K-Gruppe $\widehat{K}_0(\mathcal{O}_.)$ ist ein kontravarianter Funktor von der Kategorie der Zahlkörper in die Kategorie der abelschen Gruppen, wenn einem Morphismus $i\colon K \hookrightarrow L$ der Morphismus $i_* : \widehat{K}_0(\mathcal{O}_L) \to \widehat{K}_0(\mathcal{O}_K)$ zugeordnet wird.*

Beweis. Es genügt zu zeigen, daß für jedes kommutative Diagramm $\begin{array}{ccc} K & \xhookrightarrow{i} & L \\ & \searrow^{h} & \downarrow{\scriptstyle j} \\ & & M \end{array}$ gilt: $h_* = i_* \circ j_*$. Dies folgt jedoch unmittelbar auf der Defintion von i_*. □

15.22. Bemerkung. Folgendes Diagramm ist kommutativ:

$$\begin{array}{ccc} \widehat{K}_0(\mathcal{O}_L) & \times & \widehat{K}_0(\mathcal{O}_L) \longrightarrow \widehat{K}_0(\mathcal{O}_L) \\ \downarrow{\scriptstyle i_*} & & \uparrow{\scriptstyle i^*} \qquad\quad \downarrow{\scriptstyle i_*} \\ \widehat{K}_0(\mathcal{O}_K) & \times & \widehat{K}_0(\mathcal{O}_K) \longrightarrow \widehat{K}_0(\mathcal{O}_K). \end{array}$$

Dies folgt aus der Formel

$$i_*\left(\overline{M} \otimes_{\mathcal{O}_L} i^*\overline{N}\right) \cong i_*\overline{M} \otimes_{\mathcal{O}_K} \overline{N},$$

die für alle metrisierten $\mathcal{O}_L$-Moduln $\overline{M}$ und alle metrisierten $\mathcal{O}_K$-Moduln $\overline{N}$ gilt.

16 Grothendieck-Riemann-Roch Theorem für arithmetische Kurven

In den nächsten Vorlesungen wollen wir das folgende Riemann-Roch Problem lösen: Existiert ein Morphismus, so daß das Diagramm

$$\begin{array}{ccc} \widehat{K}_0(\mathcal{O}_L) & \xrightarrow{?} & \widehat{\mathrm{CH}}(\mathcal{O}_L) \\ \downarrow{\scriptstyle i_*} & & \downarrow{\scriptstyle i_*} \\ \widehat{K}_0(\mathcal{O}_K) & \xrightarrow{\widehat{\mathrm{ch}}} & \widehat{\mathrm{CH}}(\mathcal{O}_K) \end{array}$$

kommutiert?

16.1. Satz. *Es gilt für alle $\xi \in \widehat{K}_0(\mathcal{O}_L)$ die Formel*

$$\widehat{\mathrm{ch}}(i_*\xi) = [L:K]\,\mathrm{rg}(\xi) \oplus i_*\widehat{c}_1(\det(\xi)) + \mathrm{rg}(\xi)\cdot\widehat{c}_1(\det(L(i_*\mathcal{O}_L))).$$

Beweis. Per definitionem ist

$$\mathrm{rg}(i_*\overline{M}) = \dim_K(i_*M \otimes_{\mathcal{O}_K} K) = \dim_K(M_L) = \dim_L(M_L)\cdot[L:K] = \mathrm{rg}_L(M_L)\cdot[L:K].$$

Beide Bestandteile in $\widehat{\mathrm{CH}}^1(\mathcal{O}_K)$ der rechten Seite sind additiv auf kurzen exakten Sequenzen. Mittels vollständiger Induktion können wir uns auf den Fall beschränken, daß ξ ein metrisierter invertierbarer $\mathcal{O}_L$-Modul der Gestalt $L(\overline{\mathfrak{a}})$ ist. Es genügt also zu zeigen:

$$\det(i_*L(\overline{\mathfrak{a}})) = L(N_{L|K}(\overline{\mathfrak{a}})) \otimes_{\mathcal{O}_K} \det(i_*L(\mathcal{O}_L)). \tag{16.1.1}$$

Für die unterliegenden Moduln bedeutet (16.1.1) die Gleichheit von Idealen:

$$\det_{\mathcal{O}_K} \mathfrak{a}_f = N_{L|K}(\mathfrak{a}_f)\cdot\det_{\mathcal{O}_K}\mathcal{O}_L. \tag{16.1.2}$$

Da ein Ideal $\mathfrak{b}$ in einem Dedekindring $\mathcal{O}$ eindeutig durch seine $\mathfrak{p}$-Komponenten $\mathfrak{b}_\mathfrak{p} = \mathfrak{b}\otimes\mathcal{O}_\mathfrak{p}$ bestimmt ist (vgl. 4.11), genügt es (16.1.2) lokal zu zeigen. Für jedes Primideal $\mathfrak{p}$ von $\mathcal{O}_K$ sind $(\mathcal{O}_L)_\mathfrak{p} = (\mathcal{O}_K\setminus\mathfrak{p})^{-1}\mathcal{O}_L$ und $(\mathcal{O}_K)_\mathfrak{p}$ Hauptidealringe (vgl. Satz 2.16).

Sei nun $\alpha_\mathfrak{p}$ ein Erzeugendes von $(\mathfrak{a}_f)_\mathfrak{p}$ und $w_1,\ldots,w_n$ eine Ganzheitsbasis von $(\mathcal{O}_L)_\mathfrak{p}$ über $(\mathcal{O}_K)\mathfrak{p}$. Da $N_{L|K}(\alpha)$ gerade die Determinate der linearen Abbildung $T_\alpha\colon L\to L$ gegeben

durch $x \mapsto \alpha x$ ist und $\alpha_{\mathfrak{p}} w_i = \sum_j \alpha_{\mathfrak{p}_{ij}}$, folgt die lokale Version von (16.1.2):

$$\begin{aligned}
\det((\mathfrak{a}_f)_{\mathfrak{p}}) &= \alpha_{\mathfrak{p}} w_1 \wedge \alpha_{\mathfrak{p}} w_2 \wedge \ldots \wedge \alpha_{\mathfrak{p}} w_n \\
&= \sum_{k_1 \neq \cdots \neq k_n} \alpha_{\mathfrak{p}_{1k_1}} \ldots \alpha_{\mathfrak{p}_{nk_n}} w_{k_1} \wedge \cdots \wedge w_{k_n} \\
&= \left(\sum_{k_1 \neq \cdots \neq k_n} sgn(\sigma) \cdot \alpha_{\mathfrak{p}_{1k_1}} \cdots \alpha_{\mathfrak{p}_{nk_n}} \right) w_1 \wedge \cdots \wedge w_n \\
&= (\det T_{\alpha_{\mathfrak{p}}}) w_1 \wedge \cdots \wedge w_n \\
&= N_{L|K}(\alpha_{\mathfrak{p}})(w_1 \wedge \ldots \wedge w_n) \\
&= N_{L|K}((\mathfrak{a}_f)_{\mathfrak{p}}) \cdot \det((\mathcal{O}_L)_{\mathfrak{p}})
\end{aligned}$$

Wir vergleichen jetzt die Metriken auf der komplexifizierten Version von (16.1.1).

Wir wollen zeigen:

$$\det(i_* L(\overline{\mathfrak{a}})) = L(N_{L|K}(\overline{\mathfrak{a}})) \otimes \det(i_* L(\mathcal{O}_L)).$$

Wir vergleichen nun die Metriken. Wir setzen

$$\overline{M} = L(\overline{\mathfrak{a}}), \quad \overline{N} = L(\overline{\mathcal{O}_L}), \quad P = \mathrm{Nm}_{L|K}(\overline{\mathfrak{a}})$$

und betrachten diese als $\mathcal{O}_K$-Moduln. Es ist $M_{\mathbb{C}} = N_{\mathbb{C}} = L_{\mathbb{C}}$ und $P_{\mathbb{C}} = K_{\mathbb{C}}$ und wie üblich sei

$$M_\sigma = \bigoplus_{\tau|\sigma} \mathbb{C}, \quad N_\sigma \bigoplus_{\tau|\sigma} \mathbb{C}, \quad P_\sigma = \mathbb{C}.$$

Wir müssen zeigen, für $a, b \in P_\sigma$ und $\xi, \eta \in \det M_\sigma$ gilt

$$\langle a\xi, b\eta \rangle_{\det M_\sigma} = \langle a, b \rangle_{P_\sigma} \langle \xi, \eta \rangle_{\det N_\sigma}.$$

Ist $\mathfrak{a}_\infty = (1, (r_\tau)_{\tau \in Y(\mathbb{C})})$, dann ist

$$\begin{aligned}
\langle x, y \rangle_{M_\sigma} &= \sum_{\tau|\sigma} r_\tau^2 x_\tau \overline{y}_\tau \\
\langle x, y \rangle_{N_\sigma} &= \sum_{\tau|\sigma} x_\tau \overline{y}_\tau \\
\langle a, b \rangle_{P_\sigma} &= \left(\prod_{\tau|\sigma} r_\tau^2 \right) \cdot a \cdot \overline{b}.
\end{aligned}$$

Sei nun $\xi = x_1 \wedge \ldots \wedge x_n \in \det M_\sigma$, $\eta = y_1 \wedge \ldots \wedge y_n \in \det N_\sigma$ und $\tau_1, \ldots, \tau_n$ seien die Teiler von σ, d.h. $\tau_i | \sigma \ \forall i$. Wir bilden die Matrizen

$$A = \left((x_i)_{\tau_k} \right), \quad B = \left((y_i)_{\tau_k} \right), \quad D = \begin{pmatrix} r_{\tau_1} & & \\ & \ddots & \\ & & r_{\tau_n} \end{pmatrix}$$

und erhalten damit

$$\begin{aligned}\langle a\xi, b\eta\rangle_{\det M_\sigma} &= a\bar{b}\cdot\langle\xi,\eta\rangle_{\det M_\sigma}\\ &= a\bar{b}\cdot\det((AD)(BD)^t)\\ &= a\bar{b}\cdot\det(D^2)\cdot\det(AB^t)\\ &= \langle a,b\rangle_{P_\sigma}\cdot\langle\xi,\eta\rangle_{\det N_\sigma}.\end{aligned}$$

□

Um das Riemann-Roch Problem lösen zu können, machen wir den Ansatz

$$\begin{aligned}\widehat{\mathrm{ch}}(i_*\xi) &= i_*(\widehat{\mathrm{ch}}(\xi)\cdot(a\oplus\alpha))\\ &= i_*(a\cdot\mathrm{rg}(\xi)\oplus a\widehat{c}_1(\det(\xi))+\mathrm{rg}(\xi)\cdot\alpha)\\ &= [L:K]\cdot a\cdot\mathrm{rg}(\xi)\oplus a\cdot i_*(\widehat{c}_1(\det(\xi)))+\mathrm{rg}(\xi)\cdot i_*\alpha.\end{aligned}$$

Der Vergleich mit Satz 16.1 liefert $a=1$ und $i_*\alpha=\widehat{c}_1(\det(i_*\mathcal{O}_L))$. Wegen der Identität $i_*\circ i^*=[L:K]$ können wir $\alpha=\frac{1}{[L:K]}i^*\widehat{c}_1(\det i_*\mathcal{O}_L)$ setzen. Also gilt $a\oplus\alpha=1\oplus\frac{1}{[L:K]}i^*\widehat{c}_1(\det i_*\mathcal{O}_L)$. Im folgenden werden wir $\det i_*\mathcal{O}_L$ näher studieren.

16.2. Satz. *Es besteht ein kanonischer Isomorphismus metrisierter $\mathcal{O}_K$-Moduln*

$$(\det i_*L(\mathcal{O}_L))^{\otimes^2}=L(\partial_{L|K}),$$

wobei $\partial_{L|K}$ das Diskriminatenideal bezeichnet (vgl. Definition 7.1)

Beweis. Wir betrachten auf $\mathcal{O}_L$ die Spurabbildung $\mathrm{Tr}_{L|K}:\mathcal{O}_L\times\mathcal{O}_L\to\mathcal{O}_K$, $(x,y)\mapsto\mathrm{Tr}_{L|K}(xy)$. Sie induziert vermöge der Abbildung

$$T\colon\det i_*\mathcal{O}_L\otimes_{\mathcal{O}_K}\det i_*\mathcal{O}_L\to\mathcal{O}_K$$

gegeben durch

$$T((\alpha_1\wedge\ldots\wedge\alpha_n)\otimes_{\mathcal{O}_K}(\beta_1\wedge\ldots\wedge\beta_n))=\det(\mathrm{Tr}_{L|K}(\alpha_i\beta_j))$$

einen $\mathcal{O}_K$-Modulhomomorphismus, dessen Bild im Diskriminatenideal $\partial_{L|K}$ liegt. Wir zeigen zuerst, daß T ein Isomorphismus ist. Es genügt dies für alle Lokalisierungen $(\mathcal{O}_K)_{\mathfrak{p}}$ zu zeigen. Dann ist jedoch offensichtlich $\mathrm{Im}(T)=(\partial_{L|K})\mathfrak{p}$ und wegen $\det(\mathrm{Tr}_{L|K}(\alpha_i\beta_j))=\det(\sigma_i\alpha_j)\cdot\det(\sigma_i\beta_i)$ ist $\ker(T)=0$, also ist T auch injektiv. Deshalb ist T ein $\mathcal{O}_K$-Modulisomorphismus. Wir zeigen nun, daß

$$T_{\mathbb{C}}\colon L(\det\mathcal{O}_L)_{\mathbb{C}}^{\otimes^2}\longrightarrow(L(\partial_{L|K}))_{\mathbb{C}}$$

eine Isometrie ist. Es gilt

$$L(\mathcal{O}_L)_{\mathbb{C}}=\bigoplus_{\sigma\in X(\mathbb{C})}\mathcal{O}_{L,\sigma}\ (=\bigoplus_{\sigma\in X(\mathbb{C})}\bigoplus_{\substack{\tau\in Y(\mathbb{C})\\ \tau|\sigma}}\mathbb{C})$$

und $\mathrm{Tr}_{L|K}\colon \mathcal{O}_L \to \mathcal{O}_K$ induziert die Abbildung

$$\mathrm{Tr}_{L|K}(x) = \Sigma_\sigma \,\mathrm{Tr}_\sigma(x_\sigma),$$

wobei $\mathrm{Tr}_\sigma = \sum\limits_{\tau|\sigma} x_{\sigma,\tau}$, wobei $x_{\sigma,\tau}$ die Komponenten von $x_\sigma \in \mathcal{O}_{L,\sigma}$ bezeichnen.
Die Metrik auf $L(\mathcal{O}_L)_{\mathbb{C}}$ ist die orthogonale Summe der Standardmetrik

$$\langle x, y\rangle_\sigma = \sum_{\tau|\sigma} x_\tau \overline{y}_\tau = \mathrm{Tr}_\sigma(x\overline{y})$$

auf den Unterräumen $\mathcal{O}_{L,\sigma}$. Sei nun $x_1, \ldots, x_n, y_1, \ldots, y_n \in \mathcal{O}_{L,\sigma}$ und $x = x_1 \wedge \ldots \wedge x_n, y = y_1 \wedge \ldots \wedge y_n \in \det(\mathcal{O}_{L,\sigma})$ gegeben. Die Abbildung $T_{\mathbb{C}}$ zerfällt in die direkte Summe $T_{\mathbb{C}} = \bigoplus\limits_\sigma T_\sigma$, wobei T_σ die Abbildungen

$$T_\sigma\colon L(\det(\mathcal{O}_{L,\sigma})) \otimes L(\det(\mathcal{O}_{L,\sigma})) \to L(\partial_{L|K})_\sigma$$

mit $T_\sigma(x \otimes y) = \det(\mathrm{Tr}_\sigma(x_i y_j))$ sind. Wir wählen nun weitere n-Tupel $x_i', y_i' \in \mathcal{O}_{L,\sigma}$ und bilden die Matrizen

$$\begin{aligned} A &= (\mathrm{Tr}_\sigma(x_i y_j)), \qquad & A' &= (\mathrm{Tr}_\sigma(\overline{x}_i' \overline{y}_i') \\ B &= (\mathrm{Tr}_\sigma(x_j \overline{x}_j)), \qquad & B' &= (\mathrm{Tr}_\sigma(y_i \overline{y}_j)). \end{aligned}$$

Damit gilt dann $AA' = BB'$ und wir erhalten die gewünschte Isometrie

$$\begin{aligned} \langle T_\sigma(x \otimes y), T_\sigma(x' \otimes y')\rangle_{L(\partial_{L|K})_\sigma} &= T_\sigma(x \otimes y) \cdot \overline{T_\sigma(x' \otimes y')} \\ &= \det(\mathrm{Tr}_\sigma(x_i y_j)) \det(\mathrm{Tr}\,\overline{x}, \overline{y}) \\ &= \det(AA') = \det(BB') \\ &= \det(\mathrm{Tr}_\sigma(x_i \overline{x}_j)) \cdot \det(\mathrm{Tr}_\sigma(y_i \overline{y}_i)) \\ &= \det(\langle x_i, x_j'\rangle_\sigma) \cdot \det(\langle y_i, \overline{y}_j\rangle_\sigma) \\ &= \langle x_i, x_j'\rangle L(\det(\mathcal{O}_{L,\sigma})) \cdot \langle y, y_j'\rangle_{L(\det(\mathcal{O}_{L,\sigma}))} \\ &= \langle x \otimes y, x' \otimes y'\rangle_{L(\det(\mathcal{O}_{L,\sigma}))^{\otimes 2}} \end{aligned}$$

□

Wir fassen das bisher bewiesene zusammen.

16.3. Korollar. *Es gilt in* $\widehat{\mathrm{CH}}(\mathcal{O}_K) \otimes_L \mathbb{Q}$ *für alle* $\xi \in \widehat{K}_0(\mathcal{O}_L)$

$$\widehat{\mathrm{ch}}(i_*\xi) = i_*(\widehat{\mathrm{ch}}(\xi) \cdot (1 \oplus \frac{1}{2}\,\widehat{c}_1(L(\partial_{L|K}))).$$

Beweis: ??? `siehe Notizen`

16.4. Definition.

(i) Die Klasse $[\Omega^1_{\mathcal{O}_L|\mathcal{O}_K}] \in \widehat{K}_0(\mathcal{O}_L)$ des relativen Differentialmoduls $\Omega^1_{\mathcal{O}_L|\mathcal{O}_K}$ (vgl. 13.7) sei

$$[\Omega^1_{\mathcal{O}_L|\mathcal{O}_K}] := [L(\mathcal{D}_{\mathcal{O}_L|\mathcal{O}_K})] - [1].$$

(ii) Das arithmetische Todd Geschlecht

$$\widehat{Td}\colon \widehat{K}_0(\mathcal{O}_L) \longrightarrow \widehat{\mathrm{CH}}(\mathcal{O}_L)_{\mathbb{Q}}$$

sei gegeben durch $\widehat{Td}(\xi) = 1 \oplus 1/2\ \widehat{c}_1(\det(\xi))$.
Wir erhalten somit:

$$\begin{aligned}\widehat{Td}([\Omega^1_{\mathcal{O}_L|\mathcal{O}_K}]) &= 1 \oplus 1/2\left(\widehat{c}_1(L(\mathcal{D}_{\mathcal{O}_L|\mathcal{O}_K})) + \widehat{c}_1(L(\mathcal{O}_L))\right)\\ &= 1 \oplus 1/2\ \widehat{c}_1(L(\mathcal{D}_{\mathcal{O}_L|\mathcal{O}_K})).\end{aligned}$$

Es folgt schließlich

16.5. Satz. (Grothendieck-Riemann-Roch für arithmetische Kurven) *Mit den bisherigen Bezeichnungen ist das folgende Diagramm kommutativ*

$$\begin{array}{ccc}\widehat{K}_0(\mathcal{O}_L) & \xrightarrow{\widehat{Td}(\Omega^1_{\mathcal{O}_L|\mathcal{O}_K})\cdot\widehat{ch}(\cdot)} & \widehat{\mathrm{CH}}(\mathcal{O}_L)_{\mathbb{Q}}\\ {\scriptstyle i_*}\downarrow & & \downarrow{\scriptstyle i_*}\\ \widehat{K}_0(\mathcal{O}_K) & \xrightarrow{\widehat{ch}} & \widehat{\mathrm{CH}}(\mathcal{O}_K)_{\mathbb{Q}}\end{array}$$

In anderen Worten, für alle $\xi \in \widehat{K}_0(\mathcal{O}_L)$ gilt in $\widehat{\mathrm{CH}}(\mathcal{O}_K)_{\mathbb{Q}}$

$$\widehat{\mathrm{ch}}(i_*(\xi)) = i_*(\widehat{\mathrm{ch}}(\xi) \cdot \widehat{Td}(\Omega^1_{\mathcal{O}_L|\mathcal{O}_K})) \tag{16.5.1}$$

16.6. Satz. *Die arithmetische Euler-Minkowski Charakteristik (vgl. Definition 11.5) setzt sich in eindeutiger Weise zu einem Homomorphismus*

$$\widehat{\chi}_K\colon \widehat{K}_0(\mathcal{O}_K) \longrightarrow \mathbb{R}$$

fort. Es gilt dabei $\widehat{\chi}_K = \widehat{\deg}_{\mathcal{O}_K} \cdot \widehat{c}_1 \cdot \det$ *und* $\widehat{\chi}_K$ *heißt die arithmetische Euler-Minkowski-Charakteristik (auf* $\widehat{K}_0(\mathcal{O}_L)$*).*

Beweis. Da $\widehat{K}_0(\mathcal{O}_K)$ als additive Gruppe von invertierbaren metrisierten Moduln der Gestalt $[L(\overline{\mathfrak{a}})]$ erzeugt wird, so ist ein Homomorphismus $\alpha : \widehat{K}_0(\mathcal{O}_K) \to \mathbb{R}$ für dessen Einschränkung auf $\widehat{\mathrm{Pic}}(\mathcal{O}_K)$ sich die Abbildung $\alpha|_{\widehat{\mathrm{Pic}}(\mathcal{O}_K)}\widehat{\deg} \cdot \widehat{c}_1$ ergibt, eindeutig festgelegt. Ein solcher Homomorphismus ist aber durch das Kompositum

$$\widehat{K}_0(\mathcal{O}_K) \xrightarrow{\det} \widehat{\mathrm{Pic}}(\mathcal{O}_K) \xrightarrow{\widehat{c}_1} \widehat{\mathrm{CH}}^1(\mathcal{O}_K) \xrightarrow{\widehat{\deg}_{\mathcal{O}_K}} \mathbb{R}$$

gegeben, weil das Kompositum

$$\widehat{\mathrm{Pic}}(\mathcal{O}_K) \overset{incl}{\hookrightarrow} \widehat{K}_0(\mathcal{O}_K) \xrightarrow{\det} \widehat{\mathrm{Pic}}(\mathcal{O}_K)$$

die Identität ist. □

Anwenden von $\widehat{\deg}$ auf (16.5.1) ergibt wegen $\widehat{\deg}_{\mathcal{O}_K} \circ i_* = \widehat{\deg}_{\mathcal{O}_L}$ das

16.7. Korollar. *Sei $\overline{M}$ ein metrisierter $\mathcal{O}_L$-Modul, dann gilt:*

$$\widehat{\chi}(i_*\overline{M}) = \widehat{\deg}_{\mathcal{O}_L}(\det(\overline{M})) + \widehat{\chi}\,\mathrm{rg}(M) \cdot \widehat{\chi}(i_*\mathcal{O}_L).$$

Wir wollen zum Schluß noch zeigen, daß der bereits bewiesene arithmetische Riemann-Roch Satz (Satz 11.8 ein Spezialfall von (16.5.1) ist. Dies folgt jedoch unmittelbar aus dem folgenden Satz.

16.8. Satz. *Für vollständige Ideale $\overline{\mathfrak{a}} \in \widehat{\mathrm{Pic}}(\mathcal{O}_K)$ gilt $\widehat{\chi}(\overline{\mathfrak{a}}) = \widehat{\chi}_{\mathbb{Q}}(i_*L(\overline{\mathfrak{a}}))$, wobei $i\colon \mathbb{Q} \hookrightarrow K$ die natürliche Inklusion ist.*

Beweis. Es sei $\overline{\mathfrak{a}} = (\mathfrak{a}, (r_\sigma)_{\sigma\in X(\mathbb{C})})$. Dann ist die Metrik auf $i_*L(\overline{\mathfrak{a}})$ gegeben durch

$$\langle x, y\rangle_{i^*L(\mathfrak{a})} = \sum_{\sigma\in X(\mathbb{C})} r_\sigma^2 \overline{x}_\sigma \overline{y}_\sigma,$$

für alle $x, y \in i_*L(\overline{\mathfrak{a}})_{\mathbb{C}} = K_{\mathbb{C}} = \prod_{\sigma\in X(\mathbb{C})} \mathbb{C}$. Wenn wir mit T die F_∞-invariante Transformation $T_\sigma\colon K_{\mathbb{C}} \to K_{\mathbb{C}},\ (x_\sigma)_{\sigma\in X(\mathbb{C})} \mapsto (r_\sigma x_\sigma)_{\sigma\in X(\mathbb{C})}$ bezeichnen, dann folgt

$$\langle x, y\rangle_{i_*L(\overline{\mathfrak{a}})} = \langle Tx, Ty\rangle.$$

Deshalb ist

$$\begin{aligned}\det(i_*L(\overline{\mathfrak{a}})) &= \det i_*\mathfrak{a}, \det T^2 \cdot \langle\ ,\ \rangle \det(i^*\mathcal{O}_L)\\ &= L(\det i_*\mathfrak{a}, \det T).\end{aligned}$$

Wegen $\det i_*\mathfrak{a} = \mathrm{Nm}\,\mathfrak{a} \cdot D_K$ und $\det T = \prod_\sigma r_\sigma$ folgt

$$\begin{aligned}\widehat{\chi}(i_*L(\mathfrak{a})) &= \log \mathrm{Nm}\,\mathfrak{a} + \log D_K \sum \log r_\sigma\\ &= \log \mathrm{vol}(T \cdot \mathfrak{a}).\end{aligned}$$

□

A Grundlagen der Körpertheorie

Beweise von den hier dargestellten Grundlagen der Körpertheorie sollten in jedem guten Buch über Algebra zu finden sein (siehe z.B. [Ku2]).

A.1. Definition. Eine *algebraische Körpererweiterung* $L|K$, ist eine Körpererweiterung, so daß jedes Element $\beta \in L$ algebraisch über K ist (i.a.W. zu jedem $\beta \in L$ existiert ein $f \in K[x]$ mit $f(\beta) = 0$).

A.2. Satz. *Für einen Körper K sind äquivalent:*

(i) *K ist algebraisch abgeschlossen.*

(ii) *Die irreduziblen Polynome aus $K[x]$ sind die Polynome vom Grad 1.*

(iii) *Jedes $f \in K[x] \setminus \{0\}$ besitzt eine eindeutige Darstellung*

$$f = c \cdot (x - \alpha_1)^{\nu_1} \cdots (x - \alpha_r)^{\nu_r}$$

mit $c \in K^*, a_1, \ldots, a_r \in K,\ a_i \neq a_j$ für $i \neq j$ und $\nu_1, \ldots, \nu_r \in \mathbb{N}$.

(iv) *Ist L ein algebraischer Erweiterungskörper von K, so ist $L = K$.* □

A.3. Ein Erweiterungskörper $\overline{K}$ von K heißt *algebraische Abschließung* von K, wenn $\overline{K}|K$ algebraisch und $\overline{K}$ ist algebraisch abgeschlossen ist.
Satz.(Steinitz) *Zu jedem Körper K gibt es eine algebraische Abschließung $\overline{K}$ von K.* □

A.4. Ein nicht konstantes Polynom $f \in K[x]$ hat nur endlich viele Wurzeln in $\overline{K}$, deshalb zerfällt es bereits in einen kleinen Körper, dem *Zerfällungskörper* L von f.
Satz. *Es gilt:*

(i) $f = c \cdot (x - \alpha_1)^{\nu_1} \cdot \ldots \cdot (x - \alpha_r)^{\nu_r} \in L[x]$;

(ii) $L = K(\alpha_1, \ldots, \alpha_n)$.

(iii) Sei $n = \deg f$, dann ist $[L : K] \leq n!$ mit $[L : K]$ = Grad von L über K $= \dim_K L$.

Beweis. (i), (ii) klar.
(iii) Es gilt $[K(\alpha_1) : K] = \dim_K K(\alpha_1) = n$ und es besteht die Zerlegung $f = (x-\alpha_1) \cdot f_1(x)$ mit $f_1(x) \in K(\alpha_1)[x]$ vom Grad $n-1$. Es gilt $[K(\alpha_1, \alpha_2) : K(\alpha_1)] \leq n-1$ und deshalb $[K(\alpha_1, \alpha_2) : K] \leq n \cdot (n-1)$. Weiter ist $f_1 = (x-\alpha_2) \cdot f_2(x)$ mit $f_2 \in K(\alpha_1, \alpha_2)$ und $\deg f_2 \leq n-2$. Die Aussage folgt durch wiederholtes Anwenden des obigen Abspaltungsprinzips.□

A.5. Definition. (i) Ein irreduzibles Polynom $f \in K[x]$ heißt *separabel*, falls f in $\overline{K}$ keine mehrfachen Nullstellen besitzt.
(ii) $\beta \in L|K$ heißt *separabel algebraisch*, falls β algebraisch und sein Minimalpolynom separabel ist.
(iii) $L|K$ heißt *separabel algebraisch*, wenn jedes $\beta \in L$ separabel algebraisch ist.

A.6. Bemerkung. Ein Körper heißt *perfekt* (vollkommen), falls alle $f \in K[x]$ separabel sind. Man zeigt: alle Körper der Charakteristik 0 und alle endlichen Körper sind perfekt.

A.7. Satz. (Satz vom primitiven Element) *Sei $L|K$ eine endliche separable Erweiterung, dann existiert ein $\alpha \in L$, so daß $L = K(\alpha)$.* □

Als Beispiel dazu betrachten wir den Körper $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Es gilt $L = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, denn wegen $\dfrac{1}{\sqrt{2}+\sqrt{3}} = \dfrac{\sqrt{2}-\sqrt{3}}{2-3} = \sqrt{3}-\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$ sind $\sqrt{3}$, $\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

A.8. Satz. *Sei $L|K$ separabel mit $[L : K] = n$. Dann gibt es genau n verschiedene K-Homomorphismen $\sigma : L \hookrightarrow \overline{K}$.*

Beweis. Aufgrund des Satzes vom primitiven Element können wir annehmen $L = K[\beta]$ für ein β mit Minimalpolynom $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in K[x]$ vom Grad n. Wir haben folgende Situation

$$\begin{array}{ccc} L & \xhookrightarrow{\sigma} & \overline{K} \\ \uparrow & & \uparrow \mathrm{id} \\ K & \xhookrightarrow{\overline{\sigma}} & \overline{K} \end{array}$$

mit $\overline{\sigma} \in \mathrm{Hom}(K, \overline{K})$, $\sigma \in \mathrm{Hom}(L, \overline{K})$, $\sigma|K = \overline{\sigma}$ und $K \cong \overline{\sigma}(K)$. Weil $L|K$ separabel ist, besteht für f in $\overline{K}[x]$ die Zerlegung $f^{\overline{\sigma}}(x) = x^n + \overline{\sigma}(a_{n-1})x^{n-1} + \ldots + \overline{\sigma}(a_0) = \prod_{i=1}^{n}(x - \beta_i)$, $\beta_i \in \overline{K}$. Jede Fortsetzung σ von $\overline{\sigma}$ auf $L = K[\beta]$ ist durch die Angabe von $\sigma(\beta)$ eindeutig festgelegt, denn für beliebiges $b = \sum_{i=1}^{n} a_i\beta^i \in L$ mit $a_i \in K$ ist $\sigma(b) = \sum_{i=1}^{n} \overline{\sigma}(a_i)\sigma(\beta)^i$. Aus $f(\beta) = 0$ folgt $f^{\overline{\sigma}}(\sigma(\beta)) = 0$, deshalb muß $\sigma(\beta)$ eine der n Nullstellen von $f^{\overline{\sigma}}$ sein. Es gibt also höchstens n Fortsetzungen von $\overline{\sigma}$ zu einem K-Homomorphismus $\sigma : L \to \overline{K}$.
Sei nun $\beta_i \in \overline{K}$ eine beliebige Nullstelle von $f^{\overline{\sigma}}$. Der Ringhomomorphismus

$$\Phi_i : K[x] \to \overline{K} \quad \text{mit} \quad \Phi_i \mid_K = \overline{\sigma}, \quad \Phi_i(x) = \beta_i$$

bildet f auf 0 ab. Es gibt somit einen Ringhomomorphismus

$$\overline{\Phi}_i : K[x]/(f) \longrightarrow \overline{K}$$

mit $\overline{\Phi}_i \mid_K = \overline{\sigma}$. Da aber aufgrund des Homomorphiesatzes $K[x]/(f)$ isomorph zu $K[\beta]$ ist, bestimmt Φ_i eine Fortsetzung von $\overline{\sigma}$. Da die Nullstellen von f^{σ} verschieden sind, gibt es n verschiedene Fortsetzungen Φ_i von $\overline{\sigma}$. □

A.9. Definition Eine Körpererweiterung $L|K$ heißt *normal*, wenn sie algebraisch ist und wenn gilt: Besitzt ein irreduzibles Polynom $f \in K[x]$ eine Nullstelle in L, so zerfällt f über L in Linearfaktoren.

Man sieht sofort, daß zum Beispiel der algebraische Abschluß $\overline{K}$ von K normal ist.

A.10. Satz. (a) *Eine endliche Körpererweiterung $L|K$ ist genau dann normal, wenn L der Zerfällungskörper eines Polynoms $f \in K[x]$ ist.*

(b) *Zu jeder algebraischen Körpererweiterung $L|K$ gibt es eine Körpererweiterung $N|L$, so daß $N|K$ normal ist.*

Beweis. siehe z.B. Kunz, Algebra. □

A.11. Definition Eine Körpererweiterung $L|K$ heißt *galoissch*, falls sie endlich, separabel und normal ist.

A.12. Satz. *$L|K$ ist galoissch genau dann, wenn L der Zerfällungskörper eines separablen Polynoms aus $K[x]$ ist.* □

Für eine Körpererweiterung $L|K$ bezeichne $G(L|K)$ die Gruppe der K-Automorphismen von L, d.h. die Gruppe aller bijektiven K-Homomorphismen $\sigma : L \to L$ mit $\sigma|_K = id$, mit der Komposition als Verknüpfung.

A.13. Proposition. *Ist $[L : K] = n$, dann ist $|G(L|K)| \leq n$.*

Beweis. Sei $L = K[\alpha] = K[x]/(p_\alpha(x))$, dann ist jeder Automorphismus $\sigma \in G(L|K)$ durch $\sigma(\alpha)$ eindeutig festgelegt. Insbesondere ist $\sigma(\alpha)$ ebenfalls eine Wurzel von p_α. Umgekehrt definiert jede Wurzel ein Element von $G(L|K)$. □

Falls $L|K$ galoissch ist, heißt $G(L|K)$ die *Galoisgruppe* von $L|K$ und wird mit $\mathrm{Gal}(L|K)$ bezeichnet.

A.14. Satz. (Artin) *Sei L ein Körper und G eine endliche Untergruppe der Automorphismengruppe* $\mathrm{Aut}(L)$ *von L und $K := \{x \in L \mid \sigma(x) = x \text{ für alle } \sigma \in G\}$ die Menge der G invarianten Elemente von L. Dann ist K ein Teilkörper von L mit $[L : K] = |G|$. Weiter ist $L|K$ galoissch mit Galoisgruppe* $\mathrm{Gal}(L|K) = G$. □

A.15. Satz. (Hauptsatz der Galoistheorie) *Ist $L|K$ eine Galoiserweiterung, dann entsprechen die Untergruppen der Galoisgruppe den Zwischenkörpern von $L|K$.* □

A.16. Beispiel. Das Polynom $f(x) = x^3 - 3x + 1$ ist ireduzibel und hat die Nullstellen

$$\alpha_1 = e^{\frac{2\pi_i}{9}} + e^{-\frac{2\pi_i}{9}} = 2\cos\left(\frac{2\pi}{9}\right)$$
$$\alpha_2 = -\cos\left(\frac{2\pi}{9}\right) + \cos\left(\frac{8\pi}{9}\right) - \cos\left(\frac{4\pi}{9}\right)$$
$$\alpha_3 = -\cos\left(\frac{2\pi}{9}\right) - \cos\left(\frac{8\pi}{9}\right) + \cos\left(\frac{4\pi}{9}\right)$$

Man rechnet mit zum Beispiel mit Hilfe der Additionstheoreme der cos-Funktion leicht nach:

$$\alpha_2 = -\alpha_1^2 - \alpha_1 + 2 \text{ und } \alpha_2^2 = \alpha_1 + 2,$$
$$\alpha_3 = \alpha_1^2 - 2 \text{ und } \alpha_3^2 = -\alpha_1^2 + \alpha_1 + 4.$$

Es folgt, daß $K = \mathbb{Q}[x]/(f(x))$ galoissch mit Galoisgruppe A_3 ist. In der Tat ist $\mathrm{Gal}(K|\mathbb{Q})$ bezüglich der Basis $\alpha_1, \alpha_2, \alpha_3$ gegeben durch

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 2 \\ 0 & -1 & 1 \\ 0 & -1 & 0 \end{pmatrix} \text{ wobei } \sigma_1(\alpha_1) = \alpha_2$$
$$\sigma_2 = \begin{pmatrix} 1 & -2 & 4 \\ 0 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix} = \sigma_1^2.$$

B Kategorien und Funktoren

Wir wiederholen hier nur die Defintionen der in der Vorlesung benötigten Begriffe.

B.1. Definition. Eine *Kategorie* A wird gegeben durch

(a) eine mit $\mathrm{Ob}(A)$ bezeichnete Klasse von sogenannten Objekten,

(b) für je zwei Objekte A, B eine Menge (A, B), deren Elemente Morphismen heißen. Die Mengen $\mathrm{Mor}_A(A, B)$ und $\mathrm{Mor}_A(A', B')$ sind disjunkt, außer falls $A = A'$ und $B = B'$ und dann sind sie gleich .

(c) Für 3 Objekte A, B, C besteht eine Verküpfung

$$\mathrm{Mor}_A(B, C) \times \mathrm{Mor}_A(A, B) \longrightarrow \mathrm{Mor}_A(A, C),$$

die assoziativ ist. D.h. für die Objekte A, B, C, D und $f \in \mathrm{Mor}(A, B), g \in \mathrm{Mor}(B, C), h \in \mathrm{Mor}(C, D)$ gilt $(h \circ g) \circ f = h \circ (g \circ f)$.

(d) Zu jedem Objekt A aus A existiert ein Morphismus $\mathrm{Id}_A \in \mathrm{Mor}_A(A, A')$, welcher für alle $D \in A$ auf $\mathrm{Mor}_A(A, B)$ bzw. $\mathrm{Mor}_A(B, A)$ eine als links-responde Rechtsidentität wirkt.

B.2. Beispiele. Die Kategorie der abelschen Gruppe Ab. Die Objekte von Ab sind abelsche Gruppe und die Morphismen sind Gruppenhomomorphismen.

Die Kategorie der Zahlkörper ZK, die Objekte von ZK sind Zahlkörper und die Morphismen sind

$$\mathrm{Mor}_{ZK}(K, L) = \begin{cases} i, \text{ falls } K \subseteq L, \\ \emptyset, \text{ falls } K. \not\subseteq L \end{cases}$$

hierbei ist $i : K \to L$ die Inklusionsabbildung.

B.3. Definition. Seien A und D Kategorien. Ein *kovarianter Funktor* F ordnet jedem Objekt A von A ein Objekt $F(A)$ von B und jedem Morphismus $f \colon A \to A'$ von A einen Morphismus

$$F(f) : F(A) \to F(A') \tag{B.3.1}$$

zu, so daß die folgenden Bedingungen erfüllt sind:

$$\begin{aligned} F(\mathrm{id}_A) &= \mathrm{id}_{F(A)} \text{ für alle } A \in Ob(A), \\ F(g \circ f) &= F(g) \circ F(f) \text{ für alle } f \in \mathrm{Mor}_A(A, A') \text{ und } g \in \mathrm{Mor}_A(A', A''). \end{aligned} \tag{B.3.2}$$

Ein *kontravarianter Funktor* F ist dadurch gegeben, daß alle "Pfeile umgedreht" sind, d.h. anstelle von (B.3.1) und (B.3.2) gilt:

$$\begin{aligned} F(f) &: F(A') \to F(A) \\ F(g \circ f) &= F(f) \circ F(g). \end{aligned}$$

C Grundlagen aus der multilinearen Algebra

Wir stellen hier die von uns benutzten Eigenschaften von Tensorprodukt und alternierendes Produkt bereit (siehe z.B. Lang: Algebra).

Sei R ein kommutativer Ring und M, N, P seien R-Moduln.

C.1. Definition. Ein Paar (Q, f) bestehend aus einem R-Modul Q und einer bilinearen Abbildung $f : M \times N \to Q$ heißt Tensorprodukt von M und N, falls jede R-bilineare Abbildung $f' : M \times N \to P$ eindeutig R-linear über f faktorisiert, d.h. $f' = \alpha \circ f$ mit $\alpha : Q \to P$ R-linear. Das Tensorprodukt existiert und ist bis auf eindeutige Isomorphie eindeutig bestimmt. Es wird mit $M \otimes_R N$ bezeichnet und man setzt $f(m, n) = m \otimes n$. Das Paar $(M \otimes_R N,\ (m, n) \mapsto m \otimes n)$ ist durch folgende Eigenschaften charakterisiert:

1) Die Abbildung $M \times N \to M \otimes_R N$ ist R-bilinear und jede R-bilineare Abbildung $M \times N \to P$ ist von der Form $(m, n) \mapsto \alpha(m \otimes n)$ für eine eindeutige bestimmte R-lineare Abbildung $\alpha : M \otimes N \to P$, i.a.W.

$$\mathrm{Bilin}_R(M \times N, P) \cong \mathrm{Hom}_R(M \otimes N, P).$$

2) Als R-Modul ist $M \otimes N$ von den Symbolen $m \otimes n, m \in M$ und $n \in N$, erzeugt die den Bedingungen

$$\begin{aligned}(m + m') \otimes n &= m \otimes n + m' \otimes n,\\ m \otimes (n + n') &= m \otimes n + m \otimes n',\\ am \otimes n = a(m \otimes n) &= m \otimes an,\end{aligned}$$

genügen.

C.2. Eigenschaften. Das Tensorprodukt ist vertauschbar mit der direkten Summe, i.e. es gibt kanonische Isomorphismen

$$\begin{aligned}(\bigoplus_i M_i) \otimes_R (\bigoplus_j N_j) &\simeq \bigoplus_{i,j} M_i \otimes N_j\\ (\Sigma_i m_i) \otimes (\Sigma_j n_j) &\mapsto \Sigma_{i,j} m_i \otimes n_j\end{aligned}$$

Das Tensorprodukt ist (bis auf Isomorphie!) assoziativ und kommutativ. Gegeben sei die kurze exakte Sequenz $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$, dann ist für jeden Modul N die Sequenz

$$N \otimes M' \to N \otimes M \to N \otimes M' \to 0 \tag{C.2.1}$$

exakt.

C.3. Bemerkung. (i) Die Sequenz (C.2.1) setzt sich nur in Ausnahmefällen zu einer kurzen exakten Sequenz

$$0 \to N \otimes M' \to N \otimes M \to N \otimes M' \to 0 \tag{C.3.1}$$

fort. Wichtige Beispiele sind wie folgt: Falls $M = M' \oplus M''$ ist, dann gilt (C.3.1). Wenn N projektiver Modul ist, dann gilt ebenfalls (C.3.1).

(ii) Ist $\mathfrak{a} \subseteq R$ ein Ideal, dann ist

$$0 \to \mathfrak{a} \to R \to R/\mathfrak{a} \to 0$$

ein kurze exakte Sequenz, und für beliebige R-Modul M folgt

$$\mathfrak{a} \otimes M \xrightarrow{\alpha} M \to (R/\mathfrak{a}) \otimes M \to 0$$

und falls wir $\mathfrak{a}M = \{\Sigma a_i m_i \mid a_i \in \mathfrak{a},\ m_i \in M\}$ setzen, dann besteht der Isomorphismus

$$M/\mathfrak{a}M \cong (R/\mathfrak{a}) \otimes M.$$

C.4. Definition. Es bezeichne $\{M\}$ die Isomorphieklasse eines projektiven R-Moduls M. Die freie abelsche Gruppe solcher Isomorphieklassen sei $F_0(R) = \bigoplus_{\{M\}} \mathbb{Z}\{M\}$. Es bezeichne $R_0(R) \subseteq F_0(R)$ die Untergruppe, die durch eine Linearkombination der Form $\{M'\} - \{M\} + \{M''\}$, für die es eine kurze exakte Sequenz

$$0 \to M' \to M \to M'' \to 0$$

gibt, darstellbar ist. Die *Grothendieckgruppe von R* ist definiert als der Quotient

$$K_0(R) = F_0(R)/R_0(R).$$

Für einen projektiven Modul M bezeichne $[M]$ seine Klasse in $K_0(R)$. Aus $0 \to M' \to M \to M'' \to 0$ folgt $[M] = [M'] + [M'']$. Insbesondere ist $[M' \oplus M''] = [M'] + [M'']$.

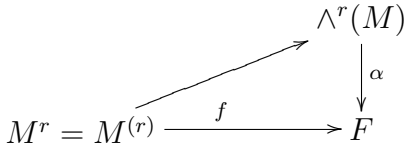
Durch die lineare Fortsetzung des Produkts $\{M\}\{N\} := \{M \otimes_R N\}$ erhalten wir ein Produkt auf $K_0(R)$. Mit obigen Eigenschaften des Tensorproduktes zeigt man leicht:

C.5. Proposition. *Die Grothendieckgruppe $K_0(R)$ von R ist ein kommutativer Ring.* □

C.6. Definition. Sei M ein R-Modul. Sei $\mathfrak{a}_r$ der Untermodul von $M^{\otimes r} = M \otimes \ldots \otimes M$, der erzeugt wird von den Elementen der Form $x_1 \otimes \ldots \otimes x_r$, wobei für ein $i \neq j$ gilt $x_i = x_j$. Dann definieren wir

$$\wedge^r(M) = M^{\otimes r}/\mathfrak{a}_r.$$

Ist $f : M \to F$ eine alternierende r-multilineare Abbildung, (d.h. $f(x_1, \ldots, x_r) = 0$, falls für ein $i \neq j,\ x_i = x_j$ gilt), dann existiert eine eindeutige R-lineare Abbildung α, so daß das Diagramm



kommutiert. Das Bild eines Tupels $(x_1, \ldots x_r)$ in $\wedge^r(M)$ wird mit $x_1 \wedge \ldots \wedge x_r$ bezeichnet. Beachte: Es gilt die Identität $x_1 \wedge \ldots \wedge x_r = \varepsilon(\sigma) x_{\sigma(1)} \wedge \ldots \wedge x_{\sigma(r)}$, hierbei bezeichnet $\varepsilon(\sigma)$ das

Vorzeichen der Permutation σ. Diese folgt aus der Formel $0 = (x+y)\wedge(x+y) = x\wedge y + y\wedge x$ mittels vollständiger Induktion. Es bezeichne

$$\wedge(M) = \bigoplus_{r=0}^{\infty} \wedge^r(M)$$

die *alternierende Algebra* (oder äußere Algebra, oder Grassmannsche Algebra), wobei das *alternierende Produkt* gegeben ist durch

$$\wedge^r(M) \times \wedge^s(M) \to \wedge^{r+s}(M)$$
$$(x_1 \wedge \ldots \wedge x_r, y_1 \wedge \ldots \wedge y_s) \mapsto x_1 \wedge \ldots \wedge x_r \wedge y_1 \wedge \ldots \wedge y_s.$$

C.7. Proposition. *Sei M ein freier R-Modul vom Rang n (d.h. $M \simeq R^n$). Sei $\{\nu_1, \ldots, \nu_n\}$ eine Basis von M über R. Ist $1 \leq r \leq n$, dann ist $\wedge^r(M)$ ein freier R-Modul und die Elemente*

$$\nu_{i_1} \wedge \ldots \wedge \nu_{i_r} \qquad \textit{mit} \quad 1 \leq i_1 < \ldots < i_r \leq n$$

bilden eine Basis von $\wedge^r(M)$. Insbesondere gilt $rg(\wedge^r(M)) = \binom{n}{r}$ und $\wedge^r = 0$, falls $r > n$.

C.8. Definition. Ist M ein freier R-Modul vom Rang n, dann ist seine Determinante der freie Rang 1 Modul

$$\det(M) = \wedge^{\max}(M) = \wedge^n(M).$$

C.9. Proposition. *Sei $0 \to M' \to M \to M'' \to 0$ eine kurze exakte Sequenz von freien R-Moduln vom jeweiligen Rang r, n und s. Dann besteht ein natürlicher Isomorphismus*

$$\varphi : \wedge^r(M') \otimes \wedge^s(M'') \to \wedge^n(M),$$

der durch folgende Eigenschaft eindeutig bestimmt ist: Sind $v_1, \ldots, v_r \in M'$, $w_1, \ldots, w_s \in M''$ Urbilder von $u_1, \ldots, u_n$, dann gilt

$$\varphi((v_1 \wedge \ldots \wedge v_r) \otimes (w_1 \wedge \ldots \wedge w_s)) = \nu_1 \wedge \ldots \wedge \nu_r \wedge u_1 \wedge \ldots \wedge u_s.$$

□

C.10. Bemerkung. Ist $M = M' \oplus M''$, dann gilt sogar

$$\wedge^n(M) \simeq \oplus_{p+q=n} \wedge^p (M') \otimes \wedge^q(M''). \tag{C.10.1}$$

Literatur

[BKK] J. Burgos, J. Kramer, and U. Kühn: Cohomological Arithmetic Chow rings. Preprint, arXiv.org/math.AG/0404122 (2003).

[FT] A. Fröhlich, M.J. Taylor: Algebraic Number Theory, Cambridge University Press (1991).

[Hü] E. Hübschke: Arakelov-Theorie für Zahlkörper. Regensburger Trichter 20 (1987).

[Ei] M. Eichler: Einführung in die Theorie der algebraischen Zahlen und Funktionen. Birkhäuser Verlag (1963).

[Ko] H. Koch: Number Theory, AMS (2000).

[Ku1] E. Kunz: Algebraische Geometrie, Vieweg-Verlag (1980).

[Ku2] E. Kunz: Algebra. Vieweg-Verlag (1990).

[La1] S. Lang: Algebra. Springer-Verlag (2002).

[La2] S. Lang: Arakelov Theory (1988). Springer Verlag.

[Mi] J.S. Milne: Algebraic number theory. www.jmilne.org

[Ne] J. Neukirch: Algebraische Zahlentheorie. Springer-Verlag (1992).

[Ri] P. Ribenboim: Classical theory of algebraic numbers. Springer-Verlag (2001).

[Ro] D. Roessler: The Riemann-Roch theorem for arithmetic curves. Diplomarbeit ETH Zürich (1993)

[SABK] C. Soulé, D. Abramovich, J.-F. Burnol, and J. Kramer: Lectures on Arakelov Geometry. Cambrigde University Press (1992).

[St] P. Stevenhagen: Number rings, lecture notes 2002. (Kopie bei mir erhältlich)

[Sw] H.P.F. Swinnerton-Dyer: A brief guide to algebraic number theory. London Mathematical Society Student Texts 50. Cambridge University Press (2001).

[Sz] L. Szpiro: Degrés, intersections, hauteurs. In: Astérisque No. 127 (1985).

Index