# Algebraische Zahlentheorie
# Wintersemester 2009/10

Prof. Dr. Annette Huber-Klawitter

Fassung vom 3. Februar 2010

**Dies ist ein Vorlesungsskript und kein Lehrbuch.**
**Mit Fehlern muss gerechnet werden!**

Math. Institut
Eckerstr.1
79104 Freiburg

0761-203-5560
annette.huber@math.uni-freiburg.de

# Kapitel 0

# Einleitung

Zahlentheorie beschäftigt sich mit Eigenschaften von Zahlen, d.h. Elementen von $\mathbb{Z}$. Damit ist sie eine der ältesten Wissenschaften überhaupt - die Königin der Mathematik. Wir wissen sehr viel, sehr vieles aber auch nicht.
In dieser Vorlesung werden Sie ein Teilgebiet kennenlernen, die algebraische Zahlentheorie.

## Gegenstand

(Polynomiale) Gleichungen oder Gleichungssysteme über den rationalen oder ganzen Zahlen.
Wir fragen nach der Existenz von Lösungen, ihrere Anzahl und vor allem nach der Struktur der Lösungsmenge. Dabei geht es eher nicht um Einzelbeispiele, sondern um allgemeine Aussagen.

**Definition 0.1.** *Sei $k$ ein Körper (z.B $\mathbb{Q}$), $F \in k[X_1, \ldots, X_n]$ ein Polynom ungleich 0. Für jede Körpererweiterung $K/k$ setzen wir*

$$V(F)(K) = \{(x_1, \ldots, x_n) \in K^n | F(x_1, \ldots, x_n) = 0\}$$

*die $K$-wertigen Punkte der Hyperfläche $V(F)$.*
*Ist $n = 2$, so heißt $V(F)$* ebene algebraische Kurve.

**Beispiel.** Sei $n \in \mathbb{N}$, $(a_{ij}) \in M_n(\mathbb{Q})$ eine symmetrische Matrix, $b_1, \ldots, b_n$ ein Vektor in $\mathbb{Q}^n$, $c \in \mathbb{Q}$. Betrachte

$$F = \sum_{i,j} a_{ij} X_i X_j + \sum_i b_i X_i + c$$

$Q = V(F)$ heißt dann *affine Quadrik*. Für $n \geq 2$ ist $Q(K)$ nicht leer genau dann, falls $V(F)(K)$ unendliche viele Elemente hat.

*Proof.* Theorie der quadratischen Formen, siehe mein Vortrag im didaktischen Seminar. □

Dieser Satz hat noch nicht viel mit Zahlentheorie zu tun, wohl aber der folgende:

**Satz 0.2.** *Für $n \geq 5$ ist $V(F)(\mathbb{Q}) \neq \emptyset$ (d.h. $F = 0$ lösbar über $\mathbb{Q}$), falls $V(F)(\mathbb{R}) \neq 0$ (d.h. über $\mathbb{R}$ lösbar).*

*Proof.* Serre: A course in arithmetic, Ch. IV, §3.2, Cor. 2. □

Der Beweis beruht auf einem *Lokal-Global-Prinzip*: Um Gleichungen über $\mathbb{Z}$ zu behandlen, muss man diese erst $\mod p$, $\mod p^2$, ... für alle Primzahlen behandeln, sowie über den reellen Zahlen. Die quadratische Gleichung im Satz 0.2 ist lösbar $\mod p^m$ für alle $m \in \mathbb{N}$ und alle Primzahlen $p$, sowie nach Voraussetzung über $\mathbb{R}$. In diesem Spezialfall folgt daraus bereits die Aussage über $\mathbb{Q}$ (Hasse-Prinzip). Die Terminologie kommt von einer ganz starken Analogie zwischen $\mathbb{Q}$ und $\mathbb{F}_p(X)$ bzw. $\mathbb{Z}$ und $\mathbb{F}_p[X]$. Hierbei entsprechen die Primzahlen den Primidealen und diese den Punkte der affinen Gerade. $\mathbb{R}$ entspricht dem unendlich fernen Punkt. Wir kommen darauf zurück.

## Grundprinzip der algebraischen Zahlentheorie:

Viele Fragen können leichter behandelt werden, wenn man nicht nur mit $\mathbb{Q}$, sondern mit endlichen Erweiterungen von $\mathbb{Q}$ arbeitet. Solche Körper heißen *Zahlkörper*.

**Satz 0.3** (Euler)**.** *Die Gleichung $x^3 + y^3 = z^3$ hat keine Lösung in natürlichen Zahlen.*

Ansatz:

$$x^3 = z^3 - y^3 = (z - y)(z - \varrho y)(z - \varrho^2 y)$$

wobei $\varrho = \mathrm{e}^{2\pi i/3}$ eine dritte Einheitswurzel ist. Allgemeiner:

$$Z^3 - y^3 = (Z - y)(Z - \varrho y)(Z - \varrho^2 y) \in \mathbb{C}[Z]$$

da die Nullstellen übereinstimmen. Sei nun $K = \mathbb{Q}(\varrho)$, $R = \mathbb{Z}[\varrho]$. Die Körpererweiterung $K/\mathbb{Q}$ ist quadratisch, denn das Minimalpolynom von $\varrho$ ist $Z^2 + Z + 1$. Es gilt

$$R = \{a + b\varrho \mid a, b \in \mathbb{Z}\} \ .$$

$R$ ist ein Hauptidealring, darin ist $\lambda = 1 - \varrho$ eine Primzahl.
Man beweist allgemeiner:

**Satz 0.4.** *Die Gleichung $x^3 + y^3 + \lambda^{3n} z^3 = 0$ hat in $R$ keine Lösungen mit $xyz \neq 0$.*

*Beweis:* Geschickte Teilbarkeitsargumente in $R$ modulo $\lambda$, vergl. Hardy-Wright, Kapitel 13.4. □

Leider funktioniert dieselbe Idee nicht für

$$x^p + y^p = z^p$$

($p$ Primzahl), da $\mathbb{Z}[\zeta_p]$ mit $\zeta_p = \mathrm{e}^{2\pi i/p}$ im Allgemeinen kein Hauptidealring ist. Dennoch: Um Eigenschaften von $\mathbb{Z}$ zu studieren, lohnt es sich, endliche Erweiterungen von $\mathbb{Q}$ zu studieren. Diese *Zahlkörper* und die darin enthaltenen Zahlringe wie $\mathbb{Z}[\zeta_p]$ sind der Hauptgegenstand dieser Vorlesung. Insbesondere müssen wir genau verstehen, wie sich die Eindeutigkeit der Primfaktorzerlegung verallgemeinern lässt. Dies führt auf den Begriff der Klassengruppe.

## Die Analogie zu algebraischen Kurven

Die Terminologie kommt aus einer sehr starken Analogie zwischen den den endlichen Erweiterungen von $\mathbb{Q}$ und den endlichen Erweiterungen von $\mathbb{F}_p(t)$. Wir kehren zurück zu unseren Hyperflächen und machen einen Crashkurs algebraische Geometrie (ohne Beweise).

**Definition 0.5.** *Sei $F \in k[X_1, \ldots, X_n]$ ein Polynom ungleich null, $V = V(F)$. Jedes Polynom $G \in k[X_1, \ldots, X_n]$ definiert eine* algebraische Funktion

$$g : V(K) \to K \qquad (x_1, \ldots, x_n) \mapsto G(x_1, \ldots, x_n)$$

*Sei $k[V]$ der Ring der algebraischen Funktionen auf $V$.*

**Beispiel.** Ist $F$ irreduzibel, so ist $k[V] = k[X_1, \ldots, X_n]/(F)$ und dieser Ring ist nullteilerfrei (d.h. $ab = 0 \Rightarrow a = 0 \vee b = 0$). (ohne Beweis/Übungsaufgabe)

**Definition 0.6.** *Sei $F$ irreduzibles Polynom, $V = V(F)$. Dann heißt der Quotientenkörper*

$$k(V) = Q(k[V]) = \left\{ \frac{a}{b} \mid a, b \in k[V], b \neq 0 \right\} / \sim$$

*(Äquivalenz von Brüchen)* Funktionenkörer *von $V$. Elemente des Funktionenkörpers heißen* rationale Funktionen *auf $V$.*

Die Funktion $\frac{a}{b}$ ist nur außerhalb der Nullstellenmenge von $b$ definiert. Dieses Verhalten kennt man von meromorphen Funktionen aus der Funktionentheorie.

**Beispiel.** Sei $F \in k[X, Y]$ ein irreduzibles Polynom. Dann ist

$$k[V] = k[X, Y]/(F)$$

und

$$k(V) = k(X)[Y]/(F)$$

Dies ist eine endliche Erweiterung von $k(X)$ (Übungsaufgabe).

Wie erwähnt ist der Fall $k = \mathbb{F}_p$ besonders interessant. Fast alle Sätze, die für endliche Erweiterungen von $\mathbb{Q}$ gelten, gelten auch für endliche Erweiterungen von $\mathbb{F}_p(t)$ – mit demselben Beweis.
Wir werden diesen Fall daher mitbetrachten. Der geometrische Fall soll Ihnen etwas mehr Intuition geben. Wenn Sie das nur verwirrt – ignorieren Sie diesen Fall einfach.

## Literatur

(i) P. Samuel, Algebraic Theory of Numbers

(ii) S. Lang, Algebraic Number Theory

(iii) J. Neukirch, Algebraic Number Theory

(iv) A. Leutbecher, Zahlentheorie - eine Einführung in die Algebra

(v) Atiyah, MacDonald, Introduction to Commutative Algebra

### Stichworte kommutative Algebra

Ringe, Ideale, Nullteiler, Primideale, Quotientenkörper rationaler Funktionenkörper $k(t)$ für Körper $k$

# Kapitel 1

# Ganze Ringerweiterungen

## Globale Körper und Ganzheitsringe

**Definition 1.1.** *Endliche Körpererrweiterungen von $\mathbb{Q}$ heißen* Zahlkörper*. Sei $p$ Primzahl. Endliche Körpererweiterung von $\mathbb{F}_p(t)$ heißen* Funktionenkörper*. Ein* globaler Körper *ist ein Zahlkörper oder ein Funktionenkörper.*

**Bemerkung.** Zahlkörper haben also Charakteristik Null, Funktionenkörper Charakteristik $p$. Die Einbettung $\mathbb{F}_p(t) \to K$ gehört zur Struktur.

**Definition 1.2.** *Sei $K$ Zahlkörper. Der* Ganzheitsring *von $K$ ist*

$$\mathcal{O}_K = \{\alpha \in K \mid \textit{es gibt } n \in \mathbb{N}, a_1, \ldots, a_n \in \mathbb{Z}, \alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0\}$$

*Ringe von dieser Form heißen* Zahlringe*.*
*Sei $K$ Funktionenkörper. Dann ersetzen wir in der Definition des Ganzheitsrings $\mathbb{Z}$ durch $\mathbb{F}_p[t]$.*

Entscheidend ist hierbei der Koeffizient 1 vor $\alpha^n$!

**Bemerkung.** $\mathbb{Z}$ und $\mathbb{F}_p[t]$ sind beides Hauptidealringe. Sind $a \in \mathbb{Z}$ oder $a' \in \mathbb{F}_p[t]$ nicht invertierbar (d.h. $a \neq \pm 1$, $a' \notin \mathbb{F}_p^*$), so sind $\mathbb{Z}/(a)$ und $\mathbb{F}_p[t]/(a')$ endliche Ringe.

**Beispiel.** Der Ganzheitsring von $\mathbb{Q}$ ist $\mathbb{Z}$, der von $\mathbb{F}_p(t)$ ist $\mathbb{F}_p[t]$.

*Proof.* Sei $x$ im Ganzheitsring. Nach Voraussetzung ist er Nullstelle eines ganzahligen Polynoms

$$X^n + a_1X^{n-1} + \cdots + a_n$$

Nach de Gauß-Lemma (z.B. Bosch, 2.7 Kor.6) ist $x$ ganzahlig. □

**Beispiel.** Sei $K/\mathbb{Q}$ quadratisch, d.h. $[K : \mathbb{Q}] = 2 \Rightarrow K = \mathbb{Q}(\sqrt{d})$ mit $d \in \mathbb{Z}$ keine Quadratzahl.

**Satz 1.3.** *Sei $K = \mathbb{Q}(\sqrt{d})$, $d$ quadratfrei (d.h. kein doppelter Faktor in der Primfaktorzerlegung). Dann gilt:*

*(i) Für* $d \equiv 2, 3 \mod 4$ *ist* $\mathcal{O}_K = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$,

*(ii) Für* $d \equiv 1 \mod 4$ *ist* $\mathcal{O}_K = \{1/2(u + v\sqrt{d}) \mid u, v \in \mathbb{Z}, u \equiv v \mod 2\}$.

*Beweis:* Es ist $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \{\mathrm{id}, \sigma\}$ mit $\sigma(\sqrt{d}) = -\sqrt{d}$. Sei $\alpha = a + b\sqrt{d} \in \mathcal{O}_K$, d.h. Nullstelle von

$$P(X) = X^n + a_1 X^{n-1} + \cdots + a_n = 0,\ a_i \in \mathbb{Z}\ .$$

Dann ist auch $\sigma(\alpha)$ eine Nullstelle von $P(X)$. Das Polynom

$$\begin{aligned} Q(\alpha) = (X - \alpha)(X - \sigma(\alpha)) &= X^2 - (\alpha + \sigma\alpha)X + \alpha\sigma\alpha \\ &= X^2 - (a + b\sqrt{d} + a - b\sqrt{d})X + (a + b\sqrt{d})(a - b\sqrt{d}) \\ &= X^2 - 2aX + (a^2 - b^2 d) \in \mathbb{Q}[X] \end{aligned}$$

muss also $P(X)$ teilen. Nach dem Gauß-Lemma hat $Q$ also ganze Koeffizienten (z.B. Bosch, 2.7 Kor.6). Es gilt also

$$2a, a^2 - b^2 d \in \mathbb{Z} \Rightarrow (2a)^2 - (2b)^2 d \in \mathbb{Z} \Rightarrow (2b^2)d \in \mathbb{Z}\ .$$

Wäre $2b \notin \mathbb{Z}$, so müssten sich die Primfaktoren des Nenners gegen Faktoren von $d$ wegheben. Wegen $(2b)^2$ müsste der Faktor sogar doppelt in $d$ vorkommen. Dies ist ein Widerspruch zur Wahl von $d$. Also:

$$\begin{gathered} a = \frac{u}{2}, b = \frac{v}{2} \text{ mit } u, v \in \mathbb{Z} \\ \Rightarrow \left(\frac{u}{2}\right)^2 - \left(\frac{v}{2}\right)^2 d = \frac{u^2 - v^2 d}{4} \in \mathbb{Z} \\ \Leftrightarrow 4 \mid u^2 - v^2 d \end{gathered}$$

Die Quadrate $u^2$ und $v^2$ können nur 0 oder 1 modulo 4 sein. Für $u^2 - v^2 d$ ergeben sich daher unterschiedliche Möglichkeiten je nach Restklasse von $d$. Man überprüft tabellarisch, dass für $d \equiv 2, 3$ nur $u^2 \equiv v^2 \equiv 0 \mod 4$ in Frage kommt, also beide gerade. Für $d \equiv 1$ ist $u^2 \equiv v^2 = 1 \mod 4$ ebenfalls möglich, also beide ungerade. □

**Beispiel.** Sei $\zeta_N$ eine primitive $N$-te Einheitswurzel. Der Ganzheitsring von $\mathbb{Q}(\zeta_N)$ ist $\mathbb{Z}[\zeta_N]$.

Der Beweis ist aufwändiger. Wir werden ihn später führen, wenn wir schon mehr über Zahlringe wissen.
In diesen Beispielen sieht man, dass $\mathcal{O}_K$ ein Ring ist. Für den allgemeinen Fall holen wir weiter aus.

**Konvention:** Alle Ringe sind kommutativ mit Eins. Alle Ringhomomorphismen bilden Eins auf Eins ab.

**Definition 1.4.** *Sei $A \subset B$ eine Ringerweiterung. Ein Element $b \in B$ heißt* ganz über $A$*, wenn es $n \in \mathbb{N}$ und $a_1, \ldots, a_n \in A$ gibt mit $x^n + a_1 x^{n-1} + \cdots + a_n = 0$. Der* ganze Abschluss *von $A$ in $B$ ist die Menge der Elemente von $B$, die ganz über $A$ sind. Die Ringerweiterung heißt* ganz*, wenn alle Elemente von $b$ ganz über $A$ sind.*

**Beispiel.** (i) $A = \mathbb{Z}$, $B = K$ endliche Körpererweiterung von $\mathbb{Q}$. Dann ist $\mathcal{O}_K$ nach Definition der ganze Abschluss von $\mathbb{Z}$ in $K$.

(ii) $K/\mathbb{F}_p(t)$ endlich. Dann ist $\mathcal{O}_K$ der ganze Abschluss von $\mathbb{F}_p[t]$ in $K$.

(iii) $A = K \subset L$ eine Körpererweiterung. Ein Element von $L$ ist genau dann ganz über $K$, wenn es algebraisch über $K$ ist. (Das Minimalpolynom kann normiert gewählt werden!).

**Satz 1.5.** *Sei $A \subset B$ eine Ringerweiterung. Dann ist der ganze Abschluss von $A$ in $B$ ein Ring.*

Insbesondere sind Ganzheitsringe Ringe!

**Bemerkung.** Zum Beweis erinnern wir uns an den Fall von Körpererweiterungen. Warum ist der algebraische Abschluss ein Körper? Warum sind Summen/Produkte von algebraischen Elementen algebraisch? In der Algebra wurde dies auf die Theorie der *endlichen* Erweiterungen zurückgeführt - endliche Erweiterungen von endlichen Erweiterungen sind endlich, endliche Erweiterungen sind endlich. Endlich bedeutet hierbei *endlichdimensional* als Vektorraum.
Dieses Argument wollen wir mit Ringen wiederholen. Dabei müssen wir Vektorräume durch Moduln ersetzen.

**Definition 1.6.** *Sei $A$ ein Ring. Ein* $A$-Modul *$M$ ist eine abelsche Gruppe $(M, +)$ zusammen mit einer Skalarmultiplikation*

$$A \times M \to M$$

*so dass für alle $a, b \in A$, $x, y \in M$ gilt:*

*(i)* $a(x + y) = ax + ay$,

*(ii)* $(a + b)x = ax + bx$,

*(iii)* $a(bx) = (ab)x$,

*(iv)* $1x = x$.

*Seien $M, N$ Moduln. Eine Abbildung $f : M \to N$ ist ein Modulhomomorphism, falls sie ein Homomorphismus abelscher Gruppen ist und zusätzlich für alle $a \in A$, $x \in M$ gilt: $f(ax) = af(x)$.*

**Beispiel.** (i) $A = k$ ein Körper. Dann ist ein $A$-Modul das Gleiche wie ein $k$-Vektorraum. Modulhomomorphismen von $k$-Vektorräumen sind genau die linearen Abbildungen.

(ii) Ein $\mathbb{Z}$-Modul ist das Gleiche wie eine abelsche Gruppe. Modulhomomorphismen von $\mathbb{Z}$-Moduln sind genau die Gruppenhomomorphismen.

Die Grundlagen der Theorie funktionieren wie für Körper. Begriffe wie linear unabhängig, Erzeugendensystem, direkte Summe, Untermodul, Quotientenmodul etc. werden genau wie in der lineare Algebra definiert. Ein Modul heißt *endlich erzeugt*, wenn er ein endliches Erzeugendensystem hat.
Beim Begriff der Basis muss man aufpassen:

**Definition 1.7.** *Sei $M$ ein $A$-Modul. Ein linear unabhängiges Erzeugendensystem von $M$ heißt* Basis*. $M$ heißt* frei*, falls es eine Basis gibt. Die Mächtigkeit einer Basis heißt* Rang *von $M$.*

Der Rang eines Moduls ist wohldefiniert, d.h. unabhängig von der Wahl der Basis (Reduktion auf den Fall eines Körpers, Übungsaufgabe).

**Beispiel.** (i) Wenn $A$ ein Körper ist, so sind alle Moduln frei. (Basisexistenzsatz, Lineare Algebra). Der Rang ist nichts anderes als die Dimension.

(ii) Sei $A = \mathbb{Z}$, $M = \mathbb{Z}/2\mathbb{Z}$. Dieser Modul ist nicht frei, denn für jedes Element gilt $2x = 0$. Es gibt keine linear unabhängigen Teilmengen!

(iii) $A^2$ ist frei vom Rang 2 mit Basis $\{(1,0),(0,1)\}$.

**Beispiel.** $A$ ist auch ein $A$-Modul. Die Untermoduln von $A$ sind genau die Ideale. Ist $A \to B$ ein Ringhomomorphismus, so ist $B$ ein $A$-Modul.

**Satz 1.8** (Homomorphiesatz, Noethersche Isomorphiesätze)**.** *Sei $f : M \to N$ ein $A$-Modulhomomorphismus. Dann ist die induzierte Abbildung*

$$\overline{f} : M/\operatorname{Ker} f \to \operatorname{Im} f$$

*ein Isomorphismus von $A$-Moduln. Sind $N, N' \subset M$ Untermoduldn, so ist*

$$(N + N')/N \cong N'/(N \cap N')$$

*ein kanonischer Isomorphismus. Sind $N' \subset N \subset M$ Untermoduln, so ist*

$$(M/N')/(N/N') \cong M/N$$

*ein kanonischer Isomorphismus.*

*Beweis:* In der Algebra zeigt man diese Ausagen für abelsche Gruppen, in der linearen Algebra für Vektorräume. Die Verträglichkeit mit der $A$-Modulstruktur ist leicht zu überprüfen. □

Die folgende Aussage werden wir brauchen.

**Lemma 1.9.** *Sei $R$ ein Ring, $B$ eine quadratische Matrix mit Koeffizienten in $B$. Wenn das Gleichungssystem $By = 0$ eine nichttriviale Lösung $(\lambda_1, \ldots, \lambda_n)$ hat, so folgt $\lambda_i \det B = 0$ für alle $i$.*

*Beweis:* Ist $R$ ein Körper, so gilt diese Aussage mit $\det B = 0$. (Lineare Algebra) Für den Ringfall gehen wir die Beweise durch: Die Determinante wird durch die Leibniz-Formel definiert. Sie ist multilinear und alternierend in den Zeilen und Spalten. Insbesondere bleibt sie unverändert, wenn man ein Vielfaches einer Spalte zu einer anderen addiert. Wir multiplizieren also die Spalte $i$ mit $\lambda_i$ (dies multipliziert die Determinante mit $\lambda_i$) und addieren dann das $\lambda_j$-fache der Spalte $j$ für alle $j \neq i$. In der neuen Matrix verschwindet die $i$-te Spalte, also auch die Determinante. □

**Stichworte kommutative Algebra**

Moduln, $\mathbb{Z}$-Moduln, Basen, freie Moduln, Wohldefiniertheit des Rangs, Untermodul, Quotienten, Kern, Bild, Homormorphiesatz

## Ganze Ringerweiterungen

**Satz 1.10.** *Seien $A \subset R$ Ringe, $x \in R$. Dann sind äquivalent:*

*(i)* *Es gibt $n \in \mathbb{N}$ und $a_1, \ldots, a_n \in A$ mit $x^n + a_1 x^{n-1} + \cdots + a_n = 0$.*

*(ii)* *$A[x] = \left\{\sum_{i=0}^{n} \alpha_i x^i \mid n \in \mathbb{N}_0, \alpha_i \in A\right\}$ ist ein endlich erzeugter $A$-Modul.*

*(iii)* *Es gibt einen Teilring $B \subset R$, der $A$ und $x$ enthält und der ein endlich erzeugter $A$-Modul ist.*

*(iv)* *$x$ ist ganz über $A$.*

**Beispiel.** Seien speziell $A \subset R$ Körper. Dann bedeuten die Bedingungen:

(i) $x$ ist algebraisch über $A$.

(ii) $A[x]$ ist ein endlich dimensionaler $A$-Vektorraum.

(iii) $A, \{x\} \subset B$ und $B$ ist ein endlich dimensionaler $A$-Vektorraum.

In dieser Form ist der Satz aus der Algebra bekannt. Der Beweis bleibt derselbe.

*Beweis:* $(i) \Rightarrow (ii)$: Sei $M \subset R$ der $A$-Modul, der von $1, x, \ldots, x^{n-1}$ erzeugt wird. Nach Vorraussetzung gilt

$$x^n = -a_1 x^{n-1} - \cdots - a_n \in M$$

Rekursiv erhält man also $x^{n+j} \in M$ für alle $j$. Es folgt $A[x] \subset M$. Die umgekehrte Inklusion ist klar. Damit ist $M = A[x]$ und insbesondere ist $A[x]$ endlich erzeugt.
$(ii) \Rightarrow (iii)$: Wähle $B = A[x]$.
$(iii) \Rightarrow (i)$: $B$ werde von $y_1, \ldots, y_n$ als $A$-Modul erzeugt. Wegen $x \in B$ gilt $xy_i \in B$. Es gibt also Koeffizienten $a_{ij} \in A$ mit

$$xy_i = \sum_j a_{ij} y_j \Leftrightarrow \sum_j (a_{ij} - \delta_{ij} x) y_j = 0$$

Dies kann als ein lineares Gleichungssystem über dem Ring $B$ für die $y_j$ gelesen werden. Sei $d$ die Determinante der Koeffizientenmatrix, also das charakteristische Polynom von $(a_{ij})$ an der Stelle $x$. Die Voraussetzung von Lemma 1.9 ist erfüllt. Also gilt $y_i d = 0$ für $i = 1, \ldots, n$. Da $B$ von den $y_i$ erzeugt wird, folgt $bd = 0$ für alle $b \in B$, insbesondere auch $1d = 0$. Das charakteristische Polynom ist die gesuchte Polynomialgleichung für $x$.
$(i) \Leftrightarrow (iv)$ gilt nach Definition. □

*Beweis von Satz 1.5.* Es gilt $x+y, x-y, xy \in A[x,y]$. Sei $x$ ganz über $A$. Dann ist $A[x]$ ein $A$-Modul mit Erzeugern $\{x_1, \ldots, x_n\}$. Sei $y$ ganz über $A$. Dann ist $A[y]$ ein $A$-Modul mit Erzeugern $\{y_1, \ldots, y_m\}$. Dann sind die Elemente $x_i y_j$ Erzeuger von $A[x,y]$, denn in $\alpha = \sum a_{kl} x^k y^l$ können $x$ und $y$ durch die $x_i$ und $y_j$ ausgedrückt werden. Durch Ausmultiplizieren erhält man eine Darstellung von $\alpha$ in Termen der $x_i y_j$. Also ist $A[x,y]$ endlich erzeugt. Nach Satz 1.10 sind dann alle Elemente von $A[x,y]$ ganz über $A$. □

Damit haben wir unser erstes Hauptziel erreicht.

**Korollar 1.11** (Transitivität)**.** *Seien $A \subset B$, $B \subset C$ ganze Ringerweiterungen. Dann ist $A \subset C$ ganz.*

*Beweis:* Sei $x \in C$. Es erfüllt also eine Gleichung

$$x^n + b_1 x^{n-1} + \cdots + b_n = 0 \ , b_i \in B$$

$B$ ist ganz über $A$, also ist $A[b_i]$ endlich erzeugter $A$-Modul. Wie beim letzten Beweis folgt $A[b_1, \ldots, b_n]$ endlich erzeugter $A$-Modul. Wegen $x \in A[b_1, \ldots, b_n]$ ist $x$ ganz über $A$ (Satz 1.10). □

**Definition 1.12.** *Sei $A$ ein Integritätsring. $A$ heißt* ganz abgeschlossen*, wenn $A$ mit seinem ganzen Abschluss im Quotientenkörper übereinstimmt.*

**Beispiel.** Faktorielle Ringe (d.h. solche mit eindeutiger Primfaktorzerlegung, z.B. $\mathbb{Z}$, diskrete Bewertungsringe) sind ganz abgeschlossen.

*Beweis:* Sei $A$ ein Hauptidealring, $K$ der Quotientenkörper, $x \in K$ ganz über $A$. Dann ist

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0, \ a_i \in A$$

Sei $x = a/b$ mit $a$ und $b$ teilerfremd. Die Gleichung wird mit $b^n$ multipliziert:

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

$b$ teilt jeden Summanden außer dem ersten, also folgt $b \mid a^n$. Dies ist ein Widerspruch zur Teilerfremdheit. Es folgt $b$ invertierbar in $A$ und damit $x \in A$. □

**Korollar 1.13.** *Ganzheitsringe sind ganz abgeschlossen.*

*Beweis:* Sei $\mathcal{O}_K$ der ganze Abschluss von $\mathbb{Z}$ in $K$, $\mathcal{O}'$ der ganze Abschluss von $\mathcal{O}_K$ in $K$. Wegen der Transitivität von ganzen Erweiterungen ist dann $\mathcal{O}'$ ganz über $\mathbb{Z}$, also $\mathcal{O}' \subset \mathcal{O}_K$. □

Der Quotientenkörper von $\mathcal{O}_K$ ist $K$. Allgemeiner:

**Lemma 1.14.** *Sei $A$ Ring mit Quotientenkörper $K$ und $L/K$ Körpererweiterung, $B$ der ganze Abschluss von $A$ in $L$. Sei $x \in L$. Dann gibt es $a \in A$ mit $ax \in B$.*

*Beweis:* $x$ erfüllt $x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n = 0$ mit $a_i \in K$. Sei $a$ der Hauptnenner der $a_i$. Multiplikation der Gleichung mit $a^n$ ergibt

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

Also gilt $ax \in B$. □

Eine $K$-Basis von $L$ darf dann einfach ganz, d.h. in $B$ angenommen werden.

**Krulldimension**

**Definition 1.15.** *Sei $A$ ein Ring. Ein* Primideal *von $A$ ist ein Ideal $\mathfrak{p} \subset A$, so dass gilt: $\mathfrak{p} \neq A$ und*

$$ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p} \text{ oder } b \in \mathfrak{p}$$

**Beispiel.** (i) Ist $A$ ein Hauptidealring, so ist $I = (f)$ genau dann ein Primideal, wenn $f$ ein Primelement (oder 0), denn

$$ab \in (f) \Leftrightarrow f|ab \Rightarrow f|a \text{ oder } f|b$$

(ii) $A$ ist ein Integritätsbereich genau dann, wenn 0 ein Primideal ist:

$$ab \in 0 \Leftrightarrow ab = 0 \Rightarrow a = 0 \text{ oder } b = 0$$

**Lemma 1.16.** *Sei $A$ ein Ring, $I$ ein Ideal. $I$ ist genau dann ein Primideal, wenn $A/I$ ein Integritätsbereich ist.*

*Beweis:* Sei $I$ ein Primideal, $a, b \in A$ mit $ab = 0 \mod I$. Dies bedeutet $ab \in I$, also ohne Einschränkung $a \in I$. Dies bedeutet wiederum $a = 0 \mod I$.
Sei umgekehrt $A/I$ Integritätsbereich, $ab \in I$. Dann ist $ab = 0 \mod I$, also ohne Einschränkung $a = 0 \mod I$. Dies bedeutet $a \in I$. □

**Korollar 1.17.** *Maximale Ideale sind Primideale.*

*Beweis:* Sei $\mathfrak{m}$ maximales Ideal von $A$. Dann ist $A/\mathfrak{m}$ ein Körper, also ein Integritätsbereich. □

**Definition 1.18.** *Sei $A$ ein Ring. Die* Krulldimension *von $A$ ist die maximale Länge $n$ einer Kette von Primidealen*

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$$

Die Krulldimension kann auch unendlich sein, sogar in noetherschen Ringen.

**Beispiel.** (i) Körper haben Krulldimension Null.

(ii) Ein Hauptidealring, der kein Körper ist, hat Krulldimension 1. Ist $p$ ein Primelement, so hat die Kette $0 \subset (p)$ keine Verfeinerung.

(iii) Schwierig: $k[X_1, \ldots, X_n]$ hat Dimension $n$.

**Korollar 1.19.** *Sei $B$ ein Integritätsring, $A \subset B$ ein Unterring, so dass $B$ ganz über $A$ ist. Dann gilt:*

$$B \text{ Körper } \Leftrightarrow A \text{ Körper}$$

*Beweis:* Sei $A$ ein Körper, $0 \neq b \in B$. Nach Satz 1.10 ist $B' = A[b]$ ein endlichdimensionaler $A$-Vektorraum. Die Multiplikation mit $B$ ist eine $A$-lineare Abbildung $B' \to B'$. Da $B$ nullteilerfrei ist, ist diese Abbildung injektiv. Da $B'$ endlich dimensional ist, ist sie dann auch surjektiv. Also hat $b$ ein multiplikatives Inverses in $B' \subset B$.
Umgekehrt sei $B$ ein Körper, $0 \neq a \in A$. Sei $b = a^{-1} \in B$. Dieses Element ist ganz über $A$, erfüllt also eine Gleichung

$$b^n + a_1 b^{n-1} + \cdots + a_n = 0 \; a_i \in A \; .$$

Diese Gleichung wird mit $a^{n-1}$ multipliziert.

$$b + a_1 + a_2 a + \ldots a_n a^{n-1} = 0 \; .$$

Alle Summanden außer dem ersten liegen in $A$, also auch $b$. □

**Satz 1.20.** *Sei $A \subset B$ ganze Erweiterung von Integritätsringen mit $A$ von Krulldimension* 1*. Dann hat $B$ ebenfalls Krulldimension* 1*.*

**Bemerkung.** Tatsächlich gilt für ganze Ringerweiterungen $\dim A = \dim B$. Der Fall von Dimension 0 war unser Korollar 1.19.

*Beweis:* Sei $\mathfrak{p} \subset B$ ein Primideal ungleich 0. Zu zeigen ist, dass $\mathfrak{p}$ maximal ist. Auch $\mathfrak{p}' = \mathfrak{p} \cap A$ ist ein Primideal.

**Behauptung.** $\mathfrak{p}' \neq 0$*.*

Sei $x \in \mathfrak{p} \setminus \{0\}$ mit

$$0 = x^n + a_1 x^{n-1} + \cdots + a_n = x(x^{n-1} + a_1 x^{n-2} + \ldots a_{n-1}) + a_n$$

und $a_i \in A$, ohne Einschränkung $a_n \neq 0$. Es folgt $a_n \in \mathfrak{p} \cap A$.
Die Abbildung

$$A/\mathfrak{p}' \to B/\mathfrak{p}$$

ist ein injektiver Ringhomomorphismus. Also ist der Integritätsring $B/\mathfrak{p}$ eine ganze Erweiterung des Körpers $A/\mathfrak{p}'$. Nach Korollar 1.19 ist dann auch $B/\mathfrak{p}$ ein Körper, d.h. $\mathfrak{p}$ ist maximal. □

**Korollar 1.21.** *Sei $K$ globaler Körper mit Ganzheitsring $\mathcal{O}_K$. Dann hat $\mathcal{O}_K$ die Krulldimension* 1*.*

*Beweis:* Wir wenden den Satz an auf $A = \mathbb{Z}$ (bzw. $A = \mathbb{F}_p[t]$) und $B = \mathcal{O}_K$. $\square$

Später werden wir auch noch einen anderen Spezialfall benötigen.

**Korollar 1.22.** *Sei $A$ ganz abgeschlossen mit Quotientenkörper $K$. Sei $L/K$ Körpererweiterung und $b_1, \ldots, b_n \in L$ seien ganz über $A$. Dann ist $B = A[b_1, \ldots, b_n]$ ganze Erweiterung von $A$ und hat Krulldimension* 1.

# Kapitel 2

# Noethersche Ringe und Spurpaarung

Ist $A \subset B$ eine ganze Ringerweiterung, $x \in B$, so ist $A[x]$ endlich erzeugter $A$-Modul. Hieraus folgt natürlich nicht, dass $B$ endlich erzeugter $A$-Modul ist. Wir könnten eine Kette

$$A \subsetneq A[x_1] \subsetneq A[x_1, x_2] \subsetneq A[x_1, x_2, x_3] \subsetneq \dots$$

haben. Es gibt Bedingungen, die das verhindern - und sie sind in unserer Situation erfüllt.

**Definition 2.1.** *Ein Ring $A$ heißt* noethersch*, wenn jedes Ideal endlich erzeugt ist.*

**Beispiel.** Hauptidealringe (d.h. ein Ring, in dem Jedes Ideal ein Hauptideal ist) sind noethersch, denn jedes Ideal wird von nur einem Element erzeugt.

**Stichworte kommutative Algebra**

Hauptidealringe, euklidischer Algorithmus, Primfaktorzerlegung

**Beispiel.** Nicht so leicht zu sehen, aber richtig: Ist $k$ ein Körper, so ist $k[X_1, \dots, X_n]$ noethersch. (Hilbertscher Basissatz)

Meist werden die folgenden Eigenschaften noetherscher Ringe ausgenutzt:

**Lemma 2.2.** *Sei $A$ ein noetherscher Ring.*

*(i)*

$$I_1 \subset I_2 \subset I_3 \subset \dots$$

*eine Folge von Idealen. Dann wird diese stationär, d.h. es gibt $n_0 \in \mathbb{N}$, so dass $I_n = I_{n+1}$ für alle $n \geq n_0$.*

*(ii) Sei $\Phi \neq \emptyset$ eine Menge von Idealen von $A$. Dann hat $\Phi$ ein maximales Element.*

*(iii) Sei $M$ ein endlich erzeugter Modul, $N \subset M$ ein Untermodul. Dann ist $M$ endlich erzeugt.*

*Beweis:* Wir betrachten eine Idealkette. Sei $I = \bigcup I_n$. Dies ist ein Ideal. Nach Vorraussetzung ist $I$ endlich erzeugt. Seien $a_1, \ldots, a_m$ Erzeuger. Dann gibt es $n_i$ für $i = 1, \ldots, m$, so dass $a_i \in I_{n_i}$. Sei $n_0 = \max n_i$. Dann gilt $a_i \in a_{n_0}$ für alle $i$. Dies bedeutet $I_{n_0} = I$, also auch $I_n = I_{n_0}$ für $n \geq n_0$.
Sei nun $\Phi$ ein Menge von Idealen von $A$. Angenommen, es gibt kein maximales Element. Sei $I_1 \in \Phi$. Da $I_1$ nicht maximal ist, gibt es $I_2 \in \Phi$ mit $I_1 \subsetneq I_2$. Da $I_2$ nicht maximal ist finden wir $I_3 \in \Phi$ mit $I_2 \subsetneq I_3$. Iterativ finden wir eine Kette von Idealen, die nicht stationär wird. Dies ist ein Widerspruch zu $A$ noethersch.
Induktion nach der Anzahl der Erzeuger. Hat $M$ nur einen Erzeuger, so ist $M \cong A/I$ für ein Ideal $I$ und $N \cong J/I \cap J$ für ein anderes Ideal. Nach Definition eines noetherschen Rings ist $J$ endlich erzeugt, also auch $J/I \cap J$. Sei nun jeder Untermodul eine Moduls mit $n$ Erzeugern endlich erzeugt. Sei $M$ ein Modul mit Erzeugern $x_0, \ldots, x_n$ und $N \subset M$ ein Untermodul. Dann wird $M/Ax_0$ von den Bildern von $x_1, \ldots, x_n$ erzeugt. Nach Induktionsvoraussetzung wird der Bildmodul $N_0 = N/N \cap Ax_0$ von endlich vielen Elementen erzeugt. Seien $f_1, \ldots, f_m$ ihre Urbilder in $N$. Der Modul $N \cap Ax_0$ ist Untermodul von $Ax_0$ (ein Erzeuger), hat also endlich viele Erzeuger $f_{m+1}, \ldots, f_N$. Man rechnet leicht nach, dass $f_1, \ldots, f_N$ dann $N$ erzeugen. □

**Definition 2.3.** *Ein* Dedekindring *ist ein noetherscher, ganz abgeschlossener* 1*-dimensionaler Ring.*

**Theorem 2.4.** *Ganzheitsringe sind Dededkindringe.*

Nach den Ergebnissen aus Kapitel 1 müssen wir dafür zeigen:

**Theorem 2.5.** *Ganzheitsringe sind noethersch.*

Wir beweisen zunächst:

**Theorem 2.6.** *Sei $A$ ein ganz abgeschlossener noetherscher Ring mit Quotientenkörper $K$ und $L/K$ separable Körpererweiterung. Dann ist der ganze Abschluss $B$ von $A$ in $L$ ein endlich erzeugter $A$-Modul. Insbesondere ist $B$ noethersch.*

**Korollar 2.7.** *Theorem 2.4 gilt für $\mathcal{O}_K$, falls $K$ Zahlkörper oder separable Erweiterung von $\mathbb{F}_p(t)$.*

*Beweis:* Ist $K$ ein Zahlkörper, so ist die Erweiterung $K/\mathbb{Q}$ separabel. Die Ringe $\mathbb{Z}$ bzw. $\mathbb{F}_p[t]$ sind als Hauptidealringe noethersch. Wir sind also in der Situation von Theorem 2.6. □

**Bemerkung.** Es fehlt also der nicht-separable Fall, der für Funktionenkörper auftauchen kann. Betrachte z.B. den Körperhomomorphism

$$\mathbb{F}_p(t_1) \to \mathbb{F}_p(t_2) \qquad t_1 \mapsto t_2^p$$

Dann erfüllt $t_2$ das Polynom $X^p - t_1 \in \mathbb{F}_p(t_1)[X]$. Dieses Polynom ist nach dem Eisensteinkriterium irreduzibel. Es ist nicht separabel, den die Ableitung ist $pX^{p-1} = 0 \in \mathbb{F}_p(t_1)[X]$.
Wir werden später ein anderes Argument sehen, dass diesen Fall erledigt.

## Norm, Spur und Diskriminante

Sei $L/K$ algebraisch und separabel, $\alpha \in L$. Das Minimalpolynom $\mathrm{Min}(\alpha)$ von $\alpha$ ist das normierte Polynom minimalen Grades mit Nullstelle $\alpha$.

**Beispiel.** In Charakteristik Null sind alle Erweiterungen separabel. Erweiterungen von endlichen Körpern ebenfalls. Dies sind die beiden wichtigsten Fälle, die bei uns vorkommen werden.

**Lemma 2.8.** $\mathrm{Min}(\alpha)$ *ist das charakteristische Polynom* $\det(X\,\mathrm{id} - m_\alpha)$ *der* $K$*-linearen Multiplikationsabbildung* $m_\alpha : K(\alpha) \to K(\alpha)$ *mit* $x \mapsto \alpha x$*.*

*Beweis:* Sei $P$ das charakteristische Polynom. Es hat den Grad $[K(\alpha) : K] = \deg \mathrm{Min}(\alpha)$. Es ist normiert. Es gilt (Satz von Cayley-Hamilton) $P(m_\alpha) = 0$ als Abbildung $K(\alpha) \to K(\alpha)$. Auswerten in 1 ergibt $P(\alpha) = 0$. Also erfüllt $P$ alle Eigenschaften von $\mathrm{Min}(\alpha)$. □

Seien $\alpha_1, \ldots, \alpha_d$ die $d$ verschiedenen ($L/K$ separabel!) Nullstellen von $\mathrm{Min}(\alpha)$ in $\overline{K}$. Jedes $\alpha_i$ definiert einen Körperhomomorphismus $\sigma_i : K(\alpha) \to \overline{K}$ mit $\sigma_i(\alpha) = \alpha_i$. Dies sind alle Körperhomomorphismen $\sigma : K(\alpha) \to K$ mit $\sigma|_K = \mathrm{id}$.

**Lemma 2.9.** *Es gilt*

$$\mathrm{Min}(\alpha) = \prod_{i=1}^{d}(X - \alpha_i) = \prod_{i=1}^{d}(X - \sigma_i(\alpha)) \ .$$

*Beweis:* Klar □

**Bemerkung.** $K(\alpha)/K$ ist galois genau dann, wenn alle $\alpha_i \in K(\alpha)$. Dann ist $\{\sigma_1, \ldots, \sigma_d\} = \mathrm{Gal}(K(\alpha)/K)$.

**Definition 2.10.** *Sei* $L/K$ *endliche Körpererweiterung,* $\alpha \in L$*. Das* charakteristische Polynom *von* $\alpha$ *ist*

$$P_\alpha(X) = \det(X\,\mathrm{id} - m_\alpha)$$

*wobei* $m_\alpha : L \to L$ *die Multiplikationsabbildung mit* $\alpha$ *ist. Die* Norm *von* $\alpha$ *ist*

$$N_{L/K}(\alpha) = \det(m_\alpha)$$

*Die* Spur *von* $\alpha$ *ist*

$$\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}(m_\alpha)$$

**Bemerkung.** Es gilt $P_\alpha(X) = X^{[L:K]} - \mathrm{Tr}(\alpha)X^{[L:K]-1} + \cdots + (-1)^{[L:K]}N(\alpha)$.

**Lemma 2.11.** *Sei $L/K$ separable Körpererweiterung, $[L : K] = d$. Seien $\alpha_1, \ldots, \alpha_d$ die Nullstellen von $\mathrm{Min}(\alpha)$, jede mit Vielfachheit $[L : K(\alpha)]$. Seien*

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

*die Einbettungen mit $\sigma_i|_K = \mathrm{id}$. Dann gilt*

$$\begin{aligned} P_\alpha(X) &= \mathrm{Min}(\alpha)^{[L:K(\alpha)]} = \prod_{i=1}^{d}(X - \alpha_i) = \prod_{i=1}^{d}(X - \sigma_i(\alpha)) \\ \mathrm{Tr}_{L/K}(\alpha) &= \sum \alpha_i = \sum \sigma_i(\alpha) \\ N_{L/K}(\alpha) &= \prod \alpha_i = \prod \sigma_i(\alpha)\ . \end{aligned}$$

*Beweis:* Es genügt, die Aussge für $P_\alpha$ zu zeigen. Es gilt

$$\{\alpha_1, \ldots, \alpha_d\} = \{\sigma_1(\alpha), \ldots, \sigma_d(\alpha)\}$$

als Mengen mit Vielfachheit, denn jede der $[K(\alpha) : K]$ vielen Einbettungen $K(\alpha) \to \overline{K}$ lässt sich auf $[L : K(\alpha)]$ viele Weisen nach $L$ fortsetzen. Der Fall $L = K(\alpha)$ ist Lemma 2.8. Sei nun $r = [L : K(\alpha)]$.

**Behauptung.** $P_{L/K} = P^r_{K(\alpha)/K}$.

Sei $y_1, \ldots, y_r$ eine Basis von $L/K(\alpha)$, $z_1, \ldots, z_q$ eine Basis von $K(\alpha)/K$. Dann ist $\{y_i z_j \mid i = 1, \ldots, r, j = 1, \ldots, q\}$ eine Basis von $L/K$. Sei $M = (m_{jk})$ die Matrix der Multiplikation mit $\alpha$ bezüglich der $z_j$, d.h. $m_\alpha(z_j) = \sum_k m_{jk} z_k$. Dann gilt $m_\alpha(y_i z_j) = \sum_k m_{jk} y_i z_k$. Die Matrix von $m_\alpha$ bezüglich der Basis $y_i z_j$ ist eine diagonale Blockmatrix aus $r$ Kopien von $M$. □

**Korollar 2.12.** *Sei $L/K$ separable Erweiterung von globalen Körpern, $\alpha \in \mathcal{O}_L$. Dann gilt $P_\alpha \in \mathcal{O}_K[X]$. Insbesondere ist $\mathrm{Tr}_{L/K}(\alpha), N_{L/K}(\alpha) \in \mathcal{O}_K$.*

**Bemerkung.** Falls $\mathcal{O}_L \cong \mathcal{O}_K^d$ (im Allgemeinen falsch!), so hat die Matrix von $m_\alpha$ Einträge in $\mathcal{O}_K$ und die Aussage ist klar.

*Beweis:* $P_\alpha(X) = \prod(X - \sigma(\alpha))$ mit $\sigma$ wie im Lemma. Nach Vorraussetzung erfüllt $\alpha$ eine Gleichung

$$X^n + a_1 X^{n-1} + \cdots + a_0 = 0 \text{ mit } a_i \in \mathcal{O}_K$$

Dann erfüllt $\sigma(\alpha)$ dieselbe Gleichung, ist also ebenfalls ganz über $\mathcal{O}_K$. Damit sind alle Koeffizienten von $P_\alpha$ ganz über $\mathcal{O}_K$. Gleichzeitig liegen sie in $K$. Da $\mathcal{O}_K$ ganz abgeschlossen ist, liegen die Koeffizienten in $\mathcal{O}_K$. □

**Beispiel.** $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{3})$, $\mathcal{O} = \mathbb{Z}[\sqrt{3}]$. Wir wählen die Basis $1, \sqrt{3}$. Sei $\alpha = a + b\sqrt{3}$. Die Multiplikation mit $\alpha$ hat die Matrix

$$\begin{pmatrix} a & 3b \\ b & a \end{pmatrix}$$

Also ist die Spur $2a$, die Norm $a^2 - 3b^2$, das charakteristische Polynom

$$P_\alpha(X) = X^2 - \mathrm{Tr}(\alpha)X + N(\alpha) = X^2 - 2aX + (a^2 - 3b^2)$$

Für $b \neq 0$ ist dies das Minimalpolynom von $\alpha$. Für $b = 0$ gilt $X^2 - 2aX + a^2 = (X - a)^2 = \mathrm{Min}(\alpha)^2$.

**Definition 2.13.** *Sei $A \subset B$ eine Ringerweiterung, $B$ ein freier $A$-Modul vom Rang $d$. Die* Spurpaarung *ist die symmetrische $A$-bilineare Abbildung*

$$(\cdot, \cdot) : B \times B \to A \ , (x, y) = \mathrm{Tr}_{B/A}(xy) \ .$$

*Sei $x_1, \ldots, x_d$ eine Basis von $B$. Dann heißt*

$$D(x_1, \ldots, x_d) = \det(\mathrm{Tr}(x_i x_j)_{i,j})$$

Diskriminante *der Basis. Die* Diskriminante $\mathcal{D}_{B/A}$ *ist das Ideal, das $D(x_1, \ldots, x_d)$ erzeugt wird.*

**Bemerkung.** Uns interessiert vor allem $L/K$ endliche Köpererweiterung, aber auch $\mathcal{O}_K/\mathbb{Z}$.

**Beispiel.** Sei $L = \mathbb{Q}[X]/(X^2+pX+q)$ mit $p, q \in \mathbb{Q}$. Dies ist ein 2-dimensionaler $\mathbb{Q}$-Vektorraum, Basis $1, X$. Es gilt $\mathrm{Tr}(1) = 2$. Multiplikation mit $X$ hat die Matrix

$$\begin{pmatrix} 0 & -q \\ 1 & -p \end{pmatrix}$$

also, $\mathrm{Tr}(X) = -p$.
Es gilt

$$D(1, X) \ = \ \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(X) \\ \mathrm{Tr}(X) & \mathrm{Tr}(X^2) \end{pmatrix} \ = \ \det \begin{pmatrix} 2 & -p \\ -p & p^2 - 2q \end{pmatrix} \ = \ p^2 \ - \ 4q$$

Dies ist genau die Diskriminate der quadratischen Gleichung.

**Lemma 2.14.** *Sei $y_1, \ldots, y_d \in B$ mit $y_i = \sum a_{ij} x_j$. Dann gilt*

$$D(y_1, \ldots, y_d) = \det(a_{ij})^2 D(x_1, \ldots, x_d)$$

*Insbesondere ist $\mathcal{D}_{B/A}$ wohldefiniert.*

*Beweis:* Es gilt

$$\mathrm{Tr}(y_p y_q) = \mathrm{Tr}\left( \sum_{i,j} a_{pi} a_{qj} x_i x_j \right) = \sum a_{pi} a_{qj} \mathrm{Tr}(x_i x_j)$$

Es folgt

$$(\mathrm{Tr}(y_p y_q))_{pq} = (a_{pi})_{pi} (\mathrm{Tr}(x_i x_j))_{ij} (a_q j)^t$$

wobei $^t$ die transponierte Matrix ist. Dies impliziert die Gleichheit der Determinanten. □

## Exkurs in die bilineare Algebra

Sei $(\cdot,\cdot) : V \times V \to k$ eine symmetrische Bilinearform, ($k$ Körper, $V$ ein Vektorraum). Sei $v_1, \ldots, v_d$ eine Basis von $V$, $M = (v_i, v_j)_{ij}$ die zugehörige symmetrische Matrix. Dann gilt für $v = \sum a_i v_i, w = \sum_j b_j v_j$

$$(v,w) = \left( \sum a_i v_i, \sum_j b_j v_j \right) = \sum_{i,j} a_i (v_i, v_j) b_j = (a_1, \ldots, a_d)^t M (b_1, \ldots, b_d)$$

**Definition 2.15.** *Die Bilinearform $(\cdot,\cdot)$ heißt nicht-degeneriert, wenn aus $(v,w) = 0$ für alle $w$ die Gleichung $v = 0$ folgt.*

**Lemma 2.16.** *$(\cdot,\cdot)$ ist nichtdegeneriert genau dann, wenn die zugehörige Matrix $M$ invertierbar ist, also genau dann, wenn* $\det M \neq 0$.

*Beweis:* Falls $M$ nicht invertierbar ist, so gibt es $v$ mit $v^t M = 0$, also auch $v^t M w = 0$ für alle $w$. Sei nun $M$ invertierbar, $v = \sum a_i v_i$. Der Fall $d = 1$ ist trivial, also sei $d > 1$. Wähle $(c_1, \ldots, c_d)$ mit

$$a_1 c_1 + \cdots + a_d c_d \neq 0$$

Wir lösen das Gleichungssystem $Mw = (c_1, \ldots, c_d)^t$. Dies ist möglich, da $M$ invertierbar ist. Es folgt $v^t M w \neq 0$. □

**Bemerkung.** Die Diskriminante entscheidet also, ob die Spurpaarung nichtdegeneriert ist.

**Beispiel.** $K = \mathbb{Q}(\sqrt{3})/\mathbb{Q}$. Es gilt

$$D(1, \sqrt{3}) = \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\sqrt{3}) \\ \mathrm{Tr}(\sqrt{3}) & \mathrm{Tr}(3) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 6 \end{pmatrix} = 12$$

**Lemma 2.17.** *Sei $(\cdot,\cdot)$ nicht-degenererierte symmetrische Bilinearform, $v_1, \ldots, v_d$ eine Basis. Dann gibt es eine* duale Basis *$w_1, \ldots, w_d$ mit $(v_i, w_j) = \delta_{ij}$.*

*Beweis:* Die Bestimmung von $w_j$ bedeutet das Lösen eines linearen Gleichungssystems $Mw_j = (0, \ldots, 1, \ldots, 0)$ (mit 1 an der $j$-ten Stelle). Dies ist möglich, da $M$ invertierbar ist. □

**Satz 2.18.** *Sei $L/K$ separable endliche Körpererweiterung. Dann ist $\mathcal{D}_{L/K} \neq 0$. Die Spurpaarung ist nicht-degeneriert.*

*Beweis:* Es gilt $\mathrm{Tr}(\alpha) = \sum \sigma_i(\alpha)$, wobei $\sigma_i : L \to \overline{K}$ für $i = 1, \ldots, d$ die Einbettungen mit $\sigma_i|_K = \mathrm{id}$ durchläuft. (Hier benutzen wir die Separabilität.) Sei $x_1, \ldots, x_d$ eine Basis von $L$ über $K$. Es gilt

$$D(x_1, \ldots, x_d) = \det\left(\mathrm{Tr}(x_i y_j)_{ij}\right) = \det\left( \sum_k \sigma_k(x_i x_j) \right)_{ij}$$

$$= \det\left( \sum_k \sigma_k(x_i)\sigma_k(x_j) \right)_{ij} = \det\left( (\sigma_k(x_i))_{ik} (\sigma_k(x_j))_{kj} \right) = \det(\sigma_i(x_j))^2$$

Angenommen diese Determinante verschwindet. Dann gibt es $u_1, \dots, u_d \in \overline{K}$ mit $\sum_i u_i \sigma_i(x_j) = 0$ für alle $j$. Da die $x_j$ eine Basis sind, folgt $\sum u_i \sigma_i = 0$ als Abbildungen $L^* \to \overline{K}$. Als Gruppenhomomorphismen $L^* \to \overline{K}^*$ sind die $\sigma_i$ jedoch linear unabhängig nach Lemma 2.19. □

**Lemma 2.19.** *Sei $G$ eine Gruppe, $k$ ein Körper, $\sigma_i : G \to k^*$ für $i = 1, \dots, m$ verschiedene Gruppenhomomorphismen. Dann sind sie linear unabhänging im $k$-Vektorraum* $\mathrm{Abb}(G, k)$.

Dies ist ein wesentlicher Schritt im Beweis des Hauptsatzes der Galoistheorie. Da das Lemma wichtig und einfach ist, führen wir den Beweis noch einmal.

*Proof.* Angenommen, die Aussage ist falsch. Dann gibt es eine minimale linear abhängige Teilmenge von $\{\sigma_1, \dots, \sigma_m\}$. Ohne Einschränkung besteht sie aus $\sigma_1, \dots, \sigma_n$ mit $n \leq m$. Es ist $n \geq 2$, denn $\sigma_1 \neq 0$, da es Werte in $k^*$ annimmt. Sei nun

$$a_1\sigma_1 + \cdots + a_n\sigma_n = 0$$

eine nichttriviale Relation in $\mathrm{Abb}(G, k)$. Wegen der Minimalität der Relation gilt $a_i \neq 0$ für alle $i$. Seien $g, h \in G$. Es gilt

$$\begin{aligned} 0 =& a_1\sigma_1(gh) + \cdots + a_n\sigma_n(gh) \\ =& a_1\sigma_1(g)\sigma_1(h) + \cdots + a_n\sigma_n(g)\sigma_n(h) \end{aligned}$$

Da dies für alle $h$ gilt, erhalten wir eine neue Relation

$$0 = a_1\sigma_1(g)\sigma_1 + \cdots + a_n\sigma_n(g)\sigma_n$$

Andererseits multiplizieren wir die ursprüngliche Relation mit $\sigma_1(g)$

$$0 = a_1\sigma_1(g)\sigma_1 + \cdots + a_n\sigma_1(g)\sigma_n$$

Durch Subtraktion ergibt sich

$$0 = 0 + a_2(\sigma_1(g) - \sigma_2(g))\sigma_2 + \cdots + a_n(\sigma_n(g) - \sigma_1(g))\sigma_n$$

Wir wählen speziell $g$ mit $\sigma_1(g) \neq \sigma_2(g)$. Dies ist möglich wegen $\sigma_1 \neq \sigma_2$. Damit haben wir eine neue, kürzere nichttrivale Relation gefunden. Dies ist ein Widerspruch zur Wahl der $\sigma_i$. □

**Beispiel.** $L = \mathbb{Q}[X]/(X^2 + pX + q)$ hatte Diskriminante $p^2 - 4q$. Diese Zahl verschwindet genau dann, wenn $X^2 + pX + q$ eine doppelte Nullstelle hat, also wenn $L$ kein Körper ist.

*Beweis von Theorem 2.6.* Sei $A$ ganz abgeschlossen und noethersch mit Quotientenkörper $K$. Sei $L/K$ separabel und $B$ der ganze Abschluss von $A$ in $B$. Wir wollen zeigen, dass $B$ endlich erzeugt als $A$-Modul ist.
Sei $x_1, \dots, x_d$ eine Basis von $L/K$. Ohne Einschränkung gilt $x_i \in B$. Sei $y_1, \dots, y_d$ die duale Basis bezüglich der Spurpaarung.

**Behauptung.** $B \subset < y_1, \ldots, y_d >_A$.

Sei $z \in B$. Wir schreiben $z = \sum b_j y_j$ mit $b_j \in K$, da die $y_j$ eine Basis bilden. Es gilt $x_i z \in B$, da $B$ ein Ring ist. Nach Korollar 2.12 ist $\mathrm{Tr}(x_i z) \in A$. Es folgt weiter

$$\mathrm{Tr}(x_i z) = \sum \mathrm{Tr}(x_i b_j y_j) = \sum b_j \mathrm{Tr}(x_i y_j) = b_i$$

$B$ ist in einem endlich erzeugten $A$-Modul enthalten. Da $A$ noethersch ist, ist $B$ selbst endlich erzeugter $A$-Modul.
Sei $I \subset B$ ein Ideal. Dann ist $I$ ein $A$-Modul. Da $B$ als $A$-Modul endlich erzeugt ist und $A$ noethersch, ist $I$ als $A$-Modul endlich erzeugt. Dann ist $I$ erst recht als $B$-Modul, d.h.als Ideal endlich erzeugt. □

**Stichworte kommutative Algebra**

Moduln über Hauptidealringen: Elementarteilersatz, Struktursatz

**Korollar 2.20.** *Sei $A$ ein Hauptidealring mit Quotientenkörper $K$ und $L/K$ eine separable Körpererweiterung vom Grad $d$. Sei $B$ der ganze Abschluss von $A$ in $L$. Dann ist $B$ ein freier $A$-Modul vom Rang $d$.*

*Beweis:* $B$ ist ein endlich erzeugter $A$-Modul. Nach dem Elementarteilersatz hat $B$ die Gestalt

$$A^r \times A/(m_1) \times \cdots \times A/(m_n)$$

für $m_i \neq 0$. Da $B \subset L$ ist, muss $n = 0$. Damit ist $B$ freier $A$-Modul von Rang $r$. Zu zeigen bleibt $r = d$.
Sei $x_1, \ldots, x_d$ eine $K$-Basis von $L$. Ohne Einschränkung liegen diese Elemente in $B$. Dort sind sie ebenfalls linear unabhängig, erzeugen also einen freien $A$-Modul vom Rang $d$. Nach Elementarteilersatz ist $d \leq r$.
Sei umgekehrt $y_1, \ldots, y_r$ eine $A$-Basis von $B$. Angenommen, die Elemente sind linear abhängig über $L$. Betrachte

$$\lambda_1 y_1 + \lambda_2 y_2 + \cdots + \lambda_r y_r = 0$$

mit $\lambda_i \in K$. Sei $0 \neq a \in A$ ein Hauptnenner für die $\lambda_i$. Dann ist

$$a\lambda_1 y_1 + \cdots + a\lambda_r y_r = 0$$

eine Relation in $A$. Da die $y_i$ linear unabhängig sind, folgt $a\lambda_i = 0$ für alle $i$. Wegen $a = 0$ folgt $\lambda_i = 0$ für alle $i$. Damit sind die $y_i$ linear unabhängig, also $r \leq d$. □

# Kapitel 3

# Der nicht separable Fall

Die Argumente des letzten Kapitels hingen wesentlich von der Separabilitätsvoraussetzung ab. Im Zahlkörperfall ist dies immer erfüllt. Im Funktionenkörperfall gibt es jedoch auch inseparable Erweiterungen, die wir ebenfalls verstehen wollen. Zur allgemeinen Theorie insepabler Erweitungen vergleiche Lang, Algebra V §6.
Sei in diesem Abschnitt alle Körper von Charakteristik $p > 0$.
Zur Erinnerung: Sei $L/K$ Körpererweiterung. Ein Element $\alpha \in L$ heißt *inseparabel*, falls das Minimalpolynom $\mathrm{Min}(\alpha)$ nicht separabel ist, d.h. mehrfache Nullstellen in $\overline{K}$ hat. Dies ist genau dann der Fall, wenn $\mathrm{Min}(\alpha)' = 0$. Eine Erweiterung heißt *rein inseparabel*, wenn alle Elemente in $L \setminus K$ inseparabel sind.

**Beispiel.** $K = \mathbb{F}_p(t)$, $L = \overline{K}$, $\alpha = t^{\frac{1}{p}}$, d.h. $\alpha^p = t$. Dieses Element hat Minimalpolynom

$$\mathrm{Min}(\alpha) = X^p - t \Rightarrow \mathrm{Min}(\alpha)' = pX^{p-1} = 0$$

Tatsächlich ist dieser Fall typisch:

**Lemma 3.1.** *Sei $L/K$ algebraische Körpererweiterung in Charakteristik $p$. Sei $\alpha \in L$ inseparabel. Dann gilt* $\mathrm{Min}(\alpha) \in K[X^p]$.

*Beweis:* Sei

$$Min(\alpha) = X^n + a_1 X^{n-1} + \cdots + a_n \Rightarrow$$
$$\mathrm{Min}(\alpha)' = nX^{n-1} + (n-1)a_1 X^{n-2} + \cdots + a_{n-1} = 0$$

Es ist also $n = 0$ in $K$, also $p|n$. Für alle $i < n$ gilt also $(n-i)a_i = -ia_i = 0$. Falls $p \nmid i$, muss $a_i = 0$ sein. □

Hinter dem Ganzen steckt der Frobeniusendomorphismus:

$$\mathrm{Fr}_p : x \mapsto x^p$$

In Charakteristik $p$ ist dies ein Körperendomorphismus, da $(x+y)^p = x^p + y^p$. Wir schreiben $K^p$ für das Bild von $\mathrm{Fr}_p$. Dies ist ein Teilkörper von $K$. Ist $K = K^p$, so ist der Körper *perfekt*, d.h. es gibt keine inseparablen Erweiterungen.

*Beweis:* Sei $P \in K[X^p]$ ein Polynom, $K = K^p$. Dann ist

$$P = \sum_{i=0}^{n} a_i X^{pi}$$

Nach Voraussetzung gibt es $b_i \in K$ mit $b_i^p = a_i$. Dann ist

$$Q = \sum_{i=0}^{n} b_i X^i$$

eine $p$-te Wurzel von $P$. Insbesondere ist $P$ nicht irreduzibel. □

**Beispiel.** (i) Für $K = \mathbb{F}_p$ ist der Frobenius die Identität (kleiner Satz von Fermat oder Theorie der endlichen Körper). Alle endlichen Körper sind daher perfekt.

(ii) Für $K = \mathbb{F}_p(t)$ ist $K^p = \mathbb{F}_p(t^p)$, denn jedes solche Polynom hat eine $p$-te Wurzel.

Der *Separabilitätsgrad* $[L:K]_s$ einer Erweiterung ist die Anzahl der Einbettungen $\sigma : L \to \overline{K}$ mit $\sigma|_K = \mathrm{id}$. Er ist multiplikativ.

**Beispiel.** Sei $L = K(\alpha)$ und

$$\mathrm{Min}(\alpha) = \prod_{i=1}^{d} (X - \alpha_i)^{e_i}$$

die Faktorisierung über dem algebraischen Abschluss. Dann ist $d = [L:K]_s$. Ist insbesondere $d = 1$, so gilt

$$\mathrm{Min}(\alpha) = (X-\alpha)^{p^m} = X^{p^m} - \alpha^{p^m}$$

mit $\alpha^{p^m} \in K$.

**Lemma 3.2.** *Sei $L/K$ rein inseparabel vom Grad $p^m$. Dann gibt es eine Kette*

$$L = L_m \supsetneq L_{m-1} \supsetneq L_{m-2} \supsetneq \ldots L_0 = K$$

*mit $[L_i : L_{i-1}] = p$.*

*Beweis:* Ohne Einschränkung ist $L/K$ einfach, d.h. $L = K(a^{\frac{1}{p^m}})$ für $a \in K$. Dann ist $L_i = K(a^{\frac{1}{p^i}})$. □

**Lemma 3.3.** *Sei $L/\mathbb{F}_p(t)$. Dann ist $[L : L^p] = p$ und die Erweiterung ist rein inseparabel.*

*Beweis:* $\mathrm{Fr}_p$ induziert einen Isomorphismus der Körpererweiterungen $L/\mathbb{F}_p(t)$ und $L^p/\mathbb{F}_p(t)^p$. Insbesondere haben diese beiden Erweiterungen denselben Grad. Wegen der Multiplikativität des Grades von Körpererweiterungen folgt

$$[L : L^p] = [F_p(t) : \mathbb{F}_p(t^p)] = p$$

Dasselbe Argument angewendet auf den Separabilitätsgrad zeigt, dass die Erweiterung rein inseparabel ist. □

**Bemerkung.** Die Voraussetzung $L/\mathbb{F}_p(t)$ ist hier wirklich notwendig. Für endliche Erweiterungen von $\mathbb{F}_p(t_1, t_2)$ ergibt dasselbe Argumente $[L : L^p] = p^2$. In dieser Situation ist der Ganzheitsring zweidimensional.

Über $\mathbb{F}_p(t)$ ist dies der einzige Fall:

**Satz 3.4.** *Sei $L/\mathbb{F}_p(t)$ rein inseparabel vom Grad $p^m$. Dann ist $L^{p^m} = \mathbb{F}_p(t)$ und $L \cong \mathbb{F}_p(t^{\frac{1}{p^m}})$.*

*Beweis:* Wegen Lemma 3.2 und vollständiger Induktion genügt es, den Fall $m = 1$ zu behandeln. Es ist $L = \mathbb{F}_p(t)(a^{\frac{1}{p}})$ mit $a \in \mathbb{F}_p(t)$. Wegen $\mathbb{F}_p(t^{\frac{1}{p}})^p = \mathbb{F}_p(t)$ hat $a$ in $\mathbb{F}_p(t^{\frac{1}{p}})$ eine Wurzel. Es gibt also eine Einbettung $L \to \mathbb{F}_p(t^{\frac{1}{p}})$. Da beide den Grad $p$ haben, folgt Gleichheit. □

**Korollar 3.5.** *Sei $L/\mathbb{F}_p(t)$ endlich und rein inseparabel. Dann ist $\mathcal{O}_L$ ein freier $\mathbb{F}_p[t]$-Modul von endlichem Rang.*

*Beweis:* Sei $p^m$ der Grad der Erweiterung. Dann ist $L = \mathbb{F}_p(t^{\frac{1}{p^m}})$. Daher ist $\mathrm{Fr}_p^m : L \to \mathbb{F}_p(t)$ ein Körperisomorphismus. Er induziert also auch einen Isomorphismus von Ringen $\mathbb{F}_p[t^{\frac{1}{p}}] \to \mathbb{F}_p[t]$. Insbesondere ist $\mathbb{F}_p[t^{\frac{1}{p}}]$ ganz abgeschlossen. Das Element $t^{\frac{1}{p}}$ ist ganz über $\mathbb{F}_p[t]$. Daher ist $\mathbb{F}_p[t^{\frac{1}{p}}]$ der Ganzheitsring. Er ist frei als Modul mit Basis $1, t^{\frac{1}{p}}, t^{\frac{2}{p}}, \ldots, t^{\frac{p-1}{p}}$ □

**Korollar 3.6.** *Sei $K/\mathbb{F}_p(t)$ endlich. Dann ist $\mathcal{O}_K$ freier $\mathbb{F}_p[t]$-Modul vom Rang $[K : \mathbb{F}_p(t)]$.*

*Beweis:* Wie im Beweis von Korollar 2.20 genügt es zu zeigen, dass $\mathcal{O}_K$ endlich erzeugter Modul ist oder (da $\mathbb{F}_p[t]$ noethersch) dass $\mathcal{O}_K$ in einem endlich erzeugten Modul enthalten ist. Daher können wir ohne Einschränkung annehmen, dass $K/\mathbb{F}_p(t)$ normal ist.
Sei $G = \mathrm{Aut}(K/\mathbb{F}_p(t))$.
Wir betrachten $K' = K^G$. Die Erweiterung $K/K'$ ist galois mit Galoisgruppe $G$, insbesondere separabel (Hauptsatz der Galoistheorie). Die Erweiterung $K'/\mathbb{F}_p(t)$ ist normal mit trivialer Automorphismengruppe, also rein inseparabel (vergleiche Lang, Algebra V Prop. 6.11). Nach Korollar 3.5 ist $\mathcal{O}_{K'}$ endlich erzeugter $\mathbb{F}_p[t]$-Modul und damit noethersch. Nach Theorem 2.6 ist $\mathcal{O}_K$ endlich erzeugter $\mathcal{O}_{K'}$-Modul. Dann ist $\mathcal{O}_K$ auch ein endlich erzeugter $\mathbb{F}_p[t]$-Modul. □

Dies beendet den Beweis von Theorem 2.4: Alle Ganzheitsringe sind Dedekindringe. Wir haben aber noch mehr gezeigt.

**Korollar 3.7.** *Sei $L/K$ endliche Erweiterung globaler Körper. Dann ist $\mathcal{O}_L$ endlich erzeugter $\mathcal{O}_K$-Modul.*

**Bemerkung.** Die Argumente dieses Kapitel funktionieren für jeden perfekten Körper $k$ statt $\mathbb{F}_p$.
Nach dem Theorem von Krull-Akzuki (Neukirch, Alg. Number Theory, Prop. 12.8) ist der ganze Abschluss eines eindimensionalen noetherschen Integritätsbereichs in einer endlichen Erweiterung des Quotientenkörpers stets ein Dedekindring. Im allgemeinen ist er aber nicht endlich erzeugt als Modul. Ringe, über denen dies gut geht heißen *exzellent*. Im wesentlichen haben wir gerade gezeigt, dass $\mathbb{F}_p[t]$ exzellent ist.

### Stichworte kommutative Algebra

Separabilitätsgrad, inseparable Erweiterung

# Kapitel 4

# Ideale von Ganzheitsringen

**Definition 4.1.** *Sei $A$ ein Dedekindring mit Quotientenkörper $K$. Ein* gebrochenes *Ideal von $A$ ist ein $A$-Untermodul $I \subset K$, so dass es $d \in A \setminus \{0\}$ gibt mit $dI \subset A$, d.h. ein gemeinsamer Hauptnenner. Gebrochene Ideale ungleich* 0 *heißen auch* invertierbare Ideale.

**Bemerkung.**

- Ein Ideal $I \subset A$ ist ein gebrochenes Ideal (mit $d = 1$). Zur Unterscheidung nennen wir sie auch *ganze* Ideale.
- Die Menge der gebrochenen Ideale hat eine Addition und Multiplikation

$$I + I' = \{a + b \mid a \in I, b \in I'\} \subset K$$

$$I \cdot I' = \left\{ \sum_{i=1}^{n} a_i b_i \mid a_i \in I, b_i \in I' \right\} \subset K$$

  Wir werden zeigen, dass die invertierbaren Ideale eine abelsche Gruppe bezüglich der Multiplikation bilden, daher auch der Begriff.

**Lemma 4.2.** *Ein Untermodul $I \subset K$ ist ein gebrochenes Ideal genau dann, wenn er endlich erzeugt ist.*
*Ist $A = \mathcal{O}_K$ ein Zahlring (bzw. Ganzheitsring eines Funktionenkörpers), so ist $I$ freie abelsche Gruppe vom Rang $[K : \mathbb{Q}]$ (bwz. freier $\mathbb{F}_p[t]$-Modul vom Rang $[K : \mathbb{F}_p(t)]$).*

*Beweis:* Sei $I =< x_1, \ldots, x_n >_A$, $d$ der Hauptnenner der $x_i$, dann gilt $dI \subset A$. Ist umgekehrt $dI \subset A$, so ist $dI$ ein Ideal eines noetherschen Rings, also endlich erzeugt. Dann ist auch $I$ endlich erzeugt.
Sei nun $A = \mathcal{O}_K$ Zahlring. Als abelsche Gruppe ist $I$ isomorph zu $dI \subset \mathcal{O}_K$. Als endlich erzeugte Untergruppe einer freien abelschen Gruppe ist er frei vom Rang höchstens $[K : \mathbb{Q}]$. Sei $a \in I$. Wegen $\mathcal{O}_K a \subset I$ ist der Rang mindestens $[K : \mathbb{Q}]$. Ebenso argumentiert man im Funktionenkörperfall. □

**Theorem 4.3.** *Sei $A$ ein Dedekindring. Dann ist jedes maximale Ideal invertierbar bezüglich der Multiplikation von gebrochenen Idealen, d.h. zu $I$ existiert $I^{-1}$ mit $I \cdot I^{-1} = A$.*

**Bemerkung.** Wäre $A$ ein Hauptidealring, so wären alle gebrochenen Ideale von der Form $Ab$ mit $b \in Q(A)$. Das inverse Ideal wäre einfach $Ab^{-1}$.

**Lemma 4.4.** *Sei $A$ noetherscher Ring, $0 \neq I$ ein (ganzes) Ideal. Dann gibt es Primideale ungleich 0 mit $I \supset \mathfrak{p}_1 \dots \mathfrak{p}_n$.*

*Beweis:* Sei $\Phi$ die Menge der Ideale $I \neq 0$ von $A$, für die das Lemma nicht gilt, d.h. die kein Produkt von Primidealen enthalten. Angenommen, $\Phi \neq \emptyset$. Da $A$ noethersch ist, hat $\Phi$ ein maximales Element $I_0$. Das Ideal $I_0$ ist nicht prim, also gibt es $x, y \in A \setminus I_0$ mit $xy \in I_0$. Nach Voraussetzung

$$I_0 \subsetneq I_0 + (x), I_0 + (y) \Rightarrow I_0 + (x), I_0 + (y) \notin \Phi$$

Also gibt es Primideale $\mathfrak{p}_1, \dots, \mathfrak{p}_n, \mathfrak{q}_1, \dots, \mathfrak{q}_m$ ungleich null mit

$$\mathfrak{p}_1 \dots \mathfrak{p}_n \subset I_0 + (x), \mathfrak{q}_1 \dots \mathfrak{q}_m \subset I_0 + (y) \Rightarrow$$
$$\mathfrak{p}_1 \dots \mathfrak{p}_n \mathfrak{q}_1 \dots \mathfrak{q}_m \subset (I_0 + (x))(I_0 + (y)) = I_0$$

Dies ist ein Widerspruch. □

*Beweis des Theorems:* Sei $\mathfrak{m} \subset A$ maximal, $\mathfrak{m} \neq 0$. Sei

$$\mathfrak{m}' = \{x \in Q(A) \mid x\mathfrak{m} \subset A\}$$

Dies ist ein $A$-Untermodul von $Q(A)$. Für $0 \neq y \in \mathfrak{m}$ folgt $y\mathfrak{m}' \in A$, also ist dies ein gebrochenes Ideal. Schließlich gilt nach Definition $\mathfrak{m}\mathfrak{m}' \subset A$. Da $\mathfrak{m}$ ein Ideal ist, gilt $A \subset \mathfrak{m}'$. Es folgt

$$\mathfrak{m} = A\mathfrak{m} \subset \mathfrak{m}'\mathfrak{m} \subset A$$

Da $\mathfrak{m}$ maximal ist, gilt

$$\mathfrak{m}'\mathfrak{m} = \mathfrak{m} \text{ oder } \mathfrak{m}'\mathfrak{m} = A$$

**Behauptung.** $\mathfrak{m}'\mathfrak{m} = \mathfrak{m}$ *ist unmöglich.*

Angenommen, $\mathfrak{m} = \mathfrak{m}'\mathfrak{m}$. Sei $x \in \mathfrak{m}' \Rightarrow x\mathfrak{m} \subset \mathfrak{m}$. Iterativ folgt

$$x^2\mathfrak{m} = x(x\mathfrak{m}) \subset x(\mathfrak{m}) \subset \mathfrak{m} \Rightarrow \dots \Rightarrow x^n\mathfrak{m} \subset \mathfrak{m} \text{ für alle } n \geq 1$$

Sei $0 \neq d \in \mathfrak{m}$, also $x^n d \in A$ für alle $n$. Dann ist $A[x]$ ein gebrochenes Ideal (mit Hauptnenner $d$), also endlich erzeugter $A$-Modul. Also ist $x$ ganz über $A$. Dies bedeutet wiederum, dass $x \in A$, da $A$ ganz abgeschlossen ist. Also $\mathfrak{m}' \subset A$. Die Inklusion $A \subset \mathfrak{m}'$ war trivial, also haben wir $A = \mathfrak{m}'$ gezeigt. Insgesamt:

$$A = \{x \in Q(A) \mid x\mathfrak{m} \subset A\}$$

Sei nun $0 \neq a \in \mathfrak{m}$, also $(a) \neq 0$. Nach Lemma 4.4 gibt es Primideale ungleich null mit $\mathfrak{p}_1 \dots \mathfrak{p}_n \subset (a)$. Ohne Einschränkung sei $n$ minimal. Es folgt

$$\mathfrak{m} \supset (a) \supset \mathfrak{p}_1 \dots \mathfrak{p}_n$$

Angenommen, für alle $i$ ist $\mathfrak{p}_i$ ist nicht in $\mathfrak{m}$ enthalten, d.h. es gibt $x_i \in \mathfrak{p}_i \setminus \mathfrak{m}$. Dann gilt $x_1 \dots x_n \in \mathfrak{p}_1 \dots \mathfrak{p}_n \subset \mathfrak{m}$. Dies ist ein Widerspruch zu $\mathfrak{m}$ Primideal. Also gibt es ein $i$ mit $\mathfrak{p}_i \subset \mathfrak{m}$, z.B. $i = n$. Nach Definition ist $\mathfrak{p}_n \neq 0$. Da $A$ eindimensional ist, folgt $\mathfrak{p}_n = \mathfrak{m}$. Damit:

$$\mathfrak{m} \supset (a) \supset \mathfrak{m}I \text{ mit } I = \mathfrak{p}_1 \dots \mathfrak{p}_{n-1}$$

$I$ ist nicht in $(a)$ enthalten, da $n$ minimal gewählt war. Sei $b \in I \setminus (a)$. Wegen $\mathfrak{m}I \subset (a)$ folgt $\mathfrak{m}b \subset (a) = Aa$. Dies impliziert $\mathfrak{m}ba^{-1} \subset A$. Also nach Definition: $ba^{-1} \in \mathfrak{m}' = A \Leftrightarrow b \in (a)$. Dies ist ein Widerspruch zur Wahl des Elementes $b$. □

**Theorem 4.5.** *Sei $A$ ein Dedekindring,* Spm $A$ *die Menge der maximalen Idealevon $A$.*

*(i) Jedes invertierbare Ideal schreibt sich eindeutig als*

$$I = \prod_{\mathfrak{p} \in \operatorname{Spm} A} \mathfrak{p}^{v_\mathfrak{p}(I)}$$

*mit $v_\mathfrak{p}(I) \in \mathbb{Z}$ fast alle null.*

*(ii) Es gilt $v_\mathfrak{p}(I) \geq 0$ für alle $\mathfrak{p}$ genau dann, wenn $I$ ein ganzes Ideal ist.*

*(iii) Der Monoid der invertierbaren Ideale ist eine Gruppe.*

*Beweis:* Zur Existenz: Es gilt $dI \subset A$, $I = (dI)(d^{-1})$. Daher genügt es, die Produktzerlegung für ganze Ideale zu zeigen, so dass gleichzeitig (ii) gilt. Sei $\Phi$ die Menge der Ideale, die keine Primidealfaktorisierung hat. Angenommen, $\Phi \neq \emptyset$. Da $A$ noethersch ist, hat $\Phi$ ein maximales Element $I$. Es ist $I \neq A$, da $A = \prod_{\mathfrak{p} \in \operatorname{Spec} A} \mathfrak{p}^0$. Also ist $I \subset \mathfrak{p}$ für ein maximales Ideal $\mathfrak{p}$. Sei $\mathfrak{p}' = \mathfrak{p}^{-1}$ das Inverse als gebrochenes Ideal. Wir betrachten $I' = I\mathfrak{p}'$. Es folgt

$$I \subset \mathfrak{p} \Rightarrow I' = I\mathfrak{p}' \subset \mathfrak{p}\mathfrak{p}' = A$$

d.h. auch $I'$ ist ein ganzes Ideal. Wegen $A \subset \mathfrak{p}'$ gilt $I \subset I' = I\mathfrak{p}$.

**Behauptung.** $I \subsetneq I'$

Angenommen, die Ideale sind gleich. Sei $x \in \mathfrak{p}'$. Nach Annahme ist $xI \subset I$, also iterativ $x^n I \subset I$ für alle $n$. Ein Hauptnenner für $I$ ist auch ein Hauptnenner für $A[x]$, also ist dieser Modul endlich erzeugt und $x$ ganz über $A$. Damit ist $x \in A$. Wir haben $\mathfrak{p}' = A$ gezeigt, dies ist ein Widerspruch.

Nach Wahl von $I \in \Phi$ ist nun $I' \notin \Phi$. Es gilt

$$I' = \mathfrak{p}_1^{v_1} \dots \mathfrak{p}_n^{v_n} \Rightarrow I = \mathfrak{p}\mathfrak{p}'I = \mathfrak{p}\mathfrak{p}_1^{v_1} \dots \mathfrak{p}_n^{v_n}$$

Tatsächlich sind hierbei die Exponenten alle größer gleich 0.

Zur Eindeutigkeit: Sei $\prod \mathfrak{p}^{n_\mathfrak{p}} = \prod \mathfrak{p}^{m_\mathfrak{p}}$, also $\prod \mathfrak{p}^{n_\mathfrak{p} - m_\mathfrak{p}} = A$. Wir schreiben die Gleichung so um, dass alle Exponenten größer gleich Null und minimal sind. Wir erhalten also

$$\mathfrak{p}_1^{n_1} \dots \mathfrak{p}_k^{n_k} = \mathfrak{q}_1^{m_1} \dots \mathfrak{q}_l^{m_l}$$

mit $\mathfrak{p}_i \neq \mathfrak{q}_j$ für alle $i, j$ und $n_i, m_j > 0$. Es gilt $\mathfrak{p}_1 \supset \mathfrak{q}_1^{m_1} \dots \mathfrak{q}_l^{m_l}$. Also enthält $\mathfrak{p}_1$ eines der $\mathfrak{q}_j$ (wie im Beweis von Theorem 4.3). Da $A$ ein Dedekindring ist, folgt $\mathfrak{p}_1 = \mathfrak{q}_j$, Widerspruch.
Die Behauptung über die Gruppenstruktur ist nun klar. □

**Definition 4.6.** *Die* Idealklassengruppe *oder Klassengruppen des Dedekindrings $A$ ist*

$$\mathrm{Cl}(A) = \frac{\textit{Gruppe der invertierbaren Ideale}}{\textit{Hauptideale} \neq 0}$$

*Die* Klassenzahl *$h$ ist die Anzahl der Elemente von $\mathrm{Cl}(A)$. Ist $A = \mathcal{O}_K$ Ganzheitsring des globalen Körpers $K$, so heißt*

$$\mathrm{Cl}(K) := \mathrm{Cl}(\mathcal{O}_K)$$

Klassengruppe *von $K$.*

**Bemerkung.** $h = 1$ bedeutet, dass jedes Ideal ein Hauptideal ist. Die Klassenzahl misst also, wie weit $\mathcal{O}_K$ davon abweicht, ein Hauptidealring zu sein. Sie ist für Zahlkörper endlich (tief! später).

**Lemma 4.7.** *Die Klassengruppe ist isomorph zur Halbgruppe der echten Ideale ungleich 0 mit Äquivalenzrelation $I(g) \sim I(f)$ für $f, g \in A \setminus \{0\}$.*

*Beweis:* Sei $C'$ die im Lemma definierte Halbgruppe. Sie bildet sich in die Klassengruppe ab. Jedes gebrochene Ideal ist äquivalent zu einem echten Ideal, also ist die Abbildung surjektiv. Die Äquivalenzrelation ist offensichtlich die gleiche, also ist sie auch injektiv. □

Dieser Beschreibung sieht man die Existenz des Inversen nicht an! Man spart also keine Arbeit gegenüber unserem Ansatz.

## Beispiel

$K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O} = \mathbb{Z}[\sqrt{-5}]$. Es gilt $\mathcal{O} \cong \mathbb{Z}[X]/(X^2 + 5)$. Wir bestimmen die Primideale: Sei $\mathfrak{p} \subset \mathcal{O}$ prim, $(p) = \mathfrak{p} \cap \mathbb{Z}$ für $p \in \mathbb{Z}$ Primzahl.

(i) $p = 2$: Wir haben

$$\mathcal{O}/(2) = \mathbb{Z}[X]/(X^2 + 5, 2) = \mathbb{F}_2[X]/X^2 + 1 = \mathbb{F}_2[X]/(X + 1)^2$$

Also ist (2) selbst kein Primideal von $\mathcal{O}$. Es gibt genau ein Primideal, das 2 enthält. Modulo 2 wird es von $X + 1$ erzeugt, also $P_2 = (2, \sqrt{-5} + 1)$.

(ii) $p = 3$

$$\mathcal{O}/(3) = \mathbb{Z}[X]/(X^2+5,3) = \mathbb{F}_3[X]/(X^2-1) = \mathbb{F}_2[X]/(X+1)(X-1)$$
$$= \mathbb{F}_3[X]/(X-1) \times \mathbb{F}_3[X]/(X+1)$$

Es gibt zwei Primideale, die 3 enthalten, nämlich $P_3 = (3, \sqrt{-5}+1)$, $P_3' = (3, \sqrt{-5}-1)$. Es gilt $(3) = P_3 P_3'$ in $\mathcal{O}$. Wichtig für diese Berechnung war nur, dass $-5$ eine Quadratzahl modulo 3 war.

(iii) $p = 5$

$$\mathcal{O}/(5) = \mathbb{Z}[X]/(X^2+5,5) = \mathbb{F}_5[X]/X^2$$

$P_5 = (5, \sqrt{-5}) = (\sqrt{-5})$ ist das einzige Primideal, das 5 enthält. Es gilt $(5) = P_5^2$.

(iv) $p = 7$

$$\mathcal{O}/(7) = \mathbb{Z}[X]/(X^2+5,7) = \mathbb{F}_7[X]/(X^2-2) = \mathbb{F}_7[X]/(X+3)(X-3)$$
$$= \mathbb{F}_7[X]/(X-3) \times \mathbb{F}_7[X]/(X+3)$$

$P_7 = (7, \sqrt{-5} \pm 3)$ (wie Fall $p = 3$)

(v) $p = 11$ In diesem Fall ist 5 keine Quadratzahl modulo 11, das Ideal (11) ist prim in $\mathcal{O}$.

beim Rechnen modulo Hauptideale gilt also: $P_2^2 \sim 1$, $P_5 \sim 1$, $P_3 \sim (P_3')^{-1}$, $P_{11} \sim 1$ etc.
Frage: Ist $P_2$ ein Hauptideal? Falls $P_2 = (\alpha)$, so gibt es $x, y$ mit

$$x\alpha = 2 \Rightarrow N(x)N(\alpha) = N(2) = 4$$
$$y\alpha = \sqrt{-5}+1 \Rightarrow N(y)N(\alpha) = N(\sqrt{-5}+1) = 6$$

Dies impliziert $N(\alpha) = 2$. Sei $\alpha = a_1 + a_2\sqrt{-5}$ $(a_i \in \mathbb{Z})$

$$a_1^2 + 5a_2^2 = 2$$

Dies führt also auf die Theorie der Lösbarkeit der quadratischen Gleichungen in $\mathbb{Z}$. Die obige ist nicht lösbar, also ist $P_2$ kein Hauptideal.

Man sieht bereits in diesem Beispiel: die Bestimmung der Klassengruppe ist schwierig, da sie unendlich viele Erzeuger und unendlich viele Relationen hat!

Die Frage nach Primidealen in $\mathbb{Z}[\sqrt{d}]$ führt auf die Frage, ob $d$ eine Quadratzahl ist modulo $p$ oder nicht. Dies wird durch Gauß' quadratisches Reziprozitätsgesetz zufriedenstellend beantwortet.

## Folgerungen

**Satz 4.8.** *Sei $A$ ein Dedekindring. Seien $I = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(I)}$ und $J = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(J)}$ ganze Ideale von $A$. Dann gilt*

$$I \cap J = \prod_{\mathfrak{p}} \mathfrak{p}^{\max(v_{\mathfrak{p}}(I), v_{\mathfrak{p}}(J))}$$
$$I + J = \prod_{\mathfrak{p}} \mathfrak{p}^{\min(v_{\mathfrak{p}}(I), v_{\mathfrak{p}}(J))}$$

*Beweis:* Aus dem Struktursatz folgt, dass Enthaltenseinsrelationen sich in $\geq$-Relationen von die Exponenten $v_{\mathfrak{p}}$ übersetzen.
Wir betrachten $v_{\mathfrak{p}}(I \cap J)$. Wegen $I \cap J \subset I$ gilt $v_{\mathfrak{p}}(I \cap J) \geq v_{\mathfrak{p}}(I)$. Ebenso folgt $v_{\mathfrak{p}}(I \cap J) \geq v_{\mathfrak{p}}(J)$, also

$$I \cap J \subset \prod_{\mathfrak{p}} \mathfrak{p}^{\max(v_{\mathfrak{p}}(I), v_{\mathfrak{p}}(J))}$$

Die rechte Seite ist in $I$ und $J$ enthalten, also auch in $I \cap J$.
Die zweite Aussage wird analog gezeigt. □

**Satz 4.9.** *Sei $A$ ein Dedekindring und $I = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(I)}$ ein ganzes Ideal. Dann gilt*

$$A/I \cong \prod A/\mathfrak{p}^{v_{\mathfrak{p}}(I)}$$

*Beweis:* Man beachte, dass die Produkte endlich sind, da fast alle $v_{\mathfrak{p}}(I) = 0$, fast alle $A/\mathfrak{p}^{v_{\mathfrak{p}}(I)} = 0$.
Die Ideale $\mathfrak{p}^{v_{\mathfrak{p}}(I)}$ für verschiedene maximale Ideale $\mathfrak{p}$ sind paarweise teilerfremd, d.h. $\mathfrak{p}_1^{v_1} + \mathfrak{p}_2^{v_2} = \mathcal{O}_K$ nach Satz 4.8. Ihr Schnitt ist $I$ nach Satz 4.8. Die Aussage ist nun genau der Chinesische Restsatz. □

**Stichworte kommutative Algebra**

Chinesischer Restsatz

**Lemma 4.10.** *Sei $A$ ein Dedekindring, $\mathfrak{p}$ ein maximales Ideal. Sei $\mathbb{F} = A/\mathfrak{p}$ der Restklassenkörper. Dann ist $\mathfrak{p}^v/\mathfrak{p}^{v+1}$ ein $\mathbb{F}$-Vektorraum der Dimension 1.*

*Beweis:* Die $A$-Operation auf $\mathfrak{p}^v/\mathfrak{p}^{v+1}$ faktorisiert durch $A/\mathfrak{p}$, dies definiert die Vektorraumstruktur. Wegen $\mathfrak{p}^v \neq \mathfrak{p}^{v+1}$ ist die Dimension wenigstens 1.

**Behauptung.** *Es gibt $y \in \mathfrak{p}^v$, das $\mathfrak{p}^v/\mathfrak{p}^{v+1}$ erzeugt.*

Sei $x \in \mathfrak{p} \setminus \mathfrak{p}^2$, also $(x) \subset \mathfrak{p}$, aber nicht $(x) \subset \mathfrak{p}^2$. Dies bedeutet $v_{\mathfrak{p}}(x) = 1$ und daher $v_{\mathfrak{p}}(x^v) = v$. Weiter ist nach Satz 4.8 $(x^v) + \mathfrak{p}^{v+1} = \mathfrak{p}^v$. Also ist $x^v$ der gesuchte Erzeuger. □

**Definition 4.11.** *Sei $\mathcal{O}_K$ Ganzheitsring eines globalen Körpers, $I \subset \mathcal{O}_K$ ein ganzes Ideal ungleich Null. Dann heißt $N(I) = |\mathcal{O}_K/I|$* Idealnorm *von $I$.*

**Beispiel.** (i) Ist $\mathcal{O}_K = \mathbb{Z}$, so ist $I = (a)$ für $a \neq 0$. Es gilt also $N(I) = |\mathbb{Z}/(a)| = |a|$.

(ii) Ist $\mathcal{O}_K = \mathbb{F}_p[t]$, so ist $I = (F)$ für ein irreduzibles Polynom $F$. Es ist also $\mathbb{F}_p[t]/(F) = \mathbb{F}_p(\alpha)$ wobei $\alpha \in \overline{\mathbb{F}}_p$ Nullstelle von $F$ ist. Es folgt $|N(I)| = p^{[\mathbb{F}_p(\alpha):\mathbb{F}_p]}$.

(iii) Ist $I = \mathfrak{p}$, so ist $\mathcal{O}_K/\mathfrak{p}$ eine ganze Erweiterung eines Körpers der Form $\mathbb{F}_p = \mathbb{Z}/(p)$, also ein endlicher Körper mit $p^e$ Elementen.

(iv) Sei $K$ Zahlkörper. Nach dem *Elementarteilersatz* gibt es eine Basis $x_1, \ldots, x_n$ von $\mathcal{O}_K$ sowie ganze Zahlen $\lambda_1, \ldots, \lambda_n$ so dass $\lambda_1 x_1, \ldots, \lambda_n x_n$ eine Basis von $I$ ist. Dann gilt (als Gruppe)

$$\mathcal{O}_K/I \cong \mathbb{Z}/(\lambda_1) \times \mathbb{Z}/\lambda_2 \times \cdots \times \mathbb{Z}/(\lambda_n)$$

Es folgt $N(I) = |\lambda_1 \ldots \lambda_n|$. Insbesondere ist die Idealnorm endlich.

(v) In diesem Fall liegen die $\lambda_i$ in $\mathbb{F}_p[t]$, man erhält

$$\mathcal{O}_K/I \cong \mathbb{F}_p[t]/(\lambda_1) \times \cdots \times \mathbb{F}_p[t]/(\lambda_n)$$

Es folgt ebenfalls $N(I) = \prod |\mathbb{F}_p[t]/(\lambda_i)| < \infty$

**Lemma 4.12.** *Sei $I = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(I)}$. Dann gilt*

$$N(I) = \prod N(\mathfrak{p})^{v_{\mathfrak{p}}(I)}$$

*Die Idealnorm ist multiplikativ.*

*Beweis:* Wegen des chinesischen Restsatzes genügt es, Ideale der Form $\mathfrak{p}^v$ zu betrachten. Für $v = 1$ gilt die Aussage. Wir schließen von $v$ auf $v + 1$. Die Abbildung

$$\mathcal{O}_K/\mathfrak{p}^{v+1} \to \mathcal{O}_K/\mathfrak{p}^v$$

ist surjektiv mit Kern $\mathfrak{p}^v/\mathfrak{p}^{v+1}$. Nach Lemma 4.10 ist dies ein $\mathcal{O}_K/\mathfrak{p}$-Vektorraum der Dimension 1, hat also $N(\mathfrak{p})$-viele Elemente. Es gilt also $N(\mathfrak{p}^{v+1}) = N(\mathfrak{p}^v)N(\mathfrak{p})$. □

**Lemma 4.13.** *(i) Sei $K$ Zahlkörper. Sei $I = (x)$. Dann gilt $N(I) = |N_{K/\mathbb{Q}}(x)|$.*

*(ii) Sei $K$ Funktionenkörper. Dann gilt $N(I) = N(N_{K/\mathbb{F}_p(t)}(x))$.*

Die Formeln sind völlig analog, da ja $|y| = N((y))$ für $y \in \mathbb{Z}$.

*Beweis:* Wir beginnen im Zahlkörperfall. Nach dem Elementarteilersatz gibt es eine $\mathbb{Z}$-Basis $x_1, \ldots, x_n$ von $\mathcal{O}_K$ und ganze Zahlen $\lambda_1, \ldots, \lambda_n$, so dass $\lambda_1 x_1, \ldots, \lambda_n x_n$ eine Basis von $I$ ist. Andererseits ist $xx_1, \ldots, xx_n$ ebenfalls eine Basis von $I$. Sei $u : K \to K$ durch $x_i \mapsto \lambda_i x_i$ gegeben. Sei $v : K \to K$ durch $x_i \mapsto x/\lambda_i x_i$ gegeben. Dann gilt $v \circ u = m_x$, also

$$N_{K/\mathbb{Q}}(x) = \det(v)\det(u) = \pm N(I)$$

denn $v$ ist eine Basiswechselmatrix auf $I$.
Dasselbe Argument ergibt im Funktionenkörperfall

$$\lambda_1 \dots \lambda_n \det(v) = N_{K/\mathbb{F}_p(t)}(x)$$

wobei $\det(v) \in \mathbb{F}_p[t]^*$. Daher erzeugen $\lambda_1 \dots \lambda_n$ und $N_{K/\mathbb{F}_p(t)}(x)$ dasselbe Ideal von $\mathbb{F}_p[t]$. Es folgt

$$N(N_{K/\mathbb{F}_p(t)}(x)) = N(\lambda_1 \dots \lambda_n) = N(I)$$

□

# Kapitel 5

# Verzweigung

Sei $L/K$ eine Erweiterung von globalen Körpern, $\mathfrak{P} \subset \mathcal{O}_L$ ein maximales Ideal. Dann ist $\mathfrak{p} = \mathcal{O}_K \cap \mathfrak{P}$ nach Satz 1.20 (genauer dessen Beweis) ebenfalls ein maximales Ideal.
Ist umgekehrt $\mathfrak{p} \subset \mathcal{O}_K$ ein Primideal und $\mathcal{O}_L\mathfrak{p}$ das von $\mathfrak{p}$ erzeugte Ideal von $\mathcal{O}_L$. Nach Theorem 4.5 gilt

$$\mathcal{O}_L\mathfrak{p} = \prod_{i=1}^{k} \mathfrak{P}_i^{e_i}$$

wobei die $\mathfrak{P}_i$ Primideale von $\mathcal{O}_L$ sind. Offensichtlich

$$\mathfrak{p} \subset \mathcal{O}_K\mathfrak{p} \subset \mathfrak{P}_i$$

**Definition 5.1.** *$\mathfrak{P}_i$ heißt* Primideal von $L$ über $\mathfrak{p}$. *Wir sagen auch, $\mathfrak{P}_i|\mathfrak{p}$ ( $\mathfrak{P}_i$ teilt $\mathfrak{p}$). Der Exponent $e_i = e(\mathfrak{P}_i/\mathfrak{p})$ heißt* Verzweigungsgrad von $L/K$ in $\mathfrak{P}_i$. *Die Erweiterung $L/K$ heißt* unverzweigt, *wenn $e(\mathfrak{P}/\mathfrak{p}) = 1$ für alle Primideale $\mathfrak{p}$ von $K$ und alle $\mathfrak{P}|\mathfrak{p}$. Der Körper $\kappa(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$ heißt* Restklassenkörper *von $K$ in $\mathfrak{p}$. Die Zahl $f(\mathfrak{P}_i/\mathfrak{p}) = [\kappa(\mathfrak{P}_i) : \kappa(\mathfrak{p})]$ heißt* Restklassengrad *von $L/K$ in $\mathfrak{P}_i$.*

Wir schreiben also

$$\mathcal{O}_L\mathfrak{p} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})}$$

**Theorem 5.2** (Gradformel)**.** $[L : K] = \sum_{\mathfrak{P}|\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) f(\mathfrak{P}/\mathfrak{p})$.

Im ersten Anlauf beweisen wir ein spezielleres Ergebnis:

**Satz 5.3.** *Sei $A$ ein Hauptidealring mit Quotientenkörper $K$, sei $L/K$ endliche Erweiterung und $B$ der ganze Abschluss von $A$ in $B$. Wir setzen voraus, dass $B$ endlich erzeugter $A$-Modul ist. Dann gilt die Gradformel für alle Primideale.*

Dieser Satz erledigt z.B. $K = \mathbb{Q}, \mathbb{Q}(i)$, $K = \mathbb{F}_p(t)$, aber nicht den allgemeinen Fall.

*Beweis:* Sei $d = [L : K]$. Wie wir uns bereit mehrfach überlegt haben, ist $B$ unter unseren Voraussetzungen freier $A$-Modul vom Rang $d$. Wir fixieren ein Primideal $\mathfrak{p}$ von $A$ mit Restklassenkörper $\kappa = \kappa(\mathfrak{p})$. Dann ist

$$B/\mathfrak{p}B \cong B \otimes_A \kappa \cong A^d \otimes_A \kappa \cong \kappa^d$$

und daher

$$d = \mathrm{rg}_A B = dim_\kappa \mathcal{O}_L/\mathcal{O}_K\mathfrak{p}$$

(Ohne Tensorprodukt formululiert:

$$\mathfrak{p}B = \{\sum_i p_i b_i | p_i \in \mathfrak{p}, b_i \in B\} \cong \mathfrak{p}A^d = \left\{\sum_i p_i(a_i^1, \ldots, a_i^d) | p_i \in \mathfrak{p}, a_i^j \in A\right\}$$

Man überlegt sich leicht, dass

$$\mathfrak{p}A^d = \mathfrak{p} \times \mathfrak{p} \cdots \times \mathfrak{p}$$

Daher ist

$$B/\mathfrak{p}B \cong A^d/\mathfrak{p}^{\oplus d} \cong (A/\mathfrak{p})^d = \kappa^d$$

Auch so liest man die $\kappa$-Dimension $d$ ab.)
Andererseits ist

$$B/\mathfrak{p}B = B/\prod_{i=1}^k \mathfrak{P}_i^{e_i}$$

Wir berechnen diese Dimension nun analog zum Beweis für die Multipliplikativität der Idealnorm (Lemma 4.12).

**Behauptung.**

$$\dim_\kappa B/\prod_{i=1}^k \mathfrak{P}_i^{e_i'} = \sum_{i=1}^k e_i' \dim_\kappa B/\mathfrak{P}$$

für $0 \leq e_i' \leq e_i$. Es handelt sich stets um Quotienten von $B/\mathfrak{p}B$, also um $\kappa$-Vektorräume. Wir argumentieren induktiv über $e = \sum_{i=1}^k e_i'$. Für $e = 1$ ist nichts zu zeigen. Wir betrachten $e > 1$. Dann gibt es einen Index $i$ mit $e_i' > 1$. Ohne Einschränkung ist dies $i = 1$. Wir betrachten die Surjektion

$$B/\prod_{i=1}^k \mathfrak{P}_i^{e_i'} \to B/\mathfrak{P}_1^{e_1'-1} \prod_{i=2}^k \mathfrak{P}_i^{e_i'}$$

Sie hat Kern isomorph zu $\mathfrak{P}_1^{e_1-1}/\mathfrak{P}_1^{e_1}$. Nach Lemma 4.10 ist dies ein $B/\mathfrak{P}$-Vektorraum der Dimension 1, also ein $\kappa$- Vektorraum der Dimension $\dim_\kappa B/\mathfrak{P}$. Aus der Dimensionsformel für $\kappa$-Vektorräume folgt die Behauptung. □

**Stichworte kommutative Algebra**

Tensorprodukt

**Geometrische Interpretation**

**Beispiel.** Sei $k$ ein algebraisch abgeschlossener Körper. Dann sind die maximalen Ideale von $k[t]$ von der Form $X - a$ für $a \in k$. Wir erhalten eine Bijektion

$$\mathbb{A}^1(k) = k \to \operatorname{Spm} k[t]$$

Sei $K = k(t)$ der Quotientenkörper. Dies ist der Funktionenkörper von $\mathbb{A}^1$ (vergleiche Definition 0.6). Wir betrachten die Erweiterung $L/K$ der Form $L = K(\sqrt{t}) = K[X]/(X^2 - t)$. Wir bestimmen den ganzen Abschluss von $k[t]$ in $L$. Wir setzen voraus, dass die Charakteristik des Körpers ungleich 2 ist und damit die Erweiterung separabel. Ein Element

$$\alpha = f + g\sqrt{t}$$

ist genau dann ganz, wenn sein charakteristisches Polynom ganz ist, also Spur und Norm ganz. Es gilt also

$$\operatorname{Tr}(\alpha) = 2f, N(\alpha) = f^2 - g^2 t \in k[t]$$

Nach Voraussetzung ist 2 invertierbar in $k$, also folgt $f \in k[t]$. Das Element $g$ hat eindeutig die Form

$$c \prod_i (t - a_i)^{e_i} \qquad c, a_1, \ldots, a_i \in k, e_i \in \mathbb{Z}$$

Also

$$g^2 t = ct \prod_i (t - a_i)^{2e_i} \in k[t]$$

Hieraus folgt $e_i \geq 0$ (auch für $a_i = 0$!). Also ist $g$ ganz. Wir haben gezeigt:

$$\mathcal{O}_L = \{f + g\sqrt{t} | f, g \in k[t]\} \cong k[t, X]/(X^2 - t)$$

Nun bestimmen wir das Maximalspectrum von $\mathcal{O}_L$. Sei $\mathfrak{P}$ maximales Ideal. Dann ist $\mathfrak{p} = k[t] \cap \mathfrak{P}$ von der Form $(X - a)$ für ein $a \in k$. Wir wollen die Primidealfaktorisierung von $\mathfrak{p}\mathcal{O}_L = (t - a)\mathcal{O}_L$ bestimmen. Hierzu reduzieren wir modulo $t - a$, setzen also $a$ für $t$ ein.

$$\mathcal{O}_L/(t - a) \cong k[X]/(X^2 - a)$$

Da $k$ algebraisch abgeschlossen ist, erhalten wir $X^2 - a = (X - \sqrt{a})(X + \sqrt{a})$.

$$\mathfrak{P} = (t - a, X - \sqrt{a}), \mathfrak{P}' = (t - a, X + \sqrt{a}) | (t - a)$$

Wir erhalten also eine Bijektion

$$V(X^2 - t)(k) = \{(a, \sqrt{a}) \in k^2 | a \in k\} \to \operatorname{Spm} \mathcal{O}_L$$

Die Projektion

$$V(X^2 - t) \to \mathbb{A}^1 \qquad (a, \sqrt{a}) \mapsto a$$

entspricht auf Spektren $\mathfrak{P} \mapsto k[t] \cap \mathfrak{P}$. Jeder Punkt $a \neq 0$ hat genau zwei Urbilder (entsprechend $\mathfrak{P}$, $\mathfrak{P}'$). Dies sind die Punkt, in denen die Erweiterung unverzweigt ist. Aus der Gradformel oder durch direkte Rechnung erhalten wir auch

$$(t-a) = \mathfrak{P}\mathfrak{P}'$$

In $a = 0$ gibt es ein "doppeltes" Urbild entsprechend der Zerlegung

$$(t) = \mathfrak{P}^2$$

Dieser Punkt ist verzweigt.
Nun betrachten wir dieselbe Erweiterung, aber in Charakteristik 2. Alle Argumente funktionieren genauso - nur dass jetzt für jedes $a$ gilt $\sqrt{a} = -\sqrt{a}$, also auch $\mathfrak{P} = \mathfrak{P}'$. Die Erweiterung ist in allen Punkten rein verzweigt.

Allgemeiner:

**Satz 5.4.** *Sei $k$ algebraisch abgeschlossener Körper, $L/k[t]$ eine endliche Erweiterung, $\mathcal{O}_L$ der ganze Abschluss von $k[t]$ in $L$. Dann gibt es $n \in \mathbb{N}$, Polynome $F_1, \ldots, F_m \in k[t, X_1, \ldots, X_n]$ und eine Bijektion*

$$\operatorname{Spm} \mathcal{O}_L \to V(F_1, \ldots, F_m)(k)$$

*Hierbei entsprechen die Teiler von $(t-a)$ für $a \in k$ den Punkten in $V(t-a, F_1, \ldots, V_m)$, also der Faser über $a$. Jede dieser Fasern enthält mit Vielfachheit gezählt genau $d = [L : k(t)]$ viele Punkte. Eine Faser ist unverzweigt, wenn $a$ genau $d$ verschiedene Urbilder hat.*

In dieser Situation heißt $C = \operatorname{Spm} \mathcal{O}_L$ *glatte affine Kurve.*

*Beweisskizze:* $\mathcal{O}_L$ ist ein endlich erzeugter $k[t]$-Modul, also von der Form $\mathcal{O}_L = k[t][\alpha_1, \ldots, \alpha_n]$ für gewisse Erzeuger (Ringerzeuger reichen). Dies induziert einen surjektiven Ringhomomorphismus

$$k[t, X_1, \ldots, X_n] \to \mathcal{O}_L \qquad X_i \mapsto \alpha_i$$

Sei $I$ der Kern. Nach Hilbertschem Basissatz ist $k[t, X_1, \ldots, X_n]$ noethersch, also $I$ endlich erzeugt. Seien $F_1, \ldots, F_m$ die Erzeuger. Jeder Punkt $(a, a_1, \ldots, a_n) \in k^{n+1}$, der die Gleichungen $F_1, \ldots, F_m$ erfüllt, definiert ein maximales Ideal $(t-a, X_1 - a_1, \ldots, X - a_n)$ von $k[t, X_1, \ldots, X_n]/I = \mathcal{O}_L$. Nach dem Hilbertschen Nullstellensatz ist die Zuordnung bijektiv.
Die Aussagen über die Anzahl der Urbilder sind nun eine Umformulierung der Gradformel. □

In der fortgeschrittenen Sprache der algebraischen Geometrie (Schemata) funktioniert diese Interpretation auch über nicht algebraisch abgeschlossenem Grundkörper und sogar für Zahlringe.
Im Spezialfall $k = \mathbb{C}$ haben die Objekte auch eine Interpretation als eindimensionale komplexe Mannigfaltigkeiten, also als Riemannsche Flächen.

**Beispiel.** Wir betrachten

$$\phi : \mathbb{C} \to \mathbb{C} \qquad z \mapsto z^n$$

Jeder Punkt hat $n$ verschiedene Urbilder indiziert durch die $n$-ten Einheitswurzeln $\mu_n = \{1, \zeta_n, \ldots, \zeta_n^n\}$, mit Ausnahme des Verzweigungspunktes 0. Mehrnoch: für $z \neq 0$ gibt es eine kleine offene Umgebung $U$, so dass

$$\phi^{-1}(U) \cong U \times \mu_n$$

$\phi$ ist genau dort unverzweigt, wo die Abbildung ein lokaler Isomorphismus ist.

### Lokalisierung

Nachdem wir ein geometrisches Bild haben, wollen wir nun eine geometrische Idee nutzen - den Übergang zu offenen Umgebungen eines Punktes. Zu jeder Funktion $f$, die in $P$ nicht verschwindet gibt es die offene Menge

$$U_f = \{Q | f(Q) \neq 0\}$$

Auf dieser Menge wird $f$ invertierbar.

**Definition 5.5.** *Sei $A$ ein Integritätsbereich mit Quotientenkörper $K$, $S \subset A$ eine multiplikativ abgeschlossene Teilmenge, $0 \notin S$. Dann heißt*

$$S^{-1}A = \left\{ \frac{a}{s} \in K \mid a \in A, s \in S \right\}$$

Lokalisierung von $A$ in $S$.
*Für $f \in A \setminus \{0\}$ und $S = \{1, f, f^2, \ldots, \}$ heißt*

$$A_f = S^{-1}A$$

Lokalisierung von $A$ an $f$.
*Für jedes Primideal $\mathfrak{p} \subset A$ und $S = A \setminus \mathfrak{p}$ heißt*

$$A_{\mathfrak{p}} = S^{-1}A$$

Lokalisierung von $A$ in $\mathfrak{p}$ *oder* lokaler Ring von $A$ in $\mathfrak{p}$.

**Bemerkung.** (i) Die Lokalisierung $S^{-1}A$ ist ein Teilring von $K$.

(ii) $\mathfrak{p} \subset A$ Primideal ist gerade äquivalent zu $A \setminus \mathfrak{p}$ multiplikativ abgeschlossen.

(iii) Speziell für $\mathfrak{p} = 0$ ist $A_{\mathfrak{p}} = K$.

**Stichworte kommutative Algebra**

Lokalisierung, allgemeiner Fall

**Satz 5.6.** *Sei $A$ ein Dedekindring, $K = Q(A)$, $\mathfrak{p} \subset A$ ein Primideal. Dann ist $A_\mathfrak{p}$ ein Hauptidealring mit einem einzigen Primideal, nämlich $\mathfrak{P} = S^{-1}\mathfrak{p}$. Es gilt $A/\mathfrak{p} = A_\mathfrak{p}/\mathfrak{P}$.*

**Definition 5.7.** *Ein Hauptidealring mit nur einem Primideal heißt* diskreter Bewertungsring.

*Beweis:* $A_\mathfrak{p}$ ist ebenfalls ein Dedekindring, wie man leicht sieht.

(i) (Integritätsring) trivial wegen $A_\mathfrak{p} \subset K$.

(ii) (ganz abgeschlossen) $x \in Q(A_\mathfrak{p}) = Q(A) = K$, ganz über $\mathfrak{p}$. Dann genügt es einer Gleichung

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

mit $a_i \in A$, $s_i \in S$. Sei $s = s_1 \dots s_n$. Dann ist $sx$ ganz über $A$, also $sx \in A$, da $A$ ganz abgeschlossen ist. Es folgt $x = sx/s \in A_\mathfrak{p}$.

(iii) (noethersch) Sei $I \subset A_\mathfrak{p}$ ein Ideal, $I' = A \cap I$. Als Ideal von $A$ ist $I'$ endlich erzeugt.

**Behauptung.** $S^{-1}I' = I$.

Die Inklusion $\subset$ ist klar. Sei umgekehrt $x = a/s \in I$. Dann liegt $a = sx \in A \cap I$, und daher $x = \frac{sa}{x} \in S^{-1}I$.

(iv) (Dimension 1) Sei nun $I \subset A_\mathfrak{p}$ prim, also $I' = A \cap I$ ein Primideal von $A$. Dann ist $I'$ entweder 0 oder maximal. Hieraus folgt, dass auch $S^{-1}I'$ entweder 0 ist oder maximal.

Wir bestimmen nun die Menge Primideale von $A_\mathfrak{p}$:

$$\operatorname{Spec} A_\mathfrak{p} = \{S^{-1}\mathfrak{q} \mid \mathfrak{q} \subset A \text{ prim }, S^{-1}\mathfrak{q} \neq S^{-1}A\}$$

Sei nun $\mathfrak{q} \neq \mathfrak{p}$ ein maximales Ideal, d.h. $\mathfrak{q} \setminus \mathfrak{p} \neq \emptyset$. Sei $s \in \mathfrak{q} \setminus \mathfrak{p} \subset S$. Dann gilt

$$1 = s/s = 1/s \cdot s/1 \in S^{-1}\mathfrak{q} \Rightarrow S^{-1}\mathfrak{q} = A_\mathfrak{p}$$

Also ist $A_\mathfrak{p}$ lokal mit maximalem Ideal $\mathfrak{P} = S^{-1}\mathfrak{p}$. Nach Theorem 4.5 hat jedes Ideal von $A_\mathfrak{p}$ die Form $\mathfrak{P}^n$ mit $n \in \mathbb{N}_0$. Sei $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$, d.h.

$$\mathfrak{P} \supset (\pi) \supset \mathfrak{P}^2$$

Wegen $(\pi) \neq \mathfrak{P}^2$ folgt $\mathfrak{P} = (\pi)$, denn andere Ideale gibt es nicht. Damit ist $A_\mathfrak{p}$ ein Hauptidealring. Schließlich betrachten wir $A/\mathfrak{p} \to A_\mathfrak{p}/\mathfrak{P}$. Dies ist ein wohldefinierter Körperhomomorphismus. Sei $a/s \in A_\mathfrak{p}$. Wegen $s \in A \setminus \mathfrak{p}$ gilt $\overline{s} \neq 0$ in $A/\mathfrak{p}$. Dann ist $\overline{s}^{-1}a$ ein Urbild von $a/s$. Die Abbildung ist surjektiv, also bijektiv. □

*Beweis von Satz 5.2.* Sei $\mathfrak{p} \subset \mathcal{O}_K$ ein Primideal, $L/K$ eine Erweiterung und

$$\mathcal{O}_L\mathfrak{p} = \prod \mathfrak{P}_i^{e_i}$$

Sei $S = \mathcal{O}_K \setminus \mathfrak{p}$, $\mathcal{O}_{K,\mathfrak{p}} = S^{-1}\mathcal{O}_K \to S^{-1}\mathcal{O}_L$ ist eine Erweiterung von Dedekindringen. Wegen $S^{-1}(II') = (S^{-1}I)(S^{-1}I')$ folgt

$$S^{-1}\mathcal{O}_L\mathfrak{p} = \prod (S^{-1}\mathfrak{P}_i)^{e_i}$$

Der Verzweigungsgrad kann also auch nach Lokalisieren an $S$ berechnet werden, ebenso wie die lokalen Körpergrade $f_i$. Die Aussage folgt nun aus Satz 5.3. □

## Diskriminante

Wir erinnern: Sei $A$ ein Hauptidealring, $A \to B$ eine Ringerweiterung mit $B \cong A^n$, Basis $x_1, \ldots, x_n$.

$$d_{B/A} = (\det(\mathrm{Tr}(x_i x_j)_{i,j}))$$

Speziell für $A = \mathbb{Z}$, $B = \mathcal{O}_K$ heißt der positive Erzeuger von $d_{B/A}$ absolute Diskriminante von $K$.

**Satz 5.8.** *Sei $K$ ein Zahlkörper. Dann ist eine Primzahl $p \in \mathbb{Z}$ unverzweigt in $K/\mathbb{Q}$, genau dann wenn $p \nmid d$.*

*Beweis:* $\mathcal{O}_K \cong \mathbb{Z}^n$ mit $n = [K : \mathbb{Q}]$. Sei $p$ Primzahl, $(p) = \prod \mathfrak{P}_i^{e_i}$. Die Erweiterung ist unverweigt über $p$, wenn $\mathcal{O}_K/(p) = \prod \mathcal{O}_K/\mathfrak{P}^{e_i}$ (chinesischer Restsatz) ein Produkt von Körpern ist. Sei $x_1, \ldots, x_n$ eine Basis von $\mathcal{O}_K$ als $\mathbb{Z}$-Modul. Dann ist $\overline{x_1}, \ldots, \overline{x_n}$ eine Basis von $\mathcal{O}_K/(p)$ als $\mathbb{Z}/(p) = \mathbb{F}_p$-Vektorraum. Nach Definition ist $d = \det(\mathrm{Tr}(x_i x_j))$, also ist $\overline{d} = \det(\mathrm{Tr}(\overline{x}_i \overline{x}_j))$ die Diskriminante von $\mathbb{F}_p \to \mathcal{O}_K/(p)$. Die Bedingung $p \nmid d$ ist äquivalent zu $\overline{d} \neq 0$. Zu zeigen ist also:

**Behauptung.** *$\mathbb{F}_p \to B = \mathcal{O}_K/(p)$ eine Ringerweiterung. Dann ist $d_{B/\mathbb{F}_p} \neq 0$ genau dann, wenn $B$ ein Produkt von Körpern ist.*

Sei zunächst $B = \prod k_i$ wobei $k_i$ endliche Körpererweiterungen von $\mathbb{F}_p$ sind. Es gilt $d_{B/\mathbb{F}_p} = \prod d_{k_i/\mathbb{F}_p}$ (rechne in Basen der $k_i$). Nach Satz 2.18 ist $d_{k_i/\mathbb{F}_p} \neq 0$.
Sei umgekehrt $B = \prod \mathcal{O}_K/\mathfrak{P}_i^{e_i}$ kein Produkt von Körpern. Dann enthält $B$ ein nilpotentes Element $x \neq 0$. Ergänze $x = x_1$ zu einer Basis $x_1, \ldots, x_n$ von $B$. Die Produkte $x_1 x_i$ sind nilpotent, also ist Multiplikation mit $x_1 x_i$ eine nilpotente Abbildung. Daher sind alle Eigenwerte 0 und $\mathrm{Tr}(x_1 x_j) = 0$. Dann verschwindet auch die Diskriminante. □

**Korollar 5.9.** *Sei $L/K$ Erweiterung von Zahlkörpern. Dann sind nur endlich viele Primideale verzweigt.*

*Beweis:* $\mathbb{Z} \subset \mathcal{O}_K \subset \mathcal{O}_L$. Sei $\mathfrak{p} \subset \mathcal{O}_K$ ein Primideal, das in $L/K$ verzweigt, d.h. $\mathcal{O}_L\mathfrak{p} = \prod \mathfrak{P}_i^{e_i}$ mit einem $e_i > 1$. Sei $(p) = \mathfrak{p} \cap \mathbb{Z}$. Es folgt

$$e(\mathfrak{P}_i/(p)) = e_i e(\mathfrak{p}/(p))$$

Also genügt es, $K = \mathbb{Q}$ zu betrachten. Dann sind die verzweigten Primideale die Teiler von $d$, also gibt es nur endlich viele. □

Im Funktionkörperfall ist es komplizierter.

**Satz 5.10.** *Sei $L/K$ Erweiterung von Funktionenkörpern. Ist $L/K$ separabel, so sind nur endlich viele Primideal verzweigt. Anderfalls sind alle Primideale verzweigt.*

*Beweis:* Sei zunächst $L/K$ separabel. Wir wählen ein Primideal $\mathfrak{p}$ von $\mathcal{O}_K$. Wir haben gezeigt, dass es einen Isomorphismus

$$\phi_{\mathfrak{p}} : (\mathcal{O}_K)_{\mathfrak{p}}^d \to (\mathcal{O}_L)_{\mathfrak{p}}$$

gibt. Er ist gegeben durch die Bilder der Einheitsbasis $\alpha_i = \phi_{\mathfrak{p}}(e_i)$. Es gilt $\alpha_i = \frac{a_i}{s_i}$ mit $a_i \in \mathcal{O}_L$ und $s_i \in \mathcal{O}_K \setminus \mathfrak{p}$. Sei $s = s_1 s_2 \dots s_d$. Nach Definition ist dann $\alpha_i \in (\mathcal{O}_L)_s$. Wir erhalten eine Homorphismus von $(\mathcal{O}_K)_s$-Moduln

$$\phi_s : (\mathcal{O}_K)_s \to (\mathcal{O}_L)_s$$

Dieser ist injektiv, da aus $\phi_{\mathfrak{p}}$ als Einschränkung entsteht. Sei $M$ der Kokern von $\phi_s$. $M$ ist endliche erzeugt, da $\mathcal{O}_L$ endlich erzeugter $\mathcal{O}_K$-Modul. Nach Voraussetzung gilt $M_{\mathfrak{p}} = 0$. Daher gibt es $t \in \mathcal{O}_K$ mit $tM = 0$. Wir gehen über zu $st$ und erhalten eine bijektiven Homorphismus

$$\phi_{st} : (\mathcal{O}_K)_{st} \to (\mathcal{O}_L)_{st}$$

Da nun $(\mathcal{O}_L)_{st}$ frei ist, haben wir die Diskriminante definiert und wie im Zahlkörperfall sind die Teiler der Diskriminaten genau die verzweigte Primideale. (Hinzu kommen eventuell die endlich vielen Teiler von $st$).
Sei nun $L/K$ inseparabel. Wegen der Multiplikativität des Verzweigungsindexes genügt es, den rein inseperablen Fall und dort speziell $K = L^p$ zu betrachten. Der Frobeniushomomorphismus ist ein Isomorphismus $L \to K$ und daher auch $\mathcal{O}_L \to \mathcal{O}_K$ und induziert eine Bijektion zwischen den maximalen Idealen von $L$ und denen von $K$. Sei $\mathfrak{P} \subset \mathcal{O}_L$ ein Primideal, $\mathfrak{p} = \mathrm{Fr}(\mathfrak{P})$. Sei $\mathfrak{P}'$ ein Primteiler von $\mathfrak{p}\mathcal{O}_L$. Jedes Element $y \in \mathfrak{p}$ hat die Form $x^p$ für ein $x \in \mathcal{O}_L$. Da $\mathfrak{P}'$ ein Primideal ist, folgt $x \in \mathfrak{P}'$. Also ist $\mathfrak{P} \subset \mathfrak{P}'$. Da $\mathcal{O}_L$ ein Dedekindring ist, folgt $\mathfrak{P} = \mathfrak{P}'$. Frobenius induziert ebenfalls einen Isomorphismus $\kappa(\mathfrak{P}) \to \kappa(\mathfrak{p})$. Da die Körper endlich sind, ist dann die Erweiterung $k(\mathfrak{P})/\kappa(\mathfrak{p})$ trivial. Der Restklassengrad ist daher 1. Aus der Gradformel folgt $e(\mathfrak{P}/\mathfrak{p}) = p$. □

Für allgemeine $L/K$ ist $\mathcal{O}_L$ kein freier $\mathcal{O}_K$-Modul, daher ist die Diskriminante bisher nicht definiert worden.

**Definition 5.11.** *Sei $L/K$ separable Erweiterung von globalen Körper. Dann ist ist das* Diskriminantenideal *definiert als*

$$\mathcal{D}_{L/K} = \prod \mathfrak{p}^{v(\mathfrak{p})} \subset \mathcal{O}_K$$

*mit $d_{\mathcal{O}_{L,\mathfrak{p}}/\mathcal{O}_{K,\mathfrak{p}}} = \mathfrak{p}_{\mathfrak{p}}^{v(\mathfrak{p})} \subset \mathcal{O}_{K,\mathfrak{p}}$. Ist $L/K$ inseparabel, so setzen wir $\mathcal{D}_{L/K} = 0$.*

**Bemerkung.** Da $\mathcal{O}_{K,\mathfrak{p}}$ ein Hauptidealring ist, ist die Diskriminante von $\mathcal{O}_{L,\mathfrak{p}}/\mathcal{O}_{K,\mathfrak{p}}$ definiert. Da fast alle Primideale unverzweigt sind, ist $v(\mathfrak{p}) = 0$ fast immer.

**Korollar 5.12.** *$L/K$ unverzweigt in $\mathfrak{p}$ genau dann, wenn $\mathcal{D}_{L/K} \nmid \mathfrak{p}$.*

*Beweis:* Verzweigung ist eine lokale Eigenschaft, ebenso die Teilbarkeit von Idealen. Wir lokalisieren also in $\mathfrak{p}$. Danach ist der Beweis der Gleiche wie in 5.8 mit $\mathcal{O}_{K,\mathfrak{p}}$ statt $\mathbb{Z}$. □

## Beispiele

Sei $K/\mathbb{Q}$ quadratisch, $(p) = \prod_{i=1}^{g} \mathfrak{p}_i$ Dann gibt es in $2 = \sum_{i=1}^{g} e_i f_i$ nur drei Möglichkeiten:

$$\begin{cases} g = 1, e = 2, f = 1 & p \text{ ist } \textit{rein verzweigt} \\ g = 2, e = 1, f = 1 & p \text{ ist } \textit{zerlegt} \\ g = 1, e = 1, f = 2 & p \text{ ist } \textit{träge} \end{cases}$$

Wir bestimmen die verzweigten Primzahlen: Sei $K = \mathbb{Q}(\sqrt{\delta})$ mit $\delta = 2, 3 \mod 4$, also $\mathcal{O}_K = \mathbb{Z}[\sqrt{\delta}]$, $d = 4\delta$. Die Erweiterung ist verzweigt in 2 und Teilern von $\delta$.
Für $\delta = 1 \mod 4$ ist $1, (1 + \sqrt{\delta})/2$ eine Basis von $\mathcal{O}_K$.

$$d = \det \begin{pmatrix} 1 & 1 \\ (1+\sqrt{\delta})/2 & (1-\sqrt{\delta})/2 \end{pmatrix}^2 = [(1-\sqrt{\delta})/2 - (1-\sqrt{\delta})/2]^2 = \delta$$

In diesem Fall ist also 2 unverzweigt.
Beispiele für träge und zerlegte Primzahlen haben wir bereits gesehen: In $\mathbb{Q}(\sqrt{-5})$ ist 3 zerlegt und 11 träge. Das quadratische Reziprozitätsgesetz impliziert, dass es das Zerlegungsverhalten nur von den Restklassen von $p \mod 5$ abhängt. Nach dem *Dirichletschen Dichtesatz* hat enthält jede Restklasse $\mod 5$ (ungleich 0) unendliche viele Primzahlen. Beide Fälle kommen also unendlich oft vor.

## Galoistheorie

Sei nun $L/K$ eine Galoiserweiterung von globalen Körpern, d.h.

$$[L : K] = \mathrm{Gal}(L/K) \Leftrightarrow L^{\mathrm{Gal}(L/K)} = K$$

wobei $\mathrm{Gal}(L/K) = \{\sigma : L \to L \mid \sigma|_K = \mathrm{id}\}$. Dies ist äquivalent dazu, dass $L/K$ separabel und normal ist, d.h. für $\alpha \in L$ liegen alle Nullstellen des Minimalpolynoms in $L$.

**Lemma 5.13.** *Sei $L/K$ eine Galoiserweiterung von globlen Körpern. Dann operiert $\mathrm{Gal}(L/K)$ auf $\mathcal{O}_L$, auf den Primidealen von $\mathcal{O}_L$ und auf den Primidealen von $\mathcal{O}_L$ über $\mathfrak{p} \subset \mathcal{O}_K$.*

*Beweis:* Sei $\sigma \in \mathrm{Gal}(L/K)$, $x \in \mathcal{O}_L$, d.h. es gibt eine Polynomgleichung

$$x^n + a_1 x^{n-1} + \ldots a_n = 0 \qquad a_i \in \mathcal{O}_K$$

Anwenden von $\sigma$ auf diese Gleichung ergibt

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

Damit ist auch $\sigma(x)$ ganz.
Sei nun $\mathfrak{q} \subset \mathcal{O}_L$ ein Primideal. Wir betrachten $\sigma(\mathfrak{q})$. Dies ist offensichtlich ein Ideal. Sei $ab \in \sigma(\mathfrak{q})$, also $\sigma^{-1}(a)\sigma^{-1}(b) \in \mathfrak{q}$. Da $\mathfrak{q}$ ein Primideal ist, folgt $\sigma^{-1}a \in \mathfrak{q}$ oder $\sigma^{-1}b \in \mathfrak{q}$, also $a \in \sigma(\mathfrak{q})$ oder $b \in \sigma(\mathfrak{q})$.
Schließlich sei $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$. Dann gilt $\sigma(\mathfrak{q}) \cap \mathcal{O}_K = \mathfrak{p}$, denn $\sigma$ lässt Elemente von $\mathcal{O}_K$ invariant. □

In dieser Situation heißen $\mathfrak{q}$ und $\sigma(\mathfrak{q})$ *konjugiert*. Verzweigungsindex und Restklassengrad von konjugierten Idealen stimmen überein.

**Lemma 5.14.** *Sei $L/K$ Galoiserweiterung von globelen Körpern. Je zwei Primideale von $\mathcal{O}_L$ über $\mathfrak{p} \subset \mathcal{O}_K$ sind konjugiert. Es gilt*

$$[L : K] = gfe$$

*wobei $g$ die Anzahl der Primideale über $\mathfrak{p}$ ist, $e$ der Verzweigungsindex, $f$ der Restklassengrad.*

*Beweis:* Die Formel folgt aus der ersten Aussage mit der Gradformel. Seien $\mathfrak{q}, \mathfrak{q}'$ über $\mathfrak{p}$ nicht konjugiert, also $\sigma(\mathfrak{q}')$ nicht in $\mathfrak{q}$ enthalten für alle $\sigma$. Seien $\mathfrak{q}'_1, \ldots, \mathfrak{q}'_k$ die Konjugierten von $\mathfrak{q}'$. Wir wählen $x_{ij} \in \mathfrak{q}'_j \setminus \mathfrak{q}'_i$ für $i \neq j$ und $x_i \in \mathfrak{q} \setminus \mathfrak{q}'_i$. Sei

$$x = x_1 \prod_{1 \neq j} x_{1j} + x_2 \prod_{2 \neq j} x_{2j} + \cdots + x_k \prod_{k \neq j} x_{kj}$$

Es gilt $x \in \mathfrak{q}$, da $x_i \in \mathfrak{q}$. Andererseits ist $x \notin \mathfrak{q}'_j$, denn jeder Summand außer dem zu $j$ enthält einen Faktor in $\mathfrak{q}'_j$ (nämlich $x_{ij}$). In dem Summanden zu $j$ ist kein Faktor in $\mathfrak{q}'_j$. Es folgt

$$N(x) = \prod \sigma(x) \in \mathcal{O}_K \cap \mathfrak{q} = \mathfrak{p} \subset \mathfrak{q}'$$

Also liegt ein $\sigma(x) \in \mathfrak{q}'$ und $x \in \sigma^{-1}\mathfrak{q}'$. Dies ist ein Widerspruch. □

**Definition 5.15.** *Sei $L/K$ Galoiserweiterung von globalen Körpern, $\mathfrak{q}$ ein Primideal von $\mathcal{O}_L$, $\mathfrak{p} = \mathcal{O}_K \cap \mathfrak{q}$. Die* Zerlegungsgruppe *von $\mathfrak{q}$ ist*

$$D_\mathfrak{q} = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{q}) = \mathfrak{q}\}$$

*Die natürliche Abbildung $\phi : D_\mathfrak{q} \to \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))$ ist ein Gruppenhomomorphismus. Die* Trägheitsgruppe *$I_\mathfrak{q}$ ist der Kern von $\phi$, d.h.*

$$I_\mathfrak{q} = \{\sigma : L \to L \mid \sigma(\alpha) = \alpha \mod \mathfrak{q} \text{ für alle } \alpha \in \mathcal{O}_L\}$$

**Lemma 5.16.** *Es gilt $|D_\mathfrak{q}| = ef$, $e = |I_\mathfrak{q}|$. Die Abbildung $\phi$ ist surjektiv.*

*Beweis:* Wie vorher sei $g$ die Anzahl der Konjugierten von $\mathfrak{q}$, d.h. $|G|/|D_\mathfrak{q}|$, denn $G$ operiert transitiv mit Standgruppe $D_\mathfrak{q}$. Also

$$g = n/|D_\mathfrak{q}| = gef/|D_\mathfrak{q}|$$

Sei nun $E = L^{D_\mathfrak{q}} \subset L$. Nach dem Hauptsatz der Galoistheorie ist $\mathrm{Gal}(L/E) = D_\mathfrak{q}$. Sei $\mathfrak{p}_E = \mathfrak{q} \cap \mathcal{O}_E$. Nach Definition liegt $\mathfrak{q}$ über $\mathfrak{p}_E$. Das Primideal $\mathfrak{q}$ wird von allen Elementen auf $D_\mathfrak{q}$ festgelassen, also ist die Zerlegungsgruppe von $\mathfrak{q}$ in $L/E$ ganz $D_\mathfrak{q}$. Damit liegt nur ein Primideal von $L$ über $\mathfrak{p}_E$ (nämlich $\mathfrak{q}$). Es folgt

$$ef = |D_\mathfrak{q}| = [L : E] = e(\mathfrak{q}/\mathfrak{p}_E) f(\mathfrak{q}/\mathfrak{p}_E)$$

Verzweigungsgrad und Restklassenindex sind multiplikativ in Körpertürmen, also folgt

$$e = e(\mathfrak{q}/\mathfrak{p}) = e(\mathfrak{q}/\mathfrak{p}_E), \qquad f = f(\mathfrak{q}/\mathfrak{p}) = f(\mathfrak{q}/\mathfrak{p}_E)$$

Dies bedeutet $\kappa(\mathfrak{p}_E) = \kappa(\mathfrak{p})$.
Nach dem Satz vom primitiven Element ist $\kappa(\mathfrak{q}) = \kappa(\mathfrak{p})(\overline{\alpha})$ für ein $\alpha \in \mathcal{O}_L$. Sei $P \in \mathcal{O}_E[X]$ das normierte Minimalpolynom von $\alpha$. Es stimmt mit dem charakteristischen Polynom von $\alpha$ überein. Dann ist $\overline{P} \in \kappa(\mathfrak{p}_E)[X]$ eine Potenz des Minimalpolynoms von $\overline{\alpha}$. Sei $\overline{\sigma} \in \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}_E))$, also $\overline{\sigma}(\overline{\alpha})$ eine Nullstelle von $\overline{P}$. Dann muss es $\sigma \in \mathrm{Gal}(L/E) = D_\mathfrak{q}$ geben mit $\sigma(\alpha) = \overline{\sigma}(\overline{\alpha})$. Dann ist $\overline{\sigma} = \phi(\sigma)$, d.h. $\phi$ ist surjektiv. Es folgt $f(\mathfrak{q}/\mathfrak{p}_E) = |\mathrm{Im}\phi| = |D_\mathfrak{q}|/|I| = ef/|I|$. □

**Korollar 5.17.** *Sei $L/K$ Galoisweiterung von globalen Körpern, $\mathfrak{p} \subset \mathcal{O}_K$ ein Primideal. Dann ist $\mathfrak{p}$ unverzweigt genau dann, wenn $|I_\mathfrak{q}| = 1$ für ein $\mathfrak{q} \mid \mathfrak{p}$. Allgemein ist $L^{I_\mathfrak{q}}/K$ unverzweigt über $\mathfrak{p}$.*

**Lemma 5.18.** *Sei $\mathfrak{q}, \sigma(\mathfrak{q}) \mid \mathfrak{p}$. Dann gilt $D_{\sigma\mathfrak{q}} = \sigma D_\mathfrak{q} \sigma^{-1}$, $I_{\sigma\mathfrak{q}} = \sigma I_\mathfrak{q} \sigma^{-1}$. Insbesondere sind diese Gruppen isomorph.*

*Proof.* Die Aussage für $D_\sigma$ ist die Formel für die Standgruppe von zwei Elementen derselben Bahn. Die Aussage für die Trägheitsgruppe rechnet man leicht nach. □

**Bemerkung.** Ist die Galoisgruppe abelsch, so gilt $D_\mathfrak{q} = D_{\sigma\mathfrak{q}}$. Wir schreiben dann auch $D_\mathfrak{p}$ und $I_\mathfrak{p}$.

# Kapitel 6

# Zyklotomische Körper

## Erinnerung

$\zeta \in \overline{\mathbb{Q}}$ heißt $n$-te Einheitswurzel, wenn $\zeta^n = 1$. Es heißt *primitive* $n$-te Einheitswurzel, wenn $\zeta^m \neq 1$ für $m < n$. Die Gruppe der $n$-ten Einheitswurzeln ist eine endliche zyklische Gruppe der Ordnung $n$. Die primitiven $n$-ten Einheitswurzeln sind gerade ihre Erzeuger. Es gibt also $\phi(n)$ viele primitive $n$-te Einheitswurzeln (Eulersche $\phi$-Funktion).
Sei $\zeta_n \in \overline{\mathbb{Q}}$ primitive $n$-te Einheitswurzel. Dann hat das Minimalpolynom $\Phi(n)$ von $\zeta_n$ den Grad $\phi(n)$. Die Erweiterung $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ ist galois mit Galoisgruppe $(\mathbb{Z}/n\mathbb{Z})^*$. Wir erhalten den Isomorphismus wie folgt: Sei $a \in \mathbb{Z}$ teilerfremd zu $n$. Dann definiert

$$\sigma_a : \zeta_n \mapsto \zeta_n^a$$

ein Element von $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Es hängt nur von der Restklasse $a \in \mathbb{Z}/n\mathbb{Z}$ ab, von dieser aber dann wirklich. Es gibt $\phi(n)$ solche Restklassen, daher hat die Galoisgruppe mindestens $\phi(n)$ Elemente. Dann ist die Erweiterung galois und unsere Zuordnung surjektiv. Man beachte, dass $\sigma_a$ unabhängig von der Wahl von $\zeta_n$ ist! Die zyklotomischen Körper sind also Beispiele von *abelschen Erweiterungen*, Galoiserweiterungen mit abelscher Galoisgruppe.

## Der Ganzheitsring

Sei $\zeta_n$ eine primitive $n$-te Einheitswurzel. Einheitswurzeln sind ganz, also gilt $\mathbb{Z}[\zeta_n] \subset \mathcal{O}_{\mathbb{Q}(\zeta_n)}$. Wir wollen Gleichheit zeigen und beginnnen langsam.

**Satz 6.1.** *Sei $n = l$ Primzahl. Dann ist*

$$\mathbb{Z}[\zeta_l] = \mathcal{O}_{\mathbb{Q}(\zeta_l)}$$

*Proof.* Sei $\mathcal{O} = \mathcal{O}_{\mathbb{Q}(\zeta_l)}$, $\zeta = \zeta_l$. Das Minimalpolynom von $\zeta$ ist $X^{p-1} + X^{p-2} + \cdots + 1$, daher ist $\mathrm{Tr}(\zeta) = -1$. Da alle primitiven Einheitswurzeln gleichberechtigt sind, folgt $\mathrm{Tr}(\zeta^i) = -1$ für $i = 1, \ldots, p-1$. Hieraus folgt $\mathrm{Tr}(1-\zeta) = p$ und $\mathrm{Tr}(\zeta^i(1-\zeta)) = 0$ für $i = 1, \ldots, p-1$.

Sei nun $x = a_0 + \cdots + a_{l-2}\zeta^{l-2} \in \mathcal{O}$ mit $a_i \in \mathbb{Q}$. Wegen $x(1-\zeta) \in \mathcal{O}$ folgt $\mathrm{Tr}(x(1-\zeta)) = a_0 l \in \mathbb{Z}$. Andererseits gilt

$$\mathrm{Tr}(x(1-\zeta)) = \sum_\sigma \sigma(x)(1-\sigma(\zeta))$$

mit $\sigma(\zeta) = \zeta^j$, also $1-\sigma(\zeta) = (1-\zeta)(1+\zeta+\cdots+\zeta^{j-1})$. Damit gilt $\mathrm{Tr}(x(1-\zeta)) \in \mathcal{O}(1-\zeta) \cap \mathbb{Z}$.

**Behauptung.** $\mathcal{O}(1-\zeta) \cap \mathbb{Z} = l\mathbb{Z}$

Mit $x = 1$ und $\mathrm{Tr}(1-\zeta) = l$ gilt $\supset$. Wäre Gleichheit falsch, so müsste $1 \in \mathcal{O}(1-\zeta)$ liegen, also $1-\zeta$ eine Einheit sein. Die Norm von $1-\zeta$ ist aber

$$N(1-\zeta) = \prod_{j=1}^{l-1}(1-\zeta^j) = \prod(X-\zeta^j)(1) = (1+X+\cdots+X^{l-1})(1) = l$$

also ist dies nicht der Fall.
Somit gilt $la_0 \in l\mathbb{Z}$, d.h. $a_0 \in \mathbb{Z}$. Dann ist auch $a_1\zeta + \ldots a_{p-2}\zeta^{p-2} = \zeta(a_1 + \ldots a_{p-2}\zeta^{p-3} \in \mathcal{O}$. $\zeta$ ist eine Einheit. Wir wiederholen nun das Argument und erhalten $a_1 \in \mathbb{Z}$ und iterativ $a_i \in \mathbb{Z}$ für alle $i$. Damit ist die Berechnung von $\mathcal{O}$ abgeschlossen. □

**Lemma 6.2.** *Sei $n = l^\nu$ eine Primzahlpotenz, $\lambda = (1-\zeta_n)$, $d = \phi(l^\nu)$. Dann ist $(\lambda)$ ein Primideal mit Restklassengrad 1. Es gilt*

$$(l) = (\lambda)^d \subset \mathcal{O}_{\mathbb{Q}(\zeta_{l^\nu})}$$

*$l$ ist rein verzweigt. Es gilt*

$$D(1, \zeta_n, \ldots, \zeta_n^{d-1}) = \pm l^s \text{ mit } s = l^{\nu-1}(\nu l - \nu - 1)$$

*Proof.* Sei $\mathcal{O} = \mathcal{O}_{\mathbb{Q}(\zeta_n)}$, $\zeta = \zeta_n$. Es gilt

$$\Phi_{l^\nu}(X) = \frac{X^{l^\nu}-1}{X^{l^{\nu-1}}-1} = X^{(l-1)l^{\nu-1}} + \cdots + X^{l^{\nu-1}} + 1$$

Einsetzen von 1 ergibt

$$l = \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^*} (1-\zeta^a)$$

Es ist

$$1-\zeta^a = (1+\zeta+\cdots+\zeta^{a-1})(1-\zeta)$$

Der Vorfaktor ist also ganz. Wegen $N(1-\zeta^a) = N(1-\zeta)$ hat er Norm 1, ist also eine Einheit in $\mathcal{O}$. Dies bedeutet $(1-\zeta) = (1-\zeta^a)$ als Ideale. Damit haben wir die Idealidentität gezeigt. Wegen $N(l) = l^d$ folgt $N(\lambda) = l$. Damit ist dies ein Primideal. Wegen $d = efg$ mit $g = 1, e = d$ ist $f = 1$.

Seien $\zeta_1, \ldots, \zeta_d$ die Konjugierten von $\zeta$. Dann gilt

$$D(1, \zeta, \ldots, \zeta^{d-1}) = \pm \begin{vmatrix} 1 & \zeta_1 & \ldots & \zeta_1^{d-1} \\ 1 & \zeta_2 & \ldots & \zeta_2^{d-1} \\ & & \ldots & \\ 1 & \zeta_d & \ldots & \zeta_d^{d-1} \end{vmatrix}^2$$

$$= \prod_{i<j} (\zeta_i - \zeta_j)^2$$

Das von diesem Ausdruck in $\mathcal{O}$ erzeugte Ideal ist nach dem Obigen eine Potenz von $(\lambda)$. Da es gleichzeitig eine ganze Zahl ist, erhalten wir (bis auf Vorzeichen) eine Potenz von $l$. Den Exponenten lesen wir ab. □

**Satz 6.3.** *Sei $n = l^\nu$ eine Primzahlpotenz. Dann ist $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$. In $\mathbb{Q}(\zeta_n)$ ist $l$ rein verzweigt, alle anderen Primideale sind unverzweigt.*

*Proof.* Sei $\mathcal{O} = \mathcal{O}_{\mathbb{Q}(\zeta_n)}$, $\zeta = \zeta_n$. Wir wissen $\mathbb{Z}[\zeta] \subset \mathcal{O}$. Sei wie oben $l^s$ die Diskriminante von $\mathbb{Z}[\zeta_n]$.
Nach Lemma 6.2 gilt $\mathbb{Z}/l\mathbb{Z} \cong \mathcal{O}/(\lambda)$ (Restklassengrad 1), also

$$\mathcal{O} = \mathbb{Z} + \lambda\mathcal{O} \Rightarrow \mathcal{O} = \mathbb{Z}[\zeta] + \lambda\mathcal{O}$$

Wir multiplizieren mit $\lambda$ und setzen das Ergebnis ein. Es gilt also

$$\mathcal{O} = \mathbb{Z}[\lambda] + \lambda^2\mathcal{O} \Rightarrow \cdots \Rightarrow \mathcal{O} = \mathbb{Z}[\lambda] + \lambda^s\mathcal{O}$$

**Behauptung.** $l^s\mathcal{O} \subset \mathbb{Z}[\zeta]$

Allgemeiner gilt $\Delta\mathcal{O} \subset < x_1, \ldots, x_d >$, wenn $x_1, \ldots, x_d \in \mathcal{O}$ mit $D(x_1, \ldots, x_d) = \Delta$. Sei $y_1, \ldots, y_d$ die duale Basis von $x_1, \ldots, x_d$ bezüglich der Spurpaarung. Wir wissen, dass

$$\mathcal{O} \subset < y_1, \ldots, y_d >_{\mathbb{Z}}$$

Es genügt also zu zeigen, dass $\Delta y_i \in < x_1, \ldots, x_d >_{\mathbb{Z}}$. Wir schreiben die $y_i$ mit Hilfe der Cramerschern Regel in Termen der $x_j$ hin. Als Nenner taucht nur $\Delta$ auf. □

Sei nun $n$ allgemein. Falls $n = n_1 n_2$ mit teilerfremde $n_1, n_2$, so gilt

$$\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{n_1})\mathbb{Q}(\zeta_{n_2})$$

denn $\zeta_{n_1}\zeta_{n_2}$ ist eine primitive $n$-te Einheitswurzel. Daher kann der folgende Satz angewendet werden:

**Satz 6.4.** *Seien $E, E'/\mathbb{Q}$ Galoiserweiterungen von Zahlkörpern. Die Diskriminanten $d, d'$ seien teilerfremd. Dann ist $\mathcal{O}_E\mathcal{O}_{E'} = \mathcal{O}_{EE'}$. Die Körpererweiterung $EE'/\mathbb{Q}$ verzweigt genau in den Primzahlen, die $dd'$ teilen. Es gilt $d_{EE'} = d^{n'}d'^{n}$.*

Wir halten fest:

**Korollar 6.5.** *Sei $n \in \mathbb{N}$. Dann ist $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$. Die Erweiterung $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ verzweigt genau in den Primteilern von $n$.*

Der Beweis von Satz 6.4 benötigt ein tiefes Ergebnis, das wir später noch zeigen werden:

**Theorem 6.6** (Hasse-Minkowski)**.** *Es gibt keine unverzweigten Erweiterungen von $\mathbb{Q}$.*

*Beweis von Satz 6.4.* Der Körper $E \cap E'$ ist eine unverzweigte Erweiterung von $\mathbb{Q}$, also nach dem Theorem von Hasse und Minkowski gleich $\mathbb{Q}$.
Sei $n = [E : \mathbb{Q}]$, $n' = [E' : \mathbb{Q}]$. Dann ist $[EE' : \mathbb{Q}] = nn'$. Es gilt $\mathrm{Gal}(EE'/\mathbb{Q}) = G(E/\mathbb{Q}) \times G(E'/\mathbb{Q})$. Sei $x_1, \dots, x_n$ eine Basis von $\mathcal{O}_E$ und $x'_1, \dots, x'_{n'}$ eine Basis von $E'$. Dann ist $\{x_i x'_j | i = 1, \dots, n, j = 1, \dots, n'\}$ eine $\mathbb{Q}$-Basis von $EE'$. Sei nun $\alpha \in \mathcal{O}_{EE'}$,

$$\alpha = \sum a_{ij} x_i x'_j$$

**Behauptung.** $a_{ij} \in \mathbb{Z}$.

Sei $G = \mathrm{Gal}(E/\mathbb{Q}) = \{\sigma_1, \dots, \sigma_n\}$, $G' = \mathrm{Gal}(E'/\mathbb{Q}) = \{\sigma'_1, \dots, \sigma'_{n'}\}$. Dann gilt

$$\mathrm{Gal}(EE'/\mathbb{Q}) = \{\sigma_k \sigma'_l | k = 1, \dots, n, l = 1, \dots, n'\}$$

Wir betrachten die Matrix $T = (\sigma'_l x'_j)$. Es gilt $d' = \det(T)^2$. Sei $a = (\sigma_1 \alpha, \dots, \sigma_{n'} \alpha)^t$. Dann gilt

$$a = Tb$$

mit $b = (\sum_i a_{i1} x_i, \sum_i a_{i2} x_i, \dots, \sum_i a_{in} x_i)^t$. Sei $T^* = \det(T) T^{-1}$. Nach der Cramerschen Regel hat sie Einträge in $\mathcal{O}_{E'}$. Daher hat

$$T^* a = \det(T) b$$

Einträge in $\mathcal{O}_{EE'}$. Hieraus folgt, dass $\sum_i d' a_{ij} x_i$ ganz ist für alle $j$. Da $x_1, \dots, x_n$ eine Basis von $\mathcal{O}_E$ ist, folgt $d' a_{ij} \in \mathbb{Z}$ für alle $i, j$.
Dieselbe Überlegung mit vertauschten Rollen von $E$ und $E'$ impliziert $d a_{ij} \in \mathbb{Z}$ für alle $i, j$. Da $d, d'$ teilerfremd sind, ist $a_{ij} \in \mathbb{Z}$.
Ist $p$ verzweigt in $E$ oder $E'$, dann offensichtlich auch in $EE'/\mathbb{Q}$. In der expliziten Basis, die wir gefunden haben, können wir auch die Diskriminate von $E_1 E_2/\mathbb{Q}$ leicht berechnen. □

**Beispiel.** Wir betrachten wieder den Fall $n = l$ ungerade Primzahl. Dann ist $\mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q}) \cong \mathbb{F}_l^*$ zyklisch der Ordnung $l - 1$. Sei $H$ die Untergruppe der Ordnung $(l-1)/2$. Wir betrachten $E = \mathbb{Q}(\zeta_l)^H$. Dies ist eine quadratische Erweiterung von $\mathbb{Q}$. Welche? In $\mathbb{Q}(\zeta_l)/\mathbb{Q}$ ist nur die Primzahl $l$ verzweigt, also ist auch in $E/\mathbb{Q}$ höchstens $l$ verzweigt. Es folgt

$$E = \begin{cases} \mathbb{Q}(\sqrt{l} & l = 1 \mod 4 \\ \mathbb{Q}(\sqrt{-l} & l = -1 \mod 4 \end{cases}$$

**Satz 6.7.** *Sei $d \in \mathbb{Z}$ quadratfrei. Dann gibt es $N$ mit $\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\zeta_N)$.*

Das minimale $N$ mit dieser Eigenschaft heißt *Führer* von $\mathbb{Q}(\sqrt{d})$.

*Proof.* Beachte, dass $i = \zeta_4$. Wir beginnen mit $d = p$ Primzahl. Ist $p = 1 \mod 4$, so gilt nach dem Beispiel $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_p)$. Für $p = 3 \mod 4$ gilt nach dem Beispiel

$$\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(i, \sqrt{-p}) \subset \mathbb{Q}(i, \zeta_p) = \mathbb{Q}(\zeta_{4p}) \ .$$

Für $p = 2$ beachten wir $\zeta_8 = \sqrt{i} = \sqrt{2}^{-1} + i\sqrt{2}^{-1}$, also $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\zeta_8)$.
Ist $d \in \mathbb{Z}$ quadratfrei, so gilt $d = \pm p_1 \dots p_n$ für verschiedene Primzahlen. Wir setzen die Fälle von vorher zusammen. Demnach gilt

$$\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\zeta_8, \zeta_{p_1}, \dots, \zeta_{p_n}) \subset \mathbb{Q}(\zeta_{8d})$$

□

Tatsächlich gilt viel allgemeiner:

**Theorem 6.8** (Kronecker-Weber)**.** *Sei $K/\mathbb{Q}$ endlich abelsche Erweiterung. Dann gibt es $N$ mit $K \subset \mathbb{Q}(\zeta_N)$.*

Dies ist ein Spezialfall von Klassenkörpertheorie. Es gibt auch einen direkten Beweis, aber wir werden dieses Semester wohl nicht mehr dazu kommen. Offensichtlich ist ein Hauptproblem, den richtigen Kandidaten für $N$ zu finden. Er wird vom Verzweigungsverhalten von $K$ diktiert.

# Kapitel 7

# Bewertungstheorie und lokale Körper

**Definition 7.1.** *Sei $k$ ein Körper. Ein* Absolutbetrag *$v$ ist ein Abbildung*

$$k \to \mathbb{R} \qquad\qquad x \mapsto |x|_v$$

*so dass*

*(i)* $|x|_v \geq 0$ *und* $|x|_v = 0 \Leftrightarrow x = 0$.

*(ii) Für alle* $x, y \in k$ *gilt* $|xy|_v = |x|_v |y|_v$.

*(iii)* $|x + y|_v \leq |x|_v + |y|_v$.

Ein Absolutbetrag definiert eine Metrik und damit eine Topologie via: $U \subset k$ heißt offen, falls für alle $x \in U$ ein $\varepsilon > 0$ existiert, so dass

$$\{y \in k \mid |y - x|_v < \varepsilon\} \subset U \ .$$

**Beispiel.**

- $\mathbb{R}, \mathbb{C}$ mit dem gewöhnlichen Absolutbetrag, ebenso $\mathbb{Q}$.
- Für $p \in \mathbb{Q}$ eine Primzahl $|x|_p = p^{-v(x)}$, wobei $v(x)$ die Vielfachheit von $p$ in $x$ ist. Dies ist der *p-adische Betrag.*

**Definition 7.2.** *Sei $k$ ein Körper. Eine* diskrete Bewertung *ist eine Abbildung* $v : k \to \mathbb{R} \cup \{\infty\}$ *mit*

*(i)* $v(x) = \infty \Leftrightarrow x = 0$.

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

*(iii)* $v(x + y) \geq \min(v(x), v(y))$

*und* $v(k^*)$ *diskrete Untergruppe von* $\mathbb{R}$ *vom Rang* 1.

Wir können jede diskrete Bewertung ohne Einschränkung so normieren, dass $v(k^*) = \mathbb{Z}$.

**Lemma 7.3.** *Sei $v$ eine diskrete Bewertung, $a > 1$ fest. Dann ist $|x|_v = a^{v(x)}$ ein Absolutbetrag.*

*Beweis:* Die Eigenschaften (i) und (ii) sind klar.
Dreiecksungleichung:

$$a^{-v(x+y)} \leq a^{-\min(v(x),v(y))} \leq a^{-v(x)} + a^{-v(y)}$$

□

**Beispiel.** Sei $\mathcal{O}$ ein Dedekindring, $\mathfrak{p}$ ein Primideal, $K$ der Quotientenkörper von $\mathcal{O}$. Für $x \in K^*$ sei $(x) = \prod \mathfrak{q}^{v_\mathfrak{q}(x)}$ die Produktzerlegung in Primideale. Dann ist die Abbildung $v : K^* \to \mathbb{Z}$ mit $x \mapsto v_\mathfrak{p}(x)$ eine diskrete Bewertung.
Durch Wahl einer reellen Zahl erhalten wir also einen Betrag. Ist $\kappa(\mathfrak{p})$ endlich, so ist eine Standardnormalisierung $a = |\kappa(\mathfrak{p})|$. Für $\mathcal{O} = \mathbb{Z}$ erhielten wir so die $p$-adischen Beträge $|\cdot|_p$.

Allgemein:

**Definition 7.4.** *Ein Dedekindring mit genau einem maximalen Ideal heißt* diskreter Bewertungsring.

**Satz 7.5.** *Sei $A$ ein Ring. Äquivalent sind:*

*(i) $A$ ist ein diskreter Bewertungsring.*

*(ii) $A$ ist Hauptidealring mit genau einem maximalen Ideal.*

*(iii) $A$ ist von der Form $\{x \in k | v(x) \geq 0\}$ für eine diskrete Bewertung eines Körpers $k$.*

*Es gilt dann $k = Q(A)$ und das maximale Ideal ist $\mathfrak{m} = \{x \in x | v(x) > 0\}$.*

*Beweis:* Die Äquivalenz der ersten beiden Aussagen folgt wie wir bereits gesehen haben aus der Strukturtheorie von Dedekindringen. Wie im Beispiel wird die Bewertung auf $k = Q(A)$ definiert. Sie hat Wertebereich $\mathbb{Z} \cup \infty$. Sei nun umgekehrt $v : k \to \mathbb{Z} \cup \infty$ eine diskrete Bewertung, $A$ und $\mathfrak{m}$ wie in (iii).

**Behauptung.** *$A$ ist ein Ring mit maximalem Ideal $\mathfrak{m}$ und Quotientenkörper $k$.*

Sei $a, b \in A$. Dann ist $v(a + b) \geq \min(v(a), v(b)) \geq 0$, also $a + b \in A$. Ebenso $v(ab) = v(a)v(b) \geq 0$. Ebenso folgt, dass $\mathfrak{m}$ ein Ideal ist. Alle Elemente $u \in A \setminus \mathfrak{m}$ haben $v(u) = 0$, also $v(u^{-1}) = 0$ und daher $u^{-1} \in A$. Sie sind invertierbar. Jedes echte Ideal muss daher in $\mathfrak{m}$ enthalten sein, es ist maximal. Ist $x \in k$ mit $v(x) < 0$, so gilt $v(x^{-1}) > 0$, also $x^{-1} \in A$. Insbesondere ist $k$ der Quotientenkörper von $A$.
Der Wertebereich von $v$ ist diskret. Sei $\pi \in \mathfrak{m}$ mit $v(\pi)$ minimal. Ohne Einschränkung ist $v(\pi) = 1$, d.h. $v(k^*) = \mathbb{Z}$.

**Behauptung.** *Jedes Element von $k^*$ hat die Form $u\pi^v$ mit $u \in A^*$, $v \in \mathbb{Z}$.*

Sei $x \in k^*$, $v = v(x)$, $u = x\pi^{-v}$. Dann gilt $v(u) = v(x) - v = 0$, also $u \in A^*$. □

**Beispiel.** Sei $F$ ein Körper, $k = F(t)$. Dann ist

$$v_\infty : k^* \to \mathbb{Z}, \qquad P \mapsto -\deg(P)$$

ebenfalls eine diskrete Bewertung. Der Bewertungsring besteht aus aus rationalen Funktionen $P/Q$ mit $\deg P < \deg Q$. Das maximale Ideal wird von $t^{-1}$ erzeugt. Tatsächlich hat diese Bewertung noch eine andere Interpretation: Sei $u = t^{-1}$. Dann gilt $k = F(u)$. Sei $P = \sum_{i=0}^{n} a_i t^i$ mit $a_n \neq 0$, also $v_\infty(P) = -n$. Dann gilt

$$P = \sum_{i=0}^{n} a_i u^{-1} = u^{-n} \sum_{i=0}^{n} a_i u^{n-i} = u^{-n} Q(u)$$

und $u \nmid Q$. Also ist $v_u(P) = -n$ in dem Polynomring $F[u]$. Die Bewertungen von $F(t)$ mit $v(F^*) = 0$ stehen tatsächlich in Bijektion mit den Punkten der *projektiven Geraden*

$$\mathbb{P}^1 := \mathbb{A}^1 \cup \{\infty\} = \operatorname{Spm} k[t] \cup \{\infty\}$$

Sie hat eine Standardüberdeckung durch die affinen Geraden $\mathbb{P}^1_F \smallsetminus \{\infty\}$ und $\mathbb{P}^1_F \smallsetminus \{0\}$. Die erste hat den Koodinatenring $F[t]$, die zweite $F[t^{-1}]$.
Analog nennen wir den gewöhnlichen Absolutbetrag auf $\mathbb{Q}$ ebenfalls $|\cdot| = |\cdot|_\infty$.

**Definition 7.6.** *Sei $v \in \operatorname{Spm} \mathbb{F}_p[t] \cup \{\infty\}$ eine diskrete Bewertung. Dann setzen wir*

$$|x|_v = |\kappa(v)|^{-v(x)}$$

**Definition 7.7.** *Sei* $\operatorname{Char} k = 0$. *Ein Betrag heißt* kanonisch, *wenn seine Einschränkung auf $\mathbb{Q}$ mit $|\cdot|_p$ für $p \leq \infty$ übereinstimmt. Sei $k/\mathbb{F}_p(t)$. Ein Betrag heißt* kanonisch, *wenn seine Einschränkung auf $\mathbb{F}_p(t)$ mit $|\cdot|_v$ für ein $v \in \mathbb{P}^1_{\mathbb{F}_p(t)}$ übereinstimmt.*

Wir interessieren uns nur für die kanonischen Beträge.

**Bemerkung.** Ist $\mathfrak{p}$ ein Primideal eines globalen Körpers $k$ mit zugehöriger diskreter Bewertung $v_\mathfrak{p}$. Dann kann in der Definition von $|\cdot|_\mathfrak{p} = a^{-v_\mathfrak{p}(\cdot)}$ die reelle Zahl $a$ so gewählt werden, dass der Betrag kanonisch ist. Ist $\operatorname{Char}(k) = 0$, $\mathfrak{p}|p$ für eine Primzahl $p$, so ist $a = p^{e(\mathfrak{p}/p)}$.

**Definition 7.8.** *Sei $k$ ein Körper mit Absolutbetrag $v$. Er heißt* vollständig, *wenn jede Cauchy-Folge konvergiert. Sei $k_v$ der Körper der Cauchy-Folgen in $k$ modulo Nullfolgen.*

**Satz 7.9.** *$k_v$ ist vollständig und enthält $k$ als dichte Teilmenge.*

*Beweis:* Wie in Analysis. □

**Beispiel.** (i) $\mathbb{R}$ ist die Komplettierung von $\mathbb{Q}$ bezüglich $|\cdot|_\infty$.

(ii) Sei $\mathbb{Q}_p$ die Komplettierung von $\mathbb{Q}$ bezüglich $|\cdot|_p$. Dies ist der Körper der $p$-adischen Zahlen.

(iii) Sei $k = \mathbb{F}_p(t)$ und $|\cdot|_0$ der Betrag zur Bewertung $v_0$, die zum Primideal $(t) = (t-0)$ gehört. Dann gilt

$$k_v = \mathbb{F}_p((t)) := \left\{ \sum_{i=n}^{\infty} a_i t^n | n \in \mathbb{Z} a_i \in \mathbb{F}_p \right\}$$

der Körper der formalen Laurent-Reihen. (Das Cauchy-Produkt ist wohldefiniert!) Beweis Übungsaufgabe, siehe auch später der allgemeine Fall.

Komplettieren entspricht also dem Entwickeln in Potenz- bzw. Laurent-Reihen. Analog fassen wir Elemente von $\mathbb{Q}_p$ als Potenzreihen in $p$ auf.

**Theorem 7.10.** *Sei $k$ ein topologischer Körper. Die folgenden Eigenschaften sind äquivalent:*

*(i) $k$ ist Komplettierung eines globalen Körpers bezüglich eines kanonischen Betrages.*

*(ii) $k$ ist vollständig, lokalkompakt und nicht-diskret.*

*(iii) $k$ ist endliche Erweiterung von $\mathbb{R}$, $\mathbb{Q}_p$ oder $\mathbb{F}_p((t))$ für eine Primzahl $p$.*

*Beweis:* vergl. Weil, Basic number theory §3 □

Solche Körper heißen *lokal*. Uns fehlt die Zeit, dies vollständig zu beweisen. Wir benutzen die Arbeitsdefinition:

**Definition 7.11.** *$k$ heißt* lokaler Körper*, wenn er Komplettierung eines globalen Körpers bezüglich eines kanonischen Betrages ist.*

Zur Erinnerung: ein metrischer Raum ist lokalkompakt, wenn jede beschränkte Folge eine konvergente Teilfolge hat.

**Satz 7.12.** *Sei $K$ ein globaler Körper, $\mathfrak{p}$ ein Primideal, $|\cdot|_v$ der kanoische Absolutbetrag zur $\mathfrak{p}$-adischen Bewertung $v_\mathfrak{p} : K^* \to \mathbb{Z}$. Sei $K_v$ die Komplettierung von $K_\mathfrak{p}$ bezüglich $v$.*

*(i) $v_\mathfrak{p}$ ist eine diskrete Bewertung auf $K_v$.*

*(ii) Der topologische Abschluss $\mathcal{O}_v$ von $\mathcal{O}_K$ in $K_v$ ist $\{x \in K_v \mid |x| \leq 1\}$, ein diskreter Bewertungsring mit Restklassenkörper $\mathcal{O}_K/\mathfrak{p}$.*

*(iii) $\mathcal{O}_v$ ist kompakt, $K_v$ ist lokalkompakt.*

*Beweis:* Sei $x \in K_v$, $x = \lim x_i$ mit $x_i \in K$. D.h. für alle $\varepsilon > 0$ gibt es $N$, so dass $|x_i - x_j| < \varepsilon$ für alle $i, j > N$. Also

$$|x_i| = |x_i - x_j + x_j| \leq \max(|x_i - x_j|, |x_j|) \leq \max(\varepsilon, |x_j|)$$

**1. Fall:** $x = 0$. Dann bilden die $x_j$ eine Nullfolge.
**2. Fall:** $x \neq 0$, die $x_i$ bilden keine Nullfolge. Dann gibt es $\varepsilon_0 > 0$, so dass es für jedes $N$ ein $i > N$ gibt mit $|x_i| > \varepsilon_0$. Für alle $\varepsilon < \varepsilon_0$ folgt dann $|x_i| \leq |x_j|$. Also wird $|x_i|$ konstant.
$|x| = |x_i|$ für großes $i$ hat denselben Wertebereich wie der Betrag auf $K$, insbesondere ist er diskret. Ebenso ist $v(x) = \lim v(x_i)$ konstant, die Bewertung auf $K_v$ ist diskret.
Sei

$$\mathcal{O}_v = \{x \in K_v \mid |x| \leq 1\} = \{x \in K_v \mid v(x) \geq 0\}$$

Sei $\mathcal{O}_\mathfrak{p} = \{a/s \in K \mid a \in \mathcal{O}, s \in \mathcal{O} \setminus \mathfrak{p}\}$ die Lokalisierung des Ganzheitsrings in $\mathfrak{p}$.

**Behauptung.** *$\mathcal{O}_v$ ist der topologische Abschluss von $\mathcal{O}_\mathfrak{p}$.*

$\mathcal{O}_\mathfrak{p}$ ist ein lokaler Hauptidealring (vergleiche Satz 5.6). Das einzige Primideal wird erzeugt von $\pi \in \mathfrak{p}\mathcal{O}_\mathfrak{p}$. Nach Definition ist $v(\pi) = 1$. Jedes Element von $K^*$ ist von der Form $u\pi^r$ mit $u \in \mathcal{O}_\mathfrak{p}^*$ und $r \in \mathbb{Z}$. Es gilt $\mathcal{O}_\mathfrak{p} \subset \mathcal{O}_v$, denn $v(a/s) = v(a) - v(s) = v(a) \geq 0$. Sei $x \in \mathcal{O}_v$, also $x = \lim x_i$, $x_i \in K$, $v(x) \geq 0$. Hieraus folgt, wie wir gesehen haben $v(x_i) > 0$ für $i$ groß genug.
Offensichtlich ist $K \cap \mathcal{O}_v = \mathcal{O}_\mathfrak{p}$. Sei $x \in K_v^*$, $r = v(x) \in \mathbb{Z}$. Dann ist $x = u\pi^r$ mit $v(u) = 0$, also $u \in \mathcal{O}_v^*$. Demnach ist auch $\mathcal{O}_v$ ein Hauptidealring, einziges Primideal $(\pi)$.

**Behauptung.** *$\mathcal{O}_K$ ist dicht in $\mathcal{O}_\mathfrak{p}$.*

Sei $x = a/s$ mit $s \in \mathcal{O}_K \setminus \mathfrak{p} = \mathcal{O}_K \cap \mathcal{O}_v^*$. Sei $N \geq 0$. $\pi^N$ und $s$ sind teilerfremd, d.h. $(\pi^N, s) = 1$. Es gibt $b, c \in \mathcal{O}_K$ mit

$$b\pi^N + sc = 1 \Rightarrow sc - ss^{-1} = -b\pi^N \Rightarrow |c - s^{-1}| = |s(c - s^{-1})|_v \leq |\pi|_v^{-N}$$

Damit wird $s^{-1}$ (und dann auch $as^{-1}$) durch ein Element von $\mathcal{O}_K$ approximiert. Beachte (Satz 5.6)

$$\mathcal{O}_K/\mathfrak{p} \cong \mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p} \to \mathcal{O}_v/(\pi)$$

Die Abbildung ist injektiv, da es ein Körperhomomorphismus ist.

**Behauptung.** *Die Abbildung ist surjektiv.*

Sei $x = \lim x_i$ mit $x_i \in \mathcal{O}_\mathfrak{p}$. Es gilt $v(x - x_i) \to \infty$, insbesondere $v(x - x_i) \geq 1$ für $i$ groß genug, d.h. $\pi \mid x - x_i$. Hieraus folgt $x = x_i$ modulo $\pi$, also liegt $x$ modulo $\pi$ im Bild von $\mathcal{O}_\mathfrak{p}$.
Dies beendet den Beweis von (ii).
Sei $x_i$ eine Folge in $\mathcal{O}_v$. Seien $\overline{x}_i$ die Bilder in $\mathcal{O}_v/(\pi)$. Dies ist ein endlicher Körper. Nach dem Schubfachprinzip enthält eine Restklasse unendlich viele Elemente, d.h. eine Teilfolge ist konstant modulo $\pi$. Iteration dieses Argumentes

liefert Teilfolgen, die konstant sind modulo $\pi^2$, dann modulo $\pi^3$. Die Diagonalfolge wird für $i$ groß genug konstant modulo $\pi^n$, d.h. $v(x_i - x_j) \geq n$ für $i, j$ groß genug. Die $x_i$ bilden eine Cauchy-Folge. Der Grenzwert existiert dann in $\mathcal{O}_v$. Abgeschlossene Kugeln in $K_v$ sind von der Form $x + \pi^r \mathcal{O}_v$, also kompakt. □

**Satz 7.13.** *Sei $k$ ein lokaler Körper ungleich $\mathbb{R}, \mathbb{C}$ mit Ganzheitsring $\mathcal{O}_k$, $E/k$ endlich und $\mathcal{O}_E$ der ganze Abschluss von $\mathcal{O}_k$ in $E$.*

*(i) $\mathcal{O}_E$ ist diskreter Bewertungsring.*

*(ii) Der kanonische Betrag auf $k$ setzt sich eindeutig nach $E$ fort und gehört zum maximalen Ideal von $\mathcal{O}_E$.*

*(iii) $E$ ist bezüglich dieses Betrages vollständig und lokalkompakt.*

**Bemerkung.** Die analoge Aussage für $\mathbb{R}$ gilt ebenfalls, Übungsaufgabe.

*Beweis:* Wie im globalen Fall ist $\mathcal{O}_E$ endlich erzeugter $\mathcal{O}_k$-Modul, und damit auch ein Dedekindring. Sei $\mathfrak{P}$ ein Primideal von $\mathcal{O}_E$. Der Betrag zu $\mathfrak{P}$ setzt dann den zu $\mathfrak{p}$ fort. Dies zeigt die Existenz. Aus der Eindeutigkeit folgt auch, dass $\mathcal{O}_E$ nur ein maximales Ideal hat.
Seien $|\cdot|_1$ und $|\cdot|_2$ zwei Fortsetzungen nach $E$.

**Behauptung.** $|\cdot|_1 = |\cdot|_2$

Wie in der reellen Analysis zeigt man, dass $E$ vollständig und lokalkompakt ist. Ebenso zeigt man (nur Lokalkompaktheit geht ein), dass sie äquivalent sind, d.h. dieselbe Topologie induzieren. Wir betrachten

$$\{x \in k \mid |x|_1 < 1\} = \{x \mid \lim_{n \to \infty} x^n = 0\}$$

Dies ist die gleiche Menge wie für $|\cdot|_2$, da Grenzwerte nur von der Topologie abhängen. Also:

$$|x|_1 > 1 \Leftrightarrow |x|_2 > 1$$

Die Topologie ist nicht diskret, da sie auf $k$ nicht diskret ist.
Sei also $y \in k$ mit $a = |y|_1 = |y|_2 > 1$. Wir betrachten nun $x \in E^*$. Dann gibt es $\alpha \geq 0$ mit $|x|_1 = a^\alpha$. Seien $m, n \in \mathbb{N}$ mit $m/n \geq \alpha$. Dann folgt

$$|x|_1 < |y|_1^{m/n} \Rightarrow \left|\frac{x^n}{y^m}\right|_1 < 1 \Rightarrow \left|\frac{x^n}{y^m}\right|_2 < 1 \Rightarrow |x|_2 < a^{m/n}$$

Ebenso argumentiert man für $m/n < \alpha \Rightarrow |x|_2 > a^{m/n}$. Da die Ungleichungen für alle $m, n$ gelten, erhalten wir $|x|_2 = a^\alpha$. □

**Bemerkung.** Insbesondere gilt für alle $\sigma \in \mathrm{Gal}(E/k)$ die Gleichung $|\sigma(x)| = |x|$, da $|\sigma \cdot|$ ein neuer kanonischer Betrag ist.

**Satz 7.14.** *Sei $K$ ein Zahlkörper, $k$ der Abschluss von $K$ bezüglich eines Betrages, der $|\cdot|_p$ fortsetzt. Dann ist $k$ eine endliche Erweiterung von $\mathbb{Q}_p$.*

*Beweis:* Wir betrachten das Kompositum $K\mathbb{Q}_p$, den Teilkörper von $K_v$, der von $K$ und $\mathbb{Q}_p$ erzeugt wird. Er ist endlich über $\mathbb{Q}_p$. Da $\mathbb{Q}_p$ lokalkompakt ist, ist es nun auch $K\mathbb{Q}_p$ (Satz 7.13) lokalkompakt und vollständig. Damit ist $K\mathbb{Q}_p = K_v$, also ist dieser Körper endlich. □

Dasselbe Argument liefert im Funktionenkörperfall eine endliche Erweiterung von $\mathbb{F}_p(t)_v$.

**Korollar 7.15.** *Sei $L/K$ Erweiterung globaler Körper, $\mathfrak{p} \in \operatorname{Spm} \mathcal{O}_K$, $\mathfrak{P}|\mathfrak{p}$ maximales Ideal von $\mathcal{O}_L$. Dann gilt*

*(i)* $[L_\mathfrak{P} : K_\mathfrak{p}] = e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})$

*(ii)* $\sum_{\mathfrak{P}|\mathfrak{p}} [L_\mathfrak{p} : K_\mathfrak{p}] = [L : K]$

*Beweis:* Die erste Ausage ist die Gradformel für die Erweiterung $L_\mathfrak{P}/K_\mathfrak{p}$. Wir bemerken nur, dass Restklassengrad und Verzweigungsindex lokal berechnet werden können. Für den Restklassengrad folgt dies auf Satz 7.12.
Sei $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. Dann ist $e(\mathfrak{P}/\mathfrak{p}) = v_\mathfrak{P}(\pi)$. Diese Formel gilt global wie lokal. □

**Bemerkung.** Wir tragen eine Definition nach: Die Komplettierung von $\mathbb{Z}$ bezüglich des $p$-adischen Betrags heißt $\mathbb{Z}_p$, die *ganzen $p$-adischen Zahlen*.

**Beispiel.** Sei $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{5})$. Sei $p$ eine Primzahl. Sei $|\cdot|_v$ ein Betrag von $L$, der $|\cdot|_p$ fortsetzt. Dann gilt

$$(|\sqrt{5}|_v)^2 = |\sqrt{5}|_p = \begin{cases} 1 & p \neq 5 \\ 1/5 & p = 5 \end{cases}$$

Hieraus folgt $|\sqrt{5}|_v = 1$ falls $p \neq 5$, $|\sqrt{5}|_v = 5^{\frac{-1}{2}}$. (Wir lesen insbesondere ab, dass 5 in der Erweiterung verzeigt ist.) Allgemein gilt, dass $L_v = \mathbb{Q}_p(\sqrt{5})$, also

$$[L_v : \mathbb{Q}_p] = 1 \Leftrightarrow \sqrt{5} \in \mathbb{Q}_p \Leftrightarrow \sqrt{5} \in \mathbb{Z}_p$$

Falls $\sqrt{5} \in \mathbb{Z}_p$, so ist 5 ein Quadrat in $\mathbb{Z}_p/(p) \cong \mathbb{Z}/(p)$. Für $p \neq 2, 5$ gilt auch die Rückrichtung (Henselsches Lemma/Liftungslemma aus der elementaren Zahlentheorie). Wir gehen die Fälle durch.

(i) $p \neq 2, 5$ und 5 ein Quadrat mod $p$. Dann ist $[L_v : \mathbb{Q}_p] = 1$ und $\kappa(v) = \kappa(p)$. Die Erweiterung ist rein zerlegt.

(ii) $p \neq 2, 5$ und 5 ein Quadrat mod $p$. Dann ist $[L_v : \mathbb{Q}_p] = 2$, $[\kappa(v) : \kappa(p)] = 2$, die Erweiterung ist träge.

(iii) $p = 5$: Wie wir oben gesehen haben, ist die Erweiterung verzweigt.

(iv) $p = 2$: In $\mathbb{F}_2$ ist 5 ein Quadrat, jedoch nicht modulo 25. Daher ist $[L_2 : \mathbb{Q}_p] = 2$. Die Erweiterung ist träge oder verzweigt. Es ist $|\sqrt{5}|_2 = 1$, diese Information hilft nicht weiter. Sei $\alpha = a + b\sqrt{5} \in \mathbb{Q}(\sqrt{5})$, also $a, b \in \mathbb{Q}_p$.

Zuerst wollen wir sehen, dass $a = u/2$, $b = v/2$ mit $u, v \in \mathbb{Z}_2$. Das Element ist ganz genau dann, wenn $|\alpha|_2 \leq 1$. Sei zunächst $|a|_2 \neq |b|_2$, dann ist

$$|a + b\sqrt{5}| = \max(|a|_2, |b|_2) \leq 1 \Rightarrow |a|_2, |b|_2 \leq 1$$

Schwieriger ist $|a|_2 = |b|_2$. Wir betrachten das charakeristische Polynom. $\alpha$ ist genau dann ganz, wenn $2a$ und $a^2 - 5b^2$ ganz sind, also $|2a|_2 \leq 1 \Rightarrow |a|_2 \leq 2$. Daher haben $a$ und $b$ die Form $a = u/2$, $b = v/2$ mit $u, v$ ganz. Nun wenden wir uns wieder der Verzweigungsfrage zu. $L_2/\mathbb{Q}_2$ ist genau dann verzweigt, wenn es ein Element $\pi \in L_2$ gibt mit $|\pi|_2 = 1/\sqrt{2}$. Dann gilt $|N(\pi)|_2 = |\pi|_2|\overline{\pi}|_2 = 1/2$, denn Elemente der Galoisgruppe lassen den Betrag invariant. Wir setzen $\pi = u/2 + v/2\sqrt{5}$ ein und erhalten

$$|u^2 - 5v^2|_2 = 2^{-3} \Leftrightarrow 8|u^2 - 5v^2, 16 \nmid u^2 - 5v^2$$

Die Quadratzahlen modulo 8 sind

$$0^2 = 4^2 = 0, (\pm 1)^2 = (\pm 3)^2 = 1, (\pm 2)^2 = 4$$

Ihr 5-Faches sind $0, 5, 4$. Gleichheit $u^2 = 5v^2$ ist nur lösbar mit $u, v \in \{0, 4 \mod 8\}$ oder $u, v \in \{\pm 2 \mod 8\}$. Im ersten Fall ist $v = 2u^2 = 0 \mod 16$. Im zweiten Fall ist $u, v \in \{\pm 2, \pm 10 \mod 16\}$ und $u^2, v^2 = 4 \mod 16$. Auf jeden Fall ist $u^2 = 5v^2 \mod 16$. Daher gibt es kein $\pi$, die Primzahl 2 ist unverzweigt.

Für $\mathbb{Q}(\sqrt{5})$ argumentieren wir genauso. Für die Primzahl 2 kommt es auf die Gleichung $|u^2 + 5v^2|_2 = 2^{-3}$ an. Dies ist lösbar mit $u = v = 2$. Das Primelement ist $\pi = 1 + \sqrt{-5}$. In diesem Fall ist 2 verzweigt.

Man kann also mit Hilfe der lokalen Körper das Zerlegungsverhalten von Primzahlen untersuchen, ohne den Ganzheitsring zu bestimmen!

**Korollar 7.16.** *Sei $L/K$ Galoiserweiterung lokaler Körper, $\mathfrak{P} \in \operatorname{Spm} \mathcal{O}_L$, $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_L$. Dann ist $L_\mathfrak{P}/K_\mathfrak{p}$ galoissch mit*

$$\operatorname{Gal}(L_\mathfrak{P}/K_\mathfrak{p}) = D_\mathfrak{P}$$

*Beweis:* Sei $\sigma \in \operatorname{Gal}(L/K)$. Die Operation von $\sigma$ setzt sich stetig auf die Komplettierung fort und induziert daher

$$\sigma : L_\mathfrak{P} \to L_{\sigma(\mathfrak{P})}$$

Sei nun $\sigma \in D_\mathfrak{P}$. d.h. $\sigma(\mathfrak{P}) = \mathfrak{P}$. Dies induziert dann einen Automorphismus von $L_\mathfrak{P}$. Wir haben eine natürliche Abbildung

$$D_\mathfrak{P} \to \operatorname{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$$

Diese ist injektiv, da $L \subset L_\mathfrak{P}$. Wegen

$$|D_\mathfrak{P}| = e(\mathfrak{P}/\mathfrak{p}) f(\mathfrak{P}/\mathfrak{p}) = [L_\mathfrak{P} : K_\mathfrak{p}]$$

ist die lokale Erweiterung galois und die natürliche Abbildung surjektiv. □

**Bemerkung.** Ein Element $x \in K$ ist genau dann ganz, wenn $x$ ganz in $K_{v_\mathfrak{p}}$ für alle maximalen Ideale $\mathfrak{p}$. Mit anderen Worten:

$$\mathcal{O}_K = \bigcap_{\mathfrak{p} \in \mathrm{Spm}(\mathcal{O}_K)} \mathcal{O}_{K,\mathfrak{p}} = K \cap \bigcap_{\mathfrak{p} \in \mathrm{Spm}(\mathcal{O}_K)} \mathcal{O}_{K_{v_\mathfrak{p}}}$$

*Beweis:* $x$ ist genau dann ganz, wenn $(x)$ ein ganzes Ideal, d.h. nach dem Struktursatz für Dedekindringe genau dann, wenn $v_\mathfrak{p}(x) \geq 0$ für alle $\mathfrak{p} \in \mathrm{Spm}(\mathcal{O}_K)$ wobei

$$(x) = \prod_{\mathfrak{p} \in \mathrm{Spm}(\mathcal{O}_K)} \mathfrak{p}^{v_\mathfrak{p}(x)}$$

Die Bewertung $v_\mathfrak{p}$ kann dann äquivalent in $K_{v_\mathfrak{p}}$ berechnet werden. □

Wir betrachten noch einmal den Funktionenkörperfall.

**Satz 7.17.** *Sei $K/\mathbb{F}_p(t)$ endlich, $\mathfrak{p} \subset \mathcal{O}_K$ maximales Ideal, $v$ die zu $\mathfrak{p}$ gehörige Bewertung. Sei $t_v \in \mathfrak{p} \setminus \mathfrak{p}^2$. Dann gilt*

$$\kappa(\mathfrak{p})((t_v)) \cong K_v$$

*Beweis:* Offensichtlich gibt es eine natürliche Abbildung $\mathbb{F}_p[t_v] \to \mathcal{O}_\mathfrak{p}$, die mit der Bewertung verträglich ist.
Wir wollen nun $\kappa(\mathfrak{p})$ nach $\mathcal{O}_\mathfrak{p}$ einbetten. Sei $q = |\kappa(\mathfrak{p})$. Dies ist eine Potenz von $p$. Sei $\overline{x} \in \kappa(\mathfrak{p})^*$ ein Erzeuger. Dann ist $\overline{x}$ Nullstelle von $X^{q-1} - 1$.

**Behauptung.** *$X^{q-1} - 1$ hat genau eine Nullstelle in $\mathcal{O}_\mathfrak{p}$ mit $x = \overline{x} \mod \mathfrak{p}$.*

Hierzu konstruieren wir eine Folge $x_n \in \mathcal{O}_\mathfrak{p}$ mit $x_{n+1} = x_n \mod \mathfrak{p}^n$ und $x_0 = \overline{x}$ mod $x$. Sei $x_n$ konstruiert. Wir machen den Ansatz:

$$x_{n+1} = x_n + t_v^n a$$

Einsetzen in die Gleichung ergibt

$$(x_n + t_v^n a)^{q-1} - 1 = x_n^{q-1} - 1 + (q-1)x_n^{q-2} t_v^n a + b t_v^{n+1}$$

für ein $b \in \mathcal{O}_\mathfrak{p}$. Nach Voraussetzung gilt

$$x_n^{q-1} - 1 = c t_v^n$$

Mit $a = (q-1)^{-1} c$ hat dann $x_{n+1}$ die gewünschte Eigenschaft. $x = \lim x_n$ erfüllt die Behauptung.
Der Teilkörper $\mathbb{F}_p(x) \subset \mathcal{O}_\mathfrak{p}$ ist dann isomorph zu $\mathbb{F}_q$. Wir erhalten eine natürliche Abbildung

$$\mathbb{F}_q[t_v] \to \mathcal{O}_\mathfrak{p}$$

verträglich mit Absolutbetrag. Diese setzt sich auf die Quotientenkörper und die Komplettierung fort, also

$$\mathbb{F}_q((t_v)) \to K_\mathfrak{p}$$

**Behauptung.** *Dies ist ein Isomorphismus.*

Es genügt zu zeigen, dass $\mathbb{F}_q[[t_v]] \cong \mathcal{O}_\mathfrak{p}$. Beides sind diskrete Bewertungsringe mit demselben Restklassenkörper und demselben Primelement $t_v$. Daher ist $\mathcal{O}_\mathfrak{p}/(t_v^n) \cong \mathbb{F}_q[[t_v]]/(t_v)^n$ für alle $n$. Daraus folgt die Behauptung. □

**Stichworte kommutative Algebra**

Komplettierung, inverser Limes, Henselsches Lemma

# Kapitel 8

# Endlichkeit der Klassenzahl

Unser Ziel ist es, im Zahlkörperfall die Endlichkeit der Klassengruppe zu zeigen. Im Funktionenkörperfall gilt die Aussage im wesentlichen auch, vielleicht kommen wir darauf zurück.

## Gittertheorie

**Definition 8.1.** *Eine Untergruppe $H \subset \mathbb{R}^n$ heißt* diskret*, wenn für jede kompakte Teilmenge $K \subset \mathbb{R}^n$ der Schnitt $K \cap H$ endlich ist.*

Eine Teilmenge $K$ ist kompakt, wenn jede offene Überdeckung eine endlich Teilüberdeckung hat. In $\mathbb{R}^n$ ist dies äquivalent dazu, dass jede Folge in $K$ ein konvergente Teilfolge hat, oder dazu, dass sie beschränkt und abgeschlossen ist (Heine-Borel).

**Beispiel.** $\mathbb{Z} \subset \mathbb{R}$ ist diskret.

**Satz 8.2.** *Sei $H \subset \mathbb{R}^n$ diskret. Dann wird $H$ von $r$ Vektoren erzeugt, die linear unabhängig über $\mathbb{R}$ sind. Insbesondere gilt $H \cong \mathbb{Z}^r$ mit $\leq n$.*

*Beweis:* Seien $e_1, \ldots, e_r \in H$ eine maximale $\mathbb{R}$-linear unabhängige Teilmenge. Sei

$$P = \left\{ \sum \alpha_i e_i \mid 0 \leq \alpha_i \leq 1 \right\} \subset \mathbb{R}^n$$

Diese Menge ist kompakt, also $P \cap H$ endlich. Sei $x \in H$. Dann ist $x = \sum \lambda_i e_i$ mit $\lambda_i \in \mathbb{R}$. Sei $x_1 = x - \sum [\lambda_i] e_i$, wobei $[\alpha]$ die kleinste ganze Zahl kleiner gleich $\alpha$ ist (Gaußklammer), also $0 \leq \alpha - [\alpha] < 1$. Dies bedeutet $x_1 \in P \cap H$. Also erzeugen die $e_i$ zusammen mit $P \cap H$ die Gruppe $H$. Wir konstruieren eine unendliche Folge $x_j \in H \cap P$, nämlich

$$x_j = jx - \sum [j\lambda_i] e_i$$

Da $P \cap H$ endlich ist, gibt es zwei Indices $j \neq k$ mit $x_j = x_k$. Es folgt

$$j\lambda_i - [j\lambda_i] = k\lambda_i - [k\lambda]_i \Leftrightarrow (j-k)\lambda_i = [j\lambda_i] - [k\lambda]$$

Insbesonder ist $\lambda_i$ rational. Damit liegt die endlich erzeugte abelsche Gruppe $H$ in dem $\mathbb{Q}$-Vektorraum, der von $e_1, \ldots, e_r$ erzeugt wird. Es folgt $H \cong \mathbb{Z}^r$. Die Erzeuger von $H$ sind linear unabhängig über $\mathbb{R}$, da $e_1, \ldots, e_r$ es sind. □

**Definition 8.3.** *Eine diskrete Untergruppe $H \subset \mathbb{R}^n$ vom Rang $n$ heißt* Gitter. *Sei $e = \{e_1, \ldots, e_n\}$ eine Basis von $H$. Dann heißt*

$$P_e = \left\{ \sum \alpha_i e_i \mid 0 \leq \alpha_i < 1 \right\}$$

Fundamentalparallelogramm *von $H$.*

**Beispiel.** $\mathbb{Z}^n \subset \mathbb{R}^n$ ist ein Gitter.

**Lemma 8.4.** *Das Volumen von $P_e$ bezüglich des Standardlebesgue-Maßes $\mu$ auf $\mathbb{R}^n$ ist unanhängig von der Wahl der Basis.*

Wir schreiben $\mathrm{vol}(H)$ für $\mu(P_e)$.

*Beweis:* $\mu$ induziert ein Maß $\overline{\mu}$ auf $\mathbb{R}^n/H$. Es gilt $\overline{\mu}(\mathbb{R}^n/H) = \mu(P_e)$. Oder: zweite Basis in Termen der ersten ausdrücken. Sie und ihr Inverses sind ganzzahlig, also die Determinante $\pm 1$. Der Absolutbetrag der Determinante taucht als Übergangsfaktor auf. (Forster Analysis 3, Bsp. (5.3)). □

**Theorem 8.5** (Minkowski)**.** *Sei $H \subset \mathbb{R}^n$ ein Gitter, $S \subset \mathbb{R}^n$ messbar mit $\mu(S) > \mathrm{vol}(H)$. Dann gibt es $x, y \in S$, $x \neq y$ mit $x - y \in H$.*

*Beweis:* Sei $e_1, \ldots, e_n$ eine Basis von $H$, $P_e$ das Fundamentalparallelogramm. Es gilt $\mathbb{R}^n = \bigcup_h h + P_e$ und daher

$$S = \dot{\bigcup_{h \in H}} S \cap (h + P_e)$$

Es folgt

$$\mu(S) = \sum_h \mu(S \cap (h + P_e) = \sum_h \mu((-h + S) \cap P_e) > \mu(P_e)$$

Also können die $(-h+S) \cap P_e)$ nicht paarweise disjunkt sein. Es gibt $h \neq h' \in H$ mit

$$P_e \cap (-h + S) \cap (-h' \cap S) \neq \emptyset$$

Also gibt es $x, y \in S$ mit $-h + x = -h' + y$. Wegen $x - y = h' - h$ liegt die Differenz in $H$ und ist ungleich 0. □

**Korollar 8.6.** *Sei $H \subset \mathbb{R}^n$ ein Gitter, $S$ messbare Teilmenge von $\mathbb{R}^n$, symmetrisch bezüglich 0 (d.h. $x \in S \Leftrightarrow -x \in S$) und konvex. Sei entweder*

*(i)* $\mu(S) > 2^n \mathrm{vol}(H)$ *oder*

*(ii)* $\mu(S) \geq 2^n \mathrm{vol}(H)$, *$S$ kompakt*

*Dann enthält $S \cap H$ einen Punkt ungleich 0.*

*Beweis:* Erster Fall: Sei $S' = \frac{1}{2}S$, also

$$\mu(S') = \frac{1}{2^n}\mu(S) > \mathrm{vol}(H)$$

Nach dem Theorem von Minkowski gibt es $x, y \in S'$ mit $0 \neq z = x - y \in H$. Es gilt $z = \frac{1}{2}(2x + (-2y)) \in S \cap H$ wie gewünscht.
Zweiter Fall: Wende den ersten Fall an auf $(1+\varepsilon)S$ mit $\varepsilon > 0$. Es folgt

$$(H \setminus \{0\}) \cap (1+\varepsilon)S \neq \emptyset$$

Dabei ist der Schnitt endlich, da $H$ diskret und $S$ kompakt. Dann ist auch

$$\bigcap_{\varepsilon > 0} (H \setminus \{0\}) \cap (1+\varepsilon)S \neq \emptyset$$

Ein Element im Schnitt liegt in $H \setminus \{0\}$ und in $\bigcap_{\varepsilon>0}(1+\varepsilon)S = S$. □

## Die kanonische Einbettung

Sei $K/\mathbb{Q}$ ein Zahlkörper, $n = [K : \mathbb{Q}]$. Dann gibt es $n$ verschiedene Körperhomomorphismen

$$\sigma_i : K \to \mathbb{C}$$

**Beispiel.** $K = \mathbb{Q}(\sqrt{d})$, $\sigma_i(\sqrt{d}) = \pm\sqrt{d}$.

Zwei Fälle sind zu unterscheiden: $\sigma_i = \overline{\sigma_i}$ (komplexe Konjugation) genau dann, wenn $\sigma_i(K) \subset \mathbb{R}$. In diesem Fall heißt $\sigma_i$ *reelle Einbettung.*
Andernfalls ist $\overline{\sigma_i} = \sigma_j$ für ein $j \neq i$. In diesem Fall heißt $\sigma_i$ *komplexe Einbettung.* $\sigma_i$ und $\sigma_j$ sind konjugiert.

**Bemerkung.** Jedes $\sigma_i$ induziert eine Absolutbetrag auf $K$ via $|x| = |\sigma_i(x)|$. Die Komplettierung von $K$ bezüglich dieses Absolutbetrages ist dann $\mathbb{R}$ bzw. $\mathbb{C}$ für reelle bzw. komplexe Einbettungen.

Sei $r_1$ die Anzahl der reellen Einbettungen von $K$, $r_2$ die Anzahl der Paare von komplexen Einbettungen, also $n = r_1 + 2r_2$. Wir nummerieren die $\sigma_i$ so, dass $\sigma_i$ reell für $i \leq r_1$, $\sigma_{r_1+i}$ konjugiert zu $\sigma_{r_1+r_2+i}$. Wir schreiben $r = r_1 + r_2$.

**Beispiel.** $K = \mathbb{Q}(\sqrt{d})$ $n = 2$. Falls $d > 0$: $r_1 = 2, r_2 = 0, r = 2$. Falls $d < 0$: $r_1 = 0, r_2 = 1, r = 1$.

**Definition 8.7.** *Die* kanonische Einbettung *ist*

$$\sigma : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$$

*via* $\alpha \mapsto (\sigma_1(\alpha), \ldots, \sigma_r(\alpha))$.

**Bemerkung.** $\sigma$ ist ein injektiver Ringhomomorphismus.

**Satz 8.8.** *Sei $M \subset K$ freier $\mathbb{Z}$-Untermodul vom Rang $n$, $x_1, \dots, x_n$ Basis von $M$. Dann ist $\sigma(M)$ ein Gitter in $\mathbb{R}^n$ mit Volumen*

$$\mathrm{vol}(\sigma(M)) = 2^{-r_2} |\det(\sigma_i(x_j)_{i,j=1}^n)|$$

*Beweis:* $\sigma(x_i)$ ist der Vektor

$$(\sigma_1(x_i), \dots, \sigma_{r_1}(x_i), \mathrm{Re}\sigma_{r_1+1}(x_i), \mathrm{Im}\sigma_{r_1+1}(x_i), \dots, \mathrm{Re}\sigma_r(x_i), \mathrm{Im}\sigma_r(x_i))$$

Zu berechnen $\mathrm{vol}(\sigma(M)) = |\det(\sigma(x_i))|$. Falls diese Zahl ungleich 0 ist, sind die $\sigma(x_i)$ linear unabhängig über $\mathbb{R}$ und spannen ein Gitter auf.
Es gilt $\mathrm{Re}z = \frac{1}{2}(z + \overline{z}), \mathrm{Im}z = \frac{1}{2i}(z - \overline{z})$. Es folgt

$$\begin{aligned}(\mathrm{Re}\sigma_{r_1+j}(x_i), \mathrm{Im}\sigma_{r_1+j}(x_i)) &= \left(\frac{1}{2}(\sigma_{r_1+j}(x_i) + \overline{\sigma_{r_1+j}(x_i)}), \frac{1}{2i}(\sigma_{r_1+j}(x_i) - \overline{\sigma_{r_1+j}(x_i)})\right) \\ &= \left(\frac{1}{2}(\sigma_{r_1+j}(x_i) + \sigma_{r+j}(x_i)), \frac{1}{2i}(\sigma_{r_1+j}(x_i) - \sigma_{r+j}(x_i))\right)\end{aligned}$$

Hieraus berechnen wir den Absolutbetrag der Determinante via Multilinearlität. Im ersten Schritt ignorieren wir den Faktor $\frac{1}{i}$, der den Betrag 1 hat. Dann beachten wir

$$\det(\dots, \frac{1}{2}(a+b), \frac{1}{2}(a-b), \dots) = -\frac{1}{2}\det(\dots, a, b, \dots)$$

und schließlich sortieren wir die $\sigma_i$ um. Wir erhalten

$$|\det(\sigma(x_i)) = |\frac{1}{2^{r_2}}\det(\sigma_j(x_i))|$$

Diese Determinante ist ungleich 0, da die Charaktere $\sigma_j$ linear unabhängig sind. □

**Korollar 8.9.** *Sei $\mathcal{O}_K \subset K$ der Ganzheitsring. Dann ist $\sigma(\mathcal{O}_K) \subset \mathbb{R}^n$ ein Gitter mit Volumen*

$$\mathrm{vol}(\sigma(\mathcal{O}_K)) = 2^{-r_2} d^{1/2}$$

*wobei $(d) = \mathcal{D}_{\mathcal{O}_K/\mathbb{Z}}$, $d \in \mathbb{N}_0$ die* absolute Diskriminante *ist.*

*Beweis:* Im Beweis von Satz 2.18 haben wir

$$D(x_1, \dots, x_n) = \det(\sigma_i(x_j))^2$$

gezeigt. $D(x_1, \dots, x_n) = \det(\mathrm{Tr}_{\mathcal{O}/\mathbb{Z}}(x_i x_j))$ war die Diskriminante, $\mathcal{D}_{\mathcal{O}/\mathbb{Z}}$ das von ihre erzeugte Hauptideal. □

**Korollar 8.10.** *Sei $I \subset \mathcal{O}_K$ ein Ideal ungleich 0. Dann ist $\sigma(I)$ ein Gitter mit Volumen*

$$\mathrm{vol}(\sigma(I)) = 2^{r_2} d^{1/2} N(I)$$

*wobei $N(I) = |\mathcal{O}_K/I|$ die Norm des Ideals ist.*

*Beweis:* $I \subset \mathcal{O}_K$ ist freier $\mathbb{Z}$-Modul vom Rang $n$. Auch $\sigma(I)$ ist ein Gitter. Wir wählen eine Basis $x_1, \ldots, x_n$ von $\mathcal{O}_K$ nach dem Elementarteilersatz so, dass gleichzeitig $\lambda_1 x_1, \ldots, \lambda_n x_n$ für gewisse $\lambda_i \in \mathbb{N}$ eine Basis von $I$ ist. Damit gilt

$$N(I) = \lambda_1 \ldots \lambda_n$$

Andererseits ist

$$\mathrm{vol}(\sigma(I)) = \frac{1}{2^{r_2}} |\det(\sigma(\lambda_i x_i))| = \frac{1}{2^{r_2}} |\lambda_1 \ldots \lambda_n \det(\sigma(x_i))| = N(I)\mathrm{vol}(\sigma(\mathcal{O}))$$

□

**Satz 8.11.** *Sei $K$ ein Zahlkörper vom Grad $n$ über $\mathbb{Q}$, $r_1$ die Anzahl der reellen, $r_2$ die Anzahl der Paare von komplexen Einbettungen, $d$ die Diskriminante über $\mathbb{Q}$. Sei $I$ ein Ideal des Ganzheitsrings. Dann enthält $I$ ein Element $x \neq 0$ mit*

$$|N_{K/\mathbb{Q}}(x)| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} d^{1/2} N(I)$$

*Beweis:* Wir betrachten die kanonische Einbettung $\sigma : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Sei $t > 0$ reell,

$$B_t = \left\{ (y_1, \ldots, y_{r_1}, z_1, \ldots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid \sum |y_i| + 2 \sum |z_j| \leq t \right\}$$

ist kompakt, konvex, symmetrisch bezüglich 0.

**Behauptung.** $\mu(B_t) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!}$

Diese Formel wird durch Induktion nach $r_1$, $r_2$ gezeigt. Sei $V(r_1, r_2, t) = \mu(B_t)$.

(i) Es gilt

$$V(1, 0, t) = \mu(\{y_1 \mid |y_1| \leq t\}) = 2t = 2^1 (\pi/2)^0 \frac{t^1}{1!}$$
$$V(0, 1, t) = \mu(\{z_1 \mid 2|z_1| \leq t\}) = \pi(t/2)^2 = 2^0 (\pi/2)^1 \frac{t^2}{2!}$$

(ii) $r_1 \mapsto r_1 + 1$

$$\begin{aligned} V(r_1 + 1, r_2, t) &= \mu(\{(y_0, \ldots, y_{r_1}, z_1, \ldots, z_{r_2}) \mid \ldots\} \\ &= \int_{\mathbb{R}} V(r_1, r_2, t - |y_0|) dy_0 \\ &= \int_{-t}^{t} 2^{r_1} (\pi/2)^{r_2} \frac{(t - |y_0|)^n}{n!} dy_0 \\ &= 2^{r_1} (\pi/2)^{r_2} \frac{2}{n!} \int_0^t (t - y_0)^n dy_0 \\ &= 2^{r_1} (\pi/2)^{r_2} \frac{1}{n!} \left. \frac{-(t - y_0)^{n+1}}{n+1} \right|_0^t \\ &= 2^{r_1+1} (\pi/2)^{r_2} \frac{t^{n+1}}{(n+1)!} \end{aligned}$$

(iii) $r_2 \mapsto r_2 + 1$

$$\begin{aligned} V(r_1, r_2+1, t) &= \mu(\{(y_1, \dots, y_{r_1}, z_0, \dots, z_{r_2}) \mid \dots\} \\ &= \int_{\mathbb{C}} V(r_1, r_2, t - 2|z_0|) d\mu(z_0) \\ &= \int_{|z_0| \le t/2} V(r_1, r_2, t - 2|z_0|) d\mu(z_0) \\ &= \int_0^{t/2} \int_0^{2\pi} 2^{r_1} (\pi/2)^{r_2} \frac{(t-2\varrho)^n}{n!} \varrho d\varrho d\theta \\ &= 2^{r_1} (\pi/2)^{r_2} \frac{2\pi}{n!} \int_0^{t/2} (t-2\varrho)^n \varrho d\varrho \\ &= 2^{r_1} (\pi/2)^{r_2+1} \frac{t^{n+2}}{(n+2)!} \end{aligned}$$

wobei in Polarkoordinaten $z_0 = \varrho e^{i\theta}$, $d\mu(z_0) = \varrho d\varrho d\theta$, und in der letzten Zeile partielle Integration $\int u'v = uv - \int uv'$ benutzt wird

$$\begin{aligned} \int_0^{t/2} (t-2\varrho)^n \varrho d\varrho &= \int_0^x (t-x)^n x/2 dx/2 \\ &= 1/4 \left[ \frac{-(t-x)^{n+1}}{n+1} x \Big|_0^x - \int_0^x \frac{-(t-x)^{n+1}}{(n+1)} dx \right] \\ &= 1/4 \left[ 0 - \frac{(t-x)^{n+2}}{(n+1)(n+2)} \Big|_0^x \right] \\ &= 1/4 \frac{t^{n+2}}{(n+1)(n+2)} \end{aligned}$$

Damit ist die Formel für das Volumen verifiziert. Wähle nun $t$ so, dass $\mu(B_t) = 2^n \mathrm{vol}(\sigma(I))$, d.h.

$$2^{r_1} (\pi/2)^{r_2} \frac{t^n}{n!} = 2^{n-r_2} d^{1/2} N(I) \Rightarrow t^n = 2^{n-r_1} \pi^{-r_2} n! d^{1/2} N(I)$$

Aus dem Theorem von Minkowski, genauer Korollar 8.6 folgt die Existenz eines $0 \neq x \in I$ mit $\sigma(x) \in B_t$ so dass

$$\begin{aligned} |N(x)| = \prod_{i=1}^n |\sigma_i(x)| &= \prod_{i=1}^{r_1} |\sigma_i(x)| \prod_{j=r_1+1}^{r_1+r_2} |\sigma_j(x)|^2 \\ &\le \left[ 1/n \sum_{i=1}^n |\sigma_i(x)| + 2/n \sum_{i=r_1+1}^{r_1+r_2} |\sigma_j(x)| \right]^n \\ &\le (t/n)^n \\ &= 2^{n-r_1} \pi^{-r_2} n! / n^n d^{1/2} N(I) \end{aligned}$$

da das geometrische Mittel kleiner ist als das arithmetische Mittel. □

**Korollar 8.12.** *Jede Idealklasse von $K$ enthält ein ganzes Ideal $J$ mit*

$$N(J) \leq (4/\pi)^{r_2} \frac{n!}{n^n} d^{1/2}$$

*Beweis:* Sei $J'$ ein Ideal, ohne Einschränkung ist $I = J'^{-1}$ ein ganzes Ideal. Sei $x$ wie im Satz, $J = xJ' = xI^{-1}$. Es gilt

$$N(J) = N(x)N(I)^{-1} \leq (4/\pi)^{r_2} \frac{n!}{n^n} d^{1/2} \frac{N(I)}{N(I)}$$

□

**Theorem 8.13** (Dirichlet)**.** *Die Klassengruppe eines Zahlkörpers ist endlich.*

*Beweis:* Nach Korollar 8.12 genügt es, Klassen von Idealen zu betrachten, deren Norm kleiner gleich einer Konstante $C$ ist. Also genügt es zu zeigen, dass es nur endlich viele Ideale mit $N(J) = q < C$ gibt für ein festes $q$. Es gilt

$$N(J) = |\mathcal{O}_K/J| = q \Rightarrow q \in J$$

Die Ideale von $\mathcal{O}_K$ mit $q \in J$ entsprechen genau den Idealen von $\mathcal{O}_K/(q)$. Dies ist ein endlicher Ring, hat also auch nur endlich viele Ideale. □

**Beispiel.** $K = \mathbb{Q}(\sqrt{-5})$, $r_1 = 0$, $r_2 = 1$, $n = 2$, Basis $1, \sqrt{-5}$. Also folgt

$$d = |\det \begin{pmatrix} 1 & \sqrt{-5} \\ 1 & -\sqrt{-5} \end{pmatrix}|^2 = |-\sqrt{-5} - \sqrt{-5}|^2 = 4 \cdot 5 = 20$$

Die Konstante aus dem Beweis ist also

$$C = \frac{4}{\pi} \frac{2}{4} 2\sqrt{5} = 4/\pi\sqrt{5} = 2,847\ldots$$

Für $1 \in J$ ist $J = A$ das triviale Element. Ideale mit $2 \in J$ entsprechen den Idealen von $\mathbb{Z}[\sqrt{-5}]/(2) = \mathcal{O}/P_2^2$ wobei $P_2$ das eindeutige Primideal ist, das 2 enthält. Die Klassengruppe wird also von $P_2$ erzeugt. Es gilt $P_2^2 = (2)$, also die Relation $P_2^2 \sim 1$. Da $\mathbb{Z}[\sqrt{-5}]$ kein Hauptidealring ist, ist die Klassengruppe isomorph zu $\mathbb{Z}/2$.

**Korollar 8.14.** *Sei $K$ ein Zahlkörper vom Grad $n$ über $\mathbb{Q}$ und Diskriminante $d$. Für $n \geq 2$ gilt*

$$d \geq \frac{\pi}{3} \left( \frac{(3\pi}{4} \right)^{n-1}$$

*Der Quotient $n/\log d$ wird durch eine Konstante unabhängig von $K$ beschränkt.*

*Beweis:* Sei wie im Beweis des Theorems $J$ ein ganzes Ideal mit

$$N(J) \leq (4/\pi)^{r_2} \frac{n!}{n^n} d^{1/2}$$

Wegen $N(J) \geq 1$ folgt

$$\begin{aligned} d^{1/2} &\geq (\pi/4)^{r_2} n^n/n! \Rightarrow \\ d &\geq (\pi/4)^{2r_2} n^{2n}/(n!)^2 \geq (\pi/4)^n n^{2n}/(n!)^2 = a_n \end{aligned}$$

da $n \geq 2r_2$ und $\pi/4 < 1$.

**Behauptung.** $a_n \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}$.

Wir zeigen dies induktiv. Für $n = 2$ gilt wie gewünscht

$$a_2 = \pi^2/4^2 \cdot 2^4/2^2 = \pi^2/4 \ .$$

Nun $a_n \mapsto a_{n+1}$:

$$\begin{aligned} \frac{a_{n+1}}{a_n} &= \frac{\pi}{4} \cdot \frac{(n+1)^{2(n+1)} n!^2}{n^{2n}(n+1)^2} \\ &= \pi/4 \cdot \frac{(n+1)^{2n}}{n^{2n}} = \pi/4(1+1/n)^{2n} \\ &\geq \pi/4 \cdot (1 + 2n \cdot 1/n) = \pi/4 \cdot 3 \end{aligned}$$

Die zweite Aussage folgt durch Logarithmieren der Ungleichung. □

**Theorem 8.15** (Hasse-Minkowski)**.** *Sei $K \neq \mathbb{Q}$ ein Zahlkörper. Dann ist seine Diskriminante ungleich* 1*. Jede echte Erweiterung von $\mathbb{Q}$ ist verzweigt.*

*Beweis:* $d \geq \pi/3 \cdot (3\pi/4)^{n-1} > 1$ □

**Theorem 8.16** (Hermite)**.** *Bis auf Isomorphie gibt es nur endlich viele Zahlkörper mit gegebenener Diskriminante.*

*Beweis:* Nach Korollar 8.14 gilt $n \leq \alpha \log d$ für eine Konstante $\alpha$, d.h. der Grad ist beschränkt. Es genügt also zu zeigen, dass es nur endlich viele Körper mit gegebenem $d, n, r_1, r_2$ gibt. Sei zunächst $r_1 > 0$. Wir betrachten $B \subset \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ definiert durch

$$\{|y_1| \leq C/2, |y_i| \leq 1/2 \text{ für } i = 2, \ldots, r_1, |z_j| \leq 1/2 \text{ für } j = 1, \ldots, r_2\}$$

wobei $C = (\pi/4)^{-r_2} 2^{n-r_2} d^{1/2}$. Die Menge $B$ ist konvex, kompakt und punktsymmetrisch bezüglich 0. Das Volumen ist

$$\mu(B) = C(1)^{r_1-1}(\pi/4)^{r_2} = 2^n \text{vol}(\sigma(\mathcal{O}))$$

nach Wahl von $C$. Nach Korollar 8.6 gibt es $0 \neq x \in \mathcal{O} \cap B$.

**Behauptung.** $K = \mathbb{Q}(x)$

Nach Voraussetzung ist $|\sigma_i(x)| \leq 1/2$ für alle $i \neq 1$. Wegen

$$N(x) = \prod_{i=1}^{n} |\sigma_i(x)| \geq 1$$

folgt $\sigma_1(x) \geq 1$, insbesondere $\sigma_1(x) \neq \sigma_i(x)$ für alle $i \neq 1$. Wäre $x$ nicht primitiv, so käme jedes Element in der Menge der $\sigma_i(x)$ mehrfach vor, also auch $\sigma_1(x)$. Folglich gilt $[\mathbb{Q}(x) : \mathbb{Q}] = n$. Dies zeigt die Behauptung.
Wegen $\sigma(x) \in B$ sind die $\sigma_i(x)$ beschränkt und damit auch alle Koeffizienten des Minimalpolynoms von $x$. Es gibt nur endlich viele Polynome in $\mathbb{Z}[X]$ vom Grad $n$ mit beschränkten Koeffizienten, also auch nur endliche viele mögliche $x$.
Es bleibt der Fall $r_1 = 0$. In diesem Fall benutzen wir

$$B = \{|\mathrm{Im} z_1| \leq C, |\mathrm{Re} z_1| \leq 1/2, |z_i| \leq 1/2 \text{ für } i = 2, \ldots, r_2\}$$

so dass $\mu(B) = 2^n \mathrm{vol}(B)$. Wie im ersten Fall finden wir $x \in \sigma(\mathcal{O}) \cap B$ mit $|\sigma_1(x)| \geq 1$. Wiederum ist $\sigma_1(x) \neq \sigma_i(x)$ für $i \neq 1$. Wegen $\mathrm{Re}\sigma_1(x) \leq 1/2$ ist $\mathrm{Im}\sigma_1(x) \neq 0$, also ist auch $\sigma_1(x) \neq \overline{\sigma}_1(x)$. Wieder ist $x$ primitives Element. $\square$

# Kapitel 9

# Die Einheitengruppe

**Definition 9.1.** *Sei $K$ ein Zahlkörper. Die* Einheiten *von $K$ sind die invertierbaren Elemente des Ganzheitsrings.*

**Beispiel.** $1, -1, i, -i$ sind Einheiten von $\mathbb{Q}(i)$. In $\mathbb{Q}(\sqrt{3})$ ist $2+\sqrt{3}$ eine Einheit mit Inversem $2-\sqrt{3}$.

**Lemma 9.2.** *$x \in K$ ist eine Einheit genau dann, wenn $x$ ganz ist und $N(x) = \pm 1$.*

*Beweis:* Ist $x$ eine Einheit, so ist $1 = N(xx^{-1}) = N(x)N(x)^{-1}$. Da die Norm eines ganzen Elementes ganz ist, folgt $N(x) = \pm 1$. Sei umgekehrt $x \in \mathcal{O}_K$ mit $N(x) = \pm 1$. Das charakteristische Polynom

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

hat ganze Koeffizienten, speziell $a_0 = \pm N(x) = \pm 1$. Es folgt

$$\pm x(x^{n-1} + \cdots + a_1) = 1$$

Damit ist $x$ eine Einheit. □

**Theorem 9.3** (Dirichlet)**.** *Sei $K$ ein Zahlkörper, $r_1$ die Zahl der reellen und $r_2$ die Zahl der komplexen Einbettungen, $r = r_1 + r_2$. Die Gruppe $\mathcal{O}_K^*$ der Einheiten von $K$ ist isomorph zu*

$$\mathcal{O}_K^* \cong \mathbb{Z}^{r-1} \times G$$

*wobei $G$ die Gruppe der Einheitswurzeln in $K$ ist, insbesondere eine endliche, zyklische Gruppe.*

**Beispiel.** Für $K = \mathbb{Q}(i)$ gilt $\mathcal{O}_K^* \cong G = \{\pm 1, \pm i\}$, da $r = 0+1$. Für $K = \mathbb{Q}(\sqrt{3})$ gilt $\mathcal{O}_K^* \cong \{\pm 1\} \times \mathbb{Z}$, da $r = 2 + 0$. Tatsächlich ist $2 + \sqrt{3}$ ein Erzeuger der freien Untergruppe. Die Frage nach Erzeugern von $\mathbb{Q}(\sqrt{d})$ für $d > 0$ führt auf die Theorie der *Pellschen Gleichung*, die mit der Theorie der Kettenbrüche behandelt werden kann.

*Beweis:* Seien wie bisher $\sigma_1, \ldots, \sigma_{r_1}$ die reellen Einbettungen, $\sigma_{r_1}, \ldots, \sigma_r$ nichtkonjugierte komplexe Einbettungen. Die *logarithische Einbettung* $L : K^* \to \mathbb{R}^r$ ist

$$L : x \mapsto (\log|\sigma_1|, \ldots, \log|\sigma_r|) \in \mathbb{R}$$

$L$ ist ein Gruppenhomomorphismus.
Sei $B \subset \mathbb{R}^r$ kompakt, $B' = L^{-1}(B) \cap \mathcal{O}_K^*$. Dann gibt es eine Konstante $C$, so dass für alle $x \in B'$ und $i = 1, \ldots, n$ gilt

$$|\sigma_i(x)| \leq C$$

Damit sind die Koeffizienten von

$$P(X) = (X - \sigma_1(x))(X - \sigma_2(x)) \ldots (X - \sigma_n(x))$$

beschränkt. Gleichzeitig sind sie ganz, da $x \in \mathcal{O}_K$. Es gibt also nur endliche viele mögliche $P$, daher ist $B'$ endlich.
Dies gilt insbesondere für $G = L^{-1}(0) \cap \mathcal{O}_K^*$. Dies ist eine endliche Gruppe, besteht also nur aus endlich vielen Einheitswurzeln. Insbesondere ist sie zyklisch (Algebra). Ist umgekehrt $\omega$ eine Einheitswurzel, so gilt $|\sigma_i(\omega)| = 1$ für alle $i$. Damit liegt $\omega$ im Kern von $L$.
Nun studieren wir das Bild von $L(\mathcal{O}_K^*) \subset \mathbb{R}^r$. Nach unserer Vorüberlegung ist dies eine diskrete Untergruppe, also $L(\mathcal{O}_K^*) \cong \mathbb{Z}^s$ für $s \leq r$.

**Behauptung.** $s \leq r - 1$.

Für $x \in \mathcal{O}_K^*$ gilt

$$\pm 1 = N(x) = \prod_{i=1}^{n} \sigma_i(x) = \prod_{i=1}^{r_1} \sigma_i(x) \prod_{j=r_1+1}^{r_2} \sigma_i(x)\overline{\sigma_i(x)}$$

Hieraus folgt

$$L(x) \in W = \left\{ (y_1, \ldots, y_r) \in \mathbb{R}^r \mid \sum_{i=1}^{r_1} y_i + 2 \sum_{j=r_1+1}^{r_2} y_j = 0 \right\}$$

$W$ hat Dimension $r - 1$, $L(\mathcal{O}^*)$ ist eine diskrete Untergruppe, also $s \leq r - 1$.

**Behauptung.** $L(\mathcal{O}^*)$ *enthält* $r - 1$ *linear unabhängige Elemente.*

Äquivalent: Für jede lineare Abbildung $f : W \to \mathbb{R}$ mit $f \neq 0$ gibt es $u \in \mathcal{O}_K^*$ mit $f(L(u)) \neq 0$. Wir identifizieren $W \cong \mathbb{R}^{r-1}$ via des Isomorphismus $(y_1, \ldots, y_r) \mapsto (y_1, \ldots, y_{r-1})$. Also schreibt sich $f(y_1, \ldots, y_r) = c_1 y_1 + \ldots c_{r-1} y_{r-1}$ für $c_i \in \mathbb{R}$. Wir wählen

$$\alpha \geq \left(\frac{2}{\pi}\right)^{r_2} d^{1/2}, \qquad \beta > \sum_{i=1}^{r-1} c_i \log \alpha$$

Wir werden eine Folge $x_h \in \mathcal{O}_K \setminus \{0\}$ konstruieren mit

$$|f(L(x_h)) - 2\beta h| < \beta, |N(x_h)| \leq \alpha$$

Aus der ersten Bedingung folgt $(2h-1)\beta < f(L(x_h)) < (2h+1)\beta$, also sind die $f(L(x_h))$ paarweise verschieden. Die $|N(x_h)|$ sind beschränkt und ganz, also gibt es nur endliche viele Ideale $(x_h)$. Also gibt es zwei Indizes $h, h'$ mit $(x_h) = (x_{h'})$. Dies bedeutet, dass es $u \in \mathcal{O}_K^*$ gibt mit $x_h = ux_{h'}$. Außerdem

$$f(L(u)) = f(L(x_h)) - f(L(x_{h'})) \neq 0$$

Damit wäre das Theorem gezeigt.
Wir konstruieren nun die $x_h$. Wähle $\lambda_1, \ldots, \lambda_r$ mit

$$\prod_{i=1}^{r_1} \lambda_i \prod_{j=r_1+1}^{r} \lambda_j^2 = \alpha, \qquad \sum_{i=1}^{r-1} c_i \log \lambda_i = 2\beta h$$

Dies ist möglich für $r \geq 2$. Im Fall $r = 1$ ist $s = 0$, und es ist nichts zu zeigen. Sei nun

$$B = \{(y_i, z_j) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid |y_i| \leq \lambda_i, |z_j| \leq \lambda_{j+r_r}\}$$

Diese Menge ist kompakt, symmetrisch und konvex. Sie hat das Maß

$$\begin{aligned}\mu(B) = \prod_{i=1}^{r_1}(2\lambda_i) \prod_{j=1}^{r_2} \pi\lambda_j^2 &= 2^{r_1}\pi^{r_2}\alpha \\ &\geq 2^{r_1}\pi^{r_2}\left(\frac{2}{\pi}\right)^{r_2} d^{1/2} = 2^{n-r_2}d^{1/2} = 2^n \mathrm{vol}(\sigma(\mathcal{O}_K))\end{aligned}$$

Nach dem Theorem von Minkowski, Korollar 8.6 gibt es $x \in \mathcal{O}_K$, $x \neq 0$ mit $|\sigma_i(x)| \leq \lambda_i$ für alle $i$. Andererseits

$$|\sigma_i(x)| = \frac{|N(x)|}{\prod_{j\neq i} |\sigma_j(x)|} \geq \frac{1}{\prod_{j\neq i} \lambda_j} = \alpha^{-1}\lambda_i$$

Also

$$\begin{gathered}\lambda_i \alpha^{-1} \leq |\sigma_i(x)| \leq \lambda_i \Rightarrow \\ \log \lambda_i - \log \alpha \leq \log |\sigma_i(x)| \leq \log \lambda_i \Rightarrow \\ \log \alpha \geq \log \lambda_i - \log |\sigma_i(x)| \geq 0\end{gathered}$$

Wir überprüfen nun die gewünschten Eigenschaften von $x$:

$$\begin{aligned}|f(L(x)) - 2\beta h| &= \left|\sum_{i=1}^{r-1} c_i \log |\sigma_i(x)| - \sum_{i=1}^{r-1} c_i \log \lambda_i\right| \leq \sum_{i=1}^{r-1} |c_i| \log \alpha < \beta \\ |N(x)| &= \prod_{i=1}^{n} |\sigma_i(x)| \leq \prod_{i=1}^{n} \lambda_i = \alpha\end{aligned}$$

□

## Die analytische Klassenzahlformel

**Definition 9.4.** *Sei $K$ Zahlkörper vom Grad $n$ mit $r_1$ reellen und $r_2$ imaginär Einbettungen, $r = r_1 + r_2$. Seien $\varepsilon_1, \ldots, \varepsilon_{r-1}$ eine Basis des freien Anteils von $\mathcal{O}_K^*$. Seien $\sigma_1, \ldots, \sigma_r : K \to \mathbb{C}$ paarweise verschiedene und paarweise nicht konjugierte Einbettungen. Sei $N_i = 1$ falls $\sigma_i$ reell und $N_i = 2$, falls $\sigma_i$ imaginär. Dann heißt*

$$R_K = \left|\det(N_i \log|\sigma_i(\varepsilon_j)|_{i,j=1}^{r-1}\right|$$

Dirichlet-Regulator *von $K$.*

**Bemerkung.** Die letzte Einbettung $\sigma_r$ bleibt also unberücksichtigt!

**Definition 9.5.** *Sei $K$ Zahlkörper, $s$ eine komplexe Variable.*

$$\zeta_K(s) = \sum_I \frac{1}{N(I)^s}$$

*(hierbei durchlauft $I$ die ganzen Ideale ungleich 0) heißt* Dedekindsche Zeta-Funktion *von $K$.*

**Beispiel.** $K = \mathbb{Q}$, dann durchäuft $I$ die Menge $(n)$ für $n \in \mathbb{N}$, also

$$\zeta_{\mathbb{Q}}(s)) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

die Riemannsche Zeta-Funktion.

**Theorem 9.6.** *$\zeta_K$ konvergiert absolut und lokal gleichmäßig für* $\mathrm{Re}\, s > 1$ *und hat eine holomorphe Fortsetzung nach $\mathbb{C} \setminus \{1\}$. In 1 hat die Funktion einen einfachen Pol. Sie erfüllt eine Funktionalgleichung, die $s$ und $1 - s$ verbindet.*

*Beweis:* Z.B. Neukirch, Algebraic Number theory, Chapter VII, §5, Lang Algebraic Number theory VIII, §2. □

**Beispiel.** Sei $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ multiplikativ. Dabei sei $N$ minimal, so dass $\chi$ definiert ist. Solche Abbildunge heißen *Dirichlet-Charaktere*. Man setzt

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

Für den trivialen Charakter $\chi = 1$ erhält man die Riemannsche $\zeta$-Funktion zurück. Für $\chi \neq 1$ hat $L(\chi, s)$ eine holomorphe Fortsetzung auf ganz $\mathbb{C}$.
Sei $K = \mathbb{Q}(\zeta_N)$. Dann gilt

$$\zeta_K(s) = \prod_{\chi:(\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*} L(\chi, s)$$

Als Konsequenz hieraus erhält man den Dirichletschen Dichtesatz: Jede arithmetische Folge enthält unendliche viele Primzahlen.

Für meine eigene Forschung ist die folgenden Aussage der Startpunkt.

**Theorem 9.7** (Analytische Klassenzahlformel)**.** *Sei $K$ Zahlkörper vom Grad $n$ mit $r_1$ reellen und $r_2$ komplexen Einbettungen. Sei $w$ die Anzahl der Einheitswurzeln in $K$. Dann ist*

$$\mathrm{Res}_1 \zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} R_k h}{w d^{1(2}}$$

*Beweis:* Man betrachtet die partiellen Zeta-Funktionen, bei denen über die Ideale einer festen Klasse summiert wird. Dann heißt es sorgfältig abschätzen in unseren bisherigen Überlegungen. Wieder siehe Neukirch, Lang o.ä. □

**Bemerkung.** Die Formel wird einfacher für $s = 0$. Dort hat $\zeta_K$ meist eine Nullstelle. Der führende Koeffizient der Taylorentwicklung ist

$$-\frac{hR}{w}$$

Die Klassenzahlformel wird - sowohl theoretisch, als auch praktisch - benutzt, um die Klassenzahl zu berechnen. Alle anderen Terme, auch das Residuum sind leichter zu berechnen als die Klassenzahl.
**Ausblick:** Die analytische Klassenzahlformel wurde vermutungsweise verallgemeinert auf die Werte von Dedekindschen $\zeta$-Funktionen an allen ganzen Zahlen und sogar für die Werte von $L$-Funktionen von Varietäten oder Motiven an ganzen Zahlen. Den Beweis dieser Vermutung für zyklotomische Körper (bzw. für die $L(\chi, s)$ führte ich einer gemeinsamen Arbeit mit Guido Kings, Regensburg: A. Huber, G. Kings. Bloch-Kato conjecture and Main Conjecture of Iwasawa theory for Dirichlet characters. Duke Mathematical Journal 199(3): 393-464, 2003.

# Kapitel 10

# Adele und Idele

Wir werden in einer anderen Sprachen nocheinmal die Endlichkeit der Klassenzahl und den Einheitensatz beweisen. In dieser Form funktioniert alles auch für Funktionenkörper.
**Literatur:** A. Weil, Basic Number Theory, Kapitel IV.

Sei nun wieder $K$ ein globaler Körper. Eine *Stelle* von $K$ ist eine Äquivalenzklasse von Absolutbeträgen. Wir interessieren uns wie uns nur für die *kanonischen Stellen*, die zu den *kanonischen Beträgen* (Definition 7.7) gehören.

**Definition 10.1.** *Sei $S(K)$ die Menge der kanonischen Stellen, für $v \in S(K)$ sei $|\cdot|_v$ der kanonische Betrag, $K_v$ die Komplettierung bezüglich $v$. Wir nennen $v$* archimedisch*, falls $K_v = \mathbb{R}, \mathbb{C}$, andernfalls heißt $v$* nicht-archimedisch*. Für jeder nicht-archimedischen Stelle $v$ gehört der Absolutbetrag zu einer Bewertung $v : K^* \to \mathbb{Z}$. Wir normieren sie so, dass $v$ surjektiv ist. Es sei $\mathcal{O}_v$ der Ganzheitsring. Die Stellen von $K$, die zu einem Primideal von $\mathcal{O}_K$ gehören, heißen* endlich*, die übrigen* unendlich*. Ist $v$ endlich, so nennen wir das Primideal $\mathfrak{p}_v$. Sei $S_\infty$ die Menge der unendlichen Stellen.*

Im Zahlkörperfall stimmen archimedische und unendliche Stellen überein. Im Funktionenkörperfall sind alle Stellen nicht-archimedisch, aber es gibt dennoch unendliche Stellen.
Wir erinnern uns, dass $K_v$ ein lokalkompakter Körper ist.

**Definition 10.2.** *Für jede endliche Teilmenge $S \subset S(K)$ mit $S_\infty(K) \subset S$ seien*

$$\mathbb{A}_K(S) = \prod_{v \in S} K_v \times \prod_{v \notin S} \mathcal{O}_v$$

*die $S$-*Adele von $K$ *und*

$$I_K(S) = \prod_{v \in S} K_v^* \times \prod_{v \notin S} \mathcal{O}_v^*$$

*die* $S$-Idele von $K$. *Es sei*

$$\mathbb{A}_k = \bigcup_{S \subset S(K)} \mathbb{A}_K(S) \qquad I_K = \bigcup_{S \subset S(K)} I_K(S)$$

*die* Adele *bzw.* Idele *von* $K$.

Idel kommt wie Ideal von ideales Element, Adel ist ein additives Idel.

**Bemerkung.** Es gilt

$$A_K = \{(x_v)_{v \in S(K)} \in \prod_{v \in S(K)} K_v | x_v \text{ ganz für fast alle } v\}$$
$$I_K = \{(x_v)_{v \in S(K)} \in \prod_{v \in S(K)} K_v^* | x_v \in \mathcal{O}_v^* \text{ für fast alle } v\}$$

Die Adele bilden einen Ring bezüglich der komponentenweisen Addtion und Multipltiplikation. Die Idele bilden eine Gruppe bezüglich der komponentenweise Multiplikation. Es gilt

$$\mathbb{A}_K^* = I_K$$

*Beweis:* Sei $(x_v)_{v \in S(S)} \in \mathbb{A}_K^*$ mit Inversem $(y_v)$. Dann ist $x_v y_v = 1$ für alle $v$. Für fast alle $v$ ist $x_v, y_v \in \mathcal{O}_v$. Damit ist $x_v, y_v \in \mathcal{O}_v^*$. □

Nun berücksichtigen wir die Topologien.

**Definition 10.3.** $\mathbb{A}_K(S)$ *und* $I_K(S)$ *erhalten die Produkttopologien,* $\mathbb{A}_K$ *und* $I_K$ *die Limestopologien der Vereinigung.*

Eine Teilmenge von $\mathbb{A}_K$ ist offen, genau dann wenn ihr Schitt mit allen $\mathbb{A}_K(S)$ offen ist. Eine Teilmenge von $\mathbb{A}_K(S)$ ist offen, wenn sie Vereinigung von Mengen der folgenden Form ist:

$$U = \prod_{v \in S \cup T} U_v \times \prod_{v \notin S \cup T} Oh_v$$

wobei $T$ eine endliche Menge von Stellen, $U_v \subset K_v$ offen für $v \in S$ und $U_v \subset \mathcal{O}_v$ offen für $v \in T \setminus S$.

**Bemerkung.** $\mathbb{A}_K(S)$ und $\mathbb{A}_K$ sind lokalkompakte topologische Ringe, d.h. $+, -, \cdot$ sind stetig. $I_K(S)$ und $I_K$ sind lokalkompakte topologische Ringe, d.h. $\cdot, \cdot^{-1}$ sind stetig. $I_K$ trägt *nicht* die Teilraumtopologie von $\mathbb{A}_K$.

**Lemma 10.4.** *Für jedes* $S$ *ist* $I_K(S) \subset I_K$ *offen.*

*Beweis:* Es genügt zu zeigen, dass $I_K(S) \subset I_K(T)$ offen ist für alle endlichen $T \supset S$. Die beiden Prokukte stimmen in fast allen Faktoren überein. Für die Komponenten zu $v \in T \setminus S$ haben wir die Inklusion $\mathcal{O}_v \subset K_v$. Dies ist eine offene Teilmenge. □

Wir werden uns nun vor allem mit den Eigenschaften der Idele beschäftigen.

**Lemma 10.5.** *Sei $x \in K^*$. Dann ist $(x)_{v \in S(K)}$ ein Idel. Die Abbildung $K^* \to I_K$ ist injektiv.*

Die Abbildung wird *Diagonaleinbettung* genannt.

*Beweis:* Es $s \in \mathcal{O}_K$, so dass $sx \in \mathcal{O}_K$. Es genügt die Behauptung für $sx$ und $s$, also für Elemente $y \in \mathcal{O}_K \setminus \{0\}$ zu beweisen. Sei $v$ eine endliche Stelle. Es ist $v(y) \neq 0$ genau dann, wenn $v$ in der Primidealfaktorisierung von $y$ vorkommt. Das sind nur endlich viele $v$.
Die Abbildung ist injektiv, da $K \to K_v$ für jedes $v$ injektiv ist. □

**Definition 10.6.** *Ein Idel heißt* Hauptidel, *wenn es im Bild der Diagonalabbildung liegt.*

**Definition 10.7.** *Sei $x = (x_v) \in I_K$ ein Idel. Dann definieren wir das von $x$ definierte gebrochene Ideal als*

$$I(x) = \prod_{v \nmid \infty} \mathfrak{p}_v^{v(x_v)}$$

$I(x)$ ist wohldefiniert, da $v(x_v) = 0$ sobald $x_v \in \mathcal{O}_v^*$, also fast immer.

**Satz 10.8.** *Die Abbildung $I(\cdot)$ von $I_K$ in die Gruppe der invertierbaren Ideale induziert einen Gruppenisomorphismus*

$$I_K / K^* I_K(S_\infty) \to \mathrm{Cl}(K)$$

*Beweis:* Offensichtlich ist $I$ ein Gruppenhomormophismus. Wir zeigen, dass $I$ surjektiv ist. Sei

$$I = \prod_{v \nmid \infty} \mathfrak{p}_v^{n_v}$$

ein beliebiges gebrochenes Ideal. Wir wählen $x_v \in K_v$ mit $v(x_v) = n_v$. Da $n_v = 0$ für fast alle $v$, gilt $x_v \in \mathcal{O}_v^*$ für fast alle $v$. Für die unendlichen Stellen wählen wir $x_v = 1$. Damit ist das Idel $x = (x_v)$ das gesuchte Urbild.
Im Kern liegen diejenigen Idele $(x_v)_v$ mit $v(x_v) = 0$ für alle endlichen Stellen, d.h. mit $x_v \in \mathcal{O}_v^*$. Dies sind nach Definition die Elemente von $I_K(S_\infty)$.
$I$ bildet Hauptidele auf Hauptideale ab, und wir erhalten die Behauptung. □

**Definition 10.9.** *Sei $S \subset S_K$ eine endliche Menge von Stellen, die alle archimedischen Stellen enthält. Dann heißt*

$$\mathrm{Cl}_S(K) = I_K / K^* I_K(S)$$

$S$-Idelklassengruppe von $K$.

**Theorem 10.10.** *Für $S \neq \emptyset$ ist $\mathrm{Cl}_S(K)$ endlich. Im Funktionenkörperfall ist $\mathrm{Cl}_\emptyset(K) \cong \mathbb{Z} \times F$ für eine endliche Gruppe $F$.*

Für den Beweis holen wir aus.
**Korrektur:** Sei $v$ eine Stelle von $K$. Wir normalisieren $|\cdot|_v$ wie folgt:

$$|x|_v = \begin{cases} |x| & K_v = \mathbb{R} \\ |x|^2 & K_v = \mathbb{C} \\ N(\mathfrak{p}_v)^{-v(x)} & v \text{ nicht-archimedisch} \end{cases}$$

**Lemma 10.11.** *Die Abbildung*

$$|\cdot|_{\mathbb{A}_K} : I_K \to \mathbb{R}_{>0} \qquad (x_v)_{v \in S(K)} \mapsto \prod_v |x_v|_v$$

*ist ein wohldefinierter Gruppenhomomorphismus.*

*Beweis:* Für fast alle $v$ ist $x_v \in \mathcal{O}_v \Leftrightarrow |x_v|_v = 1$, d.h. nur endliche viele Faktoren sind ungleich 1. Die Abbildung ist multiplikativ, da die Körpernormen $|\cdot|_v$ es sind. □

Die Abbildung heißt *Adelnorm*. Der Kern wir mit $I_K^1$ (Gruppe der 1-Idele) bezeichnet.

**Satz 10.12** (Produktformel)**.**

$$K^* \subset I_K^1$$

*Beweis:* Sei $L/K$ eine Erweiterung globaler Körper. Sei $x \in L$, $v$ eine Stelle von $K$. Dann gilt

$$|N_{L/K}(x)|_v = \prod_{w|v} |x|_w$$

(Übungsaufgabe). Hieraus folgt sofort

$$|N_{L/K}(s)|_{\mathbb{A}_K} = |x|_{\mathbb{A}_L}$$

Daher muss die Behauptung nur für $K = \mathbb{Q}, \mathbb{F}_p(t)$ überprüft werden.
Sei $K = \mathbb{Q}$, $x = \pm p_1^{r_1} \dots p_n^{r_n}$ für verschiedene Primzahlen $p_i$. Dann ist

$$|x|_v = \begin{cases} p_1^{r_1} \dots p_n^{r_n} & v = \infty \\ p_i^{-r_i} & v = p_i \\ 1 & \text{sonst} \end{cases}$$

Das Produkt ist also 1.
Sei nun $K = \mathbb{F}_p(t)$. Ohne Einschränkung gehen wir von $K$ zu $\overline{F}_p(t)$ über. Es genügt $x = (t - a)$ für ein $a \in \overline{F}_p$ zu betrachten. Dann ist

$$|x|_v = \begin{cases} p^{-1} & v = a \\ p^1 & v = \infty \\ 1 & \text{sonst} \end{cases}$$

Das Produkt ist 1. □

Im Fall von Zahlkörpern ist das Bild der Normabbildung ganz $\mathbb{R}_{>0}$, im Falle von Funktionenkörpern der Charakteristik $p$ ist das Bild der Normaabbildung in den Potenzen von $p$ enthalten, also isomorph zu $\mathbb{Z}$.

**Lemma 10.13.**

$$I_K \cong \begin{cases} I_K^1 \times \mathbb{R}_{>0} & \mathrm{Char}(K) = 0 \\ I_K^1 \times \mathbb{Z} & \mathrm{Char}(K) > 0 \end{cases}$$

*Beweis:* Sei $K$ Zahlkörper, $v$ eine unendliche Stelle. Sei $x$ ein Idel mit Norm $a$. Wir wählen $y_v$ mit $|y_v|_v = a$ und $y_w = 1$ für $w \neq v$. Dann ist $y = (y_w)$ ein Idel mit Norm $a$ und $xy^{-1} \in I_K^1$.
Sei $K$ Funktionenkörper. Sei $n \geq 1$ minimal, so dass $p^n$ im Bild von $|\cdot|_{\mathbb{A}}$. Sei $y \in I_K$ mit $|y|_{\mathbb{A}} = p^n$. Sei nun $x$ ein beliebiges Adel. Dann ist $|x|_{\mathbb{A}} = |y|_{\mathbb{A}}^m$ für ein $m \in \mathbb{Z}$. Daher liegt $xy^{-m} \in I_K^1$. □

**Satz 10.14.** *$K^* \subset I_K^1$ ist diskret.*

*Beweis:* Es genügt, $K^* \subset I_K$ zu betrachten. Die Menge

$$U = \{(x_v) \in I_K(S_\infty) || x - 1|_v < 1/2 \text{ für alle } v|\infty\}$$

ist eine offene Umgebung von 1 in $I_K$. Sei $x \in U \cap K^*$. Dann ist $x \in \mathcal{O}_K^*$ und $x - 1 \in \mathcal{O}_K$.
Die Koeffizienten des Minimalpolynoms sind dann ganz und bezüglich $|\cdot|_\infty$ beschränkt. Im Zahlkörperfall haben wir bereits mehrfach genutzt, dass es dann nur endlich viele Möglichkeiten für die Koeffizienten gibt und daher auch nur endlich viele Möglichkeiten für $x - 1$.
Im Funktionenkörperall müssen wir zeigen:

**Behauptung.** *$\{x \in \mathbb{F}_p[t] || x|_\infty < C\}$ ist endlich.*

Nach Definition ist der Grad von $x$ beschränkt, die Aussage ist offensichtlich. □

**Theorem 10.15.** *Sei $K$ ein globaler Körper, $I_K^1$ die Gruppe der 1-Idele. Die Faktorgruppe $I_K^1/K^*$ ist kompakt.*

*Beweis von Theorem 10.10.* Sei $I_K^1(S) = I_K^1 \cap I_K(S)$.

**Behauptung.** *$I_K^1/K^* I_K^1(S)$ ist endlich.*

$I_K^1(S)$ ist eine offene Untergruppe von $I_K^1$. Es ist

$$I_K^1/K^* I_K^1(S) \cong (I_K^1/K^*)/\,\mathrm{Im}(I_K^1(S)$$

Da $K^* \subset I_K^1$ diskret ist, ist die Projektion $I_K^1 \to I_K^1/K^*$ offen, d.h. Bilder offener Mengen sind offen. Damit ist auch $\mathrm{Im}(I_K^1(S)$ offen. Die Nebenklassen überdecken die kompakte Gruppe $I_K^1/K^*$, daher gibt es nur endlich viele von ihnen.
Nun müssen wir von 1-Idelen auf alle Idele schließen. Sei zunächst $K$ Zahlkörper. Dann gilt

$$I_K/K^* I_K(S) \cong I_K^1/K^* I_K^1(S)$$

da die Faktoren über unendlich in Zähler wie Nenner gleichermaßen auftauchen. Sei $K$ Funktionenkörper, $y \in I_K$ wie im Beweis von Lemma 10.13, d.h.

$$I_K = I_K^1 \times \{y\}^{\mathbb{Z}}$$

Falls $S = \emptyset$, dann ist $I(\emptyset) \subset I_K^1$ und daher

$$I^K/K^* I(\emptyset) \cong I_K^1/K^* I(\emptyset) \times \mathbb{Z}$$

Falls $S \neq \emptyset$, dann enthält $I(S)$ Elemente, die nicht in $I_K^1$ liegen. Teilt man ein solches aus $I_K^1/K^* I^1(S) \times \mathbb{Z}$ heraus, so bleibt ein endlicher Quotient. □

Wir haben damit die Frage auf eine Kompaktheitsfrage reduziert. Hierfür beginnt man additiv.

**Theorem 10.16.** *Sei $K$ ein globaler Körper. Dann ist $K$ eine diskrete Untergruppe von $\mathbb{A}_K$ und $\mathbb{A}_K/K$ ist kompakt.*

*Beweis:* Die Diskretheit sieht man wie im mulitplikativen Fall. Sei $K_0 = \mathbb{Q}, \mathbb{F}_p(t)$. Dann ist $K$ ein endlich dimensionaler $K_0$-Vektorraum. Für jede Stelle $v$ von $K_0$ ist

$$\prod_{w|v} K_w = K \otimes_{K_0} K_{0,v}$$

ein $K_{0,v}$-Vektorraum derselben Dimension. Dies ist verträglich mit Topologien und ganzen Strukturen. Daher ist auch $\mathbb{A}_K = \mathbb{A}_{K_0} \times_{\mathbb{Q}} K$ ein freier $\mathbb{A}_K$-Modul vom Rang $[K : K_0]$. Wegen

$$\mathbb{A}_K/K \cong (\mathbb{A}_{K_0}/K_p)^{[K:K_0]}$$

genügt es, den Fall $K = K_0$ zu betrachten.
Sei $K = \mathbb{Q}$. Wir betrachten $C = [-1/2, 1/2] \times \prod_p \mathbb{Z}_p \subset \mathbb{A}_{\mathbb{Q}}$. Diese Menge ist kompakt. Wir wollen zeigen, dass sie $\mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$ überdeckt, also $C + \mathbb{Q} = \mathbb{A}_{\mathbb{Q}}$. Es gilt $C + \mathbb{Z} = \mathbb{R} \times \prod_p \mathbb{Z}_p = \mathbb{A}_{\mathbb{Q}}(S_\infty)$.

**Behauptung.** $A_{\mathbb{Q}}(S_\infty) + \mathbb{Q} = \mathbb{A}_{\mathbb{Q}}$

Sei $x \in \mathbb{A}_{\mathbb{Q}}$. Sei $P$ die Menge der Primzahlen mit $x_p \notin \mathbb{Z}_p$. Es gilt $\mathbb{Q}_p = \mathbb{Z}_p + \mathbb{Q}_{(p)}$ wobei $\mathbb{Q}_{(p)} = \{a/p^n | a \in \mathbb{Z}, n \in \mathbb{Z}\} = \{x \in \mathbb{Q} || x|_q \leq 1, \text{ für alle } q \neq p\}$ (Übungsaufgabe). Wir schreiben also für $p \in P$

$$x_p = x'_p + y_p \qquad x'_p \in \mathbb{Z}_p, y_p \in \mathbb{Q}_{(p)}$$

Sei $y = \sum_{p \in P} y_p \in \mathbb{Q}$. Wir betrachten das Adel $x - y$. Es liegt in $\mathbb{A}_{\mathbb{Q}}(S_\infty)$.
Sei nun $K = \mathbb{F}_p(t)$. Wir betrachten $C = \prod_v \mathbb{F}_p(t)_v = \mathbb{A}_{\mathbb{F}_p(t)}(\emptyset)$. Diese Menge ist kompakt.

**Behauptung.** $A_{\mathbb{F}_p(t)}(\emptyset) + \mathbb{F}_p(t) = \mathbb{A}_{\mathbb{F}_p(t)}$

. Das Argument ist dasselbe wie für $\mathbb{Q}$, da wieder $\mathbb{F}_p(t)_v = \mathcal{O}_v + \mathbb{F}_p(t)_{(v)}$. □

Auf jeder kompakten topologischen Gruppe gibt es ein eindeutiges invariantes Haarsches Maß von Volumen 1. Sei $\mu$ das Haarsche Maß auf $\mathbb{A}_K/K$. (Invarianz bedeutet $\mu(S) = \mu(S + a)$ für jedes $a \in \mathbb{A}_K$ und jede messbare Teilmenge $S$.). Da $K \subset \mathbb{A}_K$ diskret ist, gibt es ein eindeutiges invariantes Maß auf $\mathbb{A}_K$, das für kleine offene Mengen mit dem Maß auf $\mathbb{A}_K/K$ übereinstimmt. Da $K$ unendlich viele Elemente hat, ist das Maß auf $\mathbb{A}_K$ unbeschränkt. Auf jedem $K_v$ gibt es ebenfalls ein Haarsches Maß. Das Produktmaß muss wegen der Eindeutigkeit mit dem Haarschen Maß übereinstimmen.

**Lemma 10.17.** *Sei $S \subset \mathbb{A}_K$ messbar, $a \in I_K$. Dann ist*

$$\mu(a\mu) = |a|_{\mathbb{A}}\mu(S)$$

*Beweis:* Wegen der Eindeutigkeit der Haarschen Maße gibt es eine Konstant $C$ mit $\mu(aS) = C\mu(S)$ für alle $S$. Es genügt also, die Aussage für ein $S$ zu beweisen. Wir betrachten

$$S = \prod\{x \in K_v || x|_v \leq 1\}$$

Dann ist

$$aS = \prod\{y \in K_v || y|_v \leq |a|_v\}$$

Für fast alle $v$ ist $|a|_v = 1$ und dies hat auf $aS$ keinen Einfluss. Diese ignorieren wir. Es bleiben endlich viele Faktoren. Ohne Einschränkung gibt es genau ein $v$ mit $a_v \neq 1$, d.h. es genügt die analoge lokale Aussage zu zeigen:

(i) Ist $v$ reell, so ist $\mu(|x| \leq 1) = 2$ und $\mu(|x| \leq |a|) = 2|a|$.

(ii) Ist $v$ reell, so ist $\mu(|z| \leq 1) = \pi$ und $\mu(|z| \leq |a|) = \pi|a|^2$.

(iii) Ist $v$ archimedisch, so genügt es $a = \pi_v$ zu betrachten. Dann wird $\mathcal{O}_v$ durch $N(\mathfrak{p}_v)$-viele Nebenklassen von $\pi\mathcal{O}_v$ überdeckt. Wegen der Translationsinvarianz des Haarschen Maßes haben sie alle dasselbe Maß, also $N(\mathfrak{p}_v)\mu(\pi\mathcal{O}_v) = \mu(\mathcal{O}_v)$. Dies passt zu unserer Normierung von $|\cdot|_v$.

□

**Lemma 10.18.** *Die Abbildung*

$$I_K \to \mathbb{A}_K \times \mathbb{A}_K \qquad x \mapsto (x, x^{-1})$$

*ist ein Homöomorphismus von $I_K$ aufs Bild.*

*Beweis:* Der Interessante Teil ist, dass Bilder offener Mengen offen sind. Übungsaufgabe. □

*Beweis von Theorem 10.15:* Sei $C \subset \mathbb{A}_K$ eine kompakte Teilmenge mit $\mu(C) > 1$. Sei $C'$ das Bild von $C \times C$ unter $- : \mathbb{A}_K \times \mathbb{A}_K \to \mathbb{A}_K$. Sei $C''$ das Bild von $C \times C$ unter $\cdot : \mathbb{A}_K \times \mathbb{A}_K \to \mathbb{A}_K$. Als Bilder kompakter Mengen sind $C'$ und $C''$ kompakt. Da $C''$ kompakt ist und $K \subset \mathbb{A}_K$ diskret, ist

$$C'' \cap K^* = \{x_1, \ldots, x_N\}$$

eine endliche Menge. Wir betrachten

$$X = \{x \in I_K | x \in C', x^{-1} \in x_i^{-1} C' \text{ für ein } i\}$$

Ihr Bild unter der Abbildung aus Lemma 10.18 ist kompakt, also ist $X$ kompakt.

**Behauptung.** $I^1 \subset XK^*$

Sei $d \in I^1$. Dann ist $\mu(dC) = |d|_{\mathbb{A}}\mu(C) > 1$. Nach dem Theorem von Minkowski gibt es zwei Elemente $dx \neq dy \in dC$ mit $dx - dy \in K$. Wegen $dx - dy \neq 0$ ist $dx - dy \in K^*$. Es folgt $c_1 = x - y \in C'$, $\delta_1 = c_1 d$. Dieselbe Argumentation für $d^{-1}$ liefert $c_2 \in C'$ mit $\delta_2 = c_2 d^{-1} \in K^*$. Es genügt zu zeigen, dass $c_2 = d\delta_2 \in X$. Es ist

$$\delta_1 \delta_2 = c_1 c_2 \in K^* \cap C'' = \{x_1, \ldots, x_n\}$$

Sei also $c_1 c_2 = x_i$. Es folgt

$$c_2^{-1} = c_1 x_i^{-1} \in x_i^{-1} C'$$

□

Auch den Einheitensatz finden wir wieder.

**Theorem 10.19.** *Sei $K$ globaler Körper, $S$ eine endliche Menge von Stellen, die alle archimedischen Stellen enthält. Sei*

$$U_S = \{x \in K^* | |x|_v = 1 \textit{ für alle } v \notin S\}$$

*Dann ist*

$$U_S \cong \mu(K) \times \mathbb{Z}^s$$

*wobei $\mu(K)$ die Gruppe der Einheitswurzeln in $K$ ist und $s = |S| - 1$ (bzw. $s = 0$ falls $S = \emptyset$).*

Der Beweis benutzt folgendes Lemma:

**Lemma 10.20.** *Sei $s \geq r \geq 0$. Sei $G$ ein Gruppe isomorph zu $\mathbb{R}^r \times \mathbb{Z}^{s-r+1}$. Sei $\lambda : G \to \mathbb{R}$ ein Homomorphismus. Falls $r > 0$, so setzen wir voraus, dass $\lambda$ surjektiv ist. Falls $r = 0$, so setzen wir voraus, dass $\lambda(G) \cong \mathbb{Z}$. Sei $G_1 = \operatorname{Ker} \lambda$. Sei weiter $\Gamma$ eine diskrete Untergruppe von $G_1$, so dass $\Gamma_1/\Gamma$ kompakt ist. Dann ist*

$$\Gamma \cong \mathbb{Z}^s$$

*Beweis:* Es ist $G_1 = \mathbb{R}^{r-1} \times \mathbb{Z}^{s-r+1}$, falls $r > 0$ und $G_1 \cong \mathbb{Z}^s$, falls $r = 0$. Als diskrete Untergruppe ist $\Gamma \cong \mathbb{Z}^t$ mit $t \leq s$. Da $G_1/\Gamma$ kompakt ist, muss $t = s$ sein. □

*Beweis von Theorem 10.19:* Falls $S = \emptyset$, so ist $U_S = \mathbb{F}_q$ für eine endliche Erweiterung von $\mathbb{F}_p$, also endlich. Sei nun $S \neq \emptyset$, $s = |S|$, $r = |S_\infty|$. Wir setzen

$U = \prod_v \{x \in K_v || x|_v = 1\}$. Dies ist eine kompakte Untergruppe von $I_K(S)$. Wir setzen

$$G = I_K(S)/U \cong \prod_{v \in S} K_v^*/\{x||x|_v = 1\}$$

Falls $v$ reell ist, so ist $\mathbb{R}^*/\{\pm 1\} \cong \mathbb{R}$ via der Logarithmusabbildung. Falls $v$ komplex ist, so ist $\mathbb{C}^*/S^1 \cong \mathbb{R}$ via der Betragsabbildung. Falls $v$ nicht-archimedisch ist, so ist $K_v^*/\mathcal{O}_v^* \cong \mathbb{Z}$ via der Bewertung $v$. Damit hat $G$ die Form der Gruppe aus dem Lemma. Es sei

$$\lambda = \log |\cdot|_{\mathbb{A}} : I_K(S) \to \mathbb{R}$$

Sie faktorisiert über $G$. Wie im Beweis von Lemma 10.13 sehen wir, dass $\lambda$ das in Lemma 10.20 nötige Bild hat. Sei $G_1 = \operatorname{Ker} \lambda = I_K^1(S)/U$, da $U \subset I_K^1(S)$. Es sei $\Gamma$ das Bild von $U_S$ in $G_1 = I_K^1(S)/U$.

**Behauptung.** *Der Kern von $U_S \to G_1$ ist endlich.*

Der Kern ist $U_S \cap U \subset I_K^1(S)$. Da $K^*$ diskret ist und $U$ kompakt, besteht er nur aus endlich vielen Elementen.

**Behauptung.** *$G_1/U_S$ ist kompakt.*

Dies ist ein Quotient von $I_K^1(S)/U_S$. Dies liegt in $I_K(S)/K^*$ und ist darin abgeschlossen, also selbst kompakt.

**Behauptung.** *$\Gamma \subset G_1$ ist diskret.*

Sei $W$ eine kompakte Umgebung der 1 in $I_K(S)$. Dann ist $WU$ ebenfalls kompakt. Daher enthält $WU$ nur endlich viele Elemente aus $U_S$. Dann enthält auch $WU/U \subset G$ nur endlich viele Elemente aus $\Gamma$.
Damit sind alle Voraussetzung von Lemma 10.20 erfüllt. Es ist $\Gamma \cong \mathbb{Z}^s$ und daher $U_S \cong \operatorname{Ker} \lambda \times \mathbb{Z}^s$. □

# Kapitel 11

# Fermatsche Gleichung

**Literatur:** Washington, Cyclotomic Fields, Einleitung.
Rosen, The history of Fermat's Last Theorem, in: Cornell, Silverman, Stevens (Eds), Modular Forms and Fermat's Last Theorem, Proceedings Boston 1995,
Wir beginnen mit dem Funktionenkörperfall, der bemerkenswert einfach ist.

**Satz 11.1.** *Sei $k$ ein Körper, $n > 2$ prim zu* $\mathrm{Char}(k)$. *Sei $K = k(t)$. Dann hat die Gleichung*

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

*nur Lösungen mit $xyz = 0$ oder $x, y, z \in k$.*

*Beweis:* Sei $(x, y, z)$ eine Lösung mit $xyz \neq 0$. Ohne Einschränkung sind $x, y, z \in k[t]$ und paarweise teilerfremd. Zu zeigen ist, dass $x, y, z$ konstante Polynome sind. Hierzu genügt es, den Fall $k = \overline{k}$ zu betrachten. Sei $\zeta$ eine primitive $n$-te Einheitswurzel in $k$. Wir faktorisieren

$$z^n = \prod_{i=1}^{n-1} (x + \zeta^i y)$$

**Behauptung.** *Die Faktoren $(x + \zeta^i y)$ sind paarweise teilerfremd.*

Sei $f$ ein gemeinsamer Teiler von $x + \zeta^i y$ und $x + \zeta^j y$. Dann teilt $f$ auch

$$x + \zeta^i y - x - \zeta^j y = \zeta^i (1 - \zeta^{i-j}) y$$
$$\zeta^j (x + \zeta^i y) - \zeta^i (x + \zeta^j) y = \zeta^j (1 - \zeta^{j-i}) x$$

Da $x, y$ teilerfremd sind, muss $f$ eine Einheit sein.
Hieraus folgt, dass die Faktoren $(x+\zeta^i y)$ von der Form $n$-te Potenz mal Einheit sind. Da $k$ algebraisch abgeschlossen ist, können wir auch aus der Einheit eine Wurzel ziehen und erhalten

$$x + y = u^n, x + \zeta y = v^n, x + \zeta^2 y = w^n$$

(Hier geht $n > 2$ ein.) Es folgt

$$w^n + \zeta u^n = x + \zeta^2 y + \zeta x + \zeta y = (1+\zeta)(x+\zeta y) = (1+\zeta)v^n$$

Wieder ziehen wir die $n$-ten Wurzeln der Koeffizienten und erhalten

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

wobei die Grade der neuen Lösung echt kleiner als die der ursprünglichen sind. Mit Fermats Methode des unendlichen Abstiegs ist dies ein Widerspruch. □

Wir versuchen es mit derselben Methode für $\mathbb{Q}$, mit wesentlich schwächerem Ergebnis.
Sei $p$ eine feste Primzahl, $p \geq 5$. Sei $\zeta = \zeta_p$ eine primitive $p$-te Einheitswurzel. Wir erinnern uns, das der Ganzheitsring $\mathbb{Z}[\zeta]$. Die Primzahl $p$ ist rein verzweigt. $(1-\zeta)$ ist der Primteiler von $p$.

**Lemma 11.2.** *Seien $r, s \in \mathbb{Z}$ mit $p \nmid r, s$. Dann*

$$\frac{\zeta^r - 1}{\zeta^s - 1} \in \mathbb{Z}[\zeta]^*$$

*Beweis:* Sei $r = st \mod p$.

$$\frac{\zeta^r - 1}{\zeta^s - 1} = \frac{\zeta^{st-1}}{\zeta^s - 1} = 1 + \zeta^t + \zeta^{2t} + \cdots + \zeta^{(s-1)t} \in \mathbb{Z}[\zeta_p]$$

Analag ist auch das Inverse ganz, insgesamt also eine Einheit. □

Hieraus folgt, dass $(1-\zeta^r) = (1-\zeta)$ für alle $p \nmid r$.

**Lemma 11.3.** *Sei $\alpha \in \mathbb{Z}[\zeta]$. Dann gibt es $a \in \mathbb{Z}$ mit*

$$\alpha^p = a \mod p$$

*Beweis:* Sei $\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$ Dann gilt

$$\alpha^p = a_0^p + a_1^p\zeta^p + \cdots + a_{p-2}^p\zeta^{p(p-2}$$

Die rechte Seite ist in $\mathbb{Z}$. □

**Bemerkung.** Die Elemente der Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ haben die Form $\zeta \mapsto \zeta^i$ für $i = 1, \ldots, p-1$. Besonders interessant ist $\iota$ mit $\iota(\zeta) = \zeta^{p-1} = \zeta^{-1}$. Unter der Einbettung $\zeta \mapsto \exp(2\pi/p)$ ist die komplexe Konjugation. Tatsächlich hängt $\iota$ nicht von der Wahl von $\zeta$ bzw. von der Wahl der komplexen Konjugation ab. $\iota$ ist *die* komplexe Konjugation auf $\mathbb{Q}(\zeta)$, wir schreiben einfach $\bar{\cdot}$ Der Fixkörper ist $\mathbb{Q}(\zeta + \zeta^{-1})$. Die Erweiterung $\mathbb{Q}/(\zeta)/\mathbb{Q}(\zeta + \zeta^{-1})$ hat Grad 2. Der Körper $\mathbb{Q}(\zeta)$ ist total komplex, $r_1 = 0$, $r_2 = (p-1)/2$. Der Teilkörper $\mathbb{Q}(\zeta+\zeta^{-1})$ ist total reell, $r_1 = (p-1)/2$, $r_2 = 0$.

**Lemma 11.4.** *Sei $u \in \mathbb{Z}[\zeta]^*$. Dann gibt es $u' \in \mathbb{Q}(\zeta + \zeta^{-1})$ und $r \in \mathbb{Z}$, so dass $u = \zeta^r u'$. Das Element $u'$ ist Einheit von $\mathbb{Q}(\zeta + \zeta^{-1})$.*

*Beweis:* Sei $\alpha = u/\overline{u}$. Dies ist Einheit, da $u$ eine Einheit ist. Auch alle Konjugierten von $\alpha$ haben Absolutbetrag 1. Damit liegt $\alpha$ im Kern der logarithmischen Einbettung. Dieser besteht genau aus den Einheitswurzeln. Also

$$\alpha = u/\overline{u} = \pm\zeta^a$$

Wir betrachten zuerst das Vorzeichen $-$. Sei

$$u = b_0 + b_1\zeta + \cdots + b_{p-2}\zeta^{p-2} \Rightarrow u = b_0 + b_1 + \cdots + b_{p-2} \mod 1 - \zeta$$

Ebenso

$$\overline{u} = b_0 + \cdots + b_{p-2} = u = -\zeta^a\overline{u} = -\overline{u} \mod 1 - \zeta$$

Dies bedeutet

$$2\overline{u} = 0 \mod 1 - \zeta$$

$(1 - \zeta)$ ist ein Primideal. Wegen $1 - \zeta \nmid 2$ folgt $1 - \zeta | \overline{u}$. Dies ist ein Widerspruch zu $u$ Einheit.
Es gilt demnach

$$\alpha = \zeta^a = \zeta^{2r} \Rightarrow u = \zeta^{2r}\overline{u} \Rightarrow \zeta^{-r}u = \zeta^r\overline{u}$$

mit $2r = a \mod p$. Wir setzen $u' = \zeta^{-r}u$. Wegen $u' = u\zeta^{-r}$ ist das Element und sein Inverses ganz. □

**Lemma 11.5.** *Sei $\alpha = a_0 + \cdots + a_{p-1}\zeta^{p-1}$ mit $a_i \in \mathbb{Z}$, wenigstens ein $a_i = 0$. Sei $n \in \mathbb{Z}$.*

$$n|\alpha \Rightarrow n|a_j \text{ für alle } j$$

*Beweis:* Jede $p - 1$-elementige Teilmenge von $\{1, \zeta, \ldots, \zeta^{p-1}\}$ ist eine $\mathbb{Z}$-Basis. Wir schreiben $\alpha$ in der Basis, die $\zeta^i$ auslässt. Dann folgt die Aussage aus der Eindeutigkeit der Darstellung. □

**Theorem 11.6** (Kummer 1847, Fermatsche Vermutung, 1. Fall)**.** *Sei $p \geq 5$ eine Primzahl mit $p \nmid h(\mathbb{Q}(\zeta))$. Die Gleichung*

$$x^p + y^p = z^p$$

*hat keine ganzzahlige Lösung mit $p \nmid x, y, z$.*

*Beweis:* Sei $x, y, z \in \mathbb{Z}$ eine Lösung mit $p \nmid x, y, z$. Ohne Einschränkung ist das Tripel primitiv, d.h. die Zahlen paarweise teilerfremd.

**Behauptung.** *$x, y, z$ können so gewählt werden, dass $x \neq y \mod p$.*

Angenommen $x = y \mod p$. Dann permutieren wir

$$x^p + (-z)^p = (-y)^p$$

Angenommen, zusätzlich $x = -z \mod p$. Dann gilt

$$2x^p = -x^p \mod p \Rightarrow p|3x^p$$

Dies ist unmöglich, da $p \geq 5$, $p \nmid x$.
Wir rechnen in $\mathbb{Z}[\zeta]$. Dort gilt

$$x^p + y^p = \prod_{r=1}^{p-1}(x + \zeta^i y)$$

Wir wollen mit Teilbarkeitsargumenten in $\mathbb{Z}[\zeta]$ argumentieren.

**Behauptung.** *Die Ideale $(x + \zeta^i y)$ sind paarweise teilerfremd.*

Sei $\mathfrak{p} \in \operatorname{Spm} \mathbb{Z}[\zeta]$ ein gemeinsamer Primteiler von $(x + \zeta^i y)$ und $(y + \zeta y)$. Dann

$$\mathfrak{p}|(\zeta^i y - \zeta^j y) = (1 - \zeta)(y)$$

Also folgt $\mathfrak{p} = (1 - \zeta)$ oder $\mathfrak{p}|y$. Analog:

$$\mathfrak{p}|\zeta^j(x + \zeta^i y) - \zeta^i(x + \zeta^j y) = (1 - \zeta)x$$

Also folgt $\mathfrak{p} = (1 - \zeta)$ oder $\mathfrak{p}|x$.
**1. Fall:** $\mathfrak{p} \neq (1 - \zeta)$. Dann ist $\mathfrak{p}|x, y$. Dies ist ein Widerspruch zu $(x, y) = 1$ bereits über $\mathbb{Z}$.
**2. Fall:** $\mathfrak{p} = (1 - \zeta)$. Dann gilt $\mod \mathfrak{p}$

$$x + y = x + \zeta^i y = 0 \mod \mathfrak{p}$$

Wegen $x + y \in \mathbb{Z}$ folgt $x + y = 0 \mod p$. Aber

$$z^p = x^p + y^p = x + y = 0 \mod p$$

Dies ist ein Widerspruch zu $p \nmid z$. Dies beweist die Behauptung.
Da die Ideale $(x + \zeta^i y)$ teilerfremd sind, muss jedes von ihnen eine $p$-te Potenz sein.

$$(x + \zeta^i y) = A_i^p$$

für ein Ideal $A_i$. Die linke Seite ist ein Hauptideal.

**Behauptung.** *$A_i$ ist ein Hauptideal.*

Wir müssen überprüfen, ob $[A_i] = 0$ in $\operatorname{Cl}(\mathbb{Z}[\zeta])$. Die Klassengruppe ist eine endliche Gruppe, deren Ordnung nach Voraussetzung nicht von $p$ geteilt wird. Daher ist Multiplikation mit $p$ ein Isomorphismus. Nach Voraussetzung ist $p[A_i] = [A_i^p] = 0$ in $\operatorname{Cl}(\mathbb{Z}[\zeta])$. Zusammen folgt die Behauptung.

Sei nun $A_i = (\alpha_i)$. Es ist also

$$x + \zeta^i y = u_i \alpha_i^p$$

für ein $u_i \in \mathbb{Z}[\zeta]^*$. Wir betrachten speziell $i = 1$ und setzen unsere Lemmata zusammen.

$$u_1 = u' \zeta^r$$

mit $u'$ total reell. Wegen Lemma 11.3 gibt es $a \in \mathbb{Z}$ mit $\alpha_i^p = a \mod p$. Daher

$$x + \zeta y = \zeta^r u' a \mod p$$

Komplex konjugiert

$$x + \zeta^{-1} y = \zeta^{-r} u' a \mod p$$

Zusammen folgt

$$\zeta^{-r}(x + \zeta y) = \zeta^r (x + \zeta^{-1} y) \mod p$$

oder

$$x + \zeta y - \zeta^{2r} x - \zeta^{2r-1} y = 0 \mod p$$

Falls $1, \zeta, \zeta^{2r}, \zeta^{2r-1}$ paarweise verschieden, dann folgt aus Lemma 11.5 (und $p \geq 5$), dass $p$ alle Koeffizienten teilt. Dies ist ein Widerspruch zu $p \nmid x, y$.
Wegen $1 \neq \zeta$ und $\zeta^{2r} \neq \zeta^{2r-1}$ bleiben 3 Fälle:

$1 = \zeta^{2r}$ Dann gilt

$$0 = x + y\zeta y - x - \zeta^{-1} y = \zeta y + \zeta^{-1} y \mod p$$

Nach Lemma 11.5 gilt $p|y$, Widerspruch.

$1 = \zeta^{2r-1}$ Dies ist äquivalent zu $\zeta = \zeta^{2r}$. Dann gilt

$$0 = x + \zeta y - \zeta x - y = (x - y) + \zeta(x - y) \mod p$$

Nach Lemma 11.5 gilt $p|x - y$, im Widerspruch zur Wahl von $x, y$.

$\zeta = \zeta^{2r-1}$ Dann gilt

$$0 = x + y\zeta - x\zeta^2 - \zeta y = x - \zeta^2 x \mod p$$

Nach Lemma 11.5 folgt $p|x$, Widerspruch.

□

**Bemerkung.** Primzahlen $p$, die $h(\mathbb{Q}(\zeta_p))$ teilen, heißen *regulär*. Die ersten irregulären Primzahlen sind

$$37, 59, 67, 101, 103, 149, 157$$

Es ist unbekannt, ob es unendlich viele reguläre Primzahlen gibt. Es gibt jedoch nur endlich viele, für die $\mathbb{Z}[\zeta]$ ein Hauptidealring ist (nämlich $p \leq 19$).

Der zweite Fall ist tiefer, vergleiche Washington §9. Neben elementaren Teilbarkeitsüberlegungen und wieder einem Klassenzahlargument, wird gebraucht:

**Theorem 11.7** (Kummer)**.** *Sei $p$ reguläre Primzahl, $u \in \mathbb{Z}[\zeta]^*$. Falls es $a \in \mathbb{Z}$ gibt mit $u = a \mod p$, dann ist $u = v^p$ für ein $v \in \mathbb{Z}[\zeta]^*$.*

Diese genaue Information bekommt durch die Analyse einer $p$-adischen Version des Regulators mit der $p$-adischen Funktion $\log : \mathbb{Q}_p^* \to \mathbb{Q}_p$. Man beweist dies heute mit den Methoden der Iwasawa-Theorie.