# Algebraische Zahlentheorie

Wolfgang M. Ruppert

Wintersemester 1992/93

17. März 1999 [1]

[1] Im Wintersemester 1992/93 am Mathematischen Institut der Universität Erlangen abgehaltene Vorlesung

# Inhaltsverzeichnis

KAPITEL 1

# Einführung

Die algebraische Zahlentheorie hat ihren Ursprung in konkreten Fragestellungen, die mit ganzen Zahlen zu tun haben. Als Beispiel betrachten wir eine Aufgabe, die schon auf Diophant (um 250) zurückgeht.

**Aufgabe:** Bestimme alle ganzzahligen Lösungen der Gleichung

$$y^2 = x^3 - 2.$$

Dazu ein paar Anmerkungen:

1. Fermat (1601–1655) stellt englischen Mathematikern die Aufgabe, zu zeigen, daß es außer $x = 3, y = \pm 5$ keine weiteren Lösungen gibt. Er schreibt[1]:

   *Ob sich jedoch außer 25 noch ein anderes Quadrat in ganzen Zahlen finden läßt, das, um 2 vermehrt, einen Kubus ergibt, das zu untersuchen scheint auf den ersten Blick sehr schwierig. Ich kann aber dennoch einen ganz sicheren Beweis dafür erbringen...*

   Leider fehlt eine Ausführung der Behauptung.
2. In Eulers Algebra wird so argumentiert[2]: Man faktorisiert die Gleichung $y^2 + 2 = x^3$ und erhält:

   $$(y + \sqrt{-2})(y - \sqrt{-2}) = x^3.$$

   Da rechts eine dritte Potenz steht, muß auch $(y + \sqrt{-2})$ eine sein, d.h.

   $$y + \sqrt{-2} = (a + b\sqrt{-2})^3$$

   mit ganzen Zahlen $a$ und $b$. Nun ist $(a + b\sqrt{-2})^3 = a^3 + 3a^2b\sqrt{-2} + 3ab^2(-2) + b^3(-2)\sqrt{-2}$ und durch Koeffizientenvergleich erhält man

   $$\begin{aligned} y &= a^3 - 6ab^2 = a(a^2 - 6b^2) \\ 1 &= 3a^2b - 2b^3 = b(3a^2 - 2b^2) \end{aligned}$$

   Aus der letzten Gleichung folgt $b = \pm 1$. Der Fall $b = -1$ führt auf $3a^2 = 1$, was nicht geht, der Fall $b = 1$ auf $a^2 = 1$ und damit schließlich auf die zwei Lösungen $x = 3$ und $y = \pm 5$.
3. Ist Eulers Argument richtig? Eulers Beweis läßt sich rechtfertigen, wenn man weiß, daß der Ring $\mathbf{Z}[\sqrt{-2}] = \{u + v\sqrt{-2} : u, v \in \mathbf{Z}\}$ faktoriell ist, nur die Einheiten $\pm 1$ hat, und daß $y + \sqrt{-2}$ und $y - \sqrt{-2}$ teilerfremd sind. (Diese (nichttrivialen) Aussagen werden in folgendem Lemma bewiesen.) Denn dann hat man Primfaktorzerlegungen

   $$y + \sqrt{-2} = \epsilon_+ \pi_1^{n_1} \dots \pi_r^{n_r}, \quad y - \sqrt{-2} = \epsilon_- \rho_1^{m_1} \dots \rho_s^{m_s},$$

   und wegen der Teilerfremdheit sind die $n_i$ und $m_j$ durch 3 teilbar, und da auch die $\epsilon$'s dritte Potenzen sind, ist es auch $y + \sqrt{-2}$. Wir bemerken noch, daß $y$ ungerade sein muß.

LEMMA. *Sei $A$ der Ring $\mathbf{Z}[\sqrt{-2}]$ und $N(a + b\sqrt{-2}) = (a + b\sqrt{-2})(a - b\sqrt{-2}) = a^2 + 2b^2$. Dann gilt:*

1. *$N$ bildet $A$ in $\mathbf{Z}$ ab und ist multiplikativ.*
2. *Die Einheiten von $A$ sind die Elemente mit Norm 1, also $\pm 1$.*
3. *$A$ ist euklidisch bezüglich der Funktion $N$.*
4. *$\sqrt{-2}$ ist ein Primelement.*
5. *Für jede ungerade Zahl $y$ sind $y + \sqrt{-2}$ und $y - \sqrt{-2}$ teilerfremd in $A$.*

*Beweis:*

1. Klar!

[1] *Pierre de Fermat,* Bemerkungen zu Diophant, Ostwald's Klassiker der exakten Wissenschaften, Nr. 234, Akademische Verlagsanstalt, Leipzig, 1932, S. 30 und S. 47

[2] *Leonhard Euler,* Algebra, ...; Euler: 1707–1783

2. Ist $\alpha$ eine Einheit, so gibt es $\beta$ mit $\alpha\beta = 1$, also $N(\alpha)N(\beta) = 1$. In $\mathbf{Z}$ folgt daraus aber sofort $N(\alpha) = 1$. Ist umgekehrt $N(a + b\sqrt{-2}) = 1$, so ist natürlich $a - b\sqrt{-2}$ das Inverse zu $a + b\sqrt{-2}$. Daß die Gleichung $N(\alpha) = 1$ nur $\pm 1$ zuläßt, ist trivial.
3. Seien $a$ und $b$ aus $A$ mit $b \neq 0$. Wir müssen zeigen, daß es $q, r \in A$ gibt mit $a = qb + r$ und $N(r) < N(b)$. Wir denken uns nun alle Zahlen als komplexe Zahlen in der komplexen Zahlenebene. Wegen $N(\alpha) = |\alpha|^2$ müssen wir zeigen, daß es zu $a$ und $b$ ein $q \in A$ gibt mit $|\frac{a}{b} - q|^2 < 1$. Nun ist aber $\mathbf{Z}[\sqrt{-2}]$ ein Gitter in der komplexen Ebene und zu jeder komplexen Zahl gibt es einen Gitterpunkt, der Abstand $\leq \sqrt{(1/2)^2 + (\sqrt{2}/2)^2} < 1$ hat. Damit findet man auch zu $a$ und $b$ ein entsprechendes $q$, w.z.z.w.
4. $\sqrt{-2}$ ist unzerlegbar, da aus $\sqrt{-2} = ab$ durch Normbildung sofort $2 = NaNb$ folgt, also muß $a$ oder $b$ $\pm 1$ sein.
5. Angenommen, es gibt ein Primelement $\pi$ mit $\pi | y + \sqrt{-2}$ und $\pi | y - \sqrt{-2}$. Dann gilt natürlich auch $\pi | 2\sqrt{-2}$ und es folgt $\pi \sim \sqrt{-2}$. Also teilt $\sqrt{-2}$ auch $y$, d.h. es gibt ganze Zahlen $u, v$ mit
$$y = \sqrt{-2}(u + v\sqrt{-2}) = -2v + u\sqrt{-2},$$
woraus durch Koeffizientenvergleich folgt, daß $y$ gerade sein muß, ein Widerspruch!

Daß die Eulersche Methode nicht immer zum Ziel führt, kann man an den folgenden Beispielen sehen.

**Übung:** Betrachte die Gleichungen $y^2 = x^3 - 11$ und $y^2 = x^3 - 26$. Suche jeweils 4 Lösungen. Lassen sich diese mit dem obigem Ansatz erklären? Was geht schief?[3]

Im Anhang sind noch ein paar Bücher zur algebraischen Zahlentheorie angegeben.

[3] Die Gleichung $y^2 = x^3 - 26$ hat mindestens die Lösungen $(3, \pm 1)$ und $(35, \pm 207)$. Nun ist $1 + \sqrt{-26}$ nur als Ideal dritte Potenz, nicht jedoch als Element. Der Ring $\mathbf{Z}[\sqrt{-26}]$ hat Klassenzahl 6. Die Gleichung $y^2 = x^3 - 11$ muß man im Ring $\mathbf{Z}[\frac{1+\sqrt{-11}}{2}]$ studieren, der wieder euklidisch ist. Lösungen sind $(3, \pm 4)$ und $(15, \pm 58)$. Literatur: *London, H., Finkelstein, R.,*, On Mordell's Equation, 1973.

KAPITEL 2

# Ganzheit

Ein algebraischer Zahlkörper $K$ ist eine endliche Körpererweiterung von $\mathbf{Q}$. Die Rolle von $\mathbf{Z}$ in $\mathbf{Q}$ übernehmen in $K$ die ganzen algebraischen Zahlen von $K$.

Sei $A$ ein Ring und $L$ ein Körper mit $A \subset L$. (Insbesondere ist also $A$ ein Integritätsring, speziell kommutativ mit Eins.)

DEFINITION. Ein $x \in L$ heißt ganz über $A$, wenn eine der folgenden äquivalenten Bedingungen erfüllt ist:

1. $x$ genügt einer Ganzheitsgleichung über $A$, d.h. es gibt $a_1, \ldots, a_n \in A$ mit
$$x^n + a_1 x^{n-1} + \cdots + a_n = 0.$$
(Der höchste Koeffizient ist also 1.)
2. Der Unterring $A[x]$ von $L$ ist ein endlich erzeugter $A$-Modul.
3. Es gibt einen endlich erzeugten $A$-Modul $M \subset L$ mit $M \neq 0$ und
$$xM \subset M.$$

Ein Ring $B$ mit $A \subset B \subset L$ heißt ganz über $A$, wenn jedes Element von $B$ ganz über $A$ ist.

**Beispiel:**

1. Ist $L$ eine endliche Körpererweiterung von $K$, so ist $L$ ganz über $K$, d.h. ist $A$ ein Körper, so bedeutet 'ganz' einfach 'algebraisch'.
2. Der Unterring $A = \mathbf{Z}[\sqrt{-2}]$ des Körpers $\mathbf{Q}(\sqrt{-2})$ ist ganz über $\mathbf{Z}$: Wähle im dritten Teil der Definition $M = A$.
3. $\frac{1+\sqrt{5}}{2}$ ist ganz über $\mathbf{Z}$, da es der Gleichung $x^2 - x - 1 = 0$ genügt.

*Beweis der Äquivalenz:*

- Aus 1. folgt 2.: Mit der definierenden Gleichung für $x$ folgt sofort $A[x] = A + Ax + Ax^2 + \cdots + Ax^{n-1}$.
- Aus 2. folgt 3.: Wähle einfach $M = A[x]$.
- Aus 3. folgt 1.: Schreibe $M = Am_1 + \cdots + Am_r$. Dann gibt es $a_{ij} \in A$ mit $xm_i = \sum_j a_{ij} m_j$. Als Matrix geschrieben:
$$x \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix} = A \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix},$$
also
$$(xE - A) \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix} = 0.$$
Die Matrix $xE - A$ mit Koeffizienten im Körper $L$ kann nicht invertierbar sein, sonst wären alle $m_i = 0$. Also gilt $\det(xE - A) = 0$, dies liefert also eine Ganzheitsgleichung für $x$ über $A$. ■

SATZ. *Sind $A \subset B \subset C$ Unterringe von $L$, und ist $B$ ganz über $A$, $C$ ganz über $B$, so ist auch $C$ ganz über $A$.*

*Beweis:* Sei $x \in C$ beliebig. Da $x$ ganz über $B$ ist, gibt es eine Gleichung

$$x^n + b_1 x^{n-1} + \cdots + b_n = 0$$

mit $b_i \in B$. Da die $b_i$'s ganz über $A$ sind, gibt es endlich erzeugte $A$-Untermoduln $M_i \neq 0$ von $L$ mit $b_i M_i \subset M_i$. Dann erfüllt auch $M = M_1 \dots M_n$ die Bedingung $b_i M \subset M$ und ist endlich erzeugt über $A$. Schließlich ist $N = M + Mx + \cdots + Mx^{n-1}$ ein endlich erzeugter $A$-Modul $\neq 0$ mit $xN \subset N$, d.h. $x$ ist auch ganz über $A$, was zu zeigen war. ■

SATZ. *Sei $A$ ein Ring in einem Körper $L$. Dann ist*

$$B = \{x \in L : x \text{ ganz über } A\}$$

*ein Ring. $B$ wird der ganze Abschluß von $A$ in $L$ genannt.*

*Beweis:* Seien $x$ und $y$ aus $B$. Dann gibt es dazu endlich erzeugte $A$-Moduln $M$ und $N \neq 0$ mit $xM \subset M$ und $yN \subset N$. Der Modul $MN$ ist dann auch endlich erzeugt, $\neq 0$ und erfüllt $(x+y)MN \subset MN$ und $xyMN \subset MN$, woraus die Behauptung folgt. ■

DEFINITION. Sei $K$ ein Zahlkörper, d.h. eine endliche Körpererweiterung von $\mathbf{Q}$. Dann heißt der ganze Abschluß von $\mathbf{Z}$ in $K$ der Ring der ganzen Zahlen von $K$ oder der Ganzheitsring von $K$ oder die Maximalordnung von $K$ und wird mit $\mathfrak{o}_K$ bezeichnet.

Für uns wird im folgenden der Ring $\mathfrak{o}_K$ eine zentrale Rolle spielen. Grundprobleme sind:

- Welche Eigenschaften hat $\mathfrak{o}_K$? Wie sehen die Einheiten aus? Ist $\mathfrak{o}_K$ Hauptidealring oder faktorieller Ring, etc.?
- Wie läßt sich $\mathfrak{o}_K$ bestimmen bei vorgegebenem $K$?

DEFINITION. Ein Ring $A$ heißt ganz abgeschlossen in einem Körper $L$, wenn jedes Element von $L$, das ganz über $A$ ist, schon in $A$ selbst liegt. $A$ heißt ganz abgeschlossen, wenn $A$ ganz abgeschlossen in seinem Quotientenkörper liegt.

**Beispiele:**

1. Die Ganzheitsringe $\mathfrak{o}_K$ sind wegen der Transitivität der Ganzheit ganz abgeschlossen.
2. Jeder faktorielle Ring $A$ ist ganz abgeschlossen, denn: Sei $\frac{a}{b} \in K = Quot(A)$ ganz über $A$ (o.E. $a$ und $b$ teilerfremd); dann gibt es $a_1, \dots, a_n \in A$ mit
$$\left(\frac{a}{b}\right)^n + a_1 \left(\frac{a}{b}\right)^{n-1} + \cdots + a_n = 0,$$
woraus durch Hochmultiplizieren von $b^n$ folgt: $b | a^n$. Da $a$ und $b$ teilerfremd waren, folgt o.E. $b = 1$, d.h. $\frac{a}{b} \in A$, q.e.d.
3. Wir sahen, daß $\mathbf{Z}[\sqrt{-2}]$ faktoriell ist, also ist der Ring ganz abgeschlossen, also $\mathfrak{o}_{\mathbf{Q}(\sqrt{-2})} = \mathbf{Z}[\sqrt{-2}]$.
4. Der Ring $\mathbf{Z}[\sqrt{5}]$ ist nicht ganz abgeschlossen, da z.B. $\frac{1+\sqrt{5}}{2}$ in $Quot(A)$ liegt, nicht aber in $A$ und der Ganzheitsgleichung $x^2 - x - 1 = 0$ genügt.

**Erinnerung an Spur und Norm:**

- $L|K$ eine endliche separable Körpererweiterung. Dann kann man $L$ als endlich dimensionalen $K$-Vektorraum betrachten. Durch Multiplikation liefert jedes $\alpha \in L$ einen $K$-Endomorphismus von $L$. Die Spur diesen Endomorphismus heißt die Spur $Sp_{L|K}(\alpha)$, seine Determinante die Norm $N_{L|K}(\alpha)$.
- Seien $\sigma_1, \dots, \sigma_n : L \to \bar{K}$ die $K$-Einbettungen von $L$ in einen algebraischen Abschluß von $K$. Dann gilt:
$$Sp_{L|K}(\alpha) = \sum \sigma_i(\alpha),$$
$$N_{L|K}(\alpha) = \prod \sigma_i(\alpha).$$
- Die Spur ist eine $K$-lineare Abbildung, die Norm ist multiplikativ. Wegen $Sp(x) = \sigma_1(x) + \cdots + \sigma_n(x)$ ist $Sp$ als Summe von verschiedenen Charakteren auf der Gruppe $L^\times$ nicht identisch 0 (nach dem Dedekindschen Unabhängigkeitssatz für Charaktere).

SATZ. *Sei $A$ ein ganz abgeschlossener Ring mit Quotientenkörper $K$ und $L$ eine endliche separable Körpererweiterung von $K$. Sei $x \in L$ ganz über $A$. Dann gilt:*

$$Sp_{L|K}(x), N_{L|K}(x) \in A.$$

*Ebenso liegen die Koeffizienten des Minimalpolynoms von $x$ in $A$.*

*Beweis:* Mit $x$ ist auch $\sigma(x)$ ganz über $A$. Da Spur und Norm Summe bzw. Produkt ganzer Elemente sind, sind sie in $K$ und ganz über $A$. Da $A$ ganz abgeschlossen ist, folgt die Behauptung. Das Minimalpolynom von $x$ ist

$$m = (X - \sigma_1(x)) \dots (X - \sigma_m(x))$$

mit geeigneten Isomorphismen $\sigma_j$. Dann folgt die Behauptung wie eben. ■

**Beispiel:** Sei $K = \mathbf{Q}(\sqrt{d})$ ein quadratischer Zahlkörper. O.E. ist also $d \in \mathbf{Z}$ quadratfrei und $\neq 1$. Wir wollen $\mathfrak{o}_K$, den ganzen Abschluß von $\mathbf{Z}$ in $K$, berechnen. Sei $\alpha = a + b\sqrt{d} \in \mathbf{Q}(\sqrt{d})$. Ist $\alpha$ ganz über $\mathbf{Z}$, so sind nach dem vorhergehenden Satz auch Spur und Norm ganz über $\mathbf{Z}$, also $Sp(\alpha), N(\alpha) \in \mathbf{Z}$. Sind umgekehrt $Sp(\alpha)$ und $N(\alpha)$ in $\mathbf{Z}$, so genügt $\alpha$ der Gleichung $\alpha^2 - Sp(\alpha)\alpha + N(\alpha) = 0$, d.h. $\alpha$ ist ganz über $\mathbf{Z}$. Also gilt:

$$\alpha \text{ ganz über } \mathbf{Z} \iff Sp(\alpha) = 2a \in \mathbf{Z} \text{ und } N(\alpha) = a^2 - db^2 \in \mathbf{Z}.$$

Wegen $2a \in \mathbf{Z}$ können wir schreiben $a = \frac{u}{2}$ mit $u \in \mathbf{Z}$. Wegen $a^2 - db^2 = \frac{1}{4}(u^2 - d(2b)^2)$ ist auch $u^2 - d(2b)^2 \in \mathbf{Z}$, also auch $2b \in \mathbf{Z}$, d.h. $b = \frac{v}{2}$ mit einem $v \in \mathbf{Z}$. Es bleibt jetzt die Bedingung $u^2 - dv^2 \in 4\mathbf{Z}$. Wir unterscheiden 3 Fälle:

- $d \equiv 1 \bmod 4$: Also muß gelten $u^2 \equiv v^2 \bmod 4$, was aber äquivalent ist mit $u \equiv v \bmod 2$, also

  $$\mathfrak{o}_K = \{\frac{u + v\sqrt{d}}{2} : u, v \in \mathbf{Z}, u \equiv v \bmod 2\}.$$

  Wegen $\frac{u+v\sqrt{d}}{2} = \frac{u-v}{2} + v\frac{1+\sqrt{d}}{2}$ ist dies äquivalent zu

  $$\mathfrak{o}_K = \mathbf{Z}[\frac{1 + \sqrt{d}}{2}].$$

- $d \equiv 2 \bmod 4$: Dann muß $u$ gerade sein, also auch $v$, d.h.

  $$\mathfrak{o}_K = \mathbf{Z}[\sqrt{d}].$$

- $d \equiv 3 \bmod 4$: Dies liefert die Bedingung $u^2 + v^2 \equiv 0 \bmod 4$, was nur durch $u \equiv v \equiv 0 \bmod 2$ zu erfüllen ist. Also:

  $$\mathfrak{o}_K = \mathbf{Z}[\sqrt{d}].$$

*Zusammenfassung:* $\mathfrak{o}_K = \mathbf{Z}[\frac{1+\sqrt{d}}{2}]$ für $d \equiv 1 \bmod 4$ und $\mathfrak{o}_K = \mathbf{Z}[\sqrt{d}]$ für $d \equiv 2, 3 \bmod 4$.

**Übung:** Löse die Gleichung $y^2 = x^3 - 11$ durch Faktorisierung in $\mathbf{Z}[\frac{1+\sqrt{-11}}{2}]$, nachdem die Euklidizität dieses Ringes gezeigt wurde. (Ergebnis: $(3, \pm 4)$ und $(15, \pm 58)$)

LEMMA. *Sei $L|K$ eine endliche separable Körpererweiterung vom Grad $n$. Dann liefert*

$$(x, y) \mapsto Sp_{L|K}(xy)$$

*eine nichtausgeartete symmetrische Bilinearform auf dem $K$-Vektorraum $L$. Insbesondere gilt: $\alpha_1, \dots, \alpha_n \in L$ bilden eine $K$-Basis von $L$ genau dann, wenn $\det((Sp(\alpha_i\alpha_j)_{ij}) \neq 0$ ist.*

*Beweis:* Daß $Sp(xy)$ eine symmetrische Bilinearform liefert, ist klar. Wäre $Sp(xy)$ ausgeartet, so gäbe es $u \in L$, $u \neq 0$ mit $Sp(uy) = 0$ für alle $y$. Da aber $L$ ein Körper ist, wäre $Sp$ identisch 0, was nicht der Fall ist. ■

DEFINITION. Bei den Bezeichnungen des Lemmas heißt

$$D(\alpha_1, \dots, \alpha_n) := \det((Sp(\alpha_i\alpha_j))$$

die Diskriminante von $\alpha_1, \dots, \alpha_n$.

SATZ. *Sei $A$ ein Hauptidealring mit Quotientenkörper $K$ und $L$ eine endliche separable Körpererweiterung von $K$ vom Grad $n$. Dann ist der ganze Abschluß $B$ von $A$ in $L$ ein freier $A$-Modul vom Rang $n$. Genauer: Ist $\alpha_1, \ldots, \alpha_n$ eine in $B$ gelegene $K$-Basis von $L$, so gilt:*

$$A\alpha_1 + \cdots + A\alpha_n \subseteq B \subseteq \frac{1}{D(\alpha_1, \ldots, \alpha_n)}[A\alpha_1 + \cdots + A\alpha_n].$$

*Bemerkung:* Jedes $x \in L$ läßt sich schreiben als $x = \frac{\alpha}{a}$ mit $\alpha \in B$ und $a \in A$. Denn: da $x$ algebraisch über $K$ ist, gibt es eine Gleichung:

$$ax^m + a_1 x^{m-1} + \cdots + a_m = 0$$

mit $a, a_1, \ldots, a_m \in A$. Multipliziert man die Gleichung mit $a^{m-1}$, so sieht man, daß $ax$ ganz über $A$ ist, woraus mit $\alpha := ax$ die Behauptung folgt.
Insbesondere kann man jede $K$-Basis von $L$ elementweise mit Elementen aus $A$ multiplizieren, so daß die neue Basis in $B$ liegt.

*Beweis:* Sei $x = \sum x_i \alpha_i$ mit $x_i \in K$ und $x$ ganz über $A$. Dann ist auch $x\alpha_i \in B$, also $Sp(x\alpha_i) \in A$. Aber $Sp(x\alpha_i) = \sum_j Sp(\alpha_i\alpha_j)x_j$. Sei $M = (Sp(\alpha_i\alpha_j))$. Dann gilt:

$$M \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in A^n,$$

also

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \frac{1}{D(\alpha_1, \ldots, \alpha_n)} \tilde{M} A^n.$$

Da $\tilde{M}$ Koeffizienten in $A$ hat, ist $\tilde{M}A^n \subseteq A^n$, also folgt schon

$$A\alpha_1 + \cdots + A\alpha_n \subseteq B \subseteq \frac{1}{D}[A\alpha_1 + \cdots + A\alpha_n]$$

Da $A$ als Hauptidealring vorausgesetzt war, muß jetzt $B$ ein freier $A$-Modul vom Rang $n$ sein. ■

Der folgende Satz gibt weitere Möglichkeiten der Determinantenberechnung an:

SATZ. *Sei $L|K$ endlich separabel vom Grad $n$ und seien $\sigma_1, \ldots, \sigma_n$ die verschiedenen $K$-Einbettungen von $L$ in einen algebraischen Abschluß $\bar{K}$. Seien $\alpha_1, \ldots, \alpha_n \in L$. Dann gilt:*

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

*Ist $L = K(\alpha)$, so ist*

$$D(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) = \prod_{i<j}(\alpha_i - \alpha_j)^2 = \textit{ Diskriminante des Minimalpolynoms von } \alpha.$$

*Beweis:* Wegen $Sp(\alpha_j\alpha_k) = \sum_i \sigma_i\alpha_j\alpha_k$ gilt:

$$\begin{pmatrix} Sp(\alpha_1\alpha_1) & \ldots & Sp(\alpha_1\alpha_n) \\ \vdots & & \vdots \\ Sp(\alpha_n\alpha_1) & \ldots & Sp(\alpha_n\alpha_n) \end{pmatrix} = \begin{pmatrix} \sigma_1\alpha_1 & \ldots & \sigma_n\alpha_1 \\ \vdots & & \vdots \\ \sigma_1\alpha_n & \ldots & \sigma_n\alpha_n \end{pmatrix} \cdot \begin{pmatrix} \sigma_1\alpha_1 & \ldots & \sigma_1\alpha_n \\ \vdots & & \vdots \\ \sigma_n\alpha_1 & \ldots & \sigma_n\alpha_n \end{pmatrix}.$$

Daraus ersieht man

$$(\sigma_i\alpha_j)^t(\sigma_i\alpha_j) = (Sp(\alpha_i\alpha_j))$$

woraus die Behauptung folgt.
Im Fall $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ hat man die Vandermondsche Determinante zu berechnen, woraus auch die zweite Behauptung folgt. ■

*Bemerkung:* Die Diskriminante eines Polynoms $f = a_0x^n + \cdots + a_n$ läßt sich wie folgt mit der Resultante berechnen:

$$D(f) = \frac{1}{a_0}(-1)^{\frac{n(n-1)}{2}} resultant_x(f, f').$$

Unmittelbar aus der linearen Algebra kennt man:

LEMMA. *Seien $(\alpha_i)$ und $(\beta_i)$ $K$-Basen von $L$ mit Übergangsmatrix $t_{ij}$: $\beta_i = \sum t_{ij}\alpha_j$. Dann gilt:*

$$D(\beta_1, \ldots, \beta_n) = \det((t_{ij}))^2 \cdot D(\alpha_1, \ldots, \alpha_n).$$

Damit können wir jetzt definieren:

DEFINITION. Sei $K$ ein Zahlkörper vom Grad $n$ über $\mathbf{Q}$.

- Ist $a$ ein freier $\mathbf{Z}$-Modul vom Rang $n$ in $K$ und $\alpha_1, \ldots, \alpha_n$ eine $\mathbf{Z}$-Basis von $a$, so heißt
$$D(a) := D(\alpha_1, \ldots, \alpha_n)$$
die Diskriminante von $a$.
- Die Diskriminante $D(\mathfrak{o}_K)$ wird die Diskriminante $D_K$ des Zahlkörpers genannt.

*Beweis der Wohldefiniertheit:* Ist $\beta_1, \ldots, \beta_n$ eine weitere $\mathbf{Z}$-Basis von $a$, so gibt es eine Transformationsmatrix $T$ mit Koeffizienten in $\mathbf{Z}$, also in $Gl(\mathbf{Z})$. Die Determinante davon ist eine Einheit in $\mathbf{Z}$, also $\pm 1$, woraus durch Quadrieren die Invarianz folgt. ■

**Beispiel:** Die Diskriminante von $\mathbf{Z}[\sqrt{d}]$ ist die Diskriminante des quadratischen Polynoms $x^2 - d$, also $4d$. Die Diskriminante von $\mathbf{Z}[\frac{1+\sqrt{d}}{2}]$ ist die Diskriminante des Polynoms $x^2 - x + \frac{1-d}{4}$, also $d$. Damit gilt: die Diskriminante des quadratischen Zahlkörpers $\mathbf{Q}(\sqrt{d})$ ist $d$ für $d \equiv 1 \bmod 4$ und $4d$ für $d \equiv 2, 3 \bmod 4$.

*Anmerkungen:*

- Sei $K$ ein Zahlkörper vom Grad $n$ über $\mathbf{Q}$ und seien $\mathfrak{a}$ und $\mathfrak{b}$ zwei freie $\mathbf{Z}$-Moduln in $K$ vom Rang $n$ mit $\mathfrak{b} \subseteq \mathfrak{a}$. Dann gibt es eine $\mathbf{Z}$-Basis $\alpha_1, \ldots, \alpha_n$ von $\mathfrak{a}$ und natürliche Zahlen $d_1, \ldots, d_n$, so daß $d_1\alpha_1, \ldots, d_n\alpha_n$ eine $\mathbf{Z}$-Basis von $\mathfrak{b}$ ist.
- Der Index $[\mathfrak{a} : \mathfrak{b}]$ von $\mathfrak{b}$ in $\mathfrak{a}$ ist die Ordnung der Gruppe $\mathfrak{a}/\mathfrak{b}$, also hier $d_1 \ldots d_n$.
- Für die Diskriminanten erhält man sofort
$$D(\mathfrak{b}) = [\mathfrak{a} : \mathfrak{b}]^2 \cdot D(\mathfrak{a}).$$
- Als Anwendung erhält man sofort: Ist $\mathfrak{a} \subseteq \mathfrak{o}_K$, so gilt $D(\mathfrak{a}) = [\mathfrak{o}_K : \mathfrak{a}]^2 D(\mathfrak{o}_K)$, also
$$[\mathfrak{o}_K : \mathfrak{a}]^2 | D(\mathfrak{a}).$$
Dadurch erhält man eine Abschätzung, wie weit man von dem eventuell unbekannten Ganzheitsring $\mathfrak{o}_K$ entfernt ist.

**Übung:** Zeige, daß $\mathbf{Q}(\sqrt[3]{2})$ den Ganzheitsring $\mathbf{Z}[\sqrt[3]{2}]$ hat, und berechne die Diskriminante.

KAPITEL 3

# Ideale

Im letzten Abschnitt haben wir die Ringe $\mathfrak{o}_K$ eingeführt. Sie sind ganz abgeschlossen. Welche Eigenschaften haben sie? Schön sind faktorielle Ringe. Folgendes Beispiel zeigt aber, daß man das i.a. nicht erwarten kann.

**Beispiel:** Der Ring $A = \mathbf{Z}[\sqrt{-5}]$ ist der Ganzheitsring von $\mathbf{Q}(\sqrt{-5})$. $A$ ist aber nicht faktoriell, wie man an der Zerlegung

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

sehen kann (Beweis als Übung!) Wie läßt sich diese Vieldeutigkeit deuten? Kummer hatte die Idee, dies durch Einführung von *idealen Zahlen* zu erklären:

$$2 = \mathfrak{p}_1\mathfrak{p}_2, \quad 3 = \mathfrak{p}_3\mathfrak{p}_4, \quad 1 + \sqrt{-5} = \mathfrak{p}_1\mathfrak{p}_3, \quad 1 - \sqrt{-5} = \mathfrak{p}_2\mathfrak{p}_4.$$

Für uns sind dies Ideale:

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

(Zeige dann die Gültigkeit obiger Zerlegung!) Wir werden zeigen, daß in $\mathfrak{o}_K$ Ideale sich eindeutig in ein Produkt von Primidealen zerlegen lassen.

*Erinnerung:* Ein Primideal $\mathfrak{p}$ eines Ringes $A$ ist ein Ideal $\neq A$, das eine der folgenden äquivalenten Bedingungen erfüllt:

- $A/\mathfrak{p}$ ist ein Integritätsring.
- $xy \in \mathfrak{p}$ impliziert $x \in \mathfrak{p}$ oder $y \in \mathfrak{p}$.

Ein Ideal $\mathfrak{m} \subseteq A$ heißt maximal, wenn $A/\mathfrak{m}$ ein Körper ist. Jedes maximale Ideal ist ein Primideal.

**Bemerkungen:**

1. $a|b \iff (b) \subseteq (a)$
2. Wir schreiben auch für Ideale $\mathfrak{a}|\mathfrak{b}$, wenn $\mathfrak{b} \subseteq \mathfrak{a}$ gilt.
3. Ein Primelement ist ein $\pi$, das keine Einheit ist, und die Bedingung erfüllt: $\pi|ab$ impliziert $\pi|a$ oder $\pi|b$, d.h. $ab \in (\pi)$ impliziert $a \in (\pi)$ oder $b \in (\pi)$, d.h. $(\pi)$ ist Primideal. Primideale sind Verallgemeinerungen von Primelementen.
4. Ist $\mathfrak{p}$ Primideal und gilt $\mathfrak{ab} \subseteq \mathfrak{p}$, so folgt $\mathfrak{a} \subseteq \mathfrak{p}$ oder $\mathfrak{b} \subseteq \mathfrak{p}$. Anders geschrieben: $p|\mathfrak{ab}$ impliziert $\mathfrak{p}|\mathfrak{a}$ oder $\mathfrak{p}|\mathfrak{b}$.
5. Für $\mathfrak{o}$-Moduln $M$ und $N$ in $K$ definiert man Produkt $MN$ und Summe $M + N$.

$$MN = \{\sum x_i y_i : x_i \in M, y_i \in N\}.$$

**Beispiel:** In $A = \mathbf{Z}[\sqrt{-5}]$ ist $\mathfrak{p} = (2, 1 + \sqrt{-5})$ ein Primideal, denn: $A = \mathbf{Z}[x]/(x^2 + 5)$ und damit:

$$A/\mathfrak{p} = \mathbf{Z}[x]/(x^2 + 5, 2, 1 + x) = \mathbf{F}_2[x]/(x^2 + 1, x + 1) = \mathbf{F}_2$$

Also ist $A/\mathfrak{p}$ ein Körper und damit $\mathfrak{p}$ maximales Ideal, insbesondere Primideal.

LEMMA. *Sei $K$ ein Zahlkörper vom Grad $n$ (über $\mathbf{Q}$). Dann ist jedes Ideal $\mathfrak{a} \neq 0$ von $\mathfrak{o}_K$ ein freier $\mathbf{Z}$-Modul vom Rang $n$, insbesondere also endlich erzeugt.*

*Beweis:* Sei $a_1, \ldots, a_n$ eine $\mathbf{Z}$-Basis von $\mathfrak{o}_K$ und $b \in \mathfrak{a}$ mit $b \neq 0$. Dann gilt:

$$\mathbf{Z}ba_1 + \cdots + \mathbf{Z}ba_n \subseteq \mathfrak{a} \subseteq \mathbf{Z}a_1 + \cdots + \mathbf{Z}a_n = \mathfrak{o}_K,$$

also folgt die Behauptung, da $\mathfrak{a}$ zwischen zwei freien $\mathbf{Z}$-Moduln vom Rang $n$ liegt. ■

**Erinnerung:** Ein noetherscher Ring $A$ ist ein kommutativer Ring, in dem eine der folgenden äquivalenten Bedingungen gilt:

- Jedes Ideal $\mathfrak{a}$ von $A$ ist endlich erzeugt, d.h. es gibt $a_1, \ldots, a_n \in A$ mit $\mathfrak{a} = (a_1, \ldots, a_n)$.
- Jede aufsteigende Folge von Idealen wird stationär: $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ldots$, dann gibt es ein $m$ mit $\mathfrak{a}_m = \mathfrak{a}_{m+1} = \ldots$.
- Jede nicht leere Menge von Idealen besitzt ein maximales Element bezüglich der Inklusion.

**Beispiele:**

1. Körper, Hauptidealringe
2. Der Basissatz von Hilbert besagt, daß für einen noetherschen Ring $A$ auch der Polynomring $A[x]$ noethersch ist. Insbesondere ist $K[x_1, \ldots, x_n]$ noethersch.
3. Nicht noethersch ist $K[x_1, x_2, \ldots]$.

SATZ. *Der Ganzheitsring $\mathfrak{o}_K$ eines Zahlkörpers $K$ ist ganz abgeschlossen, noethersch und jedes Primideal $\neq 0$ ist maximal.*

DEFINITION. Ein ganz abgeschlossener noetherscher Integritätsring, in dem jedes Primideal $\neq 0$ maximal ist, heißt Dedekindring.

Also ist $\mathfrak{o}_K$ ein Dedekindring.

*Beweis des Satzes:*

- $\mathfrak{o}_K$ ist ganz abgeschlossen, wie wir schon früher feststellten.
- Da jedes Ideal von $\mathfrak{o}_K$ ein freier $\mathbf{Z}$-Modul vom Rang $n$ ist, ist jedes Ideal insbesondere endlich erzeugt. Also ist $\mathfrak{o}_K$ noethersch.
- Sei $\mathfrak{p} \neq 0$ ein Primideal in $\mathfrak{o}_K$. Wir müssen zeigen, daß $\mathfrak{o}_K/\mathfrak{p}$ ein Körper ist. $\mathbf{Z} \cap \mathfrak{p}$ ist ein Primideal $\neq 0$ in $\mathbf{Z}$, denn sei $x \in \mathfrak{p}$, $x \neq 0$, dann sieht das Minimalpolynom so aus:

  $$x^m + a_1 x^{m-1} + \cdots + a_m = 0$$

  mit $a_m \neq 0$. Wegen $a_m \in \mathfrak{p} \cap \mathfrak{o}_K$ ist also $\mathfrak{p} \cap \mathfrak{o}_K$ ein Primideal $\neq 0$ in $\mathbf{Z}$, also von der Form $(p)$ mit einer Primzahl $p$. Nun ist also $\mathfrak{o}_K/\mathfrak{p}$ endlich erzeugt über $\mathbf{Z}/(p)$ und daher muß $\mathfrak{o}_K/\mathfrak{p}$ bereits ein Körper sein ($K[\alpha] = K(\alpha)$). Daraus folgt die Behauptung.

Im Folgenden steht $\mathfrak{o}$ für einen beliebigen Dedekindring.

SATZ. *Jedes von 0 und $\mathfrak{o}$ verschiedene Ideal von $\mathfrak{o}$ besitzt eine bis auf die Reihenfolge eindeutige Zerlegung*

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

*in Primideale $\mathfrak{p}_i$.*

Bevor wir dies beweisen zeigen wir zwei Lemmata.

LEMMA. *Zu jedem Ideal $\mathfrak{a} \neq 0$ von $\mathfrak{o}$ gibt es Primideale $\mathfrak{p}_i$ mit*

$$\mathfrak{a} \supseteq \mathfrak{p}_1 \ldots \mathfrak{p}_r,$$

*oder anders geschrieben:*

$$\mathfrak{a} | \mathfrak{p}_1 \ldots \mathfrak{p}_r.$$

*Beweis:* Sei $M = \{\mathfrak{a}$ Ideal, das das Lemma nicht erfüllt$\}$. Angenommen: $M \neq \emptyset$. Sei $\mathfrak{a} \in M$ ein maximales Element. Dann ist $\mathfrak{a}$ kein Primideal, also gibt es $a, b$ mit $ab \in \mathfrak{a}$, aber $a, b \notin \mathfrak{a}$. Die Ideale $(a) + \mathfrak{a}$ und $(b) + \mathfrak{a}$ liegen dann nicht in $M$, erfüllen also das Lemma. Nun ist aber $\mathfrak{a} \subseteq ((a) + \mathfrak{a})((b) + \mathfrak{a})$, also erfüllt auch $\mathfrak{a}$ das Lemma, ein Widerspruch. Mithin ist $M = \emptyset$. ■

LEMMA. *Ist* $\mathfrak{p}$ *ein Primideal* $\neq 0$ *von* $\mathfrak{o}$ *und*

$$\mathfrak{p}^{-1} := \{x \in K : x\mathfrak{p} \subseteq \mathfrak{o}\},$$

*so gilt:*

1. $\mathfrak{p}^{-1} \neq \mathfrak{o}$
2. $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathfrak{a}$, *wo* $\mathfrak{a}$ *ein Ideal* $\neq 0$ *ist.*
3. $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{o}$

*Beweis:*

1. Wähle $0 \neq a \in \mathfrak{p}$ und nach dem vorhergehenden Lemma $\mathfrak{p}_1 \dots \mathfrak{p}_r \subseteq (a) \subseteq \mathfrak{p}$, o.E. $r$ minimal. Weiter ist o.E. $\mathfrak{p}_1 = \mathfrak{p}$ und damit $\mathfrak{p}_2 \dots \mathfrak{p}_r \not\subseteq (a)$, also gibt es $b \in \mathfrak{p}_2 \dots \mathfrak{p}_r$ mit $b \notin (a)$. Damit ist zunächst $\frac{b}{a} \notin \mathfrak{o}$, aber $b\mathfrak{p} \subseteq (a)$, also $\frac{b}{a}\mathfrak{p} \subseteq \mathfrak{o}$, d.h. $\frac{b}{a} \in \mathfrak{p}^{-1}$.
2. Würde gelten $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$, so wäre $\mathfrak{p}$ ganz über $\mathfrak{o}$, also $\mathfrak{p}^{-1} \subseteq \mathfrak{o}$, ein Widerspruch zu 1.
3. $\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathfrak{o}$, und da $\mathfrak{p}$ maximal ist, folgt sofort $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{o}$. ■

*Beweis des Satzes:*

- Existenz: Sei $M = \{\mathfrak{a}$ Ideal ohne Primidealzerlegung$\}$. Wir wollen zeigen, daß $M$ leer ist. Angenommen, dies ist nicht der Fall. Dann gibt es maximales Element in $M$: $\mathfrak{a}$. $\mathfrak{a}$ ist kein maximales Ideal, also gibt es ein Primideal $\mathfrak{p}$ mit $\mathfrak{a} \subseteq \mathfrak{p}$. Dann ist aber $\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{o}$, also ist $\mathfrak{a}\mathfrak{p}^{-1}$ ein Ideal, das nicht in $M$ liegt, hat also eine Primidealzerlegung. Multiplikation mit $\mathfrak{p}$ liefert eine Primidealzerlegung für $\mathfrak{a}$, ein Widerspruch zur Annahme.
- Eindeutigkeit: Sei $\mathfrak{p}_1 \dots \mathfrak{p}_r = \mathfrak{q}_1 \dots \mathfrak{q}_s$. Dann gilt $\mathfrak{p}_1 | \mathfrak{q}_1 \dots \mathfrak{q}_s$, also muß es mindestens einen der Faktoren teilen, o.E. $\mathfrak{q}_1$. Wegen der Maximalität der Primideale ist aber dann schon $\mathfrak{p}_1 = \mathfrak{q}_1$. Multiplikation der Gleichung mit $\mathfrak{p}_1^{-1}$ liefert eine Gleichung mit einem Faktor weniger. Betrachte nun $\mathfrak{p}_2$, etc. ■

**Bemerkungen:**

1. Sind $\mathfrak{p}_i$, $i \in I$ die von 0 verschiedenen Primideale von $\mathfrak{o}$, so haben die Ideale $\neq 0$ von $\mathfrak{o}$ die Gestalt:
$$\prod_i \mathfrak{p}_i^{n_i},$$
wobei nur endlich viele $n_i \neq 0$ sind.
2. Wie findet man die Primideale von $\mathfrak{o}_K$? Sei $\mathfrak{p}$ ein von 0 verschiedenes Primideal. Dann ist $\mathfrak{o}_K/\mathfrak{p}$ endlich und ein Körper, also von endlicher Charakteristik $p$. D.h. $p = 0$ in $\mathfrak{o}_K/\mathfrak{p}$, also $p \in \mathfrak{p}$. Damit gilt: $\mathfrak{p}|(p)$. Ist also $(p) = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$ die Primidealzerlegung von $(p)$, so ist $\mathfrak{p}$ eines der $\mathfrak{p}_i$. Um die Primideale in $\mathfrak{o}_K$ zu finden, muß man also 'nur' die Primzahlen von $\mathbf{Z}$ in $\mathfrak{o}_K$ zerlegen.

**Beispiel:** Wie sehen die nichttrivialen Primideale von $\mathbf{Z}[\sqrt{-5}]$ aus? Wir bemerken: $\mathfrak{o}_K = \mathbf{Z}[x]/(x^2+5)$, also

$$\mathfrak{o}_K/(p) = \mathbf{F}_p[x]/(x^2+5)$$

- $p = 5$: $\mathfrak{p}_5 = (\sqrt{-5})$ ist Primideal und $\mathfrak{p}_5^2 = (5)$.
- Falls $x^2+5$ irreduzibel in $\mathbf{F}_p[x]$ ist, so ist $\mathfrak{o}_K/(p)$ ein Körper, also $(p)$ auch Primideal in $\mathfrak{o}_K$. Dies ist genau dann der Fall, wenn $-5$ kein Quadrat modulo $p$ ist, d.h. wenn $\left(\frac{-5}{p}\right) = -1$ mit dem Legendre-Symbol.
- Falls $-5$ ein Quadrat modulo $p$ ist: $-5 = a^2 + bp$, (o.E. $|b| < p$), dann ist $\mathfrak{p} = (p, a+\sqrt{-5})$ ein Primideal wegen
$$\mathfrak{o}_K/(p, a+\sqrt{-5}) = \mathbf{Z}[x]/(x^2+5, p, a+x) \simeq \mathbf{F}_p.$$
Weiter gilt:
$(p, a+\sqrt{-5})(p, a-\sqrt{-5}) = (p^2, p(a-\sqrt{-5}), p(a+\sqrt{-5}), a^2+5) = p(p, a \pm \sqrt{-5}, b) = (p)$
da $b$ und $p$ teilerfremd sind. Wann gilt:$\mathfrak{p} = \mathfrak{q}$? Angenommen: Es gilt die Gleichheit. Dann ist $a - \sqrt{-5}$ in $\mathfrak{p}$, also auch $2a$. Da $a$ teilerfremd zu $p$ ist, liegt also 2 in $\mathfrak{p}$. Dies ist aber nur möglich für $p = 2$.
- $p = 2$: $(2, 1+\sqrt{-5})^2 = (2)$.

- Das quadratische Reziprozitätsgesetz besagt nun gerade, daß das Zerlegungsverhalten von $(p)$ in $\mathfrak{o}_K$ nur von der Kongruenzklasse von $p$ modulo 20 abhängt.

DEFINITION. Ein gebrochenes Ideal (fractional ideal) von $K$ ist ein endlich erzeugter $\mathfrak{o}$-Untermodul von $K$.

**Bemerkungen:**

1. Sei $\mathfrak{a}$ ein gebrochenes Ideal $\neq 0$. Wegen der endlichen Erzeugtheit gibt es einen gemeinsamen Nenner, d.h. ein $c \in \mathfrak{o}$ mit $c\mathfrak{a} \subseteq \mathfrak{o}$. Dann ist $\mathfrak{b} := c\mathfrak{a}$ ein Ideal von $\mathfrak{o}$, also $\mathfrak{a} = \frac{1}{c}\mathfrak{b}$.
2. Sei $\mathfrak{a}$ ein Ideal von $K$. Dann ist
$$\mathfrak{a}^{-1} := \{x \in K : x\mathfrak{a} \subseteq \mathfrak{o}\}$$
ein gebrochenes Ideal von $K$, denn ist $\alpha_1 \dots \alpha_n$ eine $\mathbf{Z}$-Basis von $\mathfrak{a}$, so gilt:
$$x \in \mathfrak{a}^{-1} \iff x\alpha_i \in \mathfrak{o} \iff x \in \frac{1}{\alpha_i}\mathfrak{o},$$
also $\mathfrak{o} \subset \mathfrak{a}^{-1} = \cap_i \frac{1}{\alpha_i}\mathfrak{o} \subseteq \frac{1}{\alpha_1 \dots \alpha_n}\mathfrak{o}$.

SATZ. *Die gebrochenen Ideale bilden eine abelsche Gruppe, die Idealgruppe $I_K$ von $K$. Das neutrale Element ist $\mathfrak{o}$, das Inverse zu $\mathfrak{a}$ ist*
$$\mathfrak{a}^{-1} = \{x \in K : x\mathfrak{a} \subseteq \mathfrak{o}\}.$$

*Beweis:*

- Da $I_K$ bezüglich Multiplikation abgeschlossen ist, ist klar. Auch daß $\mathfrak{o}$ neutrales Element ist. Bleibt noch die Existenz von Inversen zu zeigen.
- Ist $\mathfrak{a} = \frac{1}{c}\mathfrak{p}_1 \dots \mathfrak{p}_r$ ein gebrochenes Ideal von $\mathfrak{o}$, so gilt mit $\mathfrak{b} = c\mathfrak{p}_1^{-1} \dots \mathfrak{p}_r^{-1}$ die Beziehung $\mathfrak{a}\mathfrak{b} = \mathfrak{o}$, d.h. $\mathfrak{b}$ ist invers zu $\mathfrak{a}$.
- Wir zeigen: $\mathfrak{b} = \mathfrak{a}^{-1}$. Ist $x \in \mathfrak{b}$, so gilt $x\mathfrak{a} \subseteq \mathfrak{o}$, also $x \in \mathfrak{a}^{-1}$. Ist umgekehrt $x \in \mathfrak{a}^{-1}$, so gilt $x\mathfrak{a} \subseteq \mathfrak{o}$, also $x\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{b}$, also $x \in \mathfrak{b}$, woraus alles folgt.

KOROLLAR. *Jedes gebrochene Ideal $\mathfrak{a}$ besitzt eine eindeutige Produktdarstellung*
$$\mathfrak{a} = \prod \mathfrak{p}^{\nu_\mathfrak{p}},$$
*nur endliche viele $\nu_\mathfrak{p}$ verschieden von 0 sind. Also ist $I_K$ die von den Primidealen $\neq 0$ erzeugte freie abelsche Gruppe.*

Die Hauptideale $(f) = f\mathfrak{o}$ mit $f \in K$, $f \neq 0$ bilden eine Untergruppe von $I_K$, die Gruppe $P_K$ der Hauptideale.

DEFINITION. Die Faktorgruppe $H_K = I_K/P_K$ heißt Klassengruppe oder auch Idealklassengruppe von $K$.

Die Klassengruppe spielt eine wichtige Rolle in der Zahlentheorie. Sie mißt die Abweichung von $\mathfrak{o}_K$ von einem Hauptidealring.

Zum Schluß dieses Paragraphen wollen wir noch die Norm für Ideale eines Zahlkörpers einführen. Für ein ganzes Ideal $\mathfrak{a}$ von $\mathfrak{o}_K$ setzen wir:
$$N(\mathfrak{a}) := [\mathfrak{o}_K : \mathfrak{a}] = \#\mathfrak{o}_K/\mathfrak{a}.$$

LEMMA. *Ist $\mathfrak{a} = \mathfrak{p}_1^{n_1} \dots \mathfrak{p}_r^{n_r}$, so gilt:*
$$N(\mathfrak{a}) = N(\mathfrak{p}_1)^{n_1} \dots N(\mathfrak{p}_r)^{n_r}$$
*Ist $\alpha \in \mathfrak{o}_K$, so ist $N((\alpha)) = |N_{K|\mathbf{Q}}(\alpha)|$.*

*Beweis:*

- Nach dem chinesischen Restsatz gilt:
$$\mathfrak{o}_K/\mathfrak{a} = \mathfrak{o}_K/\mathfrak{p}_1^{n_1} \oplus \dots \oplus \mathfrak{o}_K/\mathfrak{p}_r^{n_r},$$
also
$$N(\mathfrak{a}) = N(\mathfrak{p}_1^{n_1}) \dots N(\mathfrak{p}_r^{n_r}).$$

- Wir müssen nun noch $N(\mathfrak{p}^i)$ ausrechnen. Sei $a \in \mathfrak{p}^m$, aber $a \notin \mathfrak{p}^{m+1}$. Dann ist $\mathfrak{p}^{m+1} \subset \mathfrak{p}^{m+1} + (a) \subseteq \mathfrak{p}^m$. Wegen der eindeutigen Primidealzerlegung ist $\mathfrak{p}^{m+1} + (a) = \mathfrak{p}^m$, also ist $\mathfrak{p}^m/\mathfrak{p}^{m+1}$ ein eindimensionaler $\mathfrak{o}_K/\mathfrak{p}$-Vektorraum, insbesondere:
$$[\mathfrak{o}_K : \mathfrak{p}] = [\mathfrak{p}^m : \mathfrak{p}^{m+1}].$$
Und schließlich:
$$N(\mathfrak{p}^n) = [\mathfrak{o} : \mathfrak{p}^n] = [\mathfrak{o} : \mathfrak{p}][\mathfrak{p} : \mathfrak{p}^2] = \cdots = N(\mathfrak{p})^n$$
Daraus folgt die Behautpung.
- $N(\alpha)$ ist die Determinante einer Übergangsmatrix von $\mathfrak{o}_K$ nach $\alpha\mathfrak{o}_K$. Daraus folgt die andere Behauptung.

Trivialerweise setzt sich die Idealnorm dann auf $I_K$ multiplikativ fort.

KAPITEL 4

# Gitter

Schon beim Nachweis der Euklidizität des Ringes $\mathbf{Z}[\sqrt{-2}]$ haben wir gesehen, wie hilfreich es war, den Ring als Gitter in $\mathbf{C} \simeq \mathbf{R}^2$ zu betrachten. Der allgemeine Formalismus geht auf Minkowski zurück und wird als Geometrie der Zahlen bezeichnet.

DEFINITION. Eine Untergruppe $\Gamma$ des $\mathbf{R}^n$ heißt Gitter, wenn es eine Basis $v_1, \ldots, v_n$ des $\mathbf{R}^n$ gibt mit

$$\Gamma = \mathbf{Z}v_1 + \cdots + \mathbf{Z}v_n.$$

Die Menge

$$\{x_1 v_1 + \ldots x_n v_n : 0 \leq x_i < 1\}$$

heißt eine Grundmasche des Gitters $\Gamma$ - was natürlich von der Basiswahl abhängt -, den Inhalt der Grundmasche bezeichnen wir mit $vol(\Gamma)$, also:

$$vol(\Gamma) = |\det(v_1, \ldots, v_n)|.$$

**Bemerkung:** $vol(\Gamma)$ ist wohldefiniert, denn ist $w_1, \ldots, w_n$ eine andere Gitterbasis, so gibt es eine Transformationsmatrix $T \in GL_n(\mathbf{Z})$ mit $v_i = Tw_i$. Wegen $\det(T) = \pm 1$ ist dann $vol(\Gamma)$ basisunabhängig.

**Beispiele:**

1. $\mathbf{Z}^n$ ist ein Gitter im $\mathbf{R}^n$.
2. $\mathbf{Z} + \mathbf{Z}\sqrt{2}$ ist kein Gitter in $\mathbf{R}$.

SATZ. *Eine Untergruppe $\Gamma \subseteq \mathbf{R}^n$ ist genau dann ein Gitter, wenn sie diskret ist und den $\mathbf{R}^n$ aufspannt.*

Dabei heißt eine Untergruppe $\Gamma$ diskret, wenn 0 eine $\epsilon$-Umgebung $U$ besitzt, sodaß $U \cap \Gamma = \{0\}$ ist. Das gleiche gilt dann auch für jeden anderen Punkt von $\Gamma$. Außerdem gilt dann: In jeder kompakten Menge des $\mathbf{R}^n$ gibt es nur endlich viele Punkte von $\Gamma$.

*Beweis:*

1. Die eine Richtung ist trivial.
2. Sei $\Gamma$ diskret und spanne $\Gamma$ den $\mathbf{R}^n$ auf. Dann enthält $\Gamma$ eine $\mathbf{R}$-Basis des $\mathbf{R}^n$: $u_1, \ldots, u_n$. Also ist $\Gamma_0 = \mathbf{Z}u_1 + \cdots + \mathbf{Z}u_n$ ein Gitter. Jedes Element von $\Gamma/\Gamma_0$ hat einen Repräsentanten in der Grundmasche von $\Gamma_0$. Da diese beschränkt ist, ist also auch $\Gamma/\Gamma_0$ endlich. Sei $m = \#\Gamma/\Gamma_0$. Dann ist
$$\Gamma \subseteq \mathbf{Z}\frac{1}{m}u_1 + \ldots \mathbf{Z}\frac{1}{m}u_n,$$
also muß $\Gamma$ selbst auch frei sein. ■

Zur Erinnerung: Eine Teilmenge $X \in \mathbf{R}^n$ nennt man zentralsymmetrisch (bzgl. des Nullpunkts), wenn gilt: $x \in X \Rightarrow -x \in X$. Eine Teilmenge $X$ nennt man konvex, wenn mit zwei Punkten $x$, $y$ aus $X$ auch deren Verbindungsstrecke in $X$ liegt, d.h. $x, y \in X \Rightarrow tx + (1-t)y \in X$ für alle $0 \leq t \leq 1$.
Der entscheidende Satz ist der nun folgende Gitterpunktsatz von Minkowski.

SATZ. *Ist $\Gamma$ ein Gitter des $\mathbf{R}^n$ und $X$ eine symmetrische, konvexe Teilmenge mit*

$$vol(X) > 2^n vol(\Gamma),$$

*so enthält $X$ einen von 0 verschiedenen Gitterpunkt von $\Gamma$.*

*Beweis:*

- Es genügt zu zeigen, daß es zwei verschiedene Gitterpunkte $\gamma_1, \gamma_2$ gibt mit
$$(\frac{1}{2}X + \gamma_1) \cap (\frac{1}{2}X + \gamma_2) \neq \emptyset.$$
Denn dann gibt es $x_1, x_2 \in X$ mit
$$\frac{1}{2}x_1 + \gamma_1 = \frac{1}{2}x_2 + \gamma_2,$$
also liegt
$$\gamma_1 - \gamma_2 = \frac{1}{2}x_1 - \frac{1}{2}x_2$$
im Durchschnitt von $\Gamma$ mit $X$.
- Wir nehmen an, die Mengen $\frac{1}{2}X + \gamma$ wären paarweise disjunkt. Sei $M$ eine Grundmasche des Gitters. Dann ist:
$$\begin{aligned} vol(M) &\geq \sum vol(M \cap (\frac{1}{2}X + \gamma) = \\ &= \sum vol((M - \gamma) \cap \frac{1}{2}X) = \\ &= vol(\frac{1}{2}X) = \frac{1}{2^n} vol(X). \end{aligned}$$
Dies ist aber ein Widerspruch zur Voraussetzung. ■

**Übung:** Zeige, daß der Koeffizient $2^n$ im Minkowskischen Gitterpunktsatz bestmöglich ist.

KAPITEL 5

# Die Endlichkeit der Klassenzahl

Ziel: Wir wollen zeigen, daß die Klassenzahl $h_K = \#H_K$ endlich ist. Dazu werden wir zeigen, daß in jeder Idealklasse ein ganzes Ideal mit Norm $\leq C_K$ existiert, wo $C_K$ eine nur von $K$ abhängige Konstante ist.

Sei $K$ ein Zahlkörper vom Grad $n$ über $\mathbf{Q}$. Dann gibt es $n$ Einbettungen von $K$ in $\mathbf{C}$: $\sigma_1, \ldots, \sigma_n$.
Ein $\sigma_i$ heißt reell, wenn $\sigma(K) \subseteq \mathbf{R}$, ansonsten komplex. Ist $\sigma_i$ komplex, so ist $\bar{\sigma_i}$ eine weitere komplexe Einbettung, die von $\sigma_i$ verschieden ist.
Seien $\sigma_1, \ldots, \sigma_{r_1}$ die reellen Einbettungen und $\sigma_{r_1+1}, \overline{\sigma}_{r_1+1}, \ldots, \sigma_{r_1+r_2}, \overline{\sigma}_{r_1+r_2}$ die komplexen. Dann gilt also $r_1 + 2r_2 = n$.
Anders ausgedrückt: Sei $K = \mathbf{Q}(\alpha)$ und $f(x)$ das Minimalpolynom von $\alpha$. Dann hat $f$ komplexe Nullstellen: reelle, ...

Wir definieren $\phi : K \to \mathbf{R}^n$ durch:

$$\phi(x) = (\sigma_1 x, \ldots, \sigma_{r_1} x, Re\sigma_{r_1+1}x, \ldots, Re\sigma_{r_1+r_2}x, Im\sigma_{r_1+1}x, \ldots).$$

LEMMA. *Ist $\mathfrak{a}$ ein gebrochenes Ideal von $K$ mit Diskriminante $D(\mathfrak{a})$, so ist $\phi(\mathfrak{a})$ ein Gitter in $\mathbf{R}^n$ mit Volumen*

$$vol(\phi(\mathfrak{a})) = \frac{1}{2^{r_2}}\sqrt{|D(\mathfrak{a})|}.$$

*Beweis:* Sei $a_1, \ldots, a_n$ eine $\mathbf{Z}$-Basis von $\mathfrak{a}$. Wir berechnen die Determinante der Matrix $(\phi(a_1), \ldots, \phi(a_n))^t$. Es ist

$$|\sigma_1 a_j, \ldots, \sigma_{r_1} a_j, Re\sigma_{r_1+1}a_j, \ldots, Im\sigma_{r_1+1}a_j| = (i/2)^{r_2}|\sigma_1 a_j, \ldots, \sigma_{r_1+r_2}\bar{} a_j|,$$

woraus sofort folgt, daß die Vektoren $\phi(a_j)$ eine $\mathbf{R}$-Basis des $\mathbf{R}^n$ bilden, d.h. $\phi(\mathfrak{a})$ ist Gitter mit Volumen

$$vol(\phi(\mathfrak{a})) = \frac{1}{2^{r_2}}\sqrt{|D(\mathfrak{a})|}.$$

Beachte: $(a,b) = (a+ib, b) = \frac{1}{2i}(a+ib, 2ib) = \frac{1}{2i}(a+ib, -a+ib) = \frac{i}{2}(a+ib, a-ib)$. ■

LEMMA. *Die Menge*

$$M_t = \{\sum_{i=1}^{r_1} |x_i| + 2\sum_{i=r_1+1}^{r_1+r_2} \sqrt{x_i^2 + x_{i+r_2}^2} \leq t\}$$

*ist konvex, zentralsymmetrisch und hat Volumen*

$$vol(M) = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{t^n}{n!}.$$

*Beweis:* Die Eigenschaft zentralsymmetrisch ist klar, die Eigenschaft konvex folgt aus der Dreiecksungleichung für Absolutbeträge unter Beachtung von $\sqrt{x^2+y^2} = |x+iy|$. Nun zur Volumenberechnung:

- Wir führen Polarkoordinaten ein für $x_{r_1+i} = y_i \cos\varphi_i$ und $x_{r_1+r_2+i} = y_i \sin\varphi_i$. Dann ist $dx_{r_1+i}dx_{r_1+r_2+i} = y_i dy_i d\varphi_i$, und damit

$$vol(M_t) = \int_{M_t} dx_1 \ldots dx_n = 2^{r_1}(2\pi)^{r_2}\int_{\sum x_i + 2\sum y_j \leq t} y_1 \ldots y_{r_2} dx_1 \ldots dx_{r_1} dy_1 \ldots dy_{r_2}.$$

- Zu zeigen ist also

$$\int_{\sum x_i + 2\sum y_j \leq t} y_1 \ldots y_{r_2} dx_1 \ldots dx_{r_1} dy_1 \ldots dy_{r_2} = \frac{1}{4^{r_2}}\frac{t^n}{n!}.$$

  Wir machen Induktion nach $r_2$.

- $r_2 = 0$: Es ist zu zeigen:
$$\int_{\sum x_i \le t} dx_1 \dots dx_n = \frac{t^n}{n!}.$$
- Allgemein:

$$\begin{aligned}
\int_{M_t} dx_1 \dots dx_n &= 2^{r_1}(2\pi)^{r_2} \int_{y_{r_2}=0}^{t/2} [\int_{\sum x_i + 2\sum y_j \le t - 2y_{r_2}} y_1 \dots y_{r_2-1} dx_1 \dots dx_{r_1} dy_1 \dots dy_{r_2-1}] y_{r_2} dy_{r_2} = \\
&= 2^{r_1}(2\pi)^{r_2} \int_0^{t/2} \frac{1}{4^{r_2-1}} \frac{(t-2y)^{n-2}}{(n-2)!} y dy = \\
&= 2^{r_1}(\frac{\pi}{2})^{r_2} \int_0^t \frac{(t-z)^{n-2} z dz}{(n-2)!} = \\
&= 2^{r_1}(\frac{\pi}{2})^{r_2} \frac{1}{(n-2)!} \int_0^t (t-z)^{n-2} z dz
\end{aligned}$$

Nun ist aber

$$\begin{aligned}
\int_0^t (t-z)^{n-2} z dz &= -\int_0^t (t-z)^{n-1} dz + t\int_0^t (t-z)^{n-2} dz = \\
&= -\int_0^t z^{n-1} dz + t\int_0^t z^{n-2} dz = \\
&= -\frac{t^n}{n} + t\frac{t^{n-1}}{n-1} = \frac{1}{n(n-1)} t^n,
\end{aligned}$$

woraus dann die Behauptung unmittelbar folgt. ■

SATZ. *Ist $\mathfrak{a}$ ein gebrochenes Ideal von $K$, so gibt es $\alpha \neq 0$ in $\mathfrak{a}$ mit*
$$|N(\alpha)| \le \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|D_K|} N\mathfrak{a}.$$

*Beweis:* Wir betrachten die Bedingung
$$vol(M_t) > 2^n vol(\phi(\mathfrak{a})$$
Dies bedeutet:
$$t^n > \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|D_K|} N\mathfrak{a}.$$
Wähle
$$t^n = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|D_K|} N\mathfrak{a} + \epsilon$$
Dann gibt es ein $\alpha \neq 0$ in $\mathfrak{a}$ mit (unter Benutzung der Ungleichung zwischen geometrischem und arithmetischem Mittel):
$$N\alpha \le \left(\frac{t}{n}\right)^n = \dots + \frac{\epsilon}{n^n}$$
Da $\epsilon > 0$ beliebig gewählt werden kann, folgt die Behauptung. ■

SATZ. *In jeder Idealklasse von $K$ gibt es ein ganzes Ideal $\mathfrak{a}$ mit*
$$N\mathfrak{a} \le \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d_K|}$$

*Beweis:* Sei $\mathfrak{b}$ ein Repräsentant einer Idealklasse $C$. Dann gibt es ein $\alpha \neq 0$ in $\mathfrak{b}^{-1}$ mit $N(\alpha) \le C_K \sqrt{|D_K|} N\mathfrak{b}^{-1}$. Faktorisieren wir: $(\alpha) = \mathfrak{a}\mathfrak{b}^{-1}$, so liegt $\mathfrak{a}$ in der Klasse $C$ und hat Norm
$$N\mathfrak{a} = \frac{N\alpha}{N\mathfrak{b}^{-1}} \le C_K \sqrt{|D_K|},$$
wie behauptet. ■

Wie findet man nun Repräsentanten für $H_K$?

- Wegen der eindeutigen Primidealzerlegung, genügt es, also Primideale mit Norm $\leq c$ zu finden. Ist $\mathfrak{p}$ ein Primideal, dann gibt es eine Primzahl $p$ mit $p \in \mathfrak{p}$, also $\mathfrak{p}|p$. Faktorisieren von $(p)$ ergibt:
$$(p) = \mathfrak{p}^e \mathfrak{p}_2^{e_2} \dots \mathfrak{p}_r^{e_r},$$
wegen $Np = p^n$ ist also $N\mathfrak{p}$ eine $p$-Potenz.
- Um die Primideale mit Norm $\leq c$ zu finden, muß man also nur die Primzahlen $p \leq c$ in $\mathfrak{o}_K$ faktorisieren und die zugehörigen Primideale betrachten.

FOLGERUNG. *Die Klassengruppe $H_K$ ist endlich.*

**Beispiel:** $K = \mathbf{Q}(\sqrt[3]{2})$ hat Ganzheitsring $\mathbf{Z}[\sqrt[3]{2}]$ mit Diskriminante $-108$. Jede Idealklasse enthält ein ganzes Ideal mit Norm $\leq \frac{4}{\pi} 3! 3^3 \sqrt{108} = 2.94\dots$. Nun ist aber
$$(2) = (\sqrt[3]{2})^3$$
die Primidealzerlegung von 2 und $(\sqrt[3]{2})$ ist ein Hauptideal. Also ist $H_K = 1$, d.h. $\mathbf{Z}[\sqrt[3]{2}]$ ist ein Hauptidealring.

**Beispiel:** $K = \mathbf{Q}(\sqrt{-23})$ hat Ganzheitsring $\mathbf{Z}[\frac{1+\sqrt{-23}}{2}]$ mit Diskriminante. Jede Idealklasse enthält ein ganzes Ideal mit Norm $\leq \frac{2}{\pi}\sqrt{23} = 3.05\dots$. Die Ideale mit Norm $\leq 3$ sind
$$(1), \mathfrak{p}_2 = (2, \frac{1+\sqrt{-23}}{2}), \overline{\mathfrak{p}_2}, \mathfrak{p}_3 = (3, \frac{1+\sqrt{-23}}{2}), \overline{\mathfrak{p}_3}.$$
Man findet leicht die Relationen:
$$\mathfrak{p}_2\mathfrak{p}_3 = (\frac{1+\sqrt{-23}}{2}), \mathfrak{p}_2\overline{\mathfrak{p}_2} = 2, \mathfrak{p}_3\overline{\mathfrak{p}_3} = 3.$$
Prüft man noch, daß $\mathfrak{p}_2$ und $\mathfrak{p}_2^2$ keine Hauptideale sind, so findet man schnell $H_K = \{(1), \mathfrak{p}_2, \mathfrak{p}_2^2\}$ hat Ordnung 3.

**Beispiel:** $K = \mathbf{Q}(\sqrt{-163})$ hat Ganzheitsring $\mathbf{Z}[\frac{1+\sqrt{-163}}{2}]$ mit Diskriminante $-163$. Jede Idealklasse enthält ein ganzes Ideal mit Norm $\leq 8.1278\dots$. Nun ist $\mathfrak{o}_K = \mathbf{Z}[x]/(x^2 - x + 41)$ und das Polynom $x^2 - x + 41$ ist irreduzibel modulo $p = 2, 3, 5, 7$. Also bleiben $(2), (3), (5), (7)$ Primideale in $\mathfrak{o}_K$, also ist $H_K$ trivial, d.h. $\mathbf{Z}[\frac{1+\sqrt{-163}}{2}]$ ist Hauptidealring.

KAPITEL 6

# Einheiten

In diesem Abschnitt wollen wir die Struktur der Einheitengruppe von $\mathfrak{o}_K$ bestimmen. Wir wissen:

$$\alpha \in \mathfrak{o}_K \text{ ist Einheit } \iff N(\alpha) = \pm 1.$$

Sei $U_K$ die Einheitengruppe von $\mathfrak{o}_K$.

**Beispiel:** Einheiten imaginärquadratischer Zahlkörper $\mathbf{Q}(\sqrt{-d})$, wo $d$ quadratfrei und $< 0$ ist.

- Falls $d \equiv 2, 3 \bmod 4$ ist, so ist $\mathfrak{o}_K = \mathbf{Z}[\sqrt{-d}]$, also $N(x + y\sqrt{-d}) = x^2 + dy^2 = \pm 1$ genau dann, wenn $x^2 = 1, dy^2 = 0$ oder $x^2 = 0, dy^2 = 1$. Im ersten Fall gibt es die Lösung $\pm 1$, der zweite Fall kommt nur für $d = 1$ vor, dann ist auch $\pm\sqrt{-1}$ Einheit.
- Falls $d \equiv 3 \bmod 4$ ist, so ist $\mathfrak{o}_K = \mathbf{Z}[\frac{1+\sqrt{-d}}{2}]$ und $N(x+y\frac{1+\sqrt{-d}2}{)} = x^2 + xy + \frac{1+d}{4}y^2 = (x + y/2)^2 + dy^2/4 = 1$. Für $y = 0$ gibt es die triviale Lösung $\pm 1$. Sonst ist $dy^2 \leq 4$, woraus sofort $d = 3$ folgt. In diesem Fall ergeben sich vier zusätzliche Lösungen: $\frac{\pm 1 \pm \sqrt{-3}}{2}$.

Ergebnis: $\mathbf{Q}(i)$ hat die Einheiten $\{\pm 1, \pm i\}$, $\mathbf{Q}(\sqrt{-3})$ hat die Einheiten $\{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\}$. Für die anderen imaginärquadratischen Zahlkörper ist immer $U_K = \{\pm 1\}$.

**Geometrische Deutung:**

- Ist $K$ imaginärquadratisch, so ist die Frage nach Einheiten gleichwertig mit: Wie schneidet $\phi(\mathfrak{o}_K) \subseteq \mathbf{R}^2$ den Kreis $x^2 + y^2 = 1$? (Bild)
- Ist $K$ reellquadratisch, so ist die Frage nach Einheiten gleichwertig mit: Wie schneidet $\phi(\mathfrak{o}_K) \subseteq \mathbf{R}^2$ die Hyperbeln $xy = \pm 1$?

Den Minkowskischen Gitterpunktsatz kann man auf das Einheitenproblem nicht direkt anwenden. Der Trick besteht darin, daß wir viele Elemente mit beschränkter Norm konstruieren, dann muß es dabei welche geben, die sich nur um eine Einheit voneinander unterscheiden.

Die logarithmische Abbildung: Wir definieren $\ell : U_K \to \mathbf{R}^{r_1+r_2}$ durch:

$$\ell(u) = (\log|\sigma_1 u|, \ldots, \log|\sigma_{r_1} u|, 2\log|\sigma_{r_1+1} u|, \ldots)$$

LEMMA. 1. *$\ell$ ist ein Gruppenhomomorphismus.*
2. *$\ell(U_K)$ ist eine diskrete Untergruppe.*
3. *$\ell(U_K) \subseteq \{\sum x_i = 0\}$.*
4. *Der Kern von $\ell$ ist die Gruppe der in $K$ enthaltenen Einheitswurzeln $\mu(K)$.*

*Beweis:*

1. Klar.
2. Es genügt zu zeigen, daß es nur endlich viele Elemente $u \in \mathfrak{o}_K$ gibt mit $|\sigma_i u| \leq M$. Für die Koeffizienten des zugehörigen charakteristischen Polynoms $x^n + a_1 x^{n-1} + \ldots$ gilt dann aber: $|a_i| \leq \binom{n}{i} N^i$. Da man also nur endlich viele Polynome hat, kann es auch nur endlich viele Elemente mit entsprechender Eigenschaft geben.
3. Klar.
4. Ist $u$ im Kern, so gilt $|\sigma_i u| = 1$ für alle Einbettungen. Die Potenzen von $u$ erfüllen natürlich die gleiche Bedingung. Da es aber nur endlich viele Elemente in $K$ mit beschränkten Absolutbeträgen gibt, gibt es $r \neq s$ mit $u^r = u^s$. Wegen $u^{r-s} = 1$ ist dann $u$ eine Einheitswurzel. Die Umkehrung ist klar. ■

LEMMA. *Es gibt Einheiten $u_i$ mit*

$$\ell(u_i) = (-, \dots, -, +, -, \dots, -)$$

*Beweis:*

- Wir wollen den Minkowskischen Gitterpunktsatz anwenden. Als Gitter nehmen wir $\mathfrak{o}_K$ selbst. Wir definieren:

  $$M(c_1, \dots, c_{r_1+r_2}) = \{|x_1| \leq c_1, \dots, |x_{r_1+1} + ix_{r_1+r_2+1}| \leq c_{r_1+1}, \dots\}.$$

  Dann ist $vol(M) = 2c_1 \dots \pi c_{r_1+1}^2$. Ein Element in $M$ hat Norm $\leq c_1 \dots c_{r_1+1}^2 \dots$. Wir können jetzt $c_2$ bis $c_{r_1+r_2}$ sehr klein machen, $c_1$ entsprechend groß und erhalten nach dem Gitterpunktsatz ein $\alpha \neq 0$ in $\mathfrak{o}_K$. Also können wir eine Folge von Elementen aus $\mathfrak{o}_K$ konstruieren mit Norm $\leq N$ und:

  $$|\sigma_1 \alpha_i| < |\sigma_1 \alpha_{i+1}|$$

  und

  $$|\sigma_j \alpha_i| > |\sigma_j \alpha_{i+1}|$$

  für alle $j$ mit $2 \leq j \leq r_1 + r_2$.
- Indem wir uns auf eine Teilfolge beschränken, können wir annehmen, daß alle $\alpha_i$ gleiche Norm haben und außerdem die gleiche Restklasse modulo $N$.
- $\alpha = \beta + N\gamma$ liefert, da $\beta$ auch $N$ teilt: $\frac{\alpha}{\beta} \in \mathfrak{o}_K$, analog ist $\frac{\beta}{\alpha} \in \mathfrak{o}_K$, also $\frac{\alpha}{\beta}$ eine Einheit mit $\ell(u) = (+, -, \dots, -)$. ■

LEMMA. *Streicht man aus der Matrix $\ell(u_1), \dots, \ell(u_{r_1+r_2})$ die letzte Spalte und letzte Zeile, so ist sie regulär.*

*Beweis:* Angenommen, sie wäre nicht regulär, dann liegt im Kern ein Vektor $(a_1, \dots)$, o.E. $a_1 > 0$ und $a_1 \geq a_j$. Wir wählen in der Matrix die entsprechende Zeile der Form: $(t_1, t_2, \dots) = (+, -, -, \dots)$. Also:

$$a_1 t_1 + a_2 t_2 + \dots \geq a_1(t_1 + t_2 + \dots) = a_1(-t_{r_1+r_2}) > 0$$

ein Widerspruch! ■

FOLGERUNG. *$\ell(U_K)$ ist ein Gitter in $\sum x_i = 0$.*

*Beweis:* Wir haben gesehen, daß $\ell(U_K)$ diskret ist und eine $\mathbf{R}$-Basis enthält nach dem vorangegangenen Lemma. ■

Über die Struktur der Einheitengruppe gibt der folgende Satz von Dirichlet Auskunft:

SATZ. *$U_K$ ist eine endlich erzeugte abelsche Gruppe vom Rang $r_1 + r_2 - 1$. Genauer: Sind $\epsilon_1, \dots, \epsilon_{r_1+r_2-1}$ Einheiten, so daß $\ell(\epsilon_i)$ eine Gitterbasis von $\ell(U_K)$ ist, so hat jede Einheit in $K$ eine eindeutige Darstellung*

$$\zeta \epsilon_1^{n_1} \dots \epsilon_{r_1+r_2-1}^{r_1+r_2-1},$$

*wo $\zeta \in \mu(K)$ und $n_i \in \mathbf{Z}$ ist.*

*Beweis:* Ist $u$ eine Einheit, so gibt es $n_i$ mit

$$\ell(u) = \sum n_i \ell(\epsilon_i).$$

Da wir den Kern von $\ell$ kennen, folgt obige Darstellung. Die Eindeutigkeit ist analog trivial. ■

DEFINITION. Ein System von Einheiten $\epsilon_i$ wie im Satz heißt ein System von Grundeinheiten. Die Determinante

$$R = |\det \begin{pmatrix} \log|\sigma_1 \epsilon_1| & \dots & 2\log|\sigma_{r_1+r_2-1} \epsilon_1| \\ \vdots & & \vdots \\ \log|\sigma_1 \epsilon_{r_1+r_2-1}| & \dots & 2\log|\sigma_{r_1+r_2-1} \epsilon_{r_1+r_2-1}| \end{pmatrix}|$$

heißt der Regulator von $K$.

**Beispiel:** Für $K = \mathbf{Q}(\sqrt{11})$ ist $r_1 = 2, r_2 = 0$, der Ganzheitsring ist $\mathbf{Z}[\sqrt{11}]$. Die in $K$ gelegenen Einheitswurzeln sind $\pm 1$. Die Einheitengleichung lautet:

$$N(x + y\sqrt{11}) = x^2 - 11y^2 = \pm 1.$$

Durch Probieren findet man, daß $10 + 3\sqrt{11}$ eine Einheit ist. Ist dies schon eine Grundeinheit? Sei $\epsilon$ eine Grundeinheit und o.E. $10 + 3\sqrt{11} = \pm\epsilon^m$ mit $m \geq 2$. Dann gilt für die zwei Einbettungen:

$$|\epsilon_1| = \sqrt[m]{|10 + 3\sqrt{11}|} = \sqrt[m]{19.95} \leq 4.5, |\epsilon_2| = \sqrt[m]{|10 - 3\sqrt{11}|} = \sqrt[m]{0.05} \leq 1.$$

Also genügt $\epsilon$ einer Gleichung $x^2 - Ax \pm 1 = 0$ mit

$$|A| \leq |\epsilon_1| + |\epsilon_2| \leq 5.5.$$

O.E. ist $A \geq 0$. Also

$$\epsilon = \frac{A \pm \sqrt{A^2 \pm 4}}{2}.$$

Durch Probieren von $A = 0, 1, 2, 3, 4, 5$ sieht man, daß man nie ein Element des Körpers $\mathbf{Q}(\sqrt{11})$ erhält, d.h. $m \geq 2$ geht nicht. Also ist $10 + 3\sqrt{11}$ eine Grundeinheit.

**Bemerkung:** Für reellquadratische Zahlkörper haben die Einheiten die Form $\pm\epsilon^m$, $m \in \mathbf{Z}$, wo $\epsilon$ eine Grundeinheit ist. Wir werden später einen Kettenbruchalgorithmus kennenlernen, mit dem man ein $\epsilon$ effektiv berechnen kann.

**Übung:** Zeige, daß die Einheitengruppe von $\mathbf{Z}[\sqrt[3]{2}]$ ist

$$\{\pm(1 - \sqrt[3]{2})^m : m \in \mathbf{Z}\}.$$

KAPITEL 7

# Erweiterungen von Dedekindringen

SATZ. *Sei $\mathfrak{o}$ ein Dedekindring mit Quotientenkörper $K$, $L|K$ eine endliche separable Körpererweiterung und $\mathfrak{O}$ der ganze Abschluß von $\mathfrak{o}$ in $L$. Dann ist auch $\mathfrak{O}$ ein Dedekindring.*

*Beweis* als Übung. Wir haben alles schon gezeigt für die Situation $\mathbf{Q} \subseteq K$ und $\mathbf{Z} \subseteq \mathfrak{o}$. Übertrage den Beweis. Außerdem benötigen wir die Aussage im folgenden nur für den Zahlkörperfall, wo wir das Ergebnis schon kennen. ■

Wir setzen im folgenden die Situation des Satzes voraus. Wir wollen untersuchen, wie sich die Ideale aus $\mathfrak{o}$ in $\mathfrak{O}$ verhalten.

Sei $\mathfrak{p}$ ein Primideal von $\mathfrak{o}$. Dann ist $\mathfrak{p}\mathfrak{O}$ ein Ideal in $\mathfrak{O}$ mit $\mathfrak{p}\mathfrak{O} \neq \mathfrak{O}$ (andernfalls wäre $\mathfrak{O} = \mathfrak{p}^{-1}\mathfrak{O}$, also da $\mathfrak{O}$ ein endlicher $\mathfrak{o}$-Modul ist, $\mathfrak{p}^{-1}$ ganz über $\mathfrak{o}$, also $\mathfrak{p}^{-1} \subseteq \mathfrak{o}$, ein Widerspruch). Wir können das Ideal in $\mathfrak{O}$ in Primideale faktorisieren:

$$\mathfrak{p}\mathfrak{O} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}.$$

Es ist $\mathfrak{P}_i \cap \mathfrak{o} = \mathfrak{p}$ und $\mathfrak{O}/\mathfrak{P}_i$ ist eine endliche Körpererweiterung von $\mathfrak{o}/\mathfrak{p}$. Der Grad der Körpererweiterung heißt der Trägheitsgrad $f_i$ von $\mathfrak{P}_i$ über $\mathfrak{p}$. Der Exponent $e_i$ heißt der Verzweigungsindex von $\mathfrak{P}_i$ über $\mathfrak{p}$.

SATZ.

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

*Beweis:*

- Mit dem chinesischen Restsatz erhalten wir aus $\mathfrak{p}\mathfrak{O} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$

  $$\mathfrak{O}/\mathfrak{p}\mathfrak{O} \simeq \mathfrak{O}/\mathfrak{P}_1^{e_1} \oplus \dots \oplus \mathfrak{O}/\mathfrak{P}_r^{e_r}.$$

  Die einzelnen Teile sind Vektorräume über $\mathfrak{o}/\mathfrak{p}$. Wir vergleichen die Dimensionen der linken und rechten Seite:
- rechte Seite: Wir haben bereits früher gesehen: $\mathfrak{P}^i/\mathfrak{P}^{i+1} \simeq \mathfrak{O}/\mathfrak{P}$. Aus $\mathfrak{O} \supseteq \mathfrak{P} \supseteq \mathfrak{P}^2 \supseteq \dots \supseteq \mathfrak{P}^e$ folgt dann, daß $\mathfrak{O}/\mathfrak{P}^e$ Dimension $e$ über $\mathfrak{O}/\mathfrak{P}$ hat. Da $\mathfrak{O}/\mathfrak{P}$ ein $f$-dimensionaler $\mathfrak{o}/\mathfrak{p}$-Vektorraum ist, hat $\mathfrak{O}/\mathfrak{P}^e$ Dimension $ef$ als $\mathfrak{o}/\mathfrak{p}$-Vektorraum. Damit ergibt sich: $\oplus\mathfrak{O}/\mathfrak{P}^{e_i}$ hat Dimension $\sum e_i f_i$ über $\mathfrak{o}/\mathfrak{p}$.
- linke Seite: Seien $\omega_1, \dots, \omega_m \in \mathfrak{O}$, so daß $\overline{\omega}_1, \dots, \overline{\omega}_m$ eine Basis von $\mathfrak{O}/\mathfrak{p}\mathfrak{O}$ über $\mathfrak{o}/\mathfrak{p}$ bilden. Zu zeigen ist $m = n$, d.h. $\omega_1, \dots, \omega_m$ ist eine Basis von $L$ über $K$.
  *Annahme:* $\omega_1, \dots, \omega_m$ sind linear abhängig über $K$. Dann gibt es $a_i \in \mathfrak{o}$, nicht alle 0, mit $\sum a_i\omega_i = 0$. Wir betrachten das Ideal $\mathfrak{a} = (a_1, \dots, a_m) \subseteq \mathfrak{o}$. Wir haben $\mathfrak{a}^{-1}\mathfrak{p} \subsetneqq \mathfrak{a}^{-1}$. Wähle $\alpha \in \mathfrak{a}^{-1}$, $\alpha \notin \mathfrak{a}^{-1}\mathfrak{p}$. Dann ist $\alpha a_i \in \mathfrak{o}$, aber nicht für alle $i$ gilt $\alpha a_i \in \mathfrak{p}$. Nun folgt aus $\sum(\alpha a_i)\omega_i = 0$ durch Reduktion modulo $\mathfrak{p}$ die Beziehung $\sum(\overline{\alpha a_i})\overline{\omega}_i = 0$, da $\overline{\omega}_i$ eine Basis bilden, folgt $\overline{\alpha a_i} = 0$ und damit $\alpha a_i \in \mathfrak{p}$ für alle $i$, ein Widerspruch!
  *Behauptung:* $\omega_1, \dots, \omega_m$ erzeugt $L$ über $K$. Sei $\alpha_1, \dots, \alpha_s$ ein Erzeugendensystem von $\mathfrak{O}$ über $\mathfrak{o}$. Mit $\mathfrak{M} = \sum \mathfrak{o}\omega_i$ gilt $\mathfrak{O} = \mathfrak{M} + \mathfrak{O}\mathfrak{p}$. Dann ist

  $$\alpha_i = \sum x_{ij}\omega_j + \sum y_{ik}\alpha_k \text{ mit } x_{ij} \in \mathfrak{O}, y_{ik} \in \mathfrak{p}.$$

  Wir schreiben dies als Matrizengleichung:

  $$\alpha = X\omega + Y\alpha$$

und erhalten $(E-Y)\alpha = X\omega$. Nun ist modulo $\mathfrak{p}$: $\det(E-Y) \equiv \det(E) = 1$, also $\det(E-Y) \neq 0$, so daß folgt

$$\alpha = (E-Y)^{-1}X\omega.$$

Also erzeugen auch $\omega_1, \ldots, \omega_m$ den $K$-Vektorraum $L$, was wir zeigen wollten.
Damit haben wir gezeigt: $\omega_1, \ldots, \omega_m$ ist eine $K$-Basis von $L$, d.h. $m = n$ und damit $\dim_{\mathfrak{o}/\mathfrak{p}} \mathfrak{O}/\mathfrak{p}\mathfrak{O} = n$, was zu zeigen war. ■

In der Praxis ist es nicht immer ganz leicht, $\mathfrak{O}$ zu berechnen. Leicht ist es aber, ein über $\mathfrak{o}$ ganzes $\alpha$ zu finden mit $L = K(\alpha)$. Also $\mathfrak{o}[\alpha] \subseteq \mathfrak{O}$. Wir nennen $\mathfrak{F} = \{\lambda \in \mathfrak{O} : \lambda\mathfrak{O} \subseteq \mathfrak{o}[\alpha]\}$ den Führer von $\mathfrak{o}[\alpha]$ in $\mathfrak{O}$. Aufgrund der endlichen Erzeugtheit ist klar, daß $\mathfrak{F}$ ein Ideal $\neq 0$ in $\mathfrak{O}$ ist.

SATZ. *Sei $\mathfrak{F}$ der Führer von $\mathfrak{o}[\alpha]$ in $\mathfrak{O}$, $\phi$ das Minimalpolynom von $\alpha$ über $K$. Ist $\mathfrak{p} \subseteq \mathfrak{o}$ teilerfremd zu $\mathfrak{F} \cap \mathfrak{o}$ und $\phi(x) \equiv \prod_{i=1}^{r} \phi_i(x)^{e_i} \bmod \mathfrak{p}$ die irreduzible Zerlegung modulo $\mathfrak{p}$, so sind $\mathfrak{P}_i = \mathfrak{p}\mathfrak{O} + \phi_i(\alpha)\mathfrak{O}$ verschiedene Primideale mit $f(\mathfrak{P}_i|\mathfrak{p}) = \deg \phi_i$ und $\mathfrak{p}\mathfrak{O} = \prod \mathfrak{P}_i^{e_i}$.*

*Beweis:*

1. Aus $\mathfrak{F} \cap \mathfrak{o} + \mathfrak{p} = \mathfrak{o}$ erhält man eine Darstellung $1 = f + \rho$ mit $f \in \mathfrak{F} \cap \mathfrak{o}$ und $\rho \in \mathfrak{p}$.
2. Die natürliche Abbildung $\mathfrak{o}[\alpha] \to \mathfrak{O}/(\mathfrak{p}, \phi_i(\alpha))$ ist surjektiv wegen $\lambda = \lambda f + \lambda\rho$ mit $\lambda f \in \mathfrak{o}[\alpha]$ und $\lambda\rho \in \mathfrak{p}\mathfrak{O}$. Was ist der Kern? Sei $\lambda \in \mathfrak{o}[\alpha]$ im Kern, also $\lambda = \tau + \phi_i(\alpha)\omega$ mit $\tau \in \mathfrak{p}\mathfrak{O}$ und $\omega \in \mathfrak{O}$. Dann ist
$$\lambda = \lambda f + \lambda\rho = f\tau + \phi_i(\alpha)f\omega + \lambda\rho \in \mathfrak{p}\mathfrak{o}[\alpha] + \phi_i(\alpha)\mathfrak{o}[\alpha].$$
Also folgt
$$\mathfrak{o}[\alpha]/(\mathfrak{p}, \phi_i(\alpha)) \simeq \mathfrak{O}/(\mathfrak{p}, \phi_i(\alpha)).$$
3. Da $\phi_i(x)$ modulo $\mathfrak{p}$ irreduzibel ist, ist $\mathfrak{o}[\alpha]/(\mathfrak{p}, \phi_i(\alpha)) \simeq \mathfrak{o}/\mathfrak{p}[x]/(\phi_i(x))$ ein Körper vom Grad $\deg \phi_i$ über $\mathfrak{o}/\mathfrak{p}$. Also ist $\mathfrak{P}_i$ ein Primideal mit $f(\mathfrak{P}_i|\mathfrak{p}) = \deg \phi_i$.
4. Für $i \neq j$ ist $\phi_i(\alpha)\lambda + \phi_j(\alpha)\mu = 1 + \omega$ mit $\omega \in \mathfrak{o}\mathfrak{O}$, also $\mathfrak{P}_i + \mathfrak{P}_j = \mathfrak{O}$.
5. Aus $\prod \mathfrak{P}_i^{e_i} \subseteq \mathfrak{p}\mathfrak{O}$ folgt $\mathfrak{p} = \prod \mathfrak{P}_i^{e_i'}$ mit $e_i' \leq e_i$. Nun ist $n = \sum e_i' f_i \leq \sum e_i f_i = n$, also $e_i = e_i'$, was die Behauptung liefert. ■

**Bezeichnungen:** Das Primideal $\mathfrak{p} \subseteq \mathfrak{o}$ habe die Primidealzerlegung $\mathfrak{p}\mathfrak{O} = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_r^{e_r}$ in $\mathfrak{O}$.

- $\mathfrak{p}$ heißt voll zerlegt, falls $\mathfrak{p} = \mathfrak{P}_1 \ldots \mathfrak{P}_n$ gilt, d.h. $f(\mathfrak{P}_i|\mathfrak{p}) = 1$ und $e_i = 1$.
- $\mathfrak{p}$ heißt träge oder unzerlegt, falls $\mathfrak{p}\mathfrak{O} = \mathfrak{P}$ Primideal in $\mathfrak{O}$ ist.
- $\mathfrak{P}_i$ heißt verzweigt über $\mathfrak{o}$, falls $e_i > 1$ ist, sonst unverzweigt.
- $\mathfrak{P}_i$ heißt rein verzweigt über $\mathfrak{o}$, falls $f(\mathfrak{P}_i|\mathfrak{p}) = 1$ ist und $e_i > 1$.
- $\mathfrak{p}$ heißt verzweigt, falls ein $i$ existiert mit $e_i > 1$.

**Beispiel:** $K = \mathbf{Q}(\sqrt[3]{2})$. Der Ganzheitsring ist $\mathfrak{o} = \mathbf{Z}[\sqrt[3]{2}]$. Wir untersuchen, wie sich die Primideale $(p)$ von $\mathbf{Z}$ in $\mathfrak{o}$ verhalten. Das Minimalpolynom von $\alpha = \sqrt[3]{2}$ ist $\phi(x) = x^3 - 2$. Wir müssen also die Primfaktorzerlegung von $\phi(x) = x^3 - 2$ modulo $p$ bestimmen. Wir geben zunächst ein paar Beispiele:

- $p = 2$: Hier ist $\phi(x) \equiv x^3 \bmod 2$, also $(2) = \mathfrak{p}^3$ mit $\mathfrak{p} = (2, \alpha) = (\alpha)$.
- $p = 5$: Aus $\phi(x) \equiv (x^2 + 3x + 4)(x + 2) \bmod 5$ ergibt sich
$$(5) = \mathfrak{p}_1\mathfrak{p}_2 \text{ mit } \mathfrak{p}_1 = (5, \alpha^2 + 3\alpha + 4) \text{ und } \mathfrak{p}_2 = (5, \alpha + 2).$$
- $p = 7$: Das Polynom $\phi(x)$ ist irreduzibel modulo 7, also ist $(7)$ ein Primideal in $\mathfrak{o}$.
- $p = 31$: Hier ist $\phi(x) \equiv (x + 11)(x + 24)(x + 27) \bmod 31$, also
$$(31) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 \text{ mit } \mathfrak{p}_1 = (31, \alpha + 11), \quad \mathfrak{p}_2 = (31, \alpha + 24) \text{ und } \mathfrak{p}_3 = (31, \alpha + 27).$$

Wir betrachten jetzt die ersten 100 Primzahlen und erhalten folgende kleine Statistik:

- 51% zerfallen in der Form $(p) = \mathfrak{p}_1\mathfrak{p}_2$ $(\phi(x) \equiv (x + \ldots)(x^2 + \ldots) \bmod p)$.
- 32% sind träge, d.h. $(p) = \mathfrak{p}$, $(\phi(x) \equiv x^3 + \ldots)$.
- 15% zerfallen voll, d.h. $(p) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, $(\phi(x) \equiv (x + \ldots)(x + \ldots)(x + \ldots))$.
- 2% verzweigen in der Form $(p) = \mathfrak{p}^3$, $(\phi(x) \equiv (x + \ldots)^3 \bmod p)$.

Es scheint also wenig verzweigte Primideale zu geben.

**Beispiel:** $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 - 3\alpha - 1 = 0$. Man kann zeigen, daß der Ganzheitsring $\mathbf{Z}[\alpha]$ ist und $D_K = 81$. Um das Zerlegungsverhalten der rationalen Primzahlen zu untersuchen, müssen wir $f = x^3 - 3x - 1$ modulo $p$ faktorisieren.

- Die Primzahlen $p \leq 20$: $f$ ist irreduzibel modulo 2, 5, 7, 11, 13. Modulo 3: $f \equiv (x+2)^3$. Modulo 17: $(x+7)(x+13)(x+14)$. Modulo 19: $(x+3)(x+7)(x+9)$.
- Eine kleine Statistik der auftretenden Fälle für die ersten 100 Primzahlen:
  - $(p) = \mathfrak{p}^3$ verzweigt: 1 Fall (1%)
  - $(p)$ träge: 67 Fälle (67%)
  - $(p) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ zerfällt voll: 32 Fälle (32%)

Was ist der Unterschied zu dem vorhergehenden Fall?

SATZ. *$\mathfrak{o}[\alpha]$ habe Führer $\mathfrak{F}$ in $\mathfrak{O}$. Dann gilt für zu $\mathfrak{F} \cap \mathfrak{o}$ teilerfremde Primideale $\mathfrak{p} \subseteq \mathfrak{o}$:*

$$\mathfrak{p} \text{ verzweigt} \iff D_{L|K}(\alpha) \equiv 0 \bmod \mathfrak{p}.$$

*Beweis:* $\mathfrak{p}$ ist genau dann verzweigt, wenn das definierende Polynom $\phi$ mehrfache Nullstellen über $\mathfrak{o}/\mathfrak{p}$ hat, d.h. wenn es inseparabel ist. Dies testet aber genau die Diskriminante. ■

KOROLLAR. *Es gibt nur endlich viele verzweigte Primideale in $K$, die in $L$ verzweigen.*

*Beweis:* Die zu $\mathfrak{F}$ und $D(\alpha)$ teilerfremden Primideale sind sicher unverzweigt, also sind die verzweigten unter den restlichen endlich vielen. ■

Was kann man über den Führer im Zahlkörperfall sagen?

LEMMA. *Sei $\mathfrak{F}$ der Führer von $\mathfrak{o}[\alpha]$ in $\mathfrak{O}$. Dann gilt*

$$\mathfrak{F}^2 | D(\alpha).$$

*Beweis:* Sicher ist der Index $[\mathfrak{O} : \mathfrak{o}[\alpha]]$ in $\mathfrak{F}$, also $\mathfrak{F} | [\mathfrak{O} : \mathfrak{o}[\alpha]]$. Wegen $[\mathfrak{O} : \mathfrak{o}[\alpha]]^2 | D(\alpha)$ folgt dann die Behauptung. ■

Es drängt sich nun die Frage auf: Gibt es immer eine Potenzganzheitsbasis, d.h. kann man ein $\alpha$ finden mit $\mathfrak{o} = \mathfrak{o}_K = \mathbf{Z}[\alpha]$?

**Beispiel:** Sei $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 + \alpha^2 - 2\alpha + 8 = 0$ und $\mathfrak{o} = \mathfrak{o}_K$ der Ganzheitsring von $K$.

- Wegen $D(\alpha) = -4 \cdot 503$ und $[\mathfrak{o} : \mathbf{Z}[\alpha]]^2 | D(\alpha)$ ist $[\mathfrak{o} : \mathbf{Z}[\alpha]]$ entweder 1 oder 2.
- $\beta = \frac{\alpha + \alpha^2}{2}$ erfüllt $\beta^3 - 2\beta^2 + 3\beta - 10 = 0$, also $\beta \in \mathfrak{o}$, aber $\beta \notin \mathbf{Z}[\alpha]$. Damit ist $[\mathfrak{o} : \mathbf{Z}[\alpha]] = 2$ und folglich
$$\mathfrak{o} = \mathbf{Z} + \mathbf{Z}\alpha + \mathbf{Z}\alpha^2 + \mathbf{Z}\beta = \mathbf{Z} + \mathbf{Z}\alpha + \mathbf{Z}\beta$$
und $D_K = -503$.
- Eine kleine Multiplikationstabelle: $\alpha^2 = -\alpha + 2\beta$, $\alpha\beta = -4 + \alpha$, $\beta^2 = -2 - 2\alpha + \beta$.
- Wir wollen die Zerlegung von (2) in $\mathfrak{o}$ bestimmen. Es ist $0 \equiv \alpha^3 + \alpha^2 - 2\alpha + 8 \equiv \alpha^2(\alpha + 1) \bmod 2$ und $0 \equiv \beta^3 - 2\beta^2 + 3\beta - 10 \equiv \beta(\beta+1)^2 \bmod 2$. Wir versuchen den Ansatz: $\mathfrak{p}_1 = (2, \alpha, \beta)$, $\mathfrak{p}_2 = (2, \alpha, \beta + 1)$, $\mathfrak{p}_3 = (2, \alpha + 1, \beta + 1)$. Man findet:
$$\begin{aligned} \mathfrak{p}_1 &= \mathbf{Z} \cdot 2 + \mathbf{Z} \cdot \alpha + \mathbf{Z} \cdot \beta, \\ \mathfrak{p}_2 &= \mathbf{Z} \cdot 2 + \mathbf{Z} \cdot \alpha + \mathbf{Z} \cdot (\beta + 1), \\ \mathfrak{p}_3 &= \mathbf{Z} \cdot 2 + \mathbf{Z} \cdot (\alpha + 1) + \mathbf{Z} \cdot (\beta + 1). \end{aligned}$$
Damit folgt $\#\mathfrak{o}/\mathfrak{p}_i = 2$, d.h. die $\mathfrak{p}_i$ sind Primideale und $f(\mathfrak{p}_i|(2)) = 1$. Natürlich sind die $\mathfrak{p}_i$'s paarweise verschieden. Damit folgt $(2) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$.

- Angenommen, es gäbe eine Potenzganzheitsbasis: $\mathfrak{o} = \mathbf{Z}[\theta] = \mathbf{Z} + \mathbf{Z}\theta + \mathbf{Z}\theta^2$. Wegen $\mathfrak{o}/\mathfrak{p}_i = \{0, 1\}$ gibt es $\mathfrak{p}_i \neq \mathfrak{p}_j$, so daß entweder

$$\theta \equiv 0 \bmod \mathfrak{p}_i, \theta \equiv 0 \bmod \mathfrak{p}_j \quad \text{oder} \quad \theta \equiv 1 \bmod \mathfrak{p}_i, \theta \equiv 1 \bmod \mathfrak{p}_j$$

gilt. Ist $\lambda \in \mathfrak{p}_i$, so gibt es ein Polynom $g$ mit ganzzahligen Koeffizienten mit $\lambda = g(\theta)$. Aus $0 \equiv \lambda = g(\theta) \bmod \mathfrak{p}_i$ folgt dann $g(\theta) \equiv 0 \bmod \mathfrak{p}_j$, d.h. $\lambda \in \mathfrak{p}_j$. Dies liefert $\mathfrak{p}_i \subseteq \mathfrak{p}_j$ und damit $\mathfrak{p}_i = \mathfrak{p}_j$, einen Widerspruch. Also kann es keine Potenzganzheitsbasis geben.

KAPITEL 8

# Galoissche Erweiterungen

Sei $L|K$ eine Galoissche Erweiterung von Zahlkörpern mit Galoisgruppe $G$ und $|G| = n$. Seien $\mathfrak{o} \subseteq \mathfrak{O}$ die zugehörigen Ganzheitsringe, insbesondere ist $\mathfrak{O}$ der ganze Abschluß von $\mathfrak{o}$ in $L$.

**Vorbemerkungen:**

1. Für $\sigma \in G$ gilt $\sigma\mathfrak{O} = \mathfrak{O}$.
2. Für $\sigma \in G$ und $\mathfrak{P}|\mathfrak{p}$ gilt $\sigma\mathfrak{P}|\mathfrak{p}$, d.h. mit $\mathfrak{P}$ liegt auch $\sigma\mathfrak{P}$ über $\mathfrak{p}$.

LEMMA. *$G$ operiert transitiv auf den über $\mathfrak{p}$ liegenden Primidealen von $\mathfrak{O}$.*

*Beweis:* Angenommen, es gibt Primideale $\mathfrak{P}_1$, $\mathfrak{P}_2$ über $\mathfrak{p}$ mit $\mathfrak{P}_2 \neq \sigma\mathfrak{P}_1$ für alle $\sigma \in G$. Nach dem chinesischen Restsatz gibt es ein $x \in \mathfrak{O}$ mit $x \equiv 0 \bmod \mathfrak{P}_2$, aber $x \equiv 1 \bmod \sigma\mathfrak{P}_1$ für alle $\sigma \in G$. Wegen $x \equiv 0 \bmod \mathfrak{P}_2$ folgt $Nx \in \mathfrak{P}_2 \cap \mathfrak{o} = \mathfrak{p}$. Aus $x \equiv 1 \bmod \sigma\mathfrak{P}_1$ folgt $\sigma x \equiv 1 \bmod \mathfrak{P}_1$ und damit $Nx = \prod \sigma x \equiv 1 \bmod \mathfrak{P}_1$, was $Nx \equiv 1 \bmod \mathfrak{p}$ im Widerspruch zu $Nx \in \mathfrak{p}$ liefert. Die Annahme ist also falsch, die Behauptung also richtig. ■

FOLGERUNG. *Ist $\mathfrak{p} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$, so sind alle $f_i$ und alle $e_i$ gleich.*

*Beweis:* $\sigma$ liefert einen Isomorphismus $\mathfrak{O}/\mathfrak{P} \to \mathfrak{O}/\sigma\mathfrak{P}$, also $f(\mathfrak{P}|\mathfrak{p}) = f(\sigma\mathfrak{P}|\mathfrak{p})$, d.h. alle $f_i$ sind gleich. Sei nun $\sigma \in G$ mit $\sigma\mathfrak{P}_1 = \mathfrak{P}_i$. Dann ist

$$\mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r} = \mathfrak{p}\mathfrak{O} = \sigma(\mathfrak{p}\mathfrak{O}) = (\sigma\mathfrak{P}_1)^{e_1} \dots (\sigma\mathfrak{P}_r)^{e_r} = \mathfrak{P}_i^{e_1} \dots,$$

was $e_1 = e_i$ und damit die Gleichheit aller $e_i$ liefert. ■

DEFINITION. Sei $\mathfrak{P}$ ein Primideal von $\mathfrak{O}$. Dann heißt

$$G_{\mathfrak{P}} = \{\sigma \in G : \sigma\mathfrak{P} = \mathfrak{P}\}$$

die Zerlegungsgruppe von $\mathfrak{P}$.

$$Z_{\mathfrak{P}} = \{\alpha \in L : \sigma\alpha = \alpha \text{ für alle } \sigma \in G_{\mathfrak{P}}\} = Fix(G_{\mathfrak{P}})$$

heißt der Zerlegungskörper von $\mathfrak{P}$.

**Bemerkung:** Da die Galoisgruppe transitiv auf den über $\mathfrak{p}$ liegenden Primidealen $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ operiert, folgt $r = \frac{|G|}{|G_{\mathfrak{P}}|}$. Insbesondere ist $\mathfrak{p}$ genau dann voll zerlegt, wenn $G_{\mathfrak{P}} = 1$ gilt. $\mathfrak{p}$ ist unzerlegt, wenn $G = G_{\mathfrak{P}}$ gilt.

**Bezeichnung:** Ist $E$ ein Körper zwischen $K$ und $L$, d.h. $K \subseteq E \subseteq L$, so bezeichnet $\mathfrak{P}_E = \mathfrak{P} \cap E$ das unter $\mathfrak{P}$ liegende Primideal von $E$.

SATZ. *Wir betrachten die Filtration $K \subseteq Z_{\mathfrak{P}} \subseteq L$ und schreiben kurz $Z = Z_{\mathfrak{P}}$.*

1. *$\mathfrak{P}_Z$ ist unzerlegt in $L$.*
2. *$e(\mathfrak{P}|\mathfrak{P}_Z) = e(\mathfrak{P}|\mathfrak{p})$ und $f(\mathfrak{P}|\mathfrak{P}_Z) = f(\mathfrak{P}|\mathfrak{p})$.*
3. *Verzweigungsindex und Restklassengrad von $\mathfrak{P}_Z$ über $\mathfrak{p}$ sind 1.*
4. *$Z$ ist der kleinste Teilkörper $E$ von $L$, so daß über $\mathfrak{P}_E$ nur $\mathfrak{P}$ liegt, d.h. $\mathfrak{P}_E$ ist unzerlegt in $\mathfrak{O}$.*

*Beweis:* $\mathfrak{p}\mathfrak{O} = \mathfrak{P}^e\mathfrak{P}_2^e \dots \mathfrak{P}_r^e$, $efr = |G|$, $r = \frac{|G|}{|G_\mathfrak{P}|}$, also $ef = |G_\mathfrak{P}|$. Sei $\mathfrak{p}\mathfrak{o}_Z = \mathfrak{P}_Z^{e'} \dots$ mit Restklassengrad $f'$ und $\mathfrak{P}_Z\mathfrak{O} = \mathfrak{P}^{e''} \dots$ mit Restklassengrad $f''$. Dann ist $e''f'' = |G_\mathfrak{P}| = ef$. Aus $\mathfrak{p}\mathfrak{O} = (\mathfrak{p}\mathfrak{o}_Z)\mathfrak{O} = \mathfrak{P}^{e'e''} \dots$ folgt $e'e'' = e$ und $f'f'' = f$. Damit ist $e''f'' = ef = e''f'' \cdot e'f'$, also $e' = f' = 1$ und $e'' = e$, $f'' = f$.
Zu 1.: Die Galoisgruppe von $L|Z$ ist $G_\mathfrak{P}$, sie operiert auf den über $\mathfrak{P}_Z$ liegenden Primidealen transitiv, also liegt nur $\mathfrak{P}$ über $\mathfrak{P}_Z$.
Zu 4.: Über $\mathfrak{P}_E$ liege nur $\mathfrak{P}$. Dann ist $G(L|E)\mathfrak{P} = \mathfrak{P}$, also $G(L|E) \subseteq G_\mathfrak{P}$ und damit $Z_\mathfrak{P} \subseteq E$. ■

**Bezeichnung:** Der Restklassenkörper $\mathfrak{O}/\mathfrak{P}$ werde mit $\kappa(\mathfrak{P})$ bezeichnet. In unserem Fall ist dies ein endlicher Körper. $\kappa(\mathfrak{P})|\kappa(\mathfrak{p})$ ist also eine Körpererweiterung vom Grad $f(\mathfrak{P}|\mathfrak{p})$. Die Erweiterung ist natürlich galoissch.

SATZ. 1. *Jedes $\sigma \in G_\mathfrak{P}$ liefert vermöge $a \bmod \mathfrak{P} \mapsto \sigma a \bmod \mathfrak{P}$ einen Automorphismus $\overline{\sigma}$ von $\kappa(\mathfrak{P})$ über $\kappa(\mathfrak{p})$.*
2. *$G_\mathfrak{P} \to Gal(\kappa(\mathfrak{P})|\kappa(\mathfrak{p}))$ ist surjektiv.*

*Beweis:*

1. Wegen $\sigma\mathfrak{P} = \mathfrak{P}$ für $\sigma \in G_\mathfrak{P}$ induziert $\sigma$ einen Automorphismus $\mathfrak{O}/\mathfrak{P} \to \mathfrak{O}/\mathfrak{P}$, also folgt 1.
2. Da $\kappa(\mathfrak{p}) = \kappa(\mathfrak{P}_Z)$ ist, können wir uns auf den Schritt von $Z_\mathfrak{P}$ nach $L$ beschränken. Sei $\theta \in \mathfrak{O}$, so daß $\overline{\theta}$ die Erweiterung $\kappa(\mathfrak{P})|\kappa(\mathfrak{P}_Z)$ erzeugt. Sei $f(x)$ das Minimalpolynom von $\theta$ über $\mathfrak{o}_Z$. $G_\mathfrak{P}$ operiert transitiv auf den Nullstellen $\theta_1, \dots, \theta_s$, da $L|Z_\mathfrak{P}$ galoissch ist. Sei $\tau \in G(\kappa(\mathfrak{P})|\kappa(\mathfrak{P}_Z))$. Dann gibt es ein $\ell$ mit $\tau\overline{\theta} = \overline{\theta}_\ell$. Nun gibt es ein $\sigma_\ell \in G_\mathfrak{P}$ mit $\sigma_\ell\theta = \theta_\ell$. Da $G(\kappa(\mathfrak{P})|\kappa(\mathfrak{P}_Z))$ durch die Wirkung auf $\overline{\theta}$ bestimmt ist, folgt $\theta = \overline{\sigma}_\ell$, d.h. $G_\mathfrak{P} \to G(\kappa(\mathfrak{P})|\kappa(\mathfrak{P}_Z))$ ist surjektiv. ■

DEFINITION. Der Kern $I_\mathfrak{P} \subseteq G_\mathfrak{P}$ der Homomorphismus $G_\mathfrak{P} \to G(\kappa(\mathfrak{P})|\kappa(\mathfrak{p}))$ heißt die Trägheitsgruppe von $\mathfrak{P}$ über $K$, anders ausgedrückt:

$$I_\mathfrak{P} = \{\sigma \in G_\mathfrak{P} : \sigma x \equiv x \bmod \mathfrak{P} \text{ für alle } x \in \mathfrak{O}\}.$$

Der Fixkörper von $I_\mathfrak{P}$ heißt der Trägheitskörper $T_\mathfrak{P}$ von $\mathfrak{P}$ über $K$.

SATZ. 1. *$T_\mathfrak{P}|Z_\mathfrak{P}$ ist normal und $G(T_\mathfrak{P}|Z_\mathfrak{P}) \simeq G(\kappa(\mathfrak{P})|\kappa(\mathfrak{p}))$, $Gal(L|T_\mathfrak{P}) = I_\mathfrak{P}$.*
2. *$\#I_\mathfrak{P} = e = [L : T_\mathfrak{P}]$, $(G_\mathfrak{P} : I_\mathfrak{P}) = [T_\mathfrak{P} : Z_\mathfrak{P}] = f$.*
3. *$\mathfrak{P}|\mathfrak{P}_T$ hat Verzweigungsindex $e$ und Trägheitsindex 1, $\mathfrak{P}_T|\mathfrak{P}_Z$ hat Verzweigungsindex 1 und Trägheitsindex $f$.*

*Beweis:* $f = \#Gal(\kappa(\mathfrak{P})|\kappa(\mathfrak{p})) = \#G_\mathfrak{P}/I_\mathfrak{P}$, also $f = [T_\mathfrak{P} : Z_\mathfrak{P}]$. In $L|T_\mathfrak{P}$ passiert keine Restklassenerweiterung, d.h. $\kappa(\mathfrak{P}) = \kappa(\mathfrak{P}_T)$ und damit $f = f(\mathfrak{P}_T|\mathfrak{P}_Z)$, $e(\mathfrak{P}_T|\mathfrak{P}_Z) = 1$, was dann $f(\mathfrak{P}|\mathfrak{P}_T) = 1$, $e(\mathfrak{P}|\mathfrak{P}_T) = e$, $\#I_\mathfrak{P} = e$ liefert. ■

Im Bild:

$$K \overset{e=f=1}{\subseteq} Z_\mathfrak{P} \overset{\text{Restklassenerweiterung}}{\subseteq} T_\mathfrak{P} \overset{\text{Verzweigung}}{\subseteq} L.$$

FOLGERUNG. *Ist $\mathfrak{p}$ unverzweigt, so ist $G_\mathfrak{P} \simeq Gal(\kappa(\mathfrak{P})|\kappa(\mathfrak{p}))$ eine zyklische Gruppe der Ordnung $f$.*

FOLGERUNG. *Ist $L|K$ galoissch, aber nicht zyklisch, so gibt es keine trägen Primideale.*

*Beweis:* Wäre $\mathfrak{p}$ träge, so würde $Gal(\kappa(\mathfrak{P})|\kappa(\mathfrak{p})) \simeq G_\mathfrak{P} = G$ folgen, was nach Voraussetzung nicht der Fall sein sollte, da $Gal(\kappa(\mathfrak{P})|\kappa(\mathfrak{p}))$ zyklisch ist. ■

**Anwendung:** Wie findet man irreduzible normierte Polynome $f(x) \in \mathbf{Z}[x]$, die bezüglich jeder Primzahl reduzibel sind?
*Antwort:* Wähle $L|\mathbf{Q}$ galoissch, aber nicht zyklisch, $\alpha$ ganz mit $L = \mathbf{Q}(\alpha)$, $f = minpol(\alpha|\mathbf{Q})$. Dieses $f$ liefert dann ein gesuchtes Polynom.

**Beispiel:** $K = \mathbf{Q}(\sqrt[3]{2}, \zeta_3)$.

- Die Galoisgruppe von $K$ über $\mathbf{Q}$ ist $G \simeq S_3$. Die Zwischenkörper sind

$$\mathbf{Q}(\sqrt[3]{2}), \quad \mathbf{Q}(\sqrt[3]{2}\zeta_3), \quad \mathbf{Q}(\sqrt[3]{2}\zeta_3^2), \quad \mathbf{Q}(\zeta_3).$$

- $K|\mathbf{Q}$ ist nur verzweigt in 2 und 3. Für $p = 2$ ist $Z_{\mathfrak{P}} = \mathbf{Q}$ und $T_{\mathfrak{P}} = \mathbf{Q}(\zeta_3)$, für $p = 3$ ist $(3) = \mathfrak{p}^6$ und $T_{\mathfrak{P}} = \mathbf{Q}$.
- $\alpha = \sqrt[3]{2} + \zeta_3$ hat das Minimalpolynom $f = x^6 + 3x^5 + 6x^4 + 3x^3 + 9x + 9$ und Diskriminante $D(\alpha) = 2^4 \cdot 3^{17}$.
- Sei $p \neq 2, 3$ eine Primzahl. Es gibt verschiedene Möglichkeiten:
  - $p$ ist träge in $\mathbf{Q}(\zeta_3)$. Dann ist $(p) = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$ in $K$ und o.E. $(p) = \mathfrak{p}_1\mathfrak{p}_{23}$ in $\mathbf{Q}(\sqrt[3]{2})$ mit $\mathfrak{p}_1 = \mathfrak{P}_1$ und $\mathfrak{p}_{23} = \mathfrak{P}_2\mathfrak{P}_3$.
  - $p$ ist zerlegt in $\mathbf{Q}(\zeta_3)$: $(p) = \mathfrak{p}_1\mathfrak{p}_2$.
    - $p$ ist voll zerlegt: $(p) = \mathfrak{P}_1 \dots \mathfrak{P}_6$.
    - $\mathfrak{p}_1, \mathfrak{p}_2$ sind träge: $(p) = \mathfrak{P}_1\mathfrak{P}_2$. Dann ist $(p)$ träge in $\mathbf{Q}(\sqrt[3]{2})$.

KAPITEL 9

# Quadratische Zahlkörper

Sei $K = \mathbf{Q}(\sqrt{d})$ ein quadratischer Zahlkörper ($d$ quadratfrei). Dann ist für $d \equiv 1 \bmod 4$ die Diskriminante $D_K = d$ und $\mathfrak{o}_K = \mathbf{Z}[\frac{1+\sqrt{d}}{2}]$, für $d \equiv 2, 3 \bmod 4$ die Diskriminante $D_K = 4d$ und $\mathfrak{o}_K = \mathbf{Z}[\sqrt{d}]$.
Wir wollen untersuchen, wie sich rationale Primzahlen $p$ in $K$ zerlegen. Aus der Formel $\sum_i^r e_i f_i = 2$ wissen wir, daß es nur drei Möglichkeiten gibt:

- $(p) = \mathfrak{p}^2$, Verzweigung. Dies liegt genau dann vor, wenn $p | D_K$.
- $(p) = \mathfrak{p}_1\mathfrak{p}_2$: das Primideal $(p)$ zerfällt voll.
- $(p) = \mathfrak{p}$: das Primideal $(p)$ ist träge.

Um ein Beispiel eines Führers zu sehen, berechnen wir:

LEMMA. *Für $d \equiv 1 \bmod 4$ ist der Führer $\mathfrak{f}$ von $\mathbf{Z}[\sqrt{d}]$ in $\mathbf{Z}[\frac{1+\sqrt{d}}{2}]$ das Ideal $\mathfrak{f} = (2)$ und $\mathfrak{f} \cap \mathbf{Z} = (2)$.*

*Beweis:*

$$\begin{aligned}
\mathfrak{f} &= \{\lambda \in \mathbf{Z}[\frac{1+\sqrt{d}}{2}] : \lambda \mathbf{Z}[\frac{1+\sqrt{d}}{2}] \subseteq \mathbf{Z}[\sqrt{d}]\} \\
&= \{\lambda \in \mathbf{Z}[\sqrt{d}] : \lambda \mathbf{Z}[\frac{1+\sqrt{d}}{2}] \subseteq \mathbf{Z}[\sqrt{d}]\} \\
&= \{\lambda \in \mathbf{Z}[\sqrt{d}] : \lambda \frac{1+\sqrt{d}}{2} \in \mathbf{Z}[\sqrt{d}]\}
\end{aligned}$$

Nun ist $(x + y\sqrt{d})\frac{1+\sqrt{d}}{2} = \frac{x+yd}{2} + \frac{x+y}{2}\sqrt{d}$, also muß gelten: $x \equiv y \bmod 2$, also

$$x + y\sqrt{d} = (x - y) + 2y\frac{1+\sqrt{d}}{2} \in (2).$$

Daraus folgt die Behauptung. ■

Wie verhält sich jetzt 2 in $\mathfrak{o}_K$?

SATZ. *Für $d \equiv 2, 3 \bmod 4$ verzweigt $(2)$, für $d \equiv 1 \bmod 8$ zerfällt $(2)$, für $d \equiv 5 \bmod 8$ bleibt $(2)$ prim in $\mathfrak{o}_K$.*

*Beweis:* Für können uns auf den Fall $d \equiv 1 \bmod 4$ beschränken. Dann ist $\mathfrak{o}_K = \mathbf{Z}[x]/\phi(x)$ mit $\phi(x) = x^2 - x + \frac{1-d}{4}$.

- Für $d \equiv 1 \bmod 8$ ist $\phi(x) \equiv x(x-1) \bmod 2$, also zerfällt $(2)$:
$$(2) = (2, \frac{1+\sqrt{d}}{2}) \cdot (2, \frac{1-\sqrt{d}}{2}).$$
- Für $d \equiv 5 \bmod 8$ ist $\phi(x) \equiv x^2 + x + 1 \bmod 2$ irreduzibel, d.h. $(2)$ bleibt träge in $\mathfrak{o}_K$. ■

Wir können uns also jetzt auf Primzahlen $p > 2$, die $d$ nicht teilen beschränken. Dann gilt:

- $(p)$ zerfällt voll genau dann, wenn $x^2 - d$ reduzibel modulo $p$ ist; dies ist gleichwertig mit: $d$ ist Quadrat modulo $p$.
- $(p)$ bleibt prim in $\mathfrak{o}_K$ genau dann, falls $x^2 - d$ ist irreduzibel modulo $p$. Dies ist äquivalent mit: $d$ ist kein Quadrat modulo $p$.

Wir definieren jetzt das Legendre-Symbol:

DEFINITION. Sei $p$ eine ungerade Primzahl und $a$ eine ganze Zahl, teilerfremd zu $p$. Dann ist $\left(\frac{a}{p}\right) = 1$, falls $a$ ein Quadrat modulo $p$ ist, sonst $-1$.

Natürlich können wir das Legendre-Symbol auch als Funktion auf $\mathbf{F}_p^\times$ betrachten.

LEMMA. *Das Legendre-Symbol ist multiplikativ, d.h.*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

*Beweis:* Da $\mathbf{F}_p^\times$ zyklisch von gerader Ordnung ist, ist $\mathbf{F}_p^\times/\mathbf{F}_p^{\times 2}$ isomorph zu $\mathbf{Z}/2\mathbf{Z}$. Daraus folgt, daß das Produkt zweier Nichtquadrate wieder ein Quadrat ist, und daraus folgt dann die Behauptung. ■

Wir können jetzt das Zerlegungsgesetz umformulieren: Sei $p$ eine ungerade Primzahl, die nicht $D_K$ teilt. Dann gilt: $p$ zerfällt $\iff \left(\frac{d}{p}\right) = 1$ und $p$ bleibt träge $\iff \left(\frac{d}{p}\right) = -1$. Doch ist dies mehr als eine Umformulierung? Kann man die Bedingungen schön in Abhängigkeit von $d$ ausdrücken? Wir beginnen mit den einfachsten Fällen:

SATZ. *Für ungerade Primzahlen $p$ gilt:*

- $\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \bmod 4$.
- $\left(\frac{2}{p}\right) = 1 \iff p \equiv 1, 7 \bmod 8$.

*Beweis:* Im algebraischen Abschluß $\overline{\mathbf{F}_p}$ von $\mathbf{F}_p$ haben wir den Frobenius-Automorphismus $\sigma$ mit $\sigma(\alpha) = \alpha^p$. Ein Element $\alpha$ liegt genau dann in $\mathbf{F}_p$, wenn es unter $\sigma$ fest bleibt.

- $\left(\frac{-1}{p}\right) = 1 \iff i \in \mathbf{F}_p$, wo $i$ für eine primitive 4-te Einheitswurzel steht. Für $p \equiv 1 \bmod 4$ gilt: $\sigma(i) = i^p = i$, also $i \in \mathbf{F}_p$. Für $p \equiv 3 \bmod 4$ gilt: $\sigma(i) = i^p = i^3 = -i$, also $i \notin \mathbf{F}_p$. Daraus folgt die erste Behauptung.
- Für eine primitive 8-te Einheitswurzel gilt: $\zeta_8 = \frac{1+i}{\sqrt{2}}$, also $\sqrt{2} = (\zeta^8 + \zeta^2)\zeta^{-1} = \zeta - \zeta^3$. Also: $\left(\frac{2}{p}\right) = 1 \iff \sqrt{2} \in \mathbf{F}_p \iff \zeta - \zeta^3 \in \mathbf{F}_p$. Nun unterscheiden wir 4 Fälle:
  - $p \equiv 1 \bmod 8$: $\sigma\frac{1+i}{\zeta_8} = \frac{1+i}{\zeta_8}$.
  - $p \equiv 3 \bmod 8$: $\sigma\frac{1+i}{\zeta_8} = \frac{1-i}{\zeta_8^3} = -\frac{1+i}{\zeta_8}$.
  - $p \equiv 5 \bmod 8$: nicht invariant.
  - $p \equiv 7 \bmod 8$: invariant, da Quotient reell.

  Daraus ergibt sich die Behauptung. ■

**Bemerkung:** Für ungerade Primzahlen $p$ gilt:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \text{ und } \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{2}}.$$

Um dies zu sehen, betrachten wir jeweils die rechten Seiten:

- $(-1)^{\frac{b-1}{2}}$ hängt nur von $b$ mod 4 ab, und für $b = 1$ und $b = 3$ nimmt es die richtigen Werte an.
- $(-1)^{\frac{b^2-1}{8}}$ hängt nur von $b$ mod 8 ab, und für $b = 1, 3, 5, 7$ nimmt es die richtigen Werte an.

Der vorausgehende Satz wird verallgemeinert durch das sogenannte Gaußsche quadratische Reziprozitätsgesetz.

Aus dem vorhergehenden Beweis erhalten wir folgende Idee: Schreibe $\sqrt{d}$ als Linearkombination in Einheitswurzeln. Dann ist leicht $\sigma_p(\sqrt{d})$ zu berechnen und damit auch $\left(\frac{d}{p}\right)$. Dies geschieht in folgendem Lemma.

LEMMA. *Seien $p$ und $q$ verschiedene ungerade Primzahlen. Setzt man*

$$\tau = \sum_{a \in \mathbf{F}_q^\times} \left(\frac{a}{q}\right) \zeta_q^a,$$

*so gilt:*

$$\tau = \sqrt{\left(\frac{-1}{q}\right) q},$$

*wobei es keine Rolle spielt, ob wir die Beziehung in* $\mathbf{C}$ *oder* $\overline{\mathbf{F}_p}$ *betrachten.*

*Beweis:* In den Summationen wird jeweils über die Elemente aus $\mathbf{F}_q^\times$ summiert:

$$\tau^2 = \sum \left(\frac{ab}{q}\right) \zeta^{a+b} = \sum \left(\frac{c}{q}\right) \zeta^{b(c+1)},$$

wo wir $c = ab$ gesetzt haben. Für $c \not\equiv -1 \bmod q$ gilt:

$$\sum_b \zeta^{b(1+c)} = -1,$$

für $c \equiv -1 \bmod q$ gilt:

$$\sum_b \left(\frac{-1}{q}\right) = (q-1)\left(\frac{-1}{q}\right).$$

Also erhalten wir:

$$\tau^2 = -\sum_{c \not\equiv -1} \left(\frac{c}{q}\right) + (q-1)\left(\frac{-1}{q}\right) = -\sum \left(\frac{c}{q}\right) + q\left(\frac{-1}{q}\right).$$

Nun ist $\sum \left(\frac{c}{q}\right) = 0$, denn wählt man ein $x$ mit $\left(\frac{x}{q}\right) = -1$, so gilt: $\sum \left(\frac{c}{q}\right) = \sum_c \left(\frac{xc}{q}\right) = -\sum_c \left(\frac{c}{q}\right)$. Also gilt schließlich:

$$\tau^2 = \left(\frac{-1}{q}\right) q,$$

was wir zeigen wollten. ■

**Bemerkung:** Das Lemma zeigt, daß für eine ungerade Primzahl $q$ gilt:

$$\mathbf{Q}(\sqrt{\pm q}) \subseteq \mathbf{Q}(\zeta_q),$$

wo $\pm q$ so gewählt werden muß, daß $\pm q \equiv 1 \bmod 4$ ist.

Wir können nun das quadratische Reziprozitätsgesetz formulieren:

SATZ. *Sind* $p$ *und* $q$ *verschiedene ungerade Primzahlen, so gilt:*

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right).$$

*Anders ausgedrückt:*
*Ist* $p \equiv 1 \bmod 4$ *oder* $q \equiv 1 \bmod 4$, *so ist* $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$, *sind* $p \equiv 3 \bmod 4$ *und* $q \equiv 3 \bmod 4$, *so gilt:* $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$.

*Beweis:* Es gilt: $\left(\frac{-1}{q}\right) q$ ist Quadrat modulo $p$ genau dann, wenn $\sqrt{\left(\frac{-1}{q}\right) q} \in \mathbf{F}_p$. Daher genügt es die Wirkung von $\sigma_p$ auszurechnen:

$$\sigma_p\left(\sqrt{\left(\frac{-1}{q}\right) q}\right) = \sum_a \left(\frac{a}{q}\right) \zeta_q^{ap} = \left(\frac{p}{q}\right) \sum_a \left(\frac{ap}{q}\right) \zeta_q^{ap} = \left(\frac{p}{q}\right) \sqrt{\left(\frac{-1}{q}\right) q}.$$

Also gilt:

$$\left(\frac{\left(\frac{-1}{q}\right) q}{p}\right) = \left(\frac{p}{q}\right).$$

Da nun

$$\left(\frac{\left(\frac{-1}{q}\right) q}{p}\right) = \left(\frac{-1}{q}\right)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

ergibt sich sofort obiger Satz. ■

**Beispiele:**

- Ist 5 ein Quadrat modulo 23? Wir rechnen mit dem Legendre-Symbol:
$$\left(\frac{5}{23}\right) = \left(\frac{23}{5}\right) = \left(\frac{3}{5}\right) = -1,$$
also ist 5 kein Quadrat modulo 23.
- Ist 323 modulo 1009? 1009 ist prim, 323 jedoch nicht: $323 = 17 \cdot 19$, also:
$$\left(\frac{323}{1009}\right) = \left(\frac{17}{1009}\right)\left(\frac{19}{1009}\right) = \left(\frac{6}{17}\right)\left(\frac{2}{19}\right) = \left(\frac{2}{17}\right)\left(\frac{3}{17}\right)(-1) = \left(\frac{2}{3}\right)(-1) = 1,$$
also ist 323 ein Quadrat modulo 1009.

Um das Legendre-Symbol einfacher berechnen zu können, führen wir das Jacobi-Symbol ein:

DEFINITION. Für teilerfremde ganze Zahlen $a$ und $b$ mit $b > 0$ und $b$ ungerade wird das Jacobi-Symbol durch
$$\left(\frac{a}{b}\right) = \prod \left(\frac{a}{p_i}\right)$$
definiert, wo $b = \prod p_i$ die Primfaktorzerlegung ist. Es hängt nur von der Restklasse von $a$ modulo $b$ ab.

SATZ. *Für ungerade natürliche Zahlen $a$ und $b$ gilt das Reziprozitätsgesetz*
$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}$$
*Weiter gelten die Ergänzungssätze:*
$$\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}} \text{ und } \left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{2}}.$$

*Beweis:*

- Seien $a = \prod p_i$ und $b = \prod q_j$ jeweils die Primfaktorzerlegungen. Dann gilt:
$$\begin{aligned}\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) &= \prod_{i,j}\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = \\ &= \prod_{i,j}(-1)^{\frac{p_1-1}{2}\frac{q_j-1}{2}} = (-1)^{\sum_{i,j}\frac{p_i-1}{2}\frac{q_j-1}{2}}.\end{aligned}$$
Andererseits ist
$$(-1)^{\frac{a-1}{2}\frac{b-1}{2}} = (-1)^{\frac{\prod p_j-1}{2}\frac{\prod q_j-1}{2}},$$
also genügt es zu zeigen:
$$\sum_{i,j}\frac{p_i-1}{2}\frac{q_j-1}{2} \equiv \frac{\prod p_i-1}{2}\frac{\prod q_j-1}{2} \bmod 2.$$
- Für ungerade Zahlen $u$ und $v$ gilt:
$$\frac{uv-1}{2} \equiv \frac{u-1}{2} + \frac{v-1}{2} \bmod 2,$$
denn dies ist äquivalent mit: $\frac{(u-1)(v-1)}{2} \equiv 0 \bmod 2$, was das nach Voraussetzung gilt.
- Also gilt:
$$\frac{\prod p_i-1}{2}\frac{\prod q_j-1}{2} \equiv (\sum\frac{p_i-1}{2})(\sum\frac{q_j-1}{2}) = \sum\frac{p_i-1}{2}\frac{q_j-1}{2},$$
was zu zeigen war.

- Mit den gleichen Bezeichnungen gilt:

$$\begin{aligned}\left(\frac{-1}{b}\right) &= \prod\left(\frac{-1}{q_j}\right) = \prod(-1)^{\frac{q_j-1}{2}} = \\ &= (-1)^{\sum\frac{q_j-1}{2}} = (-1)^{\frac{\prod q_j-1}{2}} = (-1)^{\frac{b-1}{2}}.\end{aligned}$$

- Weiter gilt:

$$\begin{aligned}\left(\frac{2}{b}\right) &= \prod\left(\frac{2}{q_j}\right) = \prod(-1)^{\frac{q_j^2-1}{8}} = \\ &= (-1)^{\sum\frac{q_j^2-1}{8}} = (-1)^{\frac{\prod q_j^2-1}{8}} = (-1)^{\frac{b^2-1}{8}},\end{aligned}$$

wenn wir gezeigt haben:

$$\frac{(uv)^2-1}{8} \equiv \frac{u^2-1}{8} + \frac{v^2-1}{8} \bmod 2.$$

Dies ist aber gleichwertig mit

$$0 \equiv \frac{(u^2-1)(v^2-1)}{8} = \frac{(u-1)(u+1)(v-1)(v+1)}{8} \bmod 2,$$

was richtig ist. ■

**Beispiel:** Wir schauen nochmals obiges Beispiel an:

$$\left(\frac{323}{1009}\right) = \left(\frac{1009}{323}\right) = \left(\frac{40}{323}\right) = \left(\frac{2}{323}\right)\left(\frac{5}{323}\right) = -\left(\frac{323}{5}\right) = 1.$$

Anwendung auf das Zerlegungsverhalten der Primzahlen.

SATZ. *Das Zerlegungsverhalten von $p$ in $\mathbf{Q}(\sqrt{d})$ hängt nur von der Restklasse von $p$ modulo $D_K$ ab. Genauer: Zerlegt man $d = 2^a em$, mit $m > 0$ ungerade, $e = \pm 1$, $a = 0$ oder $1$ und definiert man*

$$\chi_{D_K}(x) = (-1)^{a\frac{x^2-1}{8}}(-1)^{\frac{em-1}{2}\frac{x-1}{2}}\left(\frac{x}{m}\right)$$

*für zu $D_K$ teilerfremde Zahlen $x$, so gilt:*

- *Für $p|D_K$ verzweigt $p$.*
- *Für $p$ teilerfremd zu $D_K$ zerfällt $p$ in $K$ genau dann, wenn $\chi_{D_K}(p) = 1$ ist.*
- *$\chi_{D_K}(x)$ hängt nur von der Restklasse von $x \bmod |D_K|$ ab.*

*Beweis:* Wir schreiben $d = 2^a em$, wo $m$ eine ungerade Zahl $> 0$ ist, $e = \pm 1$ und $a \in \{o, 1\}$. Wir brauchen nur noch die Primzahlen $p$ zu betrachten, die teilerfremd zu $D_K$ sind.

$$\begin{aligned}\left(\frac{d}{p}\right) &= \left(\frac{2^a em}{p}\right) = \left(\frac{2}{p}\right)^a\left(\frac{e}{p}\right)\left(\frac{m}{p}\right) = \\ &= (-1)^{a\frac{p^2-1}{8}}(-1)^{\frac{e-1}{2}\frac{p-1}{2}}(-1)^{\frac{m-1}{2}\frac{p-1}{2}}\left(\frac{p}{m}\right) = \\ &= (-1)^{a\frac{p^2-1}{2}}(-1)^{\frac{em-1}{2}\frac{p-1}{2}}\left(\frac{p}{m}\right)\end{aligned}$$

Damit haben wir eine Formel gefunden. Wir wollen noch sehen, daß sie nur von $p \bmod |D_K|$ abhängt. Es ist klar, daß $\left(\frac{p}{m}\right)$ nur von $p \bmod |em|$ abhängt. Also müssen wir nur noch die anderen Anteile anschauen.

- Für $a = 1$ hängt $(-1)^{\frac{p^2-1}{8}}$ von $p \bmod 8$ ab. Andererseits ist auch $|D_K| = 8 \cdot m$, woraus die Behauptung folgt.
- Für $d \equiv 3 \bmod 4$ ist $d = em$ und $(-1)^{\frac{d-1}{2}}$, wir haben also eine Abhängigkeit modulo $4d = D_K$.
- Für $d \equiv 1 \bmod 4$ ist das Symbol $\left(\frac{p}{|d|}\right)$, es hängt nur von $p \bmod |d|$ ab und $D_K = d$.

Damit ist alles gezeigt. ■

**Bemerkung:** $\chi_{D_K}$ ist ein Gruppenhomomorphismus von $\mathbf{Z}/|D_K|$ in $\{\pm 1\}$. Man nennt $\chi_{D_K}$ den zu $K$ gehörigen Charakter.

**Beispiele:**

1. $K = \mathbf{Q}(i)$, also $D_K = -4$. Dann sieht man sofort:
$$\chi(x) = 1 \text{ für } x \equiv 1 \bmod 4 \text{ und } \chi(x) = -1 \text{ für } x \equiv -1 \bmod 4.$$
2. $K = \mathbf{Q}(\sqrt{3})$. Dann ist $D_K = 12$. Unsere Formel lautet:
$$\chi_{D_K}(x) = (-1)^{\frac{x-1}{2}} \left(\frac{x}{3}\right),$$
was liefert
$$\chi(1) = 1, \chi(5) = -1, \chi(7) = -1, \chi(11) = 1.$$

**Anwendung:** Welche Primzahlen haben die Gestalt $p = x^2 + y^2$?

- Wir rechnen im Ring $\mathbf{Z}[i]$ wegen $x^2 + y^2 = N(x + yi)$. Wir betrachten nur ungerade Primzahlen, die also dann nicht verzweigen.
- $p = x^2 + y^2$ bedeutet $p = N(x + yi)$, also ist $p = (x + yi)(x - yi)$ die Primidealzerlegung von $p$, d.h. $p$ zerfällt, also $p \equiv 1 \bmod 4$.
- Ist umgekehrt $p \equiv 1 \bmod 4$, so zerfällt $p$ in $\mathbf{Q}(i)$, d.h. $p = \mathfrak{p}\overline{\mathfrak{p}}$. Da die Klassenzahl 1 ist, ist $\mathfrak{p} = (x + yi)$ Hauptideal, also $(p) = (x + yi)(x + yi) = (x^2 + y^2)$, woraus sofort $p = x^2 + y^2$ folgt.
- Ergebnis: Eine ungerade Primzahl $p$ läßt sich genau dann als Summe von zwei Quadraten schreiben, wenn $p \equiv 1 \bmod 4$ ist.

KAPITEL 10

# Die Fermatsche Gleichung und Kreisteilungskörper

**Das Fermatsche Problem:** Für eine natürliche Zahl $n \geq 2$ bestimme man alle ganzen Zahlen $x, y, z$, die der Gleichung

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

genügen.

- O.E. kann man $ggT(x, y, z) = 1$ annehmen, ansonsten dividiert man durch diesen ggT.
- Triviale Lösungen sind $(x, y, z) = (1, 0, 1), (0, 1, 1)$.
- Man kann sich leicht auf $x, y, z > 0$ beschränken.

Wir wollen zuerst den Fall $n = 2$ betrachten:

LEMMA. *Die Ringe* $\mathbf{Z}[\frac{1+\sqrt{-3}}{2}]$, $\mathbf{Z}[i]$, $\mathbf{Z}[\frac{1+\sqrt{-7}}{2}]$ *und* $\mathbf{Z}[\sqrt{-2}]$ *sind Hauptidealringe.*

*Beweis:* Für einen imaginärquadratischen Zahlkörper mit Diskriminante $D$ gilt: Jedes Idealklasse enthält ein ganzes Ideal mit Norm

$$\leq \frac{4}{\pi}\frac{2!}{2^2}\sqrt{|D|} = \frac{2}{\pi}\sqrt{|D|} = 0.636619773\sqrt{|D|}.$$

Dieser Ausdruck ist $< 2$, falls $|D| < \Pi^2$ ist, d.h. $|D| \leq 8$. Die entsprechenden imaginärquadratischen Zahlkörper haben dann Klassenzahl 1, sind also Hauptidealringe. ■

SATZ. *Alle Lösungen in natürlichen Zahlen der Gleichung* $x^2 + y^2 = z^2$ *haben die Form*

$$x = u^2 - v^2, y = 2uv, z = u^2 + v^2 oder$$

$$x = 2uv, y = u^2 - v^2, z = u^2 + v^2$$

*mit natürlichen Zahlen* $u$ *und* $v$.

*Beweis:* Sei $x, y, z$ eine Lösung.

- Sind $x$ und $y$ beide ungerade, so ist $x^2 + y^2 \equiv 2 \bmod 4$, was nicht geht. O.E. nehmen wir an: $x$ ungerade, $y$ gerade.
- Wir faktorisieren in $\mathbf{Z}[i]$:
$$(x + yi)(x - yi) = z^2$$
- $x + yi$ und $x - yi$ sind teilerfremd, denn wäre $\pi$ ein gemeinsamer Primteiler, so würde dieser auch $2x$ und $2yi$ teilen, also auch 2. Dann wäre $\pi = 1 + i$, also müßte $z$ gerade sein, ein Widerspruch.
- Folglich ist jetzt auch $x + yi$ bis auf Einheiten ein Quadrat, d.h.
$$x + yi = e(u + iv)^2 = e((u^2 - v^2) + 2uvi)$$
mit $e = 1$ oder $i$. $e = i$ geht nicht, da $x$ ungerade sein sollte. Also bleibt $e = 1$ und damit
$$x = u^2 - v^2, y = 2uv, z = u^2 + v^2$$

■

**Die Fermatvermutung:** Für $n \geq 3$ besitzt die Gleichung $x^n + y^n = z^n$ eine Lösung in natürlichen Zahlen.

Es genügt, die Vermutung für $n = 4$ und ungerade Primzahlen $n = p$ zu zeigen. Vom ersten Fall spricht man, falls $ggT(xyz, p) = 1$ ist.

Wir wollen den Fall einer ungeraden Primzahl $p$ betrachten. Was hat das mit Kreisteilungskörper zu tun? Sei $\zeta = \zeta_p$ eine primitive $p$-te Einheitswurzel. Dann gilt:

$$t^p - 1 = \prod_{i=0}^{p-1}(t - \zeta^i)$$

Setzt man $t = \frac{x}{-y}$ und multipliziert mit $(-y)^p$, so erhält man

$$x^p + y^p = \prod_{i=0}^{p-1}(x + \zeta^i y),$$

d.h. wir haben die Gleichung in $\mathbf{Q}(\zeta)$ faktorisiert.

Dies motiviert die Beschäftigung mit den Kreisteilungskörpern.

**Erinnerung:** Die Definitionsgleichung von $\zeta = \zeta_p$ ist $x^{p-1}+x^{p-2}+\cdots+x+1 = 0$. Der Kreisteilungskörper $\mathbf{Q}(\zeta)$ hat Grad $p-1$ und ist galoissch, ja sogar zyklisch. Die Automorphismen sind gegeben durch $\sigma_j\zeta = \zeta^j$, wo $j \in \mathbf{Z}/p^\times$.

Sei $\mathfrak{o}$ der Ganzheitsring von $\mathbf{Q}(\zeta)$. Wir wollen die Arithmetik von $\mathfrak{o}$ studieren. Natürlich gilt $\mathbf{Z}[\zeta] \subseteq \mathfrak{o}$.

LEMMA. *Sind $r, s$ ganze Zahlen mit $ggT(p, rs) = 1$, so ist*

$$\frac{\zeta^r - 1}{\zeta^s - 1}$$

*eine Einheit.*

*Beweis:* Es gibt eine natürliche Zahl $t$ mit $r \equiv st \bmod p$, also gilt:

$$\frac{\zeta^r - 1}{\zeta^s - 1} = \frac{\zeta^{st} - 1}{\zeta^s - 1} = \zeta^{s(t-1)} + \cdots + \zeta^2 + 1 \in \mathfrak{o}.$$

Ebenso so ist $\frac{\zeta^s-1}{\zeta^r-1} \in \mathfrak{o}$, also folgt die Behauptung. ■

LEMMA. *$(1 - \zeta)$ ist Primideal ist $\mathfrak{o}$ und*

$$(p) = (1 - \zeta)^{p-1}.$$

*Beweis:*

- Es ist $x^{p-1} + \cdots + x + 1 = \prod_{i=1}^{p-1}(x - \zeta^i)$. Setzt man $x = 1$, so erhält man:

  $$p = \prod_{i=1}^{p-1}(1 - \zeta^i).$$

  Nun ist

  $$1 - \zeta^i = \frac{1 - \zeta^i}{1 - \zeta}(1 - \zeta) \sim 1 - \zeta,$$

  also

  $$p \sim (1 - \zeta)^{p-1}.$$

  Aus $efr = n$ folgt, daß $(1 - \zeta)$ schon Primideal ist, und daraus folgt dann die Behauptung. ■

LEMMA. *Die Diskriminante von $\mathbf{Z}[\zeta]$ ist $\pm p^{p-2}$.*

*Beweis:* Die Diskriminante ist

$$\prod_{1\le i<j\le p-1}(\zeta^i - \zeta^j)^2 \sim \prod_{1\le i<j\le p-1}(1 - \zeta)^2 = (1 - \zeta)^{(p-1)(p-2)} \sim p^{p-2},$$

woraus sofort die Behauptung folgt. ■

SATZ. *Es ist $\mathfrak{o} = \mathbf{Z}[\zeta]$.*

*Beweis:* Wir wissen

$$p^{p-2}\mathfrak{o} \subseteq \mathbf{Z}[\zeta] \subseteq \mathfrak{o}.$$

Sei $\pi = 1 - \zeta$. Dann ist $\mathfrak{o}/\pi = \mathbf{Z}/p$, also sicher auch $\mathfrak{o} = \mathbf{Z} + \pi\mathfrak{o}$ und $\mathfrak{o} = \mathbf{Z}[\zeta] + \pi\mathfrak{o}$. Daraus ergibt sich durch Iteration $\mathfrak{o} = \mathbf{Z}[\zeta] + \pi^2\mathfrak{o}$, und wenn man so fortfährt:

$$\mathfrak{o} = \mathbf{Z}[\zeta] + \pi^{(p-1)(p-2)}\mathfrak{o} = \mathbf{Z}[\zeta] + p^{p-2}\mathfrak{o} = \mathbf{Z}[\zeta],$$

was wir zeigen wollten. ■

FOLGERUNG. *Die Diskriminante von $\mathbf{Q}(\zeta_p)$ ist $\pm p^{p-2}$, insbesondere ist $p$ die einzige verzweigte Primzahl in $K$.*

Wir brauchen im folgenden noch Aussagen über Einheiten:

LEMMA. *Die in $\mathbf{Q}(\zeta_p)$ enthaltenen Einheitswurzeln sind $\pm\zeta_p^i$ mit $i \in \mathbf{Z}$. Außerdem hat jede Einheit $\epsilon$ die Form $\epsilon = \zeta_p^i\epsilon_1$ mit $\epsilon_1 \in \mathbf{R}$.*

*Beweis:*

1. Da in $\mathbf{Q}(i)$ die 2 verzweigt, ist $i \notin \mathbf{Q}(\zeta_p)$. Ist $q$ eine andere ungerade Primzahl, so verzweigt $q$ in $\mathbf{Q}(\zeta_q)$, also kann $\zeta_q$ nicht in $\mathbf{Q}(\zeta_p)$ liegen. Schließlich hat $\zeta_{p^2}$ Grad $p(p-1)$ über $\mathbf{Q}$, liegt also auch nicht in $\mathbf{Q}(\zeta_p)$. Daraus folgt die erste Behauptung.
2. $e/\bar{e}$ hat bei allen Einbettungen in $\mathbf{C}$ Absolutbetrag 1, muß also eine Einheitswurzel sein. Sei $e = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$. Modulo $1-\zeta$ gilt dann $e/\bar{e} \equiv 1$. Wäre $e/\bar{e} = -\zeta^a$, so würde $2 \equiv 0 \bmod 1-\zeta$ folgen, was nicht geht. Also ist $e/\bar{e} = \zeta^a$. Wähle $b$ mit $a \equiv 2b \bmod p$. Dann ist
$$e\zeta^{-b} = \overline{e\zeta^{-b}},$$
also $e\zeta^{-b}$ reell, woraus die Behauptung folgt.

LEMMA. *Zu $\alpha \in \mathbf{Z}[\zeta_p]$ gibt es ein $m \in \mathbf{Z}$ mit*

$$\alpha^p \equiv m \bmod p.$$

*Beweis:* Für $\alpha = \sum_{i=0}^{p-2} a_i\zeta^i$ mit $a_i \in \mathbf{Z}$ gilt modulo $p$

$$\alpha^p \equiv \sum_{i=0}^{p-2} a_i^p(\zeta^p)^i \equiv \sum_{i=0}^{p-2} a_i \bmod p,$$

was sofort die Behauptung zeigt. ■

SATZ. *Sei $p \geq 5$ eine ungerade Primzahl, so daß $p$ die Klassenzahl von $\mathbf{Q}(\zeta_p)$ nicht teilt. Dann gibt es keine ganzzahligen Lösungen der Gleichung*

$$x^p + y^p = z^p \text{ unter der Bedingung } ggT(xyz, p) = 1.$$

*Beweis:*

- Wir nehmen an, es gibt eine solche Lösung. O.E. ist $ggT(x,y,z) = 1$. Statt $x^p + y^p = z^p$ können wir auch $x^p + (-z)^p = (-y)^p$ betrachten. Angenommen, es gilt $x \equiv y \equiv -z \bmod p$. Dann ist $2x^p \equiv -x^p \bmod p$, also $p = 3$, was nicht sein sollte. Wir können also $x \not\equiv y \bmod p$ voraussetzen.
- Wir zeigen, daß die Ideale $(x + y\zeta^i)$ für $i = 0, \ldots, p-1$ paarweise teilerfremd sind. Sonst gilt $\mathfrak{p}|(x+\zeta^i y)$, $\mathfrak{p}|(x+\zeta^j y)$, also $\mathfrak{p}|(1-\zeta)y$. Gilt $\mathfrak{p}|y$, so folgt $\mathfrak{p}|x$ und damit $\mathfrak{p}|z$, ein Widerspruch. Also bleibt $\mathfrak{p} = (1-\zeta)$. Dann gilt $\mathfrak{p}|x+y$ und somit $\mathfrak{p}|z^p$, also $p|z^p$, was ausgeschlossen war.
- Wir können jetzt schreiben $(x + \zeta y) = \mathfrak{a}^p$. Da die Klassenzahl zu $p$ teilerfremd ist, ist $\mathfrak{a}$ ein Hauptideal, d.h. $x + \zeta y = \zeta^r\epsilon_1\alpha^p$. Dann ist $\zeta^{-r}(x+\zeta y) = \epsilon_1\alpha^p$ und modulo $p$
$$\zeta^{-r}(x+\zeta y) \equiv \epsilon_1 a = \overline{\epsilon_1 a} \equiv \zeta^r(x+\zeta^{-1}y)$$
mit $a \in \mathbf{Z}$. Dies liefert $x+\zeta y \equiv x\zeta^{2r} + y\zeta^{2r-1} \bmod (p)$ und $x+y\zeta-y\zeta^{2r-1}-x\zeta^{2r} \equiv 0 \bmod p$. Also hat man eine Darstellung $x + y\zeta - y\zeta^{2r-1} - x\zeta^{2r} = \sum_{i=0}^{p-2} pa_i\zeta^i$. Wir unterscheiden einige Fälle:
  1. $1$, $\zeta$, $\zeta^{2r-1}$, $\zeta^{2r}$ sind verschieden: Dann folgt der Widerspruch $p|x$ und $p|y$.
  2. $1 = \zeta^{2r-1}$. Dann folgt $x + y\zeta - y - x\zeta = (x-y)(1-\zeta) \equiv 0 \bmod p$, also $x \equiv y \bmod p$, was ausgeschlossen war.

3. $1 = \zeta^{2r}$. Dies ergibt $x + y\zeta - y\zeta^{-1} - x = y\zeta^{-1}(\zeta^2 - 1)$, also den Widerspruch $p|y$.
4. $\zeta = \zeta^{2r-1}$. Mit $x + y\zeta - y\zeta - x\zeta^2 = x(1 - \zeta^2)$ ergibt sich $p|x$, was ausgeschlossen war.

Damit folgt die Behauptung. ■

**Anmerkungen:**

- Man kann allgemein zeigen: Teilt $p$ die Klassenzahl von $\mathbf{Q}(\zeta_p)$ nicht, so gilt für $p$ die Fermatsche Vermutung.
- Definiert man die Bernoulli-Zahlen durch die Formel
$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!},$$
(also:
$$B_0 = 1, B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}, B_4 = -\frac{1}{30}, B_6 = \frac{1}{42}, B_8 = -\frac{1}{30}, B_{10} = \frac{5}{66}, B_{12} = -\frac{691}{2730}, \dots)$$
so gilt:
$$p|h_p \iff p \text{ teilt den Nenner einer der Zahlen } B_2, B_4, \dots B_{p-3}.$$
- Allerdings gibt es unendlich viele $p$ mit $p|h(\mathbf{Q}(\zeta_p))$.
- Es ist nicht bekannt, ob es unendlich viele reguläre Primzahlen gibt.
- Die Gültigkeit der Fermat-Vermutung wurde im ersten Fall für alle $p < 6 \times 10^9$, im zweiten Fall für alle $p < 125000$ gezeigt.

SATZ. *In $\mathbf{Q}(\zeta_p)$ ist $p$ total verzweigt. Eine Primzahl $q \neq p$ zerlegt sich wie folgt: Ist $f$ minimal mit $q^f \equiv 1 \bmod p$, so gilt*
$$(q) = \mathfrak{q}_1 \dots \mathfrak{q}_r$$
*mit $f(\mathfrak{q}|q) = f$ und $r = \frac{p-1}{f}$.*

*Beweis:* Es ist $\mathbf{F}_q[\zeta] \simeq \mathfrak{o}/\mathfrak{q} = \mathbf{F}_{q^f}$. Dann ist aber $f$ das minimale $f$ mit $p|q^f - 1$, und das war die Behauptung. ■

**Beispiel:** $K = \mathbf{Q}(\zeta_7)$. Dann gilt:

- $q \equiv 1 \bmod 7$: $q = \mathfrak{q}_1 \dots \mathfrak{q}_6$.
- $q \equiv 2, 4 \bmod 7$: $q = \mathfrak{q}_1\mathfrak{q}_2$. $f = 3$.
- $q \equiv 3, 5 \bmod 7$: $f = 6$, $q$ bleibt prim.
- $q \equiv 6 \bmod 7$: $f = 2$, $q = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$.

**Anwendung:** Jede Idealklasse in $\mathbf{Q}(\zeta_p)$ enthält ein ganzes Ideal mit Norm
$$\leq (\frac{4}{\pi})^{(p-1)/2} \frac{(p-1)!}{(p-1)^{p-1}} p^{(p-2)/2}$$
Es ist
$$f(3) \leq 1.11, f(5) \leq 1.70, f(7) \leq 4.13, f(11) \leq 58.97, f(13) \leq 306.42, \dots$$
Also haben $\mathbf{Q}(\zeta_3)$ und $\mathbf{Q}(\zeta_5)$ Klassenzahl 1. Aus dem vorhergehenden Beispiel ersieht man auch, daß es in $\mathbf{Q}(\zeta_7)$ kein ganzes nichttriviales Ideal mit Norm $\leq 4$ gibt, d.h. auch dieser Körper hat Klassenzahl 1.

**Erinnerung:** Ist $\zeta$ eine primitive $n$-te Einheitswurzel, so ist $\mathbf{Q}(\zeta_n)$ galoissch über $\mathbf{Q}$ mit Gruppe $(\mathbf{Z}/n)^\times$. Ist $n = p_1^{r_1} \dots p_s^{r_s}$ die Primfaktorzerlegung, so ist $\mathbf{Q}(\zeta_n)$ das Kompositum der Körper $\mathbf{Q}(\zeta_{p_i^{r_i}})$ entsprechend der Zerlegung der Galoisgruppe $(\mathbf{Z}/n)^\times \simeq (\mathbf{Z}/p_1^{r_1})^\times \times \dots \times (\mathbf{Z}/p_s^{r_s})^\times$.
Ähnlich wie oben kann man für $\zeta = \zeta_{p^r}$ zeigen:

- Der Ganzheitsring von $K = \mathbf{Q}(\zeta)$ ist $\mathbf{Z}[\zeta]$.
- Die Diskriminante von $K$ ist $\pm p^{p^{r-1}(pr-r-1)}$.
- Die Primzahl $p$ ist total verzweigt in $K$.

Wir wollen später den Satz von Kronecker-Weber beweisen: Ist $L|\mathbf{Q}$ eine abelsche Körpererweiterung, so gibt es ein $n$ mit $L \subseteq \mathbf{Q}(\zeta_n)$.

KAPITEL 11

# Lokalisierung

**Idee:** Sei $K$ ein Körper und $A$ ein Ring in $K$ mit $Quot(A) = K$. Sei $S$ eine multiplikative Teilmenge von $A$ (also $1 \in S$ und mit $a$ und $b$ liegt auch $ab$ in $S$). Dann ist

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

ein Ring mit $A \subseteq S^{-1}A \subseteq K$. In $S^{-1}A$ sind alle Elemente aus $S$ Einheiten.
Ist $\mathfrak{p}$ ein Primideal in $A$, so ist $S = A - \mathfrak{p}$ eine multiplikative Menge. $A_{\mathfrak{p}} = S^{-1}A$ heißt die Lokalisierung von $A$ in $\mathfrak{p}$. Also:

$$A_{\mathfrak{p}} = \{\frac{a}{s} \in K : a \in A, s \notin \mathfrak{p}\}.$$

**Beispiele:**

1. Betrachte den Ring der reellen Polynome $\mathbf{R}[x]$. Dann ist $(x-1)$ ein Primideal. Für ein Polynom $f$ gilt: $f \notin (x-1) \iff f(1) \neq 0$. Also besteht die Lokalisierung in $(x-1)$ genau aus den rationalen Funktionen, die in 1 definiert sind, d.h.

$$\mathbf{R}[x]_{(x-1)} = \{\frac{f(x)}{g(x)} : g(1) \neq 0\}.$$

2. Für eine Primzahl $p$ gilt:

$$\mathbf{Z}_{(p)} = \{\frac{a}{s} \in \mathbf{Q} : a, s \in \mathbf{Z}, p \text{ teilt nicht } s\}.$$

3. Ist $\mathbf{Z} \subseteq R \subseteq \mathbf{Q}$ ein Ring, so gibt es eine Menge $M$ von Primzahlen, sodaß mit $S = \{\prod_{p \in M} p^{n_p} : n_p \geq 0, \text{ fast alle } 0\}$ gilt:

$$R = S^{-1}\mathbf{Z} = \{\frac{a}{\prod_{p \in M} p^{n_p}} : n_p \geq 0, a \in \mathbf{Z}\}$$

(Übung).

Ist $\mathfrak{a}$ ein Ideal in $A$, so ist $S^{-1}\mathfrak{a}$ ein Ideal in $S^{-1}A$. Ist $S \cap \mathfrak{a} \neq \emptyset$, so ist natürlich $S^{-1}\mathfrak{a} = S^{-1}A$. Für Primideale hat man zudem:

SATZ. *Die Zuordnungen*

$$\mathfrak{p} \mapsto S^{-1}\mathfrak{p} \text{ und } \mathfrak{q} \mapsto A \cap \mathfrak{q}$$

*liefern zueinander inverse Bijektionen zwischen den Primidealen in $A \setminus S$ und den Primidealen von $S^{-1}A$.*

*Beweis:* Sei $\mathfrak{p} \subseteq A - S$ ein Primideal. Dann ist auch $S^{-1}\mathfrak{p}$ ein Primideal. Außerdem ist $A \cap S^{-1}\mathfrak{p} = \mathfrak{p}$.
Ist umgekehrt $\mathfrak{q}$ ein Primideal in $S^{-1}A$, so ist natürlich $\mathfrak{q} \cap A$ ein Primideal in $A$ und trivialerweise $S^{-1}(A \cap \mathfrak{q}) = \mathfrak{q}$. Damit folgt die Behauptung. ■

KOROLLAR. *Ist $\mathfrak{p}$ ein Primideal, so ist $A_{\mathfrak{p}}$ ein lokaler Ring, d.h. besitzt ein einziges maximales Ideal, nämlich $\mathfrak{m} = \mathfrak{p}A_{\mathfrak{p}}$. Der Restklassenring $A/\mathfrak{p}$ liegt kanonisch in $A_{\mathfrak{p}}/\mathfrak{m}$ und hat den letzteren als Quotientenkörper. Im Fall, daß $\mathfrak{p}$ maximales Ideal ist, sind die beiden Restklassenringe gleich.*

DEFINITION. Ein diskreter Bewertungsring ist ein Hauptidealring $A$ mit einem einzigen maximalen Ideal $\mathfrak{m} \neq 0$.

**Bemerkungen:**

1. Das maximale Ideal $\mathfrak{m}$ hat die Form $\mathfrak{m} = (\pi)$ mit einem Primelement $\pi$. Jedes von 0 verschiedene Element $a \in A$ hat die Form
$$a = \epsilon \pi^n$$
mit einer Einheit $\epsilon$ und $n \geq 0$. Diese Darstellung hat man dann auch im Quotientenkörper von $A$, wobei nun allerdings nur noch $n \in \mathbf{Z}$ gilt. Der Exponent $n$ heißt die Bewertung $v(a)$ von $a$.
2. Setzt man $v(0) = \infty$, so hat $v$ die Eigenschaften:
$$v(ab) = v(a) + v(b), v(a+b) \geq \min(v(a), v(b)), v(a) < v(b) \Rightarrow v(a+b) = v(a).$$
3. $v(x) \geq 0 \iff x \in A$, $x$ ist Einheit $\iff v(x) = 0$.

SATZ. *Ist $\mathfrak{o}$ ein Dedekindring, $S$ eine multiplikative Teilmenge, so ist auch $S^{-1}\mathfrak{o}$ ein Dedekindring.*

*Beweis:*

- Jedes Ideal von $S^{-1}\mathfrak{o}$ ist endlich erzeugt: klar.
- $S^{-1}\mathfrak{o}$ ist ganz abgeschlossen.
- Jedes Primideal $\neq 0$ ist maximal.

FOLGERUNG. *Ist $\mathfrak{o}$ ein Dedekindring, $\mathfrak{p} \neq 0$ ein Primideal, so ist $\mathfrak{o}_\mathfrak{p}$ ein diskreter Bewertungsring.*

*Beweis:* $\mathfrak{o}_\mathfrak{p}$ ist Dedekindring mit einem einzigen maximalen Ideal $\mathfrak{m}$. Wählt man also $\pi \in \mathfrak{m} - \mathfrak{m}^2$, so gilt: $(\pi) = \mathfrak{m}$ (betrachte die Primidealzerlegung von $(\pi)$). Außer 0 gibt es nun nur die Ideale $\mathfrak{m}^n$, die Hauptideale sind. Daraus folgt die Behauptung. ■

**Bemerkung:** Ist $\mathfrak{a}$ ein Ideal mit der Primidealzerlegung $\mathfrak{a} = \prod \mathfrak{p}_i^{n_i}$, so gilt natürlich
$$\mathfrak{a}\mathfrak{o}_{\mathfrak{p}_0} = \mathfrak{p}_0^{n_0}\mathfrak{o}_{\mathfrak{p}_0},$$
die Ideale sind also durch die Lokalisierungen bestimmt.

Als Anwendungsbeispiel wollen wir folgenden Satz beweisen, den wir später noch brauchen werden.

LEMMA. *Sei $A$ ein diskreter Bewertungsring mit Quotientenkörper $K$, $L$ eine endliche Erweiterung von $K$, $B$ der ganze Abschluß von $A$ in $L$. Wir setzen voraus, daß über $\mathfrak{p}$ nur ein Primideal $\mathfrak{P}$ liegt, d.h. auch $B$ ist diskreter Bewertungsring, außer sei die Restklassenerweiterung separabel. Ist nun $\mathfrak{P} = (\pi)$ und $x \in B$ mit $B/\mathfrak{P} = A/\mathfrak{p}(x)$, so ist $B = A[x, \pi]$.*

*Beweis:* Als $A/\mathfrak{p}$-Modul wird $B/\mathfrak{P}$ erzeugt von den Potenzen von $x$. Als $B/\mathfrak{P}$-Modul wird $B/\mathfrak{p} = B/\mathfrak{P}^e$ erzeugt von den Potenzen von $\pi$. Also wir $B/\mathfrak{p}B$ über $A/\mathfrak{p}$ erzeugt von den Potenzen von $x$ mit $\pi$. Insbesondere:
$$B = A[x, \pi] + \mathfrak{p}B.$$
Nach dem Lemma von Nakayama folgt hieraus die Behauptung. ■

SATZ. *Voraussetzung wie im Lemma. Dann besitzt $B$ eine Potenzganzheitsbasis über $A$.*

*Beweis:* Nach dem Lemma ist $B = A[x, \pi]$. Sei $f \in A[X]$, so daß $f$ mod $\mathfrak{p}$ das Minimalpolynom von $x$ über $A/\mathfrak{p}$ ist. Dann ist $f(x) \equiv 0 \bmod \pi$.

**1. Fall::** $f(x) \not\equiv 0 \bmod \mathfrak{P}^2$. Dann ist $f(x)$ Primelement und die Behauptung folgt mit $B = A[x, f(x)] = A[x]$.

**2. Fall::** $f(x) \equiv 0 \bmod \mathfrak{P}^2$. Da $f'(x) \not\equiv 0 \bmod \mathfrak{P}$ ist, folgt mit
$$f(x+\pi) = f(x) + f'(x)\pi \equiv f'(x)\pi \bmod \mathfrak{P}^2$$
daß $f(x+\pi)$ ein Primelement ist. Natürlich erzeugt $x+\pi$ auch $B/\mathfrak{P}$ über $A/\mathfrak{p}$, also folgt mit dem Lemma sofort $B = A[x+\pi, f(x+\pi)] = A[x+\pi]$. ■

**Beispiel:** Wir betrachten $K = \mathbf{Q}(\sqrt{-5})$ über $\mathbf{Q}$. Die Diskriminante von $K$ ist $-20$, also ist 2 voll verzweigt: $(2) = \mathfrak{p}^2$. Sei $A = \mathbf{Z}_{(2)}$. Wir wollen den ganzen Abschluß $B$ von $A$ in $K$ bestimmen. Sei $v$ die zu $B$ gehörige Bewertung, also $v(2) = 2$. Nun ist $(1+\sqrt{-5})(1-\sqrt{-5}) = 6$. D.h. $v(1+\sqrt{-5}) = 1$, also ist $\pi = 1+\sqrt{-5}$ ein Primelement. Damit ist $B = \mathbf{Z}_{(2)}[1+\sqrt{-5}]$. Das Primelement genügt der Gleichung

$$x^2 - 2x + 6 = 0,$$

dies ist eine Eisensteingleichung.

Wir geben noch eine Folgerung aus dem Satz:

FOLGERUNG. *Sei $L$ total verzweigt über $K$, dann ist $B = A[\pi]$ und $\pi$ genügt einer Eisensteingleichung.*

*Beweis:* Wir wissen schon, daß $B = A[\pi]$ gilt. Sei

$$\pi^n + a_{n-1}\pi^{n-1} + \cdots + a_0 = 0$$

Angenommen $\pi$ teilt $a_0, a_1, \ldots, a_{i-1}$, aber nicht $a_i$ für ein $i < n$. Dann teilt auch $\pi^n$ die Zahlen $a_0, \ldots, a_{i-1}$. Insbesondere teilt $\pi^{i+1}$ alle Zahlen außer $a_i\pi^i$. Dies ist aber ein Widerspruch. Also haben wir $\pi^n | a_i$ für alle $i$. Wäre $\pi^{n+1} | a_0$, so würde genau $\pi^n$ die Gleichung teilen, das ist aber ein Widerspruch. ■

In diesem Fall gibt es also immer eine Potenzganzheitsbasis. Daß man aber das i.a. auch lokal nicht erwarten kann, zeigt nochmals unser altes Beispiel.

**Beispiel:** Sei $A = \mathbf{Z}_{(2)}$ und $K = \mathbf{Q}$, $L$ ein kubische Erweiterung von $K$, in der 2 voll zerfällt: $(2) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$. Sei $B$ der ganze Abschluß von $A$ in $L$. Dann ist $B/(2) \simeq \mathbf{F}_2 \oplus \mathbf{F}_2 \oplus \mathbf{F}_2$. Angenommen, es gäbe ein Potenzganzheitsbasis: $B = A[\alpha]$. Sei $f(x)$ das Minimalpolynom von $\alpha$ über $A$. Dann wäre

$$B/(2) = \mathbf{F}_2[x]/(f).$$

$f$ müßte drei verschiedene Nullstellen in $\mathbf{F}_2$ haben, was natürlich nicht geht.

KAPITEL 12

# Verzweigung

### Zur Motivation

**Beispiel:** Wir betrachten quadratische Zahlkörper $\mathbf{Q}(\sqrt{m})$. Dann ist $D_K = m$ für $m \equiv 1 \bmod 4$ und sonst $D_K = 4m$. Ein $p$ verzweigt in $K$ genau dann, wenn $p|D_K$.

- Welche $K$ sind genau in 13 verzweigt? $\mathbf{Q}(\sqrt{13})$.
- Welche $K$ sind genau in 3 und 13 verzweigt? $\mathbf{Q}(\sqrt{-39})$.
- Welche $K$ sind genau in 2 und 5 verzweigt? $\mathbf{Q}(\sqrt{-5})$.
- Welche $K$ sind genau in 2 verzweigt? $\mathbf{Q}(i)$, $\mathbf{Q}(\sqrt{2})$ und $\mathbf{Q}(\sqrt{-2})$.

Die Verzweigung scheint also den Zahlkörper schon recht genau zu bestimmen. Dabei scheint 2 eine Sonderrolle zu spielen. Außerdem stellt man fest, daß ungerade Primzahlen $D_K$ höchstens zur ersten Potenz teilen, während für die 2 eine der Fälle gilt: 2 teilt nicht $D_K$, $2^2||D_K$ oder $2^3||D_K$.

Wir betrachten jetzt folgende Situation: $A$ sei Hauptidealring mit Quotientenkörper $K$, $L$ eine endliche separable Körpererweiterung von $K$ und $B$ der ganze Abschluß von $A$ in $L$. Wir nehmen an, daß die Restklassenkörper endlich sind. Da $A$ ein Hauptidealring ist, können wir die Diskriminante $D_{B|A}$ wie üblich bilden.

SATZ. *Ein Primideal $\mathfrak{p}$ von $A$ verzweigt genau dann in $L$, wenn $\mathfrak{p}$ die Diskriminante $D_{B|A}$ teilt.*

*Beweis:* Sei $x_1, \ldots, x_n$ eine Ganzheitsbasis von $B$. Dann ist die Diskriminante $D_{B|A} = det(Sp(x_i x_j))$.

- $\mathfrak{p}$ verzweigt: Also $\mathfrak{p} = \mathfrak{P}_1^{e_1} \ldots$ und o.E. $e_1 > 1$. Dann ist $B/\mathfrak{p} = B/PP_1^{e_1} \oplus \ldots$. Es gibt ein $x \in B/\mathfrak{p}$, das nilpotent aber nicht 0 ist. Für alle $y \in B/\mathfrak{p}$ ist dann auch $xy$ nilpotent. Die zugehörige Matrix ist also auch nilpotent, d.h. sie hat Spur 0. Dann ist aber die Spurform ausgeartet, d.h. $D_{B|A} \equiv 0 \bmod \mathfrak{p}$.
- $\mathfrak{p}$ unverzweigt: Dann ist $B/\mathfrak{p}$ eine direkte Summe von Körpern, die Spurform ist also nicht ausgeartet, d.h. $D_K \not\equiv 0 \bmod \mathfrak{p}$.

Damit folgt die Behauptung. ■

Ist $A$ kein Hauptidealring, so können wir die Diskriminante $D_{B|A}$ nicht in der angegebenen Form definieren.

### Diskriminantenabschätzung

SATZ. *Für die Diskriminante $D_K$ eines Zahlkörpers $K$ vom Grad $n$ über $\mathbf{Q}$ gilt:*

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

*Dies läßt sich durch*

$$|D_K| \geq 0.156 \cdot 3.976^n$$

*abschätzen.*

*Beweis:* Jede Idealklasse enthält ein ganzes Ideal $\mathfrak{a}$ mit Norm

$$N\mathfrak{a} \leq (4/\pi)^{r_2} n!/n^n \sqrt{|D_K|}.$$

Nun ist $N\mathfrak{a} \geq 1$, also folgt für die Diskriminante

$$|D_K| \geq (\pi/4)^{2r_2} n^{2n}/n!^2 \geq (\pi/4)^n n^{2n}/n!^2.$$

Sei $a_n = (\pi/4)^n n^{2n}/n!^2$. Dann ist

$$a_{n+1}/a_n = \pi/4(1+1/n)^{2n}.$$

Nun weiß man, daß $(1+1/n)^n \geq 9/4$ ist, also folgt

$$a_{n+1}/a_n \geq 81\pi/64$$

Direkt sieht man $a_2 \geq \pi^2/4$, woraus dann folgt:

$$a_n \geq (81\pi/64)^{n-2}\pi^2/4 = 1024/6561 \cdot (81\pi/64)^n \geq 0.156 \cdot 3.976^n$$

■

FOLGERUNG. $\mathbf{Q}$ *besitzt keine unverzweigten Erweiterungen (Ist $K$ ein Zahlkörper $\neq \mathbf{Q}$, so gibt es immer verzweigte Primzahlen.)*

*Beweis:* Für $n = 2$ liefert die Formel 2.466 und wächst dann streng monoton, also ist $|D_K| > 1$. Die Teiler von $D_K$ sind verzweigt. ■

### Unverzweigte Erweiterungen

**Beispiel:** Sei $K = \mathbf{Q}(i, \sqrt{3})$. Dies ist eine biquadratische Erweiterung von $\mathbf{Q}$ mit den quadratischen Teilkörpern $\mathbf{Q}(i)$, $\mathbf{Q}(\sqrt{-3})$, $\mathbf{Q}(\sqrt{3})$. Die Zahl $a = i + \sqrt{3}$ hat das Minimalpolynom $x^4 - 4x^2 + 16 = 0$. Die Diskriminante davon ist $2^{16} \cdot 3^2$, also ist $K$ höchstens in 2 und 3 verzweigt. Betrachtet man die Verzweigungsindizes von 2 und 3, so sieht man sofort, daß $K|\mathbf{Q}(\sqrt{3})$ unverzweigt ist.

Es gibt also Zahlkörper mit unverzweigten Erweiterungen.

SATZ. *Das Kompositum unverzweigter Erweiterungen ist unverzweigt.*

**Beispiel:** Sind $K_1$ und $K_2$ zwei Zahlkörper mit Diskriminanten $D_1$ und $D_2$, so sind genau die Primzahlen $p$ mit $p|D_1D_2$ im Kompositum $K_1K_2$ verzweigt.

### Die Differente

Wir definieren

$$\mathfrak{M}_{B|A} = \{x \in L : Sp_{L|K}(xB) \subseteq A\}.$$

Sei $x_1, \ldots, x_n$ eine in $B$ enthaltene $K$-Basis von $L$. Da die Spurform nicht ausgeartet ist, gibt es dazu eine duale Basis $y_1, \ldots, y_n$ mit der Eigenschaft: $Sp(x_iy_j) = \delta_{ij}$. Wir setzen an $x = \sum a_iy_i$. Dann ist $Sp(xx_j) = a_j$, woraus folgt:

$$x \in \mathfrak{M} \Rightarrow a_j = Sp(xx_j) \in A,$$

d.h. $\mathfrak{M} \subseteq \sum Ay_i$. Also ist auch $\mathfrak{M}$ endlich erzeugt, also ein gebrochenes $B$-Ideal. Offensichtlich ist auch $B \subseteq \mathfrak{M}$.

DEFINITION. Das Ideal $\mathfrak{M}_{B|A}^{-1}$ heißt die Differente $\mathfrak{D}_{B|A}$ von $B$ über $A$.

**Eigenschaften:**

- Obige Bildung ist mit Lokalisieren verträglich, d.h.
$$S^{-1}\mathfrak{D}_{B|A} = \mathfrak{D}_{S^{-1}B|S^{-1}A},$$
wo $S$ eine multiplikative Teilmenge von $A$ ist.
- Ist $B = \sum Ax_i$, so ist $\mathfrak{D}_{B|A}^{-1} = \sum Ay_i$ mit der Dualbasis $y_i$, wie aus obiger Rechnung folgt. Dies gilt insbesondere, wenn $A$ Hauptidealring ist.

SATZ. *Die Norm der Differente ist die Diskriminante.*

*Beweis:* Nach Lokalisieren können wir annehmen, daß $A$ ein Hauptidealring ist, also $B = \sum Ax_i$. Dann ist $\mathfrak{D}_{B|A}^{-1} = \sum Ay_i$. Seien $t_{ij} \in K$ mit $y_i = \sum s_{ij}x_j$ und $x_i = \sum s_{ij}y_j$. Dann ist $Sp(x_ix_j) = s_{ij}$, also $Diskriminante = \det(S)$. Andererseits ist die Norm $Norm(\mathfrak{M}) = \det(T)$, also $Norm(\mathfrak{D}) = Diskriminante$. ■

SATZ. *Ist $B = A[\alpha]$ und $f$ das Minimalpolynom von $\alpha$, so gilt*

$$\mathfrak{D}_{B|A} = (f'(\alpha)).$$

*Beweis:* Sei $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ und

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

Seien $c_1, \ldots, c_n$ die Nullstellen von $f$. Nun gilt:

$$\sum \frac{f(x)}{x-c_i}\frac{c_i^r}{f'(c_i)} = x^r,$$

für $0 \le r \le n-1$, weil die Differenz ein Polynom vom Grad $\le n-1$ ist, aber die $n$ Nullstellen $c_1, \ldots, c_n$ hat. Das bedeutet:

$$Sp(\frac{f(x)c^r}{(x-c)f'(c)}) = x^r$$

und durch Koeffizientenvergleich:

$$Sp(c^i\frac{b_j}{f'(c)}) = \delta_{ij}$$

Also ist $\frac{b_j}{f'(\alpha)}$ die Dualbasis von $1, \alpha, \ldots, \alpha^{n-1}$.
Aus $f(x)/(x-\alpha) = \sum b_i x^i$ folgt durch Koeffizientenvergleich

$$a_i = b_{i-1} - \alpha b_i.$$

Also ergibt sich leicht durch Induktion

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

Genauer:

$$\begin{pmatrix} b_{n-1} \\ b_{n-2} \\ \vdots \\ b_0 \end{pmatrix} = \begin{pmatrix} 1 & & & & \\ a_{n-1} & 1 & & & \\ \vdots & & & & \\ a_1 & a_2 & \ldots & a_{n-1} & 1 \end{pmatrix} \begin{pmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{n-1} \end{pmatrix}.$$

Daraus ergibt sich sofort folgende Transformationsmatrix:

$$(b_{n-1}, \ldots, b_0)^t = T \cdot (1, \alpha, \ldots, \alpha^{n-1})^t$$

Da $\det T = 1$ ist, erzeugen die $b_i$ und die Potenzen von $\alpha$ den gleichen $A$-Modul, woraus dann sofort die Behauptung folgt. ■

**Beispiel:** Sei $B|A$ voll verzweigt, $A$ und damit auch $B$ diskreter Bewertungsring. Dann ist $B = A[\pi]$. Sei $f = a_0 + \cdots + x^n$ das Minimalpolynom von $\pi$. $f$ ist also ein Eisensteinpolynom. Die Differente wird erzeugt von

$$f'(\pi) = e\pi^{e-1} + (e-1)a_1\pi^{e-2} + \cdots + a_{e-1}.$$

Dann gibt es zwei Fälle:

- $\pi$ **teilt nicht** $e$**:** Dann ist $v(f'(\pi)) = e-1$, also $\mathfrak{D} = \pi^{e-1}$.
- $\pi$ **teilt** $e$**:** Dann ist $v(f'(\pi)) \ge e$, also $\mathfrak{D} = \mathfrak{P}^{\ge e}$.

$\pi|e$ bedeutet $e \in \mathfrak{P}$, d.h. $e = 0 \in B/\mathfrak{P}$, d.h. die Restklassencharakteristik $p$ teilt $e$.

DEFINITION. $\mathfrak{P}$ heißt zahm verzweigt, falls $p$ den Verzweigungsindex nicht teilt, andernfalls wild verzweigt.

Damit erhalten wir

LEMMA. *Sei $A$ diskreter Bewertungsring und $L|K$ total verzweigt. Ist $\mathfrak{P}$ zahm verzweigt, so ist*

$$\mathfrak{D} = \mathfrak{P}^{n-1} \text{ und } D_{B|A} = \mathfrak{p}^{n-1}$$

*Liegt wilde Verzweigung vor, so ist*

$$\mathfrak{D} = \mathfrak{P}^{n+\delta} \text{ und } D_{B|A} = \mathfrak{p}^{n+\delta}.$$

**Beispiele:**

1. Wir wissen, daß $\mathbf{Q}(\zeta_p)$ über $\mathbf{Q}$ voll verzweigt ist. Da der Körpergrad $p-1$ ist, liegt zahme Verzweigung vor. Also
$$\mathfrak{D} = \mathfrak{p}^{p-2} \text{ und } D = \pm p^{p-2},$$
was wir bereits wissen.
2. Bei den quadratischen Zahlkörpern wissen wir: Geht eine ungerade Primzahl $p$ in der Diskriminante auf, so genau zur ersten Potenz: zahme Verzweigung. Verzweigt die 2, so liegt wilde Verzweigung vor, die Diskriminante wird mindestens von 4 geteilt.

SATZ. *Schachtelungsformel für die Differente: Hat man drei Erweiterungen $K \subseteq L \subseteq M$ mit den Ganzheitsringen $A \subseteq B \subseteq C$, so gilt:*
$$\mathfrak{D}_{C|A} = \mathfrak{D}_{C|B}\mathfrak{D}_{B|A}.$$

*Beweis:*
$$x \in \mathfrak{D}_{C|A}^{-1} \iff Sp_{L|K}(Sp_{M|L}(xC)) \subseteq A \iff Sp_{M|L}(xC) \subseteq \mathfrak{D}_{B|A}^{-1}$$
$$\iff Sp_{M|L}(x\mathfrak{D}_{B|A}C) \subseteq B \iff x\mathfrak{D}_{B|A} \subseteq \mathfrak{D}_{C|B}^{-1}$$
$$\iff x \subseteq \mathfrak{D}_{C|B}^{-1}\mathfrak{D}_{B_A}^{-1}$$
woraus sofort die Behauptung folgt. ■

FOLGERUNG. *Schachtelungsformel für die Diskriminante:*
$$D_{C|A} = N_{L|K}(D_{C|B}) \cdot D_{B|A}^m$$

*Beweis:*
$$D_{C|A} = N_{L|K}N_{M|L}(\mathfrak{D}_{C|B}\mathfrak{D}_{B|A}) = N_{L|K}(D_{C|B}\mathfrak{D}_{B|A}^m) = N_{L|K}(D_{C|B}) \cdot D_{B|A}^m. \blacksquare$$

## Höhere Verzweigungsgruppen

Wir hatten schon früher Zerlegungsgruppe und Trägheitsgruppe definiert (Diagramm). Jetzt wollen wir die Verzweigung näher studieren.
Situation: $L|K$ galoissch mit Gruppe $G$, $A$ und $B$ jeweils diskrete Bewertungsringe. O.E. $B = A[\pi]$.
Wir definieren
$$G_i = \{\sigma \in G_\mathfrak{p} : \sigma \text{ operiert trivial auf } B/\mathfrak{P}^{i+1}\}$$
Wir definieren:
$$G_0 \to (B/\mathfrak{P})^* \text{ durch } \sigma \mapsto \frac{\sigma\pi}{\pi} \bmod \mathfrak{P}$$

- Die Definition hängt nicht von der Wahl von $\pi$ ab. Denn: Ist $u$ eine Einheit, so ist $\sigma u \equiv u$, also $\frac{\sigma u}{u} = 1$ in $B/\mathfrak{P}$.
- Daher ist dies ein Gruppenhomomorphismus.
- Der Kern ist $G_1$.
- Man hat also eine Einbettung $G_0/G_1 \hookrightarrow (B/\mathfrak{P})^*$.

$G_\mathfrak{P}$ operiert durch Konjugation auf $G_0$. Wie wirkt sich dies auf obige Abbildung aus?

- Sei $\sigma \in G_0$ und $\sigma\pi = a\pi$. Sei $\tau \in G_\mathfrak{P}$ und $\tau^{-1}\pi = b\pi$. Dann wird $\tau\sigma\tau^{-1}$ abgebildet auf
$$\frac{\tau\sigma\tau^{-1}\pi}{\pi} = \frac{\tau\sigma(b\pi)}{\pi} = \frac{\tau\sigma(b) \cdot \tau(a)\tau(\pi)}{\tau(b)\tau(\pi)} = \tau(a)$$
da $\sigma$ trivial auf $a$ operiert.

FOLGERUNG. *Ist $G_\mathfrak{P}$ abelsch, so ist $G_0/G_1 \subseteq (A/\mathfrak{p})^*$.*

Was passiert mit den höheren Verzweigungsgruppen?
Sei jetzt $i \geq 1$. Sei $\sigma \in G_i$. Dann ist $\sigma\pi = \pi + a\pi^{i+1}$. Wir bilden jetzt $\sigma$ ab auf $a \in B/\mathfrak{P}$.

- Homomorphismus: Sei $\sigma\pi = \pi + a\pi^{i+1}$ und $\tau\pi = \pi + b\pi^{i+1}$. Dann gilt:
$$\sigma\tau\pi = \sigma\pi + \sigma b(\sigma\pi)^{i+1} = \pi + a\pi^{i+1} + \sigma b(\pi + a\pi^{i+1})^{i+1}.$$
Nun müssen wir nur modulo $\pi^{i+2}$ rechnen. Also gilt weiter:
$$\sigma\tau\pi = \pi + (a+b)\pi^{i+1} + (\sigma b - b)\pi^{i+1},$$
woraus dann die Behauptung folgt.
- Der Kern ist trivialerweise $G_{i+1}$. Also haben wir
$$G_i/G_{i+1} \subseteq B/\mathfrak{P}.$$
- $G_{\mathfrak{P}}$ normalisiert $G_i$. Operiert $\tau$ durch Konjugation auf $G_i$, so durch $\tau(a)$ auf $B/\mathfrak{P}$.
- Ist insbesondere $G_{\mathfrak{P}}$ abelsch, so hat man also
$$G_i/G_{i+1} \subseteq A/\mathfrak{p}$$

FOLGERUNG. *Ist $p$ die Charakteristik des Restklassenkörpers, so ist $G_0/G_1$ zyklisch von zu $p$ teilerfremder Ordnung. $G_1$ ist eine $p$-Gruppe.*

SATZ. *Für die Diskriminante gilt:*
$$v_L(\mathfrak{d}) = \sum_{i\geq 0}(|G_i| - 1)$$

*Beweis:* Wir müssen den Wert von $f'(\pi)$ ausrechnen, also von
$$\prod_{\sigma\neq 1}(\pi - \sigma\pi)$$
Nun impliziert $v(\pi - \sigma\pi) = m$, daß $\sigma \in G_{m-1}$, aber $\sigma \notin G_m$. Also
$$v(\pi - \sigma\pi) = \#\{i : \sigma \in G_i\}$$
Nun ist
$$v(\mathfrak{d}) = \sum_{\sigma\neq 1} v(\pi - \sigma\pi) = \sum_{\sigma\neq 1}\#\{i : \sigma \in G_i\} = \sum_{i\geq 0}(|G_i| - 1).\blacksquare$$

**Beispiel:**

- $\mathbf{Q}(i)$. Sei $\sigma$ die komplexe Konjugation, $p = 2$, $\pi = 1 + i$. Dann gilt
$$\sigma \in G_j \iff \sigma i \equiv i \bmod \pi^{j+1} \iff \pi^{j+1}|2i \iff j+1 \leq 2 \iff j \leq 1,$$
also
$$G_0 = G_1 = \{1, \sigma\}, \quad G_2 = G_3 = \cdots = \{1\}.$$
- $\mathbf{Q}(\sqrt{2})$. Sei $\sigma$ der nichttriviale Automorphismus, $p = 2$, $\pi = \sqrt{2}$. Dann gilt
$$\sigma \in G_j \iff \sigma\sqrt{2} \equiv \sqrt{2} \bmod \pi^{j+1} \iff \pi^{j+1}|2\sqrt{2} \iff j+1 \leq 3 \iff j \leq 2,$$
also
$$G_0 = G_1 = G_2 = \{1, \sigma\}, \quad G_3 = G_4 = \cdots = \{1\}.$$

KAPITEL 13

# Der Satz von Kronecker-Weber

SATZ. *Ist $K$ abelsch über $\mathbf{Q}$, so gibt es eine Einheitswurzel $\zeta$ mit $K \subseteq \mathbf{Q}(\zeta)$.*

Beweis nach A. Speiser, Die Zerlegungsgruppe, Crelle J. **149** (1919), 174-188.

**1. Schritt:** Es gibt verzweigte Primzahlen, da $|D_K| \neq 1$

**2. Schritt:** Reduktion auf den Fall $[K : \mathbf{Q}] = p^m$.
Nach dem Hauptsatz über endliche abelsche Gruppe ist jede endliche abelsche Gruppe $G$ ein direktes Produkt von abelschen Gruppen $G_i$ von Primzahlpotenzordnung $p_i^{n_i}$: $G = G_1 \times \cdots \times G_m$. Sei $K_i = Fix(\prod_{j \neq i} G_j)$. Dann ist $K_i$ galoissch über $\mathbf{Q}$ mit Gruppe $G_i$ und $K = \prod K_i$. Es genügt die Behauptung für $K_i$ zu zeigen. $K_i$ hat Grad $p_i^{n_i}$ über $\mathbf{Q}$.

**3. Schritt:** Reduktion auf den Fall, daß nur $p$ in $K$ verzweigt

- Sei $l \neq p$ in $K$ verzweigt. $l$ ist zahm verzweigt. In $L = K(\zeta_l)$ ist $l$ auch zahm verzweigt von der Verzweigungsordnung $l - 1$, da $G_0/G_1 \subseteq \mathbf{F}_l^\times$.
- Sei $T$ die Trägheitsgruppe von $l$ in $L$. Sie hat die Ordnung $l - 1$. Sei $K_1 = Fix(T)$. Dann ist $l$ in $K_1$ unverzweigt, insbesondere ist $K_1 \cap \mathbf{Q}(\zeta_l) = \mathbf{Q}$.
- Aus Gradgründen ist $L = K_1(\zeta_l)$. Also $K \subseteq K_1(\zeta_l)$. Und $[K_1 : \mathbf{Q}] | [K : \mathbf{Q}]$.
- Da das Kompositum unverzweigter Erweiterungen unverzweigt ist, verzweigen in $K_1$ nur Primzahlen, die auch in $K$ verzweigen, bis auf $l$.
- Rekursiv zeigt man also: $K \subseteq K_0(\zeta_{l_1}, \ldots, \zeta_{l_r})$, wenn $l_i$ in $K$ verzweigen, wo nun in $K_0$ nur noch $p$ verzweigt mit $K_0$ von $p$-Potenzgrad.

**4. Schritt:** $p = 2$
Sei also $K$ von 2-Potenzgrad, so daß in $K$ nur die 2 verzweigt. Ist $[K : \mathbf{Q}] = 2$, so ist offensichtlich $K$ einer der Körper $\mathbf{Q}(i)$, $\mathbf{Q}(\sqrt{2})$ oder $\mathbf{Q}(\sqrt{-2})$. O.E. können wir $\mathbf{Q}(i) \subset K$ und $K \neq \mathbf{Q}(i)$ annehmen.

LEMMA. *$K|\mathbf{Q}(i)$ besitzt nur einen Zwischenkörper $K_0$ vom Grad 2 über $\mathbf{Q}(i)$.*

*Beweis:* Sei $K_0$ ein solcher Zwischenkörper. Da $K_0$ über $\mathbf{Q}$ abelsch ist, ist die komplexe Konjugation ein nichttrivialer Automorphismus. Der Fixkörper ist ein nur in 2 verzweigter reellquadratischer Körper, also $\mathbf{Q}(\sqrt{2})$. Damit ist $K_0 = \mathbf{Q}(i, \sqrt{2})$. ■

Betrachte nun $L = K(\zeta_{2^{m+1}})$. Dies ist ein abelscher Körper mit 2-Potenzgrad, in dem nur 2 verzweigt. Da $L|\mathbf{Q}(i)$ nur einen Zwischenkörper vom Grad 2 über $\mathbf{Q}(i)$ besitzt, ist $L|\mathbf{Q}(i)$ zyklisch. Wäre $K \neq \mathbf{Q}(\zeta)$, so wäre $L$ über $\mathbf{Q}(i)$ nicht zyklisch, ein Widerspruch. Daraus folgt die Behauptung.

**5. Schritt:** $p > 2$

LEMMA. *Ist $K|\mathbf{Q}$ abelsch vom Grad $p$, so ist $D_K = \pm p^{2(p-1)}$.*

*Beweis:*

- Sei $(p) = \mathfrak{p}^p$. Wegen wilder Verzweigung gilt für die Differente $\mathfrak{D} = \mathfrak{p}^{p+\delta}$ mit $\delta \geq 0$.
- Sei $v = v_\mathfrak{p}$. Sind $G_i$ die Verzweigungsgruppen, so gilt $|G_i| \in \{1, p\}$. Mit $v(\mathfrak{D}) = \sum(|G_i| - 1)$ folgt $v(\mathfrak{D}) = \lambda(p - 1)$. Nach dem letzten Punkt gilt $\lambda \geq 2$.

- Sei $\pi$ ein Element mit $v(\pi) = 1$ und $f = x^p + a_{p-1}x^{p-1} + \cdots + a_1 x + a_0$ das Minimalpolynom von $\pi$. Dann ist
$$v(f'(\pi)) = \min(v(p\pi^{p-1}), v((p-1)a_{p-1}\pi^{p-2}), \ldots, v(a_1)) \leq 2p-1$$
wegen des ersten Terms. Damit erhalten wir $\lambda(p-1) \leq 2p-1$, was wegen $p \geq 3$ sofort $\lambda \leq 2$ liefert. Also folgt $\lambda = 2$ und damit $\mathfrak{D} = \mathfrak{p}^{2(p-1)}$, was die Behauptung zeigt. ■

LEMMA. *Es gibt nur einen abelschen Körper $K|\mathbf{Q}$ vom Grad $p$, in dem nur $p$ verzweigt. ($K$ ist der Teilkörper von $\mathbf{Q}(\zeta_{p^2})$ vom Grad $p$.)*

*Beweis:*

- Angenommen, es gäbe zwei solcher Körper. Dann gibt es eine Erweiterung $K|\mathbf{Q}$ mit Gruppe $\mathbf{Z}/p \times \mathbf{Z}/p$, in der $p$ total verzweigt. Seien $K_i$ die $p+1$ Zwischenkörper und $H_i$ die zugehörigen Untergruppen der Galoisgruppe.
- Für die Verzweigungsgruppen gilt: $G = G_0 = G_1$. Und $G_i/G_{i+1} \subseteq \mathbf{F}_p$. Also
$$G = G_0 = G_1 = \cdots = G_r \neq G_{r+1} = \cdots = G_s \neq G_{s+1} = \cdots = \{1\}.$$
- Für $H_j = G_s$ ist für die Situation $K|K_j$ die Verzweigungsgruppenreihe $s+1$ mal die Gruppe $H_j$, dann die Gruppe $\{1\}$, also hätte $K_j$ eine andere Diskriminante als die anderen $K_i$'s, was nicht sein kann wegen des letzten Lemmas. ■

LEMMA. *Ist $K|\mathbf{Q}$ abelsch vom Grad $p^n$, so ist $K|\mathbf{Q}$ zyklisch.*

*Beweis:* Wäre $K|\mathbf{Q}$ nicht zyklisch, so gäbe es zwei verschiedene Teilkörper vom Grad $p$, was nach dem letzten Lemma unmöglich ist. ■

LEMMA. *Ist $K|\mathbf{Q}$ abelsch vom Grad $p^n$, so gilt $K \subseteq \mathbf{Q}(\zeta_{p^{n+1}})$.*

*Beweis:* Nach dem letzten Lemma muß $K$ mit dem Teilkörper von $\mathbf{Q}(\zeta_{p^{n+1}})$ vom Grad $p^n$ übereinstimmen. ■

KAPITEL 14

# Diskret bewertete Körper

DEFINITION. Ein diskret bewerteter Körper ist ein Körper $K$ zusammen mit einer Bewertung $v : K^\times \to \mathbf{Z}$, die also folgende Eigenschaften erfüllt:

- $v(xy) = v(x) + v(y)$
- $v(x+y) \geq \min(v(x), v(y))$
- $v$ ist o.E. surjektiv und $v(0) = \infty$

**Bemerkungen:**

- $v(\pm 1) = 0$, denn: $v(x) = v(1) + v(x)$, also $v(1) = 0$ und $0 = v(1) = v(-1) + v(-1) = 2v(-1)$, also $v(-1) = 0$.
- Es gilt für $v(x) \neq v(y)$: $v(x+y) = \min(v(x), v(y))$, denn sei o.E. $v(x) < v(y)$. Dann ist $v(x) = v((x+y) - y) \geq \min(v(x+y), v(y))$, woraus sofort $v(x) \geq v(x+y)$ folgt. Andererseits ist aber $v(x+y) \geq v(x)$. Daraus folgt nun die Gleichheit.
- Durch $A = \{x \in K : v(x) \geq 0\}$ erhält man einen diskreten Bewertungsring mit maximalem Ideal $m = \{x \in K : v(x) > 0\}$. Die Einheiten sind die Elemente $x$ mit $v(x) = 0$.
- Umgekehrt haben wir bereits gesehen, daß diskrete Bewertungsringe diskrete Bewertungen liefern.

**Beispiele:**

- Sei $K$ ein Zahlkörper und $\mathfrak{p}$ ein Primideal in $\mathfrak{o}_K$. Für $x \in K$, $x \neq 0$ hat dann das gebrochene Ideal $(x)$ eine eindeutige Primidealzerlegung: $(x) = \mathfrak{p}^{v_\mathfrak{p}(x)} \ldots$. Der Exponent $v_\mathfrak{p}(x)$ liefert eine diskrete Bewertung auf $K$. Der Bewertungsring ist die Lokalisierung von $\mathfrak{o}_K$ in $\mathfrak{p}$.
- Speziell für $K = \mathbf{Q}$ haben wir die $p$-adischen Bewertungen $v_p$.

Zu einer Bewertung definieren wir den zugehörigen Absolutbetrag:

$$|x| = e^{-v(x)}.$$

Statt $e$ kann man auch irgendeine andere reelle Zahl $> 1$ wählen. Man hat die Eigenschaften:

- $|x| = 0 \iff x = 0$
- $|xy| = |x||y|$
- $|x+y| \leq \max(|x|, |y|)$ und Gleichheit, falls $|x| \neq |y|$.
- Natürlich gilt insbesondere die gewöhnliche Dreiecksungleichung $|x+y| \leq |x| + |y|$.
- $|1| = |-1| = 1$.

**Beispiel:** $K = \mathbf{Q}$. Für die $p$-adische Bewertung $v_p$ setzen wir $|x|_p = p^{-v_p(x)}$. Also $|p| = 1/p$ und $|p^n| = 1/p^n$.

Hat man einen Körper mit einem Absolutbetrag, hat man auch sofort eine Metrik und Topologie:

$$d(x, y) = |x - y|$$

bezüglich der dann Addition, Multiplikation, Division stetig sind.

**Beispiele:**

- Bezüglich der $p$-adischen Bewertung $||_p$ von $\mathbf{Q}$ ist die Folge $(p^n)_n$ eine Nullfolge.

- Wegen
$$|\sum_{i=0}^{n} p^i - \frac{1}{1-p}|_p = |\frac{-p^{n+1}}{1-p}|_p = \frac{1}{p^{n+1}}$$
gilt
$$\sum_{i=0}^{\infty} p^i = \frac{1}{1-p}.$$

LEMMA. *Sei $K$ ein Körper mit einer diskreten Bewertung. Dann gilt:*

- *$(x_n)$ ist eine Cauchy-Folge genau dann, wenn $(x_{n+1} - x_n)$ eine Nullfolge ist.*
- *Die Partialsummen der Reihe $\sum a_n$ bilden eine Cauchy-Folge genau dann, wenn $(a_n)$ eine Nullfolge ist.*

*Beweis:*

- Die eine Richtung ist klar. Sei also $(x_{n+1} - x_n)$ eine Nullfolge. Sei $\epsilon > 0$ beliebig. Dann gibt es ein $N$ mit: $n \geq N$ impliziert $|x_{n+1} - x_n| < \epsilon$. Daher:
$$|x_{n+m} - x_n| = |(x_{n+m} - x_{n+m-1}) + \cdots + (x_{n+1} - x_n)| < \epsilon.$$
- Die zweite Behauptung folgt sofort aus der ersten.

**Beispiel:** Wir betrachten $\mathbf{Q}$ mit der 5-adischen Bewertung. Wir wollen eine Folge $x_n$ definieren durch die Bedingungen
$$x_0 = 2, \quad x_n^2 + 1 \equiv 0 \bmod 5^{n+1}, \quad x_n \equiv x_{n+1} \bmod 5^{n+1}.$$
Wir konstruieren die Folge rekursiv. Angenommen wir haben bereits $x_{n-1}$. Dann ist $x_{n-1}^2 + 1 = y_{n-1} \cdot 5^n$. Wir setzen an
$$x_n = x_{n-1} + a_n \cdot 5^n$$
Dann gilt modulo $5^{n+1}$:
$$x_n^2 + 1 = y_{n-1} \cdot 5^n + 2x_{n-1}a_n \cdot 5^n \equiv 0 \bmod 5^{n+1}$$
Dies ist äquivalent mit $a_n \equiv y_{n-1} \bmod 5$. Damit läßt sich $a_n$ berechnen. O.E. $0 \leq a_n \leq 4$. Mit $a_0 = 2$ gilt auch:
$$x_n = \sum_{i=0}^{n} a_n \cdot 5^n.$$
Offensichtlich ist $(x_n)$ eine Cauchy-Folge. Sie kann aber nicht konvergieren in $\mathbf{Q}$, da der Grenzwert die Gleichung $x^2 + 1 = 0$ erfüllen würde. Also ist $\mathbf{Q}$ bezüglich der 5-adischen Bewertung nicht vollständig.

DEFINITION. Ein Körper mit einer diskreten Bewertung heißt vollständig bezüglich der Bewertung, falls jede Cauchy-Folge in $K$ konvergiert.

Bezüglich des gewöhnlichen Absolutbetrages ist $\mathbf{Q}$ nicht vollständig. Dazu konstruierte man sich eine Komplettierung: die reellen Zahlen. Ähnlich gehen wir jetzt vor.

**Komplettierung**

- Sei $K$ ein diskret bewerteter Körper. Dann bilden die Cauchy-Folgen einen Ring $R = \{(c_n)\}$.
- Wegen $||c_m| - |c_n|| \leq |c_m - c_n|$ bildet $(|c_n|)$ eine Cauchy-Folge in $\mathbf{R}$, konvergiert also gegen ein $r \in \mathbf{R}$.
  - $r = 0$. Dann ist $(c_n)$ eine Nullfolge.
  - $r > 0$. Wir können mit einer eindeutigen reellen Zahl $b$ schreiben $r = e^{-b}$. Dann konvergiert in $\mathbf{R}$ die Folge $v(c_n)$ gegen $b$. Also ist $b$ eine ganze Zahl.

  Es hat also Sinn zu definieren: $v((c_n)) = \lim v(c_n)$.
- Die Nullfolgen bilden ein maximales Ideal. Denn ist $(c_n)$ keine Nullfolge, so ist auch $(\frac{1}{c_n}) \in R$ und das von $(c_n)$ erzeugte Ideal enthält die 1.
- Wir definieren $\hat{K} = R/m$. Dazu hat man eine Bewertung $\hat{v}$.
- Man erhält eine Einbettung von $K$ in $\hat{K}$ durch $c \mapsto (c, c, c, \dots)$. Jede Cauchyfolge aus $K$ konvergiert in $\hat{K}$: Ist $(c_n)$ Cauchfolge in $K$, so ist $\overline{(c_n)} \in \hat{K}$ der Grenzwert.

- $K$ liegt dicht in $\hat{K}$.
- Daher ist $\hat{K}$ vollständig.
- Man nennt $\hat{K}$ die Komplettierung von $K$. Man kann zeigen, daß sie bis auf Isomorphie eindeutig bestimmt ist.
- Sei $\hat{A}$ der Bewertungsring mit maximalem Ideal $\hat{m}$.

DEFINITION. Die Komplettierung von $\mathbf{Q}$ bezüglich der $p$-adischen Bewertung heißt der Körper $\mathbf{Q}_p$ der $p$-adischen Zahlen. Der Bewertungsring von $\mathbf{Q}_p$ sind die ganzen $p$-adischen Zahlen $\mathbf{Z}_p$.

**Bemerkungen:**

1. Sei $x \in \mathbf{Q}, x \neq 0$. Dann ist $x = \pm \prod p^{n_p}$. Für eine Primzahl $q$ gilt:
$$|x|_q = \frac{1}{q^{n_q}}$$
also
$$\prod_q |x|_q = \frac{1}{\prod_q q^{n_q}} = \frac{1}{|x|},$$
also
$$|x| \cdot \prod_p |x|_p = 1.$$
Dies nennt man auch Produktformel für die Absolutbeträge auf $\mathbf{Q}$.
2. Man schreibt auch manchmal $\mathbf{Q}_\infty = \mathbf{R}$ und $|x| = |x|_\infty$.

LEMMA. *Es ist $A/m^n \simeq \hat{A}/\hat{m}^n$. Insbesondere sind die Restklassenkörper gleich.*

*Beweis:* Natürlich hat man eine Einbettung $A/m^n \to \hat{A}/\hat{m}^n$. Wie steht es mit der Surjektivität? Sei $x \in \hat{A}$ vorgegeben. Dann gibt es ein $x_0 \in A$ mit $v(x - x_0) \geq n$, also $x \equiv x_0 \bmod \hat{m}^n$, woraus die Behauptung folgt. ■

SATZ. *Sei $M$ ein Repräsentantensystem von $A/m$ in $A$ mit $0 \in M$ und $\pi$ ein Primelement von $A$. Dann hat jedes $x \in \hat{K}$, $x \neq 0$ eine eindeutige Darstellung*
$$x = \pi^m \cdot (a_0 + a_1\pi + a_2\pi^2 + \dots)$$
*mit $a_i \in M$ und $a_0 \neq 0$. Außerdem ist $m = v(x)$.*

*Beweis:* Existenz und Eindeutigkeit. ■

**Beispiel:** $K = \mathbf{C}(x)$ mit der Bewertung $v_{(x)}$ liefert die formalen Potenzreihen.

**Beispiele:** Wir rechnen in $\mathbf{Q}_p$.

- Als Repräsentantensystem wählen wir $M = \{0, 1, 2, \dots, p-1\}$, als Primelement $p$. Dann ist $\mathbf{Z}_p$ die Menge der Zahlen
$$a_0 + a_1 p + a_2 p^2 + \dots$$
mit $0 \leq a_i \leq p - 1$.
- $-1 = \sum_{i=0}^{\infty} (p-1) \cdot p^i$.
- Die Reihe $\sum n!$ konvergiert in $\mathbf{Q}_p$. Grenzwert?
- $\sum n \cdot n! = -1$
- Was ist $\frac{2}{3}$ in $\mathbf{Q}_5$?
$$1 + \sum 5^n + \sum 2 \cdot 5^{2n}?$$

Ein wichtiges Hilfsmittel ist das folgende *Henselsche Lemma*.

LEMMA. *Sei $K$ vollständig bezüglich einer diskreten Bewertung mit Bewertungsring $A$. Hat $f \in A[x]$ eine Zerlegung*

$$f(x) \equiv \bar{g}(x)\bar{h} \bmod \pi$$

*in teilerfremde Polynome $\bar{g}$ und $\bar{h}$ aus $A/m[x]$, so gibt es eine Zerlegung*

$$f(x) = g(x)h(x)$$

*in $A[x]$ mit $g(x) \equiv \bar{g}(x) \bmod \pi$, $h(x) \equiv \bar{h}(x) \bmod \pi$ und $grad(g) = grad(\bar{g})$.*

*Beweis:* Wähle Polynome $g_0$ und $h_0$ in $A[x]$ mit $grad(g_0) = grad(\bar{g})$, $g_0 \equiv \bar{g} \bmod \pi$, $h_0 \equiv \bar{h} \bmod \pi$. Wir machen den Ansatz

$$g_n = g_0 + a_1\pi + \cdots + a_n\pi^n, h_n = h_0 + b_1\pi + \cdots + b_n\pi^n$$

und wollen die Eigenschaften $a_i, b_i \in A[x]$ und $grad(a_i) < grad(g_0)$. Außerdem natürlich $f \equiv g_n h_n \bmod \pi^{n+1}$. Wir konstruieren die Polynome induktiv. Für $n = 0$ ist alles klar.
Der Schritt von $n-1$ nach $n$. Sei $f = g_{n-1}h_{n-1} + c\pi^n$. Wir rechnen modulo $\pi^{n+1}$:

$$g_n h_n \equiv f - c\pi^n + (g_{n-1}b_n + h_{n-1}a_n)\pi^n$$

was sofort die Bedingung

$$c \equiv g_0 b_n + h_0 a_n \bmod \pi$$

ergibt. Die Teilerfremdheit von $g_0$ und $h_0$ modulo $\pi$ liefert, daß wir die Gleichung lösen können und o.E. $grad(a_n) < grad(g_0)$ (sonst wende Division mit Rest an.)
Nun setze $g(x) = \lim g_n(x)$ und $h(x) = \lim h_n(x)$. Damit folgt die Behauptung. ■

FOLGERUNG. *Hat $f(x)$ eine einfache Nullstelle $\bar{x_0}$ modulo $\pi$, so gibt es ein $x_0 \in A$ mit $f(x_0) = 0$ und $x_0 \equiv \bar{x}_0 \bmod \pi$.*

*Beweis:* Wir haben modulo $\pi$: $f(x) \equiv (x - \bar{x}_0) \cdot h(x)$. Setzt man $\bar{(g)} = x - x_0$, so folgt die Behauptung aus dem Lemma. ■

Wir ziehen sofort eine Folgerung:

SATZ. *$\mathbf{Q}_p$ enthält die $(p-1)$-ten Einheitswurzeln $\zeta_{p-1}$. Schreibt man $U_1 = \{x \in \mathbf{Z}_p : x \equiv 1 \bmod p\}$, so hat man für die multiplikative Gruppe die folgende Zerlegung:*

$$\mathbf{Q}_p^\times = \langle p \rangle \times \langle \zeta_{p-1} \rangle \times U_1$$

*Beweis:* Über dem endlichen Körper $\mathbf{F}_p$ gilt:

$$x^{p-1} - 1 = \prod_{i \in \mathbf{F}_p, i \neq 0} (x - i)$$

also zerfällt das Polynom $x^{p-1} - 1$ in $\mathbf{Q}_p$ in Linearfaktoren, d.h. $\zeta_{p-1} \in \mathbf{Q}_p$. Ist nun $x \in \mathbf{Q}_p$, $x \neq 0$, so schreibt man $x = p^n y$ mit $v(y) = 0$. Sei $y \equiv \zeta_{p-1}^k \bmod p$. Dann ist $z = y/\zeta_{p-1}^k \in U_1$ und die Zerlegung folgt. ■

Sei $a \in U_1 \subseteq \mathbf{Q}_p$. Dann ist $a \equiv 1 \bmod p$, also modulo $p$:

$$x^2 - a \equiv (x-1)(x+1) \bmod p$$

Für $p > 2$ gibt es also ein $b \in U_1$ mit $b^2 = a$. D.h. $U_1^2 = U_1$.

FOLGERUNG. *Für $p > 2$ gilt*

$$\mathbf{Q}_p^\times / \mathbf{Q}_p^{\times 2} \simeq \langle p \rangle \times \langle \zeta_{p-1} \rangle,$$

*insbesondere besitzt $\mathbf{Q}_p$ nur drei quadratische Erweiterungen, nämlich*

$$\mathbf{Q}_p(\sqrt{\zeta_{p-1}}), \mathbf{Q}_p(\sqrt{p}), \mathbf{Q}_p(\sqrt{\zeta_{p-1}p})$$

**Übung:** Ist $f = x^n + a_1 x^{n-1} + \cdots + a_n \in K[x]$ mit $a_n \in A$, aber nicht alle Koeffizienten in $A$, so ist $f$ reduzibel.

LEMMA. *Ist $f \in A[x]$ und $a \in A$ mit $f(a) \equiv 0 \bmod \pi^n$, $v(f'(a)) = k$ und $2k < n$, so gibt es ein $b \in A$ mit*

$$b \equiv a \bmod \pi^{n-k}, f(b) \equiv 0 \bmod \pi^{n+1}, v(f'(b)) = k$$

*Beweis:* Wir setzen an $b = a + \pi^{n-k}c$. Dann gilt:

$$f(b) = f(a) + f'(a)\pi^{n-k}c + \pi^{2(n-k)} \cdot Rest$$

Wähle $c$ nun entsprechend. Weiter

$$f'(b) \equiv f'(a) + f''(a)\pi^{n-k}c \bmod \pi^{2(n-k)}$$

woraus auch die andere Behauptung folgt. ■

Daraus ergibt sich sofort folgender Satz

SATZ. *Sei $K$ vollständig bezüglich einer diskreten Bewertung, $f \in A[x]$ ein Polynom und $a \in A$ mit*

$$f(a) \equiv 0 \bmod \pi^n, v(f'(a)) = k, n > 2k.$$

*Dann gibt es ein $a_0 \in A$ mit $a_0 \equiv a \bmod \pi^{n-k}$, $v(f'(a_0)) = k$ und $f(a_0) = 0$.*

**Beispiel:** Wir betrachten $\mathbf{Q}_2$. Welche Elemente aus $U_1$ sind Quadrate? Sei $b \in U_1$ und $f = x^2 - b$. Ist $a$ eine approximative Nullstelle, so ist $a \in U_1$. Weiter gilt: $v(f'(a)) = 2$. Wir brauchen also $n = 3$ um das Lemma anwenden zu können, d.h. $a^2 \equiv b \bmod 8$. Hier kennen wir aber bereits die Lösung: nur die $b$ mit $b \equiv 1 \bmod 8$ sind Quadrate modulo 8. Dies gilt nun auch global. Also gilt:

$$U_1^2 = U_3 \text{ und } U_1/U_1^2 \simeq \langle -1, 5\rangle$$

Damit erhält man das Ergebnis:

$$\mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2} \simeq \langle 2, -1, 5\rangle$$

Es gibt also 7 quadratische Erweiterungen von $\mathbf{Q}_2$.

**Beispiel:** Wir wollen das Polynom $f = x^3 + x^2 - 2x + 8$ über $\mathbf{Q}_2$ betrachten. Die Ableitung ist $f' = 3x^2 + 2x - 2$. Daher gilt: für $a \equiv 0 \bmod 2$ ist $v(f'(a)) = 1$, für $a \equiv 1 \bmod 2$ ist $v(f'(a)) = 0$. Nach dem Lemma brauchen wir also nur nach Nullstellen modulo 8 zu suchen. Modulo 8 findet man als Nullstellen: $0, 1, 2, 4, 6$.

- $a = 1$ liftet zu einer Nullstelle $a_1$, mit $a_1 \equiv a \bmod 8$, d.h. $a_1 = 1 + 0 \cdot 2 + 0 \cdot 4 + \ldots$.
- $a = 0$ liftet zu einer Nullstelle $a_2$, mit $a_2 \equiv a \bmod 4$, d.h. $a_2 = 0 + 0 \cdot 2 + \ldots$.
- $a = 2$ liftet zu einer Nullstelle $a_3$, mit $a_3 \equiv a \bmod 4$, d.h. $a_2 = 0 + 1 \cdot 2 + \ldots$.
- Die anderen beiden Nullstellen führen wieder auf $a_2$ und $a_3$.

Wir wollen die Nullstellen auf 10 Stellen genau bestimmen. Dazu berechnen wir die Nullstellen modulo $2^{12}$:

$$556 = (001101000100), 1066 = (010101000010), 2473 = (100101011001),$$
$$2604 = (001101000101), 3114 = (010101000011)$$

Also sind die drei Nullstellen:

$$a_1 = (100101011001\ldots), a_2 = (00110100010\ldots), a_3 = (01010100001\ldots)$$

KAPITEL 15

# Erweiterungen diskret bewerteter Körper

Wir wollen uns jetzt endlichen Erweiterungen zuwenden. Sei also $K$ diskret bewertet mit Bewertungsring $A$ und Primelement $\pi$ und $L$ eine endliche separable Körpererweiterung von $K$. Dann ist der ganze Abschluß $B$ von $A$ in $L$ ein Dedekindring und

$$\pi B = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$$

Wir haben Bewertungen $v$ und $v_{\mathfrak{P}_i}$. Es gilt:

$$v(\pi) = 1 \text{ und } v_{\mathfrak{P}_i}(\pi) = e_i$$

Normalisieren wir $w_i = \frac{1}{e_i} v_{\mathfrak{p}_i}$ so gilt also

$$w_i(\pi) = 1 \text{ und } w_i(\mathfrak{P}_i) = \frac{1}{e_i}$$

d.h. die Einschränkung von $w_i$ auf $K$ ist $v$. Wir denken uns im folgenden alle Bewertungen so normalisiert (bei fest gegebenem Grundkörper).
Was läßt sich sagen, wenn $K$ vollständig ist. Da wir $L$ auch als $K$-Vektorraum auffassen können, definieren wir allgemeiner:

DEFINITION. Eine Norm auf einem $K$-Vektorraum $V$ ist eine Funktion $||x||$ mit den Eigenschaften:

- $||x|| \geq 0$, und $||x|| = 0 \iff x = 0$
- $||x + y|| \leq ||x|| + ||y||$
- $||\alpha x|| = |\alpha| \cdot ||x||$, für $\alpha \in K$.

SATZ. *Ist $K$ vollständig und $V$ ein endlich dimensionaler $K$-Vektorraum, so sind je zwei Normen auf $V$ äquivalent, d.h. es gibt $\alpha, beta > 0$ mit*

$$\alpha |x|_1 \leq |x|_2 \leq \beta |x|_1.$$

*Insbesondere hängt der Konvergenzbegriff nicht von der gewählten Metrik ab.*

*Beweis:*

- Sei $v_1, \dots, v_n$ eine $K$-Basis von $V$. Definiert man für $x = x_1 v_1 + \dots x_n v_n$
$$||x|| = max(|x_i|),$$
so erhält man eine Norm auf $V$. Es genügt andere Normen mit dieser zu vergleichen.
- Sei $|x|_0$ irgendeine Norm auf $V$. Dann gilt
$$|x|_0 \leq |x_1||v_1|_0 + \dots |x_n||v_n|_0 \leq \max(|v_1|_0, \dots, |v_n|_0) \cdot ||x||,$$
d.h. die eine Ungleichung ist trivial.
- Wir zeigen die andere Ungleichung durch Induktion nach der Dimension von $V$. (Die Einschränkung einer Norm auf einen Unterraum ist wieder eine Norm.)
- $n = 1$: trivial, da $|x_1 v_1|_0 = |x_1| \cdot |v_1|_0$.
- Wir nehmen an, die Behauptung gilt bereits für Vektorräume der Dimension $\leq n - 1$. Sei $V_i$ der von $v_1, \dots, \hat{v_i}, \dots, v_n$ aufgespannte Unterraum.
- Nach Induktionsvoraussetzung ist $V_i$ auch topologisch isomorph zu $K^{n-1}$, also konvergiert jede Cauchy-Folge aus $V_i$ in $V_i$. Dies impliziert, daß $V_i$ in $V$ abgeschlossen ist.
- Also sind auch die $V_i + v_i$ abgeschlossen. Daher auch $W = \cup_i (V_i + v_i)$. Wegen $0 \notin W$, gibt es ein $\rho > 0$ mit
$$\{|x|_0 \leq \rho\} \cap W = \emptyset.$$

- Sei nun $x = x_1v_1 + \cdots + x_nv_n$ gegeben und $\neq 0$. O.E. $||x|| = |x_1|$. Dann ist $x/x_1 \in W$, also $|x/x_1|_0 \geq \rho$, also
$$|x|_0 \geq \rho|x_1| = ||x||.$$
Damit folgt die Behauptung. ■

FOLGERUNG. *$V$ ist vollständig.*

*Beweis:* Dies ist klar für die Maximumsnorm. ■

Wir wenden dies jetzt an auf unsere Situation der Körpererweiterung.

SATZ. *Ist $K$ vollständig diskret bewertet und $L$ eine endliche separable Körpererweiterung von $K$, so auch $L$. Insbesondere ist der ganze Abschluß von $A$ in $L$ ein vollständiger diskreter Bewertungsring.*

*Beweis:* Wir haben die Zerlegung $(\pi) = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$ mit $r \geq 2$. Seien $w_i$ die zugehörigen Bewertungen und $||_i$ die zugehörigen Absolutbeträge. Sei $x \in \mathfrak{P}_1$. Dann ist $(x^m)_{m\in\mathbf{N}}$ eine Nullfolge bezüglich $w_1$, also auch eine Nullfolge bezüglich $w_i$, da es nur eine Konvergenz gibt. Das bedeutet aber, daß $x^m \in \mathfrak{P}_i$ ist für große $m$, also auch $x \in \mathfrak{P}_i$. Folglich: $\mathfrak{P}_1 \subseteq \mathfrak{P}_i$, was aber nur im trivialen Fall geht, d.h. $r = 1$. Damit ist $B$ ein diskreter Bewertungsring. Die Vollständigkeit folgt aus obiger Beobachtung. ■

FOLGERUNG. *Ist $K$ vollständig, so läßt sich die Bewertung eindeutig auf den separablen Abschluß $K_{sep}$ fortsetzen durch*
$$v(x) = \frac{1}{[K(x) : K]} v(N_{K(x)|K}(x)) \text{ bzw. } |x| = sqrt[[K(x) : K]]N_{K(x)|K}(x)$$

*Beweis:* Da konjugierte Elemente den gleichen Wert haben, ist die Behauptung klar. ■

FOLGERUNG. *Es gibt ein $\alpha \in L$ mit $B = A[\alpha]$.*

*Beweis:* Dies hatten wir schon früher gezeigt unter der Annahme, daß über dem Primideal unten nur ein Primideal oben liegt. Diese Bedingung ist hier erfüllt. ■

In der lokalen Situation ist nun ein Ergebnis einfach zu zeigen, das wir früher schon benötigt hatten.

SATZ. *Sei $K$ vollständig mit endlichem Restklassenkörper. $L$ und $M$ seien unverzweigte endliche separable Erweiterungen von $K$. Dann ist auch das Kompositum $LM$ unverzweigt über $K$.*

*Beweis:*

- Da $L|K$ unverzweigt ist, findet nur eine Restklassenerweiterung statt. $\alpha \in L$ erzeuge die Restklassenerweiterung und habe das Minimalpolynom $f$. Dann ist auch $L = K(\alpha)$. Sei $g$ das Minimalpolynom von $\alpha$ über $M$. Dies ist ein Teiler von $f$, also separabel. Nach dem Henselschen Lemma bleibt also $g$ auch bei Reduktion irreduzibel, d.h. auch bei $LM|M$ findet nur eine Restklassenerweiterung statt.
- Da auch $M|K$ unverzweigt ist, ist natürlich auch $LM|K$ unverzweigt. ■

Wir wollen jetzt die globale Situation mit der lokalen vergleichen.

- Sei $K$ ein diskret bewerteter Körper mit Bewertungsring $A$, $L$ eine endliche separable Erweiterung von $K$. Wir schreiben $L = K(a)$ mit Minimalpolynom $f \in K[x]$.
- Dann ist
$$\pi B = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$$
- Sei $L_{\mathfrak{P}_i}$ die Komplettierung von $L$ bezüglich $v_{\mathfrak{P}_i}$. Dann ist natürlich $K_\mathfrak{p}$ der topologische Abschluß von $K$ in $L_{\mathfrak{P}_i}$.
- Es gilt jetzt
$$\pi B_{\mathfrak{P}_i} = \mathfrak{p}_i B_{\mathfrak{P}_i}$$
Da die Restklassenkörper erhalten bleiben, gilt
$$e_i f_i = n_i = [L_{\mathfrak{P}_i} : K_\mathfrak{p}].$$

- Sei $f_i \in K_\mathfrak{p}[x]$ das Minimalpolynom von $a$ über $K_\mathfrak{p}$. Für $i \neq j$ gilt: $f_i \neq f_j$. Andernfalls gäbe es einen Isomorphismus von $L_{\mathfrak{P}_i} \to L_{\mathfrak{P}_j}$, der auf $L$ die Identität ist. Da die Bewertungen wohlbestimmt sind, müßte der Isomorphismus auch die Konvergenz erhalten. Nun argumentiert man wie früher: $b \in \mathfrak{P}_i$ liefert die Nullfolge $(b^m)$, also wäre das auch eine Nullfolge in $L_{\mathfrak{P}_j}$, also $b \in \mathfrak{P}_j$. Schließlich erhält man einen Widerspruch.
- Alle $f_i$ teilen $f$. Da alle $f_i$ teilerfremd sind, gilt jetzt aus Gradgründen:

$$f(x) = f_1(x) \dots f_r(x)$$

Dies beweist den Satz:

SATZ. *Sei $L$ eine endliche separable Erweiterung von $K$. $K$ habe den diskreten Bewertungsring $A$ und $B$ sei der ganze Abschluß von $A$ in $L$. Ist $L = K(\alpha)$ mit Minimalpolynom $f$ und ist*

$$f = f_1 \dots f_r$$

*die Faktorisierung von $f$ über $K_\pi$, ist weiter $L_i = K_\pi[x]/(f_i)$ von der Verzweigungsordnung $e_i$ und vom Restklassengrad $f_i$, so gibt es eine Zerlegung*

$$(\pi) = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}.$$

**Beispiel:** Sei $\alpha$ eine Wurzel der Gleichung $x^3 + x^2 - 2x + 8 = 0$. Wie verhält sich (2) im Zahlkörper $\mathbf{Q}(\alpha)$? Wir haben bereits gesehen, daß über $\mathbf{Q}_2$ das Polynom $x^3 + x^2 - 2x + 8$ in drei Linearfaktoren zerfällt. Also gilt in $\mathbf{Q}(\alpha)$:

$$(2) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3.$$

(Wir hatten diese Aussage früher auf komplizierterem Weg hergeleitet, und dann benutzt um zu zeigen, daß es keine Potenzganzheitsbasis gibt.)

**Bemerkung:** Man kann auch zeigen, daß Diskriminante und Resultante lokale Begriffe sind, d.h. man kann sie lokal berechnen und dann global zusammensetzen.

**Das Newton-Polygon:** Sei $K$ vollständig diskret bewertet und die Bewertung fortgesetzt auf den algebraischen Abschluß von $K$. Zu einem Polynom

$$f = a_0 + a_1 x + \dots + a_n x^n$$

mit $a_0 a_n \neq 0$ definieren wir das Newton-Polygon wie folgt: Die konvexe Hülle von

$$\{(0, v(a_0)), (1, v(a_1)), \dots, (n, v(a_n))\}$$

wird von einem Polygon berandet, das wir das Newton-Polygon nennen. Das Polygon besteht aus einer Folge von Strecken mit streng monoton wachsenden Steigungen.
Dann gilt der Satz:

SATZ. *Ist $(r, v(a_r)) \to (s, v(a_s))$ eine Strecke des Newton-Polygons mit Steigung $-m$, so besitzt $f$ genau $s - r$ Wurzeln mit Wert $m$.*

KAPITEL 16

# Ausblick auf analytische Methoden

**Motivation:** (Existenz von unendlich vielen Primzahlen nach Euler) Für jede Primzahl $p$ hat man

$$\sum_{i\geq 0} \frac{1}{p^i} = \frac{1}{1-\frac{1}{p}}.$$

Gäbe es nur endlich viele Primzahlen, so erhielte man aus der eindeutigen Primfaktorzerlegung sofort

$$\prod_p \frac{1}{1-\frac{1}{p}} = \sum_{n=1}^{\infty} \frac{1}{n}$$

was der Divergenz der harmonischen Reihe widersprechen würde. Also gibt es unendlich viele Primzahlen.

DEFINITION. Für einen Zahlkörper $K$ heißt

$$\zeta_K(s) = \sum_{\mathfrak{a} \text{ ganz}} \frac{1}{N_{K|\mathbf{Q}}\mathfrak{a}}$$

die (Dedekindsche) Zeta-Funktion von $K$.

Für $K = \mathbf{Q}$ ergibt sich die Riemannsche Zeta-Funktion. Ohne Beweis geben wir ein paar Eigenschaften an:

**Eigenschaften:**

- Obige Reihe für $\zeta_K(s)$ konvergiert für $Re(s) > 1$. Dort gilt wegen der eindeutigen Primidealzerlegung
$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1-\frac{1}{N\mathfrak{p}^s}}$$
- $\zeta_K$ läßt sich meromorph auf ganz $\mathbf{C}$ fortsetzen.
- Nur in $s = 1$ hat $\zeta_K$ einen Pol, und zwar von ersten Ordnung mit Residuum
$$\frac{2^{r_1}(2\pi)^{r_2} h_K R}{w\sqrt{|D_K|}},$$
wo $w$ die Anzahl der in $K$ enthaltenen Einheitswurzeln, $R$ den Regulator bezeichnet.
- Setzt man
$$\Phi(s) = \left(\frac{\sqrt{|D_K|}}{2^{r_2}\pi^{n/2}}\right)^s \Gamma(\frac{s}{2})^{r_1}\Gamma(s)^{r_2}\zeta_K(s),$$
so gilt die Funktionalgleichung
$$\Phi(s) = \Phi(1-s)$$
- Aus der Funktionalgleichung sieht man, daß $\zeta_K$ in den negativen ganzen Zahlen bzw. den negativen geraden ganzen Zahlen Nullstellen hat. Diese werden triviale Nullstellen von $\zeta_K$ genannt. Die große Riemannsche Vermutung (GRH) lautet: Die nichttrivialen Nullstellen von $\zeta_K$ liegen auf der Geraden $Re(s) = \frac{1}{2}$.

Mit analytischen Methoden und der Klassenkörpertheorie kann man nachfolgenden Dichtigkeitssatz von Čebotarev herleiten. (Effektive Versionen finden sich bei Serre.)

- Sei $K$ ein Zahlkörper, galoissch über $\mathbf{Q}$ mit Gruppe $G$.

- Ist $p$ eine Primzahl, die nicht die Diskriminante $D_K$ teilt, so gibt es eine Zerlegung
$$(p) = \mathfrak{p}_1 \dots \mathfrak{p}_r$$
- Die Restklassenerweiterung $\mathfrak{o}/\mathfrak{p}_i$ über $\mathbf{Z}/(p)$ ist galoissch, und die Galoisgruppe wird von dem Frobeniusautomorphismus erzeugt. Die Galoisgruppe ist isomorph zur Zerlegungsgruppe $G_{\mathfrak{p}_i}$. Also gibt es ein wohlbestimmtes $\sigma_{\mathfrak{p}_i} \in G$ mit
$$\sigma_{\mathfrak{p}_i} x \equiv x^p \bmod \mathfrak{p}_i$$
Daraus sieht man sofort
$$\tau\sigma_{\mathfrak{p}_i}\tau^{-1} x \equiv x^p \bmod \tau\mathfrak{p}_i$$
d.h.
$$\tau\sigma_{\mathfrak{p}_i}\tau^{-1} = \sigma_{\tau\mathfrak{p}_i}$$
- Die $\sigma_{\mathfrak{p}_1}, \dots, \sigma_{\mathfrak{p}_r}$ bilden also eine Konjugationsklasse in $G$. Sie werde mit $[\sigma_p]$ bezeichnet.

Dann gilt der Čebortarevsche Dichtigkeitssatz:

SATZ. *Ist $K$ ein über $\mathbf{Q}$ galoisscher Zahlkörper mit Gruppe $G$ und $C$ eine Konjugationsklasse in $G$, so gilt:*
$$\lim_{x\to\infty} \frac{\#\{p \le x : [\sigma_p] = C\}}{\#\{p \le x\}} = \frac{|C|}{|G|}.$$

**Beispiel:** $K = \mathbf{Q}(\alpha)$, wo $\alpha$ Nullstelle des Polynoms $f = x^3 - 3x - 1$ ist, ist galoissch über $\mathbf{Q}$ mit zyklischer Galoisgruppe $G = \{1, \sigma, \sigma^2\}$. Die Konjugationsklassen in $G$ sind einelementig. $\sigma_p = 1$ bedeutet, daß keine Restklassenerweiterung stattfindet, d.h. $f$ zerfällt modulo $p$ in drei Linearfaktoren. $\sigma_p = \sigma$ oder $\sigma_p = \sigma^2$ bedeutet, daß $p$ träge bleibt, d.h. $f$ ist modulo $p$ irreduzibel. Damit liefert obiger Satz
$$\lim_{x\to\infty} \frac{\#\{p \le x : f \text{ zerfällt in drei Linearfaktoren modulo } p\}}{\#\{p \le x\}} = \frac{1}{3}$$
$$\lim_{x\to\infty} \frac{\#\{p \le x : f \text{ ist irreduzibel modulo } p\}}{\#\{p \le x\}} = \frac{2}{3}$$
Das hatten wir bereits früher aufgrund einer kleinen Statistik vermutet.

**Beispiel:** Sei $K = \mathbf{Q}(\zeta_n)$. Die Galoisgruppe ist $G = (\mathbf{Z}/(n))^\times$. Das Element $a \in \mathbf{Z}_n^\times$ liefert den Automorphismus $\zeta \mapsto \zeta^a$. Also bedeutet $\sigma_p = a$ einfach $\zeta^p = \zeta^a$, d.h. $p \equiv a \bmod n$. Also liefert unser Satz für $a \in \mathbf{Z}/(n)^\times$:
$$\lim_{x\to\infty} \frac{\#\{p \le x : p \equiv a \bmod n\}}{\#\{p \le x\}} = \frac{1}{\varphi(n)},$$
die Primzahlen sind auf die zu $n$ primen Restklassen also gleichmäßig verteilt, was insbesondere den Dirichletschen Primzahlsatz impliziert: Sind $a$ und $n$ teilerfremd, so gibt es unendlich viele Primzahlen $p$ mit $p \equiv a \bmod n$.

**Beispiel:** Die galoissche Hülle von $K = \mathbf{Q}(\sqrt[3]{2})$ ist $L = \mathbf{Q}(\sqrt[3]{2}, \zeta_3)$ mit der Galoisgruppe
$$S_3 = \{(1), (12), (13), (23), (123), (132)\}$$
mit den Konjugationsklassen
$$C_1 = \{(1)\}, C_2 = \{(12), (13), (23)\}, C_3 = \{(123), (132)\}.$$
- $[\sigma_p] = C_1$ bedeutet, daß $p$ voll zerfällt, insbesondere zerfällt $f$ modulo $p$ in drei Linearfaktoren.
- $[\sigma_p] = C_2$ bedeutet, daß $p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ in $L$, in $K$ zerfällt $p$ also in ein Primideal vom Grad 1 und ein Primideal vom Grad 2, d.h. $f$ modulo $p$ spaltet in einen Linearfaktor und einen quadratischen Faktor.
- $[\sigma_p] = C_3$ bedeutet, daß $p$ in 2 Primideale in $L$ zerfällt mit Zerlegungskörper $\mathbf{Q}(\zeta_3)$. Insbesondere bleibt $p$ träge in $K$, d.h. $f$ bleibt modulo $p$ irreduzibel.

Der Čebotarevsche Dichtigkeitssatz liefert also für das Zerfallsverhalten von $f$ modulo $p$:
- $f$ zerfällt in drei Linearfaktoren: $1/6$
- $f$ zerfällt in einen Linearfaktoren und einen irreduziblen quadratischen Faktor: $1/2$
- $f$ bleibt irreduzibel: $1/2$.

Auch diese Verteilung hatten wir bereits früher vermutet aufgrund einer statistischen Untersuchung.

ANHANG A

# Zusammenschau

**Globale Theorie.**

- Ganzheitsringe
- Dedekindringe
- Geometrie der Zahlen
- Endlichkeit der Klassenzahl
- Dirichletscher Einheitensatz

**Lokale Theorie.**

- Verzweigung
- Lokalisierung
- Komplettierung

**Spezielle Körper.**

- Quadratische Zahlkörper
- Kreisteilungskörper

**Abelsche Erweiterungen.**

- Der Satz von Kronecker-Weber
- Klassenkörpertheorie

**Analytische Methoden.**

- Zetafunktionen, mit analytischer Fortsetzung auf $\mathbf{C}$ ohne 1
- Dirichletscher Primzahlsatz
- Čebotarev (Neukirch, S. 569)

# Literaturverzeichnis


[1897] Hilbert, D., Die Theorie der algebraischen Zahlkörper.

[1963] Eichler, M., Einführung in die Theorie der algebraischen Zahlen und Funktionen.

[1963] Weiss, E., Algebraic Number Theory, McGraw-Hill Book Company, Inc., New York - San Francisco - Toronto - London.

[1966] Borewicz, S. I., Safarevic, I. R., Zahlentheorie.

[1967] Cassels, J. W. S., Fröhlich, A., Algebraic Number Theory.

[1970] Lang, S., Algebraic Number Theory.

[1974] Weil, A., Basic Number Theory.

[1977] Marcus, D. A., Number Fields.

[1978] Cohn, H., A Classical Invitation to Algebraic Numbers and Class Fields.

[1979] Serre, J.-P., Local Fields.

[1980] Hasse, H., Number Theory.

[1990] Narkiewicz, W., Elementary and Analytic Theory of Algebraic Numbers, second edition, Springer-Verlag, PWN-Polish Scientific Publishers, Warszawa.

[1991] Fröhlich, A., Taylor, M. J., Algebraic number theory, Cambridge Studies in Advanced Mathematics 27, Cambridge University Press.

[1992] Neukirch, J., Algebraische Zahlentheorie.

[1992] Koch, H., Algebraic Number Fields.