

# Kapitel I

## Ganze algebraische Zahlen

### § 1. Die Gaußschen Zahlen

Die Gleichungen

$$2 = 1+1, \quad 5 = 1+4, \quad 13 = 4+9, \quad 17 = 1+16, \quad 29 = 4+25, \quad 37 = 1+36$$

zeigen die ersten Primzahlen, die sich als eine Summe von zwei Quadratzahlen darstellen lassen. Von der 2 abgesehen sind sie alle  $\equiv 1 \pmod{4}$ , und für eine ungerade Primzahl der Form  $p = a^2 + b^2$  gilt ganz allgemein  $p \equiv 1 \pmod{4}$ , weil Quadratzahlen entweder  $\equiv 0$  oder  $\equiv 1 \pmod{4}$  sind. Dies liegt auf der Hand; keineswegs aber die bemerkenswerte Tatsache, daß sich die Aussage umkehren läßt:

**(1.1) Satz.** Für die Primzahlen  $p \neq 2$  gilt

$$p = a^2 + b^2 \quad (a, b \in \mathbb{Z}) \quad \Longleftrightarrow \quad p \equiv 1 \pmod{4}.$$

Diese Gesetzmäßigkeit im Ring  $\mathbb{Z}$  der ganzen rationalen Zahlen findet ihre natürliche Erklärung im erweiterten Bereich der **Gaußschen Zahlen**

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}, \quad i = \sqrt{-1}.$$

In diesem Ring verwandelt sich die Gleichung  $p = x^2 + y^2$  in die Produktzerlegung

$$p = (x + iy)(x - iy),$$

wodurch sich das Problem stellt, wann und wie eine Primzahl  $p \in \mathbb{Z}$  in  $\mathbb{Z}[i]$  in Faktoren zerfällt. Die Antwort auf diese Frage gründet sich auf den folgenden Satz von der eindeutigen Primzerlegung in  $\mathbb{Z}[i]$ .

**(1.2) Satz.** Der Ring  $\mathbb{Z}[i]$  ist euklidisch, insbesondere also faktoriell.

**Beweis:** Wir zeigen, daß  $\mathbb{Z}[i]$  euklidisch ist bzgl. der Funktion  $\mathbb{Z}[i] \rightarrow \mathbb{N} \cup \{0\}$ ,  $\alpha \mapsto |\alpha|^2$ . Sind  $\alpha, \beta \in \mathbb{Z}[i]$ ,  $\beta \neq 0$ , so ist die Existenz von Gaußschen Zahlen  $\gamma, \rho$  nachzuweisen mit

$$\alpha = \gamma\beta + \rho \quad \text{und} \quad |\rho|^2 < |\beta|^2.$$

Es genügt offenbar, ein  $\gamma \in \mathbb{Z}[i]$  zu finden mit  $|\frac{\alpha}{\beta} - \gamma| < 1$ . Die Gaußschen Zahlen bilden nun ein **Gitter** in der komplexen Zahlenebene  $\mathbb{C}$  (Punkte mit ganzzahligen Koordinaten bzgl. der Basis  $1, i$ ). Die komplexe Zahl  $\frac{\alpha}{\beta}$  liegt in einer Masche des Gitters und hat vom nächsten Gitterpunkt einen Abstand, der nicht größer ist, als die halbe Länge  $\frac{\sqrt{2}}{2}$  der Diagonalen der Masche. Daher gibt es ein  $\gamma \in \mathbb{Z}[i]$  mit  $|\frac{\alpha}{\beta} - \gamma| \leq \frac{\sqrt{2}}{2} < 1$ .  $\square$

Aufgrund dieses Satzes über den Ring  $\mathbb{Z}[i]$  ergibt sich der Satz (1.1) folgendermaßen. Es genügt zu zeigen, daß eine Primzahl  $p \equiv 1 \pmod{4}$  von  $\mathbb{Z}$  im Ring  $\mathbb{Z}[i]$  kein Primelement bleibt. In der Tat, ist dies bewiesen, so existiert eine Zerlegung

$$p = \alpha \cdot \beta$$

in zwei Nicht-Einheiten  $\alpha, \beta$  von  $\mathbb{Z}[i]$ . Die **Norm** von  $z = x + iy$  ist durch

$$N(x + iy) = (x + iy)(x - iy) = x^2 + y^2$$

gegeben, also durch  $N(z) = |z|^2$ . Sie ist multiplikativ, so daß

$$p^2 = N(\alpha) \cdot N(\beta).$$

Da  $\alpha$  und  $\beta$  keine Einheiten sind, so ist  $N(\alpha), N(\beta) \neq 1$  (Aufgabe 1), d.h.  $p = N(\alpha) = a^2 + b^2$ , wenn  $\alpha = a + bi$  gesetzt ist.

Um nun zu zeigen, daß eine Primzahl der Form  $p = 1 + 4n$  kein Primelement in  $\mathbb{Z}[i]$  sein kann, bemerken wir, daß die Kongruenz

$$-1 \equiv x^2 \pmod{p}$$

eine Lösung besitzt, nämlich  $x = (2n)!$ . In der Tat, wegen  $-1 \equiv (p-1)! \pmod{p}$  (Satz von Wilson) ist

$$\begin{aligned} -1 &\equiv (p-1)! = [1 \cdot 2 \cdots (2n)][(p-1)(p-2) \cdots (p-2n)] \\ &\equiv [(2n)!][(-1)^{2n}(2n)!] = [(2n)!]^2 \pmod{p}. \end{aligned}$$

Wir erhalten somit  $p \mid x^2 + 1 = (x+i)(x-i)$ . Wegen  $\frac{x}{p} \pm \frac{i}{p} \notin \mathbb{Z}[i]$  teilt  $p$  jedoch keinen der Faktoren  $x+i, x-i$  und ist daher kein Primelement im faktoriellen Ring  $\mathbb{Z}[i]$ .

Das Beispiel der Gleichung  $p = x^2 + y^2$  zeigt, daß man schon durch sehr elementare Fragen aus dem Bereich der ganzen rationalen Zahlen

auf die Betrachtung höherer Bereiche von ganzen Zahlen geführt wird. Aber nicht so sehr wegen dieser Gleichung, sondern um der allgemeinen Theorie der ganzen algebraischen Zahlen ein greifbares Beispiel voranzuschicken, haben wir den Ring  $\mathbb{Z}[i]$  eingeführt und wollen aus diesem Grund genauer auf ihn eingehen.

Im Vordergrund der Teilbarkeitslehre in einem Ring stehen zwei grundsätzliche Probleme: Die Bestimmung der **Einheiten** des Ringes einerseits und die seiner **Primelemente** andererseits. Die Antwort auf die erste Frage ist im vorliegenden Fall denkbar einfach. Eine Zahl  $\alpha = a + bi \in \mathbb{Z}[i]$  ist genau dann eine Einheit, wenn

$$N(\alpha) := (a + ib)(a - ib) = a^2 + b^2 = 1$$

ist (Aufgabe 1), d.h. wenn entweder  $a^2 = 1, b^2 = 0$  oder  $a^2 = 0, b^2 = 1$  ist. Wir erhalten daher den

**(1.3) Satz.** *Die Gruppe der Einheiten des Ringes  $\mathbb{Z}[i]$  besteht aus den vierten Einheitswurzeln,*

$$\mathbb{Z}[i]^* = \{1, -1, i, -i\}.$$

Um die Frage nach den Primelementen, d.h. irreduziblen Elementen des Ringes  $\mathbb{Z}[i]$  zu beantworten, erinnern wir daran, daß zwei Elemente  $\alpha, \beta$  in einem Ring **assoziiert** heißen, in Zeichen  $\alpha \sim \beta$ , wenn sie sich nur um einen Einheitenfaktor unterscheiden, und daß mit einem irreduziblen Element  $\pi$  auch jedes Assoziierte irreduzibel ist. Mit Hilfe des Satzes (1.1) erhalten wir den folgenden genauen Überblick über die Primzahlen von  $\mathbb{Z}[i]$ .

**(1.4) Satz.** *Die Primelemente  $\pi$  von  $\mathbb{Z}[i]$  sind bis auf Assoziierte wie folgt gegeben:*

- (1)  $\pi = 1 + i,$
- (2)  $\pi = a + bi$  mit  $a^2 + b^2 = p, p \equiv 1 \pmod{4}, a > |b| > 0,$
- (3)  $\pi = p,$   $p \equiv 3 \pmod{4}.$

Dabei bedeutet  $p$  eine Primzahl von  $\mathbb{Z}$ .

**Beweis:** Die Zahlen unter (1) und (2) sind prim, weil aus einer Zerlegung  $\pi = \alpha \cdot \beta$  in  $\mathbb{Z}[i]$  die Gleichung

$$p = N(\pi) = N(\alpha) \cdot N(\beta)$$

mit einer Primzahl  $p$  folgt, so daß entweder  $N(\alpha) = 1$  oder  $N(\beta) = 1$ , also entweder  $\alpha$  oder  $\beta$  eine Einheit ist. Die Zahlen  $\pi = p$ ,  $p \equiv 3 \pmod{4}$ , sind prim in  $\mathbb{Z}[i]$ , weil eine Zerlegung  $p = \alpha \cdot \beta$  in Nicht-Einheiten  $\alpha, \beta$  zur Folge hätte, daß  $p^2 = N(\alpha) \cdot N(\beta)$  ist, d.h.  $p = N(\alpha) = N(a + bi) = a^2 + b^2$ , woraus sich nach (1.1)  $p \equiv 1 \pmod{4}$  ergäbe.

Nach dieser Feststellung haben wir zu zeigen, daß ein beliebiges Primelement  $\pi$  von  $\mathbb{Z}[i]$  assoziiert ist zu einem der Genannten. Zunächst folgt aus

$$N(\pi) = \pi \cdot \bar{\pi} = p_1 \cdot \dots \cdot p_r,$$

$p_i$  Primzahl in  $\mathbb{Z}$ , daß  $\pi|p$  für ein  $p = p_i$ , also  $N(\pi)|N(p) = p^2$ , d.h. entweder  $N(\pi) = p$  oder  $N(\pi) = p^2$ . Im Falle  $N(\pi) = p$  ist  $\pi = a + bi$  mit  $a^2 + b^2 = p$ , d.h.  $\pi$  ist vom Typ (2) oder, wenn  $p = 2$  ist, assoziiert zu  $1 + i$ . Ist aber  $N(\pi) = p^2$ , so ist  $\pi$  zu  $p$  assoziiert, weil  $p/\pi$  wegen  $N(p/\pi) = 1$  eine Einheit ist. Es muß überdies  $p \equiv 3 \pmod{4}$  gelten, weil sonst  $p = 2$  oder  $p \equiv 1 \pmod{4}$  und nach (1.1)  $p = a^2 + b^2 = (a + bi)(a - bi)$  nicht prim wäre. Damit ist alles gezeigt.  $\square$

Mit diesem Satz ist auch die Frage nach der Zerlegung der Primzahlen  $p \in \mathbb{Z}$  in  $\mathbb{Z}[i]$  vollständig geklärt. Die Primzahl  $2 = (1 + i)(1 - i)$  ist wegen  $1 - i = -i(1 + i)$  assoziiert zum Quadrat des Primelements  $1 + i$ ,  $2 \sim (1 + i)^2$ , die Primzahlen  $p \equiv 1 \pmod{4}$  zerfallen in zwei konjugierte prime Faktoren

$$p = (a + bi)(a - bi),$$

und die Primzahlen  $p \equiv 3 \pmod{4}$  bleiben prim.

Die Gaußschen Zahlen spielen im Körper

$$\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$$

die gleiche Rolle wie die ganzen rationalen Zahlen im Körper  $\mathbb{Q}$ , sind also als die „ganzen Zahlen“ von  $\mathbb{Q}(i)$  anzusehen. Dieser Ganzheitsbegriff bezieht sich auf die Koordinaten zur Basis  $1, i$ . Wir haben jedoch die folgende, von dieser Basiswahl unabhängige Charakterisierung der Gaußschen Zahlen:

**(1.5) Satz.**  $\mathbb{Z}[i]$  besteht aus genau denjenigen Zahlen der Körpererweiterung  $\mathbb{Q}(i)|\mathbb{Q}$ , die einer normierten Gleichung

$$x^2 + ax + b = 0$$

mit Koeffizienten  $a, b \in \mathbb{Z}$  genügen.

**Beweis:** Ein Element  $\alpha = c + id \in \mathbb{Q}(i)$  ist Nullstelle des Polynoms

$$x^2 + ax + b \in \mathbb{Q}[x] \quad \text{mit} \quad a = -2c, \quad b = c^2 + d^2.$$

Sind  $c$  und  $d$  ganz, so auch  $a$  und  $b$ . Sind umgekehrt  $a$  und  $b$  ganz, so auch  $2c$  und  $2d$ . Wegen  $(2c)^2 + (2d)^2 = 4b \equiv 0 \pmod{4}$  folgt  $(2c)^2 \equiv (2d)^2 \equiv 0 \pmod{4}$ , weil Quadratzahlen nur  $\equiv 0$  oder  $\equiv 1 \pmod{4}$  sein können, und damit die Ganzheit von  $c$  und  $d$ .  $\square$

Der letzte Satz führt uns auf die allgemeine Definition einer ganzen algebraischen Zahl als einer Zahl, die einer normierten algebraischen Gleichung mit ganzrationalen Koeffizienten genügt. Für den Bereich der Gaußschen Zahlen haben wir in diesem Paragraphen eine vollständige Antwort auf die Frage nach den Einheiten, auf die Frage nach den Primelementen und auf die Frage nach der eindeutigen Primzerlegung erhalten.

Mit diesen Fragen sind gleichzeitig die grundlegenden Probleme der allgemeinen Theorie der ganzen algebraischen Zahlen angesprochen. Die im Falle  $\mathbb{Z}[i]$  gefundenen Antworten sind jedoch nicht exemplarisch; es treten an ihre Stelle ganz neuartige Entdeckungen.

**Aufgabe 1.**  $\alpha \in \mathbb{Z}[i]$  ist genau dann eine Einheit, wenn  $N(\alpha) = 1$ .

**Aufgabe 2.** Zeige, daß im Ring  $\mathbb{Z}[i]$  aus  $\alpha\beta = \varepsilon\gamma^n$  mit teilerfremden Zahlen  $\alpha, \beta$  und einer Einheit  $\varepsilon$  stets  $\alpha = \varepsilon'\xi^n$  und  $\beta = \varepsilon''\eta^n$  mit Einheiten  $\varepsilon', \varepsilon''$  folgt.

**Aufgabe 3.** Zeige, daß die ganzzahligen Lösungen der Gleichung

$$x^2 + y^2 = z^2$$

mit  $x, y, z > 0$  und  $(x, y, z) = 1$  („Pythagoräische Tripel“) durch

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

gegeben sind, mit  $u, v \in \mathbb{Z}$ ,  $u > v > 0$ ,  $(u, v) = 1$ ,  $u, v$  nicht beide ungerade, und durch die Tripel, die man hieraus durch Vertauschung von  $x$  und  $y$  erhält.

**Hinweis:** Zeige mit Hilfe von Aufgabe 2, daß  $x + iy = \varepsilon\alpha^2$  mit einer Einheit  $\varepsilon$  und einem  $\alpha = u + iv \in \mathbb{Z}[i]$  gelten muß.

**Aufgabe 4.** Zeige, daß sich der Ring  $\mathbb{Z}[i]$  nicht anordnen läßt.

**Aufgabe 5.** Zeige, daß der Ring  $\mathbb{Z}[\sqrt{-d}] = \mathbb{Z} + \mathbb{Z}\sqrt{-d}$  für eine ganze Zahl  $d > 1$  nur die Einheiten  $\pm 1$  besitzt.

**Aufgabe 6.** Zeige, daß der Ring  $\mathbb{Z}[\sqrt{d}] = \mathbb{Z} + \mathbb{Z}\sqrt{d}$  für quadratfreies  $d > 1$  unendlich viele Einheiten hat.

**Aufgabe 7.** Zeige, daß der Ring  $\mathbb{Z}[\sqrt{2}] = \mathbb{Z} + \mathbb{Z}\sqrt{2}$  euklidisch ist. Zeige ferner, daß seine Einheiten durch  $\pm(1 + \sqrt{2})^n$ ,  $n \in \mathbb{Z}$ , gegeben sind, und bestimme seine Primelemente.

## § 2. Ganzheit

Ein **algebraischer Zahlkörper** ist eine endliche Körpererweiterung  $K$  von  $\mathbb{Q}$ . Die Elemente von  $K$  heißen **algebraische Zahlen**. Eine algebraische Zahl heißt **ganz**, wenn sie Nullstelle eines normierten Polynoms  $f(x) \in \mathbb{Z}[x]$  ist. Dieser Ganzheitsbegriff betrifft aber nicht nur die algebraischen Zahlen. Er tritt in vielen verschiedenen Zusammenhängen auf und muß daher in voller Allgemeinheit behandelt werden.

Wenn im folgenden von Ringen die Rede ist, so sind damit stets kommutative Ringe mit Einselement gemeint.

**(2.1) Definition.** Sei  $A \subseteq B$  eine Ringerweiterung. Ein Element  $b \in B$  heißt **ganz** über  $A$ , wenn es einer normierten Gleichung

$$x^n + a_1x^{n-1} + \cdots + a_n = 0, \quad n \geq 1,$$

mit Koeffizienten  $a_i \in A$  genügt. Der Ring  $B$  heißt **ganz** über  $A$ , wenn alle Elemente  $b \in B$  ganz über  $A$  sind.

Die wünschenswerte Tatsache, daß mit zwei über  $A$  ganzen Elementen von  $B$  auch ihre Summe und ihr Produkt ganz sind, fällt seltsamerweise nicht vom Himmel. Sie ergibt sich aber durch die folgende abstrakte Umdeutung des Ganzheitsbegriffs.

**(2.2) Satz.** Endlich viele Elemente  $b_1, \dots, b_n \in B$  sind genau dann sämtlich ganz über  $A$ , wenn der Ring  $A[b_1, \dots, b_n]$ , aufgefaßt als  $A$ -Modul, endlich erzeugt ist.

Zum Beweis benützen wir aus der linearen Algebra den

**(2.3) Laplaceschen Entwicklungssatz.** Sei  $A = (a_{ij})$  eine  $(r \times r)$ -Matrix über einem beliebigen Ring und  $A^* = (a_{ij}^*)$  die adjungierte Matrix, d.h.  $a_{ij}^* = (-1)^{i+j} \det(A_{ij})$ , wobei die Matrix  $A_{ij}$  aus  $A$  durch Herausstreichen der  $i$ -ten Spalte und  $j$ -ten Zeile entsteht. Dann gilt

$$AA^* = A^*A = \det(A)E,$$

wobei  $E$  die Einheitsmatrix vom Grade  $r$  ist. Für einen Vektor  $x = (x_1, \dots, x_r)$  folgt die Implikation

$$Ax = 0 \implies (\det A)x = 0.$$

**Beweis zu (2.2):** Sei  $b \in B$  ganz über  $A$  und  $f(x) \in A[x]$  ein normiertes Polynom vom Grade  $n \geq 1$  mit  $f(b) = 0$ . Für ein beliebiges Polynom  $g(x) \in A[x]$  können wir dann

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

schreiben mit  $q(x), r(x) \in A[x]$  und  $\text{Grad}(r(x)) < n$ , so daß

$$g(b) = r(b) = a_0 + a_1b + \dots + a_{n-1}b^{n-1}$$

gilt. Daher wird  $A[b]$  als  $A$ -Modul durch  $1, b, \dots, b^{n-1}$  erzeugt.

Sind allgemeiner  $b_1, \dots, b_n \in B$  ganz über  $A$ , so folgt die Endlichkeit von  $A[b_1, \dots, b_n]$  über  $A$  mit vollständiger Induktion über  $n$ . Da nämlich  $b_n$  ganz über  $R = A[b_1, \dots, b_{n-1}]$  ist, so ist nach dem soeben Gezeigten  $R[b_n] = A[b_1, \dots, b_n]$  endlich erzeugt über  $R$ , also auch über  $A$ , wenn wir induktiv annehmen, daß  $R$  ein endlich erzeugter  $A$ -Modul ist.

Sei umgekehrt der  $A$ -Modul  $A[b_1, \dots, b_n]$  endlich erzeugt und  $\omega_1, \dots, \omega_r$  ein Erzeugendensystem. Für ein beliebiges Element  $b \in A[b_1, \dots, b_n]$  ist dann

$$b \omega_i = \sum_{j=1}^r a_{ij} \omega_j, \quad i = 1, \dots, r, \quad a_{ij} \in A.$$

Aus (2.3) folgt  $\det(bE - (a_{ij}))\omega_i = 0$ ,  $i = 1, \dots, r$  ( $E$  Einheitsmatrix vom Grade  $r$ ), und da  $1$  eine Darstellung  $1 = c_1\omega_1 + \dots + c_r\omega_r$  hat, erhalten wir in  $\det(bE - (a_{ij})) = 0$  eine normierte Gleichung für  $b$  mit Koeffizienten in  $A$ . Sie zeigt, daß  $b$  ganz ist über  $A$ .  $\square$

Nach diesem Satz ist mit  $b_1, \dots, b_n \in B$  jedes Element  $b$  aus  $A[b_1, \dots, b_n]$  ganz über  $A$ , weil  $A[b_1, \dots, b_n, b] = A[b_1, \dots, b_n]$  ein endlich erzeugter  $A$ -Modul ist. Insbesondere ist mit zwei Elementen  $b_1, b_2 \in B$  auch  $b_1 + b_2$  und  $b_1b_2$  ganz über  $A$ . Es folgt überdies der

**(2.4) Satz.** Seien  $A \subseteq B \subseteq C$  zwei Ringerweiterungen. Ist  $C$  ganz über  $B$  und  $B$  ganz über  $A$ , so ist  $C$  ganz über  $A$ .

**Beweis:** Sei  $c \in C$  und  $c^n + b_1c^{n-1} + \dots + b_n = 0$  eine Gleichung mit Koeffizienten in  $B$  und sei  $R = A[b_1, \dots, b_n]$ . Dann ist  $R[c]$  ein endlich

erzeugter  $R$ -Modul. Ist  $B$  ganz über  $A$ , so ist  $R[c]$  sogar endlich erzeugt über  $A$ , da  $R$  endlich erzeugt über  $A$  ist. Daher ist  $c$  ganz über  $A$ .  $\square$

Die Gesamtheit der ganzen Elemente

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

in einer Ringerweiterung  $A \subseteq B$  bildet nach dem oben Bewiesenen einen Ring. Dieser heißt der **ganze Abschluß** von  $A$  in  $B$ . Man nennt  $A$  **ganzabgeschlossen** in  $B$ , wenn  $A = \bar{A}$ . Aus (2.4) folgt unmittelbar, daß der ganze Abschluß  $\bar{A}$  immer ganzabgeschlossen ist in  $B$ . Ist  $A$  ein Integritätsbereich mit dem Quotientenkörper  $K$ , so nennt man den ganzen Abschluß  $\bar{A}$  von  $A$  in  $K$  die **Normalisierung** von  $A$  und sagt, daß  $A$  ganzabgeschlossen schlechthin ist, wenn  $A = \bar{A}$ . Jeder faktorielle Ring  $A$  ist z.B. ganzabgeschlossen. In der Tat, ist  $a/b \in K$  ( $a, b \in A$ ) ganz über  $A$  und ist

$$(a/b)^n + a_1(a/b)^{n-1} + \cdots + a_n = 0,$$

$a_i \in A$ , so ist

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

Jedes Primelement  $\pi$ , welches  $b$  teilt, teilt hiernach auch  $a$ . Denken wir uns  $a/b$  gekürzt, so folgt  $a/b \in A$ .

Wir wenden uns jetzt einer spezielleren Situation zu. Sei  $A$  ein ganzabgeschlossener Integritätsbereich,  $K$  sein Quotientenkörper,  $L|K$  eine endliche Körpererweiterung und  $B$  der ganze Abschluß von  $A$  in  $L$ . Nach (2.4) ist automatisch auch  $B$  ganzabgeschlossen. Jedes Element  $\beta \in L$  hat dann die Gestalt

$$\beta = \frac{b}{a}, \quad b \in B, \quad a \in A,$$

denn wenn

$$a_n \beta^n + \cdots + a_1 \beta + a_0 = 0, \quad a_i \in A, \quad a_n \neq 0,$$

so ist  $b = a_n \beta$  ganz über  $A$ , weil die Multiplikation der Gleichung mit  $a_n^{n-1}$  eine Gleichung

$$(a_n \beta)^n + \cdots + a'_1 (a_n \beta) + a'_0 = 0, \quad a'_i \in A,$$

ergibt. Die Ganzabgeschlossenheit von  $A$  bewirkt ferner, daß ein Element  $\beta \in L$  genau dann ganz ist über  $A$ , wenn sein **Minimalpolynom**  $p(x)$  Koeffizienten in  $A$  hat. In der Tat, sei  $\beta$  Nullstelle des normierten Polynoms  $g(x) \in A[x]$ . Dann ist  $p(x)$  ein Teiler von  $g(x)$  in  $K[x]$ , so



daß alle Nullstellen  $\beta_1, \dots, \beta_n$  von  $p(x)$  ganz sind über  $A$ , also auch alle Koeffizienten, d.h.  $p(x) \in A[x]$ .

Ein wichtiges Instrument für das Studium der ganzen Elemente in  $L$  ist durch die Spur und die Norm der Erweiterung  $L|K$  gegeben. Wir erinnern an ihre

**(2.5) Definition.** *Spur und Norm eines Elementes  $x \in L$  sind als die Spur und die Determinante der Transformation*

$$T_x : L \rightarrow L, \quad T_x(\alpha) = x\alpha,$$

*des  $K$ -Vektorraums  $L$  definiert:*

$$\text{Tr}_{L|K}(x) = \text{Tr}(T_x), \quad N_{L|K}(x) = \det(T_x).$$

In dem charakteristischen Polynom

$$f_x(t) = \det(tId - T_x) = t^n - a_1 t^{n-1} + \dots + (-1)^n a_n \in K[t]$$

von  $T_x$ ,  $n = [L : K]$ , finden wir Spur und Norm durch

$$a_1 = \text{Tr}_{L|K}(x) \quad \text{und} \quad a_n = N_{L|K}(x)$$

wieder. Wegen  $T_{x+y} = T_x + T_y$  und  $T_{xy} = T_x \circ T_y$  erhalten wir Homomorphismen

$$\text{Tr}_{L|K} : L \rightarrow K \quad \text{und} \quad N_{L|K} : L^* \rightarrow K^*.$$

Im Fall, daß die Erweiterung  $L|K$  separabel ist, erhält man die folgende galoistheoretische Interpretation der Spur und der Norm.

**(2.6) Satz.** *Ist  $L|K$  separabel und durchläuft  $\sigma : L \rightarrow \overline{K}$  die verschiedenen  $K$ -Einbettungen von  $L$  in einen algebraischen Abschluß  $\overline{K}$ , so gilt*

$$(i) \quad f_x(t) = \prod_{\sigma} (t - \sigma x),$$

$$(ii) \quad \text{Tr}_{L|K}(x) = \sum_{\sigma} \sigma x,$$

$$(iii) \quad N_{L|K}(x) = \prod_{\sigma} \sigma x.$$

**Beweis:** Das charakteristische Polynom  $f_x(t)$  ist eine Potenz

$$f_x(t) = p_x(t)^d, \quad d = [L : K(x)],$$

des Minimalpolynoms

$$p_x(t) = t^m + c_1 t^{m-1} + \cdots + c_m, \quad m = [K(x) : K],$$

von  $x$ . In der Tat,  $1, x, \dots, x^{m-1}$  ist eine Basis von  $K(x)|K$ , und wenn  $\alpha_1, \dots, \alpha_d$  eine Basis von  $L|K(x)$  ist, so ist

$$\alpha_1, \alpha_1 x, \dots, \alpha_1 x^{m-1}; \dots; \alpha_d, \alpha_d x, \dots, \alpha_d x^{m-1}$$

eine Basis von  $L|K$ . Die Matrix der linearen Transformation  $T_x : y \mapsto xy$  in dieser Basis ist offensichtlich kstchenweise eine Diagonalmatrix, wobei alle Kstchen gleich der Matrix

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 \\ -c_m & -c_{m-1} & -c_{m-2} & \cdots & -c_1 \end{pmatrix}$$

sind. Das zugehrige charakteristische Polynom ist, wie man leicht nachrechnet,

$$t^m + c_1 t^{m-1} + \cdots + c_m = p_x(t),$$

so da insgesamt  $f_x(t) = p_x(t)^d$ .

Die Menge  $\text{Hom}_K(L, \overline{K})$  der  $K$ -Einbettungen von  $L$  zerfllt nun unter der Relation

$$\sigma \sim \tau \iff \sigma x = \tau x$$

in  $m$  quivalenzklassen der Mchtigkeit  $d$ , und wenn  $\sigma_1, \dots, \sigma_m$  ein Reprsentantensystem ist, so ist

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

und  $f_x(t) = \prod_{i=1}^m (t - \sigma_i x)^d = \prod_{i=1}^m \prod_{\sigma \sim \sigma_i} (t - \sigma x) = \prod_{\sigma} (t - \sigma x)$ . Damit ist (i), und nach dem Vietaschen Wurzelsatz gleichzeitig (ii) und (iii) bewiesen.  $\square$

**(2.7) Korollar.** Fr einen Turm  $K \subseteq L \subseteq M$  endlicher Erweiterungen gilt

$$\text{Tr}_{L|K} \circ \text{Tr}_{M|L} = \text{Tr}_{M|K}, \quad N_{L|K} \circ N_{M|L} = N_{M|K}.$$

**Beweis:** Wir nehmen an, da  $M|K$  separabel ist. Die Menge  $\text{Hom}_K(M, \overline{K})$  der  $K$ -Einbettungen von  $M$  zerfllt unter der Relation

$$\sigma \sim \tau \iff \sigma|_L = \tau|_L$$

in  $m = [L : K]$  Äquivalenzklassen. Ist  $\sigma_1, \dots, \sigma_m$  ein Repräsentantensystem, so ist  $\text{Hom}_K(L, \bar{K}) = \{\sigma_i|_L \mid i = 1, \dots, m\}$  und

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

und gleichermaßen für die Norm.

Den inseparablen Fall werden wir nicht zu betrachten haben. Er folgt aber leicht aus dem oben Bewiesenen durch Übergang zur maximalen separablen Teilerweiterung  $M^s|K$ . Für den Inseparabilitätsgrad  $[M : K]_i = [M : M^s]$  hat man nämlich  $[M : K]_i = [M : L]_i [L : K]_i$  und

$$\text{Tr}_{M|K}(x) = [M : K]_i \text{Tr}_{M^s|K}(x), \quad N_{M|K}(x) = N_{M^s|K}(x)^{[M:K]_i}$$

(vgl. [143], vol I, Ch. II, § 10).  $\square$

Die **Diskriminante** einer Basis  $\alpha_1, \dots, \alpha_n$  der separablen Erweiterung  $L|K$  ist durch

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

gegeben, wobei  $\sigma_i, i = 1, \dots, n$ , die  $K$ -Einbettungen  $L \rightarrow \bar{K}$  durchläuft. Da die Matrix  $(\text{Tr}_{L|K}(\alpha_i \alpha_j))$  wegen

$$\text{Tr}_{L|K}(\alpha_i \alpha_j) = \sum_k (\sigma_k \alpha_i)(\sigma_k \alpha_j)$$

das Produkt der Matrizen  $(\sigma_k \alpha_i)^t$  und  $(\sigma_k \alpha_j)$  ist, so kann man auch

$$d(\alpha_1, \dots, \alpha_n) = \det(\text{Tr}_{L|K}(\alpha_i \alpha_j))$$

schreiben. In dem besonderen Fall einer Basis der Form  $1, \theta, \dots, \theta^{n-1}$  ist

$$d(1, \theta, \dots, \theta^{n-1}) = \prod_{i < j} (\theta_i - \theta_j)^2,$$

wobei  $\theta_i = \sigma_i \theta$ . Man sieht dies, indem man in der **Vandermondesehen Matrix**

$$\begin{pmatrix} 1 & \theta_1 & \theta_1^2 & \dots & \theta_1^{n-1} \\ 1 & \theta_2 & \theta_2^2 & \dots & \theta_2^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \theta_n & \theta_n^2 & \dots & \theta_n^{n-1} \end{pmatrix}$$

jede der  $(n-1)$  ersten Spalten mit  $\theta_1$  multipliziert und von der folgenden subtrahiert und so fortfährt.

**(2.8) Satz.** Ist  $L|K$  separabel und  $\alpha_1, \dots, \alpha_n$  eine Basis, so ist die Diskriminante

$$d(\alpha_1, \dots, \alpha_n) \neq 0,$$

und es ist

$$(x, y) = \text{Tr}_{L|K}(xy)$$

eine nicht-ausgeartete Bilinearform auf dem  $K$ -Vektorraum  $L$ .

**Beweis:** Wir zeigen zunächst, daß die Bilinearform  $(x, y) = \text{Tr}(xy)$  nicht-ausgeartet ist. Sei  $\theta$  ein primitives Element für  $L|K$ , d.h.  $L = K(\theta)$ . Dann ist  $1, \theta, \dots, \theta^{n-1}$  eine Basis, bezüglich der die Form  $(x, y)$  durch die Matrix  $M = (\text{Tr}_{L|K}(\theta^{i-1}\theta^{j-1}))_{i,j=1,\dots,n}$  gegeben ist. Diese ist nicht-ausgeartet, denn wenn  $\theta_i = \sigma_i\theta$  ist, so haben wir

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

Ist  $\alpha_1, \dots, \alpha_n$  eine beliebige Basis von  $L|K$ , so ist die Bilinearform  $(x, y)$  bzgl. dieser Basis durch die Matrix  $M = (\text{Tr}_{L|K}(\alpha_i\alpha_j))$  gegeben. Nach dem Obigen ist somit  $d(\alpha_1, \dots, \alpha_n) = \det(M) \neq 0$ .  $\square$

Nach diesem Rückblick auf die Körpertheorie kehren wir zurück zum ganzabgeschlossenen Integritätsbereich  $A$  mit dem Quotientenkörper  $K$  und seinem ganzen Abschluß  $B$  in der endlichen separablen Erweiterung  $L|K$ . Wenn  $x \in B$  ein ganzes Element von  $L$  ist, so sind offenbar auch alle Konjugierten  $\sigma x$  ganz. Beachtet man, daß  $A$  ganzabgeschlossen ist, d.h.  $A = B \cap K$ , so folgt aus (2.6)

$$\text{Tr}_{L|K}(x), N_{L|K}(x) \in A.$$

Überdies erhalten wir für die Einheitengruppe von  $B$  über  $A$

$$x \in B^* \iff N_{L|K}(x) \in A^*.$$

Denn wenn  $aN_{L|K}(x) = 1$  ist,  $a \in A$ , so ist  $1 = a \prod_{\sigma} \sigma x = yx$  mit einem  $y \in B$ . Die Diskriminante findet eine häufige Anwendung durch das

**(2.9) Lemma.** Sei  $\alpha_1, \dots, \alpha_n$  eine in  $B$  gelegene Basis von  $L|K$  mit der Diskriminante  $d = d(\alpha_1, \dots, \alpha_n)$ . Dann gilt

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

**Beweis:** Ist  $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n \in B$ ,  $a_j \in K$ , so bilden die  $a_j$  eine Lösung des linearen Gleichungssystems

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

und sind deshalb wegen  $\text{Tr}_{L|K}(\alpha_i\alpha) \in A$  als Quotient eines in  $A$  gelegenen Zählers und der Determinante  $\det(\text{Tr}_{L|K}(\alpha_i\alpha_j)) = d$  gegeben. Daher ist  $da_j \in A$ , also

$$d\alpha \in A\alpha_1 + \cdots + A\alpha_n. \quad \square$$

Unter einer **Ganzheitsbasis** von  $B$  über  $A$  (oder auch  $A$ -Basis von  $B$ ) versteht man ein System von Elementen  $\omega_1, \dots, \omega_n \in B$ , derart daß sich jedes  $b \in B$  in eindeutiger Weise als Linearkombination

$$b = a_1\omega_1 + \cdots + a_n\omega_n$$

mit Koeffizienten  $a_i \in A$  darstellen läßt. Da eine solche Ganzheitsbasis stets auch eine Basis von  $L|K$  ist, so ist ihre Länge  $n$  immer gleich dem Körpergrad  $[L : K]$ . Die Existenz einer Ganzheitsbasis bedeutet also, daß  $B$  ein **freier  $A$ -Modul** vom Rang  $n = [L : K]$  ist. Im allgemeinen gibt es aber keine Ganzheitsbasis. Ist jedoch  $A$  ein Hauptidealring, so hat man den weitergehenden

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

**Beweis:** Sei  $M \neq 0$  ein endlich erzeugter  $B$ -Untermodul von  $L$  und  $\alpha_1, \dots, \alpha_n$  eine Basis von  $L|K$ . Durch Multiplikation mit einem Element aus  $A$  können wir erreichen, daß sie in  $B$  liegt. Nach (2.9) ist dann  $dB \subseteq A\alpha_1 + \cdots + A\alpha_n$ . Sei  $\mu_1, \dots, \mu_r \in M$  ein Erzeugendensystem des  $B$ -Moduls  $M$ . Es gibt ein  $a \in A$  mit  $a\mu_i \in B$ ,  $i = 1, \dots, r$ , also  $aM \subseteq B$ . Damit ist

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

Nach dem Hauptsatz für die Moduln über Hauptidealringen ist mit  $M_0$  auch  $adM$ , also auch  $M$  ein freier  $A$ -Modul. Wegen

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

ist  $\text{Rang}(M) = \text{Rang}(M_0) = [L : K]$ . □

Ganzheitsbasen nachzuweisen ist i.a. ein schwieriges, aber in konkreten Situationen auch wichtiges Problem. Aus diesem Grund verdient der folgende Satz ein Interesse. Anstatt von Ganzheitsbasen des ganzen Abschlusses  $B$  von  $A$  in  $L$  sprechen wir dabei kurz von Ganzheitsbasen der Erweiterung  $L|K$ .

**(2.11) Satz.** Seien  $L|K$  und  $L'|K$  zwei galoissche Erweiterungen von den Graden  $n$  bzw.  $n'$  mit  $L \cap L' = K$ . Sei  $\omega_1, \dots, \omega_n$  bzw.  $\omega'_1, \dots, \omega'_{n'}$  eine Ganzheitsbasis von  $L|K$  bzw.  $L'|K$  mit der Diskriminante  $d$  bzw.  $d'$ . Sind dann  $d$  und  $d'$  teilerfremd im Sinne von  $xd + x'd' = 1$  für passende  $x, x' \in A$ , so ist  $\omega_i \omega'_j$  eine Ganzheitsbasis von  $LL'|K$  mit der Diskriminante  $d^{n'} d'^n$ .

**Beweis:** Wegen  $L \cap L' = K$  ist  $[LL' : K] = nn'$ , so daß die  $nn'$  Produkte  $\omega_i \omega'_j$  eine Basis von  $LL'|K$  bilden. Sei nun  $\alpha$  ein ganzes Element von  $LL'$  und

$$\alpha = \sum_{i,j} a_{ij} \omega_i \omega'_j, \quad a_{ij} \in K.$$

Wir haben zu zeigen, daß  $a_{ij} \in A$ . Sei dazu  $\beta_j = \sum_i a_{ij} \omega_i$ . Sei  $G(LL'|L') = \{\sigma_1, \dots, \sigma_n\}$  und  $G(LL'|L) = \{\sigma'_1, \dots, \sigma'_{n'}\}$ , so daß

$$G(LL'|K) = \{\sigma_k \sigma'_l \mid k = 1, \dots, n, l = 1, \dots, n'\}.$$

Setzen wir

$$T = (\sigma'_l \omega'_j), \quad a = (\sigma'_1 \alpha, \dots, \sigma'_{n'} \alpha)^t, \quad b = (\beta_1, \dots, \beta_{n'})^t,$$

so ist  $\det(T)^2 = d'$  und

$$a = Tb.$$

Sei  $T^*$  die zu  $T$  adjungierte Matrix. Dann folgt aus dem Laplaceschen Entwicklungssatz (2.3)

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

Da  $T^*$  und  $a$  aus ganzen Elementen von  $LL'$  bestehen, so besteht  $d'b$  aus ganzen Elementen  $d'\beta_j = \sum_i d'a_{ij} \omega_i$  von  $L$ , so daß  $d'a_{ij} \in A$ . Indem man die Rolle von  $(\omega_i)$  und  $(\omega'_j)$  vertauscht, sieht man auf die gleiche Weise  $da_{ij} \in A$ , so daß

$$a_{ij} = xda_{ij} + x'd'a_{ij} \in A.$$

Daher ist  $\omega_i \omega'_j$  in der Tat eine Ganzheitsbasis von  $LL'|K$ . Wir berechnen die Diskriminante  $\Delta$  dieser Ganzheitsbasis. Wegen  $G(LL'|K) = \{\sigma_k \sigma'_l \mid$

$k = 1, \dots, n, l = 1, \dots, n'\}$  ist sie das Quadrat der Determinante der  $(nn' \times nn')$ -Matrix

$$M = (\sigma_k \sigma'_l \omega_i \omega'_j) = (\sigma_k \omega_i \sigma'_l \omega'_j).$$

Diese Matrix ist wiederum eine  $(n' \times n')$ -Matrix von  $(n \times n)$ -Matrizen, an deren  $(l, j)$ -Stelle die Matrix  $Q \sigma'_l \omega'_j$  mit  $Q = (\sigma_k \omega_i)$  steht. Daher ist

$$M = \begin{pmatrix} Q & & O \\ & \ddots & \\ O & & Q \end{pmatrix} \begin{pmatrix} E \sigma'_1 \omega'_1 & \cdots & E \sigma'_{n'} \omega'_1 \\ \vdots & & \vdots \\ E \sigma'_1 \omega'_{n'} & \cdots & E \sigma'_{n'} \omega'_{n'} \end{pmatrix}$$

wobei  $E$  die  $(n \times n)$ -Einheitsmatrix ist. Man bringt die zweite Matrix durch Umindizierung in die Form der ersten und erhält

$$\Delta = \det(M)^2 = \det(Q)^{2n'} \det((\sigma'_l \omega'_j))^{2n} = d^{n'} d'^n. \quad \square$$

**Bemerkung.** Man kann dem Beweis entnehmen, daß der Satz für beliebige separable Erweiterungen (also nicht notwendig galoissche) gilt, wenn man anstelle von  $L \cap L' = K$  die lineare Disjunktheit fordert.

Die wichtigste Anwendung unserer Betrachtungen über die Ganzheit bezieht sich auf den ganzen Abschluß  $\mathcal{O}_K \subseteq K$  von  $\mathbb{Z} \subseteq \mathbb{Q}$  in einem algebraischen Zahlkörper  $K$ . Nach dem Satz (2.10) besitzt jeder endlich erzeugte  $\mathcal{O}_K$ -Untermodul  $\mathfrak{a}$  von  $K$  eine  $\mathbb{Z}$ -Basis  $\alpha_1, \dots, \alpha_n$ ,

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

Die Diskriminante

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

hängt nicht von der Wahl der  $\mathbb{Z}$ -Basis ab. Ist nämlich  $\alpha'_1, \dots, \alpha'_n$  eine andere Basis, so ist die Übergangsmatrix  $T = (a_{ij})$ ,  $\alpha'_i = \sum_j a_{ij} \alpha_j$ , mit ihrer Inversen ganzzahlig, hat also die Determinante  $\pm 1$ , so daß in der Tat

$$d(\alpha'_1, \dots, \alpha'_n) = \det(T)^2 d(\alpha_1, \dots, \alpha_n) = d(\alpha_1, \dots, \alpha_n).$$

Wir dürfen daher

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

setzen. Im besonderen Fall einer Ganzheitsbasis  $\omega_1, \dots, \omega_n$  von  $\mathcal{O}_K$  erhalten wir die **Diskriminante des Zahlkörpers**  $K$ ,

$$d_K = d(\mathcal{O}_K) = d(\omega_1, \dots, \omega_n).$$

Man hat allgemein den

**(2.12) Satz.** Sind  $\mathfrak{a} \subseteq \mathfrak{a}'$  zwei von Null verschiedene, endlich erzeugte  $\mathcal{O}_K$ -Untermodule von  $K$ , so ist der Index  $(\mathfrak{a}' : \mathfrak{a})$  endlich, und es gilt

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

Man hat nur zu zeigen, daß der Index  $(\mathfrak{a}' : \mathfrak{a})$  gleich dem Betrag der Determinante der Übergangsmatrix von einer  $\mathbb{Z}$ -Basis von  $\mathfrak{a}$  zu einer  $\mathbb{Z}$ -Basis von  $\mathfrak{a}'$  ist. Der Beweis gehört der wohlbekannten Theorie der endlich erzeugten  $\mathbb{Z}$ -Moduln an.

**Aufgabe 1.** Ist  $\frac{3+2\sqrt{6}}{1-\sqrt{6}}$  eine ganze algebraische Zahl?

**Aufgabe 2.** Zeige: Ist der Integritätsbereich  $A$  ganzabgeschlossen, so auch der Polynomring  $A[t]$ .

**Aufgabe 3.** Im Polynomring  $A = \mathbb{Q}[X, Y]$  betrachte man das Hauptideal  $\mathfrak{p} = (X^2 - Y^3)$ . Man zeige, daß  $\mathfrak{p}$  ein Primideal,  $A/\mathfrak{p}$  aber nicht ganzabgeschlossen ist.

**Aufgabe 4.** Sei  $D$  eine quadratfreie ganze Zahl  $\neq 0, 1$  und  $d$  die Diskriminante des quadratischen Zahlkörpers  $K = \mathbb{Q}(\sqrt{D})$ . Zeige, daß

$$d = D \quad , \text{ wenn } D \equiv 1 \pmod{4} ,$$

$$d = 4D \quad , \text{ wenn } D \equiv 2 \text{ oder } 3 \pmod{4} ,$$

und daß  $\{1, \sqrt{D}\}$  im zweiten Fall und  $\{1, \frac{1}{2}(1 + \sqrt{D})\}$  im ersten eine Ganzheitsbasis ist, und  $\{1, \frac{1}{2}(d + \sqrt{d})\}$  in jedem Fall.

**Aufgabe 5.** Zeige, daß  $\{1, \sqrt[3]{2}, \sqrt[3]{2}^2\}$  eine Ganzheitsbasis von  $\mathbb{Q}(\sqrt[3]{2})$  ist.

**Aufgabe 6.** Zeige, daß  $1, \theta, \frac{1}{2}(\theta + \theta^2)$  eine Ganzheitsbasis von  $\mathbb{Q}(\theta)$ ,  $\theta^3 - \theta - 4 = 0$ , ist.

**Aufgabe 7.** Die Diskriminante  $d_K$  eines Zahlkörpers  $K$  ist stets  $\equiv 0 \pmod{4}$  oder  $\equiv 1 \pmod{4}$ . (*Stickelbergerscher Diskriminantensatz*).

**Hinweis:** Die Determinante  $\det(\sigma_i \omega_j)$  einer Ganzheitsbasis  $\omega_j$  ist eine Summe von Termen, die mit einem Plus- oder Minuszeichen versehen sind. Ist  $P$  bzw.  $N$  die Summe der Terme mit Plus- bzw. Minuszeichen, so gilt  $d_K = (P - N)^2 = (P + N)^2 - 4PN$ .



### § 3. Ideale

Der Ring  $\mathcal{O}_K$  der ganzen Zahlen eines algebraischen Zahlkörpers  $K$  ist als Verallgemeinerung des Ringes  $\mathbb{Z} \subseteq \mathbb{Q}$  der Hauptgegenstand aller unserer Betrachtungen. Wie in  $\mathbb{Z}$ , so läßt sich auch in  $\mathcal{O}_K$  jede Nicht-Einheit  $\alpha \neq 0$  in ein Produkt von irreduziblen Elementen zerlegen. Denn wenn  $\alpha$  nicht selbst irreduzibel ist, so zerfällt es in ein Produkt  $\alpha = \beta\gamma$  von zwei Nicht-Einheiten, so daß nach § 2

$$1 < |N_{K|\mathbb{Q}}(\beta)| < |N_{K|\mathbb{Q}}(\alpha)|, \quad 1 < |N_{K|\mathbb{Q}}(\gamma)| < |N_{K|\mathbb{Q}}(\alpha)|$$

gilt und die Primzerlegung von  $\alpha$  mit vollständiger Induktion aus der von  $\beta$  und  $\gamma$  folgt. Anders jedoch als in den Ringen  $\mathbb{Z}$  und  $\mathbb{Z}[i]$  findet die Eindeutigkeit der Primzerlegung im allgemeinen nicht statt.

**Beispiel:** Im Körper  $K = \mathbb{Q}(\sqrt{-5})$  ist nach § 2, Aufgabe 4,  $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$  der Ring der ganzen Zahlen. In ihm läßt sich die Zahl 21 auf zwei Weisen zerlegen ,

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

Alle Faktoren sind irreduzibel in  $\mathcal{O}_K$ . Wäre nämlich etwa  $3 = \alpha\beta$ ,  $\alpha, \beta$  Nicht-Einheiten, so würde aus  $9 = N_{K|\mathbb{Q}}(\alpha)N_{K|\mathbb{Q}}(\beta)$  folgen, daß  $N_{K|\mathbb{Q}}(\alpha) = \pm 3$  ist. Die Gleichung

$$N_{K|\mathbb{Q}}(x + y\sqrt{-5}) = x^2 + 5y^2 = \pm 3$$

ist aber in  $\mathbb{Z}$  unlösbar. Ebenso zeigt man, daß 7,  $1 + 2\sqrt{-5}$ ,  $1 - 2\sqrt{-5}$  irreduzibel sind. Da die Brüche

$$\frac{1 \pm 2\sqrt{-5}}{3}, \quad \frac{1 \pm 2\sqrt{-5}}{7}$$

nicht in  $\mathcal{O}_K$  liegen, sind die Zahlen 3 und 7 nicht assoziiert zu  $1 + 2\sqrt{-5}$  oder  $1 - 2\sqrt{-5}$ . Es liegen also zwei verschiedene Primzerlegungen der Zahl 21 vor.

Die Betrachtung der Mehrdeutigkeit der Primzerlegung hat zu einem der großartigsten Ereignisse in der Geschichte der Zahlentheorie geführt, zur Entdeckung der Idealtheorie durch *EDUARD KUMMER*. Von der Erfindung der komplexen Zahlen geleitet, bestand die Kummersche Idee darin, daß es für die ganzen Zahlen in  $K$  einen erweiterten Bereich neuer „idealer Zahlen“ geben müsse, in dem sie sich **eindeutig** als Produkt „idealer Primzahlen“ darstellen würden. In dem Beispiel

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

etwa würden sich demnach die rechten Faktoren aus „idealen Primzahlen“  $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4$  zusammensetzen nach der Regel

$$3 = \mathfrak{p}_1 \mathfrak{p}_2, \quad 7 = \mathfrak{p}_3 \mathfrak{p}_4, \quad 1 + 2\sqrt{-5} = \mathfrak{p}_1 \mathfrak{p}_3, \quad 1 - 2\sqrt{-5} = \mathfrak{p}_2 \mathfrak{p}_4,$$

wodurch sich die obige Mehrdeutigkeit in die fabelhafte Eindeutigkeit

$$21 = (\mathfrak{p}_1 \mathfrak{p}_2)(\mathfrak{p}_3 \mathfrak{p}_4) = (\mathfrak{p}_1 \mathfrak{p}_3)(\mathfrak{p}_2 \mathfrak{p}_4)$$

aufösen würde.

Aus den von Kummer konzipierten „idealen Zahlen“ sind später die **Ideale** des Ringes  $\mathcal{O}_K$  geworden. Der Grund hierfür ist leicht einzusehen. Wie immer eine ideale Zahl  $\mathfrak{a}$  definiert ist, sie soll mit den Zahlen  $a \in \mathcal{O}_K$  in einer Teilbarkeitsrelation  $\mathfrak{a} \mid a$  stehen, die für  $a, b, \lambda \in \mathcal{O}_K$  die Regeln

$$\mathfrak{a} \mid a \text{ und } \mathfrak{a} \mid b \Rightarrow \mathfrak{a} \mid a \pm b; \quad \mathfrak{a} \mid a \Rightarrow \mathfrak{a} \mid \lambda a$$

erfüllt, und sie soll durch die Gesamtheit

$$\mathfrak{a} = \{a \in \mathcal{O}_K \mid \mathfrak{a} \mid a\}$$

aller Zahlen  $a \in \mathcal{O}_K$ , die sie teilt, eindeutig bestimmt sein. Diese Gesamtheit ist aber wegen der angegebenen Teilbarkeitsregeln ein Ideal von  $\mathcal{O}_K$ . Aus diesem Grund sind die Kummerschen „idealen Zahlen“ von *RICHARD DEDEKIND* als die Ideale von  $\mathcal{O}_K$  eingeführt worden. Die Teilbarkeit  $\mathfrak{a} \mid a$  kann dann einfach durch die Inklusion  $a \in \mathfrak{a}$  definiert werden und allgemeiner die Teilbarkeit  $\mathfrak{a} \mid \mathfrak{b}$  zwischen zwei Idealen durch  $\mathfrak{b} \subseteq \mathfrak{a}$ . Im folgenden wollen wir diesen Teilbarkeitsbegriff genauer studieren. Grundlegend dafür ist das

**(3.1) Theorem.** *Der Ring  $\mathcal{O}_K$  ist noethersch, ganzabgeschlossen, und jedes Primideal  $\mathfrak{p} \neq 0$  ist ein maximales Ideal.*

**Beweis:**  $\mathcal{O}_K$  ist noethersch, weil jedes Ideal  $\mathfrak{a}$  nach (2.10) ein endlich erzeugter  $\mathbb{Z}$ -Modul, erst recht also ein endlich erzeugter  $\mathcal{O}_K$ -Modul ist. Als ganzer Abschluß von  $\mathbb{Z}$  ist  $\mathcal{O}_K$  nach § 2 auch ganzabgeschlossen. Bleibt zu zeigen, daß jedes Primideal  $\mathfrak{p} \neq 0$  maximal ist. Nun ist  $\mathfrak{p} \cap \mathbb{Z}$  ein von Null verschiedenes Primideal ( $p$ ) in  $\mathbb{Z}$ . Die Primidealeigenschaft ist klar, und wenn  $y \in \mathfrak{p}$ ,  $y \neq 0$ , ist und

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

eine Gleichung für  $y$  mit  $a_i \in \mathbb{Z}$ ,  $a_n \neq 0$ , so ist  $a_n \in \mathfrak{p} \cap \mathbb{Z}$ . Der Integritätsbereich  $\bar{\mathcal{O}} = \mathcal{O}_K/\mathfrak{p}$  entsteht aus  $\kappa = \mathbb{Z}/p\mathbb{Z}$  durch Adjunktion

algebraischer Elemente und ist somit ein Körper (man erinnere sich an  $\kappa[\alpha] = \kappa(\alpha)$ , wenn  $\alpha$  algebraisch ist). Daher ist  $\mathfrak{p}$  ein maximales Ideal.  $\square$

Auf die drei soeben bewiesenen Eigenschaften des Ringes  $\mathcal{O}_K$  gründet sich die ganze Teilbarkeitslehre seiner Ideale. Sie wurde von Dedekind entwickelt, der damit Anlaß gab zur folgenden

**(3.2) Definition.** *Ein noetherscher, ganzabgeschlossener Integritätsbereich, in dem jedes von Null verschiedene Primideal ein maximales Ideal ist, heißt Dedekindring.*

So wie die Ringe  $\mathcal{O}_K$  als Verallgemeinerung des Ringes  $\mathbb{Z}$  anzusehen sind, so kann man die Dedekindringe als Verallgemeinerung der Hauptidealringe ansehen. Ist nämlich  $A$  ein Hauptidealring mit dem Quotientenkörper  $K$  und  $L|K$  eine endliche Körpererweiterung, so ist der ganze Abschluß  $B$  von  $A$  in  $L$  i.a. zwar kein Hauptidealring mehr, aber, wie wir noch zeigen werden, stets ein Dedekindring.

Anstelle des Ringes  $\mathcal{O}_K$  betrachten wir im folgenden einen beliebigen Dedekindring  $\mathcal{O}$  und bezeichnen mit  $K$  den Quotientenkörper von  $\mathcal{O}$ . Für zwei Ideale  $\mathfrak{a}$  und  $\mathfrak{b}$  von  $\mathcal{O}$  (allgemeiner eines beliebigen Ringes) wird die Teilbarkeitsrelation  $\mathfrak{a}|\mathfrak{b}$  durch  $\mathfrak{b} \subseteq \mathfrak{a}$  definiert und ihre Summe durch

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

Sie ist das kleinste  $\mathfrak{a}$  und  $\mathfrak{b}$  umfassende Ideal, also der  $\text{ggT}(\mathfrak{a}, \mathfrak{b})$  (größte gemeinsame Teiler) von  $\mathfrak{a}$  und  $\mathfrak{b}$ . Entsprechend ist der Durchschnitt  $\mathfrak{a} \cap \mathfrak{b}$  das  $\text{kgV}$  (kleinste gemeinsame Vielfache) von  $\mathfrak{a}$  und  $\mathfrak{b}$ . Wir definieren das **Produkt** von  $\mathfrak{a}$  und  $\mathfrak{b}$  durch

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

Hinsichtlich dieser Multiplikation erhalten wir für die Ideale von  $\mathcal{O}$ , was uns von den Elementen allein versagt wird, nämlich die **eindeutige Primzerlegung**.

**(3.3) Theorem.** *Jedes von (0) und (1) verschiedene Ideal  $\mathfrak{a}$  von  $\mathcal{O}$  besitzt eine bis auf die Reihenfolge eindeutige Zerlegung*

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

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

Dieses Theorem liegt natürlich ganz im Sinne des Erfinders der „idealen Zahlen“. Seine Gültigkeit ist aber dennoch erstaunlich, weil sein Beweis alles andere als offenkundig ist und eine tieferliegende Gesetzmäßigkeit zwischen den Zahlen in  $\mathcal{O}$  aufdeckt. Wir schicken dem Beweis zwei Lemmata voraus.

**(3.4) Lemma.** *Zu jedem Ideal  $\mathfrak{a} \neq 0$  von  $\mathcal{O}$  gibt es von Null verschiedene Primideale  $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_r$  mit*

$$\mathfrak{a} \supseteq \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_r.$$

**Beweis:** Nehmen wir an, die Menge  $\mathfrak{M}$  der sich dieser Bedingung widersetzenden Ideale wäre nicht leer. Da  $\mathcal{O}$  noethersch ist, so bricht jede aufsteigende Idealkette ab.  $\mathfrak{M}$  ist daher hinsichtlich der Inklusion induktiv geordnet und besitzt somit nach dem Zornschen Lemma ein maximales Element  $\mathfrak{a}$ . Dieses kann kein Primideal sein, d.h. es gibt Elemente  $b_1, b_2 \in \mathcal{O}$  mit  $b_1 b_2 \in \mathfrak{a}$ , aber  $b_1, b_2 \notin \mathfrak{a}$ . Setzen wir  $\mathfrak{a}_1 = (b_1) + \mathfrak{a}$ ,  $\mathfrak{a}_2 = (b_2) + \mathfrak{a}$ , so ist  $\mathfrak{a} \subsetneq \mathfrak{a}_1$ ,  $\mathfrak{a} \subsetneq \mathfrak{a}_2$  und  $\mathfrak{a}_1 \mathfrak{a}_2 \subseteq \mathfrak{a}$ . Wegen der Maximalität enthalten  $\mathfrak{a}_1$  und  $\mathfrak{a}_2$  Primidealprodukte, deren Produkt in  $\mathfrak{a}$  liegt, Widerspruch.  $\square$

**(3.5) Lemma.** *Ist  $\mathfrak{p}$  ein Primideal von  $\mathcal{O}$  und*

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

*so ist  $\mathfrak{a}\mathfrak{p}^{-1} := \{\sum_i a_i x_i \mid a_i \in \mathfrak{a}, x_i \in \mathfrak{p}^{-1}\} \neq \mathfrak{a}$  für jedes Ideal  $\mathfrak{a} \neq 0$ .*

**Beweis:** Sei  $a \in \mathfrak{p}$ ,  $a \neq 0$ , und  $\mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_r \subseteq (a) \subseteq \mathfrak{p}$  mit minimalem  $r$ . Dann ist eines der  $\mathfrak{p}_i$ , etwa  $\mathfrak{p}_1$ , in  $\mathfrak{p}$  enthalten, also  $\mathfrak{p}_1 = \mathfrak{p}$  wegen der Maximalität von  $\mathfrak{p}_1$ . Denn sonst gäbe es für jedes  $i$  ein  $a_i \in \mathfrak{p}_i \setminus \mathfrak{p}$  mit  $a_1 \dots a_r \in \mathfrak{p}$ . Wegen  $\mathfrak{p}_2 \dots \mathfrak{p}_r \not\subseteq (a)$  gibt es ein  $b \in \mathfrak{p}_2 \dots \mathfrak{p}_r$  mit  $b \notin \mathfrak{a}\mathcal{O}$ , also  $a^{-1}b \notin \mathcal{O}$ . Andererseits ist aber  $b\mathfrak{p} \subseteq (a)$ , also  $a^{-1}b\mathfrak{p} \subseteq \mathcal{O}$ , und somit  $a^{-1}b \in \mathfrak{p}^{-1}$ . Damit ist  $\mathfrak{p}^{-1} \neq \mathcal{O}$ .

Sei nun  $\mathfrak{a} \neq 0$  ein Ideal von  $\mathcal{O}$  und  $\alpha_1, \dots, \alpha_n$  ein Erzeugendensystem. Nehmen wir an, daß  $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$ . Dann ist für jedes  $x \in \mathfrak{p}^{-1}$

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

Ist  $A$  die Matrix  $(x\delta_{ij} - a_{ij})$ , so ist also  $A(\alpha_1, \dots, \alpha_n)^t = 0$ . Für die Determinante  $d = \det(A)$  folgt nach (2.3)  $d\alpha_1 = \dots = d\alpha_n = 0$  und

somit  $d = 0$ . Daher ist  $x$  als Nullstelle des normierten Polynoms  $f(X) = \det(X\delta_{ij} - a_{ij}) \in \mathcal{O}[X]$  ganz über  $\mathcal{O}$ , d.h.  $x \in \mathcal{O}$ . Es ergibt sich somit  $\mathfrak{p}^{-1} = \mathcal{O}$ , Widerspruch.  $\square$

**Beweis von (3.3).** I. **Existenz** der Primzerlegung. Sei  $\mathfrak{M}$  die Menge aller von (0) und (1) verschiedenen Ideale, die keine Primzerlegung besitzen. Ist  $\mathfrak{M}$  nicht leer, so schließen wir wie bei (3.4), daß es ein maximales Element  $\mathfrak{a}$  in  $\mathfrak{M}$  gibt. Es liegt in einem maximalen Ideal  $\mathfrak{p}$ , und wir erhalten wegen  $\mathcal{O} \subseteq \mathfrak{p}^{-1}$

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

Nach (3.5) ist  $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}$  und  $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}$ . Da  $\mathfrak{p}$  ein maximales Ideal ist, so folgt  $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$ . Wegen der Maximalität von  $\mathfrak{a}$  in  $\mathfrak{M}$  und wegen  $\mathfrak{a} \neq \mathfrak{p}$ , also  $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathcal{O}$ , besitzt  $\mathfrak{a}\mathfrak{p}^{-1}$  eine Primzerlegung  $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \dots \mathfrak{p}_r$ , also auch  $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}_1 \dots \mathfrak{p}_r\mathfrak{p}$ , Widerspruch.

II. **Eindeutigkeit** der Primzerlegung. Für ein Primideal  $\mathfrak{p}$  gilt:  $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p} \Rightarrow \mathfrak{a} \subseteq \mathfrak{p}$  oder  $\mathfrak{b} \subseteq \mathfrak{p}$ , d.h.  $\mathfrak{p} \mid \mathfrak{a}\mathfrak{b} \Rightarrow \mathfrak{p} \mid \mathfrak{a}$  oder  $\mathfrak{p} \mid \mathfrak{b}$ . Seien nun

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r = \mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_s$$

zwei Primzerlegungen von  $\mathfrak{a}$ . Dann teilt  $\mathfrak{p}_1$  einen Faktor  $\mathfrak{q}_i$ , etwa  $\mathfrak{q}_1$ , und ist wegen der Maximalität  $= \mathfrak{q}_1$ . Wir multiplizieren mit  $\mathfrak{p}_1^{-1}$  und erhalten wegen  $\mathfrak{p}_1 \neq \mathfrak{p}_1\mathfrak{p}_1^{-1} = \mathcal{O}$

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

So fortfahrend erhalten wir  $r = s$  und nach eventueller Umordnung  $\mathfrak{p}_i = \mathfrak{q}_i, i = 1, \dots, r$ .  $\square$

Faßt man in der Primzerlegung eines Ideals  $\mathfrak{a} \neq 0$  von  $\mathcal{O}$  die gleichen Primideale zusammen, so erhält man eine Produktdarstellung

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

Im folgenden soll jede solche Gleichung automatisch so verstanden sein, daß die  $\mathfrak{p}_i$  paarweise verschieden sind. Ist insbesondere  $\mathfrak{a}$  ein Hauptideal  $(a)$ , so schreibt man, der Tradition folgend, die den Idealen den Charakter „idealer Zahlen“ beimißt, häufig etwas ungenau

$$a = \mathfrak{p}_1^{\nu_1} \dots \mathfrak{p}_r^{\nu_r}.$$

Auch verwendet man oft die Bezeichnung  $\mathfrak{a} \mid \mathfrak{a}$  anstelle von  $\mathfrak{a} \mid (a)$  und schreibt  $(\mathfrak{a}, \mathfrak{b}) = 1$  bei zwei teilerfremden Idealen anstelle von  $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b} = \mathcal{O}$ . Für ein Produkt  $\mathfrak{a} = \mathfrak{a}_1 \dots \mathfrak{a}_n$  von teilerfremden Idealen

$\mathfrak{a}_1, \dots, \mathfrak{a}_n$  hat man ein Analogon des „chinesischen Restsatzes“, wie er uns aus dem Bereich der ganzen Zahlen bekannt ist. Wir können diesen Satz für einen beliebigen Ring formulieren, wenn wir beachten, daß

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

ist. In der Tat, wegen  $\mathfrak{a}_i | \mathfrak{a}$ ,  $i = 1, \dots, n$ , ist nämlich einerseits  $\mathfrak{a} \subseteq \bigcap_{i=1}^n \mathfrak{a}_i$ , und wenn  $a \in \bigcap_{i=1}^n \mathfrak{a}_i$ , so gilt  $\mathfrak{a}_i | a$ , und damit, wegen der Teilerfremdheit,  $\mathfrak{a} = \mathfrak{a}_1 \dots \mathfrak{a}_n | a$ , d.h.  $a \in \mathfrak{a}$ .

**(3.6) Chinesischer Restsatz.** Seien  $\mathfrak{a}_1, \dots, \mathfrak{a}_n$  Ideale in einem Ring  $\mathcal{O}$  mit  $\mathfrak{a}_i + \mathfrak{a}_j = \mathcal{O}$  für  $i \neq j$ . Ist dann  $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{a}_i$ , so ist

$$\mathcal{O}/\mathfrak{a} \cong \bigoplus_{i=1}^n \mathcal{O}/\mathfrak{a}_i.$$

**Beweis:** Der kanonische Homomorphismus

$$\mathcal{O} \rightarrow \bigoplus_{i=1}^n \mathcal{O}/\mathfrak{a}_i, \quad a \mapsto \bigoplus_{i=1}^n a \bmod \mathfrak{a}_i,$$

besitzt den Kern  $\mathfrak{a} = \bigcap_i \mathfrak{a}_i$ , so daß es genügt, die Surjektivität zu zeigen. Sei dazu  $x_i \bmod \mathfrak{a}_i \in \mathcal{O}/\mathfrak{a}_i$ ,  $i = 1, \dots, n$ , gegeben. Ist  $n = 2$ , so können wir  $1 = \mathfrak{a}_1 + \mathfrak{a}_2$  schreiben,  $\mathfrak{a}_i \in \mathfrak{a}_i$ , und wenn wir  $x = x_1 \mathfrak{a}_1 + x_2 \mathfrak{a}_2$  setzen, so ist  $x \equiv x_i \bmod \mathfrak{a}_i$ ,  $i = 1, 2$ .

Ist  $n > 2$ , so finden wir hiernach ein Element  $y_1 \in \mathcal{O}$  mit

$$y_1 \equiv 1 \bmod \mathfrak{a}_1, \quad y_1 \equiv 0 \bmod \bigcap_{i=2}^n \mathfrak{a}_i,$$

und analog Elemente  $y_2, \dots, y_n$ , so daß

$$y_i \equiv 1 \bmod \mathfrak{a}_i, \quad y_i \equiv 0 \bmod \mathfrak{a}_j \quad \text{für } i \neq j.$$

Setzen wir  $x = x_1 y_1 + \dots + x_n y_n$ , so ist  $x \equiv x_i \bmod \mathfrak{a}_i$ ,  $i = 1, \dots, n$ . Damit ist die Surjektivität bewiesen.  $\square$

Sei jetzt wieder  $\mathcal{O}$  ein Dedekindring. Für die von Null verschiedenen Ideale von  $\mathcal{O}$  erhalten wir wie bei den Zahlen multiplikative **Inverse**, wenn wir den Begriff der gebrochenen Ideale im Quotientenkörper  $K$  einführen.

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

Für ein Element  $a \in K^*$  ist z.B.  $(a) = a\mathcal{O}$  ein gebrochenes „Hauptideal“. Da  $\mathcal{O}$  noethersch ist, so ist ein  $\mathcal{O}$ -Untermodul  $\mathfrak{a} \neq 0$  von  $K$  offenbar genau dann ein gebrochenes Ideal, wenn es ein  $c \in \mathcal{O}$ ,  $c \neq 0$ , gibt mit  $c\mathfrak{a} \subseteq \mathcal{O}$ . Die gebrochenen Ideale werden genauso multipliziert wie die Ideale von  $\mathcal{O}$ . Letztere bezeichnen wir von nun an auch als die **ganzen Ideale** von  $K$ .

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

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

**Beweis:** Assoziativität, Kommutativität und  $\mathfrak{a}(1) = \mathfrak{a}$  sind klar. Für ein Primideal  $\mathfrak{p}$  ist nach (3.5)  $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1}$ , also  $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$  wegen der Maximalität von  $\mathfrak{p}$ . Ist  $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r$  ein ganzes Ideal, so ist hiernach  $\mathfrak{b} = \mathfrak{p}_1^{-1} \dots \mathfrak{p}_r^{-1}$  ein Inverses. Wegen  $\mathfrak{b}\mathfrak{a} = \mathcal{O}$  ist  $\mathfrak{b} \subseteq \mathfrak{a}^{-1}$ . Ist umgekehrt  $x\mathfrak{a} \subseteq \mathcal{O}$ , so ist  $x\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{b}$ , also  $x \in \mathfrak{b}$  wegen  $\mathfrak{a}\mathfrak{b} = \mathcal{O}$ . Daher ist  $\mathfrak{b} = \mathfrak{a}^{-1}$ . Ist  $\mathfrak{a}$  ein gebrochenes Ideal und  $c \in \mathcal{O}$ ,  $c \neq 0$ , mit  $c\mathfrak{a} \subseteq \mathcal{O}$ , so ist  $(c\mathfrak{a})^{-1} = c^{-1}\mathfrak{a}^{-1}$  das Inverse von  $c\mathfrak{a}$ , also  $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}$ .  $\square$

**(3.9) Korollar.** *Jedes gebrochene Ideal  $\mathfrak{a}$  besitzt eine eindeutige Produktdarstellung*

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

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

**Beweis:** Jedes gebrochene Ideal  $\mathfrak{a}$  ist Quotient  $\mathfrak{a} = \mathfrak{b}/c$  zweier ganzer Ideale  $\mathfrak{b}$  und  $c$ , die nach (3.3) eine Primzerlegung besitzen. Daher besitzt  $\mathfrak{a}$  eine Primzerlegung im Sinne des Korollars. Sie ist nach (3.3) eindeutig, wenn  $\mathfrak{a}$  ganz ist, und damit evidenterweise auch im allgemeinen Fall.  $\square$

Die gebrochenen Hauptideale  $(a) = a\mathcal{O}$ ,  $a \in K^*$ , bilden eine Untergruppe der Idealgruppe  $J_K$ . Sie wird mit  $P_K$  bezeichnet. Die Faktorgruppe

$$Cl_K = J_K/P_K$$

heißt die **Idealklassengruppe**, oder auch kurz **Klassengruppe** von  $K$ . Sie steht zusammen mit der Einheitengruppe  $\mathcal{O}^*$  von  $\mathcal{O}$  in der exakten Sequenz

$$1 \rightarrow \mathcal{O}^* \rightarrow K^* \rightarrow J_K \rightarrow Cl_K \rightarrow 1,$$

wobei der mittlere Pfeil durch  $a \mapsto (a)$  gegeben ist. Die Klassengruppe  $Cl_K$  beschreibt also die Größe der Ausdehnung und die Einheitengruppe  $\mathcal{O}^*$  die des Verlustes, die der Bereich der Zahlen beim Übergang zu den Idealen erfahren hat. Es ist uns damit die unmittelbare Aufgabe gestellt, die Gruppen  $\mathcal{O}^*$  und  $Cl_K$  genauer zu erfassen. Bei allgemeinen Dedekindringen können sie ganz beliebig ausfallen. Beim Ring  $\mathcal{O}_K$  der ganzen Zahlen eines Zahlkörpers  $K$  erhält man jedoch wichtige Endlichkeitsaussagen, die für die weitere Entwicklung der Zahlentheorie von grundlegender Bedeutung sind. Diese Ergebnisse fallen einem aber nicht leicht zu. Sie werden erhalten durch eine geometrische Betrachtung der Zahlen als Gitterpunkte im Raum, für die wir jetzt die nötigen, ganz der linearen Algebra angehörenden Begriffsbildungen bereitstellen wollen.

**Aufgabe 1.** Zerlege  $33 + 11\sqrt{-7}$  in irreduzible ganze Elemente von  $\mathbb{Q}(\sqrt{-7})$ .

**Aufgabe 2.** Zeige, daß

$$54 = 2 \cdot 3^3 = \frac{13 + \sqrt{-47}}{2} \cdot \frac{13 - \sqrt{-47}}{2}$$

zwei verschiedene Zerlegungen in irreduzible ganze Elemente in  $\mathbb{Q}(\sqrt{-47})$  sind.

**Aufgabe 3.** Sei  $d$  quadratfrei und  $p$  eine zu  $2d$  teilerfremde Primzahl. Sei  $\mathcal{O}$  der Ring der ganzen Zahlen von  $\mathbb{Q}(\sqrt{d})$ . Zeige, daß  $(p) = p\mathcal{O}$  genau dann ein Primideal in  $\mathcal{O}$  ist, wenn die Kongruenz  $x^2 \equiv d \pmod{p}$  unlösbar ist.

**Aufgabe 4.** Ein Dedekindring mit nur endlich vielen Primidealen ist ein Hauptidealring.

**Hinweis:** Ist  $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \dots \mathfrak{p}_r^{\nu_r} \neq 0$  ein Ideal, so wähle Elemente  $\pi_i \in \mathfrak{p}_i \setminus \mathfrak{p}_i^2$  und wende den chinesischen Restsatz auf die Restklassen  $\pi_i^{\nu_i} \pmod{\mathfrak{p}_i^{\nu_i+1}}$  an.

**Aufgabe 5.** Der Restklassenring  $\mathcal{O}/\mathfrak{a}$  eines Dedekindringes nach einem Ideal  $\mathfrak{a} \neq 0$  ist ein Hauptidealring.

**Hinweis:** Für  $\mathfrak{a} = \mathfrak{p}^n$  sind  $\mathfrak{p}/\mathfrak{p}^n, \dots, \mathfrak{p}^{n-1}/\mathfrak{p}^n$  die einzigen echten Ideale von  $\mathcal{O}/\mathfrak{a}$ . Wähle  $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$  und zeige  $\mathfrak{p}^\nu = \mathcal{O}\pi^\nu + \mathfrak{p}^n$ .

**Aufgabe 6.** Jedes Ideal eines Dedekindringes läßt sich durch zwei Elemente erzeugen.

**Hinweis:** Verwende Aufgabe 5.

**Aufgabe 7.** In einem noetherschen Ring  $R$ , in dem jedes Primideal maximal ist, wird jede absteigende Idealkette  $\mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \dots$  stationär.



**Hinweis:** Zeige wie in (3.4), daß  $(0)$  ein Produkt  $\mathfrak{p}_1 \cdots \mathfrak{p}_r$  von Primidealen ist und daß sich die Kette  $R \supseteq \mathfrak{p}_1 \supseteq \mathfrak{p}_1 \mathfrak{p}_2 \supseteq \cdots \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r = (0)$  zu einer Kompositionsreihe verfeinern läßt.

**Aufgabe 8.** Sei  $\mathfrak{m}$  ein ganzes Ideal  $\neq 0$  des Dedekindringes  $\mathcal{O}$ . Zeige, daß in jeder Idealklasse von  $Cl_K$  ein ganzes, zu  $\mathfrak{m}$  teilerfremdes Ideal liegt.

**Aufgabe 9.** Sei  $\mathcal{O}$  ein Ring, dessen von Null verschiedene Ideale eindeutige Primidealzerlegungen besitzen. Zeige, daß  $\mathcal{O}$  ein Dedekindring ist.

**Aufgabe 10.** Die gebrochenen Ideale  $\mathfrak{a}$  eines Dedekindringes  $\mathcal{O}$  sind projektive  $\mathcal{O}$ -Moduln, d.h. zu jedem surjektiven Homomorphismus  $M \xrightarrow{f} N$  von  $\mathcal{O}$ -Moduln läßt sich jeder Homomorphismus  $\alpha \xrightarrow{g} N$  zu einem Homomorphismus  $h : \mathfrak{a} \rightarrow M$  mit  $f \circ h = g$  hochheben.

## § 4. Gitter

In § 1 haben wir bei der Lösung der Grundprobleme über die Gaußschen Zahlen an wesentlicher Stelle die Inklusion

$$\mathbb{Z}[i] \subseteq \mathbb{C}$$

benützt und haben die ganzen Zahlen von  $\mathbb{Q}(i)$  als Gitterpunkte in der komplexen Ebene angesehen. Diese Betrachtungsweise ist von *HERMANN MINKOWSKI* (1864–1909) auf beliebige Zahlkörper ausgedehnt worden und hat zu Resultaten geführt, auf die sich die algebraische Zahlentheorie in entscheidender Weise gründet. Um die Minkowskische Theorie zu entwickeln, müssen wir zunächst den allgemeinen Begriff des Gitters einführen und einige seiner grundsätzlichen Eigenschaften studieren.

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

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

mit linear unabhängigen Vektoren  $v_1, \dots, v_m$  von  $V$ . Das  $m$ -Tupel  $(v_1, \dots, v_m)$  heißt eine **Basis** und die Menge

$$\Phi = \{x_1 v_1 + \cdots + x_m v_m \mid x_i \in \mathbb{R}, \quad 0 \leq x_i < 1\}$$

eine **Grundmasche** des Gitters. Das Gitter heißt **vollständig** oder eine  **$\mathbb{Z}$ -Struktur** von  $V$ , wenn  $m = n$  ist.

Die Vollständigkeit des Gitters ist offenbar gleichbedeutend damit, daß die sämtlichen Verschiebungen  $\Phi + \gamma$ ,  $\gamma \in \Gamma$ , der Grundmasche den ganzen Raum  $V$  überdecken.

Die obige Definition bezieht sich auf die Wahl linear unabhängiger Vektoren. Wir benötigen aber eine von solcher Wahl unabhängige Charakterisierung der Gitter. Ein Gitter ist zunächst einmal eine endlich erzeugte Untergruppe von  $V$ . Aber nicht jede endlich erzeugte Untergruppe ist auch ein Gitter, z.B.  $\mathbb{Z} + \mathbb{Z}\sqrt{2} \subseteq \mathbb{R}$  nicht. Jedes Gitter  $\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$  hat jedoch die besondere Eigenschaft, eine **diskrete** Untergruppe von  $V$  zu sein. Das soll heißen, daß jeder Punkt  $\gamma \in \Gamma$  ein isolierter Punkt ist, also eine Umgebung besitzt, die keinen weiteren Punkt von  $\Gamma$  enthält. Ist nämlich

$$\gamma = a_1v_1 + \cdots + a_mv_m \in \Gamma$$

und ergänzen wir  $v_1, \dots, v_m$  zu einer Basis  $v_1, \dots, v_n$  von  $V$ , so ist offenbar

$$\{x_1v_1 + \cdots + x_nv_n \mid x_i \in \mathbb{R}, \quad |a_i - x_i| < 1 \quad \text{für } i = 1, \dots, m\}$$

eine solche Umgebung. Diese Eigenschaft ist ausschlaggebend.

**(4.2) Satz.** *Eine Untergruppe  $\Gamma \subseteq V$  ist genau dann ein Gitter, wenn sie diskret ist.*

**Beweis:** Sei  $\Gamma$  eine diskrete Untergruppe von  $V$ . Sei  $V_0$  der lineare Unterraum von  $V$ , der durch die Menge  $\Gamma$  aufgespannt wird, und  $m$  seine Dimension. Dann können wir eine in  $\Gamma$  gelegene Basis  $u_1, \dots, u_m$  von  $V_0$  wählen und bilden damit das vollständige Gitter

$$\Gamma_0 = \mathbb{Z}u_1 + \cdots + \mathbb{Z}u_m \subseteq \Gamma$$

von  $V_0$ . Wir behaupten, daß der Index  $(\Gamma : \Gamma_0)$  endlich ist. Zum Beweis durchlaufe  $\gamma_i \in \Gamma$  ein Repräsentantensystem für die Nebenklassen in  $\Gamma/\Gamma_0$ . Da  $\Gamma_0$  vollständig ist in  $V_0$ , so überdecken die Verschiebungen  $\Phi_0 + \gamma, \gamma \in \Gamma_0$ , der Grundmasche

$$\Phi_0 = \{x_1u_1 + \cdots + x_mu_m \mid x_i \in \mathbb{R}, \quad 0 \leq x_i < 1\}$$

den ganzen Raum  $V_0$ . Daher können wir

$$\gamma_i = \mu_i + \gamma_{0i}, \quad \mu_i \in \Phi_0, \quad \gamma_{0i} \in \Gamma_0 \subseteq V_0,$$

schreiben. Da die  $\mu_i = \gamma_i - \gamma_{0i} \in \Gamma$  diskret in der beschränkten Menge  $\Phi_0$  liegen, so muß ihre Anzahl endlich sein.

Setzen wir nun  $q = (\Gamma : \Gamma_0)$ , so ist  $q\Gamma \subseteq \Gamma_0$ , also

$$\Gamma \subseteq \frac{1}{q}\Gamma_0 = \mathbb{Z}\left(\frac{1}{q}u_1\right) + \cdots + \mathbb{Z}\left(\frac{1}{q}u_m\right).$$

Nach dem Hauptsatz über endlich erzeugte abelsche Gruppen besitzt  $\Gamma$  daher eine  $\mathbb{Z}$ -Basis  $v_1, \dots, v_r$ ,  $r \leq m$ , d.h.  $\Gamma = \mathbb{Z}v_1 + \dots + \mathbb{Z}v_r$ . Die Vektoren  $v_1, \dots, v_r$  sind überdies  $\mathbb{R}$ -linear unabhängig, da sie den  $m$ -dimensionalen Raum  $V_0$  aufspannen. Daher ist  $\Gamma$  ein Gitter.  $\square$

Wir beweisen als nächstes ein Kriterium, das uns sagt, wann ein Gitter im Raum  $V$ , gegeben etwa als eine diskrete Untergruppe  $\Gamma \subseteq V$ , vollständig ist.

**(4.3) Lemma.** *Ein Gitter  $\Gamma$  in  $V$  ist genau dann vollständig, wenn es eine beschränkte Teilmenge  $M \subseteq V$  gibt, deren sämtliche Verschiebungen  $M + \gamma$ ,  $\gamma \in \Gamma$ , den ganzen Raum  $V$  überdecken.*

**Beweis:** Ist  $\Gamma = \mathbb{Z}v_1 + \dots + \mathbb{Z}v_n$  vollständig, so kann man für  $M$  die Grundmasche  $\Phi = \{x_1v_1 + \dots + x_nv_n \mid 0 \leq x_i < 1\}$  wählen.

Sei andererseits  $M$  eine beschränkte Teilmenge von  $V$ , deren Verschiebungen  $M + \gamma$ ,  $\gamma \in \Gamma$ , den Raum  $V$  überdecken. Sei  $V_0$  der durch  $\Gamma$  aufgespannte Unterraum. Wir müssen zeigen, daß  $V = V_0$  ist. Sei dazu  $v \in V$ . Wegen  $V = \bigcup_{\gamma \in \Gamma} (M + \gamma)$  können wir für jedes  $\nu \in \mathbb{N}$  schreiben

$$\nu v = a_\nu + \gamma_\nu, \quad a_\nu \in M, \quad \gamma_\nu \in \Gamma \subseteq V_0.$$

Da  $M$  beschränkt ist, ist  $\frac{1}{\nu}a_\nu$  eine Nullfolge, und es folgt wegen der Abgeschlossenheit von  $V_0$ ,

$$v = \lim_{\nu \rightarrow \infty} \frac{1}{\nu}a_\nu + \lim_{\nu \rightarrow \infty} \frac{1}{\nu}\gamma_\nu = \lim_{\nu \rightarrow \infty} \frac{1}{\nu}\gamma_\nu \in V_0. \quad \square$$

Sei jetzt  $V$  ein *euklidischer* Vektorraum, also ein  $\mathbb{R}$ -Vektorraum endlicher Dimension  $n$  mit einer symmetrischen, positiv definiten Bilinearform

$$\langle \cdot, \cdot \rangle : V \times V \rightarrow \mathbb{R}.$$

Auf  $V$  haben wir dann einen Volumenbegriff – genauer ein Haarsches Maß. Der von einer Orthonormalbasis  $e_1, \dots, e_n$  aufgespannte Würfel erhält den Inhalt 1, und allgemeiner das von  $n$  linear unabhängigen Vektoren  $v_1, \dots, v_n$  aufgespannte Parallelepiped

$$\Phi = \{x_1v_1 + \dots + x_nv_n \mid x_i \in \mathbb{R}, 0 \leq x_i < 1\}$$

den Inhalt

$$\text{vol}(\Phi) = |\det A|,$$

wenn  $A = (a_{ik})$  die Übergangsmatrix der Basis  $e_1, \dots, e_n$  zu  $v_1, \dots, v_n$  ist, d.h.  $v_i = \sum_k a_{ik} e_k$ . Wegen

$$(\langle v_i, v_j \rangle) = (\sum_{k,l} a_{ik} a_{jl} \langle e_k, e_l \rangle) = (\sum_k a_{ik} a_{jk}) = AA^t$$

kann man auch in invarianter Weise

$$\text{vol}(\Phi) = |\det(\langle v_i, v_j \rangle)|^{1/2}$$

schreiben.

Sei  $\Gamma$  das von  $v_1, \dots, v_n$  aufgespannte Gitter.  $\Phi$  ist dann eine Grundmasche von  $\Gamma$ , und wir setzen kurz

$$\text{vol}(\Gamma) = \text{vol}(\Phi).$$

Dies hängt nicht von der Wahl der Gitterbasis  $v_1, \dots, v_n$  ab, weil die Übergangsmatrix zu einer anderen mit ihrer Inversen ganzzahlige Koeffizienten hat, also eine Determinante  $\pm 1$ , so daß sie die Menge  $\Phi$  in eine Menge gleichen Inhalts transformiert.

Wir kommen nun zum wichtigsten Satz über die Gitter. Eine Teilmenge  $X$  von  $V$  heißt *zentralsymmetrisch*, wenn sie mit jedem Punkt  $x$  auch den Punkt  $-x$  enthält, und *konvex*, wenn sie mit je zwei Punkten  $x, y$  auch die Strecke  $\{ty + (1-t)x \mid 0 \leq t \leq 1\}$  von  $x$  nach  $y$  enthält. Mit diesen Definitionen gilt jetzt der

**(4.4) Minkowskische Gitterpunktsatz.** *Sei  $\Gamma$  ein vollständiges Gitter im euklidischen Vektorraum  $V$  und  $X$  eine zentralsymmetrische und konvexe Teilmenge von  $V$ . Ist dann*

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

*so enthält  $X$  mindestens einen von Null verschiedenen Gitterpunkt  $\gamma \in \Gamma$ .*

**Beweis:** Es genügt zu zeigen, daß es zwei verschiedene Gitterpunkte  $\gamma_1, \gamma_2 \in \Gamma$  gibt mit

$$\left(\frac{1}{2}X + \gamma_1\right) \cap \left(\frac{1}{2}X + \gamma_2\right) \neq \emptyset.$$

Wählen wir nämlich dann einen Punkt aus diesem Durchschnitt aus,

$$\frac{1}{2}x_1 + \gamma_1 = \frac{1}{2}x_2 + \gamma_2, \quad x_1, x_2 \in X,$$

so ist

$$\gamma = \gamma_1 - \gamma_2 = \frac{1}{2}x_2 - \frac{1}{2}x_1$$

der Mittelpunkt der Strecke von  $x_2$  nach  $-x_1$ , liegt also in  $X \cap \Gamma$ .

Wären nun die Mengen  $\frac{1}{2}X + \gamma$ ,  $\gamma \in \Gamma$ , paarweise disjunkt, so träfe dies auch auf ihre Durchschnitte  $\Phi \cap (\frac{1}{2}X + \gamma)$  mit einer Grundmasche  $\Phi$  von  $\Gamma$  zu, d.h. es wäre

$$\text{vol}(\Phi) \geq \sum_{\gamma \in \Gamma} \text{vol}\left(\Phi \cap \left(\frac{1}{2}X + \gamma\right)\right).$$

Da durch die Translation mit  $-\gamma$  aus  $\Phi \cap (\frac{1}{2}X + \gamma)$  die Menge  $(\Phi - \gamma) \cap \frac{1}{2}X$  von gleichem Volumen entsteht, und da die  $\Phi - \gamma$ ,  $\gamma \in \Gamma$ , den ganzen Raum  $V$ , also auch die Menge  $\frac{1}{2}X$  überdecken, so würden wir

$$\text{vol}(\Phi) \geq \sum_{\gamma \in \Gamma} \text{vol}\left((\Phi - \gamma) \cap \frac{1}{2}X\right) = \text{vol}\left(\frac{1}{2}X\right) = \frac{1}{2^n} \text{vol}(X)$$

erhalten, im Gegensatz zur Voraussetzung.  $\square$

**Aufgabe 1.** Zeige, daß ein Gitter  $\Gamma$  im  $\mathbb{R}^n$  genau dann vollständig ist, wenn die Faktorgruppe  $\mathbb{R}^n/\Gamma$  kompakt ist.

**Aufgabe 2.** Man zeige, daß der Minkowskische Gitterpunktsatz nicht verbessert werden kann, indem man eine konvexe, zentralsymmetrische Menge  $X \subseteq V$  mit  $\text{vol}(X) = 2^n \text{vol}(\Gamma)$  angibt, die keinen von Null verschiedenen Punkt von  $\Gamma$  enthält. Ist aber  $X$  kompakt, so ist in (4.4) auch das Gleichheitszeichen zulässig.

**Aufgabe 3.** (Minkowskischer Linearformensatz). Seien

$$L_i(x_1, \dots, x_n) = \sum_{j=1}^n a_{ij}x_j, \quad i = 1, \dots, n,$$

reelle Linearformen mit  $\det(a_{ij}) \neq 0$  und  $c_1, \dots, c_n$  positive reelle Zahlen mit  $c_1 \dots c_n > |\det(a_{ij})|$ . Zeige, daß es ganze Zahlen  $m_1, \dots, m_n \in \mathbb{Z}$  gibt mit

$$|L_i(m_1, \dots, m_n)| < c_i, \quad i = 1, \dots, n.$$

**Hinweis:** Wende den Minkowskischen Gitterpunktsatz an.

## § 5. Minkowski-Theorie

Der Hauptgedanke der Minkowskischen Betrachtungsweise eines algebraischen Zahlkörpers  $K|\mathbb{Q}$  vom Grade  $n$  besteht in der Interpretation seiner Zahlen als Punkte im  $n$ -dimensionalen Raum. Aus diesem Grund ist diese Theorie als „Geometrie der Zahlen“ bezeichnet worden. Es ist aber angebracht, der heutigen Tendenz zu folgen und sie „Minkowski-Theorie“ zu nennen, weil man inzwischen zu einer geometrischen Auffassung der Zahlentheorie in einem ganz anderen und viel umfassenderen Sinne gelangt ist. Diese werden wir in § 13 erläutern. Hier betrachten wir die kanonische Abbildung

$$j : K \rightarrow K_{\mathbb{C}} := \prod_{\tau} \mathbb{C}, \quad a \mapsto ja = (\tau a),$$

die sich durch die  $n$  komplexen Einbettungen  $\tau : K \rightarrow \mathbb{C}$  ergibt. Der  $\mathbb{C}$ -Vektorraum  $K_{\mathbb{C}}$  ist mit dem *hermiteschen Skalarprodukt*

$$(*) \quad \langle x, y \rangle = \sum_{\tau} x_{\tau} \bar{y}_{\tau}$$

ausgestattet, wobei daran erinnert sei, daß ein hermitesches Skalarprodukt durch eine im ersten Argument lineare Form  $H(x, y)$  gegeben ist, derart daß  $\overline{H(x, y)} = H(y, x)$  und  $H(x, x) > 0$  für  $x \neq 0$ . Wir sehen im folgenden  $K_{\mathbb{C}}$  stets als den mit der „Standardmetrik“  $(*)$  versehenen hermiteschen Raum an.

Die Galoisgruppe  $G(\mathbb{C}|\mathbb{R})$  wird durch die komplexe Konjugation

$$F : z \mapsto \bar{z}$$

erzeugt. Die Bezeichnung  $F$  wird ihre Erklärung erst später finden (vgl. Kap. III, § 4).  $F$  operiert einerseits auf den Faktoren des Produktes  $\prod_{\tau} \mathbb{C}$ , andererseits aber auch auf der Menge der  $\tau$ , durch die sie indiziert sind; jeder Einbettung  $\tau : K \rightarrow \mathbb{C}$  ist die komplex konjugierte  $\bar{\tau} : K \rightarrow \mathbb{C}$  zugeordnet. Insgesamt ergibt sich hieraus eine Involution

$$F : K_{\mathbb{C}} \rightarrow K_{\mathbb{C}},$$

die auf den Punkten  $z = (z_{\tau}) \in K_{\mathbb{C}}$  durch

$$(Fz)_{\tau} = \bar{z}_{\bar{\tau}}$$

gegeben ist. Das Skalarprodukt  $\langle \cdot, \cdot \rangle$  ist unter  $F$  invariant, d.h.

$$\langle Fx, Fy \rangle = F \langle x, y \rangle.$$

Auf dem  $\mathbb{C}$ -Vektorraum  $K_{\mathbb{C}} = \prod_{\tau} \mathbb{C}$  haben wir schließlich noch die lineare Abbildung

$$Tr : K_{\mathbb{C}} \rightarrow \mathbb{C},$$

die durch die Summe der Koordinaten gegeben ist; auch sie ist  $F$ -invariant. Das Kompositum

$$K \xrightarrow{j} K_{\mathbb{C}} \xrightarrow{Tr} \mathbb{C}$$

ergibt die übliche Spur von  $K|\mathbb{Q}$  (vgl. (2.6), ii),

$$Tr_{K|\mathbb{Q}}(a) = Tr(ja).$$

Unser Augenmerk gilt jetzt dem  $\mathbb{R}$ -Vektorraum

$$K_{\mathbb{R}} = K_{\mathbb{C}}^+ = [\prod_{\tau} \mathbb{C}]^+$$

der unter  $G(\mathbb{C}|\mathbb{R})$ , d.h. unter  $F$  invarianten Punkte von  $K_{\mathbb{C}}$ , also der Punkte  $(z_{\tau})$  mit  $z_{\bar{\tau}} = \bar{z}_{\tau}$ . Wegen  $\bar{\tau}a = \overline{\tau a}$  für  $a \in K$  ist  $F(ja) = ja$ , so daß wir eine Abbildung

$$j : K \rightarrow K_{\mathbb{R}}$$

erhalten. Die Einschränkung des hermiteschen Skalarprodukts  $\langle \ , \ \rangle$  von  $K_{\mathbb{C}}$  auf  $K_{\mathbb{R}}$  wird ein Skalarprodukt

$$\langle \ , \ \rangle : K_{\mathbb{R}} \times K_{\mathbb{R}} \rightarrow \mathbb{R}$$

auf dem  $\mathbb{R}$ -Vektorraum  $K_{\mathbb{R}}$ , denn für  $x, y \in K_{\mathbb{R}}$  gilt  $\langle x, y \rangle \in \mathbb{R}$  wegen  $F\langle x, y \rangle = \langle Fx, Fy \rangle = \langle x, y \rangle$ , ferner  $\langle x, y \rangle = \overline{\langle x, y \rangle} = \langle y, x \rangle$  und  $\langle x, x \rangle > 0$  für  $x \neq 0$  ohnehin.

Wir nennen den *euklidischen* Vektorraum

$$K_{\mathbb{R}} = [\prod_{\tau} \mathbb{C}]^+$$

den **Minkowski-Raum**, sein Skalarprodukt  $\langle \ , \ \rangle$  die **kanonische Metrik** und das zugehörige Haarsche Maß (vgl. § 4, S. 27) das **kanonische Maß**. Wegen  $Tr \circ F = F \circ Tr$  haben wir auf  $K_{\mathbb{R}}$  die  $\mathbb{R}$ -lineare Abbildung

$$Tr : K_{\mathbb{R}} \rightarrow \mathbb{R},$$

und es ist das Kompositum derselben mit  $j : K \rightarrow K_{\mathbb{R}}$  wieder die übliche Spur von  $K|\mathbb{Q}$ ,

$$Tr_{K|\mathbb{Q}}(a) = Tr(ja).$$

**Bemerkung:** Ohne im weiteren Bezug darauf zu nehmen, erwähnen wir, daß die Abbildung  $j : K \rightarrow K_{\mathbb{R}}$  den Vektorraum  $K_{\mathbb{R}}$  mit dem Tensorprodukt  $K \otimes_{\mathbb{Q}} \mathbb{R}$  identifiziert,

$$K \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\sim} K_{\mathbb{R}}, \quad a \otimes x \mapsto (ja)x,$$

und ebenso  $K \otimes_{\mathbb{Q}} \mathbb{C} \xrightarrow{\sim} K_{\mathbb{C}}$ . Der Inklusion  $K_{\mathbb{R}} \subseteq K_{\mathbb{C}}$  entspricht bei dieser Interpretation die kanonische Abbildung  $K \otimes_{\mathbb{Q}} \mathbb{R} \rightarrow K \otimes_{\mathbb{Q}} \mathbb{C}$ , die durch die Inklusion  $\mathbb{R} \hookrightarrow \mathbb{C}$  induziert wird, und es geht  $F$  über in  $F(a \otimes z) = a \otimes \bar{z}$ .

Explizit läßt sich der Minkowski-Raum  $K_{\mathbb{R}}$  wie folgt beschreiben. Von den Einbettungen  $\tau : K \rightarrow \mathbb{C}$  sind manche reell, d.h. sie fallen schon in  $\mathbb{R}$  hinein, und manche komplex, d.h. nicht-reell. Seien

$$\rho_1, \dots, \rho_r : K \rightarrow \mathbb{R}$$

die reellen. Die komplexen gruppieren sich zu Paaren

$$\sigma_1, \bar{\sigma}_1, \dots, \sigma_s, \bar{\sigma}_s : K \rightarrow \mathbb{C}$$

komplex konjugierter Einbettungen, so daß  $n = r + 2s$ . Aus jedem Paar wählen wir eine feste komplexe Einbettung aus und lassen  $\rho$  die Familie der reellen und  $\sigma$  die Familie der ausgewählten komplexen Einbettungen durchlaufen. Da  $F$  die  $\rho$  invariant läßt, die  $\sigma, \bar{\sigma}$  aber vertauscht, so ist

$$K_{\mathbb{R}} = \{(z_{\tau}) \in \prod_{\tau} \mathbb{C} \mid z_{\rho} \in \mathbb{R}, z_{\bar{\sigma}} = \bar{z}_{\sigma}\},$$

und es ergibt sich der

**(5.1) Satz.** *Wir erhalten einen Isomorphismus*

$$f : K_{\mathbb{R}} \rightarrow \prod_{\tau} \mathbb{R} = \mathbb{R}^{r+2s}$$

durch die Zuordnung  $(z_{\tau}) \mapsto (x_{\tau})$  mit

$$x_{\rho} = z_{\rho}, \quad x_{\sigma} = \operatorname{Re}(z_{\sigma}), \quad x_{\bar{\sigma}} = \operatorname{Im}(z_{\sigma}).$$

Dieser überführt die kanonische Metrik  $\langle \cdot, \cdot \rangle$  in das Skalarprodukt

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

wobei  $\alpha_{\tau} = 1$  bzw.  $\alpha_{\tau} = 2$  ist, je nachdem  $\tau$  reell oder komplex ist.

**Beweis:** Die Isomorphie ist klar. Sind  $z = (z_{\tau}) = (x_{\tau} + iy_{\tau})$ ,  $z' = (z'_{\tau}) = (x'_{\tau} + iy'_{\tau}) \in K_{\mathbb{R}}$ , so ist  $z_{\rho} \bar{z}'_{\rho} = x_{\rho} x'_{\rho}$  und unter Beachtung von  $y_{\sigma} = x_{\bar{\sigma}}$  und  $y'_{\sigma} = x'_{\bar{\sigma}}$ ,

$$z_{\sigma} \bar{z}'_{\sigma} + z_{\bar{\sigma}} \bar{z}'_{\bar{\sigma}} = z_{\sigma} \bar{z}'_{\sigma} + \bar{z}_{\sigma} z'_{\sigma} = 2 \operatorname{Re}(z_{\sigma} \bar{z}'_{\sigma}) = 2(x_{\sigma} x'_{\sigma} + x_{\bar{\sigma}} x'_{\bar{\sigma}}).$$

Hieraus folgt die Behauptung über die Skalarprodukte.  $\square$



Durch das Skalarprodukt  $(x, y) = \sum_{\tau} \alpha_{\tau} x_{\tau} y_{\tau}$  wird das kanonische Maß von  $K_{\mathbb{R}}$  auf  $\mathbb{R}^{r+2s}$  übertragen. Es unterscheidet sich offenbar vom üblichen Lebesgue-Maß durch

$$\text{vol}_{\text{kanonisch}}(X) = 2^s \text{vol}_{\text{Lebesgue}}(f(X)).$$

Minkowski selbst hat mit dem Lebesgue-Maß auf  $\mathbb{R}^{r+2s}$  gearbeitet, und so halten es auch die meisten Lehrbücher. Ihm entspricht auf  $K_{\mathbb{R}}$  das Maß, das durch das Skalarprodukt

$$(x, y) = \sum_{\tau} \frac{1}{\alpha_{\tau}} x_{\tau} \bar{y}_{\tau}$$

festgelegt wird. Dieses Skalarprodukt möge daher die **Minkowski-Metrik** auf  $K_{\mathbb{R}}$  genannt werden. Wir arbeiten jedoch immer mit der kanonischen Metrik und meinen mit  $\text{vol}$  das zugehörige kanonische Maß.

Durch die Abbildung  $j : K \rightarrow K_{\mathbb{R}}$  entstehen die folgenden Gitter im Minkowski-Raum  $K_{\mathbb{R}}$ .

**(5.2) Satz.** *Ist  $\mathfrak{a} \neq 0$  ein Ideal von  $\mathcal{O}_K$ , so ist  $\Gamma = j\mathfrak{a}$  ein vollständiges Gitter in  $K_{\mathbb{R}}$  mit dem Grundmaschenvolumen*

$$\text{vol}(\Gamma) = \sqrt{|d_K|}(\mathcal{O}_K : \mathfrak{a}).$$

**Beweis:** Sei  $\alpha_1, \dots, \alpha_n$  eine  $\mathbb{Z}$ -Basis von  $\mathfrak{a}$ , so daß  $\Gamma = \mathbb{Z}j\alpha_1 + \dots + \mathbb{Z}j\alpha_n$ . Wir numerieren die Einbettungen  $\tau : K \rightarrow \mathbb{C}$ ,  $\tau_1, \dots, \tau_n$ , und bilden die Matrix  $A = (\tau_l \alpha_i)$ . Dann ist einerseits nach (2.12)

$$d(\mathfrak{a}) = d(\alpha_1, \dots, \alpha_n) = (\det A)^2 = (\mathcal{O}_K : \mathfrak{a})^2 d(\mathcal{O}_K) = (\mathcal{O}_K : \mathfrak{a})^2 d_K$$

und andererseits

$$(\langle j\alpha_i, j\alpha_k \rangle) = \left( \sum_{l=1}^n \tau_l \alpha_i \bar{\tau}_l \alpha_k \right) = A \bar{A}^t.$$

Es ergibt sich hieraus in der Tat

$$\text{vol}(\Gamma) = |\det(\langle j\alpha_i, j\alpha_k \rangle)|^{1/2} = |\det A| = \sqrt{|d_K|}(\mathcal{O}_K : \mathfrak{a}). \quad \square$$

Mit diesem Resultat liefert nun der Minkowskische Gitterpunktsatz das folgende Ergebnis, auf das es uns für die Anwendung auf die Zahlentheorie vornehmlich ankommen wird.

**(5.3) Theorem.** Sei  $\mathfrak{a} \neq 0$  ein ganzes Ideal von  $K$ , und seien  $c_\tau > 0$  ( $\tau \in \text{Hom}(K, \mathbb{C})$ ) reelle Zahlen mit  $c_\tau = c_{\bar{\tau}}$  und

$$\prod_{\tau} c_\tau > A(\mathcal{O}_K : \mathfrak{a}),$$

wobei  $A = (\frac{2}{\pi})^s \sqrt{|d_K|}$ . Dann gibt es ein  $a \in \mathfrak{a}$ ,  $a \neq 0$ , mit

$$|\tau a| < c_\tau \quad \text{für alle } \tau \in \text{Hom}(K, \mathbb{C}).$$

**Beweis:** Die Menge  $X = \{(z_\tau) \in K_{\mathbb{R}} \mid |z_\tau| < c_\tau\}$  ist zentralsymmetrisch und konvex. Ihr Volumen  $\text{vol}(X)$  ergibt sich über die Abbildung (5.1)

$$f : K_{\mathbb{R}} \xrightarrow{\sim} \prod_{\tau} \mathbb{R}, \quad (z_\tau) \mapsto (x_\tau),$$

mit  $x_\rho = z_\rho$ ,  $x_\sigma = \text{Re}(z_\sigma)$ ,  $x_{\bar{\sigma}} = \text{Im}(z_\sigma)$ , als das  $2^s$ -fache des Lebesgue-Inhalts des Bildes

$$f(X) = \{(x_\tau) \in \prod_{\tau} \mathbb{R} \mid |x_\rho| < c_\rho, \ x_\sigma^2 + x_{\bar{\sigma}}^2 < c_\sigma^2\}.$$

Es ist also

$$\text{vol}(X) = 2^s \text{vol}_{\text{Lebesgue}}(f(X)) = 2^s \prod_{\rho} (2c_\rho) \prod_{\sigma} (\pi c_\sigma^2) = 2^{r+s} \pi^s \prod_{\tau} c_\tau.$$

Setzen wir (5.2) ein, so erhalten wir

$$\text{vol}(X) > 2^{r+s} \pi^s \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|} (\mathcal{O}_K : \mathfrak{a}) = 2^n \text{vol}(\Gamma).$$

Hiermit ist die Voraussetzung für den Minkowskischen Gitterpunktsatz erfüllt. Es gibt daher in der Tat einen Gitterpunkt  $ja \in X$ ,  $a \neq 0$ ,  $a \in \mathfrak{a}$ , d.h.  $|\tau a| < c_\tau$ .  $\square$

Die Minkowski-Theorie besitzt auch eine **multiplikative Version**. Sie gründet sich auf den Homomorphismus

$$j : K^* \rightarrow K_{\mathbb{C}}^* = \prod_{\tau} \mathbb{C}^*.$$

Die multiplikative Gruppe  $K_{\mathbb{C}}^*$  ist mit dem Homomorphismus

$$N : K_{\mathbb{C}}^* \rightarrow \mathbb{C}^*$$

versehen, der sich durch das Produkt der Koordinaten ergibt. Das Kompositum

$$K^* \xrightarrow{j} K_{\mathbb{C}}^* \xrightarrow{N} \mathbb{C}^*$$

ist die übliche Norm von  $K|\mathbb{Q}$ ,

$$N_{K|\mathbb{Q}}(a) = N(ja).$$

Um nun auch im multiplikativen Fall die Gitter ins Spiel zu bringen, gehen wir von den multiplikativen Gruppen zu additiven Gruppen über, indem wir den Logarithmus

$$l : \mathbb{C}^* \rightarrow \mathbb{R}, \quad z \mapsto \log |z|,$$

anwenden. Er induziert einen surjektiven Homomorphismus

$$l : K_{\mathbb{C}}^* \rightarrow \prod_{\tau} \mathbb{R},$$

und wir erhalten das kommutative Diagramm

$$\begin{array}{ccccc} K^* & \xrightarrow{j} & K_{\mathbb{C}}^* & \xrightarrow{l} & \prod_{\tau} \mathbb{R} \\ N_{K|\mathbb{Q}} \downarrow & & \downarrow N & & \downarrow Tr \\ \mathbb{Q}^* & \longrightarrow & \mathbb{C}^* & \xrightarrow{l} & \mathbb{R} \end{array}.$$

Auf allen Gruppen dieses Diagramms operiert die Involution  $F \in G(\mathbb{C}|\mathbb{R})$ , auf  $K^*$  trivial, auf  $K_{\mathbb{C}}^*$  wie zuvor und auf den Punkten  $x = (x_{\tau}) \in \prod_{\tau} \mathbb{R}$  durch  $(Fx)_{\tau} = x_{\bar{\tau}}$ . Es gilt offenbar

$$F \circ j = j, \quad F \circ l = l \circ F, \quad N \circ F = F \circ N, \quad Tr \circ F = Tr,$$

d.h. die Homomorphismen des Diagramms sind  $G(\mathbb{C}|\mathbb{R})$ -Homomorphismen. Wir gehen jetzt überall wieder zu den Fixmoduln unter der  $G(\mathbb{C}|\mathbb{R})$ -Operation über und erhalten das Diagramm

$$\begin{array}{ccccc} K^* & \xrightarrow{j} & K_{\mathbb{R}}^* & \xrightarrow{l} & [\prod_{\tau} \mathbb{R}]^+ \\ N_{K|\mathbb{Q}} \downarrow & & \downarrow N & & \downarrow Tr \\ \mathbb{Q}^* & \longrightarrow & \mathbb{R}^* & \xrightarrow{l} & \mathbb{R} \end{array}.$$

Der  $\mathbb{R}$ -Vektorraum  $[\prod_{\tau} \mathbb{R}]^+$  ist explizit wie folgt gegeben. Wir teilen die Einbettungen  $\tau : K \rightarrow \mathbb{C}$  wieder in die reellen  $\rho_1, \dots, \rho_r$  und die Paare  $\sigma_1, \bar{\sigma}_1, \dots, \sigma_s, \bar{\sigma}_s$  komplex konjugierter ein und erhalten wie zuvor bei  $[\prod_{\tau} \mathbb{C}]^+$  eine Zerlegung

$$[\prod_{\tau} \mathbb{R}]^+ = \prod_{\rho} \mathbb{R} \times \prod_{\sigma} [\mathbb{R} \times \mathbb{R}]^+.$$

Der Faktor  $[\mathbb{R} \times \mathbb{R}]^+$  besteht jetzt aus den Punkten  $(x, x)$ , und wir identifizieren ihn mit  $\mathbb{R}$  durch die Zuordnung  $(x, x) \mapsto 2x$ . Auf diese Weise erhalten wir einen Isomorphismus

$$[\prod_{\tau} \mathbb{R}]^+ \cong \mathbb{R}^{r+s},$$

bei dem die Abbildung  $Tr : [\prod_{\tau} \mathbb{R}]^+ \rightarrow \mathbb{R}$  wieder in die Abbildung

$$Tr : \mathbb{R}^{r+s} \rightarrow \mathbb{R}$$

übergeht, die durch die Summe der Koordinaten gegeben ist. Nach der Identifizierung  $[\prod_{\tau} \mathbb{R}]^+ = \mathbb{R}^{r+s}$  wird der Homomorphismus

$$l : K_{\mathbb{R}}^* \rightarrow \mathbb{R}^{r+s}$$

durch

$$l(x) = (\log |x_{\rho_1}|, \dots, \log |x_{\rho_r}|, \log |x_{\sigma_1}|^2, \dots, \log |x_{\sigma_s}|^2)$$

gegeben, wenn  $x \in K_{\mathbb{R}}^* \subseteq \prod_{\tau} \mathbb{C}^*$  in der Form  $x = (x_{\tau})$  geschrieben wird.

**Aufgabe 1.** Man gebe eine nur von  $K$  abhängige Konstante  $A$  an, so daß jedes ganze Ideal  $\mathfrak{a} \neq 0$  von  $K$  ein Element  $a \neq 0$  enthält mit

$$|\tau a| < A(\mathfrak{o}_K : \mathfrak{a})^{1/n} \quad \text{für alle } \tau \in \text{Hom}(K, \mathbb{C}), n = [K : \mathbb{Q}].$$

**Aufgabe 2.** Zeige, daß die konvexe und zentralsymmetrische Menge

$$X = \{(z_{\tau}) \in K_{\mathbb{R}} \mid \sum_{\tau} |z_{\tau}| < t\}$$

das Volumen  $\text{vol}(X) = 2^r \pi^s \frac{t^n}{n!}$  hat (vgl. III, (2.14)).

**Aufgabe 3.** Zeige, daß es in jedem Ideal  $\mathfrak{a} \neq 0$  von  $\mathfrak{o}_K$  ein  $a \neq 0$  gibt mit

$$|N_{K|\mathbb{Q}}(a)| \leq M(\mathfrak{o}_K : \mathfrak{a}),$$

wobei  $M = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}$  (die **Minkowski-Schranke**).

**Hinweis:** Man gehe mit Hilfe von Aufgabe 2 wie bei (5.3) vor und verwende die Ungleichung zwischen arithmetischem und geometrischem Mittel,

$$\frac{1}{n} \sum_{\tau} |z_{\tau}| \geq (\prod_{\tau} |z_{\tau}|)^{1/n}.$$

## § 6. Die Klassenzahl

Als erste Anwendung der Minkowski-Theorie wollen wir zeigen, daß die Idealklassengruppe  $Cl_K = J_K/P_K$  eines algebraischen Zahlkörpers  $K$  endlich ist. Um die Ideale  $\mathfrak{a} \neq 0$  des Ringes  $\mathfrak{o}_K$  zählen zu können, betrachten wir ihre **Absolutnorm**

$$\mathfrak{N}(\mathfrak{a}) = (\mathfrak{o}_K : \mathfrak{a}).$$

(Der Fall des Nullideals  $\mathfrak{a} = 0$  ist in dem ganzen Buch häufig stillschweigend ausgeschlossen, wenn er augenfälligerweise keinen Sinn ergibt.) Der

Index ist nach (2.12) endlich, und der Name rechtfertigt sich durch den Sonderfall eines Hauptideals  $(\alpha)$  von  $\mathcal{O}_K$ , für den die Gleichung

$$\mathfrak{N}((\alpha)) = |N_{K|\mathbb{Q}}(\alpha)|$$

gilt. In der Tat, ist  $\omega_1, \dots, \omega_n$  eine  $\mathbb{Z}$ -Basis von  $\mathcal{O}_K$ , so ist  $\alpha\omega_1, \dots, \alpha\omega_n$  eine  $\mathbb{Z}$ -Basis von  $(\alpha) = \alpha\mathcal{O}_K$ , und wenn  $A = (a_{ij})$  die Übergangsmatrix ist,  $\alpha\omega_i = \sum a_{ij}\omega_j$ , so ist, wie schon in § 2 bemerkt, einerseits  $|\det(A)| = (\mathcal{O}_K : (\alpha))$  und andererseits  $\det(A) = N_{K|\mathbb{Q}}(\alpha)$  nach Definition.

**(6.1) Satz.** Ist  $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_r^{\nu_r}$  die Primzerlegung eines Ideals  $\mathfrak{a} \neq 0$ , so gilt

$$\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{p}_1)^{\nu_1} \cdots \mathfrak{N}(\mathfrak{p}_r)^{\nu_r}.$$

**Beweis:** Nach dem chinesischen Restsatz (3.6) ist

$$\mathcal{O}_K/\mathfrak{a} = \mathcal{O}_K/\mathfrak{p}_1^{\nu_1} \oplus \cdots \oplus \mathcal{O}_K/\mathfrak{p}_r^{\nu_r},$$

so daß wir weiterhin  $\mathfrak{a}$  als eine Primidealpotenz  $\mathfrak{p}^\nu$  annehmen dürfen. In der Kette

$$\mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \cdots \supseteq \mathfrak{p}^\nu$$

ist  $\mathfrak{p}^i \neq \mathfrak{p}^{i+1}$  wegen der eindeutigen Primzerlegung, und jeder Quotient  $\mathfrak{p}^i/\mathfrak{p}^{i+1}$  ist ein  $\mathcal{O}_K/\mathfrak{p}$ -Vektorraum der Dimension 1. In der Tat, ist  $a \in \mathfrak{p}^i \setminus \mathfrak{p}^{i+1}$  und  $\mathfrak{b} = (a) + \mathfrak{p}^{i+1}$ , so ist  $\mathfrak{p}^i \supseteq \mathfrak{b} \supsetneq \mathfrak{p}^{i+1}$  und folglich  $\mathfrak{p}^i = \mathfrak{b}$ ,

weil sonst  $\mathfrak{b}' = \mathfrak{b}\mathfrak{p}^{-i}$  ein echter Teiler von  $\mathfrak{p} = \mathfrak{p}^{i+1}\mathfrak{p}^{-i}$  wäre. Daher bildet  $\bar{a} = a \bmod \mathfrak{p}^{i+1}$  eine Basis des  $\mathcal{O}_K/\mathfrak{p}$ -Vektorraums  $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ . Wir haben also  $\mathfrak{p}^i/\mathfrak{p}^{i+1} \cong \mathcal{O}_K/\mathfrak{p}$  und somit

$$\mathfrak{N}(\mathfrak{p}^\nu) = (\mathcal{O}_K : \mathfrak{p}^\nu) = (\mathcal{O}_K : \mathfrak{p})(\mathfrak{p} : \mathfrak{p}^2) \cdots (\mathfrak{p}^{\nu-1} : \mathfrak{p}^\nu) = \mathfrak{N}(\mathfrak{p})^\nu. \quad \square$$

Aus dem Satz folgt unmittelbar die Multiplikativität

$$\mathfrak{N}(\mathfrak{a}\mathfrak{b}) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b})$$

der Absolutnorm. Sie setzt sich daher zu einem Homomorphismus

$$\mathfrak{N} : J_K \rightarrow \mathbb{R}_+^*$$

auf alle gebrochenen Ideale  $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}}$ ,  $\nu_{\mathfrak{p}} \in \mathbb{Z}$ , fort. Das folgende, sich aus (5.3) ergebende Lemma ist für die Endlichkeit der Idealklassengruppe entscheidend.

**(6.2) Lemma.** In jedem Ideal  $\mathfrak{a} \neq 0$  von  $\mathcal{O}_K$  gibt es ein  $a \in \mathfrak{a}$ ,  $a \neq 0$ , mit

$$|N_{K|\mathbb{Q}}(a)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|} \mathfrak{N}(\mathfrak{a}).$$

**Beweis:** Zu vorgegebenem  $\varepsilon > 0$  wählen wir positive reelle Zahlen  $c_\tau$ ,  $\tau \in \text{Hom}(K, \mathbb{C})$ , mit  $c_\tau = c_{\bar{\tau}}$  und

$$\prod_{\tau} c_\tau = \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|} \mathfrak{N}(\mathfrak{a}) + \varepsilon$$

und finden nach (5.3) ein Element  $a \in \mathfrak{a}$ ,  $a \neq 0$ , mit  $|\tau a| < c_\tau$ , also

$$|N_{K|\mathbb{Q}}(a)| = \prod_{\tau} |\tau a| < \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|} \mathfrak{N}(\mathfrak{a}) + \varepsilon.$$

Da dies für alle  $\varepsilon > 0$  gilt und da  $|N_{K|\mathbb{Q}}(a)|$  stets eine natürliche Zahl ist, so muß es auch ein  $a \in \mathfrak{a}$ ,  $a \neq 0$ , geben mit

$$|N_{K|\mathbb{Q}}(a)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|} \mathfrak{N}(\mathfrak{a}). \quad \square$$

**(6.3) Theorem.** Die Idealklassengruppe  $Cl_K = J_K/P_K$  ist endlich. Ihre Ordnung

$$h_K = (J_K : P_K)$$

heißt die **Klassenzahl** von  $K$ .

**Beweis:** Ist  $\mathfrak{p} \neq 0$  ein Primideal von  $\mathcal{O}_K$  und  $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ , so ist  $\mathcal{O}_K/\mathfrak{p}$  eine endliche Erweiterung von  $\mathbb{Z}/p\mathbb{Z}$  von einem Grad  $f \geq 1$ , und es ist

$$\mathfrak{N}(\mathfrak{p}) = p^f.$$

Bei festem  $p$  gibt es nur endlich viele Primideale  $\mathfrak{p}$  mit  $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$  wegen  $\mathfrak{p}|(p)$ . Daher gibt es nur endlich viele Primideale  $\mathfrak{p}$  mit beschränkter Absolutnorm. Da jedes ganze Ideal eine Darstellung  $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \dots \mathfrak{p}_r^{\nu_r}$  mit  $\nu_i > 0$  und

$$\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{p}_1)^{\nu_1} \dots \mathfrak{N}(\mathfrak{p}_r)^{\nu_r}$$

besitzt, gibt es überhaupt nur endlich viele Ideale  $\mathfrak{a}$  von  $\mathcal{O}_K$  mit beschränkter Absolutnorm  $\mathfrak{N}(\mathfrak{a}) \leq M$ .

Es genügt hiernach zu zeigen, daß jede Klasse  $[\mathfrak{a}] \in Cl_K$  ein ganzes Ideal  $\mathfrak{a}_1$  enthält mit

$$\mathfrak{N}(\mathfrak{a}_1) \leq M = \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}.$$

Wir wählen dazu einen beliebigen Repräsentanten  $\mathfrak{a}$  der Klasse und ein  $\gamma \in \mathcal{O}_K$ ,  $\gamma \neq 0$ , mit  $\mathfrak{b} = \gamma \mathfrak{a}^{-1} \subseteq \mathcal{O}_K$ . Nach (6.2) gibt es dann ein  $\alpha \in \mathfrak{b}$ ,  $\alpha \neq 0$ , mit

$$|N_{K|\mathbb{Q}}(\alpha)| \cdot \mathfrak{N}(\mathfrak{b})^{-1} = \mathfrak{N}((\alpha)\mathfrak{b}^{-1}) = \mathfrak{N}(\alpha\mathfrak{b}^{-1}) \leq M.$$

Das Ideal  $\mathfrak{a}_1 = \alpha\mathfrak{b}^{-1} = \alpha\gamma^{-1}\mathfrak{a} \in [\mathfrak{a}]$  hat demnach die gewünschte Eigenschaft.  $\square$

Der Satz von der Endlichkeit der Klassenzahl  $h_K$  bringt zum Ausdruck, daß uns der Übergang von den Zahlen zu den Idealen nicht ins Uferlose geführt hat. Der günstigste Fall liegt natürlich vor, wenn  $h_K = 1$  ist. Dies ist gleichbedeutend damit, daß  $\mathcal{O}_K$  ein Hauptidealring ist, d.h. daß der Satz von der eindeutigen Primzerlegung im klassischen Sinne gilt. In aller Regel ist jedoch  $h_K > 1$ . Es ist z.B. inzwischen bekannt, daß die imaginär-quadratischen Zahlkörper  $\mathbb{Q}(\sqrt{d})$ ,  $d$  quadratfrei und  $< 0$ , nur für die neun Werte

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163$$

die Klassenzahl 1 haben. Die reell-quadratischen Zahlkörper neigen eher zur Klassenzahl 1. Im Bereich  $2 \leq d < 100$  sind sie durch die Werte

$$\begin{aligned} d = & 2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 31, 33, 37, \\ & 38, 41, 43, 46, 47, 53, 57, 59, 61, 62, 67, 69, 71, 73, 77, \\ & 83, 86, 89, 93, 94, 97 \end{aligned}$$

gegeben. Es wird vermutet, daß es unendlich viele reell-quadratische Zahlkörper mit der Klassenzahl 1 gibt, jedoch weiß man bis heute nicht einmal, ob es unendlich viele unter schlechthin allen Zahlkörpern gibt. Durch zahllose Untersuchungen ist immer wieder bestätigt worden, daß die Idealklassengruppen  $Cl_K$  nach Größe und Struktur ganz beliebig und ganz regellos ausfallen. Eine Ausnahme von dieser Regellosigkeit bildet eine Entdeckung von *KENKICHI IWASAWA*, wonach die Klassenzahl des Körpers der  $p^n$ -ten Einheitswurzeln hinsichtlich der  $p$ -Teilbarkeit bei laufendem  $n$  einem strengen Gesetz gehorcht (vgl. [136], Th. 13.13).

Im Falle des Körpers der  $p$ -ten Einheitswurzeln hat die Frage nach der Teilbarkeit seiner Klassenzahl durch  $p$  eine hervorragende Sonderrolle gespielt. Sie ist nämlich aufs engste mit der berühmten **Fermatschen Vermutung** verknüpft, nach der die Gleichung

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

für  $p \geq 3$  in ganzen Zahlen  $\neq 0$  unlösbar ist. Ähnlich wie die Quadratsummen  $x^2 + y^2 = (x + iy)(x - iy)$  auf das Studium der Gaußschen

Zahlen geführt haben, so führt die Zerlegung von  $x^p + y^p$  mit Hilfe einer  $p$ -ten Einheitswurzel  $\zeta \neq 1$  auf ein Problem im Ring  $\mathbb{Z}[\zeta]$  der ganzen Zahlen von  $\mathbb{Q}(\zeta)$ . Die Gleichung  $y^p = z^p - x^p$  verwandelt sich dort in die Gleichheit

$$y \cdot y \cdot \dots \cdot y = (z - x)(z - \zeta x) \cdot \dots \cdot (z - \zeta^{p-1}x),$$

d.h. man erhält unter der Annahme der Lösbarkeit zwei multiplikative Zerlegungen ein und derselben Zahl in  $\mathbb{Z}[\zeta]$ . Man kann nun zeigen, daß dies der eindeutigen Primzerlegung widerspricht, vorausgesetzt, daß sie im Ring  $\mathbb{Z}[\zeta]$  gilt. Unter der irrigen Annahme, daß dies im allgemeinen der Fall ist, daß also die Klassenzahl  $h_p$  des Körpers  $\mathbb{Q}(\zeta)$  gleich 1 ist, hat man in der Tat geglaubt, die Fermatsche Vermutung auf diese Weise bewiesen zu haben. Nicht jedoch *KUMMER*, wie lange Zeit behauptet wurde. Er bewies vielmehr, daß sich die oben angedeutete Schlußweise retten läßt, wenn man anstelle von  $h_p = 1$  nur  $p \nmid h_p$  voraussetzt. Die Primzahl  $p$  nannte er in diesem Fall **regulär**, sonst **irregulär**. Er zeigte sogar, daß  $p$  genau dann regulär ist, wenn die Zähler der **Bernoulli-schen Zahlen**  $B_2, B_4, \dots, B_{p-3}$  nicht durch  $p$  teilbar sind. Unter den ersten 25 Primzahlen  $< 100$  sind nur drei irregulär, 37, 59, 67. Man weiß aber bis heute nicht, ob es unendlich viele reguläre Primzahlen gibt. Dagegen haben kürzlich die Mathematiker *L.M. ADLEMAN*, *D.R. HEATH-BROWN* und *E. FOUVRY* die Fermatsche Vermutung für unendlich viele  $p$  im „ersten Fall“ bewiesen (vgl. [1]), d.h. unter der Voraussetzung  $p \nmid xyz$ . Aufgrund von Computerberechnungen kennt man ihre Gültigkeit für alle Primzahlen  $< 125000$ .

Für eine genauere Erörterung der angedeuteten Beziehung der Klassengruppen zur Fermatschen Vermutung verweisen wir auf [14].

**Aufgabe 1.** Wie viele ganze Ideale  $\mathfrak{a}$  gibt es mit gegebener Norm  $\mathfrak{N}(\mathfrak{a}) = n$ ?

**Aufgabe 2.** Zeige, daß die quadratischen Zahlkörper mit der Diskriminante 5, 8, 11, -3, -4, -7, -8, -11 die Klassenzahl 1 haben.

**Aufgabe 3.** Zeige, daß es in jeder Idealklasse eines Zahlkörpers  $K$  vom Grade  $n$  ein ganzes Ideal  $\mathfrak{a}$  gibt mit

$$\mathfrak{N}(\mathfrak{a}) \leq \frac{n!}{n^n} \left( \frac{4}{\pi} \right)^s \sqrt{|d_K|}.$$

**Hinweis:** Unter Benutzung von Aufgabe 3, § 5, verfähre man wie im Beweis zu (6.3).

**Aufgabe 4.** Zeige, daß der Diskriminantenbetrag  $|d_K| > 1$  ist für jeden algebraischen Zahlkörper  $K \neq \mathbb{Q}$  (Minkowskischer Diskriminantensatz, vgl. Kap. III, (2.17)).



**Aufgabe 5.** Zeige, daß der Diskriminantenbetrag  $|d_K|$  mit dem Körpergrad  $n$  gegen  $\infty$  geht.

**Aufgabe 6.** Sei  $\mathfrak{a}$  ein ganzes Ideal von  $K$  und  $\mathfrak{a}^m = (a)$ . Zeige, daß  $\mathfrak{a}$  im Körper  $L = K(\sqrt[m]{a})$  ein Hauptideal wird, d.h.  $\mathfrak{a} \mathcal{O}_L = (\alpha)$ .

**Aufgabe 7.** Zeige, daß es zu jedem Zahlkörper  $K$  eine endliche Erweiterung  $L$  gibt, in der jedes Ideal von  $K$  ein Hauptideal wird.

## § 7. Der Dirichletsche Einheitsatz

Nach der Idealklassengruppe  $Cl_K$  wenden wir uns nun der zweiten Hauptaufgabe zu, die uns der Ring  $\mathcal{O}_K$  der ganzen Zahlen eines algebraischen Zahlkörpers  $K$  stellt, der Einheitengruppe  $\mathcal{O}_K^*$ . Sie enthält die endliche Gruppe  $\mu(K)$  der in  $K$  gelegenen Einheitswurzeln, ist aber im allgemeinen nicht selbst endlich. Ihre Größe richtet sich vielmehr nach der Anzahl  $r$  der reellen Einbettungen  $\rho : K \rightarrow \mathbb{R}$  und der Anzahl  $s$  der Paare  $\sigma, \bar{\sigma} : K \rightarrow \mathbb{C}$  komplex konjugierter Einbettungen. Zu ihrer Beschreibung ziehen wir das in § 5 bereitgestellte Diagramm

$$\begin{array}{ccccc} K^* & \xrightarrow{j} & K_{\mathbb{R}}^* & \xrightarrow{l} & [\prod_{\tau} \mathbb{R}]^+ \\ N_{K|\mathbb{Q}} \downarrow & & \downarrow N & & \downarrow Tr \\ \mathbb{Q}^* & \longrightarrow & \mathbb{R}^* & \xrightarrow{\log | \cdot |} & \mathbb{R} \end{array}$$

heran. Im oberen Teil dieses Diagramms betrachten wir die Untergruppen

$$\begin{aligned} \mathcal{O}_K^* &= \{\varepsilon \in \mathcal{O}_K \mid N_{K|\mathbb{Q}}(\varepsilon) = \pm 1\}, & \text{die Einheitengruppe,} \\ S &= \{y \in K_{\mathbb{R}}^* \mid N(y) = \pm 1\}, & \text{die „Norm-Eins-Fläche“,} \\ H &= \{x \in [\prod_{\tau} \mathbb{R}]^+ \mid Tr(x) = 0\}, & \text{die „Spur-Null-Hyperebene“.} \end{aligned}$$

Wir erhalten die Homomorphismen

$$\mathcal{O}_K^* \xrightarrow{j} S \xrightarrow{l} H$$

und das Kompositum  $\lambda := l \circ j : \mathcal{O}_K^* \rightarrow H$ . Wir bezeichnen das Bild mit

$$\Gamma = \lambda(\mathcal{O}_K^*) \subseteq H$$

und erhalten den

**(7.1) Satz.** Die Sequenz

$$1 \rightarrow \mu(K) \rightarrow \mathcal{O}_K^* \xrightarrow{\lambda} \Gamma \rightarrow 0$$

ist exakt.

**Beweis:** Zu zeigen ist, daß  $\mu(K)$  der Kern von  $\lambda$  ist. Ist nun  $\zeta \in \mu(K)$  und  $\tau : K \rightarrow \mathbb{C}$  eine Einbettung, so ist  $\log |\tau \zeta| = \log 1 = 0$ , also jedenfalls  $\mu(K) \subseteq \text{Ker}(\lambda)$ . Sei umgekehrt  $\varepsilon \in \mathcal{O}_K^*$  ein Element im Kern,  $\lambda(\varepsilon) = l(j\varepsilon) = 0$ . Dies bedeutet, daß  $|\tau \varepsilon| = 1$  ist für jede Einbettung  $\tau : K \rightarrow \mathbb{C}$ , d.h. daß  $j\varepsilon = (\tau \varepsilon)$  in einem beschränkten Bereich des  $\mathbb{R}$ -Vektorraums  $K_{\mathbb{R}}$  liegt. Andererseits aber ist  $j\varepsilon$  ein Punkt des Gitters  $j\mathcal{O}_K$  von  $K_{\mathbb{R}}$  (vgl. (5.2)). Daher kann der Kern von  $\lambda$  nur endlich viele Elemente enthalten, besteht also als endliche Untergruppe von  $K^*$  aus lauter Einheitswurzeln.  $\square$

Hiernach kommt alles auf die Bestimmung der Gruppe  $\Gamma$  an. Wir benötigen dazu das folgende

**(7.2) Lemma.** *Bis auf Assoziierte gibt es nur endlich viele Elemente  $\alpha \in \mathcal{O}_K$  mit gegebener Norm  $N_{K|\mathbb{Q}}(\alpha) = a$ .*

**Beweis:** Sei  $a \in \mathbb{Z}$ ,  $a > 1$ . In jeder der endlich vielen Nebenklassen von  $\mathcal{O}_K/a\mathcal{O}_K$  gibt es bis auf Assoziierte höchstens ein Element  $\alpha$  mit  $|N(\alpha)| = |N_{K|\mathbb{Q}}(\alpha)| = a$ . Ist nämlich  $\beta = \alpha + a\gamma$ ,  $\gamma \in \mathcal{O}_K$ , ein zweites, so ist

$$\frac{\alpha}{\beta} = 1 \pm \frac{N(\beta)}{\beta} \gamma \in \mathcal{O}_K$$

wegen  $N(\beta)/\beta \in \mathcal{O}_K$ , und entsprechend  $\frac{\beta}{\alpha} = 1 \pm \frac{N(\alpha)}{\alpha} \gamma \in \mathcal{O}_K$ , d.h.  $\beta$  ist zu  $\alpha$  assoziiert. Daher gibt es bis auf Assoziierte höchstens  $(\mathcal{O}_K : a\mathcal{O}_K)$  Elemente mit der Norm  $\pm a$ .  $\square$

**(7.3) Satz.** *Die Gruppe  $\Gamma$  ist ein vollständiges Gitter im  $(r + s - 1)$ -dimensionalen Vektorraum  $H$ , ist also isomorph zu  $\mathbb{Z}^{r+s-1}$ .*

**Beweis:** Wir zeigen zuerst, daß  $\Gamma = \lambda(\mathcal{O}_K^*)$  ein Gitter in  $H$ , d.h. eine diskrete Untergruppe ist. Die Abbildung  $\lambda : \mathcal{O}_K^* \rightarrow H$  entsteht durch Einschränkung der Abbildung

$$K^* \xrightarrow{j} \prod_{\tau} \mathbb{C}^* \xrightarrow{l} \prod_{\tau} \mathbb{R},$$

und es genügt zu zeigen, daß der beschränkte Bereich  $\{(x_{\tau}) \in \prod_{\tau} \mathbb{R} \mid |x_{\tau}| \leq c\}$  für jedes  $c > 0$  nur endlich viele Punkte von  $\Gamma = l(j\mathcal{O}_K^*)$

enthält. Das Urbild dieses Bereiches unter  $l$  ist der beschränkte Bereich

$$\{(z_\tau) \in \prod_\tau \mathbb{C}^* \mid e^{-c} \leq |z_\tau| \leq e^c\}$$

wegen  $l((z_\tau)) = (\log |z_\tau|)$ . Dieser enthält aber nur endlich viele Elemente der Menge  $j\mathcal{O}_K^*$ , weil sie Teilmenge des Gitters  $j\mathcal{O}_K$  in  $[\prod_\tau \mathbb{C}]^+$  ist (vgl. (5.2)). Daher ist  $\Gamma$  ein Gitter.

Wir beweisen nun, daß  $\Gamma$  ein vollständiges Gitter in  $H$  ist. Hierin besteht die Hauptaussage des Satzes. Wir ziehen dazu das Kriterium (4.3) heran, wonach wir eine beschränkte Menge  $M \subseteq H$  finden müssen, derart daß

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

Wir konstruieren die Menge, indem wir ihr Urbild unter dem surjektiven Homomorphismus

$$l : S \rightarrow H$$

angeben, genauer konstruieren wir eine beschränkte Menge  $T$  in der Norm-Eins-Fläche  $S$ , deren *multiplikative* Verschiebungen  $Tj\varepsilon$ ,  $\varepsilon \in \mathcal{O}_K^*$ , ganz  $S$  überdecken:

$$S = \bigcup_{\varepsilon \in \mathcal{O}_K^*} Tj\varepsilon.$$

Für  $x = (x_\tau) \in T$  sind dann die Beträge  $|x_\tau|$  wegen  $\prod_\tau |x_\tau| = 1$  sowohl nach oben als auch nach unten gegen Null beschränkt, so daß auch  $M = l(T)$  beschränkt ist. Wir wählen reelle Zahlen  $c_\tau > 0$ ,  $\tau \in \text{Hom}(K, \mathbb{C})$ , mit  $c_\tau = c_{\bar{\tau}}$  und

$$C = \prod_\tau c_\tau > \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$$

und betrachten die Menge

$$X = \{(z_\tau) \in K_{\mathbb{R}} \mid |z_\tau| < c_\tau\}.$$

Für einen beliebigen Punkt  $y = (y_\tau) \in S$  ist dann

$$Xy = \{(z_\tau) \in K_{\mathbb{R}} \mid |z_\tau| < c'_\tau\}$$

mit  $c'_\tau = c_\tau |y_\tau|$ , und es gilt  $c'_\tau = c'_{\bar{\tau}}$  und  $\prod_\tau c'_\tau = \prod_\tau c_\tau = C$  wegen  $\prod_\tau |y_\tau| = |N(y)| = 1$ . Nach (5.3) gibt es daher einen Punkt

$$ja = (\tau a) \in Xy, \quad a \in \mathcal{O}_K, \quad a \neq 0.$$

Wir können nun nach Lemma (7.2) ein System  $\alpha_1, \dots, \alpha_N \in \mathcal{O}_K$ ,  $\alpha_i \neq 0$ , fixieren mit der Eigenschaft, daß jedes  $a \in \mathcal{O}_K$ ,  $a \neq 0$ , mit  $|N_{K|\mathbb{Q}}(a)| \leq C$  zu einer dieser Zahlen assoziiert ist. Die Menge

$$T = S \cap \bigcup_{i=1}^N X(j\alpha_i)^{-1}$$

hat dann die gewünschte Eigenschaft: Da  $X$  beschränkt ist, ist auch  $X(j\alpha_i)^{-1}$  und damit  $T$  beschränkt, und es gilt

$$S = \bigcup_{\varepsilon \in \mathcal{O}_K^*} Tj\varepsilon.$$

In der Tat, ist  $y \in S$ , so finden wir nach dem Obigen ein  $a \in \mathcal{O}_K$ ,  $a \neq 0$ , mit  $ja \in Xy^{-1}$ , also  $ja = xy^{-1}$ ,  $x \in X$ . Wegen

$$|N_{K|\mathbb{Q}}(a)| = |N(xy^{-1})| = |N(x)| < \prod_{\tau} c_{\tau} = C$$

ist  $a$  zu einem  $\alpha_i$  assoziiert,  $\alpha_i = \varepsilon a$ ,  $\varepsilon \in \mathcal{O}_K^*$ . Es folgt

$$y = xja^{-1} = xj(\alpha_i^{-1}\varepsilon).$$

Wegen  $y, j\varepsilon \in S$  ist  $xj\alpha_i^{-1} \in S \cap Xj\alpha_i^{-1} \subseteq T$ , also  $y \in Tj\varepsilon$ . □

Aus den Sätzen (7.1) und (7.3) ergibt sich unmittelbar der **Dirichletsche Einheitsensatz** in seiner klassischen Form.

**(7.4) Theorem.** *Die Einheitengruppe  $\mathcal{O}_K^*$  von  $\mathcal{O}_K$  ist das direkte Produkt der endlichen zyklischen Gruppe  $\mu(K)$  und einer freien abelschen Gruppe vom Rang  $r + s - 1$ .*

Mit anderen Worten: Es gibt Einheiten  $\varepsilon_1, \dots, \varepsilon_t$ ,  $t = r + s - 1$ , **Grundeinheiten** genannt, derart daß sich jede weitere Einheit  $\varepsilon$  eindeutig als ein Produkt

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

mit einer Einheitswurzel  $\zeta$  und ganzen Zahlen  $\nu_i$  ausdrücken läßt.

**Beweis:** In der exakten Sequenz

$$1 \rightarrow \mu(K) \rightarrow \mathcal{O}_K^* \xrightarrow{\lambda} \Gamma \rightarrow 0$$

ist  $\Gamma$  nach (7.3) eine freie abelsche Gruppe vom Rang  $t = r + s - 1$ . Ist  $v_1, \dots, v_t$  eine  $\mathbb{Z}$ -Basis von  $\Gamma$ , und sind  $\varepsilon_1, \dots, \varepsilon_t \in \mathcal{O}_K^*$  Urbilder der  $v_i$  und  $A \subseteq \mathcal{O}_K^*$  die durch die  $\varepsilon_i$  erzeugte Untergruppe, so wird  $A$  durch  $\lambda$  isomorph auf  $\Gamma$  abgebildet, d.h. es ist  $\mu(K) \cap A = \{1\}$  und also  $\mathcal{O}_K^* = \mu(K) \times A$ . □

Nach der Identifizierung  $[\prod_{\tau} \mathbb{R}]^+ = \mathbb{R}^{r+s}$  (vgl. § 5, S. 35) wird  $H$  ein Unterraum des euklidischen Raumes  $\mathbb{R}^{r+s}$  und ist somit selbst

ein euklidischer Raum. Wir können daher vom Grundmascheninhalt  $\text{vol}(\lambda(\mathcal{O}_K^*))$  des Einheitengitters  $\Gamma = \lambda(\mathcal{O}_K^*) \subseteq H$  sprechen und wollen diesen berechnen. Sei  $\varepsilon_1, \dots, \varepsilon_t$ ,  $t = r + s - 1$ , ein System von Grundeinheiten und  $\Phi$  die von den Vektoren  $\lambda(\varepsilon_1), \dots, \lambda(\varepsilon_t) \in H$  aufgespannte Grundmasche des Einheitengitters  $\lambda(\mathcal{O}_K^*)$ . Der Vektor

$$\lambda_0 = \frac{1}{\sqrt{r+s}} (1, \dots, 1) \in \mathbb{R}^{r+s}$$

ist offensichtlich orthogonal zu  $H$  und hat die Länge 1. Daher ist der  $t$ -dimensionale Inhalt von  $\Phi$  gleich dem  $(t+1)$ -dimensionalen Inhalt des von  $\lambda_0, \lambda(\varepsilon_1), \dots, \lambda(\varepsilon_t)$  aufgespannten Parallelepipedes in  $\mathbb{R}^{t+1}$ . Dieses aber hat den Inhalt

$$\pm \det \begin{pmatrix} \lambda_{01} & \lambda_1(\varepsilon_1) & \cdots & \lambda_1(\varepsilon_t) \\ \vdots & \vdots & & \vdots \\ \lambda_{0t+1} & \lambda_{t+1}(\varepsilon_1) & \cdots & \lambda_{t+1}(\varepsilon_t) \end{pmatrix}.$$

Addieren wir alle Zeilen zu einer festgewählten, etwa der  $i$ -ten, so stellen sich in dieser lauter Nullen ein bis auf die erste Komponente, welche gleich  $r + s$  ist. Daher ergibt sich der

**(7.5) Satz.** *Der Grundmascheninhalt des Einheitengitters  $\lambda(\mathcal{O}_K^*)$  in  $H$  ist*

$$\text{vol}(\lambda(\mathcal{O}_K^*)) = \sqrt{r+s} R,$$

wobei  $R$  der Determinantenbetrag eines beliebigen Minors vom Rang  $t = r + s - 1$  der Matrix

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

ist. Dieser Determinantenbetrag  $R$  heißt der **Regulator** des Körpers  $K$ .

Der Regulator wird erst später seine Wichtigkeit zeigen (vgl. Kap. VII, § 5).

**Aufgabe 1.** Sei  $D > 1$  eine quadratfreie ganze Zahl und  $d$  die Diskriminante des reell-quadratischen Zahlkörpers  $K = \mathbb{Q}(\sqrt{D})$  (vgl. § 2, Aufgabe 4). Sei  $x_1, y_1$  diejenige eindeutig bestimmte ganzrationale Lösung der Gleichung

$$x^2 - dy^2 = -4,$$

bzw. – falls diese Gleichung ganzrational unlösbar ist – der Gleichung

$$x^2 - dy^2 = 4,$$

für die  $x_1, y_1 > 0$  möglichst klein sind. Dann ist

$$\varepsilon_1 = \frac{x_1 + y_1\sqrt{d}}{2}$$

eine Grundeinheit von  $K$ . (Die Doppelgleichung  $x^2 - dy^2 = \pm 4$  wird die **Pellsche Gleichung** genannt.)

**Aufgabe 2.** Verifiziere die folgende Tabelle für die Grundeinheit  $\varepsilon_1$  in  $\mathbb{Q}(\sqrt{D})$ :

$D$	2	3	5	6	7	10
$\varepsilon_1$	$1 + \sqrt{2}$	$2 + \sqrt{3}$	$(1 + \sqrt{5})/2$	$5 + 2\sqrt{6}$	$8 + 3\sqrt{7}$	$3 + \sqrt{10}$

**Hinweis:** Man prüfe der Reihe nach mit  $y = 1, 2, 3, \dots$ , ob eine der beiden Zahlen  $dy^2 \mp 4$  ein Quadrat  $x^2$  ist. Nach dem Einheitensatz muß dies – mit dem Pluszeichen – sicher einmal auftreten. Man gebe aber für jedes einzelne  $y$  dem Minuszeichen den Vorrang. Der in dieser Rangordnung erste Fall mit  $dy_1^2 \mp 4 = x_1^2$  liefert die Grundeinheit  $\varepsilon_1 = (x_1 + y_1\sqrt{d})/2$ .

**Aufgabe 3. Die Schlacht von Hastings** (14.10.1066).

Harolds Mannen standen nach alter Gewohnheit dichtgedrängt in 13 gleichgroßen Quadraten aufgestellt, und wehe dem Normannen, der es wagte, in eine solche Phalanx einbrechen zu wollen. ... Als aber Harold selbst auf dem Schlachtfeld erschien, formten die Sachsen ein einziges gewaltiges Quadrat mit ihrem König an der Spitze und stürmten mit den Schlachtrufen „Ut!“, „Olicrosse!“, „Godemite!“ vorwärts. ... (vgl. „*Carmen de Hastingae Proelio*“ von Guy, Bischof von Amiens).

**Frage:** Wie groß soll die Armee Harolds II. gewesen sein?

Mitgeteilt von W.-D. GEYER.

**Aufgabe 4.** Sei  $\zeta$  eine primitive  $p$ -te Einheitswurzel,  $p$  eine ungerade Primzahl. Zeige, daß  $\mathbb{Z}[\zeta]^* = (\zeta)\mathbb{Z}[\zeta + \zeta^{-1}]^*$ .

Zeige, daß  $\mathbb{Z}[\zeta]^* = \{\pm\zeta^k(1 + \zeta)^n \mid 0 \leq k < 5, n \in \mathbb{Z}\}$ , wenn  $p = 5$ .

**Aufgabe 5.** Sei  $\zeta$  eine primitive  $m$ -te Einheitswurzel,  $m \geq 3$ . Zeige, daß die Zahlen  $\frac{1 - \zeta^k}{1 - \zeta}$  für  $(k, m) = 1$  Einheiten im Ring der ganzen Zahlen des Körpers  $\mathbb{Q}(\zeta)$  sind. Die durch sie erzeugte Untergruppe der Einheitengruppe heißt die Gruppe der **Kreiseinheiten**.

**Aufgabe 6.** Sei  $K$  ein total reeller Zahlkörper, d.h.  $X = \text{Hom}(K, \mathbb{C}) = \text{Hom}(K, \mathbb{R})$ , und  $T$  eine echte, nicht-leere Teilmenge von  $X$ . Dann gibt es eine Einheit  $\varepsilon$  mit  $0 < \tau\varepsilon < 1$  für  $\tau \in T$  und  $\tau\varepsilon > 1$  für  $\tau \notin T$ .

**Hinweis:** Wende den Minkowskischen Gitterpunktsatz auf das Einheitengitter im Spur-Null-Raum an.



<http://www.springer.com/978-3-540-37547-0>

Algebraische Zahlentheorie

Neukirch, J.

1992, XIII, 595 S., Softcover

ISBN: 978-3-540-37547-0