1 Algebraische Zahlentheorie

Vorlesung SS 2003, F. Ischebeck

In der Algebraischen Zahlentheorie werden Erweiterungskörper endlichen Grades K von $\mathbb{Q}$ und in diesen Ringe $\mathbb{Z}_K$ betrachtet, die zu K im selben Verhältnis stehen wie $\mathbb{Z}$ zu $\mathbb{Q}$. Solche Körper heißen auch Zahlkörper und die betrachteten Ringe Zahlringe.

$$\begin{array}{ccc} \mathbb{Z}_K & \longrightarrow & K \\ \uparrow & & \uparrow \\ \mathbb{Z} & \longrightarrow & \mathbb{Q} \end{array}$$

Die genaue Definition von $\mathbb{Z}_K$ geben wir später.

Nur für „wenige“ K wird $\mathbb{Z}_K$ wieder ein Hauptidealrimg sein, aber seine Ideale verhalten sich wie die eines Hauptidealrings: Jedes von (0) verschiedene Ideal von $\mathbb{Z}_K$ ist auf eindeutige Weise ein Produkt von Primidealen. Integritätsringe mit dieser Eigenschaft heißen Dedekind-Ringe.

Zu jedem Dedekind-Ring gehört eine abelsche Gruppe, seine sogenannte Klassengruppe. Für Hauptidealringe ist sie trivial. Ihre Größe gibt sozusagen an, wieweit der Ring davon entfernt ist, ein Hauptidealring zu sein. Wir werden sehen, dass die Klassengruppe eines Zahlrings immer endlich ist.

Das Studium der Zahlkörper und -ringe sollte einerseits ein eigenes Interesse beanspruchen, liefert andererseits auch Aussagen über den Ring $\mathbb{Z}$ und den Körper $\mathbb{Q}$, die man ohne Benutzung der allgemeinen Zahlringe nur schwer erhält.

Beispiel 1. Sei $K := \mathbb{Q}(i)$. Dann ist $\mathbb{Z}_K = \mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$, der sogenannte Gaußsche Zahlring. Dieser ist ein euklidischr Ring, also ein Hauptidealring. Mann kann ihn dazu benutzen, zu studieren, welche natürlichen Zahlen Summen von 2 Quadratzahlen sind.

Beispiel 2. Sei $K := \mathbb{Q}(i\sqrt{3}) = \mathbb{Q}(\zeta)$, wo $\zeta = (1 + i\sqrt{3})/2$ eine primitive 3. Einheitswurzel ist. Hier ist $\mathbb{Z}_K = \mathbb{Z}[\zeta] = \{a + b\zeta \mid a, b \in \mathbb{Z}\}$. Auch er ist ein euklidischer Ring und deshalb ein Hauptidealring. Man kann ihn dazu benutzen, die Fermat'sche Vermutung für den Exponenten 3 zu beweisen. Übrigens ist $\mathbb{Z}[i\sqrt{3}]$ ein echter Teilring von $\mathbb{Z}[\zeta]$ und kein Hauptidealring (auch kein Dedekindring), obwohl sein Quotientenkörper auch $\mathbb{Q}(\zeta)$ ist. Man muss also eine gute Definition der zu den Zahlkörpern K gehörenden Zahlringe $\mathbb{Z}_K$ finden.

Die beiden Beispiele sind Spezialfälle der Kreisteilungskörper. Sei $\zeta \in \mathbb{C}$ eine primitive n-te Einheitswurzel und $K = \mathbb{Q}(\zeta)$ dann ist $\mathbb{Z}_K = \mathbb{Z}[\zeta] =$

$\{a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{\varphi(n)-1}\zeta^{\varphi(n)-1} \mid a_j \in \mathbb{Z}\}$, wie wir sehen werden. Diese Ringe sind nur für endlich viele n Hauptidealringe. In der Vergangenheit hat man dennoch mit ihrer Hilfe in vielen Fällen die Fermat-Vermutung beweisen können. (Der inzwischen gelungene Beweis der vollen Fermat-Vermutung geht allerdings einen anderen Weg.)

Die beiden genannten Beispiele werden im Skript a usführlicher behandeltals in der Vorlesung.

2 Norm und Spur

.

Definition 2.1 *Sei $L \supset K$ eine endliche Körpererweiterung und $\alpha \in L$ und h_α die Homothetie von α, d.h. die durch $x \mapsto \alpha x$ definierte K-lineare Abbildung $L \to L$. (Natürlich ist h_α auch L-linear, da L kommutativ ist, aber wir fassen sie hier als K-lineare Abbildung des K-Vektorraums L auf. Wir definieren:*

a) Die Spur $S_{L/K}(\alpha)$ von α ist definert als die Spur von h_α, d.h. die Summe der Diagonalelemente einer Matrix, die h_α beschreibt.

b) Die Norm $N_{L/K}(\alpha)$ von α ist definiert als die Determinante von h_α.

c) Das charakteristische Polynom χ_α von α ist definiert als charakteristisches Polynom von h_α.

Wir schreiben $N := N_{L/K}$ und $S := S_{L/K}$, wenn die Körper L, K nicht fraglich sind.

2.2 Die Spur ist additiv und die Norm multiplikativ.

Norm und Spur sind – bis auf das Vorzeichen – gewisse Koeffizienten des charakteristischen Polynoms: die Norm ist $(-1)^n$-mal das konstante Glied, wenn $n := [L : K]$ ist. Die Spur ist (-1)-mal der Koeffizient von X^{n-1}. Hieraus ergibt sich:

Proposition 2.3 *Sei $g := \mathrm{Mipo}_K(\alpha) = X^d + a_{d-1}X^{d-1} + \cdots + a_1 X + a_0$ und $r := [L : k(\alpha)] = n/d$. Dann gilt:*

a) $\chi_\alpha = g^r$.

b) $N_{L/K}(\alpha) = (-1)^n a_0^r$.

c) $S_{L/K}(\alpha) = -r a_{d-1}$.

Proof: Spezieller Fall: $L = K(\alpha)$ also $d = n$. In Bezug auf die Basis $\alpha^0, \alpha^1, \ldots, \alpha^{n-1}$ wird die Homothetie h_α durch die Matrix

$$A := \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \ddots & 0 & -a_2 \\ \vdots & 0 & \ddots & \vdots & \vdots \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{d-1} \end{pmatrix}$$

beschrieben. Man berechnet leicht, dass ihr charakteristisches Polynom mit g übereinstimmt.

Allgemeiner Fall: Sei $\beta_1, \ldots, \beta_r$ eine Basis von L über $K(\alpha)$. Bezüglich er Basis $\alpha^0\beta_1, \ldots, \alpha^{d-1}\beta_1, \alpha^0\beta_2, \ldots, \alpha^{d-1}\beta_2, \ldots\ldots, \alpha^0\beta_r, \ldots \alpha^{d-1}\beta_r$ wird h_α durch die $n \times n$-Matrix

$$\begin{pmatrix} A & 0 & \cdots & 0 \\ 0 & A & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & A \end{pmatrix}$$

beschrieben. Daraus folgt alles. □

2.4 Ist $l \supset K$ separabel, und sind $\sigma_j : L \to \overline{K}$ für $j = 1, \ldots, n$ die verschiedenen K-Homomorfismen von L in einen algebraischen Abschluss von K, so ist offenbar:

$$S_{L/K}(\alpha) = \sum_{j=1}^{n} \sigma_j(\alpha) \quad \text{und} \quad N_{L/K}(\alpha) = \prod_{j=1}^{n} \sigma_j(\alpha)$$

Ist insbesondere $L \supset K$ galoissch, so gilt selbiges für $\mathrm{Gal}_K(L) = \{\sigma_1, \ldots, \sigma_n\}$.

Hieraus folgen für separable Körpertürme: $E \supset L \supset K$ die Formeln

$$S_{E/K} = S_{L/K} \circ S_{E/L} \ , \quad N_{E/K} = N_{L/K} \circ N_{E/L}$$

die sogenannte Transitivität der Norm und der Spur.

Ist $\mathrm{char}(K) = 0$, so ist $S_{L/K}$ nicht die Nullabbildung, da $S_{L/K}(1) = n$ ist.

Für allgemeine separable Erweiterungen gilt dies auf Grund der linearen Unahängigkeit von Charakteren ebenfalls. Ist $L \supset K$ inseparabel, so ist $S_{L/K} = 0$.

3 Ganze algebraische Zahlen

Wir werden hier benutzen, dass Untergruppen endlich erzeugter abelscher Gruppen endlich erzeugt sind. Für $\alpha \in \mathbb{C}$ wird mit $\mathbb{Z}[\alpha]$ der Ring aller Polynome in α über $\mathbb{Z}$ bezeichnet:

$\mathbb{Z}[\alpha] := \{\sum_{j\in\mathbb{N}} a_j\alpha^j \mid a_j \in \mathbb{Z}, a_j = 0 \text{ bis auf endlich viele } j\}$

Theorem 3.1 *Für $\alpha \in \mathbb{C}$ sind folgende Aussagen äquivalent:*

(i) $\mathbb{Z}[\alpha]$ wird „additiv" endlich erzeugt, d.h. es ist bezüglich '+' eine endlich erzeugte Gruppe;

*(ii) α genügt einer „***Ganzheitsgleichung***", d.h. es gibt $a_0, \ldots, a_{n-1} \in \mathbb{Z}$, so dass $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha = 0$ ist. (Entscheidend ist, dass der Koeffizient von α^n gleich 1 oder zumindes eine Einheit ist.)*

Man kann (ii) auch so ausdrücken: Es gibt ein „**Ganzheitspolynom**", d.h. ein $f \in \mathbb{Z}[X]$ mit Leitkoeffizienten 1, das α zur Nullstelle hat.

Proof: (i)⇒(ii): Ist eine Gruppe endlich erzeugt, so besitzt jedes Erzeugendensystem ein endliches erzeugendes Teilsystem. Die Menge $1, \alpha, \alpha^2, \ldots$ ist ein Erzeugendensystem von $\mathbb{Z}[\alpha]$ als additive Gruppe. Ist etwa α^{n-1} die höchste Potenz von α in einem endlichen erzeugenden Teilsystem des Obigen, so ist α^n eine Linearkombination der α^j mit $j < n$ mit Koeffizienten aus $\mathbb{Z}$, d.h. $\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0$ mit gewissen $a_0, \ldots, a_{n-1}$.

(ii)⇒(i): Jedes Polynom $f \in \mathbb{Z}[X]$ lässt sich durch ein Polynom aus $\mathbb{Z}[X]$ mit Leitkoeffizienten 1 innerhalb $\mathbb{Z}[X]$ mit Rest dividieren:

$$f = (X^n + a_{n-1} + \cdots + a_0) \cdot q + r$$

mit $\text{grad}(r) < n$. Für α gilt dann $f(\alpha) = r(\alpha)$. D.h. $\mathbb{Z}[\alpha]$ wird *additiv* schon von $1, \alpha, \ldots, \alpha^{n-1}$ erzeugt. □

Definition 3.2 *Eine Zahl $\alpha \in \mathbb{C}$, welches die äquivalenten Aussagen des Theorems erfüllt, heißt* **ganzalgebraisch**.

Proposition 3.3 *Die ganzalgebraischen Zahlen aus $\mathbb{Q}$ sind die Zahlen aus $\mathbb{Z}$.*

Proof: Sei $\alpha = k/m \in \mathbb{Q}$ ganzalgebraisch, $k, m \in \mathbb{Z}$ zueinander teilerfremd. Wenn man eine Ganzheitsgleichung wie oben mit m^n multipliziert und k^n auf eine Seite bringt, erhält man

$$k^n = -a_{n-1}k^{n-1}m + a_{n-2}k^{n-2}m^2 + \cdots + a_0m^n \ .$$

Hätte m einen Primfaktor, so würde dieser die rechte Seite teilen, also auch die linke und somit k, im Widerspruch zur Teilerfremdheit. Also bleibt nur $m = \pm 1$, d.h. $\alpha \in \mathbb{Z}$.

Umgekehrt ist natürlich jedes $\alpha \in \mathbb{Z}$ auch ganzalgebraisch; denn $\alpha^1 - \alpha \cdot \alpha^0 = 0$. □

Remark 3.4 Mit demselben Beweis zeigt man, dass alle Elemente im Quotientenkörper eines faktoriellen Rings A, die über A ganz sind, zu A gehören.

Proposition 3.5 *a) Die ganzalgebraischen Zahlen bilden einen Unterring von* $\mathbb{C}$.

b)Erfüllt $\beta \in \mathbb{C}$ *eine Gleichung der Form*

$$\beta^n + \alpha_1 \beta^{n-1} + \cdots + \alpha_n = 0$$

mit ganzalgebraischen α_j*, so ist schon* $\beta \in \mathbb{Z}_{\mathbb{C}}$.

Proof: a) Zunächst ist 1 ganzalgebraisch, und mit α ist es auch $-\alpha$, da $\mathbb{Z}[-\alpha] = \mathbb{Z}[\alpha]$ gilt.

Seien nun α, β ganzalgebraische Zahlen. $\mathbb{Z}[\alpha]$ sei additiv von $\alpha_1, \ldots, \alpha_n$ und $\mathbb{Z}[\beta]$ von $\beta_1, \ldots, \beta_m$ erzeugt. Die von den mn Elementen $\alpha_j \beta_k$ additiv erzeugte Untergruppe von $\mathbb{C}$ ist offenbar ein Unterring A von $\mathbb{C}$. Die Ringe $\mathbb{Z}[\alpha + \beta]$ und $\mathbb{Z}[\alpha\beta]$ sind Unterringe von A und additiv endlich erzeugt, da sie Untergruppen der endlich erzeugten abelschen Gruppe A sind.

b) Aus den Überlegungen zu a) folgt, dass der von $\alpha_1, \ldots, \alpha_n$ erzeugte Ring A eine endlich erzeugte Gruppe (bzgl. $+$) ist. Wie oben sieht man, dass $A[\beta] = A + A\beta + \cdots + A\beta^{n-1}$ gilt. $\mathbb{Z}[\beta]$ ist also eine Untergruppe der endlich erzeugten Gruppe $A[\beta]$. □

Definitions 3.6 *Der Ring aller ganzalgebraischen (komplexen) Zahlen wird mit* $\mathbb{Z}_{\mathbb{C}}$ *bezeichnet. Ist* K *ein Unterkörper von* $\mathbb{C}$*, so definieren wir* $\mathbb{Z}_K := K \cap \mathbb{Z}_{\mathbb{C}}$.

Ein **Zahlkörper** *ist ein Teilkörper von* $\mathbb{C}$*, der endlich über* $\mathbb{Q}$ *ist.*

Ist K *ein Zahlkörper, so heißt* $\mathbb{Z}_K$ *auch die* **Hauptordnung** *von* K.

Manchmal sagt man kurz **ganz** *statt ganzalgebraisch und nennt dann die Zahlen in* $\mathbb{Z}$ **ganzrational**. *Manchmal nennt man* $\mathbb{Z}_K$ *auch den* **Ring der ganzen Zahlen in** K.

Proposition 3.7 *a) Ist $\alpha \in \mathbb{C}$ algebraisch (über $\mathbb{Q}$), so gibt es eine natürliche Zahl $m > 0$ mit $m\alpha \in \mathbb{Z}_{\mathbb{C}}$. b b) Ist $K \supset \mathbb{Q}$ algebraisch, so ist K der Quotientenkörper von $\mathbb{Z}_K$.*

Proof: a) Sei $X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 = \mathrm{Mipo}_{\mathbb{Q}}(\alpha)$ und $m \in \mathbb{N}$ ein gemeinsamer Nenner der $a_0, \ldots, a_{n-1} \in \mathbb{Q}$, d.h. $ma_j \in \mathbb{Z}$. Dann erfüllt $m\alpha$ die Gleichung

$$(m\alpha)^n + ma_{n-1}(m\alpha)^{n-1} + \cdots + m^{n-1}a_1(m\alpha) + m^n a_0 = 0 \ .$$

b) folgt direkt aus a). □

3.8 Die Aussage b) trifft insbesondere auf algebraische Zahlkörper, d.h. endliche Erweiterungskörper von $\mathbb{Q}$ zu. (Endliche Körpererweiterungen sind ja algebraisch.)

Wir werden die Hauptordnungen algebraischer Zahlkörper in 2 Fällen bestimmen, erstens, wenn K ein Kreisteilungskörper, zweitens, wenn er ein quadratischer Zahlkörper ist, d.h. ein solcher vom Grad 2 über $\mathbb{Q}$.

Im ersten Fall gilt: Ist ζ eine primitive n-te Einheitswurzel, so ist $\mathbb{Z}[\zeta]$ die Hauptordnung von $\mathbb{Q}(\zeta)$. Dies ist nicht trivial und wird später bewiesen.

Im zweiten Fall ist die Beschreibung der Hauptordnung etwas komplizierter, aber es ist leichter zu beweisen, dass sie stimmt.

Wir beginnen mit einem allgemein interessanten Kriterium für die Ganzheit algebraischer Zahlen. Man braucht nicht etwa alle $f \in \mathbb{Z}[X]$ mit Leitkoeffizienten 1 daraufhin zu untersuchen, ob $f(\alpha) = 0$ ist. Sondern:

Proposition 3.9 *$\alpha \in \overline{\mathbb{Q}}$ ist genau dann ganzalgebraisch, wenn $\mathrm{Mipo}_{\mathbb{Q}}(\alpha) \in \mathbb{Z}[X]$ gilt.*

$\overline{\mathbb{Q}}$ bezeichnet den Körper aller algebraischen komplexen Zahlen.

Proof: „$\Leftarrow$“ ist trivial, da ein Minimalpolynom *per definitionem* den Leitkoeffizienten 1 hat.

„$\Rightarrow$“: Ist $\sigma \in \mathrm{Aut}(\overline{\mathbb{Q}})$, so ist mit α sicherlich auch $\sigma(\alpha)$ ganzalgebraisch. D.h., ist α ganzalgebraisch, so auch alle seine Konjugierten. Die Koeffizienten von $\mathrm{Mipo}_{\mathbb{Q}}(\alpha)$ sind (elementarsymmetrische) Polynome in den Konjugierten von α, sind also ganzalgebraisch. Andererseits liegen sie in $\mathbb{Q}$, gehören also zu $\mathbb{Z}$. □

3.10 Aus der Lösungsformel für quadratische Gleichungen sieht man, dass für jede quadratische Körpererweiterung $K \supset \mathbb{Q}$ (d.h. eine solche, für die $[K : \mathbb{Q}] = 2$ ist) ein $d \in \mathbb{Q}$ mit $K = \mathbb{Q}(\sqrt{d})$ existiert. Da für jedes $r \in \mathbb{Q}^\times$ die Gleichheit $\mathbb{Q}(\sqrt{dr^2}) = \mathbb{Q}(\sqrt{d})$ gilt, können wir ferner $d \in \mathbb{Z}$ quadratfrei annehmen. (Eine Zahl aus $\mathbb{Z}$ heißt **quadratfrei**, wenn sie nicht durch das Quadrat einer Primzahl teilbar und $\neq 1$ ist. Insbesondere ist eine quadratfreie Zahl $\neq 0$ und nicht durch 4 teilbar.)

(Um unseren Symbolen eine eindeutige Bedeutung zu geben, soll immer $\sqrt{d} > 0$ für $d > 0$ verlangt werden. Für $d < 0$ sei dann $\sqrt{d} = i\sqrt{-d}$. Im Übrigen kommt es nicht wirklich darauf an, da $\mathbb{Q}(\alpha) = \mathbb{Q}(-\alpha)$ ist.)

Proposition 3.11 *Sei $d \in \mathbb{Z}$ quadratfrei und $K := \mathbb{Q}(\sqrt{d})$. Dann gilt:*

a) Ist $d \equiv 2$ oder 3 mod 4, so ist $\mathbb{Z}_K = \mathbb{Z} + \mathbb{Z}\sqrt{d}$.

b) Ist $d \equiv 1$ mod 4, so ist $\mathbb{Z}_K = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2} =$
$\{\frac{a}{2} + \frac{b}{2}\sqrt{d} \mid a, b \in \mathbb{Z}, a \equiv b \pmod 2\}$.

Da es möglicherweise Übungen zur Vorlesung gibt, wird der Beweis hier nicht gegeben. Beachte, dass im Fall $d \equiv 1 \bmod 4$ die additive Gruppe $\mathbb{Z} + \mathbb{Z}\sqrt{d}$ ein echter Unterring von $\mathbb{Z}_K$ ist.

Examples 3.12 Ist $d = -1$, also $K = \mathbb{Q}(i)$, dann ist $\mathbb{Z}_K = \mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i$, der Gaußsche Zahlring.

Ist $d = -3$, so ist $K = \mathbb{Q}(\sqrt{-3})$ und $\mathbb{Z}_= \mathbb{Z}[\zeta]$ mit der primitiven 6. Einheitswurzel $\zeta := \frac{1+\sqrt{-3}}{2}$. Da $\zeta^2 = \frac{-1+\sqrt{-3}}{2}$ ist, gilt natürlich auch $\mathbb{Z}_K = \mathbb{Z}[\zeta^2]$.

3.13 Wir betrachten weiterhin **quadratische Zahlkörper**, d.h. diejenigen der Form $K := \mathbb{Q}(\sqrt{d})$, wo d quadratfrei ist. Ist $d < 0$, so nennt man $\mathbb{Q}(\sqrt{d})$ **imaginärquadratisch**, sonst **reellquadratisch**. Die Elemente 1 und, je nachdem, $\sqrt{d}$ bzw. $(1 + \sqrt{d})/2$ bilden eine $\mathbb{Z}$-Basis von $\mathbb{Z}_K$.

a) Sei zunächst $d < 0.$, d.h. K imaginärquadratisch. Dann ist die genannte Basis auch eine Basis von $\mathbb{C}$ über $\mathbb{R}$. D.h. $\mathbb{Z}_K$ ist ein sogenanntes Gitter in $\mathbb{C}$.

In diesem Fall ist die Gruppe der Einheiten endlich. Man sieht nämlich leicht, dass $u \in \mathbb{Z}_K$ genau dann eine Einheit ist, wenn für seine Norm $N_{K/\mathbb{Q}}(u) = 1$ gilt. In unserem Fall ist $N_{K/\mathbb{Q})}(\alpha) = |\alpha|^2$. Da jedes Gitter in $\mathbb{C}$ nur endlich viele Punkte mit einer beliebigen kompakten Menge gemeinsam hat, besitzt $\mathbb{Z}_K$ nur endlich viele Einheiten. Für $d < 0,\ d \neq -1, -3$ besitzt $\mathbb{Z}_K$ nur die Einheiten $1, -1$.

b) Sei jetzt K reellquadratisch, d.h. $d > 0$, sogar $d > 1$. In diesem Fall ist $u \in \mathbb{Z}_K$ eine Einheit genau dann, wenn $N_{K/\mathbb{Q}}(u) = \pm 1$ ist. In diesem Fall kann man zeigen, dass $\mathbb{Z}_K^\times$ isomorf zu $\{1, -1\} \times \mathbb{Z}$ ist, es also Einheiten unendlicher Ordnung gibt.

Sei σ der von der Identität verschiedene Automorfismus von $\mathbb{Q}(\sqrt{d})$. Dieser macht folgendes: $\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$. Er bildet $\mathbb{Z}_K$ auf sich ab. (Dies tun übrigens alle Automorfismen von Zahlkörpern.) Die Abbildung $\varphi : \mathbb{Q}(\sqrt{d}) \to \mathbb{R}^2,\ \alpha \mapsto (\alpha\ ,\ \sigma(\alpha))$ ist injektiv und $\mathbb{Z}$-linear. Das Bild der o.a. $\mathbb{Z}$-Basis von $\mathbb{Z}_K$ ist eine $\mathbb{R}$-Basis des $\mathbb{R}^2$, wie man leicht sieht. Wieder ist $\varphi(\mathbb{Z}_K)$ ein Gitter in $\mathbb{R}^2$.

Example 3.14 Sei speziell $K = \mathbb{Q}(\sqrt{-5})$. Dann ist $\mathbb{Z}_K = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$. In $\mathbb{Z}_K$ hat die Zahl 6 folgende Zerlegungen:

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

Mit Hilfe der Norm erkennt man, dass die angegebenen Faktoren irreduzibel sind. Ebenso sieht man mit Hilfe der Norm, das die Einheiten von $\mathbb{Z}_K$ nur $1, -1$ sind. Mn hat also zwei wesentlich verschiedene Zerlegungen von 6 in irreduzible Faktoren. Deshalb ist $\mathbb{Z}_K$ kein faktorieller, also auch kein Hauptidealring.

Nur für endlich viele imaginärquadratische Zahlkörper K gilt, dass $\mathbb{Z}_K$ ein Hauptidealring ist. Man vermutet, dass es unendlich viele reellquadratische K gibt, für die $\mathbb{Z}_K$ ein Hauptidealring ist.

4 Der Gaußsche Zahlring

Wir betrachten hier den Gaußschen Zahlenring

$$\mathbb{G} := \{a + bi \quad | \quad a, b \in \mathbb{Z}\},$$

wo i die imaginäre Einheit bezeichnet, also $i^2 = -1$ gilt.

In der Gaußschen Zahlenebene, deren Punkte beliebige komplexe Zahlen bedeuten, bilden die Elemente von $\mathbb{G}$ ein sogenanntes Gitter:

Er ist der Ring der ganzen Zahlen in $\mathbb{Q}(i)$.

Definition 4.1 *Sei $\alpha := a + bi$, $a, b \in \mathbb{Z}$ (bzw. $\mathbb{R}$).*

a) Definiere $\overline{\alpha} := a - bi$. Die Zahl $\overline{\alpha}$ heißt das **Konjugierte** *von α, die Abbildung*

$$\mathbb{G} \to \mathbb{G} \quad (bzw. \quad \mathbb{C} \to \mathbb{C}), \quad \alpha \longmapsto \overline{\alpha}$$

heißt Konjugation. (Anschaulich gesprochen, ist sie die Spiegelung des Gitters $\mathbb{G}$ (bzw. der Gaußschen Zahlenebene) an der reellen Achse.

b) Definiere $N(\alpha) := \alpha\overline{\alpha} = a^2 + b^2 \in \mathbb{N}$ (bzw. $\mathbb{R}_+$). Man nennt $N(\alpha)$ die Norm von α und $N : \mathbb{G} \to \mathbb{N}$ (bzw. $\mathbb{C} \to \mathbb{R}_+$) die Norm (-abbildung).

Remark 4.2 Mit der üblichen Betragsfunktion $|\ \ |$ (die anschaulich den Abstand eines Punktes von 0 beschreibt) gilt: $N(\alpha) = |\alpha|^2$. Beachte, dass $|1+i| = \sqrt{2}$ ist und somit die Betragsfunktion den Ring $\mathbb{G}$ nicht in $\mathbb{Z}$ abbildet.

Proposition 4.3 *Konjugation und Norm haben folgende Eigenschaften:*
a) $\overline{\alpha} + \overline{\beta} = \overline{\alpha + \beta}$;
b) $\overline{\alpha} \cdot \overline{\beta} = \overline{\alpha\beta}$;
c) $\overline{1} = 1$.
d) Die Konjugation ist ein Isomorfismus des Ringes $\mathbb{G}$ (bzw. Körpers $\mathbb{C}$) zu sich selbst, ein sogenannter Automorfismus.
e) $N(\alpha) = 0 \iff \alpha = 0$;
f) $N(\alpha\beta) = N(\alpha)N(\beta)$;
g) für $\alpha \in \mathbb{G}$ gilt: $\alpha \in \mathbb{G}^* \iff N(\alpha) = 1$.

Proof: a) und c) sind trivial, und b) ist leicht nachzurechnen.
d) folgt aus a), b) und c) und daraus, dass die Konjugation offensichtlich bijektiv ist.
e) $N(a+bi) = a^2+b^2$ für $a, b \in \mathbb{R}$. Eine Summe von Quadraten reeller Zahlen

ist genau dann Null, wenn diese selbst es sind.
f) ergibt sich sofort aus b) und der Kommutativität und Assoziativität der Multiplikation.
g) Wenn $N(\alpha) = 1$ ist, ist $\alpha\overline{\alpha} = 1$, also α eine Einheit, da mit α auch $\overline{\alpha}$ zu $\mathbb{G}$ gehört.
Umgekehrt, wenn $\alpha \in \mathbb{G}^*$ ist, gibt es ein $\beta \in \mathbb{G}$ mit $\alpha\beta = 1$, also $N(\alpha) \cdot N(\beta) = N(\alpha\beta) = 1$. Das Produkt der natürlichen Zahlen $N(\alpha)$ und $N(\beta)$ kann aber nur dann 1 sein, wenn beide Zahlen selbst es sind. □

Corollary 4.4 $\mathbb{G}^* = \{1, -1, i, -i\}$.

Denn nur die angegebenen 4 Elemente aus $\mathbb{G}$ haben die Norm 1. □

Remarks 4.5 a) Ein Element von $\mathbb{Z}$ ist offenbar genau dann in $\mathbb{Z}$ eine Summe zweier Quadrate, wenn es von der Form $N(\alpha)$ mit einem $\alpha \in \mathbb{G}$ ist. (Dabei ist der Summand 0^2 nicht ausgeschlossen: $1 = 0^2 + 1^2$, $4 = 0^2 + 2^2$.)

b) Aus a) und der Identität $N(\alpha\beta) = N(\alpha) \cdot N(\beta)$ folgt, dass ab in $\mathbb{N}$ eine Summe von 2 Quadraten ist, wenn a und b es sind.

c) Nicht jede natürliche Zahl ist in $\mathbb{Z}$ eine Summe zweier Quadrate. Denn in $\mathbb{Z}/4$ sind $\overline{0}$ und $\overline{1}$ die einzigen Quadrate. Wenn also
$n \equiv -1 \pmod 4$ ist, ist n nicht Summe zweier Quadrate.

d) Jedes Element $\alpha \in \mathbb{G} - \{0\}$ ist zu genau 4 Elementen assoziiert: $\alpha, -\alpha, i\alpha, -i\alpha$. Von diesen 4 Elementen liegt genau eines in dem Quadranten $\{x + yi \mid x > 0,\ y \geq 0\}$.
Dies ist anschaulich klar, weil die Multiplikation mit i (bzw. -1, bzw.$-i$) die Drehung der Gaußschen Zahlenebene um den Nullpunkt mit dem Winkel $\pi/2$ (bzw. π, bzw. $3\pi/2$) bedeutet.
Man kann sich jedoch auch ohne Anschauung leicht von obiger Behauptung überzeugen.

Proposition 4.6 *Der Ring $\mathbb{G}$ ist euklidisch. Genauer gilt: Zu $a, b \in \mathbb{G}$, $b \neq 0$ gibt es $q, r \in \mathbb{G}$ mit*

1) $a = bq + r$ *und* *2)* $N(r) \leq \frac{1}{2}N(b)$.

Beweis: In $\mathbb{C}$ können wir a durch b (ohne Rest) dividieren:

$$\frac{a}{b} = x + iy =: z \quad \text{mit} \quad x, y \in \mathbb{R}.$$

(Es ist sogar $x, y \in \mathbb{Q}$, wie der Leser sich überlegen möge.)
Es gibt $m, n \in \mathbb{Z}$ mit $|x - m| \leq \frac{1}{2}$ und $|y - n| \leq \frac{1}{2}$. (Z.B. sei $m = [x]$, wenn

$x \leq [x] + \frac{1}{2}$ und $m = [x] + 1$, wenn $x > [x] + \frac{1}{2}$.)
Setze $q := m + in$.
Mit $z = x + iy$ gilt dann:

$$\begin{aligned} a - bz &= 0 \quad \text{und} \\ N(z - q) &= (x - m)^2 + (y - n)^2 \leq \tfrac{1}{4} + \tfrac{1}{4} = \tfrac{1}{2}. \end{aligned}$$

Mit $r := a - bq$ folgt

$$\begin{aligned} N(r) &= N(a - bq) = N(a - bz + bz - bq) \\ &= N(bz - bq) = N(b) \cdot N(z - q) \leq \tfrac{1}{2} N(b). \end{aligned}$$ □

4.7 Der Ring $\mathbb{G}$ ist also ein Hauptidealring. Somit ist jedes irreduzible Element in $\mathbb{G}$ auch prim, und es gilt der Satz von der eindeutigen Primfaktorzerlegung. Wir wollen die Primelemente in $\mathbb{G}$ bestimmen.

Definition 4.8 *Die Primelemente von $\mathbb{G}$ heißen Gaußsche Primzahlen. Der Deutlichkeit halber werden die Primzahlen aus $\mathbb{N}$, d.h. diejenigen im bisherigen Sinne, auch rationale Primzahlen genannt.*

(In $\mathbb{Z}$ hatten wir nur die positiven Primelemente Primzahlen genannt. Jedes negative Primelement ist ja zu einer (positiven) Primzahl assoziiert. In $\mathbb{G}$ tun wir dies nicht. Denn so kanonisch die Auszeichnung der positiven ganzen Zahlen in $\mathbb{Z}$ ist, so wenig kanonisch wäre etwa die Auszeichnung des Quadranten $\{x + iy \quad | \quad x > 0, \;\; y \geq 0\}$ in $\mathbb{G}$.)

Proposition 4.9 *Wenn $\alpha \in \mathbb{G}$ und $N(\alpha)$ eine rationale Primzahl ist, dann ist α eine Gaußsche Primzahl.*

Proof: Sei $\alpha = \beta\gamma$ mit $\beta, \gamma \in \mathbb{G}$. Dann ist $N(\alpha) = N(\beta) \cdot N(\gamma)$ gemäß 12.3 f), also $N(\beta) = 1$ oder $N(\gamma) = 1$, da $N(\alpha)$ prim in $\mathbb{N}$ ist. Es folgt, dass β oder γ eine Einheit in $\mathbb{G}$, also α irreduzibel in $\mathbb{G}$, d.h. eine Gaußsche Primzahl ist. □

Example 4.10 $1+i$ ist eine Gaußsche Primzahl, da $N(1+i) = 2$ ist. Wegen $1 - i = -i(1 + i)$ ist $1 - i$ zu $1 + i$ assoziiert. Eine Primfaktorzerlegung von 2 in $\mathbb{G}$ ist also $2 = (-i)(1 + i)^2$. Die weiteren zu $1 + i$ assoziierten Zahlen sind $-1 \pm i$.

Proposition 4.11 *Sei p eine ungerade rationale Primzahl. Dann ist p entweder auch eine Gaußsche Primzahl oder die Norm einer Gaußschen Primzahl, $p = q \cdot \overline{q}$. In diesem Falle sind q und $\overline{q}$ zueinander nicht assoziierte Gaußsche Primzahlen, und $p = q \cdot \overline{q}$ ist eine Primfaktorzerlegung in $\mathbb{G}$.*

Proof: Wir betrachten eine Primfaktorzerlegung von p in $\mathbb{G}$, etwa $p = uq_1 \cdot \ldots \cdot q_r$ mit $u \in \mathbb{G}^*$ und Gaußschen Primzahlen $q_1, \ldots, q_r$.
Wegen $N(u) = 1$ nach 12.3 g) ist also $p^2 = N(p) = N(q_1) \cdot \ldots \cdot N(q_r)$.
Hieraus folgt $1 \leq r \leq 2$, da genau die Einheiten in $\mathbb{G}$ die Norm 1 haben.

1. Fall: $r = 1$, d.h. $p = uq_1$.
In diesem Fall ist p zu einer Gaußschen Primzahl, nämlich q_1, assoziiert, also selbst eine Gaußsche Primzahl.

2. Fall: $r = 2$, d.h. $p = uq_1 \cdot q_2$.
Aus $p^2 = N(q_1) \cdot N(q_2)$ folgt dann $N(q_1) = N(q_2) = p$, da $N(q_i) > 1$ ist. Für $q = q_1$ gilt also $p = q \cdot \overline{q}$. Da die Konjugation ein Isomorfismus von $\mathbb{G}$ auf sich selbst ist, ist mit q auch $\overline{q}$ eine Gaußsche Primzahl.
Wir haben noch auszuschließen, dass q zu $\overline{q}$ assoziiert ist, und setzen $q = x+iy$ mit $x, y \in \mathbb{Z}$, also $\overline{q} = x-iy$. Angenommen, es wäre $uq = \overline{q}$ mit einem $u \in \mathbb{G}^*$.
Im Falle $u = \pm 1$ wäre $y = 0$ oder $x = 0$, also $p = q\overline{q} = x^2$ oder y^2, also ein Quadrat in $\mathbb{Z}$ und deshalb p keine rationale Primzahl.
Im Falle $u = \pm i$ wäre $x = \mp y$, also $p = q\overline{q} = 2x^2$ und deshalb p keine ungerade rationale Primzahl. □

4.12 Welche rationalen Primzahlen sind nun Gaußsche Primzahlen, und welche sind Normen Gaußscher Primzahlen?

Satz: *Sei p eine ungerade rationale Primzahl. Dann gilt:*
Ist $p \equiv -1$ (mod 4), so ist p eine Gaußsche Primzahl.
Ist $p \equiv 1$ (mod 4), so ist p die Norm einer Gaußschen Primzahl.

Proof: Ist $p \equiv -1 \pmod 4$, so ist p in $\mathbb{Z}$ nicht Summe zweier Quadrate nach 12.5 c), d.h. p ist nicht die Norm irgendeiner Zahl aus $\mathbb{G}$. Gemäß 12.11 muss p eine Gaußsche Primzahl sein.
Ist $p \equiv 1 \pmod 4$, so müssen wir zeigen, dass p keine Gaußsche Primzahl ist. Aus $p \equiv 1 \pmod 4$ folgt nun $\left(\frac{-1}{p}\right) = 1$ nach 10.5. D.h. es gibt ein $x \in \mathbb{Z}$ mit $x^2 \equiv -1 \pmod p$, also $p \mid x^2 + 1 = (x+i)(x-i)$. Wäre p eine Gaußsche Primzahl, so folgte $p \mid x + i$ oder $p \mid x - i$. Das geht aber nicht. Denn für beliebige $a, b \in \mathbb{Z}$ ist $p \cdot (a + bi) = pa + pbi$ mit $pb \neq \pm 1$, da p eine rationale Primzahl ist. □

Corollary 4.13 *Sei q eine Gaußsche Primzahl. Dann gilt genau eine der drei folgenden Aussagen:*

(i) q ist assoziiert zu $1 + i$ (d.h. $q = \pm 1 \pm i$);

(ii) $N(q)$ *ist eine rationale Primzahl* p *und* $p \equiv 1$ *(mod 4);*

(iii) q *ist assoziiert zu einer rationalen Primzahl* p *mit* $p \equiv -1$ *(mod* 4*).*

Proof: Da q eine Gaußsche Primzahl ist, teilt q einen der rationalen Primfaktoren der natürlichen Zahl $q\overline{q}$. Dieser heiße p. Dann ist entweder q zu p assoziiert oder $p = q'\overline{q'}$ mit einer zu q assoziierten Zahl q'. Im letzteren Fall ist $p = N(q') = N(q)$, also entweder $p = 2$ oder
$p \equiv 1 \pmod 4$. □

Corollary 4.14 *Eine rationale Primzahl* p *ist in* $\mathbb{N}$ *eine Summe zweier Quadrate genau dann, wenn* $p = 2$ *oder* $p \equiv 1$ *(mod 4) ist. Eine solche Darstellung ist bis auf die Reihenfolge eindeutig.*

Proof: Wenn p von der Form a^2+b^2 mit $a, b \in \mathbb{N}$ ist, gilt $p = (a+bi)(a-bi)$. Also ist p in $\mathbb{G}$ nicht irreduzibel und deshalb $p = 2$ oder $p \equiv 1 \pmod 4$. Umgekehrt ist in diesen Fällen p die Norm einer Gaußschen (Prim–) Zahl, also Summe von Quadraten.
Zur Eindeutigkeit: Man hat in obigen Fällen in $\mathbb{G}$ eine Primfaktorzerlegung $p = q \cdot \overline{q}$ mit einer Gaußschen Primzahl q. Ist nun $p = a^2+b^2 = (a+bi)(a-bi)$, so muss $a+bi$ wegen der Eindeutigkeit der Primfaktorzerlegung in $\mathbb{G}$ eine zu q oder $\overline{q}$ assoziierte Gaußsche Primzahl sein. Man überlegt sich nun leicht, dass die Darstellung $p = a^2+b^2$ nicht wesentlich von der durch $p = q\overline{q}$ bestimmten Darstellung von p als Summe zweier Quadrate verschieden ist. □

Corollary 4.15 *Sei* $n \in \mathbb{N}_1$*. Genau dann ist* n *in* $\mathbb{N}$ *eine Summe zweier Quadrate, wenn für jede rationale Primzahl* $p \equiv 3$ *(mod* 4*) die Vielfachheit* $v_p(n)$ *gerade ist.*

Proof: „⇐“: Nach Voraussetzung ist n von der Form $n = m^2 p_1 \cdot \ldots \cdot p_r$ mit rationalen Primzahlen $p_i \equiv 1 \pmod 4$. Letztere sind Summen je zweier Quadrate und $m^2 = m^2 + 0^2$ auch. Nach 12.5 b) ist deshalb auch n eine solche.
„⇒“: Nach Voraussetzung ist $n = N(\alpha)$ mit einem $\alpha \in \mathbb{G}$. Sei $\alpha = u q_1 \cdot \ldots \cdot q_s$ eine Primfaktorzerlegung in $\mathbb{G}$. Dann ist

$$n = N(u)N(q_1) \cdot \ldots \cdot N(q_s) = N(q_1) \cdot \ldots \cdot N(q_s).$$

Für $i \in \{1, \ldots, s\}$ ist entweder $N(q_i) = 2$ oder $N(q_i)$ eine rationale Primzahl $p_i \equiv 1 \pmod 4$, oder es ist q_i zu einer rationalen Primzahl
$p_i \equiv -1 \pmod 4$ assoziiert, also $N(q_i) = p_i^2$. Die modulo 4 zu 3 kongruenten rationalen Primfaktoren von n treten also in gerader Potenz auf. □

Corollary 4.16 *Seien $m, n \in \mathbb{N}_1$ und $m^2 n$ in $\mathbb{N}$ eine Summe zweier Quadrate, so ist auch n eine solche.*

Corollary 4.17 *Sei $n \in \mathbb{N}$, $n = r_1^2 + r_2^2$ mit $r_1, r_2 \in \mathbb{Q}$. Dann gibt es auch $a_1, a_2 \in \mathbb{N}$ mit $n = a_1^2 + a_2^2$.*

Proof: Aus $n = \frac{m_1^2}{c_1^2} + \frac{m_2^2}{c_2^2}$ folgt $n(c_1 c_2)^2 = (m_1 c_2)^2 + (m_2 c_1)^2$. Mit Hilfe von 12.16 ergibt sich die Behauptung. □

Remark 4.18 Mit 12.14 kann man schnell feststellen, ob eine Primzahl Summe zweier Quadrate ist oder nicht. Man hat allerdings mit dieser Entscheidung eine solche Darstellung noch nicht gefunden. Bei Zahlen, deren Primfaktorzerlegung unbekannt ist, braucht man nicht viel mehr Zeit, über die Darstellbarkeit als Summe zweier Quadrate durch Probieren zu entscheiden und dabei gegebenenfalls eine solche Darstellung zu finden, als einen einzigen Primfaktor durch Probieren zu finden. Das Korollar 12.15 ist also von „nur“ theoretischem Gewicht.
Andererseits, wer will schon von einer einzelnen konkreten Zahl wirklich wissen, ob und auf welche Weise sie als Summe von zwei Quadraten darstellbar ist?

5 Die Struktur der addtiven Gruppen der Zahlringe

Definition 5.1 *Sei $n \in \mathbb{N}$. Eine freie abelsche Gruppe vom Rang n ist eine, die zu $\mathbb{Z}^n$ (mit komponentenweiser Addition) isomorf ist.*

Remark 5.2 Eine endlich erzeugte freie abelsche Gruppe ist eine, die zu $\mathbb{Z}^n$ für ein $n \in \mathbb{N}$ isomorf ist.

Eine abelsche Gruppe G ist frei vom Rang $n$genau dann, wenn sie eine endliche **Basis** besitzt, d.h. ein n-tupel $x_1, \ldots, x_n$ von Elementen von G, derart dass jedes $y \in G$ sich eindeutig in der Form $\sum_{j=1}^{n} n_j x_j$ mit $n_j \in \mathbb{Z}$ schreiben lässt.

5.3 Wir verwenden ohne Beweis folgenden Tatsachen

a) Aus $\mathbb{Z}^m \cong \mathbb{Z}^n$ folgt $m = n$.

b) Ist G eine Untergruppe von $\mathbb{Z}^n$, so ist $G \cong \mathbb{Z}^m$ mit einem $m \leq n$.

Beachte, dass in diesem Fall aus $m = n$ nicht notwendig $G = \mathbb{Z}^n$ folgt, nicht einmal, wenn $n = 1$ ist.

5.4 Wir werden die Spur einer endlichen *separablen* Körpererweiterung $K \supset F$ verwenden.

$S_{K/F}$ ist eine von 0 verschiedene F-lineare Abbildung, insbesondere ein Homomorfismus der additiven Gruppen.

Sei nun $F = \mathbb{Q}$, d.h. K ein Zahlkörper so gilt $S(\mathbb{Z}_K) \subset \mathbb{Z}$, wo $S := S_{K/\mathbb{Q}}$ sei. Denn mit α sind auch alle $\sigma_j(\alpha)$ ganzalgebraisch (wo σ_i die Einbettungen $K \to \mathbb{C}$ durchläuft). $S(\alpha)$ ist dann also ganzalgebraisch und liegt in $\mathbb{Q}$, folglich in $\mathbb{Z}$.

Theorem 5.5 *Sei $K \supset \mathbb{Q}$ eine Körpererweiterung mit $[K : \mathbb{Q}] = n < \infty$. Dann gilt für die additiven Gruppen $\mathbb{Z}_K \cong \mathbb{Z}^n$. Für die additive Gruppe jedes von (0) verschiedenen Ideals I von $\mathbb{Z}_K$ gilt ebenfalls $I \cong \mathbb{Z}^n$.*

Proof: Einer Teilmenge $M \subset K$ ordnen wir die Menge $\tilde{M} := \{x \in K \mid S(xM) \subset \mathbb{Z}\}$ zu. Für diesen „Operator“ gilt:

a) $\tilde{M}$ ist eine Untergruppe der additiven Gruppe von K

b) $M_1 \subset M_2 \Longrightarrow \tilde{M_1} \supset \tilde{M_2}$

c) $\tilde{\mathbb{Z}_K} \supset \mathbb{Z}_K$.

Sei nun $(\alpha_1, \ldots, \alpha_n)$ eine Basis von K über $\mathbb{Q}$ mit $\alpha_j \in \mathbb{Z}_K$. Eine solche gibt es, da ein ganzzahliges Vielfaches von jedem Element $\alpha \in K$ ganzalgebraisch ist. Ist $M := \{\alpha_1, \ldots, \alpha_n\}$, so gilt $\tilde{M} \supset \tilde{\mathbb{Z}_K} \supset \mathbb{Z}_K$ wegen b) und c).

Betrachte die Abbildung $\varphi : \tilde{M} \to \mathbb{Z}^n$, $x \mapsto \Big(S(x\alpha_1), \ldots, S(x\alpha_n)\Big)$. (Nach Definiton von $\tilde{M}$ ist $S(x\alpha_j) \in \mathbb{Z}$.) Diese Abbildung ist ein Gruppenhomomorfismus, weil S ein solcher ist. Sie ist auch injektiv. Denn $\varphi(x) = 0$ bedeutet, dass $S(x\alpha_j) = 0$ für alle j, also $S(xy) = 0$ für alle $y \in K$. Wäre $x \neq 0$, so hieße das $S(z) = 0$ für alle $z \in K$, was nicht so ist.

Insgesamt bekommt man einen injektiven Gruppenhomomorfismus $\mathbb{Z}_K \to \mathbb{Z}^n$, also $\mathbb{Z}_K \cong \mathbb{Z}^m$ mit einem $m \leq n$. Andererseits ist $\mathbb{Z}^n \cong \mathbb{Z}\alpha_1 + \cdot + \mathbb{Z}\alpha_n \subset \mathbb{Z}_K$. Somit gilt auch $n \leq m$.

Ist nun I ein von (0) verschiedenes Ideal von $\mathbb{Z}_K$ und $a \in I - \{0\}$, so gilt $\mathbb{Z}_K \cong a\mathbb{Z}_K \subset I \subset \mathbb{Z}_K$ für die additiven Gruppen, also auch $I \cong \mathbb{Z}^n$. □

Corollary 5.6 *Die Ideale von $\mathbb{Z}_K$ sind endlich erzeugt. D.h. in jedem Ideal I gibt es endlich viele Elemente, $a_1, \ldots, a_n$, derart dass jedes Element $b \in I$ von der Form $x_1a_1 + \cdots + x_na_n$ mit $x_j \in \mathbb{Z}_K$ ist.*

In der Tat ist jedes Erzeugendensystem von I als abelscher Gruppe ein Erzeugendensystem von I als Ideal – aber nicht umgekehrt. Wir werden später sehen, das jedes Ideal eines $\mathbb{Z}_K$ durch 2 Elemente erzeugt werden kann

Für Leser, die wissen, was Moduln sind: Genauso beweist man

Theorem 5.7 *Ist R ein Hauptidealring mit Quotientenkörper F und $K \supset F$ eine separable Körpererweiterung von endlichem Grad n, ferner $A \subset K$ der Ring aller über R ganzen Elemente von K, so ist A als R-Modul isomorf zu R^n.*

Für gewisse allgemeinere (sog. noethersche, ganz abgeschlossene)R kann man noch schließen, dass A als R-Modul endlich erzeugt ist. Ist $K \supset F$ inseparabel, so gilt dies nicht mehr allgemein.

6 Gebrochene Ideale und Dedekindringe

Definition 6.1 *Seien I, J Ideale eines Ringes A. Mit IJ wird die von $\{ab \mid a \in I, b \in J\}$ erzeugte additive Untergruppe von A bezeichnet. D.h. $IJ := \{\sum_j a_j b_j \mid a_j \in I, b_j \in J\}$.*

Remarks 6.2 a) Für Hauptideale $I = Aa, J = Ab$ gilt $IJ = Aab$. Ist $I = Aa$ ein Hauptideal und J ein beliebiges Ideal, so ist $IJ = aJ := \{ax \mid x \in J\}$. (In beiden Fällen muss A kommutativ sein.)

b) IJ ist wieder ein Ideal, und zwar das von $\{ab \mid a \in I, b \in J\}$ erzeugte.

c) $IJ \subset I \cap J$. Es ist also anders als bei dem Produkt von Untergruppen einer multiplikativ geschriebenen Gruppe.

d) $IJ = JI$ (in einem kommutativen Ring), $(II')I'' = I(I'I'')$, $I(J + J') = IJ + IJ'$. Zur Erinnerung: $I + J := \{a + b \mid a \in I, b \in J\}$ ist das von $I \cup J$ erzeugte Ideal.

6.3 In einem Hauptidealring ist jedes von (0) verschiedene Ideal ein – bis auf die Reihenfolge – eindeutiges Produkt von Primidealen. Dies folgt sofort aus der Existenz und Eindeutigkeit der Zerlegung seiner Elemente in Primfaktoren. Ferner kann man für Hauptidealringe A die multiplikative Halbgruppe der Ideale $\neq (0)$ zu der Gruppe der Teilmengen $Aa \subset Q(A)$ (mit $a \in Q(A)^\times$) ergänzen.

Nun sind zwar unsere Zahlringe $\mathbb{Z}_K$ nicht immer Hauptidealringe, aber die beiden genannten Eigenschaften haben sie dennoch. Sie gehören zu Klasse der **Dedekindringe**, für die diese beiden Eigenschaften kennzeichnend sind.

Definition 6.4 *Ein* **Dedekindring** *ist ein ganz abgeschlossener, noetherscher Integritätsring der* **(Krull-)Dimension** *1. Dabei bedeutet letzteres für einen Integritätsring, dass jedes von* (0) *verschiedenen Primideal maximal ist.*

Die Ringe $\mathbb{Z}[X]$ und $K[X, Y]$ mit einem Körper K sind zwar ganz abgeschlossene noethersche Integritätsringe, aber ihre Dimension ist > 1,da jedes von einem Primelement erzeugte Ideal weder (0) nocht maximal ist.

Proposition 6.5 *Jeder Zahlring $\mathbb{Z}_K$, wo $K \supset \mathbb{Q}$ eine endliche Körpererweiterung ist, ist ein Dedekindring.*

Proof: Wir wissen bereits, dass $\mathbb{Z}_K$ ein noetherscher, ganz abgeschlossener Integritätsring ist. Es bleibt zu zeigen, dass jedes von (0) verschiedene Ideal maximal ist.

Sei $x \in \mathfrak{p} - \{0\}$ und $a_0 x^n + a_1 x^{n-1} + \cdots + a_n = 0$ mit $a_j \in \mathbb{Z}$ und – oBdA – $a_n \neq 0$ eine algebraische Gleichung für x, so ist $a_n \in \mathfrak{p} \cap \mathbb{Z}$, also $\mathfrak{p} \cap \mathbb{Z} \neq (0)$.

Die Inklusion $\mathbb{Z} \hookrightarrow \mathbb{Z}_K$ induziert nach dem Homomorfiesatz einen injektiven Homomorfismus

$$\mathbb{Z}/(\mathfrak{p} \cap \mathbb{Z}) \to A/\mathfrak{p} \ .$$

Es folgt, dass $\mathfrak{p} \cap \mathbb{Z}$ ein Primideal von $\mathbb{Z}$ ist, also – da $\neq (0)$ – gleich einem $p\mathbb{Z}$ mit einer Primzahl p ist. (Allgemein ist das Urbild eines Primideals unter einem Ringhomomorfismus immer ein solches.)

Es ist somit $\mathfrak{p} \supset p\mathbb{Z}_K$, also hat $\mathbb{Z}_K/\mathfrak{p}$ höchstens soviele Elemente wie $\mathbb{Z}_K/p\mathbb{Z}_K$, also wie $\mathbb{Z}^n/p\mathbb{Z}^n$, mithin nur endlich viele Elemente. Jeder endliche Integritätsring ist ein Körper. Deshalb ist $\mathfrak{p}$ maximal.

Den folgenden zweiten Beweis dafür, dass $\mathbb{Z}_K/\mathfrak{p}$ ein Körper ist, bringen wir, weil er auch in allgemeineren Situationen gilt:

Sei $y \neq 0$ ein Element von $\mathbb{Z}_K/\mathfrak{p}$. Eine Ganzheitsgleichung eines Repräsentanten von y in $\mathbb{Z}_K$ ergibt eine Gleichung

$$y^n + a_1 y^{n-1} + \cdots + a_0 = 0$$

mit $a_j \in \mathbb{Z}/p$ wobei man noch $a_o \neq 0$ annehmen kann. (Notfalls dividiere man durch eine geeignete Potenz von y). Bringt man a_0 auf die rechte Seite, so kann man y links ausklammern. Da $-a_0$ in $\mathbb{Z}/p \subset \mathbb{Z}_K/\mathfrak{p}$ eine Einheit ist, sieht man, dass auch y eine solche in $\mathbb{Z}_K/\mathfrak{p}$ ist. Mithin ist $A/\mathfrak{p}$ ein Körper. □

Definition 6.6 *Sei R ein Integritätsring und $K = \mathrm{Q}(R)$. Ein* **gebrochenes Ideal** *von R ist eine Untergruppe I von K mit folgenden Eigenschaften:*

(i) $rx \in I$ für alle $r \in R,\ x \in I$, d.h. I ist ein R-Untermodul von K;

(ii) es gibt ein $s \in R - \{0\}$ mit $sI \subset R$..

Remarks 6.7 a) Die Ideale im üblichen Sinne sind natürlich gebrochene Ideale. Sie werden manchmal auch **ganze Ideale** genannt. Ein gebrochenes Ideal ist genau dann ganz, wenn es in R liegt.

b) Sei R ein Integritätsring, in dem jedes (ganze) Ideal endlich erzeugt ist, wie es z.B. für Zahlringe gilt, so ist für Untergruppen I von K, die (i) erfüllen, die Bedingung (ii) äquivalent mit

(ii') I ist über R endlich erzeugt, d.h. es gibt endlich viele $x_1, \ldots x_r$ mit $I = Rx_1 + \cdots + Rx_r$.

Gilt nämlich (ii'), so ist (ii) für jeden gemeinsamen Nenner s von $x_1, \ldots, x_r$ erfüllt. Gilt umgekehrt (ii) und ist sI von $a_i, \ldots, a_r$ ein endliches Erzeugendensystem von sI, so ist $a_1/s, \ldots, a_r/s$ ein solches für I.

c) Sind I, J gebrochene Ideal von R, so ist auch IJ ein solches, wobei IJ genauso wie das Produkt ganzer Ideale definiert ist. Offenbar folgt aus $sI \subset R, rJ \subset R$ nämlich $sIJ \subset R$.

Proposition 6.8 *Sind I, J gebrochene Ideale $\neq (0)$, so ist es auch*

$$I : J := \{x \in K \mid xJ \subset I\}$$

Proof: $I : J$ ist sicher eine additive Untergruppe von K und erfüllt obige Bedingung (i). Um (ii) zu beweisen, zeigen wir zunächst, dass es in J ein Element aus $R - \{0\}$ gibt. Nun, $J \neq (0)$ war vorausgesetzt. Ist $y = a/b \in J - \{0\}$ mit $a, b \in R - \{0\}$, so ist $a = by \in R$.

Seien nun $a, s \in R - \{0\}$ mit $a \in J$, $sI \subset R$. Ist nun $x \in I : J$, d.h. $xJ \subset I$, so ist $sxJ \subset R$, also $sxa \in R$. Somit gilt $as(I : J) \subset R$, womit Bedingung (ii) für $I : J$ gezeigt ist. □

6.9 Das Ideal R von R ist in der multiplikativen Halbgruppe aller gebrochenen Ideale das neutrale Element. Sucht man nach dem möglichen Inversen eines von (0) verschiedenen gebrochenen Ideals, so kommt sicher nur $R : I$ in Frage. Denn dieses ist das größte gebrochene Ideal J mit $IJ \subset R$.

Nun ist es keineswegs so, dass für jeden Integritätsring R das Ideal $R : I$ zu I multiplikativ invers wäre. (Ist z.B. $R = \mathbb{Q}[X, Y]$ und $I = (X, Y)$, so sieht mn leicht $R : I = R$, also $I(R : I) = I \neq R$.) Aber für unsere Zahlringe ist es so, wie wir jetzt sehen werden.

Proposition 6.10 *a) Für ein gebrochenes Ideal $I \neq (0)$ eines Integritätsringes R sind folgende Aussagen äquivalent:*

(i) Es gibt ein gebrochenes Ideal J mit $IJ = R$.

(ii) Es ist $I(R : I) = R$.

(iii) Es gibt (endlich viele) $a_1 \ldots, a_n \in I$ und $b_1, \ldots, b_n \in R : I$ mit $\sum_{i=1}^{n} a_i b_i = 1$.

b) Gilt ferner $IJ = R$, so ist $J = R : I$.

c) Hat I die Eigenschaften (i) bis (iii) aus a), so ist I endlich erzeugt. (Von einer Umkehrung kann nicht die Rede sein.)

Proof: „$(ii) \Longrightarrow (i)$“ ist trivial.

Nach Definition gilt $IJ \subset R$ genau dann, wenn $J \subset R : I$ ist. Also folgt „$(i) \Longrightarrow (ii)$“.

„$(ii) \Longrightarrow (iii)$“ ist trivial.

(iii) bedeutet $1 \in I(R : I) \subset R$ also (ii).

b) Aus $IJ = R$ folgt $I(R : I) = R$ wegen a). Deshalb ist $J = J \cdot I \cdot (R : I) = R : I$.

c) Ist $x \in I$, so gilt mit a_i, b_i wie in (iii) folgendes $x = x \cdot 1 = x \sum_i a_i b_i = \sum_i (xb_i)a_i$. Da $b_i \in R : I$, ist $xb_i \in R$. Es folgt, dass I von $a_1, \ldots, a_n$ erzeugt ist. □

Definitions 6.11 *a) Ein gebrochenes Ideal eines Integritätsringes heißt* **invertierbar**, *wenn es die o.a. äquivalenten Eigenschaften (i) bis (iii) hat.*

b) Ist I ein invertierbares Ideal von A, so wollen wir $I^{-1} := A : I$ schreiben.

Um zu zeigen, dass alle von (0) verschiedenen Ideale eines Zahlrings $A = \mathbb{Z}_K$ invertierbar sind, beweisen wir mehrere Lemmata.

Lemma 6.12 *Sei A ein noetherscher Integritätsring, $I \neq (0)$ ein Ideal von A. Es gibt endlich viele Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \neq (0)$ mit $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset I$.*

Proof: Wäre dieMenge der Ideale $I \neq (0)$, die o.a. Eigenschaft nicht haben, nicht leer, so hätte sie ein maximales Element J. Dieses ist kein Primideal und auch nicht gleich A ($r = 0$). Also gibt es $x, y \in A - J$ mit $xy \in J$. Wegen der Maximalität von J erfüllen die echt größeren Ideale $J + Ax,\ J + Ay$ die Aussage des Satzes: $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset J + Ax,\ \mathfrak{p}_{r+1} \cdots \mathfrak{p}_{r+s} \subset J + Ay$. Somit ist $\mathfrak{p}_1 \cdots \mathfrak{p}_{r+s} \subset (J + Ax)(J + Ay) \subset J$, Widerspruch! □

Lemma 6.13 *Sei $\mathfrak{m}$ ein maximales Ideal eines Integritätsringes A der Dimension 1. Es gilt $A : \mathfrak{m} \neq A$.*

Proof: Sei $a \in \mathfrak{m} - (0)$ und seien $\mathfrak{p}_1, \ldots \mathfrak{p}_r$ Primideale mit $Aa \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r$. Wir dürfen noch annehmen, dass r minimal ist. Da $\mathfrak{m}$ ein Primideal ist, muss $\mathfrak{m} \supset \mathfrak{p}_j$ für ein j gelten, etwa für $j = 1$. Da jedes von (0) verschiedene Primideal maximal ist, gilt dann schon $\mathfrak{p}_1 = \mathfrak{m}$. Wegen der Minimalität von r ist aber $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subset Aa$. Sei $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r - Aa$. Dann ist $b\mathfrak{m} \subset \mathfrak{m}\mathfrak{p}_2 \cdots \mathfrak{p}_r \subset Aa$, folglich $(b/a)\mathfrak{m} \subset A$, aber $b/a \notin A$ wegen $b \notin Aa$. Somit ist $b/a \in (A : \mathfrak{m}) - A$. □

Lemma 6.14 *Jedes maximale Ideal eines Dedekindringes A ist invertierbar.*

Proof: Zum Beweis ziehen wir noch die Ganz-Abgeschlossenheit von A heran. Wegen $A \subset A : \mathfrak{m}$ und der Definition von $A : \mathfrak{m}$ gilt $\mathfrak{m} \subset \mathfrak{m}(A : \mathfrak{m}) \subset A$. Ist also das maximale Ideal $\mathfrak{m}$ nicht invertierbar, so ist $\mathfrak{m}(A : \mathfrak{m}) = \mathfrak{m}$. Es gibt ein $x \in (A : \mathfrak{m}) - A$. Für ein solches gilt also $x\mathfrak{m} \subset \mathfrak{m}$, also $x^{j+1}\mathfrak{m} \subset x^j\mathfrak{m}$ Hieraus schließt man $x^n\mathfrak{m} \subset \mathfrak{m} \subset A$. Es folgt $A[x] \subset A : \mathfrak{m}$. Da A noethersch ist, ist $A : \mathfrak{m}$ ein endlich erzeugter A-Modul, und $A[x]$ desgleichen. Es folgt $x \in A$, Widerspruch. □

Theorem 6.15 *Sei A ein Dedekindring. Dann gilt:*

a) Jedes Ideal $I \neq (0)$ ist ein Produkt von maximalen Idealen.

b) Eine solche Produktzerlegung ist – bis auf die Reihenfolge – eindeutig.

c) Jedes gebrochene Ideal $\neq (0)$ ist invertierbar.

Proof: a) Gölte dies nicht, so hätte die Menge der Ideale, die nicht dergestalt zerlegbar sind, ein maximales Element I. Da $I \neq A$ ist, gibt es ein maximales Ideal $\mathfrak{m}$ mit $I \subset \mathfrak{m}$, also $I \subset \mathfrak{m}^{-1}I \subset A$.

Behauptung: $I \neq \mathfrak{m}^{-1}I$

Ansonsten wäre $xI \subset I$ für alle $x \in \mathfrak{m}^{-1}$. Wie im letzten Beweis folgte daraus $x^nI \subset I$, also $x^n \in A : I$ für alle n. Es folgte $\mathfrak{m}^{-1} \subset A$, was oben schon widerlegt wurde. –

Wegen der Maximalität von I ist $\mathfrak{m}^{-1}I = \mathfrak{p}_2 \cdots \mathfrak{p}_n$ mit gewissen Primidealen $\mathfrak{p}_j$, mithin $I = \mathfrak{p}_1 \cdots \mathfrak{p}_n$, wo $\mathfrak{p}_1 := \mathfrak{m}$ gesetzt wurde.

c) folgt für ganze Ideale aus a), da ein Produkt invertierbarer Ideale offenbar invertierbar ist. Ist I ein beliebiges gebrochenes Ideal, so gibt es ein $a \in A - \{0\}$ mit $aI \subset A$. Dann ist $(aI)^{-1}Aa$ zu I invers.

b) Sei I ein maximales Gegenbeispiel und $\mathfrak{m}$ ein maximales Ideal von A mit $\mathfrak{m} \supset I$. In jeder Zerlegung von I in Primideale muss $\mathfrak{m}$ ein Faktor sein. Dann hätte aber das echt größere Ideal $\mathfrak{m}^{-1}I$ auch verschiedene Primfaktorzerlegungen. □

Remark 6.16 Jedes gebrochene Ideal $\neq (0)$ ist auf i.W. eindeutige Weise ein Produkt von Primidealpotenzen mit ganzzahligen Exponenten.

6.17 Ist R ein Dedekindring und A der ganze Abschluss von R in einer endlichen Erweiterung $K \supset Q(R)$, so kann man zeigen, dass A auch ein Dedekindring ist. (Satz von Krull-Akizuki, siehe Bourbaki.) Allerdings muss A

nicht immer endlich über R, d.h. ein endlich erzeugter R-Modul sein. Dies ist allerdings so, wenn K über $Q(R)$ separabel ist, wie wir oben gesehen haben. (Ist A endlich über R, so ist A noethersch, und man sieht wie oben, dass dann A ein Dedekindring ist.) Ist F ein Körper und A der ganze Abschluss von $F[X]$ in einer endlichen Erweiterung von $F(X)$, so ist A endlich über $F[X]$. (S. BIV 9.40)

6.18 Sei A ein Dedekindring. Die Ideale der Form Ax mit $x \in Q(A)$ heißen die **gebrochenen Hauptideale**. Wenn man das 0-Ideal weglässt, bilden sie eine Untergruppe $H(A)$ der Gruppe $I(A)$ der gebrochene Ideale $\neq (0)$. Die Faktorgruppe $C(A) := I(A)/H(A)$ heißt die **Klassengruppe** von A (manchmal auch von $Q(A)$) und ihre Elementezahl heißt die **Klassenzahl.**

Genau dann ist $C(A) = \{1\}$, wenn A ein Hauptidealring ist. Je größer $C(A)$ ist, umso mehr ist A davon entfernt, ein Hauptidealring zu sein. Es gibt viele Dedekindringe mit unendlicher Klassenzahl.

Für unsere Zahlringe gilt die bemerkenswerte Tatsache, dass ihre Klassenzahl endlich ist. D.h. man kann sagen, sie seien fast Hauptidealringe.

In dem nächste Paragrafen (der nicht für diese Vorlesung geschrieben wurde) wird in der Vorlesung ein erster Beweis der Endlichkeit der Klassenzahl gebracht. Später werden wir noch einen weiteren Beweis kennenlernen, der mit der berühmten Methode der Geometrie der Zahlen von Minkowski arbeitet und den Vorzug hat, viel bessere obere Schranken für die Klassenzahl zu liefern.

7 The Finiteness of the Class Number

Our goal is to prove the following important classical result.

Theorem 7.1 *Let $R = \mathbb{Z}$ or $R = F[X]$ with a finite field F. Let further $A \supset R$ be a finite ring extension, A a domain. Then there are only finitely many isomorphism classes of ideals of A. Especially,* $\mathrm{Pic}(A)$ *is a finite group.*

($\mathrm{Q}(A)$ is a so named global field and A an order in it.)

Remarks 7.2 a) Recall the following facts on ideals, fractional ideals and rank 1 projective modules of a domain A. Ideals I, J are isomorphic, iff there is an $x \in \mathrm{Q}(A)^\times$ with $xI = J$. By (**??**) every rank 1 projective module over the domain A is isomorphic to an invertible ideal of A. Especially $\mathrm{Pic}(A) \cong (A)/(A)$, where (A) denotes the group of invertible fractional ideals, (A) that of principal fractional ideals of A. Note that every fractional ideal is isomorphic to an 'integral' one, i.e. one contained in A. (If $I \subset s^{-1}A$, then $sI \subset A$.)

b) If A is the integral closure of R in a finite field extension of $\mathrm{Q}(R)$, then A is finite over R according to (**??**) and (**??**).

7.3 If $f \in R - (0)$, then R/fR is a finite ring. We define $|f| := \#(R/Rf)$ if $f \neq 0$ and $|0| = 0$. If $R = \mathbb{Z}$ this is the usual absolute value. If $R = F[X]$, $q := \#F$ and $f \in R - (0)$ we have $|f| = q^{\deg(f)}$. In both cases:

$$|fg| = |f| \cdot |g| \quad \text{and} \quad |f + g| \leq |f| + |g|. \tag{1}$$

(Even $|f + g| \leq \{|f|, |g|\}$ in the case $R = F[X]$.)

As an R-module the ring A is torsion-free and f.g., hence free. Since $K = \mathrm{Q}(A) = \{a/s \mid a \in A, s \in R - (0)\}$ by Remark **??**b), clearly A is of rank $n := [\mathrm{Q}(A) : \mathrm{Q}(R)]$. Fix an R-basis $\alpha_1, \ldots, \alpha_n$ of A. This is also a basis of $\mathrm{Q}(A)$ as a vector space over $\mathrm{Q}(R)$.

Now let $I \neq (0)$ be an ideal of A. It is also a f.g. torsion-free R-module, hence free. Let $\alpha \in I - (0)$. Then the homothesy of α on the $\mathrm{Q}(R)$-vector-space $\mathrm{Q}(A)$ is an automorphism. Therefore $\alpha\alpha_1, \ldots, \alpha\alpha_n$ are linearly independent over $\mathrm{Q}(R)$, hence over R. It follows that I, contained in A and containing $\alpha\alpha_1, \ldots, \alpha\alpha_n$, is a free R-module of rank n and that A/I is a finite ring. We write $\|I\| := \#(A/I)$.

Lemma 7.4 *Let $\alpha \in A$ and h_α denote the homothesy of α on A, regarded as a free R-module. Then:*

a) $\det(h_\alpha) \in A\alpha$,

b) $\|A\alpha\| = |\det(h_\alpha)|$.

Proof: The case $\alpha = 0$ being clear, assume $\alpha \neq 0$. By the Elementary Divisor Theorem **??** there are an R-basis $\alpha'_1, \ldots, \alpha'_n$ of A and $d_1, \ldots, d_n \in R$ with $\alpha\alpha'_i = d_i\alpha'_i$. So $\det(h_\alpha) = d := d_1 \cdots d_n \in A\alpha$.

Further both sides of *b)* are equal to $|d|$. □

As a consequence of *a)* we see that $I \cap R \neq (0)$ for every non-zero ideal I of A, in other words, that A/I is a torsion module over R.

Lemma 7.5 *There is an integer $C > 0$ such that in every non-zero ideal I of A there is a $\gamma \neq 0$ with $\|A\gamma\| \leq C\|I\|$, i.e. $\#(I/A\gamma) \leq C$.*

Proof: Let $\alpha_i\alpha_j = \sum_{i,j,k} a_{ijk}\alpha_k$ with $a_{ijk} \in R$. For $\beta = \sum_j b_j\alpha_j$ with $b_j \in R$ we have $\beta\alpha_i = \sum_{j,k} b_j a_{ijk}\alpha_k$. So $\det(h_\beta)$ is a homogeneous polynomial of degree n in the b_j over R. Therefore by (1) there is a $C \in \mathbb{N}$ such that $|b_j| \leq r$ implies $|\det(h_\beta)| \leq Cr^n$.

Now let $I \neq (0)$ be an ideal of A. To find γ, we distiguish two cases.

Case 1: $R = \mathbb{Z}$. Let $m \in \mathbb{N}$ be such that $m^n \leq \|I\| < (m+1)^n$. At least two of the following $(m+1)^n$ elements

$$\sum_{j=1}^{n} b_j\alpha_j, \quad b_j \in \mathbb{Z}, \quad 0 \leq b_j \leq m$$

must be congruent modulo I, since $\#(A/I) < (m+1)^n$. Their difference will be our γ.

Case 2: $R = F[X]$. Let $q = \#F$ and $s \in \mathbb{N}$, such that $q^{sn} \leq \|I\| < q^{(s+1)n}$. Two of the following $q^{(s+1)n}$ elements

$$\sum_{j=1}^{n} b_j\alpha_j, \quad b_j \in F[X], \quad |b_j| \leq q^s \ \text{ (i.e. } \deg(b_j) \leq s)$$

must be congruent modulo I. Again call their difference γ.

In both cases γ has the properties:

(i) $\gamma \in I - (0)$,

(ii) $\gamma = \sum_{j=1}^{n} m_j \alpha_j, \quad m_j \in R, \quad |m_j|^n \leq \|I\|, \quad$ hence

(ii') $\|A\gamma\| = |\det(h_\gamma)| \leq C\|I\|$.

The latter follows from (ii) and the considerations at the beginning of the proof. □

Proof of Theorem 7.1: Let $c \in R$ be the product of all $a \in R - (0)$ with $|a| \leq C$. (There are only finitely many of them.) We will show that every ideal $I \neq (0)$ of A is isomorphic to one between A and Ac. Since A/Ac is a finite ring there are only finitely many of the latter.

Choose γ as in Lemma 7.5. Then $I\gamma^{-1}/A \cong I/A\gamma$ is of order $\leq C$. There is an R-module isomorphism $I\gamma^{-1}/A \cong R/(d_1) \oplus \cdots \oplus R/(d_m)$ with suitable $d_i \in R - (0)$. Then $|d_i| \leq C$, whence $d_i | c$. So $c(I\gamma^{-1}/A) = 0$, i.e. $c\gamma^{-1}I \subset A$. On the other hand $cA \subset c\gamma^{-1}I$, and we are done. □

Corollary 7.6 *Let A be as above. For every $n \in \mathbb{N}$ there are only finitely many isomorphism classes of projective A-modules P of rank n.*

Proof: Since $\dim(A) = \dim(R) = 1$, by Proposition **??** we have $P \cong I \oplus A^{n-1}$ with an invertible ideal I. □

A strong generalization of the theorem and its corollary is the Jordan-Zassenhaus Theorem. See [Swan??] Theorem 3.9.

The finiteness of class number has other interesting consequences:

Proposition 7.7 *Let A be a Dedekind ring with finite Picard group. (Or more general, let A be any domain with only finitely many isomorphism classes of ideals.) Then there is an $f \in A - (0)$, such that A_f is a PID.*

Proof: Let the ideals $I_1, \ldots, I_n$ represent the isomorphism classes of the non-zero ideals and choose $f \in I_1 \cdots I_n - (0)$. Then every non-zero ideal of A_f is isomorphic to one of the $(I_j)_f = A_f$, hence principal. □

Proposition 7.8 *Let A be a Dedekind ring whose Picard group is a torsion group. Then for every ideal I of A there is an $f \in I$ with $\sqrt{I} = \sqrt{Af}$. In the terminology of the next chapter, every ideal is a set theoretical complete intersection.*

Proof: For $I \neq (0)$ there is an r with $I^r = Af$ for some $f \in A$. This f has the required property. □

8 Diskriminante

Die Bedeutung der Diskriminante für die Algebraische Zahlentheorie kann gar nicht überschätzt werden.

Definition 8.1 *Sei $A \subset B$ eine Ringerweiterung derart, dass B ein freier A-Modul vom endlichen Rang n ist, und $(x_1, \ldots, x_n) \in B^n$. Wir definieren die Diskriminante* $\mathrm{disc}(x_1, \ldots, x_n)$ *durch*

$$\mathrm{disc}(x_1, \ldots, x_n) := \det(S(x_i x_j))_{i,j}$$

Remark 8.2 Wenn $(y_1, \ldots, y_n)$ durch die Matrix $\alpha := (a_{ij})_{i,j} \in \mathrm{M}_n(A)$ aus $(x_1, \ldots, x_n)$ hervorgeht, so ist

$$\mathrm{disc}(y_1, \ldots, y_n) = \det(\alpha)^2 \mathrm{disc}(x_1, \ldots, x_n)$$

Denn $S(y_p y_q) = S(\sum_{i,j} a_{pi} a_{qj} x_i x_j) = \sum_{i,j} a_{pi} a_{qj} S(x_i x_j)$. Hieraus folgt die Matrix-Gleichung:

$$(S(y_p y_q)) = (a_{pi})(S(x_i x_j)^t (a_{qj})$$

also die behauptete Gleichung für die Determinanten.

Sind also $(x_1, \ldots, x_n)$ und $(y_1, \ldots, y_n)$ Basen von B über A und ist deshalb α invertierbar, so unterscheiden sich $\mathrm{disc}(x_1, \ldots, x_n)$ und $\mathrm{disc}(y_1, \ldots, y_n)$ um eine Einheit, sogar um das Quadrat einer Einheit. Die Ideale $\mathrm{disc}(x_1, \ldots, x_n)A$ und $\mathrm{disc}(y_1, \ldots, y_n)A$ stimmen mithin überein.

Ist $A = \mathbb{Z}$, so gilt unter o.a. Voraussetzung sogar $\mathrm{disc}(x_1, \ldots, x_n) = \mathrm{disc}(y_1, \ldots, y_n)$.

Definition 8.3 *Die Diskriminante $\mathcal{C}(B/A)$ der Ringerweiterung $A \subset B$ ist das Ideal $A \cdot \mathrm{disc}(x_1, \ldots, x_n)$, wo $(x_1, \ldots, x_n)$ eine Basis des A-Moduls B ist.*

Proposition 8.4 *Seien $K \subset L$ eine separable endliche Körpererweiterung, $\sigma_1, \ldots, \sigma_n$ die verschiedenen K-Einbettungen von L in $\overline{K}$ und $(x_1, \ldots, x_n)$ eine Basis dieser Erweiterung, so ist*

$$\mathrm{disc}(x_1, \ldots, x_n) = (\det(\sigma_i(x_j))^2 \neq 0$$

Proof:

$$\mathrm{disc}(x_1, \ldots, x_n) = \det(\sum_k \sigma_k(x_i x_j) \tag{2}$$

$$= \det(\sum_k (\sigma_k(x_i)\sigma_k(x_j)) = \det(\sigma_k((x_i) \det(\sigma_k(x_i)) \tag{3}$$

Wäre $\det(\sigma_i(x_j)) = 0$, so wären die Zeilen der Matrix linear abhängig. Dann wären aber auch die Charaktere $\sigma_1, \ldots, \sigma_n$ linear abhängig. □

Wir wollen eine spezielle Diskriminante berechnen.

Lemma 8.5 *Sei $K \subset K(\alpha)$ eine separable algebraische einfache Körpererweiterung vom Grad n und $f := \mathrm{Mipo}_K(\alpha)$. Ferner seien $\alpha_1, \ldots, \alpha_n$ die Konjugierten von α. Dann gilt*

$$\mathrm{disc}(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{1 \le r < s \le n} (\alpha_r - \alpha_s)^2 = \pm N(f'(\alpha) \qquad (4)$$

wobei das Vorzeichen ein + genau dann ist, wenn $n \equiv 0$ oder 1 modulo 4 ist.

Proof: Durch $\sigma_i(\alpha) = \alpha_i$ werden die verschiedenen Einbettungen $K(\alpha) \to \overline{K}$ definiert. Die Determinante

$$\det(\sigma_i(\alpha^j))_{i,j} = \det((\sigma_i(\alpha))^j) = \det(\alpha_i^j)$$

ist die Vandermondesche Determinante, hat also den Wert

$$\prod_{1 \le r < s \le n} (\alpha_s - \alpha_r).$$

Daraus folgt die erste Gleichheit in (4).

Für die zweite Geichheit sieht man zunächst

$$\prod_{1 \le r < s \le n} (\alpha_s - \alpha_r) = \pm \prod_{(r,s),\ r \ne s} (\alpha_r - \alpha_s)$$

Denn links und rechts stehen bis aufs Vorzeichen dieselben Faktoren. (Und zwar haben $n(n-1)/2$ Faktoren links und rechts verschiedene Vorzeichen. Hieraus folgt die Aussage über das genaue Vorzeichen.)

Es ist

$$f = \prod_{s=1}^{n} (X - \alpha_s) \qquad (*)$$

Also ist f' die Summe von n Produkten, wo von $(*)$ jeweils ein Faktor gestrichen ist. Setzt man α_r ein, so bleibt ein Summand übrig. Also

$$f'(\alpha_r) = \prod_{s,\ s \ne r} (\alpha_r - \alpha_s).$$

Deshalb gilt

$$N(f'(\alpha)) = \prod_r \sigma_r(f'(\alpha)) = \prod_r f'(\alpha_r) = \prod_{(r,s),\ r \ne s} (\alpha_r - \alpha_s)$$

□

Definition 8.6 *Wir schreiben in obiger Situation* $\mathrm{disc}(\alpha) := \mathrm{disc}(1, \alpha, \ldots, \alpha^{n-1})$

Später benötigen wir:

Corollary 8.7 *Sei ω eine primitive m-te Einheitswurzel. Dann ist* $\mathrm{disc}(\omega)$ *eine Teiler von $m^{\varphi(m)}$*

Proof: Sei f das m-te Kreisteilungspolynom. Dann gibt es ein $g \in \mathbb{Z}[X]$ mt $X^m - 1 = fg$. Durch Ableitung ergibt sich $mX^{m-1} = f'g + fg'$. Wir setzen ω für X ein und erhalten: $m\omega^{m-1} = f'(\omega)g(\omega)$, also $m = f'(\omega)\omega g(\omega)$. Nun bilden wir die Norm: $m^{\varphi(m)} = \pm\mathrm{disc}(\omega)N((\omega)$. Da die Norm eines ganzalgebraischen Elementes in $\mathbb{Z}$ liegt, ist das Korollar bewiesen. □

Proposition 8.8 *Sei K ein Zahlkörper mit einer Basis $\alpha_1, \ldots, \alpha_n$ über $\mathbb{Q}$, die aus ganzalgebraischen Elementen besteht, ferner $d := \mathrm{disc}(\alpha_1, \ldots, \alpha_n)$. Dann ist jede ganzalgebraische Zahl aus K von der Form*

$$\frac{m_1\alpha_1 + \cdots + m_n\alpha_n}{d}$$

mit $m_j \in \mathbb{Z}$ und $d|m_j^2$ für alle j.

Proof: Sei $\alpha \in \mathbb{Z}_K,\ \alpha := x_1\alpha_1 + \cdots + x_n\alpha_n$ mit $x_i \in \mathbb{Q}$. Indem man alle Einbettungen $\sigma_i : K \to \mathbb{C}$ auf diese Gleichung anwendet, bekommt man das Gleichungssystem

$$\sigma_i(\alpha) = x_1\sigma_i(\alpha_1) + \cdots + x_n\sigma_i(\alpha_n)\ ,\quad I = 1, \ldots, n$$

Sei δ die Determinante der Koeffizientenmatrix. Wir wissen $\delta^2 = d$. Nach der Cramerschen Regel gilt $x_j = \gamma_j/\delta = \delta\gamma_j/d$, wobei γ_j eine Determinante einer Matrix mit Einträgen aus $\mathbb{Z}_K$, also selber aus $\mathbb{Z}_K$ ist. Ebenso ist $\delta \in \mathbb{Z}_K$.

Da $\delta\gamma_j/d \in \mathbb{Q}$ ist $m_j := \delta\gamma_j \in \mathbb{Z}_K \cap \mathbb{Q} = \mathbb{Z}$. Schließlich ist $m_j^2/d = \delta^2\gamma_j^2/\delta^2 \in \mathbb{Q} \cap \mathbb{Z}_K = \mathbb{Z}$. □

9 Ganze Zahlen in Kreisteilungskörpern

9.1 Sei ω eine primtive m-te Einheitswurzel und $K := \mathbb{Q}(\omega)$. Dann ist sicher $\mathbb{Z}(\omega) = \mathbb{Z} + \mathbb{Z}\omega + \cdots + \mathbb{Z}\omega^{\varphi(m)-1}$ eine Teilmenge von $\mathbb{Z}_K$ ist. Wir wollen zeigen, dass sogar die Gleichheit gilt.

Lemma 9.2 *a)* $\mathbb{Z}[\omega] = \mathbb{Z}[1-\omega]$ *b)* $\mathrm{disc}(\omega) = \mathrm{disc}(1-\omega)$,
c) Ist $m > 2$*, so ist* $N(\omega) = 1$, *d) Ist* $m = p^r$ *mit einer Primzahl* p *und* $r \geq 1$*, so gilt* $N(1-\omega) = p$

Proof: a) ist trivial.

b) folgt aus a) und Bemerkung 8.2. Ebenso kann man es aus Satz 8.8 folgern, da $(\omega_r - \omega_s)^2 = ((1-\omega_r) - (1-\omega_s))^2$ ist.

c) $N(\omega)$ ist das Produkt der verschiedenen primitiven m-ten Einheitswurzeln. Ist aber ζ eine primitive m-te Einheitswurzel, so auch ζ^{-1}. Und für $m \geq 3$ ist dann $\zeta \neq \zeta^{-1}$.

d) ζ ist genau dann eine primitive p^r-te Einheitswurzel, wenn ζ eine Nullstelle des Polynoms $X^{p^r} - 1$, aber keine Nullstelle von $X^{p^{r-1}} - 1$ ist. D.h. die primitiven p^r-ten Einheitswurzeln sind die Nullstellen von

$$f(X) := \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1} = 1 + X^{p^{r-1}} + X^{2p^{r-1}} + \cdots + X^{(p-1)p^{r-1}}$$

Da $f(X) = \prod_\zeta (X - \zeta)$ ist, wo ζ die primitiven p^r-ten Einheitswurzeln durchläuft, ist $N(1-\omega) = f(1) = p$. □

Theorem 9.3 *Sei* ω *eine primitive* p^r*-te Einheitswurzel und* $K := \mathbb{Q}(\omega)$*. Dann ist* $\mathbb{Z}_K = \mathbb{Z}[\omega]$*.*

Proof: Nach (8.8) kann jedes $\alpha \in \mathbb{Z}_K$ geschrieben werden in der Form

$$\alpha = \frac{m_0 + m_1(1-\omega) + \cdots + m_{n-1}(1-\omega)^{n-1}}{d},$$

wo $n = \varphi(p^r$ und $d = \mathrm{disc}(1-\omega) = \mathrm{disc}(\omega)$ ist. Nach Korollar 8 ist d ein Teiler von $(p^r)^{\varphi}(p^r)$ also eine p-Potenz. Wir nehmen jetzt an, es gäbe ein $\alpha \in \mathbb{Z}_K - \mathbb{Z}[1-\omega]$. Durch Kürzen Multiplikation mit einer p-Potenz und Subtraktion eines Elementes von $\mathbb{Z}[1-\omega]$ erhält man ein Element $\mathbb{Z}_K$ von der Form

$$\beta = \frac{m_i(1-\omega)^i + \cdots + m_{n-1}(1-\omega)^{n-1}}{p}$$

mit $p \nmid m_i$. Wegen c) des obigen Lemmas ist $p(1-\omega)^{-n} \in \mathbb{Z}[\omega]$. Denn p ist Produnkt von n Faktoren der Form $1-\omega^k$ und jeder dieser Faktoren ist in $\mathbb{Z}[\omega]$ durch $1-\omega$ teilbar. Also ist auch $p(1-\omega)^{-i-1} \in \mathbb{Z}[\omega]$ und somit $\beta p(1-\omega^{-i-1} \in \mathbb{Z}_K$. Indem wir noch ein Element von $\mathbb{Z}_K$ subtrahieren, erhalten wir $m_i(1-\omega)^{-1} \in \mathbb{Z}_K$. Es folgt, dass $P = N(1-\omega)$ ein Teiler von $m_i^n = N(m_i)$ ist, im Widerspruch zu $p \nmid m_i$. □

9.4 Um den entsprechenden Satz für beliebige m-te Einheitswurzeln zu zeigen, benötigen wir ein allgemeines Theorem über den Ring der ganen Zahlen in einem Körperkompositum. Seien $K, L \subset \mathbb{C}$ Zahlkörper und $(x_1, \ldots, x_n)$ bzw. $(y_1, \ldots, y_m)$ Ganzheitsbasen von K, bzw. L. Ist ferner $[KL : \mathbb{Q}] = nm$, so ist $(x_i y_j)_{i,j}$ eine Körperbasis von KL, die aus ganzalgebraischen Elementen besteht, und der von ihnen erzeugte $\mathbb{Z}$-Modul $E = \mathbb{Z}_k\mathbb{Z}_L$ ist ein Unterring von $\mathbb{Z}_{KL}$.

Aber in vielen Fällen ist $E \neq \mathbb{Z}_{KL}$. Immerhin gilt:

Theorem 9.5 *In obiger Situation sei d der g.g.T. der beiden Diskriminanten* $\mathrm{disc}(x_1, \ldots, x_n)$ *und* $\mathrm{disc}(y_1, \ldots, y_m)$*. Dann gilt*

$$\mathbb{Z}_{KL} \subset \frac{1}{d}\mathbb{Z}_K \cdot \mathbb{Z}_L \ .$$

Proof: Sei $\alpha \in \mathbb{Z}_{KL}$. Es hat eine Darstellung in der Form

$$\alpha = \frac{1}{r}\sum_{i,j} m_{ij} x_i y_j \qquad (*)$$

mit $m_{ij}, r \in \mathbb{Z}$, wobei man noch $r > 0$ minimal annehmen kann. Es ist zu zeigen: $r|\mathrm{disc}(x_1, \ldots, x_n)$, da dann aus Symmetriegründen auch $r|\mathrm{disc}(y_1, \ldots, y_m)$ gilt.

Die L-Einbettungen $KL \to \mathbb{C}$ entsprechen – per Einschränkung – bijektiv den Einbettungen $K \to \mathbb{C}$. Wendet an eine solche σ auf α an, erhält man aus $(*)$

$$\sigma(\alpha) = \frac{1}{r}\sum_{i,j} m_{ij} y_j \sigma(x_i)$$

Setzen wir

$$w_i := \frac{1}{r}\sum_{j=1}^{n} m_{ijj}$$

so erhält man n Gleichungen

$$\sum_{i=1}^{n} \sigma(x_i) w_i = \sigma(\alpha)$$

eine für jedes σ. Wenn man diese nach der Cramerschen Regel nach den w_i auflöst, erhält man $w_i = \gamma_i/\delta$, wobei $\gamma_i,\ \delta$ ganzalgebraisch sind und $\delta^2 = e := \mathrm{disc}(x_1, \ldots, x_n)$. Dann ist $ew_i = \delta\gamma_i$ ganzalgebraisch, deshalb auch

$$ew_i = \frac{e}{r} \sum_{j=1}^{n} m_{ij} y_j \in \mathbb{Z}_L$$

Da r keinen gemeinsamen Teiler mit allen m_{ij} (wegen der Minimalität), und $y_1, \ldots, y_m$ eine Ganzheitsbasis ist, muss e von r geteilt werden. □

Corollary 9.6 *Sei ω eine primitive m-te Einheitswurzel und $K = \mathbb{Q}(\omega)$, dann ist $\mathbb{Z}_K = (\omega)$.*

Proof: Induktion nach m. Ist m eine Primzahlpotenz, so sind wir bereits fertig. Ansonsten lässt sich m in zwei teilerfremde Faktoren m_1, m_2 zerlegen, die beide $< m$ sind. Sind nun ω_1, und ω_2 je eine primitive m_1-te, bzw. m_2-te Einheitswurzel, so ist $\omega := \omega_1\omega_2$ eine primitive m-te Einheitswurzel. Das impliziert $\omega \in \mathbb{Z}[\omega_1]\mathbb{Z}[\omega_2]$, also $\mathbb{Z}[\omega] \subset \mathbb{Z}_[\omega]\mathbb{Z}[\omega_2]$. Daraus folgt die Gleichheit, da die umgekehrte Inklusion trivial ist. Nach Induktionsannahme sind $\mathbb{Z}[\omega_i]$ bereits die vollen Zahlringe in den Körpern $\mathbb{Q}(\omega_i)$. Umdas Korollar zu beweisen, ist erstens zu zeigen, dass $\mathrm{disc}(\omega_1)$ und $\mathrm{disc}(\omega_2)$ zueinander teilerfremd sind. Dies ist aber so, da $\mathrm{disc}(\omega_i)$ eine Potenz von m_i teilt, und m_1, m_2 teilerfremd sind. Zweitens muss man noch zeigen, dass $[\mathbb{Q}(\omega) : \mathbb{Q}] = [\mathbb{Q}(\omega_1 : \mathbb{Q}][\mathbb{Q}(\omega_2] : \mathbb{Q}]$ ist. Dies bedeutet $\varphi(m_1m_2) = \varphi(m_1)\varphi(m_2)$, was wegen der schwachen Multiplikativität von φ richtig ist. □

10 Minkowskis Geometrie der Zahlen

Definition 10.1 *Eine diskrete Untergruppe des $\mathbb{R}^n$ ist eine Untergruppe der additiven Gruppe von $\mathbb{R}^n$, die mit jeder beschränkten Teilmenge des $\mathbb{R}^n$ nur endlich viele Elemente gemeinsam hat.*

Examples 10.2 a) Sei $0 \leq r \leq n$, dann ist die Abbildung $\mathbb{Z}^r \to \mathbb{R}^n$, $(m_1, \ldots, m_r) \mapsto (m_1, \ldots, m_r, 0, \ldots, 0)$ injektiv, und ihr Bild ist eine diskrete Untergruppe von $\mathbb{R}^n$. Wir werden sehen, dass bis auf Basiswechsel des $\mathbb{R}^n$ alle diskreten Untergruppen von dieser Art sind.

b) Sei K ein quadratischer Zahlkörper. Ist K imaginärquadratisch, so liegt er in $\mathbb{C}$, das wir mit $\mathbb{R}^2$ identifizieren können. Ist K reellquadratisch, so haben wir oben eine Einbettung $K \to \mathbb{R}^2$ angegeben, so dass in beiden Fällen $\mathbb{Z}_K$ zu einer diskreten Untergrupe von $\mathbb{R}^2$ wird. Wir werden sehen, dass man auf analoge Weise jeden Zahlkörper K vom Grad n über $\mathbb{Q}$ in den $\mathbb{R}^n$ so einbetten kann, dass $\mathbb{Z}_K$ zu einer diskreten Untergruppe von $\mathbb{R}^n$ wird.

Proposition 10.3 *Sei H eine diskrete Untergruppe des $\mathbb{R}^n$. dann gibt es $r \leq n$ über $\mathbb{R}$ linear unabhängige Elemente $y_1, \ldots, y_r$, derart dass $H = \mathbb{Z}y_1 + \cdots + \mathbb{Z}y_r$ ist.*

Proof: Seien $e_1, \ldots, e_r \in H$ über $\mathbb{R}$ linear unabhängig, und sei r dabei größtmöglich. (Wir können nicht erwarten, dass sie schon H erzeugen.) Sei

$$P := \{\sum_{j=1}^{r} \alpha_j e_j \mid 0 \leq \alpha_j \leq 1\}$$

das von ihnen aufgespannte abgeschlossene, und deshalb kompakte, Parallelotop. Nach Voraussetzung ist $H \cap P$ endlich. Jedes $x \in H$ ist eine reelle Linearkombination der e_j, da r maximal gewählt: $x = \sum_{j=1}^{r} \lambda_j e_j$. Für jedes $k \in \mathbb{Z}$ setzen wir

$$x_k = kx - \sum_{j=1}^{r} [k\lambda_j] e_j = \sum_{j=1}^{r} (k\lambda_j - [k\lambda_j]) e_j \ ,$$

wo [ ] die Gaußklammer bezeichnet. Aus der ersten Darstellung sieht man $x_k \in H$, aus der zweiten $x_k \in P$.

Ferner ist $x = x_1 + \sum_{j=1}^{r} [\lambda_j] e_j$, also $x \in H$ eine Linearkombination von Elementen aus $P \cap H$ mit Koeffizienten aus $\mathbb{Z}$. Daraus folgt, dass H endlich erzeugt ist, also von der Form $\mathbb{Z}^s$, da H sicher torsionsfrei ist. Da $P \cap H$ endlich, $\mathbb{Z}$ hingegen unendlich ist, gibt es verschiedene k, l mit $x_k = x_l$.

Hiermit folgt $(k-l)\lambda_j = [k\lambda_j] - [l\lambda_j]$ und somit, dass die λ_j rational sind. Sei jedes Element eines endlichen Erzeugendensystems als rationale Linearkombination der e_j dargestellt, und sei $d \neq 0$ ein gemeinsamer Nenner aller Koeffizienten. Dann gilt offenbar $dH \subset \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_r \subset H$, wobei noch H und dH zueinander isomorf sind. Aus der ersten Ungleichung folgt dann $\mathrm{rg}H \leq r$ aus der zweiten $r \leq \mathrm{rg}H$, somit $\mathrm{rg}H = r$.

Ferner weiß man, dass es eine $\mathbb{Z}$-Basis $f_1, \ldots, f_r$ von $\mathbb{Z}e_1 + \cdots + \mathbb{Z}e_r$ gibt, derar dass dH von $(n_1 f_1, \ldots, n_r f_r)$ mit gewissen $n_j \in \mathbb{Z}$ erzeugt wird. Da $\mathrm{rg}H = r$ ist, sind die $n_j \neq 0$. Also ist $(n_1 f_1, \ldots, n_r f_r)$ ein Erzeugendensystem von H, das über $\mathbb{R}$ linear unabhängig ist. □

Definition 10.4 *Ein* **Gitter** *im* $\mathbb{R}^n$ *ist eine diskrete Untergruppe vom Rang* n*.*

10.5 Sei $G \subset \mathbb{R}^n$ ein Gitter. Dann gibt es eine $\mathbb{Z}$-Basis $e = (e_1, \ldots, e_n)$ von G, die auch eine $\mathbb{R}$-Basis des $\mathbb{R}^n$ ist. Für jede andere $\mathbb{Z}$-Basis e' von G gibt es eine Übergangsmatrix $S \in \mathrm{M}_n(\mathbb{Z})$. Für die Übergangsmatrix $S' \in \mathrm{M}_n(\mathbb{Z})$ von e' nach e gilt dann $SS' = 1_n$. Es ist $\det(S)\det(S') = 1$. Da S und S' ganzzahlige Einträge haben, ist nach der Leibniz-Formel $\det(S), \det(S') \in \mathbb{Z}$. Es folgt $\det(S) = \det(S') = \pm 1$.

Da S invertierbar ist, ist e' ebenfalls über $\mathbb{R}$ linear unabhängig.

Das halboffene Parallelotop $P_e := \{\sum_{j=1}^n \lambda_j e_j \mid 0 \leq \lambda_j < 1\}$ hat die Eigenschaft, dass jedes Element von $\mathbb{R}^n/G$ genau einen Repräsentanten in P_e besitzt. Man nennt es auch eine **Grundmasche** von G. Sein Volumen $\mu(P_e)$, (das natürlich mit dem des abgeschlossenen Parallelotops übereinstimmt), ist nur von dem Gitter G und nicht von der speziellen Basis e abhängig. Denn $\mu(P_{e'}) = |\det(S)|\mu(P_e)$. Man nennt es – etwas inkonsequent – auch das **Volumen** $v(G)$ von G.

Natürlich ist $\mu(P_e) = |\det(e_1, \ldots, e_n)|$.

Lemma 10.6 *Seien* G *ein Gitter in* $\mathbb{R}^n$ *und* S *eine messbare Teilmenge in* $\mathbb{R}^n$*, so dass* $\mu(S) > v(G)$*. Dann gibt es in* S *zwei verschiedene Punkte* x, y *mit* $x - y \in G$*.*

Proof: Sei e eine Basis von G und P_e die zugehörige Grundmasche. Der $\mathbb{R}^n$ ist die disjunkte Vereinigung aller $P_e + g$ mit $g \in G$. Also ist auch S disjunkte Vereinigung der $S \cap (P_e + g)$. Somit ist $\mu(S) = \sum_g \mu(S \cap (P_e + g))$. Es gilt $S_g := S \cap (P_e + g)) - g \subset P_e$ und $\mu(S_g) = \mu(S \cap (P_e + g))$. Aus $S_g \subset P_e$ und $\sum_{g \in G} \mu(S_g) = \mu(S) > \mu(P_e)$ folgt: Es gibt verschiedene $g, h \in G$ mit $S_g \cap S_h \neq \emptyset$. D.h. es gibt ein $x \in S \cap (P_e + g)$ und ein $y \in S \cap (P_e + h)$ mit $x - g = y - h$. D.h. $x - y = g - h \in G$ und $x \neq y$, da $P_e + g$und $P_e + h$ disjunkt sind. □

Lemma 10.7 *Sei $S \subset \mathbb{R}^n$ sternförmig bezüglich 0. Dann ist $\bigcap_{\varepsilon>0}(1+\varepsilon)S \subset \overline{S}$, wo $\overline{S}$ den Abschluss von S bezeichnet.*

Proof: Sei $x \in (1+\varepsilon)S - \{0\}$. Dann gibt es ein $y \in S$ mit $x = (1+\varepsilon)y$. Dann ist $|x-y| = |y+\varepsilon y - y| = \varepsilon|y| < \varepsilon|x|$. Ist also $x \in (1+\varepsilon)S$ für alle $\varepsilon > 0$, so liegt in jeder $(\varepsilon|x|)$-Umgebung von x ein Punkt $y \in S$. Also gilt $x \in \overline{S}$.

Aus den Lemmata folgt:

Theorem 10.8 (Minkowski) *Sei G ein Gitter im $\mathbb{R}^n$ und S eine Teilmenge des $\mathbb{R}^n$, die messbar, konvex und symmetrisch bzgl. 0 ist. Ferner gelte eine der folgenden Bedingungen:*

a) $\mu(S) > 2^n v(G)$ oder
b) S ist kompakt und $\mu(S) \geq 2^n v(G)$.

Dann ist $S \cap (G - \{0\}) \neq \emptyset$.

a) Wende das Lemma auf $S' := \frac{1}{2}S$ an. Dann ist $\mu(S') = 2^{-n}\mu(S) > v(G)$. Es gibt also verschiedene $x, y \in S'$ mit $x - y \in G$. Dann gilt $x - y = \frac{1}{2}(2x + (-2y)) \in S$, da S konvex und symmetrisch bzgl. 0 ist. Andererseits ist natürlich $x - y \in G - \{0\}$.

b) Fall a) kann man auf die Menge $(1+\varepsilon)S$ mit $\varepsilon > 0$ anwenden. Die Mengen $(G - \{0\} \cap (1+\varepsilon)S$ sind also nicht leer und außerdem – da $(1+\varepsilon)S$ kompakt ist – natürlich endlich. Da sie eine Kette bilden, ist auch ihr Durchschnitt $(G - \{0\}) \cap S$ nicht leer. □

10.9 Wir werden jetzt für einen Zahlkörper K vom Grad n den Zahlring $\mathbb{Z}_K$ als Gitter im $\mathbb{R}^n$ darstellen. Seien $\sigma_j : K \to \mathbb{C}$, $j = 1, \ldots, n$ die verschiedenen Einbettungen und $\alpha : \mathbb{C} \to \mathbb{C}$ die komplexe Konjugation. Mit $\sigma : K \to \mathbb{C}$ ist auch $\alpha \circ \sigma$ eine Einbettung. Genau dann gilt $\sigma = \alpha \circ \sigma$, wenn $\sigma(K) \subset \mathbb{R}$ eine sogenannte reelle Einbettung ist. Die Anzahl der komplexen, d.h. nicht reellen Einbettungen ist gerade, etwa $= 2s$. Wir bezeichnen die Anahl der reellen Einbettungen mit r. Dann ist $n = r + 2s$.

Wir wählen die Nummerierung der σ_j so, dass die ersten r die reellen Einbettungen sind und $\sigma_{r+s+j} = \alpha \circ \sigma_{r+j}$ für $j = 1, \ldots, s$ ist. Dann sind die n Einbettungen schon durch die ersten $r+s$ bestimmt; und letztere geben einen injektiven (Ring-)Homomorfismus

$$\sigma : K \to \mathbb{R}^r \times \mathbb{C}^s.$$

Als $\mathbb{R}$-Vetorraum identifizieren wir $\mathbb{C}$ mit $\mathbb{R}^2$, also $\mathbb{R}^r \times \mathbb{C}^s = \mathbb{R}^n$.

Proposition 10.10 *Sei $M \subset K$ ein freier $\mathbb{Z}$-Untermodul vom Rang n und $x_1, \ldots, x_n$ eine Basis von M. Dann ist $\sigma(M)$ ein Gitter in $\mathbb{R}^n$ mit dem Volumen*

$$v(\sigma(M)) = 2^{-s} |\det(\sigma_i(x_j))|.$$

Proof: Für $x \in K$ ist

$$\sigma(x) = (\sigma_1(x), \ldots, \sigma_r(x), \mathrm{Re}(\sigma_{r+1}(x)), \mathrm{Im}(\sigma_{r+1}(x)), \ldots, \mathrm{Re}(\sigma_{r+s}(x),)\mathrm{Im}(\sigma_{r+s}(x))$$

Man bekommt eine $n \times n$-Matrix, wenn man für x die x_j einsetzt. Beachte $\mathrm{Re}(z) = (z + \overline{z})/2$ und $\mathrm{Im}(z) = (z - \overline{z})/2i$. Durch spezielle elementare Umformungen nach dem Muster

$$((z + \overline{z})/2 \ , \ (z - \overline{z})/2i) \mapsto (z, \ (z - \overline{z})/2i) \mapsto (z, \ i\overline{z}/2)$$

kommt man zur Matrix

$$(\sigma_1(x_j), \ldots, \sigma_r(x_j), \sigma_{r+1}(x_j), i\sigma_{r+s+1}(x_j)/2, \ldots, \sigma_{r+s}(x_j), i\sigma_n(x_j)/2)_{1 \le j \le n}$$

Der Betrag ihrer Determinante ist der oben angegebene.

Das Quadrat dieses Betrages ist bis aufs Vorzeichen gleich $\mathrm{disc}(x_1, \ldots, x_n) \neq 0$. Also erzeugt das n-tupel $(\sigma(x_1), \ldots, \sigma(x_n))$ ein Gitter im $\mathbb{R}^n$. □

Corollary 10.11 *Sei d die absolute Diskriminante von K (d.h. der Betrag der Diskriminante einer Ganzheitsbasis) und $I \neq (0)$ ein ganzes Ideal. Dann sind $\sigma(\mathbb{Z}_K)$ und $\sigma(I)$ Gitter im $\mathbb{R}^n$, und es gilt*

$$v(\sigma(\mathbb{Z}_K) = 2^{-s}\sqrt{d} \quad \textit{und} \quad v(\sigma(I)) = 2^{-s}\sqrt{d}N(I).$$

Proof: Die erste Aussage über $\mathbb{Z}_K$ und I ist klar, die zweite Aussage für $\mathbb{Z}_K$ auch. Die Letzte Aussage folgt, da $N(I) = [\mathbb{Z}_K : I]$ ist. Man sieht nämlich, dass man einen Fundamentalbereich für I aus $[\mathbb{Z}_K : I]$ Fundamentalbereichen von $\mathbb{Z}_K$ zusammensetzen kann. ($[\mathbb{Z}_K : I][\mathbb{Z}_K : I]$ bezeichnet den Untergruppenindex.) □

To every endomorphism α there is a unique **adjoint** α^*, defined by the property $\langle \alpha v, w\rangle = \langle v, \alpha^* w\rangle$ for all $v, w \in \mathbb{F}^n$. With respect to the canonical basis and the above described canoncal inner product, α^* as a matrix is the transposed conjugate of α. One has $(\beta\circ\alpha)^* = \alpha^*\circ\beta^*$.

One calls α hermitian, iff $\alpha = \alpha^*$. By the Spectral Theorem ([**?**] XV Theorem 6.7) a hermitian matrix α is similar to a diagonal matrix with real entries. More explicitely there is an automorphism σ of $\mathbb{F}^n$ as an inner product space (i.e. $\sigma^{-1} = \sigma^*$) such that

$$\sigma\alpha\sigma^* = \mathrm{diag}(\lambda_1, \ldots, \lambda_n) \quad \text{with} \quad \lambda_j \in \mathbb{R} \tag{5}$$

An hermitian α is called **positive**, resp. **semipositive**, if $\langle \alpha v, v\rangle > 0$, resp. ≥ 0 for all $v \in F^n - \{0\}$. Exactly in this case one has $\lambda_j > 0$, resp. $\lambda_j \geq 0$. resp. ≥ 0 for all j. So every positive hermitian endomorphism is invertible and its inverse is hermitian too.

Especially $\beta^*\beta$ is semipositive hermitian for every endomorphism β. So $I + \beta\beta^*$ is positive hermitian.

Every semipositive hermitian endomorphism α has a unique semipositive hermitian square root $\sqrt{\alpha}$, i.e. $(\sqrt{\alpha})^2 = \alpha$. Namely with the notation of () set

$$\sqrt{\alpha} = \sigma^*\mathrm{diag}(\sqrt{\lambda_1}, \ldots, \sqrt{\lambda}_n)\sigma \ .$$

11 Die Endlichkeit der Klassenzahl 2

Mit Hilfe der Geometrie der Zahlen beweisen wir die Endlichkeit der Klassenzahl zum zweite Mal und erhalten dabei bessere Schranken.

Theorem 11.1 *Sei K ein Zahlkörper. Dann gibt es ein $c > 0$, so dass für jedes ganze Ideal $I \neq (0)$ ein $x \in I$ existiert mit*

$$|N(x)| \leq cN(I) \tag{6}$$

Dieses c kann man genauer angeben als

$$c = (4^s\pi^{-s}n!n^{-n}\sqrt{d}$$

wobei n der Grad von K und s die Anzahl der komplexen Einbettungen von K und d der Betrag der Diskriminante einer Ganzheitsbasis ist.

Proof: Sei $\sigma : K \to \mathbb{R}^r \times \mathbb{C}^s$ die kanonische Einbettung. Für $t > 0$ sei B_t die Menge aller $(y_1, \ldots, y_r, z_1, \ldots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s$ mit

$$\sum_{i=1}^{r} |y_i| + 2 \sum_{j=1}^{s} |z_j| \leq t$$

Dann ist B_t kompakt, konvex und symmetrisch bzgl. 0 in $\mathbb{R}^n$. Das Volumen von B_t kann man berechnen:

$$\mu(B_t) = 2^r - s\pi^s t^n (n!)^{-1}$$

Wähle nun t so, dass $\mu(B_t) = 2^n (v(I)$. Das bedeutet

$$2^r \pi^s 2^{-s} t^n (n!)^{-1} = 2^{n-s} \sqrt{d} N(I) \quad \text{d.h.} \quad t^n = 2^{2s} \pi^{-s} n! \sqrt{d} N(I).$$

Nach Theorem 10.8 gibt es für dieses t ein $x \in I - (0)$ mit $\sigma(x) \in B_t$. Für den Betrag seiner Norm gilt

$$|N(x)| = \prod_{j=1}^{r} |\sigma_j(x)| \prod_{j=r+1}^{r+s} |\sigma_j(x)|^2.$$

Wir wenden die Ungleichung zwischen dem geometrischen und arithmetischen Mittel an:

$$|N(x)| \leq \left(\frac{1}{n} \sum_{j=1}^{r} |\sigma_j(x)| + \frac{2}{n} \sum_{j=r+1}^{r+s} |\sigma_j(x)| \right) \leq t^n n^{-n}.$$

Daraus folgt die Behauptung. □

11.2 Dies ist Lemma 7.5 mit dem Unterschied, dass hier die Schranke c, die dort λ genannt wurde, genauer angegeben wird. Unser c ist verhältnismäßig klein, da es den Faktor $N!/n^n$ enthält.

Wie im Abschnitt über „the finiteness of class number“ folgt aus obigem Theorem die Endlichkeit der Klassenzahl.

Wir wollen noch zwei weitere Schlüsse ziehen.

Corollary 11.3 *Jede Idealklasse von $\mathbb{Z}_K$ enthält ein ganzes Ideal I mit*

$$N(I) \leq c = 4^s \pi^{-s} n! n^{-n} \sqrt{d} \tag{7}$$

Proof: Sei J ein Ideal dieser Idealklasse, derart dass J^{-1} ganz ist. Wähle $x \in J^{-1}$, so dass die Ungleichung 5 für J^{-1} anstatt I gilt. Dann ist $I := xJ$ ganz in derselben Klasse wie J und erfüllt die gwünschte Ungeichung. □

Corollary 11.4 *Sei K ein Zahlkörper vom Grad $n > 1$ und der Diskriminante d. Dann gilt*

$$d \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}$$

Für alle Zahlkörper gibt es eine gemeinsame obere Schranke von $n/\log(d)$.

Proof: Da die Ungleichung 6 für mindestens ein ganzes Ideal I gilt und $N(I) \geq 1$ ist, folgt

$$\sqrt{d} \geq \left(\frac{\pi}{4}\right)^s \frac{n^n}{n!}$$

Durch elementare Überlegungen und Abschätzungen folgt hieraus die gewünschte Ungleichung.

Die letzte Behauptung folgt durch Logaritmieren. □ As unmittelbare Folgerung erhält man folgendes Theorem, dessen Bedeutung man erst später verstehen wird.

Theorem 11.5 (Hermite, Minkowski) *Ist $K \neq \mathbb{Q}$, so ist* $\mathrm{disc}(K) \neq \pm 1$.

Theorem 11.6 (Hermite) *Zu jeder ganzen Zahl n gibt es nur endlich viele Zahlkörper $K \subset \mathbb{C}$ mit* $\mathrm{disc}(K) = n$.

Proof: Wegen Theorem 11.5 ist der Grad eines solchen Körpers beschränkt. Deshalb darf man n, r, s als fest ansehen. Sei $\sigma : K \to \mathbb{R}^r \times \mathbb{C}^s$ die kanonische Einbettung. In $\mathbb{R}^r \times \mathbb{C}^s$ sei die Teilmenge B folgendermaßen definiert:

1. Ist $r > 0$, so sei B die Menge der $(y_1, \ldots, y_{r+s}$ mit $|y_1| \leq 2^{n+s}\pi^{-s}\sqrt{d}$ und $|y_j| \leq 1/2$ für alle $j \geq 2$.

2. Ist $r = 0$, so sei B definiert durch $|y_1 - \overline{y_1}| \leq 2^{n+s-1}\pi^{1-s}\sqrt{d}$, $|y_1 + \overline{y_1}| \leq 1/2$ und $|y_j| \leq 1/2$ für $j \geq 2$.

B ist kompakt, konvex und symetrish zu 0 in $\mathbb{R}^n$. Sein Volumen berechnet sich zu $2^{n-s}d$. Auf Grund des Satzes von Minkowski gibt es ein $x \in \mathbb{Z}_K - (0)$ mit $\sigma(x) \in B$.

12 Der Dirichletsche Einheitensatz

Sei K ein Zahlkörper. Wir wollen zeigen, dass die Gruppe der Einheiten von $\mathbb{Z}_K$ (manchmal auch die Einheiten von K genannt) endlich erzeugt ist, und den Rang dieser Gruppe genauer bestimmen.

Lemma 12.1 *Ein Element $x \in \mathbb{Z}_K$ ist genau dann eine Einheit (in $\mathbb{Z}_K$), wenn für seine Norm $N(x) = \pm 1$ gilt.*

Proof: Ist $x \in \mathbb{Z}_K$ eine Einheit, so gibt es ein $y \in \mathbb{Z}_K$ mit $xy = 1$. Also ist dann auch $N(x)N(y) = 1$. Da $N(x), N(y) \in \mathbb{Z}$, ist $N(x) = \pm 1$:

Sei umgekehrt $N(x) = \pm 1$, so erfüllt x eine Gleichung der Form $x^n + a_1 x^{n-1} + \cdots + a_{n-1}x \pm 1 = 0$ mit $a_j \in \mathbb{Z}$. D.h. $x(x^{n-1} + a_1 x^{n-2} + \cdots a_{n-1}) = \pm 1$, womit x eine Einheit in $\mathbb{Z}_K$ ist. □

Theorem 12.2 (Dirichlet) *$\mathbb{Z}_K^\times$ ist eine endlich erzeugte (abelsche) Gruppe. Der Torsionsbestandteil ist zyklisch und besteht aus den in K enthaltenen Einheitswurzeln. Der torsionsfreie Anteil ist (frei) vom Rang $r + s - 1$*

Proof: Es ist leicht zu sehen, dass die Elemente endlicher Ordnung von $\mathbb{Z}_K^\times$ genau die Einheitswurzeln in K sind. (Man kann hier schon sehen, dass diese eine endlicne zyklische Gruppe bilden. Denn wenn eine m-te Einheitswurzel in K liegt, muss $\varphi(m) \leq [K : \mathbb{Q}]$ sein. Und es gibt zu jeder endlichen Schranke s nur endlich viele m mit $\varphi(m) \leq s$. Und eine endliche Gruppe von Einheitswurzeln ist immer zyklisch, nicht wahr?)

Jetzt zeigen wir, dass $\mathbb{Z}_K^\times$ endlich erzeugt ist. Dazu betrachten wir die kanonische Eibettung

$$\sigma = (\sigma_1, \ldots, \sigma_{r+s}) : K \to \mathbb{R}^r \times \mathbb{C}^s.$$

Hieraus bekommt man eine Abbildung

$$L : K^\times \to \mathbb{R}^{r+s} \ , \ \ + x \mapsto (\log|\sigma_1(x)|, \ldots, \log|\sigma_{r+s}(x)|).$$

Diese ist ein Gruppenhomomorfismus: $L(ab) = L(a) + L(b)$.

Behauptung 1. Ist $B \subset \mathbb{R}^{r+s}$ beschränkt, so ist die Menge B' aller $x \in \mathbb{Z}_K^\times$ mit $L(x) \in B$ endlich.

Beweis: Da B beschränkt ist, gibt es eine reelle Zahl $c > 1$ mit $c^{-1} < |\sigma_j(x)| < c$ für $j = 1, \ldots, r + 2s$. (Hier ist $\sigma_{r+s+j}(x) = \overline{\sigma_{r+j}(x)}$.) Die Koeffizienten der Minimalpolynome der $x \in B'$ sind dann ebenfalls beschränkt.

Denn sie sind – bis auf den Leitkoeffizienten, der 1 ist – elementarsymmetrische Funktionen in höchstens $[K : \mathbb{Q}]$ Unbestimmten. Da sie in $\mathbb{Z}$ liegen, gibt es nur endlich viele solche Minimalpolynome, also auch nur endlich viele $x \in B'$. –

Es folgt zunächst, dass der Kern von L endlich ist. Da das Bild von L in der additiven Gruppe von $\mathbb{R}^{r+s}$ liegt, ist es torsionsfrei. Also ist der Torsionsbestandteil von $\mathbb{Z}_K^\times$ endlich.

Der torsionsfreie Bestandteil von $\mathbb{Z}_K^\times$ ist isomorf einer diskreten Untergruppe von $\mathbb{R}r + s$, also frei vom Rang $\leq r+s$. Der Rang ist sogar $\leq r+s-1$. Denn für die Norm jeder Einheit x gilt

$$1 = |N(x)| = |\prod_{j=1}^{r+2s} \sigma_j(x)| = \prod_{j=1}^{r} |\sigma_j(x)| \prod_{j=1}^{s} |\sigma_{r+j}(x)\overline{\sigma_{r+j}(x)} \tag{8}$$

$$= \prod_{j=1}^{r} |\sigma_j| \prod_{j=1}^{s} |\sigma_{r+j|^2} \tag{9}$$

Also ist $L(\mathbb{Z}_K^\times)$ eine diskrete Untergruppe der durch die Gleichung

$$y_1 + \cdots + y_r + 2y_{r+1} + \cdots + 2y_{r+s} = 0 \tag{10}$$

definierten Hyperebene W von $\mathbb{R}^{r+s}$, ist also frei vom Rang $\leq r+s-1$

Mit Hilfe der Minkowskitheorie wollen wir jetzt Einheiten $u_1, \ldots, u_{r+s}$ in $\mathbb{Z}_k$ finden, derart dass der Rang des $(r+s)$-tupels $L(u_1), \ldots, L(u_{r+s})$ gleich $r+s-1$ ist.

Zunächst finden wir Elemente aus $\mathbb{Z}_K - (0)$ mit gewissen Eigenschaften.

Behauptung 2. Zu $k \in \{1, \ldots, r+s\}$ und $\alpha \in \mathbb{Z}_K - (0)$ gibt es ein $\beta \in \mathbb{Z}_K - (0)$ mit

$$|N(\beta)| \leq 2^s \pi^{-s} \sqrt{d}$$

für welches darüberhinaus gilt:
Ist $L(\alpha) = (a_1, \ldots, a_{r+s})$ und $L(\beta) = (b_1, \ldots, b_{r+s})$ so ist $b_j < a_j$ für $j \neq k$.

Beweis: Betrachte in $\mathbb{R}^n$ die Teilmenge B, die durch $|x_1| \leq c_1, \ldots, |x_r| \leq c_r$ und $x_{r+1}^2 + x_{r+2}^2 \leq c_{r+1}, \ldots, x_{n-1}^2 + x_n^2 \leq c_{r+s}$ definiert ist. Dabei seien die c_j so definiert, dass

$$0 < c_j < \exp(a_j) \; für \; j \neq k \;\text{ und }\; c_{1r+s} = 2^s \pi^{-s} \sqrt{d} \;\text{ ist.}$$

Dann ist B symmetrisch zur 0, konve und kompakt, ferner $\mu(B) = 2^r \pi^s c_1 \cdots c_{r+s} = 2^n (\sigma(\mathbb{Z}_K)$ Nach Minkowski gibt es jetzt ein $\beta \in \mathbb{Z}_K - (0)$ mit $\sigma(\beta) \in B$. Dies erfüllt die Behauptung. –

BEHAUPTUNG 3. Zu jedem $k \in \{1, \ldots, r+s\}$ gibt es eine Einheit $u_k \in \mathbb{Z}_K^\times$, derart dass für $L(u) = (y_1, \ldots, y_{r+s})$ gilt:

$$y_k > 0,\ y_j < 0 \text{ falls } j \neq k.$$

BEWEIS: Wir starten mit einem beliebigen $\alpha_1 \in \mathbb{Z}_K - (0)$. Mit Hilfe von Behauptung 1 finden wir zu einem bereits konstruierten α_r ein α_{r+1}, so dass α_r, α_{r+1} die Rolle von α, β in Beh. 1 spielen. So erhalten wir eine Folge $\alpha_1, \alpha_2, \ldots$. Da die α_r die Ungleichung $N(\alpha_r \leq 2^s \pi^{-s} \sqrt{d}$ erfüllen, ist die Menge der Zahlen $\#(\mathbb{Z}_K/(\alpha_r)$ beschränkt. Deshalb gibt es unter den Idealen (α_r) nur endlich viele verschiedene. Deshalb gibt es r, s mit $r < s$ und $(\alpha_r) = (\alpha_s)$. Dann erfüllt $u_k := \alpha_r/\alpha_s$ die Behauptung. –

Der Satz folgt nun offenbar aus folgendem Lemma über reelle Matritzen:

LEMMA: Sei $\alpha = (a_{ij})$ eine reelle $m \times m$-Matrix mit folgenden Eigenschaften:

$$a_{ii} > 0\ ,\quad a_{ij} < 0 \text{ für } i \neq j\ ,\quad \sum_{j=1}^{m} a_{ij} = 0\ .$$

Dann gilt $\mathrm{rg}(\alpha) = m - 1$.

BEWEIS: Seien $v_1, \ldots, v_m$ die Spalten von α. Nach Voraussetzung ist $\sum_{j=1}^m v_j = 0$, also $(\alpha) \leq m - 1$. Waere nun $(v_1, \ldots, v_{m-1})$ linear abhängig, so gäbe es $t_1, \ldots, t_{m-1}$, nicht alle 0, mit $\sum_{j=1}^{m-1} v_j = 0$. Man kann sogar annehmen, dass es dabei ein k mit $t_k = 1$ und $t_j \leq 1$ für $j \neq k$ gibt. (Zunächst kann man annehmen, dass mindestens ein t_j positiv ist, indem man notfalls mit -1 multipliziert. Dann dividiere man durch das größte t_k.) Jetzt betrachte man, was obige Darstellung des 0-Vektos für die k-te Zeile bedeutet:

$$0 = \sum_{j=1}^{m-1} t_j a_{kj} \geq \sum_{j=1}^{m-1} a_{kj} > \sum_{j=1}^{m} a_{kj} = 0$$

Die erste Ungleichung gilt wegen $t_k a_{kk} = a_{kk}$, und da aus $t_j \leq 1$ und $a_{kj} < 0$ für $j \neq k$ folgt $t_j a_{kj} \geq a_{kj}$. Die zweite Ungleichung gilt, da $k < m$ und deshalb $a_{km} < 0$ ist.

Widerspruch. □