Protokoll zur Vorlesung Algebraische Zahlentheorie WS 25/26

W. Bley

31. Oktober 2025

1 Ganzheitsringe und Diskriminanten

1.1 Motivation und grundlegende Definitionen

Für eine ungerade Primzahl p gilt:
a) Es gibt genau dann Zahlen $x, y \in \mathbb{Z}$ mit $x^2 + y^2 = p$, wenn $p \equiv 1 \pmod 4$.
b) Es gibt genau dann Zahlen $x, y \in \mathbb{Z}$ mit $x^2 - 6y^2 = p$, wenn $p \equiv \pm 1 \pmod 8$.
Die Diskussion der Beweise dieser beiden Resultate hat uns auf folgende Definitionen geführt.

Definition 1.1.1 Eine endliche Körpererweiterung von $\mathbb{Q}$ heißt algebraischer Zahlkörper oder kurz Zahlkörper.

Definition 1.1.2 Sei K ein Zahlkörper. Dann heißt

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

Ring der ganzen Zahlen von K.

Example 1.1.3 *Sei $d \in \mathbb{Z}\setminus\{0,1\}$ quadratfrei. Sei $K = \mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper. Dann gilt:*

$$\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\omega \text{ mit } \omega = \begin{cases} \sqrt{d}, & \text{falls } d \equiv 2,3 \pmod 4, \\ \frac{1+\sqrt{d}}{2}, & \text{falls } d \equiv 1 \pmod 4. \end{cases}$$

Man zeigt relativ leicht:
a) $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.
b) $\mathbb{Z}[\sqrt{2}]^\times = \{\pm(1+\sqrt{2})^k \mid k \in \mathbb{Z}\}$.
Im Allgemeinen gibt der Dirichletsche Einheitensatz Auskunft über die Struktur der Einheitengruppe $\mathcal{O}_K^\times$.

Satz 1.1.4 *(Dirichletscher Einheitensatz) Sei K ein Zahlkörper. Dann ist $\mathcal{O}_K^\times$ eine endlich erzeugte abelsche Gruppe. Insbesondere also $\mathcal{O}_K^\times \simeq \left(\mathcal{O}_K^\times\right)_{tors} \times \mathbb{Z}^r$.*
Zusatz: r nennt man den Einheitenrang und es gilt: $r = s + t - 1$, wobei

$$\begin{aligned} s &= \text{Anzahl der reellen Einbettungen von } K \text{ in } \mathbb{C}, \\ t &= \text{halbe Anzahl der komplexen Einbettungen von } K \text{ in } \mathbb{C}. \end{aligned}$$

Bei der Diskussion der Geleichung $p = x^2 + 6y^2$ sind wir auf das Phänomen gestoßen, dass Ganzheitsringe im allgemeinen keine Hauptidealringe sind. Wir werden im Rahmen der Vorlesung die sogenannte Idealklassengruppe

$$\mathrm{cl}_K := \text{Gruppe der gebrochenen Ideale/Untergruppe der Hauptideale}$$

studieren und beweisen, dass dies eine endliche Gruppe ist. Es gilt:

$$\mathrm{cl}_K = 1 \iff \mathcal{O}_K \text{ ist ein Hauptidealring.}$$

Ein weiteres Thema des ersten Teils der Vorlesung werden Zerlegungsgesetze sein. Ganzheitsringe in Zahlkörpern sind Dedekindringe, und in Dedekindringen gilt der Satz von der eindeutigen Primidealzerlegung. Falls nun L/K eine Erweiterung von Zahlkörpern ist, so werden wir für ein Primideal $\mathfrak{p}$ von $\mathcal{O}_K$ die Primidealzerlegung von $\mathfrak{p}\mathcal{O}_L$ studieren.
Hier ein erstes Beispiel:
Sei $K = \mathbb{Q}(\sqrt{d})$ mit d wie oben ein quadratischer Zahlkörper und $p \neq 2$ eine Primzahl. Dann gilt:

$$p\mathcal{O}_K = \begin{cases} \mathfrak{p}\bar{\mathfrak{p}}, \mathfrak{p} \neq \bar{\mathfrak{p}}, & \text{falls } \left(\frac{d}{p}\right) = 1, p \nmid d, \\ \mathfrak{p}, & \text{falls } \left(\frac{d}{p}\right) = -1, p \nmid d, \\ \mathfrak{p}^2, & \text{falls } p \mid d. \end{cases}$$

Hierbei bezeichnet $\left(\frac{a}{p}\right)$ das Legendresymbol.

Satz 1.1.5 *(Quadratisches Reziprozitätsgesetz) a) Seien $p \neq q$ zwei ungerade Primzahlen. Dann gilt:*

$$\left(\frac{p}{q}\right) = \varepsilon \left(\frac{q}{p}\right)$$

mit

$$\varepsilon = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} +1, \text{ falls } p \equiv 1 \pmod 4 \text{ oder } q \equiv 1 \pmod 4, \\ -1, \text{ falls } p \equiv 3 \pmod 4 \text{ und } q \equiv 3 \pmod 4, \end{cases}$$

(1.Ergänzungssatz und 2.Ergänzungssatz) Sei $p \neq 2$ eine Primzahl. Dann gilt:

$$b) \qquad \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} +1, & \text{falls } p \equiv 1 \pmod 4, \\ -1, & \text{falls } p \equiv 3 \pmod 4. \end{cases}$$

$$c) \qquad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} +1, & \text{falls } p \equiv \pm 1 \pmod 8, \\ -1, & \text{falls } p \equiv \pm 3 \pmod 8. \end{cases}$$

Mit den Methoden, die wir im Laufe der Vorlesung entwickeln, werden wir in der Lage sein, folgendes Theorem zu beweisen.

Satz 1.1.6 *Sei $p \neq 2$ eine Primzahl und $d \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei. Dann gibt es genau dann $x, y \in \mathbb{Z}$ mit $p = x^2 - dy^2$, wenn $\left(\frac{d}{p}\right) = +1$ und $\mathfrak{p}$ ein Hauptideal ist. Für $d > 0$ gibt es in diesem Fall unendlich viele Lösungen, für $d < 0$ nur endlich viele.*

1.2 Ganze Zahlen

Konvention: Alle unsere Ringe sind, wenn nicht ausdrücklich anders gesagt, stets kommutativ und haben eine 1.

Definition 1.2.1 Sei $A \subseteq B$ eine Ringerweiterung. Ein Element $b \in B$ heißt ganz über A, wenn b Nullstelle eines normierten Polynoms $f \in A[X]$ ist. Der Ring B heißt ganz über A, falls alle $b \in B$ ganz über A sind.

Satz 1.2.2 *Sei $A \subseteq B$ eine Ringerweiterung und seien $b_1, \ldots, b_n \in B$. Dann gilt:*

$$b_1, \ldots, b_n \text{ ganz über } A \iff A[b_1, \ldots, b_n] \text{ ist endlich erzeugter } A\text{-Modul.}$$

Insbesondere sind also Summen und Produkte von ganzen Elementen wieder ganz.

Folgerung 1.2.3 *Sei $K/\mathbb{Q}$ ein Zahlkörper. Dann ist $\mathcal{O}_K$ ein Ring.*

Ganzheit ist gewissermaßen transitiv:

Satz 1.2.4 *Seien $A \subseteq B \subseteq C$ Ringerweiterungen. Sei B ganz über A und $c \in C$ ganz über B. Dann ist c ganz über A.*

Definition 1.2.5 Sei $A \subseteq B$ eine Ringerweiterung.
a) Der Ring

$$\mathcal{O}_{A,B} := \{b \in B \mid b \text{ ist ganz über } A\}$$

heißt ganzer Abschluss von A in B.
b) Falls $\mathcal{O}_{A,B} = A$ gilt, so heißt A ganz abgeschlossen in B.

Als Beispiel haben wir eingesehen, dass faktorielle Ringe ganz abgeschlossen in ihrem Quotientenkörper sind.
Wir betrachten nun die folgende Situation: A sei ein nullteilerfreier Ring, der ganz abgeschlossen in seinem Quotientenkörper K ist. L/K sei eine endliche separable Körpererweiterung und B der ganze Abschluss von A in L, also $B = \mathcal{O}_{A,L}$.

Lemma 1.2.6 *In dieser Situation gilt: $L = \mathrm{Quot}(B)$. Genauer gilt sogar, dass jedes $\beta \in L$ in der Form*

$$\beta = \frac{b}{a} \text{ mit } b \in B \text{ und } a \in A$$

geschrieben werden kann.

Lemma 1.2.7 *In obiger Situation gilt für $\beta \in L$:*

$$\beta \in B \iff \mathrm{Mipo}_{K,\beta} \in A[X].$$

Remark 1.2.8 Für den Beweis von Lemma 1.2.6 braucht man die Voraussetzung "A ganz abgeschlossen" noch nicht.

Sei nun L/K eine endliche Körpererweiterung. Sei $\alpha \in L$ und

$$T_\alpha \colon L \longrightarrow L, \quad \beta \mapsto \alpha\beta$$

die lineare Abbildung Multiplikation mit α.

Definition 1.2.9 a) $\mathrm{Tr}_{L/K}(\alpha) := \mathrm{Spur}(T_\alpha)$ heißt (körpertheoretische) Spur von α.
b) $\mathrm{N}_{L/K}(\alpha) := \det(T_\alpha)$ heißt Norm von α.

Aus der linearen Algebra ist der folgende Zusammenhang zwischen charakteristischem Polynom und Norm und Spur bekannt.

Lemma 1.2.10 *Sei L/K eine endliche Körpererweiterung und $\alpha \in L$.*
a) Sei $\chi_\alpha(t) = \det(tE - T_\alpha) \in K[t]$ das charakteristische Polynom von T_α. Sei explizit

$$\chi_\alpha(t) = t^n - a_1 t^{n-1} + \ldots (-1)^n a_n.$$

Dann gilt: $\mathrm{Tr}_{L/K}(\alpha) = a_1, \mathrm{N}_{L/K}(\alpha) = a_n$.
b) $\mathrm{Tr}_{L/K}$ *ist K-linear.*
c) $\mathrm{N_{L/K}}$ *ist multiplikativ.*

Satz 1.2.11 *Sei L/K eine endliche separable Körpererweiterung. Sei $\bar{K}$ ein algebraischer Abschluss von K und $G = G(L/K, \bar{K}/K)$ die Menge der K-Automorphismen von L. Dann gilt:*
a) $\chi_\alpha(t) = \prod_{\sigma \in G}(t - \sigma(\alpha))$.
b) $\mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha)$.
c) $\mathrm{N}_{L/K}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha)$.

Folgerung 1.2.12 *Sei $K \subseteq L \subseteq M$ ein Turm von endlichen separablen Körpererweiterungen. Dann gilt:*
a) $\mathrm{Tr}_{M/K}(\alpha) = \mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(\alpha))$.
b) $\mathrm{N}_{M/K}(\alpha) = \mathrm{N}_{L/K}(\mathrm{N}_{M/L}(\alpha))$.

Definition 1.2.13 Sei L/K eine endliche separable Körpererweiterung vom Grad n. Seien $\alpha_1, \ldots, \alpha_n$ Elemente aus L. Ferner sei $G(L/K, \bar{K}/K) = \{\sigma_1, \ldots, \sigma_n)$. Dann heißt

$$d(\alpha_1, \ldots, \alpha_n) := \Big(\det\left(\sigma_i(\alpha_j)\right)_{1 \le i,j \le n}\Big)^2$$

Diskriminante von $\alpha_1, \ldots, \alpha_n$.

Lemma 1.2.14 *Es gilt:*
a)

$$d(\alpha_1, \ldots, \alpha_n) = \det\left(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)\right)_{1 \le i,j \le n}.$$

b) Für $\theta \in L$ gilt:

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

wobei $\theta_i := \sigma_i(\theta)$.

Satz 1.2.15 *Sei L/K eine endliche separable Körpererweiterung und seien $\alpha_1, \ldots, \alpha_n \in L$. Dann gilt:*
a) $\alpha_1, \ldots, \alpha_n$ ist K-Basis von $L \iff d(\alpha_1, \ldots, \alpha_n) \neq 0$.
b) Die Abbildung $L \times L \longrightarrow K, (x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$, definiert eine nicht-ausgeartete Bilinearform auf L.

Wir betrachten nun wieder die Situation wie oben: A sei ein nullteilerfreier Ring, der ganz abgeschlossen in seinem Quotientenkörper K ist. L/K sei eine endliche separable Körpererweiterung und B der ganze Abschluss von A in L, also $B = \mathcal{O}_{A,L}$.

Lemma 1.2.16 *In dieser Situation gilt:*
a) Für alle $b \in B$ gilt: $\mathrm{Tr}_{L/K}(b), \mathrm{N}_{L/K}(b) \in A$.
b) Für $b \in B$ gilt:

$$b \in B^\times \iff \mathrm{N}_{L/K}(b) \in A^\times.$$

Lemma 1.2.17 *In obiger Situation gilt gilt für jede in B gelegene K-Basis $\alpha_1, \ldots, \alpha_n$ von L mit $d := d(\alpha_1, \ldots, \alpha_n)$*

$$dB \subseteq A\alpha_1 \oplus \ldots \oplus A\alpha_n.$$

Aus der Theorie der Moduln über Hauptidealringen erhalten wir das nächste Resultat.

Satz 1.2.18 *In obiger Situation sei A ein Hauptidealring. Dann ist jeder endlich-erzeugte B-Untermodul $M \neq 0$ von L ein freier A-Modul vom Rang $n = [L : K]$. Insbesondere gibt es $\alpha_1, \ldots, \alpha_n \in B$, so dass*

$$B = A\alpha_1 \oplus \ldots \oplus A\alpha_n.$$

Definition 1.2.19 Eine A-Basis von B wie im Satz nennt man Ganzheitsbasis von L/K (bezüglich des Grundrings A). Speziell sprechen wir von einer Ganzheitsbasis des Zahlkörpers L, falls $A = \mathbb{Z}$ und $B = \mathcal{O}_L$.

Definition 1.2.20 Sei $L/\mathbb{Q}$ ein Zahlkörper und $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_L$ eine Ganzheitsbasis. Dann nennt man

$$d_L := d(\alpha_1, \ldots, \alpha_n)$$

die Diskriminante von L/K.

Man beachte, dass diese Bildung unabhängig von der Wahl der Ganzheitsbasis ist.

Definition 1.2.21 Sei $L/\mathbb{Q}$ ein Zahlkörper und $M \neq 0$ ein endlich erzeugter $\mathcal{O}_L$-Teilmodul von L. Sei $\alpha_1, \ldots, \alpha_n$ eine $\mathbb{Z}$-Basis von M. Dann nennt man

$$d(M) = d_{L/K}(M) := d(\alpha_1, \ldots, \alpha_n)$$

die Diskriminante von M.

Es gilt dann:

Satz 1.2.22 *Seien $L/\mathbb{Q}$ ein Zahlkörper und $0 \neq M \subseteq M'$ zwei endlich erzeugte $\mathcal{O}_L$-Teilmoduln von L. Dann ist $[M' : M] < \infty$ und es gilt*

$$d(M) = [M' : M]^2 d(M').$$

Folgerung 1.2.23 *Sei $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_L$ eine $\mathbb{Q}$-Basis von L und $d(\alpha_1, \ldots, \alpha_n)$ sei quadratfrei. Dann ist $\alpha_1, \ldots, \alpha_n$ eine Ganzheitsbasis.*

1.3 Ideale

Wir erinnern zunächst an die Definition und grundlegende Eigenschaften noetherscher Ringe und Moduln. Im Folgenden ist R stets ein kommutativer Ring mit Eins.

Definition 1.3.1 Ein R-Modul M heißt noethersch, falls alle seine R-Teilmoduln endlich erzeugt sind.

Insbesondere können wir R als R-Modul betrachten. R ist genau dann noethersch, wenn jedes Ideal in R endlich erzeugt ist.
Für einen noetherschen Ring R und einen R-Modul M gilt:

$$M \text{ ist noethersch } \iff M \text{ ist endlich erzeugt.}$$

Satz 1.3.2 *Sei M ein R-Modul. Dann sind folgende Aussagen äquivalent:*
a) M ist noethersch.
b) Jede aufsteigende Kette

$$M_1 \subseteq M_2 \subseteq \ldots$$

von R-Teilmoduln von M wird stationär.
c) Jede nicht-leere Familie von R-Teilmoduln von M enthält maximale Elemente (bez. der Inklusion).

Wir kommen nun zu einem ersten zentralen Resultat der Vorlesung.

Satz 1.3.3 *Sei K ein Zahlkörper. Dann ist $\mathcal{O}_K$ noethersch, ganz abgeschlossen und jedes Primideal $\mathfrak{p} \neq 0$ ist ein maximales Ideal.*

Definition 1.3.4 Ein nullteilerfreier Ring R heißt Dedekindring, falls folgende Eigenschaften erfüllt sind:
a) R ist noethersch.
b) R ist ganz abgeschlossen.
c) Jedes Primideal $\mathfrak{p} \neq 0$ ist ein maximales Ideal.

Nach dieser Definiton ist auch jeder Körper ein Dedekindring. Wir interessieren uns aber vor allem für Dedekindringe, die keine Körper sind. Satz 1.3.3 besagt also, dass der Ring $\mathcal{O}_L$ der ganzen Zahlen in einem Zahlkörper L stets ein Dedekindring ist.

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

Satz 1.3.5 *Sei $\mathfrak{a}$ ein nicht-triviales Ideal, d.h. $\mathfrak{a} \neq (0), \mathcal{O}$. Dann gibt es eine bis auf Reihenfolge eindeutige Darstellung*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r \tag{1}$$

von $\mathfrak{a}$ als Produkt von Primidealen $\mathfrak{p}_i$. Schreibt man (1) in der Form

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}$$

mit paarweise verschiedenen Primidealen $\mathfrak{p}_1, \ldots \mathfrak{p}_s$, $s \leq r$, $e_i \in \mathbb{Z}_{>0}$, so gilt auch

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cap \ldots \cap \mathfrak{p}_s^{e_s}.$$

Mit der Notation aus dem Satz erhalten wir aus dem Chinesischen Restsatz

$$\mathcal{O}/\mathfrak{a} \simeq \mathcal{O}/\mathfrak{p}_1^{e_1} \times \ldots \mathcal{O}/\mathfrak{p}_s^{e_s}.$$

Wie üblich in der Ringtheorie werden wir folgende Konventionen, Sprech- und Schreibweisen übernehmen. Seien dazu $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}$ Ideale.

a) $\mathfrak{a} \mid \mathfrak{b} \iff \mathfrak{b} \subseteq \mathfrak{a}$.

b) $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$ nennen wir den ggT von $\mathfrak{a}$ und $\mathfrak{b}$. Fall $\mathfrak{a} + \mathfrak{b} = \mathcal{O}$ gilt, so sagen wir, dass $\mathfrak{a}$ und $\mathfrak{b}$ teilerfremd sind.

c) $\mathfrak{a} \cap \mathfrak{b}$ nennen wir auch das kgV von $\mathfrak{a}$ und $\mathfrak{b}$.

Lemma 1.3.6 *Sei $\mathfrak{a}$ ein nicht-triviales Ideal von $\mathcal{O}$ und $\mathfrak{p} \neq 0$ ein Primideal. Dann gilt:*

$$\mathfrak{a} = \mathfrak{p}^n \mathfrak{b} \text{ mit } n \in \mathbb{Z}_{\geq 0} \text{ and } (\mathfrak{b}, \mathfrak{p}) = \mathcal{O} \iff \mathfrak{a} \subseteq \mathfrak{p}^n \text{ und } \mathfrak{a} \nsubseteq \mathfrak{p}^{n+1}.$$

Im Weiteren wollen wir den Idealbegriff erweitern, so dass die sogenannten gebrochenen Ideale eine Gruppe bezüglich der Modulmultiplikation bilden.

Definition 1.3.7 Ein gebrochenes Ideal in K ist ein endlich erzeugter $\mathcal{O}$-Teilmodul $\mathfrak{a} \neq 0$ von K.

Lemma 1.3.8 *Sei $0 \neq \mathfrak{a} \subseteq K$ ein $\mathcal{O}$-Teilmodul. Dann gilt:*

$$\mathfrak{a} \text{ ist ein gebrochenes Ideal } \iff \exists c \in \mathcal{O}, c \neq 0 \text{ mit } c\mathfrak{a} \lhd \mathcal{O}.$$

Satz 1.3.9 *Die Gruppe der gebrochenen Ideale bildet eine Gruppe $J_{\mathcal{O}}$ bez. der Multiplikation von Idealen. Das Einselement ist gegeben durch $\mathcal{O}$ und für ein gebrochenes Ideal $\mathfrak{a}$ gilt*

$$\mathfrak{a}^{-1} = (\mathcal{O} : \mathfrak{a})$$

mit

$$(\mathcal{O} : \mathfrak{a}) := \{x \in K \mid x\mathfrak{a} \subseteq \mathcal{O}\}.$$

Folgerung 1.3.10 *Jedes gebrochene Ideal* $\mathfrak{a}$ *von* K *besitzt eine eindeutige Produktdarstellung*

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_\mathfrak{p}}, \quad \nu_\mathfrak{p} \in \mathbb{Z}, \nu_\mathfrak{p} = 0 \text{ für fast alle } \mathfrak{p}.$$

Hierbei durchläuft $\mathfrak{p}$ *alle Primideale ungleich* 0 *von* $\mathcal{O}$.

Folgerung 1.3.11 *Jedes gebrochene Ideal* $\mathfrak{a}$ *von* K *kann man eindeutig in der Form*

$$\mathfrak{a} = \mathfrak{b}/\mathfrak{c}$$

mit ganzen, zueinander teilerfremden Ideal $\mathfrak{b}, \mathfrak{c}$ *schreiben.*

Definition 1.3.12 a) $P_\mathcal{O} := \{\alpha\mathcal{O} \mid \alpha \in K^\times\}$ heißt Gruppe der (gebrochenen) Hauptideale.
b) $\mathrm{cl}_\mathcal{O} := J_\mathcal{O}/P_\mathcal{O}$ heißt Idealklassengruppe oder kurz Klassengruppe von $\mathcal{O}$.
c) Für $\mathfrak{a} \in J_\mathcal{O}$ bezeichne $[\mathfrak{a}] := \mathfrak{a}P_\mathcal{O}$ die Klasse von $\mathfrak{a}$.

Ein nächstes Ziel der Vorlesung wird sein, die Endlichkeit von $\mathrm{cl}_K := \mathrm{cl}_{\mathcal{O}_K}$ zu beweisen, falls K ein Zahlkörper ist.

Satz 1.3.13 *Sei* $\mathcal{O}$ *ein Dedekindring mit nur endlich vielen Primidealen. Dann ist* $\mathcal{O}$ *ein Hauptidealring.*

Satz 1.3.14 *Sei* $0 \neq \mathfrak{m} \subseteq \mathcal{O}$ *ein ganzes Ideal. Dann gibt es in jeder Idealklasse* $c \in \mathrm{cl}_\mathcal{O}$ *ganze, zu* $\mathfrak{m}$ *teilerfremde Ideale. Mit anderen Worten: es gibt ganze Ideal* $\mathfrak{a}$ *mit* $[\mathfrak{a}] = c$ *und* $(\mathfrak{a}, \mathfrak{m}) = \mathcal{O}$.