Kap. 3

§ 5 Ideale in Dedekindringen

Im Ring der ganzen Zahlen $\mathcal{O}_K$ einer algebraischen Zahlkörpers K lässt sich zwar jede Nichteinheit $\alpha \neq 0$ in ein Produkt irreduzibler Elemente zerlegen. Jedoch ist diese Zerlegung – im Gegensatz zur Primzerlegung in $\mathbb{Z}$ – nicht eindeutig.

Standardbeispiel: Sei $K = \mathbb{Q}(\sqrt{5})$, dann ist $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$. Die Zahl 21 lässt sich hier auf zwei verschiedene Arten zerlegen,

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

Alle Faktoren, 3, 7, $1+2\sqrt{5}$, $1-2\sqrt{5}$ sind jedoch irreduzibel und paarweise nicht-assoziiert.

Wäre z.B. $3 = \alpha\beta$ in $\mathcal{O}_K$, $\alpha, \beta \in \mathcal{O}_K$, nicht-Einheiten so wäre $9 = N_{K/\mathbb{Q}}(\alpha)\, N_{K/\mathbb{Q}}(\beta)$.

Also $N_{K/\mathbb{Q}}(\alpha) = \pm 3$. Aber die Gln.

$$N_{K/\mathbb{Q}}(a + b\sqrt{-5}) = a^2 + 5b^2 = \pm 3$$

hat keine Lsg in ganzen Zahlen $a, b \in \mathbb{Z}$.

Da $\frac{1 \pm 2\sqrt{-5}}{3} \notin \mathcal{O}_K$ ist 3 auch nicht zu $1+2\sqrt{-5}$ oder $1-2\sqrt{-5}$ assoziiert.

Analog argumentiert man für 7 und $1 \pm 2\sqrt{5}$.

Das Fehlen einer eindeutigen Primfaktorzerlegung veranlasste Kummer, sog. "ideale Zahlen" zu betrachten, eine Idee, die von Dedekind zur Theorie der Ideale in $\mathcal{O}_K$ ausgebaut wurde.

Erinnerung: Ein Ring A heißt noethersch, wenn eine der folgenden äquivalenten Bedingungen erfüllt ist:

- Jede aufsteigende Kette von Idealen in A stagniert, d.h. zu
$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \mathfrak{a}_3 \subset \dots$$
gibt es ein n s.d. $\mathfrak{a}_{n+i} = \mathfrak{a}_n$ für alle i.
- Jedes Ideal in A ist endl. erzeugt

Satz 1 Sei K ein Zahlkörper und $\mathcal{O}_K$ der Ring der ganzen algebraischen Zahlen in K.
Dann gilt: $\mathcal{O}_K$ ist noethersch, q.a. und jedes Primideal $\mathfrak{p} \neq 0$ in $\mathcal{O}_K$ ist ein maximales Ideal.

Bew: Der Ring $\mathcal{O}_K$ ist noethersch, weil jedes Ideal endl. erzeugter $\mathbb{Z}$-Modul, (s. §3, Satz 7 mit $k=\mathbb{Q}$) also auch endl. erzeugter $\mathcal{O}_K$-Modul ist.

Als ganzer Abschluss von $\mathbb{Z}$ in K ist $\mathcal{O}_K$ insbesondere ganz abgeschl.

Sei nun $\mathfrak{p} \neq 0$ ein Primideal in $\mathcal{O}_K$.
Dann ist $\mathfrak{p} \cap \mathbb{Z}$ ein Primideal $(p)(\neq 0)$ in $\mathbb{Z}$.
Ist $y \in \mathfrak{p}$, $y \neq 0$ und
$$y^n + a_{n-1}y^{n-1} + \dots + a_0 = 0 \qquad (a_0 = N_{K/\mathbb{Q}}(y))$$
eine Gln für y mit $a_i \in \mathbb{Z}$, $a_0 \neq 0$, so hat man $a_0 \in \mathfrak{p} \cap \mathbb{Z}$.
Also $(p) = \mathfrak{p} \cap \mathbb{Z} \neq (0)$.

(anderes Argument:

Der Integritätsbereich $\mathcal{O}_K/\mathfrak{p}$ geht aus dem Körper $\kappa = \mathbb{Z}/p\mathbb{Z}$ durch Adjunktion algebraischer Elemente hervor und ist somit ein Körper (beachte: $\kappa[\alpha] = \kappa(\alpha)$, wenn α algebraisch).)

Der Integritätsbereich $\mathcal{O}_K/(p)$ ist endlich (oder endl. erzeugt über $\mathbb{Z}/p\mathbb{Z}$)

$\Rightarrow$ $\mathcal{O}_K/\mathfrak{p}$ endl. (oder $\mathfrak{p} \supset (p)$)

somit ist $\mathcal{O}_K/\mathfrak{p}$ ein Körper (endl. Integritätsbereich $\Rightarrow$ Körper)

$\Rightarrow$ $\mathfrak{p}$ ist maximales Ideal. □

Definition 2: Ein noetherscher ganz abgeschl. Integritätsbereich, in dem jedes Primideal $\neq 0$ maximal ist, heißt Dedekindring.

Für den Rest des § bezeichne $\mathcal{O}$ einen bel. Dedekindring und K seinen Quotientenkörper.

Für Ideale $\mathfrak{a}, \mathfrak{b}$ von $\mathcal{O}$ sind die Teilbarkeitsrelation $\mathfrak{a} \mid \mathfrak{b}$ durch $\mathfrak{b} \subset \mathfrak{a}$, die Summe durch

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

und das Produkt durch

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

definiert.

Satz 3 Jedes von (0) und (1) verschiedene Ideal $\mathfrak{a}$ von $\mathcal{O}$ besitzt eine bis auf die Reihenfolge eindeutige Zerlegung

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

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

Zum Beweis benötigen wir zwei Hilfsaussagen.

Lemma 4 Zu jedem Ideal $\mathfrak{a} \neq 0$ von $\mathcal{O}$ gibt es von Null verschiedene Primideale $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ mit

$$\mathfrak{a} \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

Beweis: Sei $\mathfrak{M}$ die Menge der Ideale $\neq 0$ von $\mathcal{O}$, für welche die Behauptung nicht gilt. Annahme: $\mathfrak{M} \neq \emptyset$. Da $\mathcal{O}$ noethersch ist, bricht jede aufsteigende Kette von Idealen ab. Betrachtet man die Inklusion „$\subset$" als Ordnungsrelation, so hat folglich jede geordnete Teilmenge von $\mathfrak{M}$ ein größtes Element. ($\mathfrak{M}$ ist induktiv geordnet bezügl. „$\subset$") Mit dem Zornschen Lemma folgt also es gibt ein maximales Element $\mathfrak{a} \in \mathfrak{M}$.

Nun ist $\mathfrak{a}$ nicht Primideal $\Rightarrow$ es gibt $b_1, b_2 \in \mathcal{O}$ mit $b_1 b_2 \in \mathfrak{a}$ aber $b_1 \notin \mathfrak{a}, b_2 \notin \mathfrak{a}$

Setze $\mathfrak{a}_1 = (b_1) + \mathfrak{a}$, $\mathfrak{a}_2 = (b_2) + \mathfrak{a}$ so hat man

$\mathfrak{a} \subsetneq \mathfrak{a}_1$, $\mathfrak{a} \subsetneq \mathfrak{a}_2$ und $\mathfrak{a}_1 \mathfrak{a}_2 \subseteq \mathfrak{a}$.

Da $\mathfrak{a}$ maximal in $\mathfrak{M}$, sind $\mathfrak{a}_1, \mathfrak{a}_2 \notin \mathfrak{M}$, sie enthalten also Produkte von Primidealen

$\mathfrak{a}_1 = \mathfrak{p}_2 \cdots \mathfrak{p}_r$ $\quad \mathfrak{a}_2 = \mathfrak{q}_1 \cdots \mathfrak{q}_s$ $\quad \mathfrak{a}_1\mathfrak{a}_2 = \mathfrak{p}_1 \cdots \mathfrak{p}_r \cdot \mathfrak{q}_1 \cdots \mathfrak{q}_s$

und deren Produkt liegt wiederum in $\mathfrak{a}$.

Widerspruch $\square$

Lemma 5: Ist $\mathfrak{p}$ ein Primideal von $\mathcal{O}$ und

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

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

Bew: Wir zeigen zunächst $\mathfrak{p}^{-1} \neq \mathcal{O}$:

Sei $a \in \mathfrak{p}$, $a \neq 0$ und $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq (a) \subseteq \mathfrak{p}$ mit r minimal (ex. nach L. 4)

Dann ist ein $\mathfrak{p}_i \subseteq \mathfrak{p}$ und damit ($\mathfrak{p}_i$ da maximal) $\mathfrak{p}_i = \mathfrak{p}$. OE $i = 1$.

(Ist $\mathfrak{p}_1 \neq \mathfrak{p}$, so gibt es ein $a_1 \in \mathfrak{p}_1 \setminus \mathfrak{p}$ und $a_1 \cdot a_2 \cdots a_r \in \mathfrak{p}$)

Wegen $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subseteq (a)$ gibt es ein $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ mit $b \notin a\mathcal{O}$ also $a^{-1}b \notin \mathcal{O}$.

Andererseits ist jedoch $b\mathfrak{p} \subseteq (a)$, also $a^{-1}b\mathfrak{p} \subseteq \mathcal{O}$. Damit $a^{-1}b \in \mathfrak{p}^{-1}$. $\Rightarrow \mathfrak{p}^{-1} \neq \mathcal{O}$.

Nun sei $\mathfrak{a} \neq 0$ Ideal von $\mathcal{O}$, $\mathfrak{a} = (\alpha_1, \dots, \alpha_n)$.

Annahme: $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$

Dann gilt für jedes $x \in \mathfrak{p}^{-1}$ $\quad x\alpha_i = \sum_j a_{ij}\alpha_j$ mit $a_{ij} \in \mathcal{O}$.

Ist $A = (x\delta_{ij} - a_{ij})_{ij}$, so gilt $\quad A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = 0$.

Für $d = \det A$ folgt somit $d\alpha_1 = \dots = d\alpha_n = 0$ also $d = 0$.

Also ist x Nullstelle des normierten Polynoms

$$f(X) = \det(X\delta_{ij} - a_{ij}) \in \mathcal{O}[X]$$

$\Rightarrow x$ ganz über $\mathcal{O}$. Da $\mathcal{O}$ g.a. folgt $\mathfrak{p}^{-1} = \mathcal{O}$.
Widerspruch. ∎

Beweis von Satz 3

I Zur Existenz der Primzerlegung

Sei $\mathfrak{M}$ die Menge der Ideale $\neq (0), \neq (1)$, die keine Primzerlegung besitzen.
Annahme $\mathfrak{M} \neq \emptyset$: Da $\mathcal{O}$ noethersch (und somit $\mathfrak{M}$ induktiv geordnet bezügl. „⊂") folgt wieder (Zorns Lemma) dass es ein max $\mathfrak{a} \in \mathfrak{M}$ gibt. Dann ex. maximales Ideal $\mathfrak{p}$ mit $\mathfrak{a} \subseteq \mathfrak{p}$ und wegen $\mathcal{O} \subseteq \mathfrak{p}^{-1}$ folgt

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

Nach L.5 ist $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}$ und $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}$.
Da $\mathfrak{p}$ maximales Ideal $\Rightarrow \mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$.
Wegen $\mathfrak{a}$ max. ($\mathfrak{a} \in \mathfrak{M}$) in $\mathfrak{M}$ und wegen $\mathfrak{a} \neq \mathfrak{p}$, also $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathcal{O}$, lässt sich $\mathfrak{a}\mathfrak{p}^{-1}$ als $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ zerlegen, folglich auch

$$\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}_1 \cdots \mathfrak{p}_r \cdot \mathfrak{p}, \quad \text{Widerspruch.}$$

II. Eindeutigkeit

Für ein Primideal $\mathfrak{p}$ gilt:
$\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p} \Rightarrow \mathfrak{a} \subseteq \mathfrak{p}$ oder $\mathfrak{b} \subseteq \mathfrak{p}$ (d.h. $\mathfrak{p} \mid \mathfrak{a}\mathfrak{b} \Rightarrow \mathfrak{p} \mid \mathfrak{a}$ oder $\mathfrak{p} \mid \mathfrak{b}$)

Seien nun
$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$$
zwei Primfaktorlegungen von $\mathfrak{a}$. Dann teilt $\mathfrak{p}_1$ einen Faktor $\mathfrak{q}_i$, OE $i=1$, somit (Kommutativität) $\mathfrak{p}_1 = \mathfrak{q}_1$. Multipliziere mit $\mathfrak{p}_1^{-1}$, wegen $\mathfrak{p}_1 + \mathfrak{p}_1\mathfrak{p}_1^{-1} = \mathcal{O}$ hat man

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

Induktiv ergibt sich $r=s$ und (evtl nach Umordnen) $\mathfrak{p}_i = \mathfrak{q}_i$.

Analog zur Situation in $\mathbb{Z}$ schreibt man $\mathfrak{a} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}$ mit $\mathfrak{p}$ paarweise verschieden □

Zwei Ideale $\mathfrak{a}$ und $\mathfrak{b}$ von $\mathcal{O}$ sind teilerfremd, ~~genau dann,~~ wenn $\mathfrak{a} + \mathfrak{b} = \mathcal{O}$.

~~In der Tat, hätte wenn $\mathfrak{p}$ Primideal mit~~
~~Allgemeiner: Sind $\mathfrak{a}$ und~~

Sind $\mathfrak{a}, \mathfrak{b}$ Ideale von $\mathcal{O}$ und $\mathfrak{p}$ ein Primideal mit $\mathfrak{a} \subseteq \mathfrak{p}$ und $\mathfrak{b} \subseteq \mathfrak{p}$ so gilt auch $\mathfrak{a}+\mathfrak{b} \subseteq \mathfrak{p}$ also $\mathfrak{p} \mid \mathfrak{a}+\mathfrak{b}$.

Deshalb schreibt man häufig auch
$$\mathfrak{a}+\mathfrak{b} = \mathrm{ggT}(\mathfrak{a},\mathfrak{b})$$ für Ideale in einem Dedekindring $\mathcal{O}$.

entsprechend auch
$$\mathfrak{a} \cap \mathfrak{b} = \mathrm{kgV}(\mathfrak{a},\mathfrak{b})$$

35 ist hier ($\mathfrak{p} \supseteq \mathfrak{a}\cap\mathfrak{b} \Rightarrow \mathfrak{p} \supseteq \mathfrak{a} \vee \mathfrak{p} \supseteq \mathfrak{b}$)

Ideale in Dedekindringen (Fortsetzung)

Erinnerung:
- Ein Integritätsring R heißt **Dedekindring**, falls:
  - R noethersch
  - R ganz abg. in $\mathrm{Quot}(R)$
  - Jedes Primideal $\{0\} \neq \mathfrak{p} \subset R$ ist maximal.

Bsp: $K/\mathbb{Q}$ endl., $\mathcal{O}_K \subset K$ Ring der ganzen Zahlen in K (d.h. der ganze Abschluss von $\mathbb{Z}$ in K). $\mathcal{O}_K$ ist Dedekindring.

Satz: Sei R Dedekindring. Jedes Ideal $\{0\} \neq \mathfrak{a} \subset R$, $\mathfrak{a} \neq (0), (1)$, besitzt eine eindeutige Primidealfaktorisierung $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$.

(*) ff!

Chinesischer Restsatz
Sei R Ring und $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subset R$ paarweise koprime Ideale (d.h. $\mathfrak{a}_i + \mathfrak{a}_j = (1)$ $\forall i \neq j$). Dann ist der kanon. Homom. $R \to R/\mathfrak{a}_1 \oplus \ldots \oplus R/\mathfrak{a}_n$ surjektiv und $\ker = \bigcap_{i=1}^n \mathfrak{a}_i$.

Beweis (Algebra)

Sei nun $\mathcal{O}$ Dedekindbereich mit $K = \mathrm{Quot}(\mathcal{O})$.

Def: Ein gebrochenes Ideal in K ist ein endl. erz. $\mathcal{O}$-Untermodul $\mathfrak{a} \subset K$ mit $\mathfrak{a} \neq 0$.

Bem: Ist $a \in K^*$, so ist $(a) = a\mathcal{O} \subset K$ ein gebrochenes Ideal. Ideal in $\mathcal{O}$ ist gebr. Ideal (ganze Ideale).

Bem 6: $\mathfrak{a} \subset K$ gebr. Ideal $\Leftrightarrow$ $\exists\, c \in K^*$: $c\mathfrak{a} \subset \mathcal{O}$ Ideal.

Bew: „$\Rightarrow$“ : $\mathfrak{a}$ endl. erz.

„$\Leftarrow$“ : $\mathcal{O}$ noethersch. □

Satz 7: Die gebr. Ideale $\mathfrak{a} \subset K$ bilden mit der Mult. von Idealen eine abelsche Gruppe, die **Ideal-Gruppe** J_K von K.

Einh-El : $(1) = \mathcal{O}$

Inverses von $\mathfrak{a}$: $\mathfrak{a}^{-1} = \{x \in K;\ x\mathfrak{a} \subset \mathcal{O}\}$.

Bew: • Assoziativität, Kommutativität sind klar.

• $\mathfrak{a}\cdot(1) = \mathfrak{a}$: klar.

• Inverse:

Sei $\mathfrak{p} = \mathfrak{a} \subset \mathcal{O}$ Primideal.

Lemma 5 $\Rightarrow$ $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}$

Prinzip $\Rightarrow$ $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$.

Sei nun $\mathfrak{a} \subset \mathcal{O}$ ein gebr. gewöhnliches Ideal.
Sei $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ eine Primideal-Faktorisierung.
Dann ist

$$\mathfrak{b} := \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1}$$

ein echtes Ideal in K, also $\mathfrak{a}\mathfrak{b} = (1)$.

Falls $\mathfrak{a} \subset \mathcal{O}$ ein gebr. Ideal,
so schreibe $\mathfrak{a} = c^{-1} \cdot (c\mathfrak{a})$ mit $c \in \mathcal{O}$,
so dass $c\mathfrak{a} \subset \mathcal{O}$ ganz.
Dann ist $\mathfrak{b} = c \cdot (c\mathfrak{a})^{-1}$ ein echtes Ideal. □

Satz 8: Jedes gebr. Ideal $\mathfrak{a} \subset K$
hat eine eind. Primidealfaktorisierung

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}}$$
$$0 \neq \mathfrak{p} \subset \mathcal{O} \text{ prim}$$

mit $v_{\mathfrak{p}} \in \mathbb{Z}$ und $v_{\mathfrak{p}} = 0$ für fast alle $\mathfrak{p}$.

Sei $P_K = \{(a) \subset K ; a \in K^*\} \subset J_K$
die Untergruppe der gebr. Hauptideale.
Def: Die Faktorgruppe

$$Cl_K = J_K / P_K$$

heißt Idealklassengruppe von K.

Kern 9: Wir haben die exakte Sequenz

$$1 \longrightarrow \mathcal{O}^* \longrightarrow K^* \longrightarrow J_K \longrightarrow Cl_K \longrightarrow 1.$$
$$a \longmapsto (a), \quad u \longmapsto u P_K$$

Erinnerung: Eine Sequenz von Homs

$\to A \xrightarrow{\varphi} B \xrightarrow{\psi} C \to \dots$

heißt exakt bei B, falls

$\operatorname{Ker}(\psi) = \operatorname{Im}(\varphi)$.

G_K „misst" wie stark $\mathcal{O}$ davon abweicht Hauptidealring zu sein.

$\mathcal{O}^*$ „misst" wie stark sich Zahlen in K^* von gew. Hauptidealen unterscheiden.

Ziel: Verstehe diese Gruppen.

(*) ggT: In R Dedekindring, $a, b \in R$ Ideale $\neq (0), (1)$.

$\operatorname{ggT}(a,b) = a+b$

$\operatorname{kgV}(a,b) = a \cap b \quad (\supset a \cdot b)$

a, b teilerfremd, falls $a+b = (1)$

Im diesem Fall ist $a \cdot b = a \cap b$.

Zerl. $a = \prod_p p^{v_p(a)}$, $b = \prod_p p^{v_p(b)}$

so gilt

$$a+b = \prod_p p^{\min(v_p(a), v_p(b))} \quad (*)$$

$$a \cap b = \prod_p p^{\max(v_p(a), v_p(b))}$$

Satz 6: In R Dedekindring. Jedes Ideal $a \neq 0$ lässt sich durch 2 Elemente erzeugen.

Satz: Sei $\mathfrak{a} \neq (0), (1)$.

Sei $\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n}$ die Primfaktorzerlegung.

Sei $0 \neq \alpha \in \mathfrak{a}$.

$\Rightarrow (\alpha) \subset \mathfrak{a}$

$\Rightarrow \mathfrak{p}_i^{r_i} \mid (\alpha) \quad \forall i = 1, \dots, n$.

Seien $\mathfrak{q}_1, \dots, \mathfrak{q}_m$ die zu $\mathfrak{a}$ coprimen Primideale, die in der Fl.-Zerl. von (α) vorkommen.

Chin. Restsatz für $\mathfrak{p}_i^{r_i+1}$, $i = 1, \dots, n$

$\mathfrak{q}_j$, $j = 1, \dots, m$

$\exists \beta \in R: \quad \beta \equiv \beta_i \pmod{\mathfrak{p}_i^{r_i+1}}$ mit $\beta_i \in \mathfrak{p}_i^{r_i} \setminus \mathfrak{p}_i^{r_i+1}$

$\beta \equiv 1 \pmod{\mathfrak{q}_j}$

Dann gilt:

$\mathfrak{p}_i^{r_i} \mid \alpha$, $\mathfrak{p}_i^{r_i} \nmid \beta$, $\mathfrak{p}_i^{r_i+1} \nmid \beta$

$\mathfrak{q}_j \mid \alpha$, $\mathfrak{q}_j \nmid \beta$

$\mathfrak{p} \nmid \alpha \quad \forall \mathfrak{p} \neq \mathfrak{p}_i, \mathfrak{q}_j$

$\overset{(*)}{\Rightarrow} (\alpha, \beta) = \prod_{\mathfrak{p}} \mathfrak{p}^{\min((\alpha),(\beta))} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n}$. $\square$

Sei nun $K/\mathbb{Q}$ Zahlkörper mit Ganzheitsring $\mathcal{O}_K \subset K$.

Satz: $\mathcal{O}_K$ ist freier $\mathbb{Z}$-Modul vom Rang $n = [K:\mathbb{Q}]$, also $\cong \mathbb{Z}^n$ als ab. Gr.

Man kann $\mathcal{O}_K^*$ und $\mathcal{O}_K$ studieren,
indem man $\mathcal{O}_K$ mit den
$\sigma_i \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$
in einen $\mathbb{R}^n$ einbettet.
Dann mit dem Bild ein Gitter.