$\mathcal{O} :=$ Dedekindring, $K := \mathrm{Quot}(\mathcal{O})$, Id. = Ideal

Lemma 1.1. *Zu jedem Ideal $\mathfrak{a} \neq 0$ von $\mathcal{O}$, existiert ein $r \in \mathbb{N}$ und von Null verschiedene Primideale $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ mit*

$$\mathfrak{a} \supseteq \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_r$$

Beweis: Sei M die Menge aller Id. die die obige Eig. nicht erfüllen. Angenommen M sei nicht leer. Da $\mathcal{O}$ noetherisch ist bricht jede aufsteigende Kette von Id. ab. M ist induktiv durch Inklusion geordnet, also existiert ein maximales Ideal in M, sage $\mathfrak{a}$. $\mathfrak{a}$ ist nicht ein Primideal, also für $b_1, b_2 \in \mathcal{O}$ mit $b_1 b_2 \in \mathfrak{a}$ folgt $b_1, b_2 \notin \mathfrak{a}$. Seien $\mathfrak{a}_1 := \mathfrak{a} + (b_1)$, $\mathfrak{a}_2 := \mathfrak{a} + (b_2)$.
Dann gilt $\mathfrak{a} \subsetneq \mathfrak{a}_1$, $\mathfrak{a} \subsetneq \mathfrak{a}_2$, und $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}$.
Aber dann existieren Primideale $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{a}_1$, $\mathfrak{q}_1 \cdots \mathfrak{q}_n \subseteq \mathfrak{a}_2$, $r, n \in \mathbb{N}$, und es folgt:

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{q}_1 \cdots \mathfrak{q}_n \subseteq \mathfrak{a}_1 \mathfrak{a}_2 \subseteq \mathfrak{a} \quad ⚡ \quad \square$$

Lemma 1.2. *Ist $\mathfrak{p}$ ein Primideal von $\mathcal{O}$ und*

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

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

Beweis: Sei $\mathfrak{p}$ ein Primideal, und $a \overset{\neq 0}{\in} \mathfrak{p}$. Wähle wie in Lemma 1.1 Primideale s.d. $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq (a) \subseteq \mathfrak{p}$, und wähle $r \in \mathbb{N}$ minimal. Dann ist eines dieser $\mathfrak{p}_i$, o.B.d.A. $\mathfrak{p}_1$ in $\mathfrak{p}$ enthalten, und wegen der Maximalität von $\mathfrak{p}_1$ folgt $\mathfrak{p}_1 = \mathfrak{p}$.
Weil sonst wähle für jedes i ein $a_i \in \mathfrak{p}_i \setminus \mathfrak{p}$, und es gilt $a_1 \cdots a_r \in \mathfrak{p}$.
Wegen $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subseteq (a)$, wähle 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 $b\mathfrak{p} \subseteq (a)$, also $a^{-1}b\mathfrak{p} \subseteq \mathcal{O}$ also $a^{-1}b \in \mathfrak{p}^{-1}$.
Somit folgt $\mathfrak{p}^{-1} \neq \mathcal{O}$.

Sei $\mathfrak{a} \neq 0$ ein Id. von $\mathcal{O}$ und $\alpha_1, \ldots, \alpha_n$, $n \in \mathbb{N}$, ein Erzeugendensystem.
Angenommen dass $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$. Sei $x \in \mathfrak{p}^{-1}$, dann gilt:

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

Sei $A := (x\delta_{ij} - a_{ij})$. Dann gilt:

$$A\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix} = \begin{pmatrix} x\delta_{11} - a_{11} & x\delta_{12} - a_{12} & \cdots \\ x\delta_{21} - a_{21} & \ddots & \\ \vdots & & \end{pmatrix}\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix}$$

$$= \begin{pmatrix} \sum_j x \delta_{ij} \alpha_j - a_{ij}\alpha_j \\ \vdots \\ \sum_j x \delta_{nj} \alpha_j - a_{nj}\alpha_j \end{pmatrix} = \underline{0}$$

Dann folgt $(\det A)\alpha_i = 0$, $\forall i \in \{1,\dots,n\}$, also $\det A = 0$

Daher ist x als Nullstelle vom Poly. $f(x) := \det(X\delta_{ij} - a_{ij}) \in \mathcal{O}[X]$ ganz über $\mathcal{O}$, d.h. $x \in \mathcal{O}$. $\square$

Satz 1.3. *Jedes von (0) uns (1) verschiedene Ideal $\mathfrak{a}$ von $\mathcal{O}$ besitzt eine, bis auf Vertauschung, eindeutige Zerlegung*

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

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

Beweis: (Existenz)

Sei M die Menge aller Id. die die obige Eig. nicht erfüllen, angenomen M sei nicht leer. Argumentiere wie in Lemma 1.1, also es existiert ein maximaler Id., sage $\mathfrak{a}$, in M. Dieser ist in einen maximalen Primideal $\mathfrak{p}$ enthalten. Wir erhalten wegen $\mathcal{O} \subseteq \mathfrak{p}^{-1}$, dass:

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

Nach Lemma 1.2 folgt $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}$. Wegen der Maximalität von $\mathfrak{p}$ folgt dass $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$. Weiterhin, wegen der Maximalität von $\mathfrak{a}$ in M und wegen $\mathfrak{a} \neq \mathfrak{p}$, also $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathcal{O}$, besitzt $\mathfrak{a}\mathfrak{p}^{-1}$ eine Primzerlegung, sage: $\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{a}\mathfrak{p}^{-1}$, $r \in \mathbb{N}$

Dann folgt $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{p}$ $\checkmark$

(Eindeutigkeit) $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p} \Rightarrow \mathfrak{a} \subseteq \mathfrak{p} \vee \mathfrak{b} \subseteq \mathfrak{p}$ d.h.

$$\mathfrak{p} \mid \mathfrak{a}\mathfrak{b} \Rightarrow \mathfrak{p} \mid \mathfrak{a} \vee \mathfrak{p} \mid \mathfrak{b}$$

Seien nun

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_n \quad , r, n \in \mathbb{N}$$

Dann teilt $\mathfrak{p}_1$ eines der $\mathfrak{q}_i$, o.B.d.A. $\mathfrak{q}_1$ und wegen den Maximalität $= \mathfrak{q}_1$. Multipliziere mit $\mathfrak{p}_1^{-1}$, und erhalte $\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_n$

So fortfahrend erhalte $r = n$ und nach Vertauschung $\mathfrak{p}_i = \mathfrak{q}_i$, $\forall i$ $\checkmark$

Def. Ein gebrochenes Ideal von K ist ein endl. erzeugter $\mathcal{O}$-Untermodul von K. Ein ganzes Ideal von K ist ein Ideal von $\mathcal{O}$.

Satz 1.4. *Die gebrochenen Ideale bilden eine abelsche Gruppe, die Idealgruppe J_K von K. Das Einselement $(1) = \mathcal{O}$, und das Inverse zu $\mathfrak{a}$ ist*

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

Beweis: Assoz., Komm. und $\mathfrak{a}(1) = \mathfrak{a}$ ist klar.

Für ein Primid. $\mathfrak{p}$ ist nach Lemma 1.1 $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}$, also $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$.

Ist $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ ein ganzes Id., so ist $\mathfrak{b} := \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1}$, $r \in \mathbb{N}$ ein Inverses. Wegen $\mathfrak{b}\mathfrak{a} = \mathcal{O}$, folgt $\mathfrak{b} \subseteq \mathfrak{a}^{-1}$.

Ist umgekehrt $x\mathfrak{a} \subseteq \mathcal{O} \Rightarrow x\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{b} \Rightarrow x \in \mathfrak{b}$ wegen $\mathfrak{a}\mathfrak{b} = \mathcal{O}$. Also folgt $\mathfrak{b} = \mathfrak{a}^{-1}$.

Ist $\mathfrak{a}$ ein gebrochenes Id., und $c \in \mathcal{O}$, $c \neq 0$, mit $c\mathfrak{a} \subseteq \mathcal{O}$, so ist $(c\mathfrak{a})^{-1} = c^{-1}\mathfrak{a}^{-1}$ das Inverse von $c\mathfrak{a}$. Also folgt $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}$. □

Korollar 1.4.1. *Jedes gebrochene Ideal $\mathfrak{a}$ besitzt eine eindeutige Produktdarstellung*

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

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

Beweis: Jedes gebrochene Id. $\mathfrak{a}$ ist Quotient $\mathfrak{a} = \mathfrak{b}/c$, von ganzen Id. $\mathfrak{b}, c$.

Der Rest folgt aus Satz 1.3. □

Bem.: Zu jedem Primid. $\mathfrak{p} \neq 0$ von $\mathcal{O}$ existiert ein diskreter Bewertungsring $\mathcal{O}_\mathfrak{p}$ und eine Bewertung des Quotientenkörpers:

$$v_\mathfrak{p} : K^\times \longrightarrow \mathbb{Z}$$

Ist $x \in K^\times$ und

$$(x) = \prod_\mathfrak{p} \mathfrak{p}^{\nu_\mathfrak{p}}$$

so gilt

$$\nu_\mathfrak{p} = v_\mathfrak{p}(x)$$

Def Die Klassengruppe ist definiert als die Faktorgruppe:

$$Cl_K := J_K / P_K$$

wobei P_K besteht aus den gebrochenen Hauptidealen $(a) = a\mathcal{O}$, $a \in K^\times$

Bem.:
- $P_K < J_K$
- für gebr. Id. $\mathfrak{I}, \mathfrak{J}$: $\quad \mathfrak{I} \sim \mathfrak{J} \Leftrightarrow \mathfrak{I} P_K = \mathfrak{J} P_K$
$$\Leftrightarrow \exists x \in K^\times : \mathfrak{I} = (x)\mathfrak{J}$$
$$\Leftrightarrow \exists x \in K^\times : \mathfrak{I} = x\mathfrak{J}$$
- $\mathcal{O}$ ist ein Hauptidealring wenn Cl_K trivial ist

Bsp. $K := \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$, quadratfrei, es gibt nur endl. viele neg. $d \in \mathbb{Z}$ mit Cl_K trivial:

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