Def: Ein Ideal $A \subsetneq \mathcal{O}_K$ heisst ein <u>Maximalideal</u>, wenn es kein Ideal $B$ gibt mit $A \subsetneq B \subsetneq \mathcal{O}_K$

Lemma 7.25: (i) Für jede aufsteigende Kette

$$A_1 \subseteq A_2 \subseteq \dots \subseteq \mathcal{O}_K$$

von Idealen existiert ein $n \in \mathbb{N}$ sodass

$$A_n = A_{n+1} = A_{n+2} = \dots$$

(ii) Jedes Ideal ist in einem Maximalideal enthalten oder ist $\mathcal{O}_K$.

Beweis: Übungsaufgabe

Satz 7.26: (i) Jedes Maximalideal ist ein Primideal

(ii) Jedes von $\langle 0 \rangle$ verschiedene Primideal ist ein Maximalideal.

Beweis: Sei $M$ ein Maximalideal und $a, b \in \mathcal{O}_K$ mit $ab \in M$.

Angenommen $a \notin M$, dann ist

$$M \subsetneq M + \langle a \rangle$$

$$\Rightarrow M + \langle a \rangle = \mathcal{O}_K \quad \text{(da } M \text{ maximal ist)}$$

$$\Rightarrow \exists\, m \in M \text{ und } \alpha \in \mathcal{O}_K \text{ sodass}$$

$$m + \alpha a = 1$$

$$\Rightarrow b = (m + \alpha a) b = mb + \alpha(ab) \in M.$$

(ii): Fall 1: $K = \mathbb{Q}$

Sei $P$ ein von $\langle 0 \rangle$ verschiedenes Primideal

Dann ist $P = \langle p \rangle$ mit $p \in \mathbb{P}$

Nach Lemma 7.25 gibt es ein Maximalideal $M$ mit $\langle p \rangle \subseteq M$.

und nach Teil V(i) ist $M = \langle q \rangle$ mit $q \in \mathbb{P}$

$p \in \langle p \rangle \subseteq M = \langle q \rangle \Rightarrow q \mid p$

$\Rightarrow q = p$

$\Rightarrow \langle p \rangle = M$ ist ein Maximalideal

Fall 2: $K = \mathbb{Q}[\sqrt{a}]$

Sei $P$ ein von $\langle 0 \rangle$ verschiedenes Primideal

Es gilt $P \cap \mathbb{Z} = p\mathbb{Z}$ für ein $p \in \mathbb{P}$ (L. 7.24)

Angenommen $P$ ist nicht maximal.

Dann existiert ein Maximalideal $M$ mit $P \subsetneq M$

Es gilt $p\mathbb{Z} = P \cap \mathbb{Z} \subseteq M \cap \mathbb{Z} \subsetneq \mathbb{Z}$ ($1 \notin M$ sonst wäre $M = \mathcal{O}_K$)

$p\mathbb{Z}$ ist aber maximal in $\mathbb{Z}$, also ist

$p\mathbb{Z} = P \cap \mathbb{Z} = M \cap \mathbb{Z}$

Sei $\alpha \in M \setminus P$, dann ist also $\alpha \notin \mathbb{Z}$

Es ist aber $N(\alpha) = \alpha\sigma(\alpha) \in M \cap \mathbb{Z} = P \cap \mathbb{Z}$

Da $\alpha^2 - Sp(\alpha)\alpha + N(\alpha) = 0$, ist dann

$$\alpha(\alpha - Sp(\alpha)) \in P \cap \mathbb{Z}$$

Aber $\alpha \notin P$, also ist $\alpha - Sp(\alpha) \in P$ (P ein Primideal)

Ausserdem ist $N(\alpha) = \alpha\sigma(\alpha) \in P$ aber $\alpha \notin P$

$$\Rightarrow \sigma(\alpha) \in P \subseteq M$$

$$\Rightarrow Sp(\alpha) = \alpha + \sigma(\alpha) \in M \cap \mathbb{Z} = P \cap \mathbb{Z}$$

also ist $\alpha = Sp(\alpha) + (\alpha - Sp(\alpha)) \in P$ ↯ □

Für natürliche Zahlen gibt es eine eindeutige Primfaktorzerlegung. Genauso gibt es in $\mathcal{O}_K$ eine eindeutige Primidealzerlegung - unser Ziel ist, dieses Ergebnis zu beweisen. Das nächste Lemma ist ein „erster Schritt".

Lemma 7.27: Sei $\langle 0 \rangle \neq A \subseteq \mathcal{O}_K$ ein Ideal.

Dann gibt es von $\langle 0 \rangle$ verschiedene Primideale

$P_1, \dots, P_n$, sodass $P_1 \cdot \dots \cdot P_n \subseteq A$

Beweis: Die Aussage gilt offensichtlich für $A = \mathcal{O}_K$.

Angenommen, es gibt ein Ideal $A$, für das die Aussage nicht gilt.

Wegen Lemma 7.25 (i) gibt es dann ein Ideal $A$, sodass die Aussage für $A$ nicht gilt, aber für alle Ideale $B$ mit $A \subsetneq B \subseteq \mathcal{O}_K$ gilt.

sonst gäbe es eine unendliche aufsteigende Kette

$A_1 \subsetneq A_2 \subsetneq A_3 \subsetneq \dots \subsetneq \mathcal{O}_K$ von Idealen

Es ist dann offensichtlich $A$ nicht prim, also existieren $b_1, b_2 \in \mathcal{O}_K$ mit $b_1, b_2 \notin A$ aber $b_1 b_2 \in A$

Sei $A_1 := A + \langle b_1 \rangle$ und $A_2 := A + \langle b_2 \rangle$

Es gilt $A_1 \cdot A_2 = (A + \langle b_1 \rangle)(A + \langle b_2 \rangle)$

$= A^2 + A\langle b_1 \rangle + A\langle b_2 \rangle + \langle b_1 \rangle \langle b_2 \rangle$

$\subseteq A$

Aber $A \subsetneq A_1, A_2$

also existieren Primideale $P_1, \dots, P_n$

$Q_1, \dots, Q_m$

sodass $P_1 \cdot \dots \cdot P_n \subseteq A_1$

$Q_1 \cdot \dots \cdot Q_m \subseteq A_2$

$\Rightarrow P_1 \cdot \dots \cdot P_n \cdot Q_1 \cdot \dots \cdot Q_m \subseteq A_1 \cdot A_2 \subseteq A$ ↯ □

wir brauchen auch das anschaulich ähnliche (aber viel einfachere) Ergebnis:

Lemma 7.28: Sei $P \subseteq \mathcal{O}_K$ ein Primideal und

$A_1, \dots, A_n$ Ideale mit $A_1 \cdot \dots \cdot A_n \subseteq P$.

Dann gibt es ein $i$ mit $A_i \subseteq P$.

Beweis: Sonst gäbe es $a_1, \dots, a_n$ mit $a_i \in A_i \setminus P \ \forall i$

und $a_1 \cdot \dots \cdot a_n \in P$

Aber $P$ ist ein Primideal ↯ □

---

Hiermit ist der prüfbare Teil des Kurses beendet.

---

Für Ideale in $\mathcal{O}_K$ ist $\langle 1 \rangle = \mathcal{O}_K$ die multiplikative Identität.

Allerdings gilt für Ideale $A, B \subseteq \mathcal{O}_K$, $A \neq \mathcal{O}_K$

$$A \cdot B \subseteq A \subsetneq \mathcal{O}_K$$

also gibt es kein multiplikatives Inverses (außer für $\mathcal{O}_K$ selbst)

(verglichen mit $\mathbb{N}^+$ oder $\mathbb{Z}$)

Wir brauchen für Ideale eine Konstruktion, die den rationalen Zahlen entspricht.

## Gebrochene Ideale

Def: Eine Teilmenge $A \subseteq K$ heisst ein gebrochenes Ideal in $K$ wenn es ein $\alpha \in \mathcal{O}_K$, $\alpha \neq 0$ gibt, sodass

$$\alpha A = \{\alpha a : a \in A\}$$

ein Ideal in $\mathcal{O}_K$ ist.

Man beachte: Ein gebrochenes Ideal ist nicht unbedingt ein Ideal
Aber ein Ideal ist ein gebrochenes Ideal ($\alpha = 1$)

Zur besseren Unterscheidung nennen wir Ideale in $\mathcal{O}_K$ jetzt ganze Ideale. Ein Ideal kann also ganz und gebrochen sein.

Beispiel: Für $K = \mathbb{Q}$, $\mathcal{O}_K = \mathbb{Z}$ und $n \in \mathbb{N}^+$ ist
$A = \{\frac{a}{n} : a \in \mathbb{Z}\}$ ein gebrochenes Ideal, da $nA = \mathbb{Z}$

Ein paar Eigenschaften:

Lemma 7.29: Für ein gebrochenes Ideal $A \subseteq K$ gilt

(i) $\exists\, n \in \mathbb{N}^+$ sodass $nA$ ein ganzes Ideal ist

(ii) $A$ ist (bezüglich Addition) eine endlich erzeugte abelsche Gruppe.

(iii) $A$ ist ein ganzes Ideal $\Leftrightarrow A \subseteq \mathcal{O}_K$