Korrektur von Vorlesung 24:

Multiplikation von Idealen:

Def: $I_1 \cdot I_2 := \left\{ \sum_{i=1}^{n} \alpha_i \beta_i : \alpha_i \in I_1,\ \beta_i \in I_2,\ n \in \mathbb{N}^+ \right\}$

Nicht so wie einfache Multiplikation von Mengen

Ergibt ein neues Ideal

Wichtig für Satz 7.19

von nun an ist $K = \mathbb{Q}[\sqrt{d}]$ oder auch $K = \mathbb{Q}$

wir werden den folgenden Satz aus der Algebra brauchen:

Satz 7.20: Sei G eine abelsche Gruppe.

G ist endlich erzeugt $\Leftrightarrow G \cong \mathbb{Z}^n \times \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_k\mathbb{Z}$

mit $n, k \in \mathbb{N}$, $m_1, \dots, m_k \in \mathbb{N}^+$

und mit koordinatenweiser Addition.

G ist endlich erzeugt $\Rightarrow$ jede Untergruppe von G ist endlich erzeugt.

Beweis: Aufgabe $\Leftarrow$ ist einfach

$\Rightarrow$: Nehme die kleinst-mögliche erzeugende Menge und zeige, dass die erzeugenden Elemente voneinander unabhängig sind (d.h. es gibt keine nicht-triviale Darstellung der Null).

Mit Hilfe dieses Satzes beweisen wir

Lemma 7.21: Sei $A \in \mathcal{O}_K$ ein Ideal

Dann ist A eine endlich erzeugte abelsche Gruppe und ist Summe endlich vieler Hauptideale.

Beweis: $\mathcal{O}_K$ ist eine endlich erzeugte abelsche Gruppe (von $\{1, \omega_d\}$ nach K. 7.12, oder $\{1\}$ wenn $K = \mathbb{Q}$)

Nach Satz 7.20 ist also A (als Untergruppe) endlich erzeugt.

Seien $a_1, \dots, a_r$ die erzeugenden Elemente, dann ist

$$A = \langle a_1, \dots, a_r \rangle = \langle a_1 \rangle + \dots + \langle a_r \rangle$$ □

Def: Ein <u>Hauptidealring</u> ist ein Ring, in dem jedes Ideal ein Hauptideal ist.

Ein <u>euklidischer Ring</u> ist ein Ring, in dem es einen euklidischen Algorithmus bezüglich einer Funktion f gibt

(es gibt eine Funktion $f: R \setminus \{0\} \to \mathbb{N}^+$ sodass $\forall\, 0 \neq a, b \in R$ existieren $q, r \in R$ mit $b = qa + r$ und $r = 0$ oder $f(r) < f(a)$.)

Mit einem euklidischen Algorithmus existiert auch einen größten gemeinsamen Teiler.

Satz 7.22: Wenn $\mathcal{O}_K$ euklidisch ist, dann ist $\mathcal{O}_K$ ein Hauptidealring.

Beweis: Nach Lemma 7.21 ist jedes Ideal endlich erzeugt. Wir zeigen, dass $\forall\, a, b \in \mathcal{O}_K$, $\langle a, b\rangle = \langle a\rangle + \langle b\rangle$ ein Hauptideal ist.

(Dann folgt die Behauptung mit Induktion über die Anzahl der erzeugenden Elemente.)

Da $\mathcal{O}_K$ euklidisch ist, existiert $ggT(a,b)$ und $n, m \in \mathbb{Z}$ sodass $na + mb = ggT(a,b)$

aber $na \in \langle a\rangle$
$mb \in \langle b\rangle$

$\Rightarrow na + mb \in \langle a\rangle + \langle b\rangle$

$\Rightarrow \langle ggT(a,b)\rangle \subseteq \langle a\rangle + \langle b\rangle$

Ist $x = n'a + m'b \in \langle a\rangle + \langle b\rangle$

dann gilt $ggT(a,b) \mid x$

$\Rightarrow x \in \langle ggT(a,b)\rangle$

Also ist $\langle a\rangle + \langle b\rangle = ggT(a,b)$ □

Bemerkung: Die Rückrichtung gilt nicht unbedingt.

Es gilt Ganzheitsringe, die Hauptidealringe, aber nicht euklidisch sind, und auch welche, die nicht Hauptidealringe sind.

Def: Zwei Ideale $A, B \subseteq \mathcal{O}_K$ heissen teilerfremd wenn

$$A + B = \langle 1 \rangle = \mathcal{O}_K$$

Bemerkung: Seien $a, b \in \mathbb{Z}$. Dann sind a, b teilerfremd
$\iff \langle a \rangle$ und $\langle b \rangle$ in $\mathbb{Z}$ teilerfremd sind.

Lemma 7.23: Seien $A, B \subseteq \mathcal{O}_K$ teilerfremde Ideale
Dann ist $A \cdot B = A \cap B$

Beweis: Es ist offensichtlich $A \cdot B \subseteq B$
und $A \cdot B \subseteq A$
$\Rightarrow A \cdot B \subseteq A \cap B$

Da A, B teilerfremd sind, ist $A + B = \langle 1 \rangle$
also existieren $a \in A$, $b \in B$ sodass $a + b = 1$

Sei $x \in A \cap B$, dann ist

$$x = 1 \cdot x = (a+b)x = ax + bx$$

und $ax \in A \cdot B$ da $x \in B$
$bx \in A \cdot B$ da $x \in A$

$\Rightarrow ax + bx \in A \cdot B$ also ist $A \cdot B = A \cap B$

Def: Ein Ideal $P \subsetneq \mathcal{O}_K$ heisst <u>Primideal</u> wenn $\forall a, b \in \mathcal{O}_K$ gilt

$$ab \in P \Rightarrow a \in P \text{ oder } b \in P$$

Man beachte: Für $\mathcal{O}_K = \mathbb{Z}$ and $p \in \mathbb{P}$ ist $\langle p \rangle$ ein Primideal

Wir haben $\mathcal{O}_K = \langle 1 \rangle$ ausgeschlossen aber

Vorsicht!: $\{0\} = \langle 0 \rangle$ ist ein Primideal

Bei manchen Anwendungen muss man das Nullideal als Primideal betrachten.

Deswegen werden wir es oft extra ausschliessen müssen

Beobachtung: Sei $0 \neq z \in \mathcal{O}_K$.

$\langle z \rangle$ ist ein Primideal $\Leftrightarrow$ z ein Primelement ist

(Folgt direkt aus den entsprechenden Definitionen)

Lemma 7.24: Sei $\langle 0 \rangle \neq P \subseteq \mathcal{O}_K$ ein Primideal.

Dann ist $P \cap \mathbb{Z} = p\mathbb{Z}$ für ein $p \in \mathbb{P}$

Beweis: Für $K = \mathbb{Q}$ (also $\mathcal{O}_K = \mathbb{Z}$) ist das klar

Sei also $K = \mathbb{Q}[\sqrt{d}]$

Aus der Definition folgt, dass $P \cap \mathbb{Z}$ ein Primideal in $\mathbb{Z}$ ist.

Ausserdem ist für $0 \neq x \in P$ auch $x \cdot \sigma(x) \in P$

$\Rightarrow 0 \neq x \cdot \sigma(x) = N(x) \in P \cap \mathbb{Z}$

also ist $P \cap \mathbb{Z} \neq \{0\} = \langle 0 \rangle$ und die Behauptung folgt. $\square$