B4: Algebra II
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

2.Vorlesung

15. April 2021

In diesem Skript werden wir den Ring $\mathcal{O}_K$, wobei K ein quadratischer Zahlkörper ist, weiter untersuchen. Wir werden sehen, dass $\mathcal{O}_K$ nicht immer faktoriell ist, und werden alternative Eigenschaften erforschen. Wir werden Kapitel 1 mit einer Untersuchung der Gruppe der Einheiten $\mathcal{O}_K^\times$ beenden. Zum Schluß werden wir Kapitel 2 anfangen.

Sei $K = \mathbb{Q}(\sqrt{D})$ stets ein quadratischer Zahlkörper.

§Faktorisierung in $\mathcal{O}_K$

- Der fundamentaler Satz der Arithmetik besagt dass $\mathbb{Z} = \mathcal{O}_\mathbb{Q}$ faktoriell ist. Im Allgemeinen ist aber $\mathcal{O}_K$ nicht faktoriell:
- (ÜB) Betrachte $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Dann ist $3 \in \mathbb{Z}[\sqrt{-5}]$ irreduzibel aber nicht prim. Andererseits haben wir in der B3 gezeigt, dass in einem faktoriellen Ring irreduzibele sind prim. Also ist $\mathbb{Z}[\sqrt{-5}]$ nicht faktoriell.
- (ÜB) Wir werden zeigen, dass $\mathcal{O}_K$ "noethersch" ist und damit gilt die Existenz der Faktorisierung in irreduzibele Elemente. Was fehlt also i.A ist die Eindeutigkeit:
- (ÜB) In $\mathbb{Z}[\sqrt{-5}]$ gilt

  (†) $$6 = 2.3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

  $2, 3, 1+\sqrt{-5}$ und $1-\sqrt{-5}$ sind alle irreduzibel und nicht assoziiert.

Erinnerung: Seien I, J Ideale,

$$IJ := \{ \underbrace{\sum_i a_i b_i}_{\text{endliche Summe}} \mid a_i \in I, b_i \in J\} .$$

Zum Beispiel $I =< a >$ und $J =< b > \Rightarrow IJ =< ab >$

Die Idee von Kummer und Dedekind ist eine Faktorisierung von Idealen zu betrachten.

Beispiel 2.1
Die Faktorisierung vom Hauptideal $< 6 >$ in $\mathbb{Z}[\sqrt{-5}]$ ist:

(‡) $$< 6 >=< 2, 1+\sqrt{-5} >< 2, 1-\sqrt{-5} >< 3, 1+\sqrt{-5} >< 3, 1-\sqrt{-5} >$$

Um (‡) zu beweisen, genügt es wegen (†) zu zeigen dass:

Behauptung 1:

$$< 2, 1+\sqrt{-5} >< 2, 1-\sqrt{-5} >=< 2 > , \; < 3, 1+\sqrt{-5} >< 3, 1-\sqrt{-5} >=< 3 > .$$

Beweis von 1 für $< 2 >$*:* Wir berechnen

$$< 2, 1+\sqrt{-5} >< 2, 1-\sqrt{-5} >=< 4, 2+2\sqrt{-5}, 2-2\sqrt{-5}, 6 >$$

und sehen, dass alle Erzeuger hier gerade sind, also gilt

$$< 2, 1+\sqrt{-5} >< 2, 1-\sqrt{-5} >\subseteq< 2 > .$$

Umgekehrt:

$$2 = 6 - 4 \in< 4, 2+2\sqrt{-5}, 2-2\sqrt{-5}, 6 >$$

und damit ist

$$< 2 >\subseteq< 2, 1+\sqrt{-5} >< 2, 1-\sqrt{-5} > .$$

Der Beweis von 1 für $< 3 >$ ist analog (ÜA). Wie angekündigt erhalten wir nun durch (†):

$$< 2, 1+\sqrt{-5} >< 2, 1-\sqrt{-5} >< 3, 1+\sqrt{-5} >< 3, 1-\sqrt{-5} >=< 2 >< 3 >=< 6 > .$$

□

Behauptung 2: (ÜB) Alle vier Ideale sind Primideale. Wir argumentieren folgendermassen für $< 3, 1-\sqrt{-5} >$. Die Abbildung ϕ ist ein surjektiver Homomorphismus mit $ker(\phi) =< 3 >$

$$\begin{array}{rccc} \phi: & \mathbb{Z} & \to & \mathbb{Z}[\sqrt{-5}]/ < 3, 1-\sqrt{-5} > \\ & z & \mapsto & z+ < 3, 1-\sqrt{-5} > \end{array}$$

also ist $\mathbb{Z}[\sqrt{-5}]/ < 3, 1-\sqrt{-5} >\cong \mathbb{Z}/ < 3 >$ ein Körper.

Bemerkung 2.1
(ÜB) Man könnte auch zeigen dass

$$< 2, 1+\sqrt{-5} >< 3, 1+\sqrt{-5} >=< 1+\sqrt{-5} > , \; < 2, 1-\sqrt{-5} >< 3, 1-\sqrt{-5} >=< 1-\sqrt{-5} >$$

und die andere Faktorisierung von 6 in (†) ausnutzen.

§Einheiten

Wir berechnen nun explizit die Einheiten von $\mathcal{O}_K = \mathbb{Z}[\omega]$. Dafür führen wir die Norm ein:

(1) $N : \mathbb{Q}(\sqrt{D}) \to \mathbb{Q}$

$$\begin{aligned} N(a+b\sqrt{D}) &:= (a+b\sqrt{D})\overline{(a+b\sqrt{D})} \\ &= (a+b\sqrt{D})(a-b\sqrt{D}) \\ &= a^2 - b^2 D \end{aligned}$$

(2) (i) Für $D \equiv 2, 3 \bmod 4, \omega = \sqrt{D}, \alpha \in \mathbb{Z}[\omega], \alpha = r+s\sqrt{D} \in \mathbb{Z}[\omega]$, mit $r, s \in \mathbb{Z}$ und $N(\alpha) = N(r+s\sqrt{D}) = r^2 - s^2 D \in \mathbb{Z}$.

(ii) Für $D \equiv 1 \bmod 4$, $\omega = \frac{1+\sqrt{D}}{2}$, $\alpha \in \mathbb{Z}[\omega]$, $\alpha = r + s\frac{1+\sqrt{D}}{2} = (r+\frac{s}{2}) + (\frac{s}{2})\sqrt{D}$, mit $r, s \in \mathbb{Z}$ und
$N(\alpha) = (r+\frac{s}{2})^2 - D(\frac{s}{2})^2$, also $N(\alpha) = r^2 + rs + \frac{1-D}{4}s^2 \in \mathbb{Z}$.

Wir haben bewiesen: $N(\alpha) \in \mathbb{Z}$ für alle $\alpha \in \mathbb{Z}[\omega]$.

(3) Für $r, s \in \mathbb{Z}$ ist also $N : \mathbb{Z}[\omega] \to \mathbb{Z}$ durch $N(\alpha) = N(r + s\omega) = (r + s\omega)\overline{(r + s\omega)} = (r + s\omega)(r + s\overline{\omega})$ gegeben, wobei

$$\overline{\omega} = \begin{cases} -\sqrt{D} \text{ falls } D \equiv 2, 3 \bmod 4 \\ \frac{1-\sqrt{D}}{2} \text{ falls } D \equiv 1 \bmod 4 \end{cases}$$

(4) $r + s\overline{\omega} \in \mathbb{Z}[\omega]$ (ÜA).

(5) Die Norm ist multiplikativ (ÜA).

(6) **Behauptung:** $\alpha \in \mathbb{Z}[\omega]^\times \Leftrightarrow N(\alpha) = \pm 1$

Beweis. „$\Rightarrow$“ $\alpha \in \mathbb{Z}[\omega]^\times \Rightarrow \exists \beta \in \mathbb{Z}[\omega]$ mit $\alpha\beta = 1$, also ist $N(\alpha\beta) = N(\alpha)N(\beta) = 1$ also $N(\alpha) \in \mathbb{Z}^\times \Rightarrow N(\alpha) = \pm 1$.
„$\Leftarrow$“ Sei $N(r + s\omega) = \pm 1$, also ist $(r + s\omega)\underbrace{\overline{(r + s\omega)}}_{\in \mathbb{Z}[\omega]} = \pm 1$ also ist $r + s\omega$ invertierbar in $\mathbb{Z}[\omega]$ mit Inverse $\pm\overline{(r + s\omega)}$. □

Bemerkung 2.2
Betrachte die Diophantine'sche Gleichung $x^2 - Dy^2 = \pm 1$ (die Pell'sche Gleichung). Wir haben gezeigt: $x, y \in \mathbb{Z}$ ist eine Lösung$\Leftrightarrow x + y\omega \in \mathbb{Z}[\omega]^\times$

Kapitel 2: Moduln

§Moduln

R ist stets ein kommutativer Ring mit Eins.

Definition 2.1 (i) Ein R-Modul ist eine abelsche Gruppe $(M, +)$ versehen mit einer Verknüpfung (Skalarmultiplikation):

$$\begin{array}{ccc} R \times M & \to & M \\ (r, x) & \mapsto & rx \end{array},$$

so dass für alle $x, y \in M$ und $r, s \in R$ Folgendes gilt:

(1) $1.x = x$

(2) $r(sx) = (rs)x$

(3) $(r + s)x = rx + sx$

(4) $r(x + y) = rx + ry$

(ii) Eine Untergruppe $N \leq M$ ist ein Untermodul, wenn $RN \subseteq N$.