Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

3.Vorlesung

4. Mai 2017

§Einheiten

Wir berechnen nun explizit die Einheiten in $\mathbb{Z}[\omega]$.

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

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

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

(ii) $D \equiv 1 \bmod 4$, $\omega = \frac{1+\sqrt{D}}{2}$, $\alpha \in \mathbb{Z}[\omega]$, $\alpha = r + s\frac{1+\sqrt{2}}{2}$, $r, s \in \mathbb{Z}$.
Berechne:$N(\alpha) = (r+\frac{s}{2})^2 - D(\frac{s}{2})^2$, also $N(\alpha) = r^2 + rs + \frac{1-D}{4}s^2 \in \mathbb{Z}$.
Damit ist bewiesen: $N(\alpha) \in \mathbb{Z}$ für $\alpha \in \mathbb{Z}[\omega]$

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

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

Behauptung: $r + s\overline{\omega} \in \mathbb{Z}[\omega]$ (prüfe es!)

(4) Die Norm ist mulktiplikativ (prüfe es)

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

Beweis. „⇒“$\alpha \in \mathbb{Z}[\omega]^\times \Rightarrow \exists \beta \in \mathbb{Z}[\omega]$ mit $\alpha\beta = 1$, also ist $N(\alpha\beta) = N(\alpha)N(\beta) = 1$ also $N(\alpha) \in \mathbb{Z}^\times \Rightarrow N(\alpha) = \pm 1$.

„⇐“ Sei $N(r+s\omega) = \pm 1$, $r, s \in \mathbb{Z}$, 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 3.1
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

1. Moduln
2. Moduln über HIR
3. Noether'sche Moduln

§Moduln

R ist stets ein kommutativer Ring mit Eins.

Definition 3.1 (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 $RN \subseteq N$.

Beispiel 3.1 (i) $R = K$ Körper.

K-Modul=K-Vektorraum.

Untermodul=Unterraum.

(ii) $R = \mathbb{Z}$.

$\mathbb{Z}$-Modul=abelsche Gruppe.

Untermodul=Untergruppe.

(iii) $M = \{0\}$ trivialer Modul.

(iv) $M = R$ ist ein R-Modul.

Untermodul=Ideal von R.

Definition 3.2
Seien M, N zwei R-Moduln.

(i) Ein R-Moduln Homomorphismus ist ein Gruppenhomomorphismus $\phi : M \to N$, so dass $\phi(rx) = r\phi(x)$ für alle $x \in M$ und $r \in R$.

(ii) Sei $N \leq M$ ein Untermodul. Die Faktorgruppe M/N ist ein R-Modul, wenn sie mit der folgenden Skalarmultiplikation versehen ist:

$$\begin{array}{rcl} R \times M/N & \to & M/N \\ (r, x+N) & \mapsto & rx+N \end{array}$$

(iii) Bezeichnung: $\mathrm{Hom}_R(M,N) := \{\phi : M \to N \mid \phi \text{ ist ein } R-\text{Modul Homomorphismus}\}$

Lemma 3.1
Seien M, N, V drei R-Moduln.

(i) $\phi \in \mathrm{Hom}_R(M,N) \wedge \psi \in \mathrm{Hom}_R(N,V) \Rightarrow \psi \circ \phi \in \mathrm{Hom}_R(M,V)$.

(ii) $\phi \in \mathrm{Hom}_R(M,N) \Rightarrow \ker(\phi) \leq M \wedge$ Im $(\phi) \leq N$.

(iii) $\phi \in \mathrm{Hom}_R(M,N)$ bijektiv $\Rightarrow \phi^{-1} \in \mathrm{Hom}_R(N,M)$, ϕ ist dann ein R-Modul Isomorphismus.

(iv) (Projektion) Sei $N \leq M$ ein Untermodul.

$$\begin{array}{rccl} \pi : & M & \to & M/N \\ & x & \mapsto & x+N \end{array}$$

ist ein R-Modul Homomorphismus.

(v) Wenn $N \leq M$, induziert π eine Bijektion zwischen den Untermoduln von M, die N enthalten, und den Untermoduln von M/N.

Beweis. Übungsaufgabe. □

Proposition 3.2 (Homomorphiesatz für Moduln)
Sei $\phi \in \mathrm{Hom}_R(M,N)$; es gilt $M/\ker(\phi) \cong$ Im (ϕ)

Beweis. Übungsaufgabe. □

Definition 3.3 (i) Die Summe einer Familie $(M_i)_{i \in I}$ von Untermoduln eines R-Moduls M ist

$$\sum_{i \in I} M_i = \{\sum_{i \in I} x_i \mid x_i \in M_i \text{ und } x_i = 0 \text{ für fast alle } i\}$$

Es ist $\sum_{i \in I} M_i \leq M$. (ÜA)

(ii) Für $a \in M$ sei $Ra := \{ra \mid r \in R\} \leq M$. (ÜA)

(iii) Sei $A \subseteq M$. Der von A erzeugte Untermodul von M ist

$$\sum_{a \in A} Ra$$

(iv) M ist endlich erzeugt, wenn es $A \subseteq M$ existiert mit A endlich und $M = \sum_{a \in A} Ra$.

Lemma 3.3
Für $A \subseteq M$ ist $\sum_{a \in A} Ra$ der kleinste Untermodul von M, der A enthält.

Beweis. ÜA. □

Definition 3.4 (i) Die direkte Summe einer Familie $(M_i)_{i\in I}$ von R-Moduln ist der R-Modul

$$\bigoplus_{i\in I} M_i := \{(x_i)_{i\in I} \in \prod_{i\in I} M_i \mid x_i = 0 \text{ für fast alle } i\}$$

mit $r(x_i)_{i\in I} = (rx_i)_{i\in I}$ für $r \in R$.

(ii) Ein R-Modul M ist direkte Summe einer Familie $(M_i)_{i\in I}$ von Untermoduln (in Zeichen $M = \bigoplus_{i\in I} M_i$) wenn der R-Modul Homomorphismus

$$\begin{array}{ccc} \bigoplus_{i\in I} M_i & \to & M \\ (x_i)_{i\in I} & \mapsto & \sum_{i\in I} x_i \end{array}$$

ein R-Moduln-Isomorphismus ist.

(iii) Sei M ein R-Modul und $N \leq M$ ein Untermodul. Existiert ein Untermodul $V \leq M$ mit $M = N \bigoplus V$, so heißt N direkter Summand von M und V ein Komplement zu N.

4