- Algebraische Zahlentheorie -

Algebra B IV

SS 2013

3. Vorlesung am 22.04.2013

- Kuhlmann -

---

§ Einheiten.

Algebra: Kapitel 6
Norm Spur
Diskriminante

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

① Norm auf $\mathbb{Q}(\sqrt{D})$

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

das Konjugierte

$$N(a+b\sqrt{D}) = (a+b\sqrt{D})\overline{(a+b\sqrt{D})}$$

$$= (a+b\sqrt{D})(a-b\sqrt{D})$$

$$= a^2 - Db^2$$

② (a) $D \equiv 2,3 \mod 4$ $\quad \omega = \sqrt{D}$

$$N(r+s\sqrt{D}) = \underbrace{r^2 - Ds^2}_{\in \mathbb{Z}}, \quad r,s \in \mathbb{Z}$$

(ii) $D \equiv 1 \bmod 4 \qquad \omega = \frac{1+\sqrt{D}}{2}$

$\alpha \in \mathbb{Z}[\omega] \qquad \alpha = r + s\left(\frac{1+\sqrt{D}}{2}\right)$

$r, s \in \mathbb{Z}$

$$= \left(r + s/2\right) + \left(s/2\right)\sqrt{D}$$

Berechne:

$N(\alpha) = \left(r+s/2\right)^2 - D\left(s/2\right)^2$ also

$N(\alpha) = r^2 + rs + \underbrace{\frac{(1-D)}{4}}_{\in \mathbb{Z}} s^2$

Damit ist bewiesen:

$N(\alpha) \in \mathbb{Z}$ für $\alpha \in \mathbb{Z}[\omega]$.

(3) $N : \mathbb{Z}[\omega] \longrightarrow \mathbb{Z}$

ist durch

$$N(\alpha) = N(r + s\omega) = (r+s\omega)\overline{(r+s\omega)}$$

$$= (r + s\omega)(r + s\bar{\omega}) \quad \text{gegeben}$$

wobei $r, s \in \mathbb{Z}$ und

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

Beh: $r + s\bar{\omega} \in \mathbb{Z}[\omega]$ (prüfe es!).

④ die Norm ist multiplikativ (" ").

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

Beweis: "$\Rightarrow$" $\alpha \in \mathbb{Z}[\omega]^\times \Rightarrow \exists \beta \in \mathbb{Z}[\omega]$

mit $\alpha\beta = 1$. Also ist $N(\alpha\beta) = N(\alpha)N(\beta) = 1$

$N(\alpha), N(\beta) \in \mathbb{Z}^\times$

$\Rightarrow$

$N(\alpha) = \pm 1$.

"$\Leftarrow$" Sei $N(r + s\omega) = \pm 1$ also ist

$r, s \in \mathbb{Z}$

$(r + s\omega)\underbrace{(r + s\omega)}_{\in \mathbb{Z}[\omega]} = \pm 1$

also ist $(r + s\omega)$ invertierbar in $\mathbb{Z}[\omega]$

mit Inverse $\pm \overline{(r + s\omega)}$ ∎

Bemerkung: Betrachte die Diophantine'sche Gleichung $x^2 - Dy^2 = \pm 1$ (die Pell'sche Gleichung)

$D \equiv 2, 3 \bmod 4$

Wir haben gezeigt: $x, y \in \mathbb{Z}$ ist eine Lösung

$\Leftrightarrow x + y\omega \in \mathbb{Z}[\omega]^\times$ ∎

Kapitel II. 1. Moduln
2. Moduln über HIR
3. Noethersche Moduln.

Moduln.

R kommutativ mit Eins. stets.

Definition 1. (i) Ein *R-Modul* ist eine abel'sche Gruppe $(M,+)$ versehen mit einer Verknüpfung (Skalarmultiplikation):

$$R \times M \longrightarrow M$$

$$(r, x) \longmapsto rx$$

so daß $\forall x, y \in M$, $\forall r, s \in R$:

1. $1x = x$
2. $(rs)x$
3. $(r+s)x = rx + sx$
4. $r(x+y) = rx + ry$.

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

Beispiele: (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 R-Modul

Untermodul = Ideal von R.

Definition 2. M, N R-Moduln

(i) Ein R-Modulhomomorphismus ist ein Gruppenhomomorphismus

$$\varphi : M \longrightarrow N \text{ so daß}$$

$$\varphi(rx) = r\,\varphi(x) \qquad \forall\, x \in R,\ x \in M$$

(ii) Sei $N \leq M$ Untermodul, die Faktorgr.

M/N ist R-Modul wenn versehen

mit der Skalarmult.

$$R \times M/N \longrightarrow M/N$$

$$(r,\ x+N) \longmapsto rx + N$$

(iii) **Bezeichnung:**

$$\mathrm{Hom}_R(M,N) := \{ \varphi : M \to N \mid \varphi \text{ } R\text{-Modul Homomorphismus} \}.$$

Lemma 1 Seien M, N, V R-Moduln

(i) $\varphi \in \mathrm{Hom}_R(M,N)$, $\psi \in \mathrm{Hom}_R(N,V)$

$\Rightarrow \psi \circ \varphi \in \mathrm{Hom}_R(M,V)$.

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

(iii) $\varphi \in \mathrm{Hom}_R(M,N)$ bijektiv $\Rightarrow$

$\varphi^{-1} \in \mathrm{Hom}_R(N,M)$

φ ist also R-Modul-Isomorphismus.

(iv) (Projektum) Sei $N \leq M$ Untermodul.

$$\pi : M \longrightarrow M/N$$

$$x \longmapsto x + N$$

ist R-Modul Homomorphismus.

(v) $N \leq M$ so induziert

π eine Bijektion zwischen der

Untermoduln von M, die N enthalten

und den Untermoduln von M/N. ∎

Beweis: ü A.

Homomorphisatz für Moduln.

Sei $\varphi \in \mathrm{Hom}_R(M, N)$; es ist

$$M/\ker\varphi \cong \mathrm{Im}\,\varphi .$$

Beweis: ü A. ∎

Definition 3.

(i) die <u>Summe</u> einer Familie $(M_i)_{i \in I}$

von Untermoduln eines R-Moduls M ist

$$\sum_{i \in I} M_i := \left\{ \sum_{i \in I} x_i \;\middle|\; x_i \in M_i \text{ ; fast alle } x_i = 0 \right\}$$

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

(ii) Für $a \in M$ sei

$$Ra := \{ra \mid r \in R\} \leq M. \quad (ÜA).$$

(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 existiert, $A \subseteq M$, A endlich, mit $M = \sum_{a \in A} Ra$

Lemma 2. Für $A \subseteq M$ ist $\sum_{a \in A} Ra$ der kleinste Untermodul von M, der A enthält.

Beweis: ÜA. ∎

Definition 4.

(i) die <u>direkte Summe</u> einer Familie $(M_i)_{i \in I}$ von R-Moduln ist der R-Modul

$$\bigoplus_{i \in I} M_i := \left\{ (x_i)_{i \in I} \in \prod_{i \in I} M_i \;\middle|\; x_i = 0 \text{ für fast alle } i \right\}$$

mit $r \cdot (x_i)_{i \in I} := (r x_i)_{i \in I}$

für $r \in R$.

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

$$\bigoplus_{i \in I} M_i \longrightarrow M$$

$$(x_i)_{i \in I} \longmapsto \sum_{i \in I} x_i$$

ein R-Moduln-Isomorphismus ist.

(iii) Sei M ein R-Modul und $N \leq M$ ein Untermodul. Existiert ein Untermodul $V \leq M$ mit $M = N \oplus V$ so heißt N ein <u>direkter Summand</u> von M und V ein <u>Komplement</u> zu N.
