

Algebraische Zahlentheorie  
 B IV SS 2013  
 - Kuhlmann -

4. Vorlesung am 25.04.2013.

Lemma 1. Sei  $M$   $R$ -Modul,  $N, V \subseteq M$

Untermoduln. Es sind äquivalent:

(1)  $M = N \oplus V$

(2)  $M = N + V$  und  $N \cap V = \{0\}$

(3) jedes  $x \in M$  läßt sich eindeutig schreiben als  $x = y + z$  mit  $y \in N, z \in V$ .  $\square$

Beweis:  
 ÜA.

Beispiel.  $G = \mathbb{Z}_4$   $H = \langle 2 \rangle$  hat kein Komplement im  $\mathbb{Z}$ -Modul  $G$ ; weil die einzigen Untermoduln von  $G$   $\{0\}, H$  und  $G$  sind.  $\square$

Definition 1. (i) Sei  $S \subseteq M$ . Eine lineare Kombination aus  $S$  Elemente ist  $x \in M; x = \sum r_i x_i$ ,  $r_i \in R, x_i \in S$   
endliche Summe      Koeffiziente

Notation, Bemerk: (ii)  $\text{Span}_R S := \{x \mid x \text{ lin. Komb. aus } S\}$   
 $= \sum_{S \in S} R_S$

Lemma 2. Sei  $N \subseteq M$ . Es gelten:

(1)  $M$  endl. erzeugt  $\Rightarrow M/N$  endl. erzeugt

Beweis:

üA.

(2)  $N$  und  $M/N$  endl. erz.  $\Rightarrow M$  endl. erz.  $\square$

Definition 3.  $S \subseteq M$  ist linear unabhängig

wenn

$$\sum r_i x_i = 0 \Rightarrow r_i = 0 \quad \forall i$$

$r_i \in R$

endl.

$x_i \in S$

Summe

Definition 4. (i)  $x \in M$  ist Torsionselement  $\Leftrightarrow$

$\exists r \in R$  kein Nullteiler mit  
 $rx = 0$

(ii)  $M_{\text{tor}} := \{x \mid x \text{ Torsionel}\}$

ist ein Untermodul (vgl. üB2);

der Torsionsmodul von  $M$ .

(iii)  $M$  ist torsionfrei  $\Leftrightarrow M_{\text{tor}} = \{0\}$ .

Bemerkung:  $x \in M_{\text{tor}} \Rightarrow \{x\}$  ist nicht linear unabh.

Definition 5. (i)  $S \subseteq M$  ist eine Basis  $\Leftrightarrow$

$S$  erzeugt  $M$  und  $S$  ist lin. unabh.

Konvention:  $S = \emptyset$  ist l. unabh. und  $\text{span } \emptyset = \{0\}$

(ii)  $M$  ist frei wenn es eine Basis hat.

Bemk (i)  $S$  Basis  $\Leftrightarrow$  jedes  $x \in M$  eine eindeutige Darstellung als l. K aus  $S$  Elemente hat.

(ii) jeder  $K$ -Vektorraum hat eine Basis als ist frei als  $K$ -Modul, betrachte aber:

Beispiel:  $G = \mathbb{Z}_2 = \langle 1 \rangle$  ist nicht frei als  $\mathbb{Z}$ -Modul weil  $1 \in G_{\text{tor}}$ .

Lemma 3. sind äquivalent

Beweis: (1)  $M$  ist frei mit Basis  $S$   
 $\bar{u} A$  (2)  $M = \bigoplus_{x \in S} Rx$  □

Lemma 4 Sei  $I \neq R$ ;  $M$   $R$ -Modul dann ist

(1)  $IM := \left\{ \sum_{\text{endl. Summe}} r_j y_j \mid r_j \in I; y_j \in M \right\}$   
ein Untermodul

(2)  $M/IM$  ist ein  $R/I$ -Modul.

Beweis  $R/I \times M/IM \longrightarrow M/IM$   
 $\bar{u} A$   $(\bar{r}, \bar{x}) \longmapsto \overline{rx}$  □

Lemma 5. Sei  $M$  frei mit Basis  $\{x_j\}_{j \in J}$

und  $I \triangleleft_+ R$ . Dann ist  $M/IM$  frei als

$R/I$ -Modul mit Basis  $\{\bar{x}_j\}_{j \in J}$

Beweis.  $\{\bar{x}_j\}$  erzeugt  $M/IM$  **üA.**

Wir zeigen lin. Unab über  $R/I$ .

$$\text{Nun } \sum_j r_j \bar{x}_j = 0 \Leftrightarrow \sum_j r_j x_j \in IM$$

$$\Leftrightarrow \sum_j r_j x_j = \sum_l t_l y_l \quad \text{für geeignete}$$

$t_l \in I$   
 $y_l \in M$

Nun  $y_l = \sum_k r_{lk} x_k$  so wir schreiben

$$\sum_l t_l y_l \text{ um und bekommen } \sum_j r_j x_j = \sum_k s_k x_k$$

nun mit  **$s_k \in I$** .

Die Eindeutigkeit der Darstellung bezgl

einer Basis impliziert nun  $r_j \in I \quad \forall j$

oder  $\bar{r}_j = 0$  wie erwünscht.  $\square$

Korollar 6 Sei  $M$  ein  $R$ -Modul und  
 $S$  eine Basis mit  $|S| = n \in \mathbb{N}$   
Dann haben alle andere Basen  
Kardinalität  $n$ .

Beweis  $\Leftrightarrow R$  ist kein Körper (sonst ist  $R = K$   
und  $M$   $K$ -Vektorraum und  $\dim_K M = n$   
ist eindeutig).

Sei  $I \triangleleft R$  maximal. Sei  $S = \{x_j\}$ ;

dann ist  $\{\bar{x}_j\}$   $R/I$ -Basis für den

$K := R/I$ -Vektorraum  $M/IM$ .

Wenn  $\{y_k\}$  eine beliebige Basis von  $M$  ist;

dann ist ebenso  $\{\bar{y}_k\}$  eine  $R/I$ -Basis

für den Vektorraum.  $\square$

Korollar 7  $M$  endl erzeugt und frei  $\Rightarrow$   
jede Basis ist endlich.

Beweis  $\{x_j\}$  endl. und erzeugend

$\Rightarrow \{\bar{x}_j\}$  erzeugend für  $M/IM$  als

$R/I$ -Vektorraum ( $I$  maximales Ideal) also ist

$M/IM$  endlich dimensional, und damit sind  
notwendigerweise alle Basen von  $M$  endlich.  $\square$

Bemerk. Wir haben gezeigt:

$M$  frei mit  $\{x_j\}_{j \in J}$  Basis

dann ist  $|J|$  eindeutig definiert.

Definition 6 Sei  $M$  frei mit Basis  $\{x_j\}_{j \in I}$ .

Notation:

Definiere  $\dim_R M := |I|$ .

Bemerk. Wir haben gezeigt in Korollar 6:

$$\dim_R M = \dim_K V \quad I \nsubseteq R \text{ (Maximal)}$$

wobei  $K = R/I$  und  $V = M/IM$ .  $\square$