Algebraische Zahlentheorie

Algebra B IV

Kuhlmann

6. Vorlesung am 02.05.2013

Beweis (vom Satz 4 der 5. Vorlesung):

Betrachte den Homomorphismus

$$\varphi : M \twoheadrightarrow M/_{M_{tor}}$$

$$x \longmapsto \bar{x}$$

Nun ist $M/_{M_{tor}}$ endlich erzeugt und torsionsfrei

also (Satz 3 5. Vor) ist er frei

Lemma 5 (5. Vor) liefert $F \leq M$; F frei

mit $M = \ker \varphi \oplus F$

und $\varphi\restriction_F : F \simeq M/_{M_{tor}}$,

damit ist $\dim_R F = \dim_R M/_{M_{tor}}$

eindeutig bestimmt $\square$

Wir wollen nun M_{tor} weiter untersuchen; wir untersuchen also endlich erzeugte Torsionsmoduln.

Definition und Notation.

(a) $r \in R$: $M[r] := \{x \in M \mid rx = 0\}$

der r-Torsionsuntermodul

(b) $M[r^\infty] := \bigcup_{k \in \mathbb{N}} M[r^k]$.

Bemerkung 1: $\{0\} \neq M = M_{tor}$ endl. erzeugt Torsionsmodul $\Rightarrow \exists\, a \in R,\ a \neq 0$ mit $aM = 0$

(Seien $v_1, \dots, v_s$ Erzeuger; $a_1, \dots, a_s \in R$ $a_i \neq 0$ mit $a_i v_i = 0$; setze $a := a_1 \cdots a_s$).

Lemma 1 Sei M endl. erzeugt Torsionsmodul und wähle $0 \neq a \in R$ mit $aM = 0$ und $a = bc$ mit $ggT(b, c) = 1$.

Es ist: $M = M[b] \oplus M[c]$.

Beweis $\exists\ x, y \in R$ mit $1 = xb + yc$
(Vgl Prop 4 5. Vor. B3 am 8.11. 2012)

Sei $v \in M$; es ist $v = xbv + ycv$

dann ist $xbv \in M[c]$ und $ycv \in M[b]$,

also $M = M[b] + M[c]$.

Sei $v \in M[b] \cap M[c]$; wir rechnen

$$v = (xb + yc)v = \underbrace{xbv}_{=0} + \underbrace{ycv}_{=0} = 0. \quad \square$$

Satz 1 Sei $0 \neq M$ endl. erzeugt Torsionsmodul.

Dann ist
$$M = \bigoplus_{\substack{p \text{ prim} \\ M[p^\infty] \neq 0}} M[p^\infty]$$

Bemerkung 2: M endl. erzeugt $\Rightarrow$
$|\{p \in R \mid p \text{ prim und } M[p^\infty] \neq 0\}| < \infty$

Beweis Wähle $a \neq 0$ mit $aM = 0$ $\quad a \in R$

Lemma 1 und Induktion anwenden ergibt

$$M = M[a] = \bigoplus_{\substack{p \mid a \\ p \text{ prim} \\ M[p^\infty] \neq 0}} M[p^\infty].$$

Bemerkung 3 Die Darstellung hängt nicht von a ab;

ist nämlich $M = M[b]$; q prim ;

$q \mid b$ aber $q \nmid a$ dann ist $ggT(a,q) = 1$

und damit $M = M[aq] = M[a] \oplus M[q]$
$= M$

also $M[q] = 0$. ∎

Satz 2 Sei $0 \neq M$ endl. erzeugt ; $p \in R$

prim mit $M[p^\infty] \neq 0$. Dann existiert

eine eindeutige Folge

$$1 \leq \nu_1 \leq \ldots \leq \nu_s \quad \in \mathbb{N} \text{ sodaß}$$

$$M[p^\infty] \simeq R/\langle p^{\nu_1}\rangle \oplus \ldots \oplus R/\langle p^{\nu_s}\rangle$$

Korollar :

Struktursatz für endlich erzeugte Moduln

über HIR : Sei R HIR , M R-Modul , ist

M endl. erzeugt über R so ist

$$M \simeq R^d \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{t_s} R/\langle p_i^{\nu_{ij}}\rangle$$

mit eindeutigen:

$d, s \in \mathbb{N}_0$; $p_1, \ldots, p_s$ paarweise verschiedene

Primelemente; $t_s \in \mathbb{N}$;

$1 \leq \nu_{ij} \leq \ldots \leq \nu_{it_s} \in \mathbb{N}$. $\blacksquare$

Für den Beweis vom Satz 2 brauchen wir einiges.
(Terminologie, Bemerkung 5, Lemma 3).
Terminologie: (I) $y_1, \ldots, y_m \in M$ sind unabhängig

wenn $\operatorname{Span}_R\{y_1, \ldots, y_m\} \simeq \bigoplus_{i=1}^{m} R y_i$; oder die folgende

äquivalente Bedingung gilt:

$a_1 y_1 + \cdots + a_m y_m = 0 \quad \Rightarrow \quad a_i y_i = 0$

für $a_1, \ldots, a_m \in R \qquad \forall\, i = 1, \ldots, m$.

Bemerkung 4 lineare Unabhängigkeit $\Rightarrow$ Unabhängigkeit immer,

die Umkehrung gilt für torsionsfreie Moduln.

(II) Sei $x \in M$; $\varphi_x : R \twoheadrightarrow Rx$, $r \longmapsto rx$; es gelten

$I_x := \ker \varphi_x$ ist Hauptideal und $R/_{I_x} \simeq Rx$.

Ein Erzeuger für I_x heißt eine Periode für x.

Bemerkung 5

(i) Sei $0 \neq M = M[p^\nu]$ ein p^ν-Torsionsmodul;

Sei $x \neq 0$ $x \in M$, dann ist eine Periode für x

(bis auf Einheiten) der Gestalt p^l; mit $l \leq \nu$;

in der Tal sei $l :=$ die kleinste natürliche

Zahl wofür es gelte $p^l x = 0$.

(ii) ist ν minimal dafür daß $M = M[p^\nu]$

so gebt es $x \in M$ mit Periode genau p^ν.

(iii) sei $x_1 \in M$ mit Periode p^ν; setze $\overline{M} := M/_{Rx_1}$

Es ist $\overline{M} = \overline{M}[p^\nu]$ und für jeden

Vertreter y von $\bar{y} \in \overline{M}$ mit Perioden

p^l beziehungsweise $p^{\bar{l}}$

gilt $l \geq \bar{l}$ (ie $p^l \geq p^{\bar{l}}$).

(iv) ist p^ν minimal dafür daß $M = M[p^\nu]$

und p^μ min. dafür daß $\bar{M} = \bar{M}[p^\mu]$

dann gilt $\mu \leq \nu$.

Lemma 3 Sei $p \in R$ prim ; $M = M[p^\nu]$; $\nu \geq 1$

und minimal dafür. Wähle $x_1 \in M$ mit Periode p^ν.

Setze $\bar{M} := M / Rx_1$.

Seien $\bar{y}_1, \dots, \bar{y}_m \in \bar{M}$ unabhängig

Dann gibt es Vertreter $y_i \in \bar{y}_i$

mit Periode y_i = Periode $\bar{y}_i$;

und so daß: $x_1, y_1, \dots, y_m$ unabhängig.

Beweis. Sei $\bar{y} \in \bar{M}$ mit Periode p^n ; $n \geq 1$.

Sei $y \in \bar{y}$ ein Vertreter.
$y \in M$.

Dann ist $p^n \bar{y} = 0$ oder $p^n y \in R x_1$ also

$$p^n y = p^s c \; x_1 \quad (+)$$

für $c \in R$; $p \nmid c$; $s \leq \nu$.
[weil P rim faktorisierung ist in R vorhanden !]

Ist $s = \nu$ dann gilt $p^n y = p^\nu x_1$, $c = 0$

also y hat Periode $\leq p^n$ und damit genau $= p^n$;

und ist der Fall erledigt.

Ist aber $s < \nu$, dann hat $p^s c x_1$ Periode $p^{\nu - s}$

und damit hat y Periode $p^{n+\nu-s}$

also muss $n + \nu - s \leq \nu$ gelten

(weil $p^\nu M = 0$), also $n \leq s$, wir sehen

also daß $y - p^{s-n} c x_1 \in \overline{y}$ [vgl (+)]

und hat Periode p^n.

Fortsetzung vom Beweis folgt in der 7. Vorlesung

am Mo 06. 05. 2013.