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

## 6.Vorlesung

15. Mai 2017

*Beweis vom Satz 5.4.* Betrachte den Homomorphismus:

$$\begin{array}{rccc} \phi: & M & \to & M/M_{\text{tor}} \\ & x & \mapsto & \bar{x} \end{array}$$

Nun ist $M/M_{\text{tor}}$ endlich erzeugt, also ( Satz 5.3) ist er frei.
Lemma 5.5 liefert $F \leq M$, $F$ frei mit $M = \ker(\phi) \bigoplus F$ und $\phi \restriction F : F \cong M/M_{\text{tor}}$, damit ist $\dim_R F = \dim_R M/M_{\text{tor}}$ eindeutig bestimmt. □

Wir werden nun $M_{\text{tor}}$ weiter untersuchen; wir untersuchen also endlich erzeugte Torsionsmoduln.

**Definition und Notation** (a) Für $r \in R$ ist $M[r] := \{x \in M \mid rx = 0\}$ der <u>$r$-Torsionsmodul</u>.

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

**Bemerkung 6.1**
$\{0\} \neq M = M_{\text{tor}}$ endlich erzeugter Torsionsmodul $\Rightarrow \exists a \in R, a \neq 0$ mit $aM = 0$ (Seien $v_1, \ldots, v_n$ Erzeuger, $a_1, \ldots, a_n \in R$ mit $a_i \neq 0$ und $a_i v_i = 0$; setze $a := a_1 \ldots a_n$).

**Lemma 6.1**
Sei $M$ endliche erzeugter Torsionsmodul und wähle $0 \neq a \in R$ mit $aM = 0$ und $a = bc$ mit $ggT(b, c) = 1$. Es ist $M = M[b] \bigoplus M[c]$.

*Beweis.* Es existieren $x, y \in R$ mit $1 = xb + yc$. 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 $v = (xb + yc)v = xbv + ycv = 0$. □

**Satz 6.2**
Sei $0 \neq M$ endlich erzeugter Torsionsmodul. Dann ist

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

**Bemerkung 6.2**
$M$ endlich erzeugt $\Rightarrow |\{p \in R \mid p \text{ prim und } M[p^\infty] \neq 0\}| < \infty$.

*Beweis.* Wähle $a \neq 0$ mit $aM = 0$, $a \in R$. Lemma 6.1 und Induktion anwenden ergibt

$$M = M[a] = \bigoplus_{p|a, p \text{ prim}, M[p^\infty]\neq 0} M[p^\infty]$$

□

**Bemerkung 6.3**
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 $M = M[aq] = M[a] \bigoplus M[q] = M$, also $M[q] = 0$

**Satz 6.3**
Sei $0 \neq M$ endlich erzeugt; $p \in R$ prim mit $M[p^\infty] \neq 0$. Dann existiert eine eindeutige Folge $1 \leq \nu_1 \leq \cdots \leq \nu_s \in \mathbb{N}$, so daß $M[p^\infty] \cong R/ < p^{\nu_1} > \oplus \cdots \oplus R/ < p^{\nu_s} >$.

**Korollar 6.4** (Struktursatz für endlich erzeugte Moduln über HIR)
Sei $R$ ein HIR und $M$ ein $R$-Modul. Ist $M$ endlich erzeugt über $R$, so ist

$$M \cong R^d \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{t_i} R/ < p_i^{\nu_{ij}} >$$

mit eindeutigen $d, s \in \mathbb{N}_0$, $p_1, \ldots, p_s$ paarweise verschiedene Primelemente, $t_s \in \mathbb{N}$ und $1 \leq \nu_{ij} \leq \cdots \leq \nu_{it_s} \in \mathbb{N}$.

□

Für den Beweis vom Satz 6.3 brauchen wir einiges (Terminologie, Bemerkung, Lemma).

Terminologie:

1. $y_1, \ldots, y_m \in M$ sind unabhängig wenn $\mathrm{Span}\{y_1, \ldots, y_m\} \cong \bigoplus_{i=1}^m Ry_i$, oder die folgende äquivalente Bedingung gilt: $a_1y_1 + \cdots + a_my_m = 0 \Rightarrow a_iy_i = 0$ für $a_1, \ldots, a_m \in R$ $\forall i = 1, \ldots, m$.

   **Bemerkung 6.4**
   lineare Unabhängigkeit$\Rightarrow$ Unabhängigkeit immer; die Umkehrung gilt für Torsionsfreie Moduln.

2. Sei $x \in M$, $\begin{array}{cccc} \phi_x : & R & \to & Rx \\ & r & \mapsto & rx \end{array}$; es gelten $I_x := \ker(\phi_x)$ ist Hauptideal und $R/I_x \cong Rx$.
   Ein erzeuger für $I_x$ heißt eine <u>Periode</u> für $x$.

**Bemerkung 6.5** (i) Sei $0 \neq M = M[p^\nu]$ ein $p^\nu$-Torsionsmodul. Sei $x \neq 0$, $x \in M$, dann ist eine Periode für $x$ (bis auf Einheit) der Gestalt $p^l$ mit $l \leq \nu$; in der Tat sei $l :=$ die kleinste natürliche Zahl, wofür es gilt $p^lx = 0$.

(ii) ist $\nu$ minimal dafür, daß $M = M[p^\nu]$, so gibt es $x \in M$ mit Periode genau $p^\nu$.

(iii) Sei $x_1 \in M$ mit Periode $p^\nu$; setze $\overline{M} := M/Rx_1$. Es ist $\overline{M} = \overline{M}[p^\nu]$ und für jeden Vertreter $y$ von $\bar{y} \in \bar{M}$ mit Perioden $p^l$ beziehungsweise $p^{\bar{l}}$ gilt $l \geq \bar{l}$.

(iv) Ist $p^\nu$ minimal dafür, daß $M = M[p^\nu]$ und $p^\mu$ minimal dafür, daß $\bar{M} = \bar{M}[p^\mu]$, dann gilt $\mu \leq \nu$.

**Lemma 6.5**
Sei $p \in R$ prim, $M = M[p^\nu]$, $\nu \geq 1$ und minimal dafür. Wähle $x_1 \in M$ mit Periode $p^\nu$. Setze $\overline{M} := M/Rx_1$. Seien $\bar{y}_1, \ldots, \bar{y}_m \in \overline{M}$ unabhängig. Dann gibt es Vertreter $y_i \in \bar{y}_i$ mit Periode($y_i$)=Periode($\bar{y}_i$) und so daß $x_1, y_1, \ldots, y_m$ unabhängig.

*Beweis.* Sei $\bar{y} \in \bar{M}$ mit Periode $p^n$, $1 \leq n$. Sei $y \in \bar{y}$ ein Verterter. Dann ist $p^n\bar{y} = 0$ oder $p^ny \in Rx_1$, also

$$p^ny = p^scx_1 \tag{†}$$

für $c \in R, p \nmid c, s \leq \nu$ (weil Primfaktorisierung in $R$ vorhanden ist). Ist $s = \nu$, dann gilt $p^ny = p^\nu x_1c = 0$, also $y$ hat Periode $\leq p^n$ und damit genau $= p^n$, und so ist der Fall erledigt.
Is aber $s < \nu$, dann hat $p^scx_1$ 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 $y - p^{s-n}cx_1 \in \bar{y}$ (vgl (†)) und hat Periode $p^n$.
Fortsetzung vom Beweis folgt in der 7. Vorlesung. □