Vorlesung 8 (11.11.16)

3.5. Endlich erzeugte Moduln

In diesem Abschnitt einige Spezialitäten für endlich erzeugte Moduln, die für unendlich erzeugte Moduln im Allgemeinen falsch sind.

Lemma[1]: Ist V ein endlich erzeugter A-Modul, so ist jeder echte Untermodul in einem maximalen Untermodul enthalten. Ist $V \neq 0$, so besitzt V insbesondere einen maximalen Untermodul.

Beweis: Sei $\{v_1, \ldots, v_n\}$ Erzeugendensystem von V und $U \subsetneq V$ Untermodul. Sei Σ die Menge aller echten Untermoduln, die U enthalten. Es ist $U \in \Sigma$, also $\Sigma \neq \emptyset$. Sei $(W_\lambda)_{\lambda \in \Lambda}$ Kette in Σ. Dann ist

$$W := \bigcup_{\lambda \in \Lambda} W_\lambda$$

ein Untermodul von V. Angenommen, $V = W$. Für jedes $i = 1, \ldots, n$ gibt es dann λ_i mit $v_i \in W_{\lambda_i}$. Sei W_λ der größte der W_{λ_i} (geht, da Kette). Dann ist $v_1, \ldots, v_n \in W_\lambda \Rightarrow V = W_\lambda$ $\lightning$ zu $W_\lambda \in \Sigma$ und damit echter Untermodul. Also ist $W \subsetneq V$ und damit $W \in \Sigma$. Aussage folgt nun aus Zorns Lemma. $\square$

Bem[2]: Für unendlich erzeugte Moduln muss das nicht stimmen, z.B. hat $\mathbb{Q}$ als $\mathbb{Z}$-Modul keinen maximalen Untermodul (siehe Übung).

Lemma (Cayley-Hamilton)[3] Sei V ein endlich erzeugter A-Modul, der von n Elementen erzeugt werden kann. Sei $I \trianglelefteq A$ ein Ideal und $f \in \mathrm{End}_A(V) = \mathrm{Hom}_A(V,V)$ mit $f(V) \subseteq IV$. Dann gibt es monisches Polynom

$$p = X^n + a_1 X^{n-1} + \ldots + a_n \in A[X]$$

mit
$$0 = p(f) = f^n + a_1 f^{n-1} + \dots + a_n = 0.$$

Es ist weiterhin $a_i \in I^i$.

<u>Beweis</u>: Seien $v_1, \dots, v_n$ Erzeuger von V. Können dann schreiben

$$(1) \qquad f(v_i) = \sum_{j=1}^{n} a_{ij} v_j$$

für gewisse $a_{ij} \in I$. Sei $M := (a_{ij}) \in Mat_n(A)$ und $v := (v_1, \dots, v_n) \in V^n$.
Können V als $A[X]$-Modul betrachten, sodass X über f operiert, d.h. $Xw := f(w)$ für $w \in V$. Aus (1) folgt dann

$$\underbrace{(X 1_n - M)}_{n \times n \text{ Matrix über } A[X]} \cdot v = 0$$

Multiplikation mit der adjunkten Matrix von $X1_n - M$ ergibt

$$\underbrace{\det(X 1_n - M)}_{=: p(X) \in A[X]} \cdot v = 0,$$

d.h. $p(X) v_i = 0$ für alle i, d.h. $p(f) = 0$ da X über f operiert.
Das Polynom ist monisch (d.h. Leitkoeffizient 1 und der Koeffizient a_i von X^0 ist in I^i enthalten). $\square$

<u>Korollar</u>[4]: Sei V endlich erzeugter A-Modul und $I \trianglelefteq A$ Ideal mit $IV = V$. Dann gibt es $a \in A$ mit $a \equiv 1 \mod I$ und $aV = 0$.

<u>Beweis</u>: Sei $f = id_V \in End_A(V)$. Nach Cayley-Hamilton gibt es dann

$p = X^n + a_1 X^{n-1} + \ldots + a_n \in A[X]$ mit $p(f) = 0$ und $a_i \in I$ $\forall i$.
Sei $a := 1 + a_1 + \ldots + a_n$. Dann gilt $a \equiv 1 \bmod I$ und $aV = 0$. $\square$

<u>Korollar[5] (Nakayamas Lemma)</u> Sei V endlich erzeugter A-Modul und $I \trianglelefteq A$ ein Ideal mit $I \subseteq \mathrm{Jac}(A)$. Ist $IV = V$, so gilt $V = 0$. $\square$

<u>Beweis:</u> Nach Korollar 3.5.4 gibt es $a \in A$ mit $a \equiv 1 \bmod I$ und $aV = 0$. Da $1 - a \in I \subseteq \mathrm{Jac}\, A$, folgt mit Lemma 2.4.5, dass $a \in A^\times$. Wegen $aV = 0$, muss dann aber $V = 0$ sein. $\square$

<u>Korollar[6]:</u> Sei V endlich erzeugter A-Modul, $U \subseteq V$ Untermodul und $I \trianglelefteq A$ mit $I \subseteq \mathrm{Jac}\, A$. Gilt $V = IV + U$, so muss bereits $U = V$ sein.

<u>Beweis:</u> $V = IV + U \Rightarrow V/U = I(V/U)$. Also $V/U = 0 \Rightarrow V = U$ mit Nakayama's Lemma. $\square$

<u>Korollar[7]:</u> Sei A ein lokaler Ring mit maximalem Ideal M. Sei $K := A/M$. Sei V ein endlich erzeugter A-Modul und $v_1, \ldots, v_n \in V$, sodass $\overline{v}_1, \ldots, \overline{v}_n \in V/MV$ eine K-Basis sind. Dann erzeugen $v_1, \ldots, v_n$ bereits V und bilden minimales Erzeugendensystem.

<u>Beweis:</u> Sei $U := A\{v_1, \ldots, v_n\} \subseteq V$. Nach Annahme ist $(U + MV)/MV = V/MV$, also $U + MV = V$. Das Korollar 3.5.6 impliziert nun $U = V$.
Minimalität folgt, da Vektorraumbasis minimal. $\square$

<u>Korollar[8]:</u> Sei V endlich erzeugter A-Modul und $f: V \to V$ A-Modulmorphismus. Ist f surjektiv, so ist f bereits bijektiv.

<u>Beweis:</u> Betrachte V als $A[X]$-Modul, sodass X über f operiert.

Sei $I := (X) \trianglelefteq A[X]$. Da f surjektiv, gilt $IV = V$.
Cayley-Hamilton angewandt auf den $A[X]$-Modulmorphismus $id_V : V \to V$ gibt Polynom

$$p = Y^n + a_1 Y^{n-1} + \dots + a_n \in (A[X])[Y], \quad \underline{a_i \in I}$$

mit $p(id_V) = 0$, d.h.

$$0 = id_V^n + a_1 id_V^{n-1} + \dots + a_n = id_V + a_1 id + \dots + a_n.$$

Da $a_i \in I = (X)$, gibt es $a_1', \dots, a_n' \in A[X]$ mit $a_i' X = a_i$. Sei

$$q := -(a_1' + \dots + a_n')$$

Dann gilt

$$0 = (1 - qX)v, \text{ d.h. } v = (qX)v \quad \forall v \in V.$$

$$\overset{X \text{ operiert über } f}{\Longrightarrow} \quad 0 = 1 - \underbrace{q(f)}_{\in End_A(V)} f \Rightarrow q(f) f = 1$$

$\Rightarrow f$ hat Umkehrabbildung $q(f)$. $\square$

<u>Korollar</u>: Sei V endlich erzeugter freier A-Modul und $n := rk V$. Dann ist jedes Erzeugendensystem aus n Elementen bereits eine Basis von V.

<u>Beweis</u>: Seien $v_1, \dots, v_n$ Erzeuger. Das definiert surjektiven A-Modulmorphismus $A^n \xrightarrow{f} V$. Da V frei vom Rang n gibt es Isomorphismus $V \xrightarrow{g} A^n$. Wir erhalten also einen surjektiven Morphismus $A^n \to A^n$. Nach Korollar 3.5.8 ist dies bereits Isomorphismus. Dann ist aber auch $f = (fg)g^{-1}$ ein Isomorphismus und damit $(v_1, \dots, v_n)$ Basis $\square$