§ 6. Anwendungen: abelsche Gruppen und Matrizen

Wir wenden die Ergebnisse von § 5 in zwei Situationen an:
$R = \mathbb{Z}$ und $R = K[x]$ (K ein Körper).

$\boxed{\text{Zuerst } R = \mathbb{Z}.}$ $\mathbb{Z}$-Moduln sind abelsche Gruppen (und umgekehrt).
Endlich erzeugte (= noethersche) $\mathbb{Z}$-Moduln sind endlich erzeugte abelsche Gruppen.
$\mathbb{Z}$ ist eine freie abelsche Gruppe, $\mathbb{Z}^n$ auch für jedes $n \in \mathbb{N}$, vom Rang n.
Jede Untergruppe einer freien abelschen Gruppe vom Rang n ist selbst frei abelsch, vom Rang $r \leq n$. Was bedeutet das für $\mathbb{Z}$?
Jede endlich erzeugte abelsche Gruppe ist Quotient einer freien abelschen Gruppe, vom Rang $n \in \mathbb{N}$.
Die Sätze 5.16 und 5.20 (zusammen mit Korollar 5.17) liefern die Klassifikation:

<u>6.1 Theorem</u> (Hauptsatz über endlich erzeugte abelsche Gruppen):
Sei G eine endlich erzeugte abelsche Gruppe. Dann gilt:

(a) $G \cong \mathbb{Z}^n \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/d_k\mathbb{Z}$ mit $1 < d_1 | d_2 | \dots | d_k$, wobei $n, d_1, \dots, d_k$ eindeutig bestimmt sind.

(b) $G \cong \mathbb{Z}^n \oplus \mathbb{Z}/p_1^{n_1}\mathbb{Z} \oplus \mathbb{Z}/p_2^{n_2}\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/p_l^{n_l}\mathbb{Z}$ mit Primzahlen $p_1, \dots, p_l$, wobei $n, p_1, \dots, p_l, n_1, \dots, n_l$ eindeutig bestimmt sind.

Die endlichen abelschen Gruppen sind Torsion, d.h. sie haben keinen freien Summanden, und die Torsionsuntergruppen der endlich erzeugten abelschen Gruppen sind endlich.

Wie sehen die beiden Zerlegungen aus für $\mathbb{Z}/24\mathbb{Z}$, $\mathbb{Z}/240\mathbb{Z}$, $\mathbb{Z}/24\mathbb{Z} \oplus \mathbb{Z}/240\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/27\mathbb{Z}$?

Damit sind insbesondere die endlich abelschen Gruppen bestimmt.

Jetzt: kein Körper, $\boxed{R = K[x]}$. Die Klassifikation der Moduln sieht natürlich analog aus, aber was bedeutet sie?

Erinnerung: ein $K[x]$-Modul M ist ein K-Vektorraum M zusammen mit einem Endomorphismus $\varphi \in \mathrm{End}_K(M)$ und: $\underset{\substack{\cap \\ M}}{x \cdot m} = \varphi(m)$

(M, φ) und (M', ψ) sind als $K[x]$-Moduln isomorph $\Leftrightarrow$ $\exists$ Vektorraumisomorphismus $\alpha: M \xrightarrow{\sim} M'$ so daß

$$\begin{array}{ccc} M & \xrightarrow{\alpha} & M' \\ \varphi \downarrow & & \downarrow \psi \\ M & \xrightarrow{\alpha} & M' \end{array}$$

$\psi \circ \alpha = \alpha \circ \varphi$, d.h. $\varphi = \alpha^{-1} \circ \psi \circ \alpha$, d.h. φ und ψ sind ähnlich

(oder in Basen: $M = M'$, α bedeutet Basiswechsel, dann sind die darstellenden Matrizen von φ und von ψ zueinander ähnlich)

Um mit linearer Algebra zu vergleichen, wählen wir einen K-Vektorraum M mit $\dim M < \infty$ und $\varphi \in \mathrm{End}_K(M)$, also einen $K[x]$-Torsionsmodul).

M zerfällt in eine direkte Summe von Moduln der Form

$K[x]/\langle f_i(x) \rangle$ mit $f_i \neq 0$ und o.B.d.A. normiert, nicht konstant

Sei $f_i = f$ (fest sei), $f(x) = x^n + \sum_{i=0}^{n-1} a_i x^i$, $a_i \in K$, $n > 0$, V der Summand von M

<u>6.2 Proposition:</u> Ein $K[x]$-Modul ist genau dann isomorph zu $K[x]/\langle f(x) \rangle$ wenn der zugrundeliegende Vektorraum V eine Basis besitzt, bezüglich derer die zu $x + \langle f(x) \rangle$ gehörende ~~k~~ lineare Abbildung die darstellende Matrix

$$\mu(f) = \begin{pmatrix} 0 & \cdots & 0 & -a_0 \\ 1 & 0 \cdots & 0 & -a_1 \\ 0 & 1 \; 0 \cdots & 0 & -a_2 \\ \vdots & & & \vdots \\ 0 & 0 \cdots & 0 & -a_{n-2} \\ 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}_{n \times n}$$ hat.

erinnern Sie sich?

($\mu(f)$ heißt die <u>Begleitmatrix</u> von f)

Die beiden Hauptergebnisse aus Kapitel 5 liefern daher zwei Normalformen für lineare Abbildungen (genauer: Endomorphismen):

6.3 Theorem: Sei M ein endlich-dimensionaler K-Vektorraum und $\varphi \in \mathrm{End}_K(M)$. Dann gibt es ~~fin~~ normierte Polynome $f_1, f_2, \dots, f_r \in K[X]$, so daß φ bezüglich einer geeigneten Basis die Form

$$\begin{pmatrix} \mu(f_1) & 0 & \cdots & 0 \\ 0 & \mu(f_2) & & \vdots \\ \vdots & & \ddots & \\ 0 & \cdots & 0 & \mu(f_r) \end{pmatrix}$$

hat und $\underbrace{f_1 | f_2 | \dots | f_r}$ (die Elementarteiler von φ).

Außerdem gibt es normierte Polynome $g_1, \dots, g_s \in K[X]$, jedes Potenz eines irreduziblen Polynoms, so daß φ bezüglich einer geeigneten Basis die Form

$$\begin{pmatrix} \mu(g_1) & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \mu(g_s) \end{pmatrix}$$

hat.

Assoziiertenklassen irred. Elemente

Spezialfall: $K = \bar{K}$. Dann können wir $\mathcal{P} = \{(X-a) \mid a \in K\}$ wählen.

Der $(X-a)$-Torsionsuntermodul von M ist also $\quad a \cdot \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$

$$T_{X-a}(M) = \{ m \in M : \exists n \in \mathbb{N} \text{ mit } (\varphi - a\,\mathrm{id})^n(m) = 0 \},$$

der verallgemeinerte Eigenraum von φ zum Eigenwert a.

M ist also die direkte Summe der verallgemeinerten Eigenräume.

Mit einer Basis $(X-a)^{n-1} + \langle f \rangle, (X-a)^{n-2} + \langle f \rangle, \dots, X-a + \langle f \rangle, 1 + \langle f \rangle$ von $K[X]/\langle f \rangle$

erhalten wir eine Blockmatrix der Form

$$\mu(a,n) = \begin{pmatrix} a & 1 & \cdots & 0 \\ 0 & \ddots & \ddots & \\ \vdots & & \ddots & 1 \\ 0 & \cdots & 0 & a \end{pmatrix}$$

und durch Zusammensetzen der Blöcke die Jordan-Normalform.

Theorem 6.3 bietet uns also zwei verschiedene Normalformen von Matrizen an bzw. zwei verschiedene Repräsentantensystem für die ~~Äq~~ Ähnlichkeitsklassen quadratischer Matrizen.
Die erste ~~1.~~ Form (mit den Elementarteilern) wird rationale Normalform (rational canonical form) oder Frobenius-~~Kom~~-Normalform genannt, die zweite Weierstraß-Normalform. Diese Bezeichnungen sind aber nicht eindeutig.
Zyklische Zerlegung bzw. Primärzerlegung des Moduls lässt eher an der richtige denken (und wird in der kommutativen Algebra verwendet).

Warum gibt es mehrere Normalformen?
Schon bei den abelschen Gruppen sehen wir, daß es schwierig ist, sich für eine Normalform zu entscheiden: Was ist normaler: $\mathbb{Z}/6\mathbb{Z}$ oder $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$?
Die erste Normalform in 6.3 liefert weniger Blöcke, in aufsteigender Größe.
Die zweite Normalform liefert mehr Blöcke und mehr kleinere.
Die erste Normalform ändert sich nicht, wenn man K durch einen größeren Körper ersetzt.
Die zweite Normalform hängt von K ab, weil Polynome über einem größeren Körper nicht mehr irreduzibel sein müssen.

Beispiel: $A = \begin{pmatrix} 0 & 3 & 1 \\ 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix} \in \mathrm{Mat}(\mathbb{Q}, 3\times 3)$, $\chi_A = X^3 - 3X - 2 = (X-2)(X+1)^2$

$\rightsquigarrow$ Normalformen: $\begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 3 \\ 0 & 1 & 0 \end{pmatrix}$

$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & -2 \end{pmatrix}$

$\begin{pmatrix} 2 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 1 & -1 \end{pmatrix}$