9. Der Elementarteilersatz

Beispiel: $R=\mathbb{Z},\ R^*=\{1,-1\}$ Einheitengruppe

$$M=\begin{pmatrix}27&12&24\\39&18&36\\30&24&30\end{pmatrix}\in R^{3\times 3}\to\begin{pmatrix}3&12&0\\3&18&0\\-18&24&-18\end{pmatrix}\to\begin{pmatrix}3&12&0\\0&6&0\\0&96&-18\end{pmatrix}$$

$$\to\begin{pmatrix}3&0&0\\0&6&0\\0&96&-18\end{pmatrix}\to\begin{pmatrix}3&0&0\\0&6&0\\0&0&18\end{pmatrix}$$

Erlaubte Umforumgen:

U1: Addiere ein λ-faches einer Zeile (Spalte) zu einer anderen $(\lambda\in\mathbb{R})$

U2: Vertausche Zeilen (Spalten)

U3: Multipliziere eine Zeile (Spalte) mit $\lambda\in R^*$

9.1. Elementarteilersatz

Sei $M\in\mathbb{R}^{n\times n}$

Durch U1, U2, U3 kann M auf Diagonalgestalt M' gebracht werden:

$$M'=\begin{pmatrix}d_1&&&&&0\\&\ddots&&&&\\&&d_r&&&\\&&&0&&\\&&&&\ddots&\\0&&&&&0\end{pmatrix}$$

$0\neq d_i$

d_i teilt d_{i+1} $\qquad i=1,\dots,r-1$

Die Zahlen d_i heißen **Elementarteiler** von M

? PROBLEM: Sind die d_i eindeutig ?

Der Elementarteilersatz gilt für $R\in\{\mathbb{Z},K[K],\text{euklidischer Ring }\mathbb{Z}[.],\text{Hauptidealring}\}$

> Hauptidealring: R kommutativ, nullteilerfrei
> I Ideal von $R\Rightarrow\exists a\in R$ mit $I=\langle a\rangle$

$$\text{U1:}\quad M \to \underbrace{\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & \cdots\lambda & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}}_{E_\lambda} M$$

Elementarmatrix

$M \to E_\lambda M$ Addiere das λ-fache der j-ten Zeile zur i-ten Zeile

$M \to ME_\lambda$ Addiere das λ-fache der j-ten Zeile zur i-ten Zeile

$$\text{U2:}\quad M \to \begin{pmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & 1 & & & & & & \\ & & & 0 & & & & & \\ & & & & 1 & & & & \\ & & & & & \ddots & & & \\ & & & & & & 1 & & \\ & & & & & & & 0 & \\ & & & & & & & & 1 \\ & & & & & & & & & \ddots \end{pmatrix} M$$

Permutationsmatrix P_i

Elementarmatrix

$$\text{U3:}\quad M \to \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & \lambda & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} M$$

$M \to MS_\lambda$ Elementarmatrix

$\mathbb{Z} \in \mathbb{Q}$

$R \leq \operatorname{quad}(R) =: \mathbb{Q}$

Zum Beispiel: $\operatorname{quad}(K[X]) : \left\{ \frac{A(X)}{B(X)} \middle| B \neq C \right\}$

$R^{n\times n} \subseteq Q^{n\times n}$

$\not\subset$ L.S.

$A \to \det A \in R$

$\det A \neq 0 \;\Rightarrow\; A^{-1}$ existiert in $Q^{n\times n}$

9.2. a) Sei $A \in \mathbb{R}^{n\times n}$

$A^{-1} \in \mathbb{R}^{n\times n} \Leftrightarrow \det A \in R^*$

b) Die Elemntarmatrizen sind in R invertierbar

Beweis: a) $"\Rightarrow"$

$$A^{-1} = (\det A)^{-1} \underbrace{A^{adj.}}_{\in R^{n\times n}}$$

$$\text{Beispiel: } A = \begin{pmatrix} 2 & 1 \\ 3 & 5 \end{pmatrix} \to A^{-1} = \frac{1}{7}\begin{pmatrix} 5 & -1 \\ -3 & 2 \end{pmatrix}$$

$$A^{-1} \in R^{n\times n} \Rightarrow \det A^{-1} = (\det A)^{-1} \in R$$

$$\Rightarrow \det A \in R^*$$

$"\Leftarrow"$

$$\det A \in R^* \overset{\text{s.o.}}{\Rightarrow} A^{-1} \in R^{n\times n}$$

9.3. Korollar

Zu $M \in R^{n\times n}$ existieren über R invertierbare Matrizen $B, C \in R^{n\times n}$ mit $M' = BMC$

Lineare Algebra $A \in K^{n\times n}, R = K[X]$

$$M := \begin{pmatrix} a_{11}X & a_{12}\cdots & a_{1n} \\ a_{21} & a_{22}X & a_{2n} \\ \vdots & \ddots & \\ a_{n1} & \cdots & a_{nn}X \end{pmatrix} = A - \operatorname{diag}(X,\ldots,X) = A - X\mathbb{1}_n \in R^{n\times n}$$

Charakteristisches Polynom $\operatorname{char} A = \det(A - X\mathbb{1}_n)$

9.4. Seien $d_1,\ldots,d_r$ die Elemntarteoöer der Matrizen M.

Dann gilt: $\operatorname{char} A = d_1 \cdot d_2 \cdots d_r$ (bis auf eine Normierung)

Beweis: $M' = BMC$, $B, C \in R^{n\times n}$ invertierbar in R

$$\det M' = \det BMC = \underbrace{\det B}_{\in R^*} \cdot \det M \cdot \underbrace{\det C}_{\in R^*}$$

$$(R \in K[X],\ R^* = K^*)$$

R kommutativer, nullteilerfreier Ring und $Q = \text{quad}\, R$

Definitionen und Bemerkungen:

Eine abelsche Gruppe $V = V(+)$ heißt ***R*-Modul**, wenn jedem $\lambda \in R, v \in V$ ein Element $\lambda v \in V$ zugeordnet ist, so dass

$$(\lambda + \mu)v = \lambda v + \mu v$$
$$\lambda(\mu v) = (\lambda\mu)v$$
$$1v = v$$

(Wenn R Körper, dann ist Modul = Vektorraum)

Beispiele:

1) Sei $V = V(+)$ abelsche Gruppe und $R = \mathbb{Z}$

$i \in \mathbb{N}: \quad iv = \underbrace{v + \ldots + v}_{i-\text{mal}}$

$(-i)v := -(iv) \qquad (0 \cdot i = 0)$

Potenzgesetze: $(i + j)v = iv + jv$

$i(jv) = (ij)v$

$\Rightarrow \quad V$ ist $\mathbb{Z}$-Modul

2) Sei V Vektorraum über dem Körper K und $\varphi : V \to V$ lin.Abb.

$A = A(X) = a_0 + a_1 X + \ldots + a_n X^n \in \underbrace{K[X]}_{R}$

$v \in V, \; Av := a_0 v + a_1\varphi(v) + a_2\varphi^2(v) + \ldots + a_n\varphi^n(v) = (A(\varphi))(v)$

Einsetzungsregel:

$(A+B)(\varphi) = A(\varphi) + B(\varphi) \quad \Rightarrow (A+B)v = Av + Bv$

$(AB)(\varphi) = A(\varphi)B(\varphi) \quad \Rightarrow (AB)(v) = A(B(v))$

V ist ein $K[X]$-Modul via φ

$\underbrace{A(\varphi)}_{a_0\,\text{id} + a_1\varphi + \ldots + a_n\varphi^n} \; : \; V \to V \;\; \text{lin.Abb.}$

$v \mapsto (A(\varphi))(v) = a_0 v + a_1\varphi(v) + \ldots + a_n\varphi^n(v)$

3) Man mache den Ring R zum R-Modul

$V = R(+)$

λv ist das Produkt von λv in R

$\Rightarrow V$ ist R-Modul, $\quad V = R$

4) $R^n = \{(r_1, r_2, ..., r_n) | r_i \in R\}$ ist R-Modul: Alles komponentenweise
$\lambda(r_1, ..., r_n) = (\lambda r_1, ..., \lambda r_n)$

Definitionen und Bezeichnungen:

Sei V R-Modul

1) Eine Untergruppe U von der additiven Gruppe $V(+)$ heißt **Untermodul**, wenn
$u \in U,\ \lambda \in R \ \Rightarrow\ \lambda u \in U$
$\Rightarrow U$ ist R-Modul
U_1, U_2 Untermodul von $V \Rightarrow U_1 \cap U_2$ und $U_1 + U_2 = \{u_1 + u_2 | u_i \in U_i\}$ sind Untermodul

Beispiel:
Sei $V = R$, U Untermodul
$v \in U,\ \lambda \in R \ \Rightarrow\ \lambda u \in U$ Untermodul $=$ Ideal

Sei U Untermodul
Die Faktorgruppe V/U ist R-Modul bzgl. $\lambda(v+U) \overset{\text{def.}}{=} \lambda v + U$

2) Sei $v_1, ..., v_n \in V$
$\langle v_1, ..., v_n \rangle \overset{\text{def.}}{=} \left\{ \sum_{i=1}^{n} \lambda_i v_i \middle| \lambda_i \in R \right\}$ $(= \mathrm{span}(v_1, ..., v_m) = \text{Lineare Hülle})$
$\langle v_1, ..., v_m \rangle$ ist der kleinste Untermodul von V, der $v_1, ..., v_m$ enthält
V heißt **endlich erzeugt**, wenn $v_1, ..., v_n$ existieren mit $V = \langle v_1, ..., v_n \rangle$

Beispiel:
$V = R^n$
$e_i = (0, ..., 0, \underset{i}{1}, 0, ..., 0)$ $i = 1, ..., n$
$V = \langle e_1, ..., e_n \rangle$