Das Minimalpolynom

Sei V $\mathbb{K}$-Vektorraum, $\mathcal{A} : V \to V$ eine lineare Abbildung, also $\mathcal{A}$ ein (Vektorraum-)Endomorphismus, $\mathcal{A} \in \mathrm{End}(V)$, und $A \in \mathbb{K}^{n\times n}$ eine Matrix(darstellung von $\mathcal{A}$).

Ideale:

Sei R kommutativer Ring, dann ist $\mathcal{I} \subset R$ Ideal, wenn gilt:

(I1) $p, q \in \mathcal{I} \Longrightarrow p - q \in \mathcal{I}$.

(I2) $p \in \mathcal{I}$, $q \in R \Longrightarrow q \cdot p \in \mathcal{I}$.

Ein Ideal heißt **Hauptideal**, falls $\exists a \in R$, so daß

$$\mathcal{I} = a \cdot R \equiv \{a \cdot r \,|\, r \in R\}.$$

Einsetzungshomomorphismus:

$$\Phi_{\mathcal{A}} : \mathbb{K}[x] \to \mathrm{End}(V) \;:\; p(x) \to p(\mathcal{A}),$$

wobei für $p(x) = a_0 + a_1 x + \ldots + a_k x^k$ der Endomorphismus $p(\mathcal{A})$ durch

$$p(\mathcal{A})(v) = a_0 \mathrm{Id}_V(v) + a_1 \mathcal{A}(v) + \ldots + a_k \mathcal{A}^k(v)$$

mit $\mathcal{A}^k(v) = (\underbrace{\mathcal{A} \circ \ldots \circ \mathcal{A}}_{k\text{-mal}})(v)$ definiert ist.

Beachte:

- $\Phi_{\mathcal{A}}$ ist ein Ring- und Vektorraumhomomorphismus.
- $\mathbb{K}[\mathcal{A}] \equiv \mathrm{Bild}(\Phi_{\mathcal{A}})$ ist kommutativer Unterring von $\mathrm{End}(V)$.
- $\mathcal{I}_{\mathcal{A}} \equiv \mathrm{Kern}(\Phi_{\mathcal{A}})$ ist ein Ideal in $\mathbb{K}[x]$.
- $p_{\mathcal{A}} \in \mathcal{I}_{\mathcal{A}}$.

Minimalpolynom:

In jedem Ideal $\{0\} \neq \mathcal{I} \subset \mathbb{K}[x]$ existiert ein eindeutiges Polynom $m(x)$ mit den Eigenschaften

(i) m ist **normiert**, d.h. $m(x) = x^d + \gamma_{d-1}x^{d-1} + \ldots + \gamma_1 x + \gamma_0$.

(ii) $\forall p \in \mathcal{I}$ existiert $q \in \mathbb{K}[x]$, so daß $p = q \cdot m$, d.h. m ist **minimal** (m hat minimalen Grad aller Polynome in $\mathcal{I} \setminus \{0\}$).

Ist $\mathcal{I} = \mathcal{I}_{\mathcal{A}}$, dann heißt $m \equiv m_{\mathcal{A}}$ das Minimalpolynom von $\mathcal{A}$.

Beachte:

a) $m_{\mathcal{A}}$ teilt $p_{\mathcal{A}}$.

b) $p_{\mathcal{A}}$ teilt $m_{\mathcal{A}}^n$.

Daraus folgt z.B., daß $m_{\mathcal{A}} = p_{\mathcal{A}}$, falls $\mathcal{A}$ n verschiedene Eigenwerte besitzt.