Themen dieser Woche

Wir betrachten folgende Themen:

- Polynomringe, insbesondere Teilbarkeit und Ideale
- Primfaktorzerlegung von Polynomen
- das Minimalpolynom
- (Satz von Cayley-Hamilton)
- die Hauptraumzerlegung
- nilpotente Matrizen
- Jordansche Normalform

Themen nächster Woche

- Bilinearformen und quadratische Formen
- Skalarprodukte und euklidische/hermitesche Vektorräume
- orthogonale/hermitesche Matrizen und Abbildungen

Der Polynomring über einem Körper

Definition Ein *Ring* R ist eine Menge R mit einer

- Addition, bezüglich derer R eine abelsche Gruppe wird,
- Multiplikation, die assoziativ und distributiv (bzgl. Addition) ist und für die es ein neutrales Element 1_R gibt.

Ein Ring R heißt *kommutativ*, falls die Multiplikation kommutativ ist.

Beispiele

- $\mathbb{Z}$ und jeder Körper $\mathbb{K}$ sind kommutative Ringe
- Die Menge $\mathbb{K}^{n\times n}$ der $n \times n$-Matrizen über einem Körper $\mathbb{K}$
- Die Menge $\mathrm{End}(V)$ der Endomorphismen eines $\mathbb{K}$-Vektorraums
- Der *Polynomring* $\mathbb{K}[X]$ über einem Körper $\mathbb{K}$ ist die Menge aller Folgen $(a_0, a_1, \ldots)$ in $\mathbb{K}$, die irgendwann Null werden, mit
$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots, a_n + b_n, \ldots)$$
$$(a_0, a_1, \ldots) \cdot (b_0, b_1, \ldots) = (a_0 b_0, a_0 b_1 + a_1 b_0, \ldots, \textstyle\sum_{k=0}^{n} a_k b_{n-k}, \ldots)$$
man schreibt die Elemente (Polynome) $(a_0, a_1, \ldots)$ als $\sum_k a_k X^k$

Ringhomomorphismen

Definition Ein *Homomorphismus* zwischen Ringen R, S ist eine Abb. $f: R \to S$ mit $f(x+y) = f(x) + f(y)$ und $f(x \cdot y) = f(x) \cdot f(y)$

Beispiele

- die Abbildung $\mathrm{End}(V) \to \mathbb{K}^{n\times n}$, gegeben durch $f \mapsto {}_B[f]_B$, wobei V ein n-dimensionaler $\mathbb{K}$-VR mit Basis B ist
- die *Polynom-Auswertung* an $\lambda \in \mathbb{K}$ als Abb. $\mathrm{ev}_\lambda: \mathbb{K}[X] \to K$ mit $p = \sum_k a_k X^k \mapsto \sum_k a_k \lambda^k =: p(\lambda)$

Beispiel Für jedes $A \in \mathbb{K}^{n\times n}$ erhalten wir einen Homomorphismus

$$\mathrm{ev}_A: \mathbb{K}[X] \to \mathbb{K}^{n\times n}, \quad p = \sum_k a_k X^k \mapsto \sum_k a_k A^k =: p(A).$$

Analog: $\mathrm{ev}_f: \mathbb{K}[X] \to \mathrm{End}(V)$ für $f \in \mathrm{End}(V)$.

Minimalpolynom und Teilbarkeit in Polynomringen

Definition Das *Minimalpolynom* μ_A einer Matrix $A \in \mathbb{K}^{n\times n}$ ist das Polynom p kleinsten Grades mit Leitkoeffizient 1 mit $p(A) = 0$

Satz 1 μ_A teilt jedes andere $q \in \mathbb{K}[X]$, welches $q(A) = 0$ erfüllt.

Der Beweis benutzt:

Satz 2 (*Polynomdivison mit Rest*) Für alle $p, q \in \mathbb{K}[X]$ mit $p \neq 0$ gibt es $r, d \in K[X]$ mit $q = p \cdot d + r$ und $\mathrm{Grad}(r) < \mathrm{Grad}(p)$.

Beweis Induktion über $\mathrm{Grad}\, q$. □

Beweis von 2 Seien $q(A) = 0$, $p = \mu_A$ und r, d wie oben. Dann folgt $r(A) = 0$ und wegen Minimalität von μ_A folgt $r = 0$. □

Definition Ein kommutativer, nullteilerfreier Ring R heißt *euklidisch*, wenn es eine Abbildung $\deg: R \setminus \{0\} \to \mathbb{N}$ gibt mit

- $\deg(xy) \geq \deg(x)$ für alle $x, y \in R$
- für alle $x, y \in R$, $x \neq 0$ gibt es $d, r \in R$ mit $y = dx + r$ und $r = 0$ oder $\deg(r) < \deg(x)$.

Algebraischer Hintergrund: Hauptidealringe

Definition Eine Teilmenge I eines Ringes R heißt *Ideal*, falls $x + y \in I$ für alle $x, y \in I$ und $rx, xr \in I$ für alle $x \in I$, $r \in R$.

Beispiele

- für jeden Homomorphismus $f\colon R \to S$ der Kern $\ker f = f^{-1}(0)$, denn aus $f(x) = f(y) = 0$ folgt $f(x + y) = f(xr) = f(rx) = 0$
- für jedes $A \in \mathbb{K}^{n\times n}$ die Menge $\{q \in \mathbb{K}[X] : q(A) = 0\} = \ker \mathrm{ev}_A$
- für jeden Ring R, jedes $a \in R$ die Menge $(a) = \{xay : x, y \in R\}$, das *von a erzeugte Hauptideal*

Satz Jeder *euklidischer Ring* (wie z.B. $\mathbb{K}[X]$) ist ein *Hauptidealring*.
Beweis Sei I ein Ideal. Wähle $a \in I \setminus \{0\}$ mit $\deg(a)$ minimal.
Klar: $(a) \subseteq I$.
Jedes $b \in I$ hat die Form $b = da + r$ mit $r = 0$ oder $\deg(r) < \deg(a)$.
Aus $b \in I$ und $a \in I$ folgt $r = b - da \in I$. Nach Wahl von a ist $\deg(r) < \deg(a)$ nicht möglich, also $r = 0$ und $b = da \in (a)$.

Primfaktorzerlegung des Minimalpolynoms

Fundamentalsatz der Algebra In $\mathbb{C}[X]$ zerfällt jedes Polynom p als Produkt von Linearfaktoren:

$$p = (X - \lambda_1)^{r_1} \cdots (X - \lambda_k)^{r_k}$$

Definition Ein Polynom $p \in \mathbb{K}[X]$ heißt *reduzibel*, wenn es echte Teiler hat, ansonsten *irreduzibel*. Ein Körper $\mathbb{K}$ heißt algebraisch abgeschlossen, wenn jedes irreduzible Polynom Grad 1 hat.

Beispiele

- Ist $\lambda \in \mathbb{K}$ eine Nullstelle von $p \in \mathbb{K}[X]$, so folgt $p = d(X - \lambda)$ für ein $d \in \mathbb{K}[X]$ (Polynomdivision).
- In $\mathbb{R}[X]$ ist $X^2 + 1$ irreduzibel.

Satz Jedes Polynom in $\mathbb{K}[X]$ ist das Produkt von irreduziblen Polynomen, die bis auf Umordnung eindeutig bestimmt sind.

Hauptraumzerlegung

Satz Sei $A \in \mathbb{C}^{n\times n}$ und $\mu_A = \underbrace{(X-\lambda_1)^{r_1}}_{q_1} \cdots \underbrace{(X-\lambda_k)^{r_k}}_{q_k}$. Dann gilt

$$\mathbb{C}^n = \ker q_1(A) \oplus \cdots \oplus \ker q_k(A).$$

Beweis (1) Sind $p, q \in \mathbb{C}[X]$ teilerfremd (das kleinste p und q enthaltende Ideal ist $\mathbb{C}[X]$, bzw. p, q haben keine gemeinsame Nullstelle), so gilt

$$\ker(pq)(A) = \ker p(A) \oplus \ker q(A):$$

Annahme $\Rightarrow$ es gibt $a, b \in \mathbb{C}[X]$ mit $ap + bq = 1$. Für $v \in \ker(pq)(A)$ folgt

$$v = \underbrace{a(A)p(A)v}_{\in \ker q(A)} + \underbrace{b(A)q(A)v}_{\in \ker p(A)}.$$

Falls $v \in \ker p(A) \cap \ker q(A)$, folgt $v = 0 + 0 = 0$.

(2) Per Induktion folgt aus (1):

$$\mathbb{C}^n = \ker \mu_A(A) = \ker q_1(A) \oplus \ker(q_2 \cdots q_k)(A) = \cdots = \ker q_1(A) \oplus \cdots \oplus \ker q_k(A).$$

Zerlegung in Diagonalanteil und nilpotenten Anteil

Sei $A \in \mathbb{C}^{n\times n}$ und $\mu_A = \underbrace{(X-\lambda_1)^{r_1}}_{q_1} \cdots \underbrace{(X-\lambda_k)^{r_k}}_{q_k}$, also

$$\mathbb{C}^n = \ker q_1(A) \oplus \cdots \oplus \ker q_k(A).$$

Satz 1. Für jedes i gilt $A \ker q_i(A) \subseteq \ker q_i(A)$.

2. $A|_{\ker q_i(A)} = \lambda_i + (A|_{\ker q_i(A)} - \lambda_i)$, wobei $(A|_{\ker q_i(A)} - \lambda_i)^{r_i} = 0$
3. Ist S_i Basis von $\ker q_i$ und $S = (S_1 \ \ldots \ S_n)$, so gilt

$$S^{-1}AS = \underbrace{\begin{pmatrix} \lambda_1 E_{d_1} & & \\ & \ddots & \\ & & \lambda_k E_{d_k} \end{pmatrix}}_{\text{Diagonalmatrix}} + \underbrace{\begin{pmatrix} N_1 & & \\ & \ddots & \\ & & N_k \end{pmatrix}}_{=:N \text{ nilpotente Matrix}}$$

mit $N_i^{r_i} = 0$, also $N^{\max_i r_i} = 0$

Beweis 1. $q_i(A)v = 0 \Rightarrow q_i(A)Av = Aq_i(A)v = 0$

Normalform für nilpotente Matrizen

Satz Sei $N \in \mathbb{C}^{d\times d}$ nilpotent, also $N^k = 0$ für ein k.
Dann gibt es eine Basis S von $\mathbb{C}^d$ so, dass

$$S^{-1}NS = \begin{pmatrix} 0 & \epsilon_1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & & & \ddots & \epsilon_{d-1} \\ 0 & \cdots & \cdots & \cdots & 0 \end{pmatrix} \text{ mit } \epsilon_i \in \{0,1\}$$

Beweis (Idee) Es gilt $\{0\} = \ker N^0 \subseteq \cdots \subseteq \ker N^k = \mathbb{C}^d$.

Sei $W^l = \ker N^l / \ker N^{l-1}$ und $[v]_l = v + \ker N^{l-1} \in W^l$ für $v \in \ker N^l$.

Wegen $N \ker N^{l+1} \subseteq \ker N^l$ ist $N_{(l+1)} \colon W^{l+1} \to W^l$, $[v]_{l+1} \mapsto [Nv]_l$ wohldefiniert und *injektiv*.

Wähle Basis W^k. Deren Bild unter $N_{(k)}$ ist in W^{k-1} linear unabhängig (weil $N_{(k)}$ injektiv). Ergänze zu Basis von W^{k-1}. Deren Bild unter N_{k-1} ist in W^{k-2} linear unabhängig. Ergänze zu Basis von $W^{k-2}\ldots$

Die erhaltenen Basen von $W^k, \ldots, W^0$ liefern dann die gesuchte Basis S.

Die Jordansche Normalform

Satz Jedes $A \in \mathbb{K}^{n\times n}$ ist zu einer Matrix in Jordan-Normalform ähnlich: es gibt eine Basis S von $\mathbb{C}^n$ so, dass

$$S^{-1}AS = \begin{pmatrix} \lambda_1 & \epsilon_1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & & & \ddots & \epsilon_{n-1} \\ 0 & \cdots & \cdots & \cdots & \lambda_n \end{pmatrix} \text{ mit } d_i \in \{0,1\}$$

Beweis Hauptraum-Zerlegung: es gibt S mit

$$S^{-1}AS = \begin{pmatrix} \lambda_1 E_{d_1} & & \\ & \ddots & \\ & & \lambda_k E_{d_k} \end{pmatrix} + \begin{pmatrix} N_1 & & \\ & \ddots & \\ & & N_k \end{pmatrix}$$

mit N_i nilpotent. Wähle nun für jedes i eine Basis S_i des i-ten Hauptraumes so, dass $S_i^{-1} N_i S_i$ wie im vorigen Satz aussieht.