Fachbereich Mathematik
Prof. Dr. J.H. Bruinier
Martin Fuchssteiner
Kay Schwieger

TECHNISCHE UNIVERSITÄT DARMSTADT

WS 07/08 22.01.08

Lineare Algebra I

13. Tutorium mit Lösungshinweisen

(T 1)

Berechnen Sie charakteristische Polynom der Matrix

$$A = \begin{pmatrix} 0 & \dots\dots & & 0 & -\alpha_0 \\ 1 & 0 & \dots & 0 & -\alpha_1 \\ & 1 & \ddots & \vdots & \vdots \\ & & \ddots & 0 & -\alpha_{n-2} \\ & & & 1 & -\alpha_{n-1} \end{pmatrix} .$$

Welche Polynome treten als charakteristisches Polynom einer Matrix auf?

Lösung: Mit vollständiger Induktion zeigt man, dass die Matrix A das charakteristische Polynom

$$P_A(x) = (x^n + \alpha_{n-1}x^{n-1} + \alpha_{n-2}x^{n-2} + \dots + \alpha_1 x + \alpha_0)$$

besitzt. Das zeigt, dass jedes Polynom vom Grad n mit Leitkoeffizient 1 als charakteristisches Polynom einer $(n \times n)$-Matrix auftreten kann. Umgekehrt hat das charakteristische Polynom einer solchen Matrix stets Grad n und Leitkoeffizient 1. Es gilt folglich: Ein Polynom ist genau dann charakteristisches Polynom einer $(n \times n)$-Matrix, wenn es vom Grad n ist und Leitkoeffizient 1 hat.

(T 2) Der Grad eines Polynoms

Wir betrachten die Polynome mit Koeffizienten in einem Körper $\mathbb{K}$. Der *Grad* eines solchen Polynoms $P = \sum_{k=0}^{n} \alpha_k x^k$ ist definiert durch:

$$\mathrm{Grad}(P) := \begin{cases} \max\{\, k \mid \alpha_k \neq 0 \,\} & \text{, falls } P \neq 0 \\ -\infty & \text{, sonst.} \end{cases}$$

Zeigen Sie, dass für alle Polynome P, Q gilt:

$$\mathrm{Grad}(P+Q) \leq \max\{\, \mathrm{Grad}(P), \mathrm{Grad}(Q) \,\} \ ,$$
$$\mathrm{Grad}(P \cdot Q) = \mathrm{Grad}(P) + \mathrm{Grad}(Q) \ .$$

Lösung: Seien $P(x) = \sum_{k=0}^{n} \alpha_k x^k$ und $Q(x) = \sum_{k=0}^{m} \beta_k x^k$ Polynome. Wir können o.B.d.A. $\mathrm{Grad}(P) = n$ und $\mathrm{Grad}(Q) = m$ annehmen, d.h. $\alpha_n \neq 0$ und $\beta_m \neq 0$. Ist nämlich eines der Polynome das Nullpolynom, so ist die Aussage trivial. Weiter können wir o.B.d.A. $n \geq m$ annehmen. Für die Summe ergibt sich nach Definition

$$(P+Q)(x) = \sum_{k=0}^{n} (\alpha_k + \beta_k) x^k$$

und somit $\text{Grad}(P+Q) \leq n = \max\{\,\text{Grad}(P), \text{Grad}(Q)\,\}$. Für das Produkt ergibt sich

$$(P\cdot Q)(x) = \sum_{i=0}^{n}\sum_{j=0}^{m} \alpha_i\beta_j x^{i+j}\ .$$

Wegen $\alpha_n \neq 0$ und $\beta_m \neq 0$ folgt auch $\alpha_n\beta_m \neq 0$ und folglich

$$\text{Grad}(P\cdot Q) = n+m = \text{Grad}(P) + \text{Grad}(Q)\ .$$

(T 3) Abspalten von Nullstellen

Sei $\mathbb{K}$ ein Körper und $P \neq 0$ ein Polynom mit Koeffizienten in $\mathbb{K}$. Sei weiter $\lambda \in \mathbb{K}$ eine Nullstelle von P. Zeigen Sie, dass es dann ein Polynom Q gibt, mit

(a) $P(x) = (x-\lambda)\cdot Q(x)$,

(b) $\text{Grad}(P) = \text{Grad}(Q) + 1$.

Sie können beim Beweis wie in Aufgabe (T3) im 3. Tutorium vorgehen und zuerst $\lambda = 0$ betrachten.

Lösung: Wir zeigen die Behauptung zuerst für den Fall $\lambda = 0$. Sei also $0 \neq P(x) = \sum_{k=0}^{n}\alpha_k x^k$ ein Polynom mit Nullstelle $\lambda = 0$. Dann gilt

$$0 = P(0) = \sum_{k=0}^{n}\alpha_k 0^k = \alpha_0\ .$$

P ist also von der Form

$$P(x) = \sum_{k=1}^{n}\alpha_k x^k = x\cdot\sum_{k=0}^{n-1}\alpha_{k+1}x^k\ .$$

Die Behauptung ist damit für das Polynom $Q(x) := \sum_{k=0}^{n-1}\alpha_{k+1}x^k$ erfüllt.

Sei nun $\lambda \neq 0$ und P ein Polynom mit Nullstelle λ. Wir betrachten das Polynom $P'(x) := P(x+\lambda)$. Dieses Polynom hat den selben Grad wie P und eine Nullstelle in 0. Nach dem vorherigen Beweis gibt es also ein Polynom Q' mit $\text{Grad}(P) = \text{Grad}(P') = \text{Grad}(Q') + 1$ und

$$P(x+\lambda) = P'(x) = x\cdot Q'(x)\ .$$

Das Polynom $Q(x) := Q'(x-\lambda)$ erfüllt dann die Behauptung, denn es hat den selben Grad wie Q', folglich $\text{Grad}(P) = \text{Grad}(Q)+1$, und es gilt

$$P(x) = P'(x-\lambda) = (x-\lambda)\cdot Q'(x-\lambda) = (x-\lambda)\cdot Q(x)\ .$$

(T 4) Formale Polynome

Sei $\mathbb{K}$ ein Körper. Wir bezeichnen mit $\mathcal{F}_{\text{fin}}$ die Menge der Folgen $(\alpha_k)_{k\in\mathbb{N}_0}$, bei denen nur endlich viele Folgenglieder von Null verschieden sind, d.h.

$$\mathcal{F}_{\text{fin}} = \{\,(\alpha_k)_k \mid \exists N_0 \in \mathbb{N}.\forall k \geq N. \quad \alpha_k = 0\,\}\ .$$

(a) Definieren Sie auf $\mathcal{F}_{\text{fin}}$ einen Addition und Skalarmultiplikation mit Skalarkörper $\mathbb{K}$, die $\mathcal{F}_{\text{fin}}$ zu einem Vektorraum macht.

(b) Jede Folge $(\alpha_k)_k \in \mathcal{F}_{\text{fin}}$ lässt sich als sog. *formales Polynom* $P(x) = \sum_{k=0}^{\infty}\alpha_k x^k$ auffassen. (Man beachte, dass nur endlich viele α_k von Null verschieden sind.)
Wie würden Sie zwei solcher formalen Polynome $P(x) = \sum_{k=0}^{n}\alpha_k x^k$ und $Q(x) = \sum_{k=0}^{m}\beta_k x^k$ multiplizieren? Definieren Sie eine Abbildung

$$* : \mathcal{F}_{\text{fin}} \times \mathcal{F}_{\text{fin}} \longrightarrow \mathcal{F}_{\text{fin}}$$

welche dieser Polynom-Multiplikation entspricht. Die hier definierte Operation heißt auch *Faltungsprodukt*.

Wir schreiben im Folgenden für den Vektorraum $\mathcal{F}_{\text{fin}}$ mit der definierten Multiplikation $\mathbb{K}[x]$ und nennen ihn den *Raum der formalen Polynome mit Koeffizienten in* $\mathbb{K}$.

LÖSUNG: (a) Wir definieren für alle $(\alpha_k)_k, (\beta_k)_k \in \mathcal{F}_{\text{fin}}$ und $\lambda \in \mathbb{K}$:

$$(\alpha_k)_k + (\beta_k)_k := (\alpha_k + \beta_k)_k \ , \qquad\qquad \lambda \cdot (\alpha_k)_k := (\lambda\alpha_k)_k \ .$$

Man verifiziert leicht, dass dann bei $(\alpha_k)_k+(\beta_k)_k$ und $\lambda\cdot(\alpha_k)_K$ nur endlich viele Folgenglieder von Null verschieden sind. Diese Addition und Skalarmultiplikation ist damit wohldefiniert. Außerdem zeigt man direkt, dass $\mathcal{F}_{\text{fin}}$ durch diese Operationen zu einem Vektorraum über dem Körper $\mathbb{K}$ wird.

(b) Für zwei solche Polynome $P(x) = \sum_{k=0}^{n} \alpha_k x^k$ und $Q(x) = \sum_{k=0}^{m} \beta_k x^k$ zu den Folgen $a = (\alpha_k)_k$ und $b = (\beta_k)_k$ aus $\mathcal{F}_{\text{fin}}$ würde man das Produkt durch

$$(P \cdot Q)(x) := \sum_{i=0}^{n} \sum_{j=m} \alpha_i \beta_j x^{i+j} = \sum_{k=0}^{n+m} \Big(\sum_{i=0}^{k} \alpha_i \beta_{k-i} \Big) x^k$$

definieren. Dies entspricht der Folge

$$a * b := \Big(\sum_{i=0}^{k} \alpha_i \beta_{k-i} \Big)_k \ .$$

Man überlegt sich leicht, dass auch die Folge $(a * b)$ wieder nur endlich viele von Null verschiedene Folgenglieder besitzt und somit in $\mathcal{F}_{\text{fin}}$ liegt. Die Abbildung

$$* : \mathcal{F}_{\text{fin}} \times \mathcal{F}_{\text{fin}} \longrightarrow \mathcal{F}_{\text{fin}}, \quad (a, b) \mapsto a * b$$

ist damit wohldefiniert und entspricht der Polynom-Multiplikation.

(T 5) Formale Polynome vs. Polynomfunktionen

Für einen Körper $\mathbb{K}$ betrachten wir den Vektorraum $\mathbb{K}[x]$ der (formalen) Polynome mit Koeffizienten in $\mathbb{K}$ wie in Aufgabe T4 und den Vektorraum $\mathbb{K}^{\mathbb{K}}$ aller Funktionen $f : \mathbb{K} \to \mathbb{K}$.

(a) Jedem formalem Polynom $P(x) = \sum_{k=0}^{n} \alpha_k x^k$ in $\mathbb{K}[x]$ lässt sich seine Polynomfunktion

$$f_P : \mathbb{K} \to \mathbb{K}, \quad f_P(a) := \sum_{k=0}^{n} \alpha_k a^k$$

zuordnen. Wir bezeichnen mit $\Phi : \mathbb{K}[x] \to \mathbb{K}^{\mathbb{K}}$ die Abbildung, die jedem Polynom $P \in \mathbb{K}[x]$ seine Polynomfunktion $f_P \in \mathbb{K}^{\mathbb{K}}$ zuordnet. Zeigen Sie, dass die Abbildung $\Phi : \mathbb{K}[x] \to \mathbb{K}^{\mathbb{K}}$ linear ist.

(b) Sei speziell $\mathbb{K} = \mathbb{F}_p$ der endlicher Körper mit p Elementen. Finden Sie zwei Polynome $P, Q \in \mathbb{F}_p[x]$ mit gleicher Polynomfunktion.

(c) Zeigen Sie mit Hilfe der Vandermonde-Determinante (Aufgabe G5 der 9. Übung), dass ein Körper $\mathbb{K}$ genau dann unendlich ist, wenn es keine zwei Polynome mit gleicher Polynomfunktion gibt.

LÖSUNG: (a) Seien $P(x) = \sum_{k=0}^{n} \alpha_k x^k$ und $Q(x) = \sum_{k=0}^{n} \beta_k x^k$ Polynome in $\mathbb{K}[x]$ und $\lambda \in \mathbb{K}$. Dann gilt für alle $a \in \mathbb{K}$

$$\begin{aligned}
\Phi(P+Q)(a) &= \Phi\Big(\sum_{k=0}^{n} (\alpha_k + \beta_k) x^k\Big)(a) = \sum_{k=0}^{n} (\alpha_k + \beta_k) a^k = \sum_{k=0}^{n} \alpha_k a^k + \sum_{k=0}^{n} \beta_k a^k \\
&= \Phi(P)(a) + \Phi(Q)(a) = \big(\Phi(P) + \Phi(Q)\big)(a) \ , \\
\Phi(\lambda \cdot P)(a) &= \Phi\Big(\sum_{k=0}^{n} (\lambda\alpha_k) a^k\Big) = \sum_{k=0}^{n} (\lambda\alpha_k) a^k = \lambda \sum_{k=0}^{n} \alpha_k a^k = \lambda \cdot \Phi(P)(a) \\
&= \big(\lambda \cdot \Phi(P)\big)(a) \ ,
\end{aligned}$$

und somit $\Phi(P+Q) = \Phi(P) + \Phi(Q)$ und $\Phi(\lambda P) = \lambda\Phi(P)$.

(b) Die Polynome $P(x) := 0$ und $Q(x) := x \cdot (x-1) \cdot \ldots \cdot (x-(n-1)) = x^p - x$ haben die gleiche Polynomfunktion, denn für jedes $a \in \mathbb{F}_p$ gilt $f_P(a) = f_Q(a) = 0$.

(c) Die Aussage, dass es keine zwei Polynome mit gleicher Polynomfunktion gibt, ist äquivalent zur Injektivität von Φ und somit zu $\ker \Phi = \{ 0 \}$.

Ist $\mathbb{K}$ endlich mit $\mathbb{K} = \{ a_1, \ldots, a_n \}$, so betrachten wir das Polynom

$$P(x) := \sum_{i=0}^{n} (x - a_i) \ .$$

Weil für jedes $a \in \mathbb{K}$ einer der Faktoren $(a - a_i)$ verschwindet, hat dieses Polynom die Nullfunktion als Polynomfunktion. D.h. P liegt im Kern von Φ.

Sei nun $\mathbb{K}$ unendlich. Sei $P = \sum_{k=0}^{n} \alpha_k x^k$ ein Polynom in $\mathbb{K}[x]$ im Kern von Φ, d.h. mit Polynomfunktion $f_P = 0$. Wir wählen paarweise verschiedene Elemente $b_0, \ldots, b_n \in \mathbb{K}$. Dann gilt

$$\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} f_P(b_0) \\ f_P(b_1) \\ \vdots \\ f_P(b_n) \end{pmatrix} = \begin{pmatrix} \sum_{k=0}^{n} \alpha_k b_0^k \\ \sum_{k=0}^{n} \alpha_k b_1^k \\ \vdots \\ \sum_{k=0}^{n} \alpha_k b_n^k \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & b_0 & \ldots & b_0^n \\ 1 & b_1 & \ldots & b_1^n \\ \vdots & \vdots & & \vdots \\ 1 & b_n & \ldots & b_n^n \end{pmatrix}}_{=:A} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \ . \tag{1}$$

In Aufgabe G5 der 9. Übung haben wir die Determinante der Matrix A berechnet:

$$\det A = \prod_{i=0}^{n} \prod_{j=i+1}^{n} (b_i - b_j) \ .$$

Da die Elemente $b_0, \ldots, b_n$ alle paarweise verschieden gewählt waren, sind auch die Faktoren $(b_i - b_j)$ alle von Null verschieden. Es folgt $\det A \neq 0$. Die Matrix A ist damit invertierbar. Insbesondere folgt dann $(\alpha_0, \ldots, \alpha_n)^T = 0$ aus Gleichung (1) und somit $P = 0$.