Fachbereich Mathematik
Prof. Dr. J.H. Bruinier
Martin Fuchssteiner
Eric Hofmann
Fredrik Strömberg

TECHNISCHE UNIVERSITÄT DARMSTADT

SS 2008 06.05.2008

Lineare Algebra II

5. Tutorium mit Lösungshinweisen

(T 21) Irreduzible Polynome

Sei $\mathbb{K}$ ein Körper und sei $\mathcal{P}(\mathbb{K})$ der Vektoraum der Polynome mit Koeffizenten aus $\mathbb{K}$. Ein Polynom $p \in \mathcal{P}(\mathbb{K})$ heißt *irreduzibel*, wenn es keine Polynome $q, r \in \mathcal{P}(K)$ vom Grad größer 0 gibt, mit der Eigenschaft, dass $p = qr$.

(a) Wie sehen irreduzible Polynome in $\mathcal{P}(\mathbb{C})$ aus? Wie in $\mathcal{P}(\mathbb{R})$?

(b) Geben Sie ein Beispiel für ein irreduzibles Polynom in $\mathcal{P}(\mathbb{Q})$, dessen Grad größer als 2 ist.

LÖSUNG:

(a) Da jedes Polynom über $\mathbb{C}$ in Linearfaktoren zerfällt, sind die irreduziblen Polynome in $\mathcal{P}(\mathbb{C})$ genau die linearen Polynome.

Die irreduziblen Polynome in $\mathcal{P}(\mathbb{R})$ sind entweder linear oder quadratische Polynome der Form

$$Q(X) = aX^2 + bX + c, \quad \text{mit} \quad b^2 - 4ac < 0.$$

(b) Ein mögliches Beispiel ist etwa

$$X^3 - 2.$$

Natürlich zerfällt dieses, wie jedes solche Beispiel, in $\mathcal{P}(\mathbb{R})$,

$$X^3 - 2 = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + (\sqrt[3]{2})^2).$$

(T 22) Euklidscher Algorithmus

In der Vorlesung wurde ein Verfahren zur Ermittlung des ggT zweier Zahlen behandelt, der sogenannte *Euklidsche Algorithmus*, den man kurz folgendermaßen beschreiben kann. **Bestimmung von** $\mathrm{ggT}(a, b)$**:**

- Schritt 0: Setze $a_1 = \min\{a, b\}$, $a_0 = \max\{a, b\}$.
- Schritt k, $k = 1, 2, \ldots$: Führe eine Division mit Rest aus,

$$a_{k-1} = q_k a_k + r_k.$$
$$a_{k+1} := r_k.$$

- Falls $a_{k+1} = 0$, so ist $a_k = \mathrm{ggT}(a, b)$ und man kann aufhören.

(a) Sei n die Zahl an Schritten, die der Algorithmus benötigt, um $\mathrm{ggT}(a_0, b_0)$ zu ermitteln. Betrachten Sie die Matrix $M \in M_2(\mathbb{Z})$,

$$M = \begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix}.$$

Zeigen Sie, dass M^{-1} ebenfalls nur ganzzahlige Einträge hat, und berechnen Sie

$$M^{-1} \begin{pmatrix} a_1 \\ a_0 \end{pmatrix}.$$

Welche Bedeutung haben die Einträge von M^{-1}?

(b) Finden Sie eine Folge $f_0, f_1, \dots$ von ganzen Zahlen mit der Eigenschaft, dass die Berechnung von $\mathrm{ggT}(f_m, f_{m+1})$ genau m Schritte benötigt (ohne Schritt 0).
Hinweis: Fibonacci-Zahlen, vgl. letztes Semester, Aufgabe (A 37) in der 12. Übung.

(c) Zeigen Sie, dass es kein Paar (a, b) ganzer Zahlen gibt mit $a < f_{m+1}$ und $b < f_m$, für welches m Schritte oder mehr benötigt werden.

LÖSUNG:

(a) Jede der Matrizen $\left(\begin{smallmatrix} 0 & 1 \\ 1 & q_k \end{smallmatrix}\right)$, aus denen M zusammengetzt ist, hat Determinante gleich -1. Also ist $\det M = (-1)^k$. Folglich ist

$$M^{-1} = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}^{-1} = (-1)^k \begin{pmatrix} m_{22} & -m_{12} \\ -m_{21} & m_{11} \end{pmatrix}$$

ebenfalls in $M_n(\mathbb{Z})$. Mit den obigen Bezeichnungen gilt folgende Gleichung:

$$\begin{pmatrix} 0 & 1 \\ 1 & q_k \end{pmatrix} \begin{pmatrix} a_{k+1} \\ a_k \end{pmatrix} = \begin{pmatrix} a_k \\ a_{k-1} \end{pmatrix}.$$

Also hat man

$$\begin{aligned} M^{-1} \begin{pmatrix} a_1 \\ a_0 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix}^{-1} \begin{pmatrix} 0 & 1 \\ 1 & q_{n-1} \end{pmatrix}^{-1} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix}^{-1} \begin{pmatrix} a_1 \\ a_0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix}^{-1} \begin{pmatrix} 0 & 1 \\ 1 & q_{n-1} \end{pmatrix}^{-1} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix}^{-1} \begin{pmatrix} a_2 \\ a_1 \end{pmatrix} = \cdots = \begin{pmatrix} 0 \\ \mathrm{ggT}(a_0, a_1) \end{pmatrix}. \end{aligned}$$

Sei $M^{-1} = \left(\begin{smallmatrix} k & l \\ m & n \end{smallmatrix}\right)$. Dann sind m, n die Koeffizenten, um $\mathrm{ggT}(a_0, a_1)$ als ganzzahlige Linearkombination von a_0, a_1 darzustellen. Für k und l gilt hingegen $ka_0 = \mathrm{kgV}(a_0, a_1) = -la_1$.

(b) Idee: Man geht den Euklidschen Algorithmus rückwärts durch und betrachtet ihn als Rekursionsvorschrift. Im letzten, $m$ten Schritt ist immer $a_{m+1} = 0$. Also setzt man $f_0 = 0$. Man überlegt weiter, dass der Algorithmus am längsten läuft, wenn a_0, a_1 teilerfremd sind und alle Reste möglichst groß sind, also $a_k = \mathrm{ggT}(a_0, a_1) = 1$ und $q_k = 1$ für alle k.

Behauptung: Die rekursiv definierte Folge

$$f_0 = 0, f_1 = 1, \ f_{m+1} = f_m + f_{m-1},$$

hat die gewünschte Eigenschaft.
Induktionsbeweis. *Verankerung:* Die Berechnung von $\mathrm{ggT}(f_1, f_2)$ läuft so ab:

$$a_1 = f_1 = 1, a_2 = f_2 = 1, \quad \text{Schritt 1:} \quad a_2 = f_2 - f_1 = 0.$$

Induktionsschritt: Bei der Berechnung des ggT von $(a_0, a_1) = (f_{m+1}, f_m)$ erhält man $q_1 = 1$ und $a_2 = f_{m-1}$, da

$$f_{m+1} > f_m > f_{m-1} = f_{m+1} - f_m.$$

Dazu benötigt man einen Schritt. Per Induktionsvoraussetzung sind nun noch $m-1$ Schritte nötig, um den ggT zu berechnen.

(c) **Annahme:** Es gibt ein solches Paar (a, b). Ohne Beschränkung der Allgemeinheit nehmen wir an, dass $a \geq b$ und dass a, b teilerfremd sind (sonst bräuchte man weniger Schritte). Es ist also $a_m = \mathrm{ggT}(a, b) = 1 = f_1$ und $a_{m+1} = 0 = f_0$. Induktiv ergibt sich hieraus $a_{m+1-k} \geq f_k$, für alle $k = 0, \ldots, m+1$, denn

$$a_{m+1-k} = a_{m+1-(k-2)} + q_{m+1-(k-1)} a_{m+1-(k-1)} \geq f_{k-2} + f_{k-1} = f_k.$$

(Beachte: Die $q_l \geq 1$, $l = 1, \ldots, m$.) Insbesondere sind also $a = a_0 \geq f_{m+1}$ und $b = a_1 \geq f_m$. **Widerspruch!**

(T 23)

Sei $\mathcal{P}_m$ der Vektorraum der Polynome vom Grad $\leq m$ über dem Körper $\mathbb{K} = \mathbb{R}, \mathbb{C}$. Weiterhin sei $D \in \operatorname{End} \mathcal{P}$ definiert durch die Ableitung, also

$$Df = f'.$$

Zeigen Sie, dass D nilpotent ist und bestimmen Sie eine zyklische Basis für D. Geben auch eine Basis an, in der D Jordan-Normalform hat.

LÖSUNG:

Dass D nilpotent ist, ergibt sich daraus, dass $Dc = 0$ für jede Konstante $c \in \mathbb{K}$ und sich der Grad eines nicht-konstanten Polynoms beim Ableiten jeweils um 1 reduziert. D.h. für ein Polynom f vom Grad k ist $D^k f$ konstant. Also ist D^{m+1} auf $\mathcal{P}_m$ die 0-Abbildung.

Bestimmung einer zyklischen Basis: D hat den einzigen Eigenwert 0. Jedes konstante Polynom ist somit Eigenvektor. Wie wählen $e_0 = 1$ als ersten Basisvektor.

Ein Vektor $e_1 \in \mathcal{P}_4$ mit $De_1 = 1$ ist offenbar durch $e_1 = X$ gegeben.

Induktiv erhält man nun weitere Vektoren einer zyklischen Basis e_k, $k = 0, 1, 2, \ldots, m$:

$$e_k = \frac{1}{k!} X^k, \quad \text{da} \quad De_k = \frac{k}{k!} X^{k-1} = \frac{1}{(k-1)!} X^{k-1} = e_{k-1} \quad \text{und} \quad D^k e_k = e_0.$$

Da D nilpotent ist, ist die angegeben zyklische Basis auch schon eine Jordan-Basis.

(T 24)

Im Folgenden bezeichnet K einen Körper, $K = \mathbb{R}$ oder $\mathbb{C}$.

(a) Betrachten Sie einen Jordanblock der Größe 2×2, zu einem Eigenwert $\lambda \in \mathbb{K}$, also eine Matrix

$$J(\lambda) = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}.$$

Finden Sie eine Formel für $J^m(\lambda)$, $m \geq 0$.

(b) Betrachten Sie die Matrix

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

Bestimmen Sie die Eigenwerte von A und finden Sie Transformationsmatrizen S und S^{-1}, so dass $S^{-1}AS$ Jordan Normalform hat.
(Hinweis: Benötigt wird hierzu eine zyklische Basis für jeden (verallgemeinerten) Eigenraum von A.)

(c) Berechnen Sie die Matrix A^{2008}.

LÖSUNG:

(a)Wie man schnell sieht, etwa indem man für einige m $J(\lambda)^m$ berechnet,

$$J(\lambda)^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ J(\lambda)^1 = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix},\ J(\lambda)^2 = \begin{pmatrix} \lambda^2 & 2\lambda \\ 0 & \lambda^2 \end{pmatrix},\ J(\lambda)^3 = \begin{pmatrix} \lambda^3 & 3\lambda^2 \\ 0 & \lambda^3 \end{pmatrix}$$

lautet der gesuchte Ausruck

$$J(\lambda)^m = \begin{pmatrix} \lambda^m & m\lambda^{m-1} \\ 0 & \lambda^m \end{pmatrix}.$$

Dies beweist man einfach durch Induktion nach m.

Induktionsanfang: siehe oben,

Induktionssschritt:

$$J(\lambda)^{m+1} = J(\lambda)^m J(\lambda) = \begin{pmatrix} \lambda^m & m\lambda^{m-1} \\ 0 & \lambda^m \end{pmatrix} \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} = \begin{pmatrix} \lambda^{m+1} & m\lambda^m + 1\lambda^m \\ 0 & \lambda^{m+1} \end{pmatrix}.$$

(b) Bestimmung der Eigenwerte:

$$\det(\lambda E - A) = \begin{vmatrix} \lambda+1 & 0 & 1 \\ 1 & \lambda+1 & 2 \\ 0 & 0 & \lambda-1 \end{vmatrix} = (\lambda+1)^2(\lambda-1).$$

Die Eigenwerte von A sind $+1$ und -1, letzterer mit algebraischer Vielfachheit 2.

Zum Eigenwert -1**:** Die Matrix

$$B =: A + E = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 2 \\ 0 & 0 & 2 \end{pmatrix}$$

hat Rang 2. Somit ist die geometrische Vielfachheit des Eigenwerts -1 gleich 1. Wir bestimmen nun eine zyklische (Orthogonal-)Basis des verallgemeinerten Eigenraums $V_{-1}^2(A)$.

Bestimmung eines *Eigenvektors*: Der Kern der linearen Abbildung B wird von dem Eigenvektor $(0,1,0)^t$ aufgespannt.

Bestimmmung eines *Hauptvektors*: Gesucht ist ein Lösungsvektor $x = (x_1, x_2, x_3)^t$ für die Gleichung

$$Bx = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 2 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}.$$

Offenbar ist $x = (1,0,0)^t$ eine solche Lösung, welche außerdem senkrecht auf $(0,1,0)^t$ steht. Somit sind $(0,1,0)^t$ und $(1,0,0)^t$ eine zyklische Basis von $V_{-1}^2(A)$.

Zum Eigenwert $+1$: Die geometrische Vielfachheit ist 1, einen Eigenvektor v erhält man aus der Gleichung

$$0 = (A-E)v = \begin{pmatrix} -2 & 0 & 1 \\ 1 & -2 & 2 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix}.$$

Für die Komponenten hat man $v_3 = 2v_1$ und $v_2 = 5/2 v_1$, also ist $(1, \frac{5}{2}, 2)^t$ ein Eigenvektor (, welcher den Eigenraum $V_1(A)$ aufspannt.

Eine Jordan-Basis für A setzt sich nun aus den Basen von $V_{-1}^2(A)$ und $V_1(A)$ zusammen, ist also zum Beispiel durch die Vektoren

$$\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ \frac{5}{2} \\ 2 \end{pmatrix}$$

gegeben. Damit erhält man die Transformationsmatrizen

$$S = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & \frac{5}{2} \\ 0 & 0 & 2 \end{pmatrix} \quad \text{und} \quad S^{-1} = \begin{pmatrix} 0 & 1 & -\frac{5}{4} \\ 1 & 0 & -\frac{1}{2} \\ 0 & 0 & \frac{1}{2} \end{pmatrix}$$

und rechnet nach:

$$\begin{aligned} J =: S^{-1}AS &= \begin{pmatrix} 0 & 1 & -\frac{5}{4} \\ 1 & 0 & -\frac{1}{2} \\ 0 & 0 & \frac{1}{2} \end{pmatrix} \begin{pmatrix} -1 & 0 & 1 \\ 1 & -1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & \frac{5}{2} \\ 0 & 0 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & -1 & \frac{3}{4} \\ -1 & 0 & \frac{1}{2} \\ 0 & 0 & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & \frac{5}{2} \\ 0 & 0 & 2 \end{pmatrix} = \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{aligned}$$

(c) Es gilt $A^{2008} = S\,J^{2008}S^{-1}$. Da die in der Jordanzerlegung auftretenden Teilräume zueinander orthogonal sind, ist offenbar

$$J^{2008} = \begin{pmatrix} \left(\begin{smallmatrix} -1 & 1 \\ 0 & -1 \end{smallmatrix}\right)^{2008} & \left(\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right) \\ (0,0) & 1^{2008} \end{pmatrix} =^{(a)} \begin{pmatrix} (-1)^{2008} & 2008\,(-1)^{2007} & 0 \\ 0 & (-1)^{2008} & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -2008 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Man berechnet nun noch

$$\begin{aligned} A^{2008} = SJ^{2008}S^{-1} &= \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & \frac{5}{2} \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & -2008 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & -\frac{3}{4} \\ 1 & 0 & -\frac{1}{2} \\ 0 & 0 & \frac{1}{2} \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 & 1 \\ 1 & -2008 & \frac{5}{2} \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} 0 & 1 & -\frac{3}{4} \\ 1 & 0 & -\frac{1}{2} \\ 0 & 0 & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} 1 & 0 & -\frac{3}{4} \\ -2008 & 1 & \frac{1}{2} \\ 0 & 0 & 1 \end{pmatrix}. \end{aligned}$$

(T 25) Polynome von Jordan-Blöcken

Sei $p(X)$ ein Polynom und J ein Jordan-Block der Größe $n \times n$,

$$J = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \dots & 0 \\ \vdots & & \ddots & & \vdots \\ \vdots & & & \ddots & \vdots \\ \dots & \dots & \dots & 0 & \lambda \end{pmatrix}.$$

Zeigen Sie, dass

$$p(J) = \begin{pmatrix} p(\lambda) & \frac{p'(\lambda)}{1!} & \frac{p''(\lambda)}{2!} & \dots & \frac{p^{(n-1)}(\lambda)}{(n-1)!} \\ 0 & p(\lambda) & \frac{p'(\lambda)}{1!} & \dots & \frac{p^{(n-2)}(\lambda)}{(n-2)!} \\ \vdots & & \ddots & & \vdots \\ \vdots & & & \ddots & \vdots \\ \dots & \dots & \dots & 0 & p(\lambda) \end{pmatrix},$$

wobei wie üblich $p^{(k)}$ die k-te Ableitung von p bezeichnet.

LÖSUNG:

Am Besten beweist man die Aussage zunächst für das Polynom $p(X) = X^m$, für $m \geq 0$. Bekanntlich gilt

$$p^{(k)}(X) = \begin{cases} m(m-1)\cdots(m-k+1)X^{m-k} & \text{für } m \geq k \\ 0 & \text{sonst} \end{cases}.$$

Also ist

$$\frac{1}{k!}p^{(k)}(X) = \frac{m!}{k!(m-k)!}X^{m-k} = \binom{m}{k}X^{m-k},$$

Für $p(X) = X^m$ lautet die Behauptung also:

$$(J^m)_{i,j} = \begin{cases} \binom{m}{j-i}\lambda^{m-(j-i)} & \text{für } j \geq i \quad \text{und } m \geq (j-i) \\ 0 & \text{für } j < i \quad \text{oder } m < (j-i). \end{cases}$$

Wir führen den Beweis per Induktion. **Induktionsverankerung:** Auf der rechten Seite der Gleichung sind für $m = 0$ nur die Einträge auf der Diagonalen $\neq 0$, nämlich $\lambda^0 = 1$. Und in der Tat steht links $J^0 = E$.

Induktionsschritt $m \longrightarrow m+1$: Der Eintrag in der i-ten Spalte und j-ten Zeile von J^{m+1} ist 0 für $j < i$ (Produkt oberer Dreiecksmatrizen!). Für $j > i$ ist eine Fallunterscheidung nötig: Falls $m \geq j - i$ gilt

$$\begin{aligned} (J^{m+1})_{i,j} &= (J^m J)_{i,j} \\ &= 0 + \dots + 0 + \binom{m}{j-i}\lambda^{m-(j-i)} \cdot 1 + \binom{m}{j-(i+1)}\lambda^{m-(j-(i+1))} \cdot \lambda + 0 + \cdots \\ &= \left[\binom{m}{j-i-1} + \binom{m}{j-i}\right]\lambda^{m+1-(j-i)} = \binom{m+1}{j-i}\lambda^{m+1-(j-i)}. \end{aligned}$$

Falls hingegen $m < j - i$, so muss man $m = j - i - 1$ gesondert betrachten. Hier hat man

$$(J^m J)_{i,j} = 0 \cdot 1 + \underbrace{\binom{m}{0}}_{=1}\lambda^0 \cdot \lambda = \lambda = \binom{m+1}{0}\lambda^1 = \binom{m+1}{(m+1)-(j-i)}\lambda^{m+1-(j-i)}.$$

Sonst, also für $m < j - i - 1$, verschwinden alle Summanden, die zu $(J^{m+1})_{i,j}$ beitragen, also $(J^{m+1})_{i,j} = 0$. Zusammen ergibt sich die Behauptung für $p(X) = X^m$.

Nun ergibt sich der allgemeine Fall für ein Polynom $p(X)$, vom Grad M

$$p(X) = \sum_{m=0}^{M} c_m X^m$$

einfach aus der Linearität der Ableitung und der Vektorraumsstruktur der $n \times n$ Matrizen:

$$p(J) = \sum_{m=0}^{M} c_m J^m = \begin{pmatrix} \sum_{m=0}^{M} c_m \lambda^m & \sum_{m=0}^{M} c_m \frac{d}{d\lambda} \lambda^m & \sum_{m=0}^{M} c_m \frac{d^2}{(d\lambda)^2} \frac{\lambda^m}{2!} & \cdots & \cdots \\ \vdots & \ddots & & & \vdots \\ \vdots & & \ddots & & \vdots \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & & & 0 & \sum_{m=0}^{M} c_m \lambda^m \end{pmatrix}.$$