Musterlösung Serie 1

Trigonalisierung, Minimalpolynom

1. Ein kommutativer Ring mit Eins R heisst *Integritätsring*, falls er nullteilerfrei ist, also falls gilt:
$$\forall p, q \in R : (pq = 0 \Rightarrow p = 0 \vee q = 0)\,.$$
Typische Beispiele sind die ganzen Zahlen $R = \mathbb{Z}$ oder Körper $R = K$. Sei nun R ein Integritätsring.

   (a) Zeigen Sie, dass der Ring der Polynome $R[t]$ ein Integritätsring ist.

   (b) Sei $n \geqslant 1$ und $f \in R[t]$, so dass $f \mid t^n$. Zeigen Sie, dass $f = \alpha t^m$ für ein $\alpha \in R^*$ und $m \geqslant 0$.

   (c) (Eisenstein Kriterium "light") Sei nun $f \in \mathbb{Z}[t]$ von der Form
$$f = t^n + a_{n-1}t^{n-1} + \cdots + a_0\,.$$
Weiter sei p eine Primzahl, so dass $p \mid a_i$ für alle i und $p^2 \nmid a_0$. Zeigen Sie, dass $f \in \mathbb{Z}[t]$ *irreduzibel* ist, d.h., gilt $f = gh$ für $g, h \in \mathbb{Z}[t]$, so muss $g = \pm 1$ oder $h = \pm 1$ sein.
Hinweis: Betrachten Sie die Gleichung $f = gh$ in $\mathbb{F}_p[t]$.

Bemerkung: Allgemein nennt man ein Element f eines kommutativen Ringes R irreduzibel*, falls aus $f = pq$ (mit $p, q \in R$) folgt, dass p oder q invertierbar ist.*

Lösung:

   (a) Seien $f, g \in R[t]$ von der Form
$$f = a_m t^m + \cdots + a_0\,, \quad g = b_k t^k + \cdots + b_0\,,$$
mit $a_m \neq 0$, $b_k \neq 0$. Angenommen, $fg = 0$. Betrachten des Koeffizienten von t^{m+k} ergibt $a_m b_k = 0$. Da R Integritätsring ist ergibt sich ein Widerspruch.

   (b) Seien $f, g \in R[t]$ wie oben. Angenommen, $fg = t^n$ und $g \neq 0$. Sei i maximal, so dass $a_j = 0$ für alle $j < i$ und $a_i \neq 0$. Betrachten des Koeffizienten von t^i ergibt:
$$0 = a_i b_0 + a_{i-1}b_1 + \cdots + a_0 b_i = a_i b_0\,,$$
also $b_0 = 0$, da R Integritätsring ist. Analog ergibt dann der t^{i+1}-Koeffizient, dass $b_1 = 0$, und so weiter. Daher $b_\ell = 0$ für alle $\ell < n - i$. Da $g \neq 0$ ist also $i = m$, somit $f = a_m t^m$. Außerdem ist $a_m b_k = 1$, also $a_m \in R^*$.

(c) Wir verwenden Reduktion modulo p, also den Ringhomomorphismus

$$\mathbb{Z}[t] \to \mathbb{F}_p[t] .$$

Angenommen $f = gh$ in $\mathbb{Z}[t]$ mit

$$g = b_k t^k + \cdots + b_0 , \quad h = c_{n-k} t^{n-k} + \cdots + c_0 .$$

Da f normiert ist, muss $b_k = \pm 1$ und $c_{n-k} = \pm 1$. Das Bild in $\mathbb{F}_p[t]$ ist dann $\bar{f} = t^n = \bar{g}\bar{h}$. Nach Teilaufgabe (b) folgt, dass $\bar{g} = \alpha t^k$, $\bar{h} = \beta t^{n-k}$. Falls $0 < k < n$ folgt daher insbesondere $p \mid b_0$ und $p \mid c_0$, also $p^2 \mid a_0$, ein Widerspruch.

2. Für $n \geqslant 1$ und einen beliebigen Parameter $\lambda \in K$ betrachten wir die $n \times n$-Matrix

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

Bestimmen Sie A^k für alle $k \geqslant 0$.

Lösung:

Wir schreiben $A = \lambda I_n + N$ mit der Einheitsmatrix I_n und der Matrix

$$N = \Big(\delta_{j-i,1}\Big)_{1 \leqslant i,j \leqslant n} = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ \vdots & 0 & 1 & \ddots & \vdots \\ \vdots & & 0 & \ddots & 0 \\ \vdots & & & \ddots & 1 \\ 0 & \dots & \dots & \dots & 0 \end{pmatrix} .$$

Mit einem Induktionsargument folgt für alle $m \geqslant 0$

$$N^m = \Big(\delta_{j-i,m}\Big)_{1 \leqslant i,j \leqslant n} .$$

Insbesondere ist N^m die Nullmatrix für alle $m \geqslant n$. Da N und I_n kommutieren, folgt aus der binomischen Formel

$$\begin{aligned} A^k &= (\lambda I_n + N)^k = \sum_{m=0}^{k} \tbinom{k}{m} \lambda^{k-m} N^m \\ &= \Big(\sum_{m=0}^{k} \tbinom{k}{m} \lambda^{k-m} \delta_{j-i,m}\Big)_{i,j} \\ &= \Big(\tbinom{k}{j-i} \lambda^{k-j+i}\Big)_{1 \leqslant i,j \leqslant n} , \end{aligned}$$

wobei wir $\binom{k}{j-i}\lambda^{k-j+i}$ für $j-i \notin \{0,\dots,k\}$ als 0 interpretieren.

In den Fällen $n = 1, 2, 3, 4$ ergeben sich konkret

$$\begin{aligned}
&(\lambda^k) && \text{für } n=1\\
&\begin{pmatrix}\lambda^k & k\lambda^{k-1}\\ 0 & \lambda^k\end{pmatrix} && \text{für } n=2\\
&\begin{pmatrix}\lambda^k & k\lambda^{k-1} & \frac{k(k-1)}{2}\lambda^{k-2}\\ 0 & \lambda^k & k\lambda^{k-1}\\ 0 & 0 & \lambda^k\end{pmatrix} && \text{für } n=3\\
&\begin{pmatrix}\lambda^k & k\lambda^{k-1} & \binom{k}{2}\lambda^{k-2} & \binom{k}{3}\lambda^{k-3}\\ 0 & \lambda^k & k\lambda^{k-1} & \binom{k}{2}\lambda^{k-2}\\ 0 & 0 & \lambda^k & k\lambda^{k-1}\\ 0 & 0 & 0 & \lambda^k\end{pmatrix} && \text{für } n=4\,.
\end{aligned}$$

3. (a) Trigonalisieren Sie folgende Matrix über $\mathbb{Q}$:

$$A = \begin{pmatrix}3 & 0 & 2 & 1\\ 2 & 0 & 2 & 2\\ 5 & -2 & 4 & 5\\ 1 & 0 & -2 & 3\end{pmatrix}.$$

(b) Ist die Trigonalisierung einer Matrix eindeutig?

Lösung:

(a) Wir folgen dem Schema zur Berechnung einer Trigonalisierung siehe Fischer, Seite 247-248. Das charakteristische Polynom von A berechnet sich als:

$$p_A(t) = (t-2)^3(t-4)\,.$$

Ein Eigenvektor zum Eigenwert 2 ist bspw. $v_1 = (1,0,0,-1)^T$. Wir setzen daher

$$S_1^{-1} = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ -1 & 0 & 0 & 1\end{pmatrix}.$$

Die inverse Matrix ist

$$S_1 = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 1 & 0 & 0 & 1\end{pmatrix}.$$

Wir berechnen nun

$$A_2 = S_1 A S_1^{-1} = \begin{pmatrix} 2 & 0 & 2 & 1 \\ 0 & 0 & 2 & 2 \\ 0 & -2 & 4 & 5 \\ 0 & 0 & 0 & 4 \end{pmatrix}.$$

Der Untervektorraum U aufgespannt durch die Standardbasisvektoren e_2, e_3, e_4 ist A-invariant. Ein Eigenvektor der Einschränkung von A auf U zum Eigenwert 2 ist bspw. $v_2 = (0, 1, 1, 0)^T$. Wir setzen daher

$$S_2^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix},$$

wobei die ersten zwei Spalten obige Eigenvektoren sind. Die inverse Matrix ist

$$S_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

Wir berechnen nun

$$A_3 = S_2 A S_2^{-1} = \begin{pmatrix} 2 & 2 & 2 & 1 \\ 0 & 2 & 2 & 2 \\ 0 & 0 & 2 & 3 \\ 0 & 0 & 0 & 4 \end{pmatrix}.$$

Wir haben also eine Trigonalisierung von A gefunden.

(b) Die Trigonalisierung einer Matrix ist keineswegs eindeutig. Beispielsweise ist die Matrix

$$\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$$

diagonalisierbar, da sie zwei verschiedene Eigenwerte hat (1 und 2). Sie ist also ähnlich zu

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

und somit sind die zwei Matrizen verschiedene Trigonalisierungen ein und derselben Matrix. Auch die Matrix in Teilaufgabe (a) besitzt unterschiedliche Trigonalisierungen.

4. Seien $A, B \in \mathrm{M}(n \times n, K)$ ähnliche Matrizen. Zeigen Sie, dass A und B das gleiche Minimalpolynom haben.

Lösung:

Seinen f_A und f_B das Minimalpolynom von A bzw. B. Aus der Ähnlichkeit folgt, dass es eine invertierbare Matrix C gibt, so dass $A = C^{-1}BC$. Für beliebiges $k >$ folgt dann auch

$$A^k = C^{-1}BC \cdots C^{-1}BC = C^{-1}B^kC\,,$$

und somit

$$f_B(A) = C^{-1}f_B(B)C = 0\,,$$

also $f_A \mid f_B$. Analog folgt $f_B \mid f_A$; da beide Polynome normiert sind folgt $f_A = f_B$.

5. Sei p eine Primzahl und $n > 0$.

   (a) Zeigen Sie, dass das Polynom $t^n - p$ irreduzibel über $\mathbb{Q}$ ist.
   Bemerkung: In der Algebra I lernen Sie das Gauß Lemma kennen, welches die Irreduzibilität obigen Polynoms über $\mathbb{Q}$ impliziert.

   (b) Wir betrachten die Matrix $A \in \mathrm{M}(n \times n, \mathbb{Q})$ definiert als

$$A = \begin{pmatrix} 0 & 0 & \dots & 0 & p \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & \dots & \dots & 1 & 0 \end{pmatrix}.$$

   Zeigen Sie, dass $\{0\}$ und $\mathbb{Q}^n$ die einzigen A-invarianten Untervektorräume in $\mathbb{Q}^n$ sind.

Lösung:

(a) Wir nehmen an, dass $f = t^n - p = gh$ mit Polynomen $g,\ h \in \mathbb{Q}[t]$, mit $1 \leqslant r := deg(g) < n$. Wir können o.B.d.A. auch gleich annehmen, dass g und h normiert sind.
Wir betrachten diese Gleichung nun in $\mathbb{C}[t]$. Die n Nullstellen von f sind $\zeta_k = \sqrt[n]{p}e^{2\pi i\frac{k}{n}}$ mit $k = 0, \dots, n-1$, jeweils mit Vielfachheit 1. Dann muss also gelten, für eine echte Teilmenge $S \subsetneq \{0, \dots, n-1\}$ mit $|S| = r$

$$g = \prod_{k \in S}(t - \zeta_k).$$

Der konstante Koeffizient in g hat also den Absolutbetrag

$$p^{\frac{r}{n}}.$$

Dies ist (für $1 \leqslant r < n$) keine rationale Zahl, was man gleich beweist wie die Irrationalität von $\sqrt{2}$ in Analysis I. Genauer: Wäre $p^{\frac{r}{n}} = \frac{a}{b}$ mit ganzen Zahlen a, b, so wäre

$$p^r b^n = a^n.$$

Betrachtet man die Potenz der Primzahl p in den Primfaktorzerlegungen beider Seiten, so ist diese Potenz rechts ein Vielfaches von n und links kein Vielfaches von n, ein Widerspruch Also ist $p^{\frac{r}{n}}$ irrational, im Widerspruch zu $g \in \mathbb{Q}[t]$.

(b) Sei $V \subset \mathbb{Q}^n$ ein A-invarianter Unterraum und g das charakteristische Polynom der Einschränkung von A auf V. Weiter sei f das charakteristische Polynom von A. Man errechnet leicht, dass $f = (-1)^n \, (t^n - p)$. Da $g \mid f$ folgt nach Teilaufgabe (a), dass V trivial ist, also $\{0\}$ oder $\mathbb{Q}^n$.