Serie 14 (Ferienserie)

1. Berechne den Rang der folgenden Matrizen:

a)

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

b)

$$B = \begin{pmatrix} 2 & 5 & -3 & 0 \end{pmatrix}$$

2. Man berechne die Inverse der Matrix

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

3. Sei V der Vektorraum der reellen Polynome vom Grad kleiner oder gleich 2. Definiere $V^* := \mathrm{Hom}\,(V, \mathbb{R})$ als den Vektorraum der linearen Abbildungen von V nach $\mathbb{R}$. Seien die Vektoren $\phi_1, \phi_2, \phi_3, \phi_4$ in V^* gegeben durch

$$\begin{aligned} \phi_1(p) &:= p(0), \\ \phi_2(p) &:= p'(0) + p(0), \\ \phi_3(p) &:= \frac{p''(0)}{2} + p'(0) + p(0) \quad \big(= p(1)\big), \\ \phi_4(p) &:= \int_{-1}^{1} p(t)\, dt \end{aligned}$$

für $p \in V$.

a) Zeige, dass ϕ_1, ϕ_2, ϕ_3 eine Basis von V^* ist.

b) Schreibe ϕ_4 als Linearkombination der Vektoren ϕ_1, ϕ_2, ϕ_3.

Bitte wenden!

Die folgenden Aufgaben sind als Spass- und Repetitionsaufgaben gedacht.

4. Sei $S \subset V$ ein *minimales Erzeugendensystem*, d. h.

(i) $\mathrm{Span}(S) = V$,

(ii) Für alle $t \in S$ gilt $\mathrm{Span}(S \setminus \{t\}) \neq V$.

Zeige direkt aus den Definitionen, dass S eine Basis von V ist.

5. Seien $0 \leq n \leq N$. Wieviele n-dimensionale Unterräume von $(\mathbb{F}_2)^N$ gibt es?

6. Welche der folgenden Abbildungen sind $\mathbb{R}$-linear?

a) $C^0(\mathbb{R}) \longrightarrow \mathbb{R}$, $\qquad f \longmapsto f(0) + \int_{-1}^{1} f(x)\, e^{x^2}\, dx$,

b) $C^0((0,\infty)) \longrightarrow C^0((0,\infty))$, $\qquad f \longmapsto \Big(x \longmapsto x\, f(1/x) \Big)$,

c) $C^0(\mathbb{R}/2\pi\mathbb{Z}) \longrightarrow \mathbb{R}$, $\qquad f \longmapsto \int_{f(0)-\frac{\pi}{2}}^{f(0)+\frac{\pi}{2}} f(2x)\, dx$.

(Mit $C^0(Z)$ wird der Raum der stetigen reellwertigen Funktionen auf Z bezeichnet.)

7. Sei f ein Endomorphismus des endlichdimensionalen Vektorraums V.

Beweise: Ist jeder Unterraum $U \subseteq V$ invariant unter f (d.h. $f(U) \subseteq U$), so ist f ein Vielfaches der Identität.

8. **a)** Es seien a, b und c drei paarweise verschiedene, komplexe Zahlen. Bestimme den Rang der Matrix

$$\begin{pmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{pmatrix}.$$

b) Errate einen Satz, der dieses Resultat verallgemeinert, und beweise den Satz.

Siehe nächstes Blatt!

9. Zeige, dass für eine nilpotente Matrix $N \in \mathbb{K}^{n\times n}$ gilt:

a) $N^n = 0$,

b) $I + N$ ist invertierbar.

10. **a)** Gib eine lineare Abbildung $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ an, so dass $\varphi^n = 0$, aber $\varphi^{n-1} \neq 0$.

b) Gib für jedes $2 \leq k \leq n$ eine lineare Abbildung $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ an, so dass $\varphi^k = \mathrm{Id}$ gilt, aber $\varphi^\ell \neq \mathrm{Id}$ für alle $\ell \in \{1, \ldots, k-1\}$.

11. **a)** Zeige: Falls $a \neq c$ ist, so gilt für jede positive ganze Zahl m

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^m = \begin{pmatrix} a^m & \dfrac{b(a^m - c^m)}{a-c} \\ 0 & c^m \end{pmatrix}.$$

b) Leite eine analoge Formel für den Fall $a = c$ her.

12. Seien $\mathcal{B} := (\sin, \cos, \sin\cdot\cos, \sin^2, \cos^2)$ und $V := \mathrm{Span}(\mathcal{B}) \subseteq \mathbb{R}^{\mathbb{R}}$. Betrachte den Endomorphismus

$$D : V \to V,\ u \mapsto u'.$$

a) Zeige, dass $\mathcal{B}$ eine Basis von V ist.

b) Bestimme die Abbildungsmatrix A von D bezüglich $\mathcal{B}$.

c) Betrachte die 5×5-Matrix A als lineare Abbildung $A : \mathbb{R}^5 \to \mathbb{R}^5$ und berechne deren Kern und Bild.

d) Was sind die entsprechenden Untervektorräume in V?

13. (*Hill-Chiffrierung über* $\mathbb{Z}/n\mathbb{Z}$) In einem auf Lester S. Hill zurückgehenden Chiffrierverfahren aus dem Jahre 1929 werden die Buchstaben A-Z wie folgt durch Elemente aus $\mathbb{Z}/26\mathbb{Z}$ codiert.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Bitte wenden!

In der einfachsten Variante der Hill-Chiffrierung werden sukzessive *Paare* von Symbolen wie folgt verschlüsselt.

1. Wähle eine 2×2-Matrix A mit Einträgen aus $\mathbb{Z}/26\mathbb{Z}$ (die zur Ermöglichung einer späteren Dechiffrierung gewisse zusätzliche Eigenschaften haben sollte).
2. Gruppiere den Quelltext in *Buchstabenpaare* (unter Hinzufügung eines beliebigen Zeichens am Textende bei ungerader Quelltextlänge).
3. Betrachte die numerischen Werte x_1, x_2 jedes der gebildeten Zeichenpaare als zweielementigen Spaltenvektor x und berechne den *numerischen Codevektor* Ax modulo 26.
4. Der Empfänger konvertiert den numerischen Codevektor zurück in ein Buchstabenpaar.

Beispiel: Sei A die Matrix

$$\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}.$$

Der Text "I AM HIDING" wird (durch Hinzufügen von G am Ende) in die Paare

IA MH ID IN GG

gruppiert. Es gilt nun beispielsweise

$$A\begin{pmatrix} 9 \\ 1 \end{pmatrix} = \begin{pmatrix} 11 \\ 3 \end{pmatrix}, \quad A\begin{pmatrix} 13 \\ 8 \end{pmatrix} = \begin{pmatrix} 29 \\ 24 \end{pmatrix} = \begin{pmatrix} 3 \\ 24 \end{pmatrix}.$$

Als Chiffrierfolge ergibt sich insgesamt schliesslich KCCXQLKPUU.

a) Zeige: Falls eine Matrix $B \in (\mathbb{Z}/26\mathbb{Z})^{2\times 2}$ existiert mit

$$BA = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

dann kann B zum Dechiffrieren einer Nachricht benutzt werden.

b) Bestimme die Dechiffriermatrix $B \in (\mathbb{Z}/26\mathbb{Z})^{2\times 2}$ zu der Chiffriermatrix

$$A = \begin{pmatrix} 5 & 6 \\ 2 & 3 \end{pmatrix}.$$

c) Entziffere damit unter der Verwendung von Matlab die Zeichenfolge

HNSBGAAKTFWKDXEZGFXWYHEYZCWBUUIODWRR.

Abgabe: Keine.