

Übungsaufgaben¹ Lineare Algebra und analytische Geometrie I*

Serie 11 zum 31.1.11

- 1.* Wir betrachten eine Folge endlichdimensionaler K -Vektorräume V_i und linearer Abbildungen

$$\mathbf{0} \xrightarrow{f_0} V_1 \xrightarrow{f_1} V_2 \xrightarrow{f_2} \cdots \xrightarrow{f_{n-1}} V_n \xrightarrow{f_n} \mathbf{0},$$

für die $\operatorname{im}(f_i) = \ker(f_{i+1})$ gilt, $i = 0, \dots, n-1$. Beweisen Sie

$$\sum_{i=1}^n (-1)^i \cdot \dim_K(V_i) = 0.$$

2. F sei ein endlicher Körper; beweisen Sie: Die Anzahl der Elemente von F ist Potenz einer Primzahl.
3. Eine Nachricht wird in der folgenden Weise verschlüsselt, indem zunächst Buchstaben auf Elemente des Primkörpers $\mathbb{F}_{29}$ abgebildet werden.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

P	Q	R	S	T	U	V	W	X	Y	Z	-	,	
15	16	17	18	19	20	21	22	23	24	25	26	27	28

Die entstandenen Ziffern werden als Folge von Zahlenpaaren angeordnet (wobei ggf. am Ende der Nachricht ein Leerzeichen einzufügen ist, damit eine gerade Anzahl von Buchstaben entsteht).

Nun bezeichne A eine reguläre Matrix aus $M(2; \mathbb{F}_{29})$; die zugehörige lineare Abbildung $\mathbb{F}_{29}^2 \rightarrow \mathbb{F}_{29}^2$ der Standardräume bildet die Paare der Folge auf neue Paare ab.

Als verschlüsselte Nachricht bezeichnen wir denjenigen Text, der der Folge der Bilder der Zahlenpaare entspricht.

EMIL hat eine Nachricht unter Verwendung der Matrix $A \in M(2, \mathbb{F}_{29})$ nach obiger Methode verschlüsselt; diese lautet nun

„WGPLH,ABVTIM“.

Wir nehmen an, dass EMIL in der Nachricht eine gerade Anzahl von Zeichen verwendet und der Brief mit dem Vornamen EMIL endet.

Entschlüsseln Sie die Nachricht.

¹ Ein * weist auf eine fakultative Aufgabe hin.

Entnommen aus M. Roczen, H. Wolter, W. Pohl, D. Popescu, R. Laza: Lineare Algebra individuell
Online-Version 0.62, <http://www.math.hu-berlin.de/~roczen/la.htm>

4. Wir untersuchen die folgende Matrix

$$A = \begin{pmatrix} -1 & 1 & 0 & 2 & 0 \\ 1 & 0 & -1 & -2 & -1 \\ 1 & 0 & -2 & 1 & 1 \\ -1 & 2 & -2 & 5 & 1 \end{pmatrix} \in M_{\mathbb{R}}(4, 5).$$

- (1) Welchen Rang hat A ?
- (2) φ sei der Homomorphismus von $\mathbb{R}^5$ nach $\mathbb{R}^4$, der durch A definiert wird. Bestimmen Sie jeweils eine Basis von $\text{im}(\varphi)$ und $\text{ker}(\varphi)$.
- (3) Ergänzen Sie die gefundene Basis von $\text{im}(\varphi)$ zu einer Basis von $\mathbb{R}^4$.

5. P_2 sei der Unterraum der Polynome vom Grad ≤ 2 im $\mathbb{R}$ -Vektorraum $\mathbb{R}[X]$ der Polynome in einer Unbestimmten über $\mathbb{R}$. Wir betrachten die lineare Abbildung $\varphi : P_2 \rightarrow P_2$, die bezüglich der Basis $\mathcal{B} := (1, X, X^2)$ durch die folgende Matrix

$$M_{\mathcal{B}}(\varphi) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

beschrieben wird.

- (1) Zeigen Sie, dass $\mathcal{B}' := (2, -X^2 + 2X - 1, -X^2 - X - 1)$ eine Basis von P_2 ist.
- (2) Bestimmen Sie $M_{\mathcal{B}'}(\varphi)$.

Lineare Algebra und analytische Geometrie I*
Lösungsblatt der Aufgabenserie 11 zum 31.1.11

3. **Lösung.** Zunächst stellen wir die Zuordnung der Buchstaben zu den Elementen von $\mathbb{F}_{29}$ her und erhalten die folgende Liste von Paaren

$$(22, 6), (15, 11), (7, 27), (0, 1), (21, 19), (8, 12).$$

Wir haben die Matrix A zu finden. Nun sind „EM“ und „IL“ die letzten beiden Buchstabenpaare der Nachricht. Offensichtlich entsprechen diese gerade den Zahlenpaaren $w_1 = (4, 12)$ und $w_2 = (8, 11)$. Durch Multiplikation ihrer Transponierten mit der Matrix A erhalten wir die letzten zwei Paare der obigen Liste, d.h. $u_1 = (-8, -10)$ $u_2 = (8, 12)$. Es folgt $A \cdot W = U$ mit

$$U = \begin{pmatrix} -8 & 8 \\ -10 & 12 \end{pmatrix}, \quad W = \begin{pmatrix} 4 & 8 \\ 12 & 11 \end{pmatrix}.$$

Daraus ergibt sich

$$A = U \cdot W^{-1} = \begin{pmatrix} 8 & -13 \\ 6 & 2 \end{pmatrix}.$$

Durch Multiplikation der Transponierten der Paare u mit der Matrix

$$A^{-1} = \begin{pmatrix} -8 & 6 \\ -5 & -3 \end{pmatrix},$$

d.h. durch ${}^t u \mapsto A^{-1} \cdot {}^t u$ erhalten wir die gesuchten Urbilder; das erste entsteht beispielsweise durch

$$\begin{pmatrix} 22 \\ 6 \end{pmatrix} \mapsto A^{-1} \cdot \begin{pmatrix} 22 \\ 6 \end{pmatrix} = \begin{pmatrix} 5 \\ 17 \end{pmatrix}.$$

Die Resultate werden wiederum als Liste von Paaren aus $\mathbb{F}_{29}^2$ angeordnet; es ergibt sich

$$(5, 17), (4, 8), (19, 0), (6, 26), (4, 12), (8, 11).$$

Wir stellen gemäß der Tabelle die Zuordnung zu den Buchstaben her und erhalten die unverschlüsselte Nachricht

„FREITAG-EMIL“.

4. **Ergebnis.**

(1) Die Matrix A hat den Rang 3.

(2) Eine Basis für $\ker(\varphi)$ ist

$$((3, 3, 2, 0, 1), (5, 3, 3, 1, 0)),$$

eine Basis für $\operatorname{im}(\varphi)$ ergibt sich als

$$((-1, 1, 1, -1), (1, 0, 0, 2), (0, -1, -2, -2)).$$

(3) Die zuvor gefundene Basis für $\operatorname{im}(\varphi)$ lässt sich folgendermaßen zu einer Basis von $\mathbb{R}^4$ ergänzen:

$$((-1, 1, 1, -1), (1, 0, 0, 2), (0, -1, -2, -2), (1, 0, 0, 0))$$

5. **Ergebnis (2).** Es ist

$$M_{\mathcal{B}'}(\varphi) = \frac{1}{6} \cdot \begin{pmatrix} -6 & 9 & 0 \\ -4 & 0 & 0 \\ -8 & 6 & 6 \end{pmatrix}.$$