Übungsaufgaben[1] Lineare Algebra und analytische Geometrie I*

Serie 7 zum 3.1.11

1. Für Zahlen $f, g \in \mathbb{Z}$, $g \neq 0$ wird die Division mit Rest in der Form

   $$f : g = q \text{ Rest } r$$

   angegeben, wobei $f = g \cdot q + r$ mit $q, r \in \mathbb{Z}$ und $|\, g \,| > r \geq 0$.

   Ausgehend von den Zahlen $r_{-1} := f$, $r_0 := g$, $v_{-1} := 0$, $v_0 := 1$ und mit dem Startindex $i = -1$ führen wir das folgende Verfahren aus:

   Berechne {
   $i := i + 1$,
   $r_{i-1} : r_i = q_{i+1}$ Rest r_{i+1},
   falls $\{r_{i+1} \neq 0\}$ $v_{i+1} = v_{i-1} - v_i \cdot q_{i+1}$,
   } **solange** $\{r_{i+1} \neq 0\}$,
   $k := i$ (letzter Index),
   $u_k = (r_k - v_k \cdot g)/f$.

   Das Ergebnis des Verfahrens sind die Zahlen r_k, u_k und v_k.

   (i) Zeigen Sie, dass r_k der größte gemeinsame Teiler von f und g ist und $u_k f + v_k g = r_k$.

   (ii) Verwenden Sie das obige Verfahren zur Berechnung des multiplikativen Inversen von 22 im endlichen Primkörper $\mathbb{F}_{41}$.

2.* a, b, c seien reelle Zahlen. Bestimmen Sie den Rang der Matrix

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

3. Überprüfen Sie die folgenden Behauptungen für Matrizen über dem Körper K.

   (1) A sei die Diagonalmatrix

   $$\begin{pmatrix} a_1 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & a_n \end{pmatrix}$$

   mit $a_i \in K$. Dann gilt $\operatorname{rang}(A) = n - |\{i \mid a_i = 0\}|$.

   (2) Eine obere Dreiecksmatrix

   $$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & a_{nn} \end{pmatrix}$$

   hat genau dann den Rang n, wenn $a_{11} \cdot a_{22} \cdot \ldots \cdot a_{nn} \neq 0$.

---

[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

(3) B sei eine Matrix der Gestalt

$$\begin{pmatrix} a_1b_1 & a_1b_2 & \dots & a_1b_n \\ a_2b_1 & a_2b_2 & \dots & a_2b_n \\ \vdots & \vdots & \ddots & \vdots \\ a_nb_1 & a_nb_1 & \dots & a_nb_n \end{pmatrix}$$

mit $a_i, b_j \in K$, wobei wenigstens eine der Zahlen a_i und wenigstens eine der Zahlen b_j von Null verschieden sind. Dann hat die Matrix B den Rang 1.

(4) Permutationsmatrizen aus $\mathrm{M}(n; K)$ haben den Rang n.

4. Bestimmen Sie den Rang der Matrix

$$\begin{pmatrix} \sqrt{2} & \sqrt{2}+\sqrt{3} & \sqrt{3} \\ 2 & \sqrt{3}+1 & \sqrt{2} \\ 2+2\sqrt{3} & 5+\sqrt{6}+\sqrt{3} & 2\sqrt{6} \end{pmatrix} \in \mathrm{M}(3; \mathbb{R}).$$

5. 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 $\mathrm{M}(2; \mathbb{F}_{29})$; die zugehörige Abbildung $\mathbb{F}_{29}^2 \to \mathbb{F}_{29}^2$ bildet die Paare der Folge auf neue Paare ab.

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

Eine Nachricht wurde unter Verwendung der Matrix $A = \begin{pmatrix} -6 & 11 \\ 4 & 11 \end{pmatrix}$ verschlüsselt und lautet jetzt „MLTOEIUVOKHG“. Finden Sie die Nachricht.

Lineare Algebra und analytische Geometrie I*
Lösungsblatt der Aufgabenserie 7 zum 3.1.11

1. **Lösung.** (i) Dass r_k größter gemeinsamer Teiler von f und g ist, folgt aus dem euklidischen Algorithmus, der hier nur um die Berechnung der Zahlen u_k und v_k erweitert wurde (das angegebene Verfahren trägt deshalb auch die Bezeichnung *erweiterter euklidischer Algorithmus*).
Um die Darstellung von r_k als Vielfachensumme zu gewinnen, definieren wir $u_{-1} := 1$ und $u_0 := 0$ sowie mit Hilfe zweier Unbestimmter X und Y die Startgrößen $s_{-1} := u_{-1}{\cdot}X - v_{-1}{\cdot}Y$ und $s_0 := u_0{\cdot}X - v_0{\cdot}Y$ aus $\mathbb{Z}[X,Y]$. Nun kann der vertraute euklidische Algorithmus in jedem Schritt um die Berechnung von

$$s_{i+1} = s_{i-1} - s_i{\cdot}q_{i+1}$$

erweitert werden; es folgt

$$s_{i+1} = u_{i+1}{\cdot}X - v_{i+1}{\cdot}Y = (u_{i-1} - u_i{\cdot}q_{i+1}){\cdot}X - (v_{i-1} - v_i{\cdot}q_{i+1}){\cdot}Y.$$

Mit $X = f$ und $Y = g$ gilt $s_i = r_i$. Für alle Reste r_i ist damit eine Darstellung als Vielfachensumme der Ausgangszahlen gewonnen.
Der Kunstgriff und Vorteil des vorliegenden Verfahrens besteht darin, nur die Zahlen v_i zu berechnen; u_k kann dann im letzten Schritt durch Division erhalten werden.
(ii) Das Verfahren ist gut geeignet zur Inversenberechnung in einem endlichen Primkörper. Wir initialisieren r_{-1} mit der Primzahl p und r_0 mit der zu invertierenden Zahl z. Das Verfahren liefert

$$u_k{\cdot}p + v_k{\cdot}z = 1.$$

Es folgt $z^{-1} = v_k$ in $\mathbb{F}_p$ (vgl. 1/2/29). Auf die Berechnung von u_k kann hier verzichtet werden.
Um das multiplikative Inverse von 22 in $\mathbb{F}_{41}$ zu bestimmen, wird also

$$r_{-1} = 41,\ r_0 = 22$$

initialisiert. Es entsteht die Tabelle:

$41 : 22 = 1$ Rest 19	$v_{-1} - 1{\cdot}v_0 = v_1$	$v_1 = -1$
$22 : 19 = 1$ Rest 3	$v_0 - 1{\cdot}v_1 = v_2$	$v_2 = 2$
$19 : 3 = 6$ Rest 1	$v_1 - 6{\cdot}v_2 = v_3$	$v_3 = -13$

Wir erhalten als Resultat $22^{-1} = -13$ im Körper $\mathbb{F}_{41}$.

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

$$(12,11),(19,14),(4,8),(20,21),(14,10),(7,6).$$

Durch Multiplikation der Transponierten der Paare p mit der Matrix

$$A^{-1} = \begin{pmatrix} -3 & 3 \\ 9 & -1 \end{pmatrix},$$

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

$$\begin{pmatrix}12\\11\end{pmatrix} \mapsto A^{-1}\cdot\begin{pmatrix}12\\11\end{pmatrix} = \begin{pmatrix}26\\10\end{pmatrix}.$$

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

$$(26,10),(14,12),(12,28),(3,14),(17,0),(26,28).$$

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

„-KOMM DORA- “.