Übungsaufgaben[1] Lineare Algebra und analytische Geometrie I

Serie 9 zum 5.1.09

1. Geben Sie alle Einheiten der folgenden Ringe an:
   (1) $\mathbb{Z}/(7)$,
   (2) $\mathbb{Z}/(8)$,
   (3)* $\mathbb{Z}/(n)$,
   (4)* $\mathbb{Z}[i\sqrt{5}] := \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\}$ (als Unterring von $\mathbb{C}$).

2. Bestimmen Sie das multiplikative Inverse der Zahl 42 im endlichen Primkörper $\mathbb{F}_{47}$.

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 $\mathrm{M}(2; \mathbb{F}_{29})$; 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 $A = \begin{pmatrix} -2 & -10 \\ -6 & 10 \end{pmatrix}$ verschlüsselt und lautet jetzt „C VKBZ D,SMCXA“. Finden Sie die Nachricht.

4. Es seien $f_1, f_2, \ldots, f_n \in K[X]$ Polynome und $d \in K[X]$ ihr größter gemeinsamer Teiler. Bekanntlich gilt $\mathrm{V}(f_1, f_2, \ldots, f_n) = \mathrm{V}(d)$. Verwenden Sie diese Eigenschaft zur Berechnung der folgenden Nullstellenmengen.
   (1) $\mathrm{V}(2X^6 + 2X^5 - 3X^4 + X^3 + X^2 - 4X + 2, X^5 - X^4 - 4X^3 - 2X^2 - 2X + 3) \subseteq \mathbb{R}$,
   (2) $\mathrm{V}(X^4 + 2X^3 - 12X^2 - 39X - 36, 3X^5 - 4X^4 - 27X^3 - 26X^2 + 21X + 12, 3X^4 + 8X^3 + 5X^2 - 6X - 3) \subseteq \mathbb{C}$,
   (3) $\mathrm{V}(X^6 - 2X^5 - X^4 + 2X^3 + X^2 - 2X, X^7 - X^6 + 2X^5 - 2X^4 + 2X) \subseteq \mathbb{F}_5$.

[1] Entnommen aus M. Roczen, H. Wolter, W. Pohl, D. Popescu, R. Laza: Lineare Algebra individuell Online-Version 0.61, http://www.math.hu-berlin.de/~roczen/la.htm

5. Bestimmen Sie die Zerlegung von $f = 3X^4 - 6X^3 - 4X^2 + 7X + 2$ in irreduzible Faktoren, wenn f als Polynom über dem jeweils angegebenen Körper K betrachtet wird.
   (1) $K = \mathbb{Q}$,
   (2) $K = \mathbb{R}$,
   (3) $K = \mathbb{C}$,
   (4) $K = \mathbb{F}_2$,
   (5) $K = \mathbb{F}_3$.

Lineare Algebra und analytische Geometrie I
Lösungsblatt der Aufgabenserie 9 zum 5.1.09

2. **Lösung.** Der größte gemeinsame Teiler von $f = 47$ und $g = 42$ ist 1, denn f ist Primzahl. Wir stellen 1 als Vielfachensumme von f und g dar. Dazu setzen wir $r_{-1} := f$ und $r_0 := g$. Für $i > 0$ wird mit r_i der Rest bei der i-ten Division bezeichnet. Es ergibt sich die folgende Tabelle:

$47 : 42 = 1$ Rest 5	$r_{-1} - 1 \cdot r_0 = r_1$	$r_1 = f - g$
$42 : \ 5 = 8$ Rest 2	$r_0 \ - 8 \cdot r_1 = r_2$	$r_2 = -8f + 9g$
$5 : \ 2 = 2$ Rest 1	$r_1 \ - 2 \cdot r_2 = r_3$	$r_3 = 17f - 19g$

Die erste Spalte enthält den euklidischen Algorithmus (vgl. 1/2/26). In der zweiten Spalte sind die Rekursionen der Reste angegeben. Die letzte Spalte der Tabelle entsteht aus der zweiten durch Einsetzen der bereits bekannten Ausdrücke und enthält die Darstellung der Reste als Vielfachensummen. Der größte gemeinsame Teiler ist $r_3 = 1$; er ergibt sich als Vielfachensumme

$$1 = 17f - 19g.$$

Bei Übergang zu den Restklassen verschwindet der erste Summand und es folgt in $\mathbb{F}_{47}$ (vgl. 1/2/29)

$$-19 = 42^{-1}.$$

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

$$(2, 28), (21, 10), (1, 25), (28, 3), (27, 18), (12, 2), (23, 0).$$

Durch Multiplikation der Transponierten der Paare p mit der Matrix

$$A^{-1} = \begin{pmatrix} -11 & -11 \\ 5 & 8 \end{pmatrix},$$

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

$$\begin{pmatrix} 2 \\ 28 \end{pmatrix} \mapsto A^{-1} \cdot \begin{pmatrix} 2 \\ 28 \end{pmatrix} = \begin{pmatrix} 18 \\ 2 \end{pmatrix}.$$

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

$$(18, 2), (7, 11), (4, 2), (7, 19), (27, 18), (20, 18), (8, 28).$$

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

„SCHLECHT,SUSI “.

4. **Hinweise zur Lösung.**
   (1) Als Nullstellenmenge ergibt sich $\mathrm{V}(X^2 + X - 1)$ und aus den leicht zu bestimmenden Nullstellen des Polynoms das Resultat.

(2) Die Nullstellenmenge ist $\mathrm{V}(X^3 - X^2 - 9X - 12, 3X^4 + 8X^3 + 5X^2 - 6X - 3) = \mathrm{V}(X^2 + 3X + 3)$; das zuletzt gefundene Polynom ist wiederum leicht zu faktorisieren.

(3) Die Nullstellenmenge ist $\mathrm{V}(2X^4 + 2X^3 + X^2 - X) = \{2, 0\}$.

5. **Ergebnis.**

(1) $f = (3X^2 - 3X - 1) \cdot (X - 2) \cdot (X + 1)$.

(2) Unter (1) ist noch $3X^2 - 3X - 1$ in Linearfaktoren zu zerlegen.

(3) Die Zerlegung ist dieselbe wie unter (2).

(4) $f = (X^2 + X + 1) \cdot (X + 1) \cdot X$.

(5) $f = -1 \cdot (X + 1)^2$.