Lösungen zu den Übungsaufgaben im Buch *Lineare Algebra: Eine anwendungsorientierte Einführung* von Andreas Müller, ISBN 978-3-662-67865-7, https://link.springer.com/book/10.1007/978-3-662-67866-4, Website zum Buch: https://linalg.ch

Kapitel 5: Polynome

5.1. Gegeben ist das Polynom

$$a(X) = X^5 - 15X^3 + 10X^2 + 60X - 72 \in \mathbb{Q}[X].$$

Wenn $a(X)$ eine mehrfache Nullstelle α hat, dann ist $a(X) = (X-\alpha)^2 q(X)$ und die Ableitung

$$a'(X) = 2(X-\alpha)q(X) + (X-\alpha)^2 q'(X)$$

hat ebenfalls α als Nullstelle. Insbesondere haben $a(X)$ und $a'(X)$ einen gemeinsamen Teiler. Der größte gemeinsame Teiler von $a(X)$ und $a'(X)$ kann also die Suche nach Nullstellen vereinfachen. Verwenden Sie diese Idee, um das Polynom $a(X)$ zu faktorisieren.

Lösung. Wir wenden den euklidischen Algorithmus für Polynome auf die beiden Polynome $a(X)$ und $b(X) = a'(X)$ an. Dazu muss erst der Quotient $a(X) : a'(X)$ berechnet werden, es ergibt sich

$$a(X) = \underbrace{\frac{X}{5}}_{=q_0(X)} a'(X) \underbrace{- 6X^3 + 6X^2 + 48X - 72}_{=r_0(X)}. \tag{1}$$

Der nächste Quotient ist dann $a'(X) : r_0(X)$ mit dem Resultat

$$a'(X) = \underbrace{-\frac{5}{6}(X+1)}_{=q_1(X)} r_0(X) + 0. \tag{2}$$

Da der Rest $r_1(X) = 0$ ist, bricht der Algorithmus an dieser Stelle ab. In der Tabelle zusammengefasst:

k	$a_k(X)$	$b_k(X)$	$q_k(X)$	$r_k(X)$
0	$a(X)$	$a'(X)$	$\frac{1}{5}X$	$-6X^3 + 6X^2 + 48X - 72$
1	$a'(X)$	$-6X^3 + 6X^2 + 48X - 72$	$-\frac{5}{6}(X+1)$	0

Wir können jetzt den größten gemeinsamen Teiler ablesen als

$$-6X^3 + 6X^2 + 48X - 72 = -6(X^3 - X^2 - 8X + 12).$$

Der normierte größte gemeinsame Teiler ist also $h(X) = X^3 - X^2 - 8X + 12$.

Der größte gemeinsame Teiler kann aber auch mit der Tableau-Methode von Satz 5.9 berechnet werden, womit die doch eher mühsamen Polynomdivisionen (**??**) und (**??**) vermieden werden können. Das zugehörige Tableau ist

s_3	s_2	s_1	s_0	t_4	t_3	t_2	t_1	t_0	h_3	h_2	h_1	h_0
1				5								
0	1			0	5							
−15	0	1		−45	0	5						
10	−15	0	1	20	−45	0	5					
60	10	−15	0	60	20	−45	0	5				
−72	60	10	−15		60	20	−45	0	1			
	−72	60	10			60	20	−45		1		
		−72	60				60	20			1	
			−72					60				1

linalg.ch/gauss/50

Die Durchführung des Gauß-Algorithmus liefert das Tableau:

s_3	s_2	s_1	s_0	t_4	t_3	t_2	t_1	t_0	h_3	h_2	h_1	h_0
1	0	0	0	0	0	$-\frac{5}{6}$	$-\frac{5}{36}$	$-\frac{35}{216}$	$-\frac{1}{216}$	0	0	0
0	1	0	0	0	0	$-\frac{5}{6}$	$-\frac{35}{36}$	$-\frac{65}{216}$	$-\frac{7}{216}$	0	0	0
0	0	1	0	0	0	0	$-\frac{5}{6}$	$-\frac{35}{36}$	$-\frac{1}{36}$	0	0	0
0	0	0	1	0	0	0	0	$-\frac{5}{6}$	$-\frac{1}{6}$	0	0	0
0	0	0	0	1	0	$\frac{1}{6}$	$\frac{1}{36}$	$\frac{7}{216}$	$\frac{1}{1080}$	0	0	0
0	0	0	0	0	1	$\frac{1}{6}$	$\frac{7}{36}$	$\frac{13}{216}$	$\frac{7}{1080}$	0	0	0
0	0	0	0	0	0	0	0	0	1	1	0	0
0	0	0	0	0	0	0	0	0	8	0	1	0
0	0	0	0	0	0	0	0	0	−12	0	0	1

(3)

Für den größten gemeinsamen Teiler als normiertes Polynom ist $h_3 = 1$, daraus kann man jetzt das Tableau zur Bestimmung der h-Koeffizienten ableiten:

h_2	h_1	h_0	
1	0	0	−1
0	1	0	−8
0	0	1	12

$$\Rightarrow \qquad h(X) = X^3 - X^2 - 8X + 12.$$

Aus dem Tableau (**??**) kann man jetzt auch die Polynome $s(X)$ und $t(X)$ ablesen. Für das Polynom $t(X)$ beachten wir, dass die Variablen t_0 bis t_2 frei wählbar sind, wir setzen sie = 0. Dann folgt

$$s(X) = -\frac{1}{216}(X^3 + 7X^2 + 6X + 36)$$
$$t(X) = \frac{1}{1080}(X^4 + 7X^3).$$

Durch Ausmultiplizieren kann

$$s(X)a(X) + t(X)b(X) = h(X)$$

verifiziert werden.

Die Nullstellen von $h(X)$ sind auch Nullstellen von $a(X)$ und $a'(X)$. Da aber die Ordnung einer gemeinsamen Nullstellen von $a'(X)$ jeweils um eins kleiner ist als die Ordnung der Nullstelle von

$a(X)$, müssen die Nullstellen auch im Quotienten auftauchen. Der größten gemeinsamen Teiler ist ein Polynom vom Grad 3, der Quotient ist das Polynom

$$a(X) : h(X) = X^2 + X - 6 = (X + 3)(X - 2).$$

Das Polynom $h(X)$ muss also die Nullstellen 2 und -3 ebenfalls als Nullstellen haben, wir teilen daher

$$h(X) : X^2 + X - 6 = X^3 - X^2 - 8X + 12 : X^2 + X - 6 = X - 2.$$

Damit ist jetzt die Faktorisierung geschafft:

$$a(X) = (X - 2)(X + 3)h(X) = (X - 2)(X + 3) \cdot (X - 2)(X + 3) \cdot (X - 2) = (X - 2)^3(X + 3)^2. \quad \bigcirc$$

5.2. Man finde das Minimalpolynom der Matrix

$$A = \begin{pmatrix} 0 & -3 & -2 & 0 \\ 1 & -4 & -2 & 0 \\ -3 & 7 & 3 & 0 \\ -14 & 25 & 5 & 1 \end{pmatrix}.$$

linalg.ch/gauss/51

Lösung. Aus den Potenzen

$$A^2 = \begin{pmatrix} 3 & -2 & 0 & 0 \\ 2 & -1 & 0 & 0 \\ -2 & 2 & 1 & 0 \\ -4 & 2 & -2 & 1 \end{pmatrix}, \quad A^3 = \begin{pmatrix} -2 & -1 & -2 & 0 \\ -1 & -2 & -2 & 0 \\ -1 & 5 & 3 & 0 \\ -6 & 15 & 3 & 1 \end{pmatrix} \quad \text{und} \quad A^4 = \begin{pmatrix} 5 & -4 & 0 & 0 \\ 4 & -3 & 0 & 0 \\ -4 & 4 & 1 & 0 \\ -8 & 4 & -4 & 1 \end{pmatrix}$$

kann man das Gleichungssystem für die Koeffizienten des Minimalpolynoms mit dem Tableau

a_{11}	a_{12}	a_{13}	a_{14}	a_{21}	a_{22}	a_{23}	a_{24}	a_{31}	a_{32}	a_{33}	a_{34}	a_{41}	a_{42}	a_{43}	a_{44}	m_0	m_1	m_2	m_3	m_4
1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	1	0	0	0	0
0	−3	−2	0	1	−4	−2	0	−3	7	3	0	−14	25	5	1	0	1	0	0	0
3	−2	0	0	2	−1	0	0	−2	2	1	0	−4	2	−2	1	0	0	1	0	0
−2	−1	−2	0	−1	−2	−2	0	−1	5	3	0	−6	15	3	1	0	0	0	1	0
5	−4	0	0	4	−3	0	0	−4	4	1	0	−8	4	−4	1	0	0	0	0	1

schreiben. Durchführung des Gauss-Algorithmus ergibt

a_{11}	a_{12}	a_{13}	a_{14}	a_{21}	a_{22}	a_{23}	a_{24}	a_{31}	a_{32}	a_{33}	a_{34}	a_{41}	a_{42}	a_{43}	a_{44}	m_0	m_1	m_2	m_3	m_4
1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1
0	1	0	0	−1	2	0	0	1	−1	1	0	0	3	3	1	0	$-\frac{1}{2}$	−1	$\frac{1}{2}$	2
0	0	1	0	1	−1	1	0	0	−2	−3	0	0	−3	0	−2	0	−1	$-\frac{1}{4}$	$\frac{1}{2}$	$-\frac{5}{4}$
0	0	0	0	0	0	0	0	0	0	0	0	1	−2	−1	0	0	$\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{4}$
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	−2	0	1

Daraus liest man die Koeffizienten $m_0, \ldots, m_4$ und damit das Minimalpolynom

$$m(X) = X^4 - 2X^2 + 1 = (X^2 - 1)^2 = (X - 1)^2(X + 1)^2. \quad \bigcirc$$

5.3. Führen Sie die nachfolgenden Berechnungen unter Verwendung des Multiplikations-Spreadsheets[1] für den Körper $\mathbb{F}_{2^8}$ durch, wie er in AES implementiert wird.

a) Berechnen Sie die dritten Potenzen von

$$z_1 = \texttt{0x67}, \quad z_2 = \texttt{0xa7}, \quad z_3 = \texttt{0xc0}.$$

Zeigen Sie, dass alle drei Elemente Nullstellen des Polynoms $P(Z) = Z^3 + \texttt{0x07} \in \mathbb{F}_{2^8}[Z]$ sind.

b) Multiplizieren Sie

$$(Z + z_1)(Z + z_2)(Z + z_3) = (Z + \texttt{0x67})(Z + \texttt{0xa7})(Z + \texttt{0xc0})$$

und zeigen Sie, dass dies eine Faktorisierung von $P(Z)$ ist.

c) Bestimmen Sie z_1^{-1}.

d) Weil für alle drei Elemente z_k die Gleichung $z_k^3 = 7$ gilt, müssen

$$\zeta_1 = 1 = \frac{z_1}{z_1}, \quad \zeta_2 = \frac{z_2}{z_1} \quad \text{und} \quad \zeta_3 = \frac{z_3}{z_1}$$

dritte Einheitswurzeln sein. Berechnen Sie ζ_2 und ζ_3 und prüfen Sie nach, dass $\zeta_2^3 = \zeta_3^3 = 1$ ist.

Lösung. a) Die Rechnung mit dem Spreadsheet ergibt

$$\begin{aligned} \texttt{0x67} \cdot \texttt{0x67} &= \texttt{0xd2} & \texttt{0x67} \cdot \texttt{0xd2} &= \texttt{0x07} \\ \texttt{0xa7} \cdot \texttt{0xa7} &= \texttt{0xe3} & \texttt{0x67} \cdot \texttt{0xe3} &= \texttt{0x07} \\ \texttt{0xc0} \cdot \texttt{0xc0} &= \texttt{0x31} & \texttt{0xc0} \cdot \texttt{0x31} &= \texttt{0x07} \end{aligned}$$

Für alle drei Elemente gilt also $z_k^3 = \texttt{0x07}$ oder $z_k^3 + \texttt{0x07} = 0$.

b) Ausmultiplizieren ergibt zunächst

$$\begin{aligned} (Z + \texttt{0x67})(Z + \texttt{0xa7})(Z + \texttt{0xc0}) &= Z^3 + \underbrace{(\texttt{0x67} + \texttt{0xa7} + \texttt{0xc0})}_{=0} Z^2 \\ &\quad + (\texttt{0x67} \cdot \texttt{0xa7} + \texttt{0x67} \cdot \texttt{0xc0} + \texttt{0xa7} \cdot \texttt{0xc0}) Z \\ &\quad + \texttt{0x67} \cdot \texttt{0xa7} \cdot \texttt{0xc0} \\ &= Z^3 + \underbrace{(\texttt{0x31} + \texttt{0xe3} + \texttt{0xd2})}_{=0} Z^2 + \texttt{0x31} \cdot \texttt{0xc0} \\ &= Z^3 + \texttt{0x07}. \end{aligned}$$

c) Die Inverse von $z_1 = \texttt{0x67}$ ist $z_1^{-1} = \texttt{0x43}$.

[1] Versionen für verschiedene Tabellenkalkulationsprogramme unter https://linalg.ch/files/f256/

d) Durch Multiplikation mit z_1^{-1} findet man

$$\zeta_2 = \texttt{0xa7} \cdot \texttt{0x43} = \texttt{0xbc}$$
$$\zeta_3 = \texttt{0xc0} \cdot \texttt{0x43} = \texttt{0xbd}$$

Durch Ausmultiplizieren kontrolliert man

$$\texttt{0xbc}^2 = \texttt{0xbc} \cdot \texttt{0xbc} = \texttt{0xbd}$$
$$\texttt{0xbc}^3 = \texttt{0xbc} \cdot \texttt{0xbc}^2 = \texttt{0xbc} \cdot \texttt{0xbd} = \texttt{0x01}$$
$$\texttt{0xbd}^2 = \texttt{0xbd} \cdot \texttt{0xbd} = \texttt{0xbc}^2 \cdot \texttt{0xbc}^2 = \texttt{0xbc}^3 \cdot \texttt{0xbc} = \texttt{0xbc}$$
$$\texttt{0xbd}^3 = \texttt{0xbc} \cdot \texttt{0xbd} = \texttt{0xbc} \cdot \texttt{0xbc}^2 = \texttt{0xbc}^3 = 1$$

Die Elemente ζ_k sind also tatsächlich dritte Einheitswurzeln. ○

5.4. Zeigen Sie, dass die Matrix

$$C = \begin{pmatrix} \texttt{0x02} & \texttt{0x03} & \texttt{0x01} & \texttt{0x01} \\ \texttt{0x01} & \texttt{0x02} & \texttt{0x03} & \texttt{0x01} \\ \texttt{0x01} & \texttt{0x01} & \texttt{0x02} & \texttt{0x03} \\ \texttt{0x03} & \texttt{0x01} & \texttt{0x01} & \texttt{0x02} \end{pmatrix},$$

die im AES-Algorithmus für das Mischen der Spalten verwendet wird, invertierbar ist.

Lösung. Die direkte Invertierung mit dem Gauss-Algorithmus ist etwas mühsam, da dazu viele Divisionen nötig sind. Es genügt aber zu zeigen, dass die Determinanten $\neq 0$ ist, was man mit dem Entwicklungssatz sofort machen kann:

$$\begin{aligned}
\det(C) &= \begin{vmatrix} \texttt{0x02} & \texttt{0x03} & \texttt{0x01} & \texttt{0x01} \\ \texttt{0x01} & \texttt{0x02} & \texttt{0x03} & \texttt{0x01} \\ \texttt{0x00} & \texttt{0x03} & \texttt{0x01} & \texttt{0x02} \\ \texttt{0x00} & \texttt{0x00} & \texttt{0x03} & \texttt{0x02} \end{vmatrix} \\
&= \texttt{0x02} \begin{vmatrix} \texttt{0x02} & \texttt{0x03} & \texttt{0x01} \\ \texttt{0x03} & \texttt{0x01} & \texttt{0x02} \\ \texttt{0x00} & \texttt{0x03} & \texttt{0x02} \end{vmatrix} + \texttt{0x01} \begin{vmatrix} \texttt{0x03} & \texttt{0x01} & \texttt{0x01} \\ \texttt{0x03} & \texttt{0x01} & \texttt{0x02} \\ \texttt{0x00} & \texttt{0x03} & \texttt{0x02} \end{vmatrix} \\
&= \texttt{0x02} \begin{vmatrix} \texttt{0x02} & \texttt{0x03} & \texttt{0x01} \\ \texttt{0x01} & \texttt{0x02} & \texttt{0x03} \\ \texttt{0x00} & \texttt{0x03} & \texttt{0x02} \end{vmatrix} + \texttt{0x01} \begin{vmatrix} \texttt{0x03} & \texttt{0x01} & \texttt{0x01} \\ \texttt{0x00} & \texttt{0x00} & \texttt{0x01} \\ \texttt{0x00} & \texttt{0x03} & \texttt{0x02} \end{vmatrix} \\
&= \texttt{0x02} \left(\texttt{0x02} \begin{vmatrix} \texttt{0x02} & \texttt{0x03} \\ \texttt{0x03} & \texttt{0x02} \end{vmatrix} + \texttt{0x01} \begin{vmatrix} \texttt{0x03} & \texttt{0x01} \\ \texttt{0x03} & \texttt{0x02} \end{vmatrix} \right) + \texttt{0x01} \begin{vmatrix} \texttt{0x03} & \texttt{0x01} & \texttt{0x01} \\ \texttt{0x00} & \texttt{0x03} & \texttt{0x02} \\ \texttt{0x00} & \texttt{0x00} & \texttt{0x01} \end{vmatrix} \\
&= \texttt{0x02}(\texttt{0x02}(\texttt{0x04} + \texttt{0x05}) + (\texttt{0x06} + \texttt{0x03})) + \texttt{0x030x03} \\
&= \texttt{0x02}(\texttt{0x02} + \texttt{0x05}) + \texttt{0x05} = \texttt{0x0e} + \texttt{0x05} = \texttt{0x0a} \neq 0.
\end{aligned}$$

○