A2.3: Reduzible und irreduzible Polynome

$m = 2$	$a_1(x) = x^2 + x$ $a_2(x) = x^2 + 1$
$m = 3$	$a_3(x) = x^3$ $a_4(x) = x^3 + 1$ $a_5(x) = x^3 + x$ $a_6(x) = x^3 + x + 1$ $a_7(x) = x^3 + x^2 + 1$
$m = 4$	$a_8(x) = x^4 + 1$ $a_9(x) = x^4 + x^3 + 1$ $a_{10}(x) = x^4 + x^2 + 1$

Wichtige Voraussetzungen für das Verständnis der Kanalcodierung sind Kenntnisse der Polynomeigenschaften. Wir betrachten in dieser Aufgabe Polynome der Form

$$a(x) = a_0 + a_1 \cdot x + a_2 \cdot x^2 + \ \ldots \ + a_m \cdot x^m \ ,$$

wobei für die Koeffizienten $a_i \in \text{GF}(2) = \{0, 1\}$ gilt $(0 \le i < m)$ und der höchste Koeffizient stets zu $a_m = 1$ vorausgesetzt wird. Man bezeichnet m als den Grad des Polynoms. Nebenstehend sind zehn Polynome angegeben, wobei der Polynomgrad entweder $m = 2$ (rote Schrift), $m = 3$ (blaue Schrift) oder $m = 4$ (grüne Schrift) ist.

Ein Polynom $a(x)$ bezeichnet man als **reduzibel**, wenn es als Produkt zweier Polynome $p(x)$ und $q(x)$ mit jeweils niedrigerem Grad dargestellt werden kann:

$$a(x) = p(x) \cdot q(x)$$

Ist dies nicht möglich, das heißt, wenn für das Polynom

$$a(x) = p(x) \cdot q(x) + r(x)$$

mit einem Restpolynom $r(x) \neq 0$ gilt, so nennt man das Polynom als **irreduzibel**. Solche irreduziblen Polynome sind für die Beschreibung von Fehlerkorrekturverfahren von besonderer Bedeutung.

Der Nachweis, dass ein Polynom $a(x)$ vom Grad m irreduzibel ist, erfordert mehrere Polynomdivisionen $a(x)/q(x)$, wobei der Grad des jeweiligen Divisorpolynoms $q(x)$ stets kleiner ist als m. Nur wenn alle diese Modulo–2–Divisionen stets einen Rest $r(x) \neq 0$ liefern, ist nachgewiesen, dass $a(x)$ ein irreduzibles Polynom beschreibt.

Dieser exakte Nachweis ist sehr aufwändig. Notwendige Voraussetzungen dafür, dass $a(x)$ überhaupt ein irreduzibles Polynom sein könnte, sind die beiden Bedingungen (bei nichtbinärer Betrachtungsweise wäre „= 1" durch „≠ 0" zu ersetzen):

- $a(x = 0) = 1$,
- $a(x = 1) = 1$.

Ansonsten könnte man für das zu untersuchende Polynom schreiben:

$$a(x) = q(x) \cdot x \quad \text{bzw.} \quad a(x) = q(x) \cdot (x + 1) \, .$$

Die oben genannten Voraussetzungen sind zwar notwendig, jedoch nicht hinreichend, wie das folgende Beispiel zeigt:

$$a(x) = x^5 + x^4 + 1 \quad \Rightarrow \quad a(x = 0) = 1 \, , \ \ a(x = 1) = 1 \, .$$

Trotzdem ist dieses Polynom reduzibel:

$$a(x) = (x^3 + x + 1)(x^2 + x + 1) \, .$$

Hinweis: Die Aufgabe gehört zum Themengebiet von **Kapitel 2.2.**

Fragebogen zu "A2.3: Reduzible und irreduzible Polynome"

a) Wieviele Polynomdivisionen (N_D) sind erforderlich, um exakt nachzuweisen, dass ein GF(2)–Polynom $a(x)$ vom Grad m irreduzibel ist?

$$\boldsymbol{m = 2}\text{: } \boldsymbol{N_D} =$$

$$\boldsymbol{m = 3}\text{: } \boldsymbol{N_D} =$$

$$\boldsymbol{m = 4}\text{: } \boldsymbol{N_D} =$$

b) Welche der Grad–2–Polynome sind irreduzibel?

- ☐ $a_1(x) = x^2 + x$,
- ☐ $a_2(x) = x^2 + x + 1$.

c) Welche der Grad–3–Polynome sind irreduzibel?

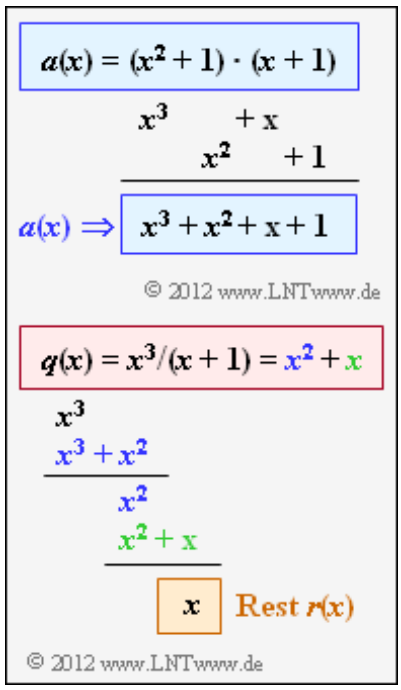
- ☐ $a_3(x) = x^3$,
- ☐ $a_4(x) = x^3 + 1$,
- ☐ $a_5(x) = x^3 + x$,
- ☐ $a_6(x) = x^3 + x + 1$,
- ☐ $a_7(x) = x^3 + x^2 + 1$.

d) Welche der Grad–4–Polynome sind irreduzibel?

- ☐ $a_8(x) = x^4 + 1$,
- ☐ $a_9(x) = x^4 + x^3 + 1$,
- ☐ $a_{10}(x) = x^4 + x^2 + 1$.

Z2.3: Polynomdivision

In dieser Aufgabe beschäftigen wir uns mit der Multiplikation und insbesondere der Division von Polynomen im Galoisfeld GF(2). In der Abbildung ist jeweils die Vorgehensweise an einem einfachen und selbsterklärenden Beispiel verdeutlicht:



- Die Multiplikation der beiden Polynome $x^2 + 1$ und $x + 1$ liefert das Ergebnis $a(x) = x^3 + x^2 + x + 1$.
- Die Division des Polynoms $a(x) = x^3$ durch $p(x) = x + 1$ liefert den Quotienten $q(x) = x^2 + x$ und den Rest $r(x) = x$.
- Man kann das letztere Ergebnis wie folgt überprüfen:

$$\begin{aligned} a(x) &= p(x) \cdot q(x) + r(x) = \\ &= [(x+1) \cdot (x^2 + x)] + x = \\ &= [x^3 + x^2 + x^2 + x] + x = x^3 . \end{aligned}$$

Hinweis: Die Aufgabe gehört zum Themengebiet von **Kapitel 2.2.**

Fragebogen zu "Z2.3: Polynomdivision"

a) Welches Ergebnis liefert $a(x) = (x^3 + x + 1) \cdot (x^2 + 1)$?

- ☐ $a(x) = x^5 + x^3 + x^2 + 1$,
- ☐ $a(x) = x^5 + x^2 + x + 1$,
- ☐ $a(x) = x^6 + x^3 + x^2 + 1$.

b) Welche der Polynomdivisionen ergeben keinen Rest $r(x)$?

- ☐ $(x^5 + x^2 + x + 1)/(x^3 + x + 1)$,
- ☐ $(x^5 + x^2 + x + 1)/(x^2 + 1)$,
- ☐ $(x^5 + x^2 + x + 1)/(x^2)$,
- ☐ $(x^5 + x^2 + x)/(x^2 + 1)$.

c) Es sei $a(x) = x^6 + x^5 + 1$ und $p(x) = x^3 + x^2 + 1$. Bestimmen Sie $q(x)$ und $r(x)$ entsprechend der Beschreibungsgleichung $a(x) = p(x) \cdot q(x) + r(x)$.

- ☐ $q(x) = x^3 + x^2 + 1, \quad r(x) = 0$,
- ☐ $q(x) = x^3 + 1, \quad r(x) = 0$,
- ☐ $q(x) = x^3 + 1, \quad r(x) = x^2$.

A2.4: GF(2^2)–Darstellungsformen

Nebenstehend sehen Sie für den Erweiterungskörper GF(2^2) die Additions– sowie die Multiplikationstabelle in drei verschiedenen Varianten:

- die *Polynomdarstellung*,
- die *Koeffizientenvektordarstellung*,
- die *Exponentendarstelluung*.

Hinweis: Die Aufgabe bezieht sich auf das **Kapitel 2.2.**

Alle notwendigen Informationen zu GF(2^2) finden Sie auf der **Seite 1** dieses Kapitels.

(A) Polynomdarstellung: $k_1 \cdot \alpha + k_0$

+	z_0 0	z_1 1	z_2 α	z_3 $1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

·	z_0 0	z_1 1	z_2 α	z_3 $1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

(B) Koeffizientenvektordarstellung:

+	z_0 00	z_1 01	z_2 10	z_3 11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

·	z_0 00	z_1 01	z_2 10	z_3 11
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01
11	00	11	01	10

(C) Exponentendarstellung: 0, α^i $(0 \le i \le 2)$

+	z_0 0	z_1 α^0	z_2 α^1	z_3 α^2
0	0	α^0	α^1	α^2
α^0	α^0	0	α^2	α^1
α^1	α^1	α^2	0	α^0
α^2	α^2	α^1	α^0	0

·	z_0 0	z_1 α^0	z_2 α^1	z_3 α^2
0	0	0	0	0
α^0	0	α^0	α^1	α^2
α^1	0	α^1	α^2	α^0
α^2	0	α^2	α^0	α^1

Fragebogen zu "A2.4: GF(2^2)–Darstellungsformen "

a) Welche Charakteristika erkennt man aus der Polynomdarstellung?

- ☐ Die Elemente α und $1+\alpha$ sind weder 0 noch 1.
- ☐ Die Rechenoperationen erfolgen modulo 2.
- ☐ Die Rechenoperationen erfolgen modulo 4.
- ☐ Man erkennt „$\alpha^2 + \alpha + 1 = 0$” aus der Additionstabelle.
- ☐ Man erkennt „$\alpha^2 + \alpha + 1 = 0$” aus der Multiplikationstabelle.

b) Welcher Zusammenhang besteht zwischen der Koeffizientenvektor– und der Polynomdarstellung? Es gelte $k_0 \in \{0, 1\}$ und $k_1 \in \{0, 1\}$.

- ☐ $(k_0\ k_1)$ bezieht sich auf das Element $k_1 \cdot \alpha + k_0$.
- ☐ $(k_1\ k_0)$ bezieht sich auf das Element $k_1 \cdot \alpha + k_0$.
- ☐ Zwischen beiden Darstellungen besteht keinerlei Zusammenhang.

c) Wie hängen Polynom– und Exponentendarstellung zusammen?

- ☐ Es sind keine Zusammenhänge erkennbar.
- ☐ Die Elemente 0, 1 und α sind in beiden Darstellungen gleich.
- ☐ Das Element $1+\alpha$ lautet in der Exponentendarstellung α^2.
- ☐ Das Element α^2 der Exponentendarstellung steht für $\alpha \cdot (1+\alpha)$.

d) Berechnen Sie die Ausdrücke A und B nach diesen drei Darstellungsformen. Welche Aussagen treffen zu?

- ☐ Es gilt $A = z_2 \cdot z_2 + z_2 \cdot z_3 + z_3 \cdot z_3 = z_0$,
- ☐ Es gilt $B = (z_0 + z_1 + z_2) \cdot (z_0 + z_1 + z_3) = z_1$,
- ☐ Es gilt $A = z_2 \cdot z_2 + z_2 \cdot z_3 + z_3 \cdot z_3 = z_2$,
- ☐ Es gilt $B = (z_0 + z_1 + z_2) \cdot (z_0 + z_1 + z_3) = z_3$.

Z2.4: Endliche und unendliche Körper

In der Mathematik unterscheidet man verschiedene Zahlenmengen:

- die Menge der natürlichen Zahlen: $N = \{0, 1, 2, ...\}$,
- die Menge der ganzen Zahlen: $Z = \{..., –1, 0, +1, ...\}$,
- die Menge der rationalen Zahlen: $Q = \{m/n\}$ mit $m \in Z$, $n \in Z \setminus \{0\}$,
- die Menge R der reellen Zahlen,
- die Menge der komplexen Zahlen: $C = \{a + \text{j} \cdot b\}$ mit $a \in R$, $b \in R$ und der imaginären Einheit j.

Eine solche Menge (englisch: *Set*) bezeichnet man dann (und nur dann) als einen **Körper** (englisch: *Field*) im algebraischen Sinne, wenn in ihr die vier Rechenoperationen Addition, Subtraktion, Multiplikation und Division erlaubt und die Ergebnisse im gleichen Körper darstellbar sind. Einige diesbezügliche Definitionen finden Sie im **Theorieteil.** Soviel vorneweg: Nicht alle der oben aufgelisteten Mengen sind Körper.

Daneben gibt es auch noch **endliche Körper** (englisch: *Finite Fields*), die in unserem Lerntutorial als **Galoisfeld** GF(P^m) bezeichnet werden, wobei

- $P \in N$ eine Primzahl angibt,
- und $m \in N$ eine natürliche Zahl bezeichnet.

Ist der Exponent $m \geq 2$, so spricht man von einem **Erweiterungskörper** (englisch: *Extension Field*). In dieser Aufgabe beschränken wir uns auf Erweiterungskörper zur Basis $P = 2$.

Die beiden ersten Teilaufgaben beziehen sich auf die Klassifizierung von Polynomen. Ein Grad–m–Polynom nennt man reduzibel im Körper K, wenn es in der Form

$$p(x) = \prod_{i=1}^{m} (x - x_i) = (x - x_1) \cdot (x - x_2) \cdot \ldots \cdot (x - x_m)$$

darstellbar ist und für alle Nullstellen $x_i \in K$ gilt. Ist dies nicht möglich, so spricht man von einem **irreduziblen Polynom**.

Gerolamo Cardano
(1501 – 1576)

Rafael Bambelli
(1526 – 1572)

Évariste Galois
(1811 – 1832)

Hinweis: Die Aufgabe bezieht sich auf die Thematik von **Kapitel 2.2.** Oben sehen Sie Abbildungen der italienischen Mathematiker **Gerolamo Cardano** sowie **Rafael Bombelli,** die erstmals imaginäre Zahlen zur Lösung algebraischer Gleichungen einführten, sowie von **Évariste Galois,** der schon in sehr jungen Jahren die Grundlagen der endlichen Körper geschaffen hat.

Fragebogen zu "Z2.4: Endliche und unendliche Körper"

a) Welche Polynome sind irreduzibel im reellen Körper?

- ☐ $p_1(x) = x^2 + 1$,
- ☐ $p_2(x) = x^2 - 1$,
- ☐ $p_3(x) = x^2 + x + 1$,
- ☐ $p_4(x) = x^2 + x - 2$.

b) Welche Polynome sind irreduzibel in GF(2)?

- ☐ $p_1(x) = x^2 + 1$,
- ☐ $p_2(x) = x^2 - 1$,
- ☐ $p_3(x) = x^2 + x + 1$,
- ☐ $p_4(x) = x^2 + x - 2$.

c) Bei welchen Mengen handelt es sich im algebraischen Sinne um Körper?

- ☐ die Menge N der natürlichen Zahlen,
- ☐ die Menge Z der ganzen Zahlen,
- ☐ die Menge Q der rationalen Zahlen,
- ☐ die Menge R der reellen Zahlen,
- ☐ die Menge C der komplexen Zahlen.

d) Welche Körper sind Teilmenge (Unterraum) eines anderen Körpers?

- ☐ $Q \subset C$,
- ☐ $C \subset R$,
- ☐ $\text{GF}(2) \subset \text{GF}(2^2)$,
- ☐ $\text{GF}(2^3) \subset \text{GF}(2^2)$.

e) Zwischen welchen Körpern bestehen gewisse Analogien?

- ☐ Menge Q der rationalen Zahlen und $\text{GF}(2^2)$,
- ☐ Menge C der komplexen Zahlen und $\text{GF}(2^2)$,

☐ Menge C der komplexen Zahlen und GF(2^3).

A2.5: Drei Varianten von GF(2^4)

Irreduzible und primitive Polynome haben große Bedeutung für die Beschreibung von Verfahren zur Fehlerkorrektur. In **[LN97]** findet man zum Beispiel die folgenden irreduziblen Polynome vom Grad $m = 4$:

- $p(x) = x^4 + x + 1$,
- $p(x) = x^4 + x^3 + 1$,
- $p(x) = x^4 + x^3 + x^2 + x + 1$.

Die beiden ersten Polynome sind auch primitiv. Dies erkennt man aus den Potenztabellen, die rechts angegeben sind – die untere Tabelle (B) allerdings nicht ganz vollständig. Aus beiden Tabellen erkennt man, dass alle Potenzen α^i für $1 \le i \le 14$ in der Polynomdarstellung ungleich 1 sind. Erst für $i = 15$ ergibt sich

$$\alpha^{15} = \alpha^0 = 1 \quad \Rightarrow \quad \text{Koeffizientenvektor } 0001\,.$$

Nicht angegeben wird, ob sich die rot hinterlegte Tabelle (A) aus dem Polynom $x^4 + x + 1$ oder aus $x^4 + x^3 + 1$ ergibt. Diese Zuordnungen sollen Sie in den Teilaufgaben (a) und (b) treffen. In der Teilaufgabe (c) sollen Sie zudem die fehlenden Potenzen α^5, α^6, α^7 und α^8 in der Tabelle (B) ergänzen.

Die Teilaufgabe (d) bezieht sich auf das ebenfalls irreduzible Polynom $p(x) = x^4 + x^3 + x^2 + x + 1$. Entsprechend den oben genannten Kriterien sollen Sie entscheiden, ob dieses Polynom primitiv ist oder nicht.

Hinweis: Die Aufgabe gehört ebenfalls zum Themengebiet von **Kapitel 2.2.**

Tabelle (A)

Potenz von α	Polynom in α	Vektor der Koeffizienten
$\alpha^{-\infty}=0$	0	0000
$\alpha^0=1$	1	0001
α^1	α	0010
α^2	α^2	0100
α^3	α^3	1000
α^4	$\alpha+1$	0011
α^5	$\alpha^2+\alpha$	0110
α^6	$\alpha^3+\alpha^2$	1100
α^7	$\alpha^3+\alpha+1$	1011
α^8	α^2+1	0101
α^9	$\alpha^3+\alpha$	1010
α^{10}	$\alpha^2+\alpha+1$	0111
α^{11}	$\alpha^3+\alpha^2+\alpha$	1110
α^{12}	$\alpha^3+\alpha^2+\alpha+1$	1111
α^{13}	$\alpha^3+\alpha^2+1$	1101
α^{14}	α^3+1	1001
α^{15}	1	0001

Tabelle (B)

Potenz von α	Polynom in α	Vektor der Koeffizienten
$\alpha^{-\infty}=0$	0	0000
$\alpha^0=1$	1	0001
α^1	α	0010
α^2	α^2	0100
α^3	α^3	1000
α^4	α^3+1	1001
α^5	????	????
α^6	????	????
α^7	????	????
α^8	????	????
α^9	α^2+1	0101
α^{10}	$\alpha^3+\alpha$	1010
α^{11}	$\alpha^3+\alpha^2+1$	1101
α^{12}	$\alpha+1$	0011
α^{13}	$\alpha^2+\alpha$	0110
α^{14}	$\alpha^3+\alpha^2$	1100
α^{15}	1	0001

Fragebogen zu "A2.5: Drei Varianten von GF(2^4)"

a) Welches Polynom liegt der Tabelle (A) zugrunde?

- ○ $p(x) = x^4 + x + 1$,
- ○ $p(x) = x^4 + x^3 + 1$.

b) Welches Polynom liegt der Tabelle (B) zugrunde?

- ○ $p(x) = x^4 + x + 1$,
- ○ $p(x) = x^4 + x^3 + 1$.

c) Berechnen Sie die in der Tabelle (B) fehlenden Einträge. Welche der folgenden Angaben sind richtig?

- ☐ $\alpha^5 = \alpha^3 + \alpha + 1 \Rightarrow$ Koeffizientenvektor „1011”,
- ☐ $\alpha^6 = \alpha^2 + 1 \Rightarrow$ Koeffizientenvektor „0111”,
- ☐ $\alpha^7 = \alpha^3 + \alpha^2 + \alpha + 1 \Rightarrow$ Koeffizientenvektor „1111”,
- ☐ $\alpha^8 = \alpha^3 + \alpha^2 + \alpha \Rightarrow$ Koeffizientenvektor „1110”.

d) Ist $p(x) = x^4 + x^3 + x^2 + x + 1$ ein primitives Polynom? Klären Sie diese Frage anhand der Potenzen α^i (i soweit erforderlich).

- ○ Ja.
- ○ Nein.

Z2.5: Einige Berechnungen über GF(2^3)

Elemente von GF(2^3) als		
Potenzen von α	Polynome in α	Vektoren der Koeffizienten
$\alpha^{-\infty}=0$	0	0 0 0
$\alpha^0=1$	1	0 0 1
α^1	α	0 1 0
α^2	α^2	1 0 0
α^3	$\alpha+1$	0 1 1
α^4	$\alpha^2+\alpha$	1 1 0
α^5	$\alpha^2+\alpha+1$	1 1 1
α^6	α^2+1	1 0 1
α^7	1	0 0 1

Wir betrachten nun den Erweiterungskörper (englisch: *Extension Field*) mit den acht Elementen ⇒ GF(2^3) entsprechend der nebenstehenden Tabelle. Da das zugrunde liegende Polynom

$$p(x) = x^3 + x + 1$$

sowohl irreduzibel als auch primitiv ist, kann das vorliegende Galoisfeld in folgender Form angegeben werden:

$$\mathrm{GF}(2^3) = \{\, 0,\ 1,\ \alpha,\ \alpha^2,\ \alpha^3,\ \alpha^4,\ \alpha^5,\ \alpha^6 \,\}.$$

Das Element α ergibt sich dabei als Lösung der Gleichung $p(\alpha) = 0$ im Galoisfeld GF(2). Damit erhält man folgende Nebenbedingung:

$$\alpha^3 + \alpha + 1 = 0 \quad \Rightarrow \quad \alpha^3 = \alpha + 1\,.$$

Für die weiteren Elemente gelten folgende Berechnungen:

$$\begin{aligned}
\alpha^4 &= \alpha \cdot \alpha^3 = \alpha \cdot (\alpha + 1) = \alpha^2 + \alpha\,,\\
\alpha^5 &= \alpha \cdot \alpha^4 = \alpha \cdot (\alpha^2 + \alpha) = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1\,,\\
\alpha^6 &= \alpha \cdot \alpha^5 = \alpha \cdot (\alpha^2 + \alpha + 1) = \alpha^3 + \alpha^2 + \alpha = \alpha + 1 + \alpha^2 + \alpha = \alpha^2 + 1\,.
\end{aligned}$$

In dieser Aufgabe sollen Sie einige algebraische Umformungen in diesem Galoisfeld GF(2^3) vornehmen. Unter anderem ist gefragt nach der multiplikativen Inversen des Elementes α^4. Dann muss gelten:

$$\alpha^4 \cdot \mathrm{Inv_M}(\alpha^4) = 1\,.$$

Hinweis: Die Aufgabe bezieht sich auf das **Kapitel 2.2** und ist als Ergänzung zur etwas schwierigeren **Aufgabe A2.5** gedacht.

Fragebogen zu "Z2.5: Einige Berechnungen über GF(2^3)"

a) Welche der Aussagen treffen für die höheren Potenzen von α zu ($i \geq 7$)?

- ☐ $\alpha^7 = 1$,
- ☐ $\alpha^8 = \alpha$,
- ☐ $\alpha^{13} = \alpha^2 + 1$,
- ☐ $\alpha^i = \alpha^{i \bmod 7}$.

b) Welche Umformung ist für $A = \alpha^8 + \alpha^6 - \alpha^2 + 1$ zulässig?

- ☐ $A = 1$,
- ☐ $A = \alpha$,
- ☐ $A = \alpha^2$,
- ☐ $A = \alpha^3$,
- ☐ $A = \alpha^4$.

c) Welche Umformung ist für $B = \alpha^{16} - \alpha^{12} \cdot \alpha^3$ zulässig?

- ☐ $B = 1$,
- ☐ $B = \alpha$,
- ☐ $B = \alpha^2$,
- ☐ $B = \alpha^3$,
- ☐ $B = \alpha^4$.

d) Welche Umformung ist für $C = \alpha^3 + \alpha$ zulässig?

- ☐ $C = 1$,
- ☐ $C = \alpha$,
- ☐ $C = \alpha^2$,
- ☐ $C = \alpha^3$,
- ☐ $C = \alpha^4$.

e) Welche Umformung ist für $D = \alpha^4 + \alpha$ zulässig?

- ☐ $D = 1$,

- ☐ $D = \alpha$,
- ☐ $D = \alpha^2$,
- ☐ $D = \alpha^3$,
- ☐ $D = \alpha^4$.

f) Welche Umformung ist für $E = A \cdot B \cdot C/D$ zulässig?

- ☐ $E = 1$,
- ☐ $E = \alpha$,
- ☐ $E = \alpha^2$,
- ☐ $E = \alpha^3$,
- ☐ $E = \alpha^4$.

g) Welche Aussagen gelten für die multiplikative Inverse zu $\alpha^2 + \alpha$?

- ☐ $\text{Inv}_\text{M}(\alpha^2 + \alpha) = 1$,
- ☐ $\text{Inv}_\text{M}(\alpha^2 + \alpha) = \alpha + 1$,
- ☐ $\text{Inv}_\text{M}(\alpha^2 + \alpha) = \alpha^3$,
- ☐ $\text{Inv}_\text{M}(\alpha^2 + \alpha) = \alpha^4$.

A2.6: GF(P^m). Welches P, welches m?

+	z_0 00	z_1 01	z_2 02	z_3 10	z_4 11	z_5 12	z_6 20	z_7 21	z_8 22
00	00	01	02	10	11	12	20	21	22
01	01	02	00	11	12	10	21	22	20
02	02	00	01	12	10	11	22	20	21
10	10	11	12	20	21	22	00	01	02
11	11	12	10	21	22	20	01	02	00
12	12	10	11	22	20	21	02	00	01
20	20	21	22	00	01	02	10	11	12
21	21	22	20	01	02	00	11	12	10
22	22	20	21	02	00	01	12	10	11

·	z_0 00	z_1 01	z_2 02	z_3 10	z_4 11	z_5 12	z_6 20	z_7 21	z_8 22
00	00	00	00	00	00	00	00	00	00
01	00	01	02	10	11	12	20	21	22
02	00	02	01	20	22	21	10	12	11
10	00	10	20	11	21	01	22	02	12
11	00	11	22	21	02	10	12	20	01
12	00	12	21	01	10	22	02	11	20
20	00	20	10	22	12	02	11	01	21
21	00	21	12	02	20	11	01	22	10
22	00	22	11	12	01	20	21	10	02

Es soll ein Galoisfeld GF(q) mit $q = P^m$ Elementen analysiert werden, das durch die nebenstehenden Tabellen für Addition (gekennzeichnet mit „+”) und Multiplikation (gekennzeichnet mit „·”) vorgegeben ist. Dieses Galoisfeld

$$\mathrm{GF}(q) = \{\, z_0,\ z_1,\ \ldots,\ z_{q-1} \}$$

erfüllt alle Anforderungen an einen endlichen Körper, die im **Kapitel 2.1** aufgeführt sind. Kommutativ–, Assoziativ– und Distributivgesetz werden erfüllt. Weiterhin gibt es

- ein neutrales Element hinsichtlich Addition $\Rightarrow N_\mathrm{A}$:

$$\exists\ z_j \in \mathrm{GF}(q): \quad z_i + z_j = z_i$$
$$\Rightarrow \quad z_j = N_\mathrm{A} = \text{”0”} \quad (\text{Nullelement}),$$

- ein neutrales Element hinsichtlich Multiplikation $\Rightarrow N_\mathrm{M}$:

$$\exists\ z_j \in \mathrm{GF}(q): \quad z_i \cdot z_j = z_i$$
$$\Rightarrow \quad z_j = N_\mathrm{M} = \text{”1”} \quad (\text{Einselement}),$$

- für alle Elemente z_i eine additive Inverse $\Rightarrow$ $\mathrm{Inv_A}(z_i)$:

$$\forall\ z_i \in \mathrm{GF}(q)\ \exists\ \mathrm{Inv_A}(z_i) \in \mathrm{GF}(q):$$
$$z_i + \mathrm{Inv_A}(z_i) = N_\mathrm{A} = \text{”0”} \quad \Rightarrow \quad \text{kurz}: \mathrm{Inv_A}(z_i) = -z_i,$$

- für alle Elemente z_i mit Ausnahme des Nullelements eine multiplikative Inverse $\Rightarrow$ $\mathrm{Inv_M}(z_i)$:

$$\forall\ z_i \in \mathrm{GF}(q),\ z_i \neq N_\mathrm{A}\ \exists\ \mathrm{Inv_M}(z_i) \in \mathrm{GF}(q):$$
$$z_i \cdot \mathrm{Inv_M}(z_i) = N_\mathrm{M} = \text{”1”} \quad \Rightarrow \quad \text{kurz}: \mathrm{Inv_M}(z_i) = z_i^{-1}.$$

Hinweis: Die Aufgabe bezieht sich auf das **Kapitel 2.2.** In den Tabellen sind die Elemente z_0, ... , z_8 als Koeffizientenvektoren bezeichnet. So steht zum Beispiel „21” für die ausführliche Schreibweise $2 \cdot \alpha + 1$.

Fragebogen zu "A2.6: GF(P^m). Welches P, welches m?"

a) Geben Sie die Parameter des hier betrachteten Galoisfeldes an.

$\boldsymbol{P}$ =

$\boldsymbol{m}$ =

$\boldsymbol{q}$ =

b) Wie lautet das neutrale Element für die Addition?

- ☐ Das neutrale Element der Addition ist N_A = „00”,
- ☐ Das neutrale Element der Addition ist N_A = „01”,

c) Wie lautet das neutrale Element für die Multiplikation?

- ☐ Das neutrale Element der Multiplikation ist N_M = „00”,
- ☐ Das neutrale Element der Multipliaktion ist N_M = „01”,

d) Welche Aussagen gelten hinsichtlich der additiven Inversen?

- ☐ Es gilt Inv_A („02”) = „01”,
- ☐ Es gilt Inv_A („11”) = „22”,
- ☐ Es gilt Inv_A („22”) = „00”.

e) Welche der folgenden Aussagen treffen für die Multiplikation zu?

- ☐ Die Multiplikation erfolgt modulo $p(\alpha) = \alpha^2 + 2$.
- ☐ Die Multiplikation erfolgt modulo $p(\alpha) = \alpha^2 + 2\alpha + 2$.

f) Welche Aussagen gelten hinsichtlich der multiplikativen Inversen?

- ☐ Es gibt für alle Elemente $z_i \in \text{GF}(P^m)$ eine multiplikative Inverse.
- ☐ Es gilt Inv_M(„12”) = „10”.
- ☐ Es gilt Inv_M(„21”) = „12”.

g) Gilt („20” + „12”) · („12”) = „20” · „12” + „12” · „12”?

- ○ Ja,
- ○ Nein.