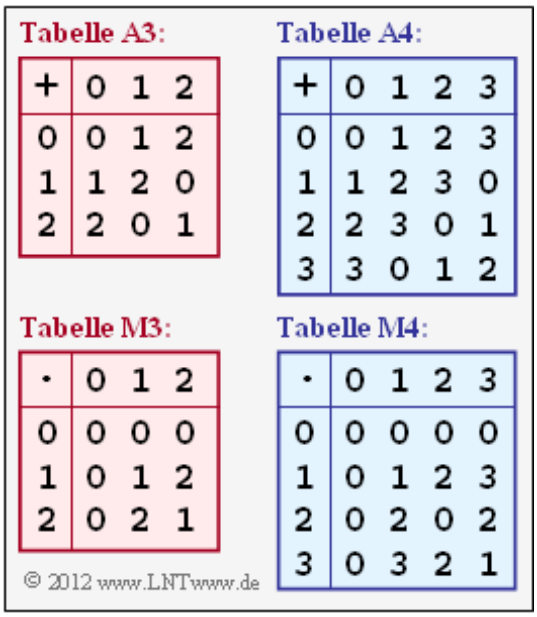
A2.1: Gruppe, Ring, Körper



Im Theorieteil zu diesem Kapitel 2.1 wurden verschiedene algebraische Begriffe definiert. Für das Folgende setzen wir voraus, dass alle Mengen aus jeweils q Elementen bestehen, wobei hier entweder $q = 3$ oder $q = 4$ gelten soll. Dann gilt:

- Eine **algebraische Gruppe** ist eine endliche Menge $G = \{0, 1, \text{...} , q–1\}$ zusammen mit einer zwischen allen Elementen definierten Verknüpfungsvorschrift. Eine additive Gruppe wird mit $(G, +)$ bezeichnet, eine multiplikative mit $(G, \cdot)$.
- Ein **algebraischer Ring** kennzeichnet eine Menge $R = \{0, 1, \text{...} , q–1\}$ zusammen mit zwei darin definierten Rechenoperationen, nämlich der Addition („+") und der Multiplikation („·").
- Ein **algebraischer Körper** ist ein Ring, bei dem zusätzlich die Division erlaubt ist und stets das Kommutativgesetz erfüllt wird.

Da wir hier ausschließlich endliche Mengen betrachten, ist ein Körper (englisch: *Field*) gleichzeitig ein Galoisfeld GF(q) der Ordnung q.

Eine wesentliche Eigenschaft des Galoisfeldes

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

ist, dass es mindestens ein primitives Element besitzt. Ein Element $z_i \neq 0$ bezeichnet man als primitiv, wenn die folgende Bedingung erfüllt ist (k ganzzahlig).

$$z_i^k \bmod q = \begin{cases} \neq 1 & \text{für } 1 \le k < q-1 \\ 1 & \text{für } k = q-1 \end{cases} \quad \Rightarrow \quad z_i \text{ ist ein primitives Element.}$$

Nur bei einem primitiven Element z_i ergeben sich durch die Rechenoperation z_i^k (mit $k = 1, 2, 3, \text{...}$) alle Elemente des Galoisfeldes mit Ausnahme des Nullelementes $z_0 = 0$.

Hinweis: Die Aufgabe behandelt das Themengebiet von **Kapitel 2.1.** Beachten Sie, dass bei Gruppe, Ring und Körper mit jeweils q Elementen die Rechenoperationen „+" und „·" jeweils modulo q zu verstehen sind.

Fragebogen zu "A2.1: Gruppe, Ring, Körper"

a) Welche der angegebenen Tabellen beschreiben eine Gruppe?

- ☐ Tabelle A3,
- ☐ Tabelle M3,
- ☐ Tabelle A3 und Tabelle M3 gemeinsam,
- ☐ Tabelle A4 und Tabelle M4 gemeinsam.

b) Welche der angegebenen Tabellen beschreiben einen Ring?

- ☐ Tabelle A3,
- ☐ Tabelle M3,
- ☐ Tabelle A3 und Tabelle M3 gemeinsam,
- ☐ Tabelle A4 und Tabelle M4 gemeinsam,
- ☐ Tabelle A3 und Tabelle M4 gemeinsam.

c) Welche der Tabellen beschreiben einen Körper bzw. ein Galoisfeld?

- ☐ Tabelle A3,
- ☐ Tabelle M3,
- ☐ Tabelle A3 und Tabelle M3 gemeinsam,
- ☐ Tabelle A4 und Tabelle M4 gemeinsam.

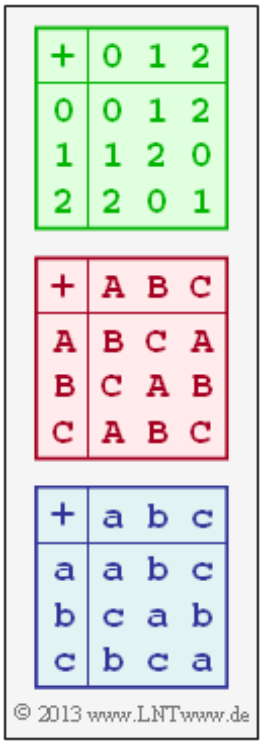
d) Welche Elemente der Menge $\{0, 1, 2\}$ $\Rightarrow$ $q = 3$ sind primitiv?

- ☐ $z_0 = 0$,
- ☐ $z_1 = 1$,
- ☐ $z_2 = 2$.

e) Welche Elemente der Menge $\{0, 1, 2, 3\}$ $\Rightarrow$ $q = 4$ sind primitiv?

- ☐ $z_0 = 0$,
- ☐ $z_1 = 1$,
- ☐ $z_2 = 2$,
- ☐ $z_3 = 3$.

Z2.1: Welche Tabellen beschreiben Gruppen?



In dieser Aufgabe betrachten wir Mengen mit jeweils drei Elementen, allgemein bezeichnet mit $\{z_0, z_1, z_2\}$. Die Elemente können dabei sein:

- Zahlen, beispielsweise $z_0 = 0$, $z_1 = 1$, $z_2 = 2$,
- algebraische Ausdrücke wie $z_0 = A$, $z_1 = B$, $z_2 = C$,
- irgendwas, beispielsweise z_0 = „Apfel”, z_1 = „Birne”, z_2 = „Citrone”.

Eine Gruppe (G, „+”) hinsichtlich der Addition ergibt sich dann, wenn durch eine Tabelle die „+”–Verknüpfung zwischen je zwei Elementen so definiert wurde, dass folgende Bedingungen erfüllt sind (die Laufvariablen i, j, k können dabei jeweils die Werte 0, 1, 2 annehmen):

- Für alle $z_i \in G$ und $z_j \in G$ gilt $(z_i + z_j) \in G$ $\Rightarrow$ **Closure–Kriterium**. Die Bedingung muss auch für $i = j$ erfüllt sein.
- Für alle z_i, z_j, z_k gilt $(z_i + z_j) + z_k = z_i + (z_j + z_k)$ $\Rightarrow$ **Assoziativgesetz**.
- Es gibt ein **hinsichtlich Addition neutrales Element** $N_{\rm A} \in G$, so dass für alle $z_i \in G$ gilt: $z_i + N_{\rm A} = z_i$.
- Für alle $z_i \in G$ gibt es ein **hinsichtlich Addition inverses Element** $\text{Inv}_{\rm A}(z_i) \in G$, so dass für die Summe $z_i + \text{Inv}_{\rm A}(z_i) = N_{\rm A}$ gilt.

Wird zudem für alle $z_i \in G$ und $z_j \in G$ zusätzlich noch das **Kommutativgesetz** $\Rightarrow$ $z_i + z_j = z_j + z_i$ erfüllt, so spricht man von einer kommutativen Gruppe oder – nach dem norwegischen Mathematiker **Niels Hendrik Abel** – von einer **abelschen Gruppe**.

Die Zahlenmenge {0, 1, 2} ist eine abelsche (kommutative) Gruppe. Entsprechend der grün umrandeten Additionstabelle in obiger Grafik ist hier die Addition modulo 3 zu verstehen. Somit ist auch die Summe stets 0, 1 oder 2. Das neutrale Element ist $N_{\rm A} = 0$ und das zu z_i inverse Element $\text{Inv}_{\rm A}(z_i) = -z_i$:

$$\text{Inv}_{\rm A}(0) = 0,\ \text{Inv}_{\rm A}(1) = (-1)\ \text{mod}\ 3 = 2,\ \text{Inv}_{\rm A}(2) = (-2)\ \text{mod}\ 3 = 1\,.$$

In dieser Aufgabe sollen Sie überprüfen, ob auch die beiden weiteren in der obigen Grafik dargestellten Additionstabellen jeweils zu einer algebraischen Gruppe gehören.

Hinweis: Die Aufgabe bezieht sich auf die Seite **Algebraische Gruppe und Beispiele** im **Kapitel 2.1.**

Fragebogen zu "Z2.1: Welche Tabellen beschreiben Gruppen?"

a) Welche Aussagen ergeben sich aus der rot umrandeten Additionstabelle?

- ☐ Das neutrale Element ist N_A = C.
- ☐ Die Inversen sind $\text{Inv}_A(A) = B$, $\text{Inv}_A(B) = A$, $\text{Inv}_A(C) = C$.
- ☐ Es handelt sich hier um eine additive Gruppe $(G, +)$.
- ☐ Auch die Bedingung einer abelschen Gruppe wird erfüllt.

b) Ändert sich etwas gegenüber Teilaufgabe a), wenn die Elemente A, B, C nun für „Apfel", „Birne" und „Citrone" stehen?

- ○ Ja.
- ○ Nein.

c) Welche Aussagen ergeben sich aus der blau umrandeten Additionstabelle?

- ☐ Das neutrale Element ist N_A = a.
- ☐ Die additiven Inversen sind $\text{Inv}_A(a) = a$, $\text{Inv}_A(b) = b$, $\text{Inv}_A(c) = c$.
- ☐ Es handelt sich um eine abelsche Gruppe.

A2.2: Eigenschaften von Galoisfeldern

Wir betrachten hier die Zahlenmengen

- $Z_5 = \{0, 1, 2, 3, 4\} \Rightarrow q = 5$,
- $Z_6 = \{0, 1, 2, 3, 4, 5\} \Rightarrow q = 6$.

In nebenstehender Grafik sind die (teilweise unvollständigen) Additions– und Multiplikationstabellen für $q = 5$ und für $q = 6$ angegeben, wobei sowohl die Addition („+") als auch die Multiplikation („·") modulo q zu verstehen sind.

Zu überprüfen ist, ob die Zahlenmengen Z_5 und Z_6 alle Bedingungen eines Galoisfeldes GF(5) bzw. GF(6) erfüllen. Im **Theorieteil** werden insgesamt acht Bedingungen genannt, die alle erfüllt sein müssen. Von ihnen überprüft werden sollen nur zwei dieser Bedingungen:

(D) Für alle Elemente gibt es eine **additive Inverse** (*Inverse for* „+"):

$$\forall\ z_i \in \mathrm{GF}(q),\ \exists\ \mathrm{Inv_A}(z_i) \in \mathrm{GF}(q):$$
$$z_i + \mathrm{Inv_A}(z_i) = 0 \quad \Rightarrow \quad \mathrm{Inv_A}(z_i) = -z_i.$$

(E) Alle Elemente haben eine **multiplikative Inverse** (*Inverse for* „·"):

$$\forall\ z_i \in \mathrm{GF}(q),\ z_i \neq 0,\ \exists\ \mathrm{Inv_M}(z_i) \in \mathrm{GF}(q):$$
$$z_i \cdot \mathrm{Inv_M}(z_i) = 1 \quad \Rightarrow \quad \mathrm{Inv_M}(z_i) = z_i^{-1}.$$

Die weiteren Bedingungen für ein Galoisfeld, nämlich

- Closure,
- Existenz von Null– und Einselement,
- Gültigkeit von Kommutativ–, Assoziativ– und Distributivgesetz

werden sowohl von Z_5 als auch von Z_6 erfüllt.

Hinweis: Die Aufgabe bezieht sich auf das **Kapitel 2.1.**

Operationen für $q = 5$:

+	0	1	2	3	4
0	0	1	2	3	A_{04}
1	1	2	3	4	A_{14}
2	2	3	4	0	A_{24}
3	3	4	0	1	A_{34}
4	4	0	1	2	A_{44}

·	0	1	2	3	4
0	0	0	0	0	M_{04}
1	0	1	2	3	M_{14}
2	0	2	4	1	M_{24}
3	0	3	1	4	M_{34}
4	0	4	3	2	M_{44}

Operationen für $q = 6$:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	0	1
2	2	3	4	0	1	2
3	3	4	0	1	2	3
4	4	0	1	2	3	4
5	5	4	0	1	2	3

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

© 2013 www.LNTwww.de

Fragebogen zu "A2.2: Eigenschaften von Galoisfeldern"

a) Ergänzen Sie die Additionstabelle für $q = 5$. Geben Sie folgende Werte ein:

$$A_{04} =$$

$$A_{14} =$$

$$A_{44} =$$

b) Ergänzen Sie die Multiplikationstabelle für $q = 5$. Geben Sie folgende Werte ein:

$$M_{04} =$$

$$M_{14} =$$

$$M_{44} =$$

c) Erfüllt die Menge Z_5 die Bedingungen eines Galoisfeldes?

- ☐ Ja.
- ☐ Nein, es gibt nicht für alle Elemente (0 – 4) eine additive Inverse.
- ☐ Nein, die Elemente 1–4 haben nicht alle eine multiplikative Inverse.

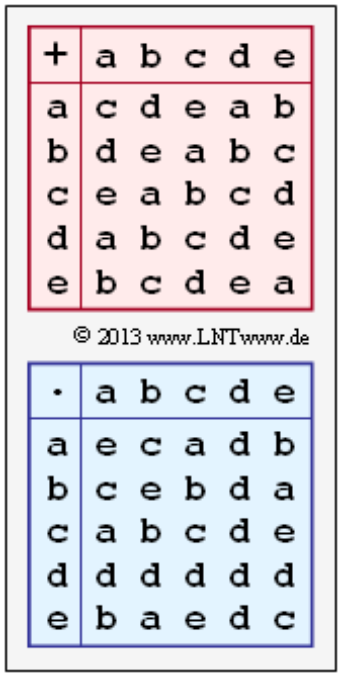
d) Erfüllt die Menge Z_6 die Bedingungen eines Galoisfeldes?

- ☐ Ja.
- ☐ Nein, es gibt nicht für alle Elemente (0 – 5) eine additive Inverse.
- ☐ Nein, die Elemente 1–5 haben nicht alle eine multiplikative Inverse.

e) Die Zahlenmengen Z_2, Z_3, Z_5 und Z_7 ergeben ein Galoisfeld, die Mengen Z_4, Z_6, Z_8, Z_9 dagegen nicht. Was folgern Sie daraus?

- ☐ $Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ ist ein Galoisfeld?
- ☐ $Z_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ ist ein Galoisfeld?
- ☐ $Z_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ ist ein Galoisfeld?

Z2.2: Galoisfeld GF(5)



+	a	b	c	d	e
a	c	d	e	a	b
b	d	e	a	b	c
c	e	a	b	c	d
d	a	b	c	d	e
e	b	c	d	e	a

© 2013 www.LNTwww.de

·	a	b	c	d	e
a	e	c	a	d	b
b	c	e	b	d	a
c	a	b	c	d	e
d	d	d	d	d	d
e	b	a	e	d	c

Wie in **Aufgabe A2.2** betrachten wir einen endlichen Körper der Ordnung $q = 5$ und damit das Galoisfeld

$$\mathrm{GF}(5) = \{a, b, c, d, e\}.$$

Über die Elemente werden weiter keine Aussagen getroffen. Es können sowohl ganze Zahlen sein oder irgendwelche mathematische Ausdrücke. Das Galoisfeld wird ausschließlich bestimmt durch

- eine Additionstabelle modulo 5,
- eine Multiplikationstabelle modulo 5.

Die wichtigsten Eigenschaften eines Galoisfeldes sind auf **Theorieseite 1** zusammengestellt. In dieser Aufgabe wird Bezug genommen auf

- das Kommutativ– und das Distributivgesetz,
- die neutralen Elemente von Addition und Multiplikation,
- die inversen Elemente von Addition und Multiplikation, sowie
- die Bestimmung primitiver Elemente.

Im vorliegenden Beispiel wäre β ein primitives Element, wenn β^2, β^3 und β^4 (allgemein: β^{q-1}) die übrigen Elemente des Galoisfeldes GF(5) mit Ausnahme des Nullelementes ergeben.

Hinweis: Die Aufgabe bezieht sich auf das Themengebiet von **Kapitel 2.1.**

Fragebogen zu "Z2.2: Galoisfeld GF(5)"

a) Bestimmen Sie das neutrale Element der Addition.

- ☐ $N_A = a$,
- ☐ $N_A = b$,
- ☐ $N_A = c$,
- ☐ $N_A = d$,
- ☐ $N_A = e$.

b) Bestimmen Sie das neutrale Element der Multiplikation.

- ☐ $N_M = a$,
- ☐ $N_M = b$,
- ☐ $N_M = c$,
- ☐ $N_M = d$,
- ☐ $N_M = e$.

c) Ist das Kommutativgesetz erfüllt,

- ☐ hinsichtlich Addition, z.B. $a + b = b + a$, ... , $d + e = e + d$,
- ☐ hinsichtlich Multiplikation, z.B. $a \cdot b = b \cdot a$, ... , $d \cdot e = e \cdot d$.

d) Für welche Ausdrücke ist das Distributivgesetz erfüllt?

- ☐ $a \cdot (b + c) = a \cdot b + a \cdot c$,
- ☐ $d \cdot (b + c) = d \cdot b + d \cdot c$,
- ☐ $e \cdot (a + b) = e \cdot a + e \cdot b$.

e) Ersetzen Sie a, b, c, d, e durch Elemente der Zahlenmenge {0, 1, 2, 3, 4}, so dass sich gleiche Operationstabellen ergeben.

$\boldsymbol{a}$ =

$\boldsymbol{b}$ =

$\boldsymbol{c}$ =

$\boldsymbol{d}$ =

$\boldsymbol{e}$ =

f) Welche Aussagen gelten hinsichtlich der inversen Elemente?

- ☐ Für alle $z_i \in \{0, 1, 2, 3, 4\}$ gibt es eine additive Inverse.
- ☐ Nur für $z_i \in \{1, 2, 3, 4\}$ gibt es eine additive Inverse.
- ☐ Für alle $z_i \in \{0, 1, 2, 3, 4\}$ gibt es eine multiplikative Inverse.
- ☐ Nur für $z_i \in \{1, 2, 3, 4\}$ gibt es eine multiplikative Inverse.

g) Welche der Elemente sind primitiv?

- ☐ $a = 3$,
- ☐ $b = 2$,
- ☐ $e = 4$.