

Diskrete Mathematik

Sebastian Iwanowski
FH Wedel

Kap. 5: Algebraische Strukturen

Referenzen zum Nacharbeiten:

Biggs 20, 22, 23

Kurzweil (deutschsprachige Vertiefung, insb. für Endliche Körper)

Hachenberger 10 (Vertiefung für Polynome)

Teschl 3.2, 4

5. Algebraische Strukturen für Zahlenmengen

5.1 Gruppen

Definition der Struktur einer Gruppe:

Sei G eine nichtleere Menge und $\oplus$ eine Verknüpfung zwischen den Elementen von G .
Dann heißt die Struktur $(G, \oplus)$ eine **abelsche Gruppe**, wenn folgende Eigenschaften erfüllt sind:

1) $\forall a, b \in G: a \oplus b \in G$

innere Verknüpfung

2) $\forall a, b, c \in G: (a \oplus b) \oplus c = a \oplus (b \oplus c)$

Assoziativgesetz

3) $\exists e \in G \forall a \in G: e \oplus a = a \oplus e = a$

Neutrales Element

4) $\forall a \in G \exists a^{-1} \in G: a^{-1} \oplus a = a \oplus a^{-1} = e$

Inverses Element

5) $\forall a, b \in G: a \oplus b = b \oplus a$

Kommutativgesetz

nur Eigenschaft 1):	Gruppoid
nur Eigenschaft 1), 2):	Halbgruppe
nur Eigenschaft 1), 2), 3), 4):	Gruppe

Vorbilder: $(\mathbb{Z}, +)$ für eine unendliche Gruppe $(\mathbb{Z}_n, +)$ für eine endliche Gruppe

5. Algebraische Strukturen für Zahlenmengen

5.1 Gruppen

Beispiele für oder gegen unendliche Gruppen bzw. Unterstrukturen:

- | | |
|---|---|
| 1) $(\mathbb{N}, +)$ | 11) $(\{f: \mathbb{R} \rightarrow \mathbb{R}\}, \cdot)$ |
| 2) $(\mathbb{Z}, +)$ | 12) $(\{f: \mathbb{R} \setminus \{0\} \rightarrow \mathbb{R} \setminus \{0\}\}, \cdot)$ |
| 3) $(\mathbb{Z}, \cdot)$ | 13) $(\{f: \mathbb{R}^+ \rightarrow \mathbb{R}^+\}, \cdot)$ |
| 4) $(\mathbb{Q}, +)$ | 14) $(\{f: \mathbb{R} \rightarrow \mathbb{R}\}, \circ)$ |
| 5) $(\mathbb{Q}, \cdot)$ | 15) $(\{f: \mathbb{R} \rightarrow \mathbb{R}, f \text{ bijektiv}\}, \circ)$ |
| 6) $(\mathbb{Q} \setminus \{0\}, \cdot)$ | 16) $(\{f: \mathbb{R} \rightarrow \mathbb{R}, f \text{ differenzierbar}\}, \circ)$ |
| 7) $(\mathbb{Q}^+, \cdot)$ | 17) $(\{f: \mathbb{R} \rightarrow \mathbb{R}, f \text{ bijektiv und differenzierbar}\}, \circ)$ |
| 8) $(\mathbb{R} \setminus \{0\}, \cdot)$ | 18) $(\{f: \mathbb{R} \rightarrow \mathbb{R}, f \text{ linear}\}, \circ)$ |
| 9) $(\mathbb{R} \setminus \{0\}, +)$ | 19) $(\{f: \mathbb{R} \rightarrow \mathbb{R}, f \text{ linear}\}, +)$ |
| 10) $(\{f: \mathbb{R} \rightarrow \mathbb{R}\}, +)$ | 20) $(\{f: \mathbb{R} \rightarrow \mathbb{R}, f \text{ Polynomfunktion}\}, +)$ |

5. Algebraische Strukturen für Zahlenmengen

5.1 Gruppen

Beispiele für endliche Gruppen bzw. Halbgruppen:

1) $(\mathbb{Z}_n, +)$

(zyklische Gruppe mit additiver Verknüpfung)

2) $(\mathbb{Z}_n, \cdot)$

3) $(\mathbb{Z}_n \setminus \{[0]_n\}, \cdot)$

4) $(\mathbb{Z}_n^*, \cdot)$ *(multiplikative Gruppe der zu n teilerfremden Restklassen, prime Restklassengruppe mod n)*

$\odot$	$[1]_8$	$[3]_8$	$[5]_8$	$[7]_8$
$(\mathbb{Z}_8^*, \odot)$:	$[1]_8$	$[3]_8$	$[5]_8$	$[7]_8$
$[3]_8$	$[3]_8$	$[1]_8$	$[7]_8$	$[5]_8$
$[5]_8$	$[5]_8$	$[7]_8$	$[1]_8$	$[3]_8$
$[7]_8$	$[7]_8$	$[5]_8$	$[3]_8$	$[1]_8$

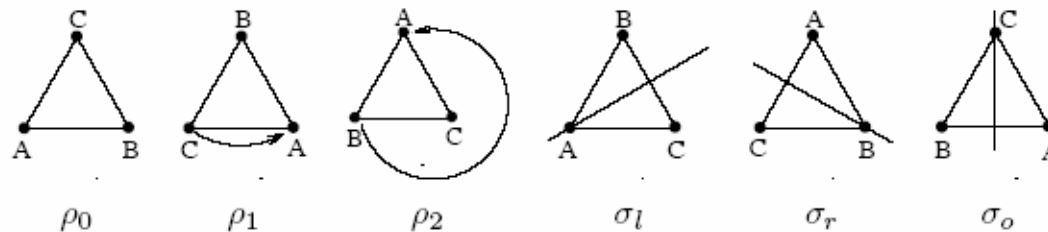
$\odot$	$[1]_{10}$	$[3]_{10}$	$[7]_{10}$	$[9]_{10}$
$(\mathbb{Z}_{10}^*, \odot)$:	$[1]_{10}$	$[3]_{10}$	$[7]_{10}$	$[9]_{10}$
$[3]_{10}$	$[3]_{10}$	$[9]_{10}$	$[1]_{10}$	$[7]_{10}$
$[7]_{10}$	$[7]_{10}$	$[1]_{10}$	$[9]_{10}$	$[3]_{10}$
$[9]_{10}$	$[9]_{10}$	$[7]_{10}$	$[3]_{10}$	$[1]_{10}$

5. Algebraische Strukturen für Zahlenmengen

5.1 Gruppen

Beispiele für endliche Gruppen bzw. Halbgruppen:

5) Symmetriegruppe eines gleichseitigen Dreiecks



$(S_3, \circ)$:

$\circ$	ρ_0	ρ_1	ρ_2	σ_l	σ_r	σ_o
ρ_0	ρ_0	ρ_1	ρ_2	σ_l	σ_r	σ_o
ρ_1	ρ_1	ρ_2	ρ_0	σ_o	σ_l	σ_r
ρ_2	ρ_2	ρ_0	ρ_1	σ_r	σ_o	σ_l
σ_l	σ_l	σ_r	σ_o	ρ_0	ρ_1	ρ_2
σ_r	σ_r	σ_o	σ_l	ρ_2	ρ_0	ρ_1
σ_o	σ_o	σ_l	σ_r	ρ_1	ρ_2	ρ_0

5. Algebraische Strukturen für Zahlenmengen

5.1 Gruppen

Beispiele für endliche Gruppen bzw. Halbgruppen:

6) $(\{x, \frac{1}{x}, 1-x, \frac{x-1}{x}, \frac{1}{1-x}, \frac{x}{x-1}\}, \circ)$ (Hintereinanderschaltung der Funktionen)

$(\mathbb{Q}_6, \circ)$:

$\circ$	x	$\frac{1}{x}$	$1-x$	$\frac{x-1}{x}$	$\frac{1}{1-x}$	$\frac{x}{x-1}$
x	x	$\frac{1}{x}$	$1-x$	$\frac{x-1}{x}$	$\frac{1}{1-x}$	$\frac{x}{x-1}$
$\frac{1}{x}$	$\frac{1}{x}$	x	$\frac{1}{1-x}$	$\frac{x}{x-1}$	$1-x$	$\frac{x-1}{x}$
$1-x$	$1-x$	$\frac{x-1}{x}$	x	$\frac{1}{x}$	$\frac{x}{x-1}$	$\frac{1}{1-x}$
$\frac{x-1}{x}$	$\frac{x-1}{x}$	$1-x$	$\frac{x}{x-1}$	$\frac{1}{1-x}$	x	$\frac{1}{x}$
$\frac{1}{1-x}$	$\frac{1}{1-x}$	$\frac{x}{x-1}$	$\frac{1}{x}$	x	$\frac{x-1}{x}$	$1-x$
$\frac{x}{x-1}$	$\frac{x}{x-1}$	$\frac{1}{1-x}$	$\frac{x-1}{x}$	$1-x$	$\frac{1}{x}$	x

5. Algebraische Strukturen für Zahlenmengen

5.1 Gruppen

Beispiele für endliche Gruppen bzw. Halbgruppen:

7) $(\mathbb{Z}_n \times \mathbb{Z}_n, +)$ *(2-dimensionale zyklische Gruppe mit koordinatenweise additiver Verknüpfung)*

$\oplus_2$	(0, 0)	(0, 1)	(1, 0)	(1, 1)
(0, 0)	(0, 0)	(0, 1)	(1, 0)	(1, 1)
(0, 1)	(0, 1)	(0, 0)	(1, 1)	(1, 0)
(1, 0)	(1, 0)	(1, 1)	(0, 0)	(0, 1)
(1, 1)	(1, 1)	(1, 0)	(0, 1)	(0, 0)

$\oplus_3$	(0, 0)	(0, 1)	(0, 2)	(1, 0)	(1, 1)	(1, 2)	(2, 0)	(2, 1)	(2, 2)
(0, 0)	(0, 0)	(0, 1)	(0, 2)	(1, 0)	(1, 1)	(1, 2)	(2, 0)	(2, 1)	(2, 2)
(0, 1)	(0, 1)	(0, 2)	(0, 0)	(1, 1)	(1, 2)	(1, 0)	(2, 1)	(2, 2)	(2, 0)
(0, 2)	(0, 2)	(0, 0)	(0, 1)	(1, 2)	(1, 0)	(1, 1)	(2, 2)	(2, 0)	(2, 1)
(1, 0)	(1, 0)	(1, 1)	(1, 2)	(2, 0)	(2, 1)	(2, 2)	(0, 0)	(0, 1)	(0, 2)
(1, 1)	(1, 1)	(1, 2)	(1, 0)	(2, 1)	(2, 2)	(2, 0)	(0, 1)	(0, 2)	(0, 0)
(1, 2)	(1, 2)	(1, 0)	(1, 1)	(2, 2)	(2, 0)	(2, 1)	(0, 2)	(0, 0)	(0, 1)
(2, 0)	(2, 0)	(2, 1)	(2, 2)	(0, 0)	(0, 1)	(0, 2)	(1, 0)	(1, 1)	(1, 2)
(2, 1)	(2, 1)	(2, 2)	(2, 0)	(0, 1)	(0, 2)	(0, 0)	(1, 1)	(1, 2)	(1, 0)
(2, 2)	(2, 2)	(2, 0)	(2, 1)	(0, 2)	(0, 0)	(0, 1)	(1, 2)	(1, 0)	(1, 1)

5. Algebraische Strukturen für Zahlenmengen

5.1 Gruppen

Beispiele für endliche Gruppen bzw. Halbgruppen:

8) $((\mathbb{Z}_n)^r, +)$ *(r-dimensionale zyklische Gruppe mit koordinatenweise additiver Verknüpfung)*

$\oplus_2$	(0, 0, 0)	(0, 0, 1)	(0, 1, 0)	(0, 1, 1)	(1, 0, 0)	(1, 0, 1)	(1, 1, 0)	(1, 1, 1)
$\mathbb{Z}_2^3$: (0, 0, 0)	(0, 0, 0)	(0, 0, 1)	(0, 1, 0)	(0, 1, 1)	(1, 0, 0)	(1, 0, 1)	(1, 1, 0)	(1, 1, 1)
(0, 0, 1)	(0, 0, 1)	(0, 0, 0)	(0, 1, 1)	(0, 1, 0)	(1, 0, 1)	(1, 0, 0)	(1, 1, 1)	(1, 1, 0)
(0, 1, 0)	(0, 1, 0)	(0, 1, 1)	(0, 0, 0)	(0, 0, 1)	(1, 1, 0)	(1, 1, 1)	(1, 0, 0)	(1, 0, 1)
(0, 1, 1)	(0, 1, 1)	(0, 1, 0)	(0, 0, 1)	(0, 0, 0)	(1, 1, 1)	(1, 1, 0)	(1, 0, 1)	(1, 0, 0)
(1, 0, 0)	(1, 0, 0)	(1, 0, 1)	(1, 1, 0)	(1, 1, 1)	(0, 0, 0)	(0, 0, 1)	(0, 1, 0)	(0, 1, 1)
(1, 0, 1)	(1, 0, 1)	(1, 0, 0)	(1, 1, 1)	(1, 1, 0)	(0, 0, 1)	(0, 0, 0)	(0, 1, 1)	(0, 1, 0)
(1, 1, 0)	(1, 1, 0)	(1, 1, 1)	(1, 0, 0)	(1, 0, 1)	(0, 1, 0)	(0, 1, 1)	(0, 0, 0)	(0, 0, 1)
(1, 1, 1)	(1, 1, 1)	(1, 1, 0)	(1, 0, 1)	(1, 0, 0)	(0, 1, 1)	(0, 1, 0)	(0, 0, 1)	(0, 0, 0)

5. Algebraische Strukturen für Zahlenmengen

5.1 Gruppen

Wann gelten zwei Gruppen als gleich?

Definition: Zwei Gruppen $(G, \oplus)$ und $(H, \odot)$ gelten als gleich (isomorph), wenn es zwischen ihnen eine bijektive Abbildung $I: G \rightarrow H$ gibt, welche die Verknüpfungsstruktur erhält:

$$\forall a, b \in G: I(a \oplus b) = I(a) \odot I(b)$$

$$\forall a, b \in H: I^{-1}(a \odot b) = I^{-1}(a) \oplus I^{-1}(b)$$

I wird *Isomorphismus* genannt.

Charakteristische Größen endlicher Gruppen:

Ordnung eines Elements: Für $a \in G$ und $z, z' \in \mathbb{Z}$ sei $o(a) = z : \Leftrightarrow (a^z = e \wedge (a^{z'} = e \Rightarrow z' \geq z))$

Ordnung einer Gruppe: maximale Ordnung ihrer Elemente

Erzeugnis eines Elements $a \in G$: $\{a^1, a^2, \dots, a^{o(a)}\}$ (bildet eine Untergruppe)

Definition: Gruppen, die durch **ein** Element erzeugt werden, heißen **zyklisch**. **Bsp.:** $(\mathbb{Z}_n, +)$

Erzeugnis zweier Elemente $a, b \in G$: $\{c \in G \mid c = a^i \oplus b^j, i=1, \dots, o(a), j=1, \dots, o(b)\}$
(bildet eine Untergruppe)

Analog: Erzeugnis mehrerer Elemente

5. Algebraische Strukturen für Zahlenmengen

5.1 Gruppen

Charakteristische Invarianten endlicher Gruppen:

Satz: Jede endliche Gruppe wird durch endlich viele Elemente erzeugt.

Bemerkung: Auch unendliche Gruppen können durch endlich viele Elemente erzeugt werden (aber niemals durch ein einzelnes).

Satz: Jeder Isomorphismus bildet Elemente aufeinander ab, die dieselbe Ordnung haben.

Satz: Erzeugende Elemente werden auf erzeugende Elemente abgebildet.

Korollar: Isomorphe Gruppen enthalten für jede Ordnungszahl dieselbe Anzahl von Elementen mit dieser Ordnung.

Korollar: Isomorphe Gruppen werden durch dieselbe Zahl von Elementen erzeugt: Die Abbildung der erzeugenden Elemente legt den Rest der Abbildung fest.

5. Algebraische Strukturen für Zahlenmengen

5.2 Körper

Definition der Struktur eines Körpers:

Sei K eine nichtleere Menge und $\oplus, \odot$ Verknüpfungen zwischen den Elementen von G . Dann heißt die Struktur $(K, \oplus, \odot)$ ein **Körper**, wenn folgende Eigenschaften erfüllt sind:

1) $(K, \oplus)$ ist abelsche Gruppe mit neutralem Element e_0

2) $(K, \odot)$ ist Halbgruppe

3) $\forall a, b, c \in K: (a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$
 $c \odot (a \oplus b) = (c \odot a) \oplus (c \odot b)$

Distributivgesetze

4) $\exists e_1 \in K \forall a \in K: e_1 \odot a = a \odot e_1 = a$

Neutrales Element

5) $\forall a \in K \setminus \{e_0\} \exists a^{-1} \in K \setminus \{e_0\}: a^{-1} \odot a = a \odot a^{-1} = e_1$

Inverses Element

6) $\forall a, b \in K: a \odot b = b \odot a$

Kommutativgesetz

nur Eigenschaft 1), 2), 3) (bei Lang auch 4), 6)): Ring

nur Eigenschaft 1), 2), 3), 4), 6) + Nullteilerfreiheit: Integritätsbereich

nur Eigenschaft 1), 2), 3), 4), 5): Schiefkörper

Vorbilder: $(\mathbb{Q}, +, \cdot)$ für einen unendlichen Körper $(\mathbb{Z}_2, +, \cdot)$ für einen endlichen Körper

5. Algebraische Strukturen für Zahlenmengen

5.2 Körper

Beispiele von unendlichen Körpern, Ringen, etc.:

1) $(\mathbb{Z}, +, \cdot)$

2) $(\mathbb{Q}, +, \cdot)$

3) $(\mathbb{R} \setminus \{0\}, +, \cdot)$

4) $(\{f: \mathbb{R} \rightarrow \mathbb{R}\}, +, \cdot)$

5) $(\{f: \mathbb{R} \rightarrow \mathbb{R}, f \text{ bijektiv}\}, +, \circ)$

6) $(\{f: \mathbb{R} \rightarrow \mathbb{R}, f \text{ bijektiv}\}, \circ, +)$

7) $(\{f: \mathbb{R} \rightarrow \mathbb{R}, f \text{ linear}\}, +, \cdot)$

8) $(\{f: \mathbb{R} \rightarrow \mathbb{R}, f \text{ Polynomfunktion}\}, +, \cdot)$

5. Algebraische Strukturen für Zahlenmengen

5.2 Körper

Endliche Körper:

- 1) $(\mathbb{Z}_p, +, \cdot)$ für beliebige Primzahl p
- 2) $((\mathbb{Z}_p)^r, +, \cdot)$ für beliebige Primzahl p und beliebige natürliche Zahl r

Satz (Galois, 1811-1832): *Das sind alle!*

Endliche Körper gibt es nur mit p^r Elementen (p Primzahl, r natürliche Zahl). Jeder endliche Körper ist bis auf Isomorphie gleich zu den oben genannten. Der Körper mit q Elementen wird $GF(q)$ genannt (GF = Galoisfeld)

Wie sieht die multiplikative Verknüpfung für $r > 1$ aus ?

Satz:

Die multiplikative Gruppe des Körpers $((\mathbb{Z}_p)^r, +, \cdot)$ ist isomorph zu $(\mathbb{Z}_{p^r-1}, +)$.

5. Algebraische Strukturen für Zahlenmengen

5.2 Körper

Endliche Körper:

1) $(\mathbb{Z}_p, +, \cdot)$ für beliebige Primzahl p

2) $((\mathbb{Z}_p)^r, +, \cdot)$ für beliebige Primzahl p und beliebige natürliche Zahl r

Bsp.: $(\mathbb{Z}_2)^3$ Additionsgruppe

$\oplus_2$	$(0, 0, 0)$	$(0, 0, 1)$	$(0, 1, 0)$	$(0, 1, 1)$	$(1, 0, 0)$	$(1, 0, 1)$	$(1, 1, 0)$	$(1, 1, 1)$
$(0, 0, 0)$	$(0, 0, 0)$	$(0, 0, 1)$	$(0, 1, 0)$	$(0, 1, 1)$	$(1, 0, 0)$	$(1, 0, 1)$	$(1, 1, 0)$	$(1, 1, 1)$
$(0, 0, 1)$	$(0, 0, 1)$	$(0, 0, 0)$	$(0, 1, 1)$	$(0, 1, 0)$	$(1, 0, 1)$	$(1, 0, 0)$	$(1, 1, 1)$	$(1, 1, 0)$
$(0, 1, 0)$	$(0, 1, 0)$	$(0, 1, 1)$	$(0, 0, 0)$	$(0, 0, 1)$	$(1, 1, 0)$	$(1, 1, 1)$	$(1, 0, 0)$	$(1, 0, 1)$
$(0, 1, 1)$	$(0, 1, 1)$	$(0, 1, 0)$	$(0, 0, 1)$	$(0, 0, 0)$	$(1, 1, 1)$	$(1, 1, 0)$	$(1, 0, 1)$	$(1, 0, 0)$
$(1, 0, 0)$	$(1, 0, 0)$	$(1, 0, 1)$	$(1, 1, 0)$	$(1, 1, 1)$	$(0, 0, 0)$	$(0, 0, 1)$	$(0, 1, 0)$	$(0, 1, 1)$
$(1, 0, 1)$	$(1, 0, 1)$	$(1, 0, 0)$	$(1, 1, 1)$	$(1, 1, 0)$	$(0, 0, 1)$	$(0, 0, 0)$	$(0, 1, 1)$	$(0, 1, 0)$
$(1, 1, 0)$	$(1, 1, 0)$	$(1, 1, 1)$	$(1, 0, 0)$	$(1, 0, 1)$	$(0, 1, 0)$	$(0, 1, 1)$	$(0, 0, 0)$	$(0, 0, 1)$
$(1, 1, 1)$	$(1, 1, 1)$	$(1, 1, 0)$	$(1, 0, 1)$	$(1, 0, 0)$	$(0, 1, 1)$	$(0, 1, 0)$	$(0, 0, 1)$	$(0, 0, 0)$

5. Algebraische Strukturen für Zahlenmengen

5.2 Körper

Endliche Körper:

1) $(\mathbb{Z}_p, +, \cdot)$ für beliebige Primzahl p

2) $((\mathbb{Z}_p)^r, +, \cdot)$ für beliebige Primzahl p und beliebige natürliche Zahl r

Bsp.: $(\mathbb{Z}_2)^3$ Versuch mit einer zyklischen Gruppe für die Multiplikation

	$\odot$	(0, 0, 1)	(0, 1, 0)	(0, 1, 1)	(1, 0, 0)	(1, 0, 1)	(1, 1, 0)	(1, 1, 1)
$\mathbb{Z}_2^3 \setminus \{(0, 0, 0)\}$:	(0, 0, 1)	(0, 0, 1)	(0, 1, 0)	(0, 1, 1)	(1, 0, 0)	(1, 0, 1)	(1, 1, 0)	(1, 1, 1)
(falscher Versuch)	(0, 1, 0)	(0, 1, 0)	(0, 1, 1)	(1, 0, 0)	(1, 0, 1)	(1, 1, 0)	(1, 1, 1)	(0, 0, 1)
	(0, 1, 1)	(0, 1, 1)	(1, 0, 0)	(1, 0, 1)	(1, 1, 0)	(1, 1, 1)	(0, 0, 1)	(0, 1, 0)
	(1, 0, 0)	(1, 0, 0)	(1, 0, 1)	(1, 1, 0)	(1, 1, 1)	(0, 0, 1)	(0, 1, 0)	(0, 1, 1)
	(1, 0, 1)	(1, 0, 1)	(1, 1, 0)	(1, 1, 1)	(0, 0, 1)	(0, 1, 0)	(0, 1, 1)	(1, 0, 0)
	(1, 1, 0)	(1, 1, 0)	(1, 1, 1)	(0, 0, 1)	(0, 1, 0)	(0, 1, 1)	(1, 0, 0)	(1, 0, 1)
	(1, 1, 1)	(1, 1, 1)	(0, 0, 1)	(0, 1, 0)	(0, 1, 1)	(1, 0, 0)	(1, 0, 1)	(0, 0, 0)

Leider ist das Distributivgesetz verletzt!



5. Algebraische Strukturen für Zahlenmengen

5.2 Körper

Endliche Körper:

1) $(\mathbb{Z}_p, +, \cdot)$ für beliebige Primzahl p

2) $((\mathbb{Z}_p)^r, +, \cdot)$ für beliebige Primzahl p und beliebige natürliche Zahl r

Bsp.: $(\mathbb{Z}_2)^3$ Erfolgreicher Versuch einer zyklischen Gruppe für die Multiplikation

$\odot_2^g$	(0, 0, 0)	(0, 0, 1)	(0, 1, 0)	(0, 1, 1)	(1, 0, 0)	(1, 0, 1)	(1, 1, 0)	(1, 1, 1)
(0, 0, 0)	(0, 0, 0)	(0, 0, 0)	(0, 0, 0)	(0, 0, 0)	(0, 0, 0)	(0, 0, 0)	(0, 0, 0)	(0, 0, 0)
(0, 0, 1)	(0, 0, 0)	(0, 0, 1)	(0, 1, 0)	(0, 1, 1)	(1, 0, 0)	(1, 0, 1)	(1, 1, 0)	(1, 1, 1)
(0, 1, 0)	(0, 0, 0)	(0, 1, 0)	(1, 0, 0)	(1, 1, 0)	(0, 1, 1)	(0, 0, 1)	(1, 1, 1)	(1, 0, 1)
(0, 1, 1)	(0, 0, 0)	(0, 1, 1)	(1, 1, 0)	(1, 0, 1)	(1, 1, 1)	(1, 0, 0)	(0, 0, 1)	(0, 1, 0)
(1, 0, 0)	(0, 0, 0)	(1, 0, 0)	(0, 1, 1)	(1, 1, 1)	(1, 1, 0)	(0, 1, 0)	(1, 0, 1)	(0, 0, 1)
(1, 0, 1)	(0, 0, 0)	(1, 0, 1)	(0, 0, 1)	(1, 0, 0)	(0, 1, 0)	(1, 1, 1)	(0, 1, 1)	(1, 1, 0)
(1, 1, 0)	(0, 0, 0)	(1, 1, 0)	(1, 1, 1)	(0, 0, 1)	(1, 0, 1)	(0, 1, 1)	(0, 1, 0)	(1, 0, 0)
(1, 1, 1)	(0, 0, 0)	(1, 1, 1)	(1, 0, 1)	(0, 1, 0)	(0, 0, 1)	(1, 1, 0)	(1, 0, 0)	(0, 1, 1)

Wie kamen wir darauf?

→ Konstruktionsanleitung mit Hilfe von Polynomen

5. Algebraische Strukturen für Zahlenmengen

5.2 Körper

Definition Polynom für einen beliebigen Körper K:

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

Hierbei steht x für eine Variable mit Definitionsbereich K , a_i für eine beliebige Konstante aus K und x^i bedeutet die i -fache Hintereinanderschaltung der multiplikativen Verknüpfung angewendet auf das Körperelement x .

Ein Polynom ist durch die Angabe des Tupels $(a_n, a_{n-1}, \dots, a_1, a_0)$ eindeutig charakterisiert.

Das größte n mit $a_n \neq 0$ wird als *Grad des Polynoms* bezeichnet.

Die Menge der Polynome über einem Körper K wird mit $K[x]$ bezeichnet.

Satz:

$(K[x], +, \cdot)$ bildet einen Ring.

5. Algebraische Strukturen für Zahlenmengen

5.2 Körper

Weitere Definitionen:

Eine **Nullstelle** zu einem gegebenen Polynom ist ein Wert des Körpers K , dessen Einsetzung in das Polynom den Wert 0 ergibt.

Ein **Polynom** $f[x]$ über einem Körper K heißt **reduzibel**, wenn es zwei Polynome $g[x], h[x]$ in $K[x]$ gibt mit $f[x] = g[x] \cdot h[x]$ (übliche Polynommultiplikation). Wenn es keine solche Zerlegungsmöglichkeit gibt, heißt $f[x]$ **irreduzibel**.

Satz: $f[x]$ ist irreduzibel $\Rightarrow f[x]$ hat keine Nullstelle

Für Polynome $f[x]$ mit $\text{Grad} \leq 3$ gilt sogar: $f[x]$ ist irreduzibel $\Leftrightarrow f[x]$ hat keine Nullstelle.

Polynomdivision mit Rest:

Seien $f[x], g[x]$ Polynome.

Dann gibt es Polynome $q[x], r[x]$ mit $\text{Grad}(r[x]) < \text{Grad}(g[x])$:

$$f[x] = q[x] \cdot g[x] + r[x]$$

Die Polynome $q[x], r[x]$ werden analog zum schriftlichen Divisionsverfahren von Zahlen gebildet. (Euklidischer Algorithmus).

Analog zur Definition bei Zahlen wird das Restpolynom $r[x]$ auch $f[x] \bmod g[x]$ genannt.

5. Algebraische Strukturen für Zahlenmengen

5.2 Körper

Konstruktionsanleitung für GF (q) mit $q = p^r$ (p Primzahl, r natürliche Zahl):

- 1) Bestimme die Additions- und Multiplikationstabellen von GF (p):
Dieser *Primkörper* ist isomorph zum Restklassenkörper $(\mathbb{Z}_p, +, \cdot)$.
- 2) Identifiziere die Elemente aus GF (q) mit den p^r verschiedenen Polynomen über $(\mathbb{Z}_p, +, \cdot)$ mit Grad $< r$
- 3) Bilde die Additionstabelle wie bei Polynomen üblich.
(Anmerkung: Die entstehende Gruppe ist isomorph zu $((\mathbb{Z}_p)^r, +)$)
- 4) Wähle ein irreduzibles Polynom $g[x]$ über GF (p) mit Grad = r.
Bilde die Multiplikationstabelle wie bei Polynomen üblich,
aber *rechne modulo $g[x]$* , um jeweils Polynome mit Grad $< r$ zu erzeugen.
(Anmerkung: Die entstehende Gruppe ist isomorph zu $(\mathbb{Z}_{q-1}, +)$)

5. Algebraische Strukturen für Zahlenmengen

5.2 Körper

Beispiel: GF (8) $8 = 2^3$ ($p = 2, r = 3$)

Elemente: $\{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$

0, 1, 2, 3, 4, 5, 6, 7

Irreduzibles Polynom: x^3+x+1

Der Primkörper ist also GF(2)

Alle Polynome mit Grad < 3

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	6	7	4	5
3	3	2	1	0	7	6	5	4
4	4	5	6	7	0	1	2	3
5	5	4	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1
7	7	6	5	4	3	2	1	0

·	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	3	1	7	5
3	0	3	6	5	7	4	1	2
4	0	4	3	7	6	2	5	1
5	0	5	1	4	2	7	3	6
6	0	6	7	1	5	3	2	4
7	0	7	5	2	1	6	4	3

5. Algebraische Strukturen für Zahlenmengen

5.2 Körper

Beispiel: GF (9) $9 = 3^2$ ($p = 3, r=2$)

Der Primkörper ist also GF(3)

Elemente: $\{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$

Alle Polynome mit Grad < 2

0, 1, 2, 3, 4, 5, 6, 7, 8

Irreduzibles Polynom: x^2+1

+	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	0	4	5	3	7	8	6
2	2	0	1	5	3	4	8	6	7
3	3	4	5	6	7	8	0	1	2
4	4	5	3	7	8	6	1	2	0
5	5	3	4	8	6	7	2	0	1
6	6	7	8	0	1	2	3	4	5
7	7	8	6	1	2	0	4	5	3
8	8	6	7	2	0	1	5	3	4

·	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	1	6	8	7	3	5	4
3	0	3	6	2	5	8	1	4	7
4	0	4	8	5	6	1	7	2	3
5	0	5	7	8	1	3	4	6	2
6	0	6	3	1	7	4	2	8	5
7	0	7	5	4	2	6	8	3	1
8	0	8	4	7	3	2	5	1	6