Algebraische Strukturen

Fragen?

Abgeschlossenheit: es darf nichts anderes rauskommen als eine Restklasse

$\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

$\bullet : \mathbb{Z}_4 \times \mathbb{Z}_4 \longrightarrow \mathbb{Z}_4$

$(\bar{a}, \bar{b}) \longmapsto \bar{a} \bullet \bar{b} := \overline{a \cdot b}$

$\bullet$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

$\in \mathbb{Z}_4$

keine $\bar{1}$ d.h. $\bar{0} \cdot \sqcup \neq \bar{1}$

d.h. zu $\bar{0}$ gibt es kein Inv.

$\bar{2}$ nicht inv.

(Abg) ✓

(Ass.) $(\bar{a} \cdot \bar{b}) \cdot \bar{c} = \bar{a} \cdot (\bar{b} \cdot \bar{c})$ ✓ } Halbgruppe ✓

(neutr. Elt.) $\bar{1}$ $\quad \bar{1} \cdot \bar{a} = \bar{a} = \bar{a} \cdot \bar{1}$ ✓

(inv. Elt.) $\bar{a} \cdot \sqcup = \bar{1}$ $\quad \forall \bar{a} \in \mathbb{Z}_4$ ✗ } Gruppe

(Komm.) $\bar{a} \cdot \bar{b} = \overline{ab} = \overline{ba} = \bar{b} \cdot \bar{a}$. ✓

Bsp nicht abgeschlossen: $\mathbb{Z}_4 \setminus \{\bar{0}\}$: $= \{\bar{1}, \bar{2}, \bar{3}\}$

$\bullet$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$			
$\bar{2}$		$\bar{0} \notin \mathbb{Z}_4 \setminus \{\bar{0}\}$	
$\bar{3}$			

- $(\mathbb{Z}, \cdot)$ Halbgruppe, keine Gruppe da z.B. 2 nicht inv. $\quad 2 \cdot \sqcup \neq 1$

*** (kommutative) (Halb-)Gruppe?** Welche der folgenden Mengen besitzt welche algebraische Struktur?

	Halbgruppe? (Abg., Ass.)	Gruppe? (Abg., Ass., Neutr. Elt., Inverse Elte.)	Kommutativ? / abelsch
a) $(\mathbb{N} = \{1, 2, 3, ...\}, +)$	✓	✗ • kein neutr. Elt! $0 \notin \mathbb{N}$ • keine inv. Elte, z.B. $1 + \_ = 0$ $\quad -1 \notin \mathbb{N}$	✓
b) $(\mathbb{Z}, +)$	✓	✓ • $0 \in \mathbb{Z}$ ist neutrales Elt. • zu $a \in \mathbb{Z}$ ist $-a \in \mathbb{Z}$ invers: $a + (-a) = 0$	✓
c) $(\mathbb{Z}\backslash\{0\}, \cdot)$	✓	✗ • neutral. E.: $1 \in \mathbb{Z}\backslash\{0\}$ ✓ • inv. Elte, z.B. $2 \cdot \_ \neq 1$, $\frac{1}{2} \notin \mathbb{Z}\backslash\{0\}$ ✗	✓
d) $(\mathbb{Q}\backslash\{0\}, \cdot)$	✓	✓ • neutr. E.: $1 \in \mathbb{Q}\backslash\{0\}$ • inv. Elte: zu $\frac{a}{b} \in \mathbb{Q}\backslash\{0\}$ ist $\frac{b}{a} \in \mathbb{Q}\backslash\{0\}$ invers: $\frac{a}{b} \cdot \frac{b}{a} = 1$	✓

<u>Bsp. nicht abgeschlossen</u>: $\mathbb{N}_0 \cup \{-1\} = \{-1, 0, 1, 2, 3, \dots\}$ bzgl. $+$

$$(-1) + (-1) = -2 \notin$$

Eigener Lösungsversuch.

	Halbgruppe?	Gruppe?	Kommutativ?
a) $(\mathbb{N} = \{1, 2, 3, ...\}, +)$			
b) $(\mathbb{Z}, +)$			
c) $(\mathbb{Z}\backslash\{0\}, \cdot)$			
d) $(\mathbb{Q}\backslash\{0\}, \cdot)$			

$\{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$ Restklassen modulo n

* **Algebraische Struktur von $\mathbb{Z}_n$.** Welche der folgenden Mengen besitzt welche algebraische Struktur?

z.B. $\bar{2} + \underline{\bar{1}} = \bar{0}$ $\quad \bar{1} = \overline{-2} = \overline{3-2} \in \mathbb{Z}_3$

<table>
<tr><th></th><th>Halbgruppe?</th><th>Gruppe?</th><th>Kommutativ?</th></tr>
<tr><td>$\{\bar{0}, \bar{1}, \bar{2}\}$
a) $(\mathbb{Z}_3, +)$</td><td>✓
abg.
Ass. ✓
$\begin{array}{c|ccc} + & \bar{0} & \bar{1} & \bar{2} \\ \hline \bar{0} & \bar{0} & \bar{1} & \bar{2} \\ \bar{1} & \bar{1} & \bar{2} & \bar{0} \\ \bar{2} & \bar{2} & \bar{0} & \bar{1} \end{array} \in \mathbb{Z}_3$</td><td>✓
• neutr. Elt. $\bar{0}$
• inv. Elte: $\bar{a} + \_ = \bar{0}$
$\bar{a} + \overline{-a} = \bar{0}$, $\overline{-a} = \overline{3-a}$</td><td>✓</td></tr>
<tr><td>$\{\bar{1}, \bar{2}\}$
b) $(\mathbb{Z}_3 \setminus \{0\}, \cdot)$</td><td>abg. ✓
Ass. ✓
$\begin{array}{c|cc} \cdot & \bar{1} & \bar{2} \\ \hline \bar{1} & \boxed{\bar{1}} & \bar{2} \\ \bar{2} & \bar{2} & \boxed{\bar{1}} \end{array} \in \mathbb{Z}_3 \setminus \{0\}$</td><td>✓
• neutr. Elt: $\bar{1}$
• inv. Elte
$\bar{1} \cdot \bar{1} = \bar{1}$ ✓
$\bar{2} \cdot \bar{2} = \bar{1}$ ✓</td><td>✓</td></tr>
<tr><td>c) $(\mathbb{Z}_4, +)$</td><td>✓
siehe Vorlesung!</td><td>✓</td><td>✓</td></tr>
<tr><td colspan="4">Allg.: $\boxed{(\mathbb{Z}_n, +) \text{ abelsche Gruppe}}$</td></tr>
<tr><td>d) $(\mathbb{Z}_4 \setminus \{0\}, \cdot)$</td><td>abg. ✗
$\begin{array}{c|ccc} \cdot & \bar{1} & \bar{2} & \bar{3} \\ \hline \bar{1} & & & \\ \bar{2} & & & \\ \bar{3} & & & \end{array}$ $\quad \bar{0} \notin \mathbb{Z}_4 \setminus \{0\}$</td><td>✗</td><td>✓</td></tr>
<tr><td>e) $(\mathbb{Z}_4, \cdot)$</td><td>abg. ✓
Ass. ✓
$\begin{array}{c|cccc} \cdot & \bar{0} & \bar{1} & \bar{2} & \bar{3} \\ \hline \bar{0} & \bar{0} & \bar{0} & \bar{0} & \bar{0} \\ \bar{1} & \bar{0} & \boxed{\bar{1}} & \bar{2} & \bar{3} \\ \bar{2} & \bar{0} & \bar{2} & \bar{0} & \bar{2} \\ \bar{3} & \bar{0} & \bar{3} & \bar{2} & \boxed{\bar{1}} \end{array}$</td><td>✗
• neutr. Elt: $\bar{1}$ ✓
• inv. Elte: nicht für alle!
$\bar{0} \cdot \_ \neq \bar{1}$
$\bar{2} \cdot \_ \neq \bar{1}$ ✗</td><td>✓</td></tr>
</table>

(Inverse gibt es zu
$\bar{1} \cdot \underline{\bar{1}} = \bar{1} \quad \bar{1}^{-1} = \bar{1}$
$\bar{3} \cdot \underline{\bar{3}} = \bar{1} \quad \bar{3}^{-1} = \bar{3}$)

Eigener Lösungsversuch.

	Halbgruppe?	Gruppe?	Kommutativ?
a) $(\mathbb{Z}_3, +)$			
b) $(\mathbb{Z}_3 \backslash \{0\}, \cdot)$			
c) $(\mathbb{Z}_4, +)$			
d) $(\mathbb{Z}_4 \backslash \{0\}, \cdot)$			
e) $(\mathbb{Z}_4, \cdot)$			

Zusammenfassung: Algebraische Struktur von $\mathbb{Z}_n$.

$$\forall n \in \mathbb{N} : \boxed{(\mathbb{Z}_n, +) \text{ ist eine abelsche Gruppe}}$$

(siehe Skript!)

- neutr. Elt: $\bar{0}$
- inv. Elte: zu $\bar{a}$ ist $\overline{-a} = \overline{n-a}$ $\quad \left(\overline{n-a} = \underbrace{\bar{n}}_{\bar{0}} + \overline{-a} = \overline{-a} \right)$

$$\left(\begin{array}{l} \text{z.B. } \mathbb{Z}_{1024} : \overline{-386} = \overline{1024-386} = \overline{638} \\ \Rightarrow \overline{386} + \overline{638} = \overline{1024} = \bar{0} \end{array} \right)$$

$$\boxed{(\mathbb{Z}_n \setminus \{0\}, \cdot) \text{ ist abelsche Gruppe} \iff n \text{ ist prim}}$$

(Skript ↝ nächstes mal!)

- neutr. Elt: $\bar{1}$
- inv. Elte: ? — Existieren für alle Restklassen $\bar{a}$ $\iff$ n prim!

z.B. $n = 4$: $\mathbb{Z}_4$: Für $\bar{a} = \bar{2}$ gibt es kein Inverses, s.o.

Inverse berechnen.

1.* Berechnen Sie (falls möglich) $\bar{5}^{-1}$ in $\mathbb{Z}_{1024}$.

2. Berechnen Sie (falls möglich) $\bar{2}^{-1}$ in $\mathbb{Z}_{1024}$.

3. Wann ist $\bar{a} \in \mathbb{Z}_n$ bzgl. $\cdot$ invertierbar?

Lösung. 1. $\bar{5} \cdot \bar{x} = \bar{1}$ $\quad$ (Suche $\bar{x}$, falls es existiert gilt $\bar{5}^{-1} = \bar{x}$)

$$\iff 5x = 1 + q \cdot 1024 \iff \underbrace{5x + 1024 \cdot \underbrace{(-q)}_{y} = 1}_{\text{Dioph. Gl.}}$$

1. EEA mit a = 5 und b = 1024 :

a =	q *	b +	r	x	y	ggT =	a *	x +	b *	y
5 =	0 *	1024 +	5	205	-1	1 =	5 *	205 +	1024 *	-1
1024 =	204 *	5 +	4	-1	205	1 =	1024 *	-1 +	5 *	205
5 =	1 *	4 +	1	1	-1	1 =	5 *	1 +	4 *	-1
4 =	4 *	1 +	0	0	1	1 =	4 *	0 +	1 *	1

$\operatorname{ggT}(5, 1024) = 1 \mid 1 \Rightarrow$ lösbar!

$\bar{x} = \overline{205}$ $\quad$ (Inverses ist in einer Halbgruppe eindeutig bestimmt!) $\quad$ 2. ✗ $\quad$ 3. ✗

[Probe: $\bar{5} \cdot \overline{205} = \overline{1025} = \bar{1}$]

Lösung.

2. $\overline{2}\cdot\overline{x} = \overline{1} \iff 2x = 1 + q\cdot 1024 \iff \underline{2}\,x + \underline{1024}\,\underbrace{(-q)}_{y} = \underline{1}$

$\operatorname{ggT}(2, \underbrace{1024}_{2^{10}}) = 2 \nmid 1$ d.h. <u>nicht</u> lösbar, d.h. es gibt kein Inverses $\overline{x}$!

3. $\overline{a}\cdot\overline{x} = \overline{1} \iff a\cdot x = 1 + q\cdot n \iff \underline{a}\cdot x + \underline{n}\,\underbrace{(-q)}_{y} = \underline{1}$

Die dioph. Gleichung ist lösbar $\iff \operatorname{ggT}(a, n) = 1$

<u>Invertierbarkeitskriterium</u>: $\boxed{\overline{a} \text{ invertierbar in } (\mathbb{Z}_n\setminus\{0\},\cdot) \iff \operatorname{ggT}(a,n) = 1}$

d.h. a, n <u>teilerfremd</u>

Eigener Lösungsversuch.

lässt man gerne weg!

Invertierbarkeitskriterium. Sind $\overline{537}$ und $\overline{8491}$ in $\mathbb{Z}_{63481}$ invertierbar?

Lösung.

- $\text{ggT}(537, 63481) \overset{EA}{=} 1 \overset{\text{Inv.krit.}}{\iff} \overline{537}$ ist invertierbar!

a	=	q	*	b	+	r
537	=	0	*	63481	+	537
63481	=	118	*	537	+	115
537	=	4	*	115	+	77
115	=	1	*	77	+	38
77	=	2	*	38	+	$\boxed{1}$
38	=	38	*	$\boxed{1}$	+	0

- $\text{ggT}(8491, 63481) \overset{EA}{=} 1$ Ja!

a	=	q	*	b	+	r
8491	=	0	*	63481	+	8491
63481	=	7	*	8491	+	4044
8491	=	2	*	4044	+	403
4044	=	10	*	403	+	14
403	=	28	*	14	+	11
14	=	1	*	11	+	3
11	=	3	*	3	+	2
3	=	1	*	2	+	$\boxed{1}$
2	=	2	*	$\boxed{1}$	+	0

Eigener Lösungsversuch.