

Lineare Algebra I

für die Fachrichtung Informatik

Wintersemester 2023/24

Algebraische Strukturen

Halbgruppen

Monoide

Gruppen

Ringe

Körper

Vektorräume

Binäre Verknüpfung auf einer Menge S

$$*: S \times S \longrightarrow S$$

$*$ ist kommutativ, falls $\forall x, y \in S \quad x * y = y * x$

$*$ ist assoziativ, falls $\forall x, y, z \in S \quad (x * y) * z = x * (y * z)$

$(S, *)$ Halbgruppe, falls $*$ assoziativ ist.

z.B.: $+: \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$

$$(\mathbb{R}, +) \neq (\mathbb{R}, \cdot)$$

$3 + 4$
↑
Infix

$+(3, 4)$
↑
Präfix

$(3, 4) +$
↑
Postfix

Anmerkung:

S = Menge der Gleitkommazahlen (floating point numbers)

$$+ : S \times S \longrightarrow S$$

Addition ist NICHT assoziativ!

$$x = 1$$

$$y = 10^{30}$$

$$z = -10^{30}$$

$$(x + y) + z$$

$$(1 + 10^{30}) + (-10^{30})$$

$$\underbrace{\underbrace{1 + 10^{30}}_{= 10^{30}} + (-10^{30})}_{= 0}$$

$\neq$

$$x + (y + z)$$

$$1 + \underbrace{(10^{30} + (-10^{30}))}_{= 0}$$

$$\underbrace{1 + 0}_{= 1}$$

$$D = \{i, s_1, s_2, s_3, g, u\}$$

6 verschiedene
Elemente

$$\star: D \times D \rightarrow D$$

$\star$	i	s_1	s_2	s_3	g	u
i	i	s_1	s_2	s_3	g	u
s_1	s_1	i	g	u	s_2	s_3
s_2	s_2	u	i	g	s_3	s_1
s_3	s_3	g	u	i	s_1	s_2
g	g	s_3	s_1	s_2	u	i
u	u	s_2	s_3	s_1	i	g

"Cayley-Table"

$(D, \star)$ Halbgruppe

$$i^{-1} = i$$

$$s_1^{-1} = s_1$$

$$s_2^{-1} = s_2$$

$$s_3^{-1} = s_3$$

$$u^{-1} = g$$

$$g^{-1} = u$$

Def. 3.1.4 $(S, *)$ Halbgruppe $e \in S$

e heißt **neutrales Element** von $(S, *)$ falls

$$\forall x \in S \quad e * x = x = x * e.$$

Eine Halbgruppe $(S, *)$ heißt **Monoid**, falls $(S, *)$ ein Neutralelement hat.

Lemma 3.1.5 Eine Halbgruppe $(S, *)$
hat höchstens ein Neutralelement.

Bw: Angenommen, e und f seien Neutralelemente für $(S, *)$.

$$e = e * f = f$$

weil f Neutralelement

weil e Neutralelement.



z.B.:

$$S = (\mathcal{P}(X), \cap)$$

$$A \cap X = A = X \cap A$$

$\Rightarrow X$ ist das Neutralelement.

$$S = (\mathcal{P}(X), \cup)$$

$$A \cup \emptyset = A = \emptyset \cup A$$

$\Rightarrow \emptyset$ ist das Neutralelement.

$$S = (\mathbb{R}, +), (\mathbb{Q}, +), (\mathbb{Z}, +), (\mathbb{N}_0, +)$$

0 Neutralelement

$$S = (\mathbb{R}, \cdot), (\mathbb{Q}, \cdot), (\mathbb{Z}, \cdot), (\mathbb{N}_0, \cdot), (\mathbb{N}, \cdot)$$

1 Neutralelement

Def 3.1.7 Geg: $(S, *)$ Monoid mit e Neutralelement.

$x \in S$ heißt invertierbar, wenn

$$\exists y \in S : x * y = e = y * x.$$

Z.B.: $7 \in \mathbb{R}$ $(\mathbb{R}, +)$ Neutralelement = 0

7 ist invertierbar und das Inverse ist -7

$$(-7) + 7 = 0 = 7 + (-7)$$

$(\mathbb{R}, \cdot)$ Neutralelement = 1.

7 ist invertierbar mit Inverse $\frac{1}{7}$

$$\frac{1}{7} \cdot 7 = 1 = 7 \cdot \frac{1}{7}.$$

0 ist in $(\mathbb{R}, \cdot)$ nicht
invertierbar. $0 \cdot y = 0 \neq 1$ $\nexists$
 $0 = 1$ $\nexists$.

Lemma 3.1.9 $(S, *)$ Monoid mit Neutralelement e

Wenn x invertierbar ist, dann ist das Inverse eindeutig.

Bw: Ang $y, z \in S$ seien Inverse von x .

$$(z.z: y = z)$$

$$\begin{array}{ccc} e & & z \\ \text{Neutral} & & \text{Inverse von } x \\ \downarrow & & \downarrow \\ y & = & y * e = y * (x * z) \end{array}$$

$$\begin{array}{c} \nearrow \\ = (y * x) * z \\ \text{Assoziativit\u00e4t} \end{array}$$

$$\begin{array}{ccc} & & e * z = z \\ & \nearrow & \uparrow \\ y & \text{Inverse von } x & e \\ & & \text{Neutral} \end{array}$$

□

Notation: Wenn $x \in S$ invertierbar ist, dann

$x^{-1} :=$ Inverse von x .

z.B.: 3.1.9 X Menge

$X^X = \{ f: X \rightarrow X \}$ $(X^X, \circ)$ Monoid.

$$\text{id}_X \circ f = f = f \circ \text{id}_X \quad \text{id}_X: (x \mapsto x)$$

Geg. $f \in X^X$. Wann ist f invertierbar in $(X^X, \circ)$?

$\exists g?$ $f \circ g = \text{id} = g \circ f$?

f ist invertierbar bzgl. $\circ \iff f$ bijektiv

Lemma 3,1,10 $(S, *)$ Monoid

x, y sind invertierbar

$\implies x * y$ invertierbar

$$\text{und } (x * y)^{-1} = y^{-1} * x^{-1}$$

Bw: $a = y^{-1} * x^{-1}$

z.z: $a * (x * y) = e$
 $(x * y) * a = e$

$$\begin{aligned} a * (x * y) &= (y^{-1} * x^{-1}) * (x * y) \\ &= y^{-1} * \underbrace{x^{-1} * x}_e * y = y^{-1} * e * y \\ &= y^{-1} * y = e. \end{aligned}$$

$$(x * y) * a = \dots$$

$$= e$$



Notation: $(S, *)$ Monoid

$$(S, *)^{\times} := \{x \in S \mid x \text{ invertierbar}\} \subseteq S.$$

$$e \in (S, *)^{\times}$$

$$e * e = e$$

$$\text{mit } e^{-1} = e.$$

$$x, y \in (S, *)^{\times} \Rightarrow x * y \in (S, *)^{\times}$$

$$x \in (S, *)^{\times} \Rightarrow x^{-1} \in (S, *)^{\times} \quad \text{mit} \quad (x^{-1})^{-1} = x.$$

Achtung:

$$a * x = e$$

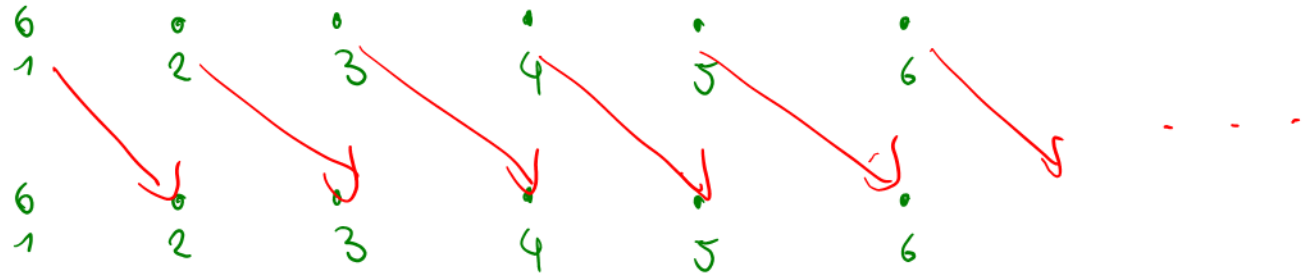
$\nRightarrow x$ invertierbar.

z.B.:

$$X = \mathbb{N}$$

$$(X^X, \circ)$$

Monoid.



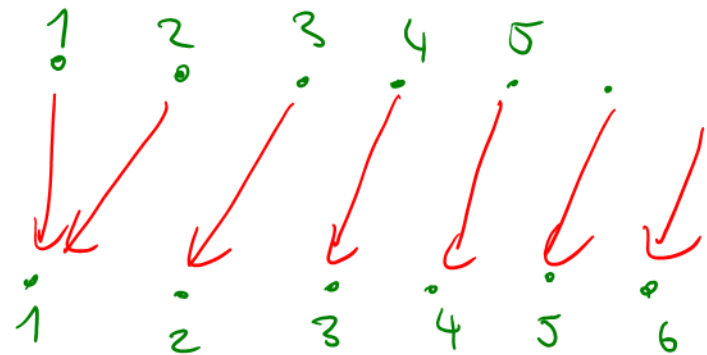
$$f: \begin{pmatrix} \mathbb{N} \rightarrow \mathbb{N} \\ k \mapsto k+1 \end{pmatrix}$$

injektiv, nicht surjektiv.

$$f \notin (X^X, \circ)^*$$

$$g: \begin{pmatrix} \mathbb{N} \rightarrow \mathbb{N} \\ 1 \mapsto 1 \\ k \mapsto k-1 \text{ für } k \geq 2 \end{pmatrix}$$

g surjektiv, nicht injektiv.



$$g \circ f = \text{id}_N$$

g ist „Links inverses von f “.

Aber $f \circ g \neq \text{id}$

$$f \circ g : \begin{pmatrix} 1 \mapsto 2 \\ k \mapsto k \\ \text{für } k \geq 2 \end{pmatrix}$$

f, g sind
NICHT
invertierbar!

Anmerkung: $(\mathbb{R}^{n \times n}, \cdot)$ Monoid mit Neutral. $1 = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}$.

Hier gilt: $AB = 1 \Rightarrow B$ invertierbar.

(Satz 4.3.4) Später.

Notation: $(S, *)$ Monoid mit Nutrallem. e .

$$n \in \mathbb{N}.$$

$$x \in S$$

$$x^n := \underbrace{x * x * \dots * x}_{n \text{ mal.}}$$

$$x^0 := e$$

$$x \in (S, *)^*$$

$$x^{-n} := \underbrace{x^{-1} * x^{-1} * \dots * x^{-1}}_n$$

$$x^0 := e$$

$$x^{n+1} = x^n * x.$$

Es gilt:

$$x^{k+l} = x^k * x^l$$

für $k, l \geq 0$.

Falls

x invertierbar:

$$x^{k+l} = x^k * x^l$$

für $k, l \in \mathbb{Z}$

$$(X * y)^k \neq X^k * y^k \quad \text{im Allgemeinen}$$

z.B.:

$$(AB)^2 \neq A^2 B^2$$

$$A, B \in (\mathbb{R}^{n \times n}, \cdot)$$

$$\underbrace{\left(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \right)^2}_{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}} \neq \underbrace{\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}^2}_{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}}$$

Def: Eine Gruppe $(G, *)$

ist ein Monoid, in dem jedes Element
invertierbar ist, d.h.

G Menge,

$$*: G \times G \longrightarrow G$$

$$(\forall x, y, z \in G) (x * y) * z = x * (y * z)$$

$$\exists e \quad x * e = x = e * x$$

$$\forall x \in G$$

$$\exists y \in G$$

$$y * x = e = x * y$$

G ist
(abgeschlossen unter $*$)

($*$ ist assoziativ)

(Neutralelement)

(Jedes Element hat ein
Inverses)

Eine kommutative Gruppe heißt auch abelsche Gruppe.

$(S, *)$ Monoid

Dann ist $(S, *)^*$ eine Gruppe bzgl.
der eingeschränkten Gruppenoperation.

Diese Gruppe ist die
Einheitsgruppe von $(S, *)$.

z.B.: $(\mathbb{Z}, \cdot)^* = (\{-1, 1\}, \cdot)$

$$(\mathbb{Q}, \cdot)^* = (\mathbb{Q} \setminus \{0\}, \cdot)$$

$$(\mathbb{R}, \cdot)^* = (\mathbb{R} \setminus \{0\}, \cdot)$$

$$(\mathbb{N}, \cdot)^* = (\{1\}, \cdot)$$

$$(\mathbb{D}, \star)^* = (\mathbb{D}, \star).$$

$$(\mathcal{P}(X), \cup)^* = (\{\emptyset\}, \cup)$$

$$(\mathcal{P}(X), \cap)^* = (\{X\}, \cap)$$

z.B.: X Menge

$(X^X, \circ)$ Monoid mit Neutralelement id_X .

$$S(X) := (X^X, \circ)^X = \{ f: X \rightarrow X \mid f \text{ bijektiv} \}$$

Permutationsgruppe auf X

oder Symmetrische Gruppe

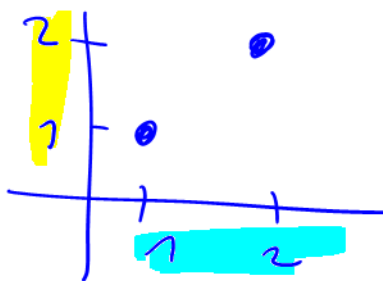
$$X = \{1, \dots, n\}$$

$$S(n) := S(\{1, \dots, n\}) = \{ \sigma: \{1, \dots, n\} \rightarrow \{1, \dots, n\} \text{ bijektiv} \}$$

$n=2$

$\{1, 2\}$

id



$$\text{id} = \begin{array}{c|c} 1 & 2 \\ \hline 1 & 2 \end{array}$$

$$\begin{array}{c|c} 1 & 2 \\ \hline 2 & 1 \end{array}$$

$$\mathcal{P}(2) = \left\{ \text{id}, \begin{array}{c|c} 1 & 2 \\ \hline 2 & 1 \end{array} \right\}.$$

$$n=3 \quad \{1, 2, 3\} \longrightarrow \{1, 2, 3\}$$

$$\text{id} = \begin{array}{c|c|c} 1 & 2 & 3 \\ \hline 1 & 2 & 3 \end{array}$$

$$\begin{array}{c|c|c} 1 & 2 & 3 \\ \hline 2 & 1 & 3 \end{array}$$

$$|\mathcal{P}(3)| = 6.$$

$$\begin{array}{c|c|c} 1 & 2 & 3 \\ \hline 2 & 3 & 1 \end{array}$$

$$\begin{array}{c|c|c} 1 & 2 & 3 \\ \hline 3 & 2 & 1 \end{array}$$

$$\begin{array}{c|c|c} 1 & 2 & 3 \\ \hline 3 & 1 & 2 \end{array}$$

$$\begin{array}{c|c|c} 1 & 2 & 3 \\ \hline 1 & 3 & 2 \end{array}$$

Induktion:

$$|\mathcal{P}(n)| = n!$$

$$\begin{array}{c|c|c} 1 & 2 & 3 \\ \hline 3 & 1 & 2 \end{array} \circ \begin{array}{c|c|c} 1 & 2 & 3 \\ \hline 1 & 3 & 2 \end{array} = \begin{array}{c|c|c} 1 & 2 & 3 \\ \hline 3 & 2 & 1 \end{array}$$

Beispiele für Mengen S mit binärer Verknüpfung $*$: $S \times S \rightarrow S$

$$x \uparrow y = x^y$$

* kommutativ

(floating point nbs, +)

$(\mathbb{N}, \uparrow)$

* assoziativ, d.h. $(S, *)$ ist Halbgruppe

$(\mathbb{N}, +)$

$(S, *)$ Monoid

$(\mathbb{N}, \cdot)$ $(\mathcal{P}(X), \cup)$ $(\mathcal{P}(X), \cap)$

$(X^X, \circ)$ $(\mathbb{R}^{n \times n}, \cdot)$ $n \geq 2$

$(\mathbb{Z}, \cdot)$ $(\mathbb{Q}, \cdot)$ $(\mathbb{R}, \cdot)$

$(S, *)$ Gruppe

$(\mathbb{Z}, +)$ $(\mathbb{Q}, +)$ $(\mathbb{R}, +)$

$\mathcal{P}(X)$

$\{1\}, \cdot$ $\{1, -1\}, \cdot$ $(\mathbb{Q}^x, \cdot)$ $(\mathbb{R}^x, \cdot)$

$\mathcal{P}(n)$
 $n \geq 3$

$(\mathbb{R}^n, +)$ $(\mathbb{R}^{m \times n}, +)$

$(\mathbb{D}, \star)$