

Lineare Algebra I

Woche 04

07.11.2023 und 09.11.2023

Definition

Eine **algebraische Struktur** ist eine Menge X , ausgestattet mit einer oder mehreren Verknüpfungen.

„Rechenoperationen“

Beispiel

- Halbgruppe $\} \text{ eine Verknüpfung}$
- Gruppe $\} \text{ eine Verknüpfung}$
- Ring $\} \text{ zwei Verknüpfungen}$
- Körper $\} \text{ zwei Verknüpfungen}$
- Vektorraum $\} \text{ Kapitel 3}$

Verknüpfung

Definition

Operation

Es sei X eine Menge. Eine **(innere) Verknüpfung** auf X ist eine Abbildung

$$\star: X \times X \rightarrow X.$$

Wir schreiben $a \star b$ statt $\star(a, b)$.

Beispiel

$$+: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} \quad \text{Addition}$$

$$\cdot: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} \quad \text{Multiplikation}$$

– ist keine Verknüpfung auf \mathbb{N}

Verknüpfung

Verknüpfungstafel $\begin{matrix} a & \xrightarrow{*} & b \\ \downarrow & & \downarrow \\ & & 0 \end{matrix}$ $a * b$

Beispiel

- ① Auf $\{0, 1\}$ definieren wir die zwei Verknüpfungen

$+_2$		0	1	\cdot_2		0	1
0		0	1	0		0	0
1		1	0	1		0	1

- ② X eine Menge, $(S, *)$ Struktur

$$S^X = \{ f \mid f: X \rightarrow S \}$$

$$*: S^X \times S^X \rightarrow S^X \text{ mit } (f * g)(x) := \underbrace{f(x)} \underbrace{*}_{\text{punktweise}} \underbrace{g(x)} \in S$$

- ③ X eine Menge und $X^X = \{ f \mid f: X \rightarrow X \}$

$$\circ X^X \times X^X \rightarrow X^X \text{ mit } (f \circ g)(x) := f(g(x)) \in X$$

Halbgruppe

Definition

Eine **Halbgruppe** (H, \star) ist eine Menge H mit einer assoziativen Verknüpfung \star auf H , also

$$(x \star y) \star z = x \star (y \star z)$$

Beispiel

① $(\mathbb{N}, +)$, $(\mathbb{N}_0, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ und $(\mathbb{C}, +)$ Halbgruppen ✓
- auf \mathbb{Z} ist nicht assoziativ!! $(1-2)-3 = -4$
 $1-(2-3) = 2$

② (\mathbb{N}, \cdot) , (\mathbb{N}_0, \cdot) , (\mathbb{Z}, \cdot) , (\mathbb{Q}, \cdot) , (\mathbb{R}, \cdot) und (\mathbb{C}, \cdot) Halbgruppe ✓

③ $(\{0, 1\}, +_2)$ und $(\{0, 1\}, \cdot_2)$ Halbgruppen

$$0 +_2 (1 +_2 0) = (0 +_2 1) +_2 0 \text{ usw. } \checkmark$$

Beispiel

- 4 X eine Menge, $(S, *)$ Halbgruppe
Dann ist $(S^X, *)$ Halbgruppe. Assoziativität vererbbar!

$$[(f * g) * h](x) = \dots$$

$$[f * (g * h)](x) = \dots$$

- 5 X eine Menge, (X^X, \circ) ist Halbgruppe
Komposition von Funktionen ist assoziativ
(Lemma 6.16)

- 6 $(\mathcal{P}(X), \cap)$, $(\mathcal{P}(X), \cup)$ und $(\mathcal{P}(X), \Delta)$ Halbgruppen

denn \cap , \cup und Δ sind assoziativ

neutrales Element

Definition

Es sei (H, \star) eine Halbgruppe.

Ein $e \in H$ heißt ein neutrales Element von (H, \star) , wenn gilt:

$$e \star x = x \quad \text{und} \quad x \star e = x \quad \text{für alle } x \in H$$

Eine Halbgruppe (H, \star) mit einem neutralen Element heißt ein Monoid.

Lemma

Es sei (H, \star) eine Halbgruppe. Sind e_1 und e_2 beides neutrale Elemente von (H, \star) , dann gilt $e_1 = e_2$.

Beweis.

$$\begin{aligned} e_1 &= e_1 \star e_2 \\ &= e_2 \end{aligned}$$

da e_2 neutral

da e_1 neutral

Halbgruppe mit/ohne neutralem/s Element

Beispiel

- ① $(\mathbb{N}, +)$ besitzt kein neutrales Element.
- ② $(\mathbb{N}_0, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ und $(\mathbb{C}, +)$ haben alle das neutrale Element 0.
- ③ (\mathbb{N}, \cdot) , (\mathbb{N}_0, \cdot) , (\mathbb{Z}, \cdot) , (\mathbb{Q}, \cdot) , (\mathbb{R}, \cdot) und (\mathbb{C}, \cdot) haben alle das neutrale Element 1.

Verknüpfung mit 0 von links

④	$+2$	$\begin{array}{ c c} \hline 0 & 1 \\ \hline \end{array}$		$\cdot 2$	$\begin{array}{ c c} \hline 0 & 1 \\ \hline \end{array}$	
\rightarrow	$\begin{array}{ c c} \hline 0 & 1 \\ \hline \end{array}$	$\begin{array}{ c c} \hline 0 & 1 \\ \hline \end{array}$	0 neutrales Element	\rightarrow	$\begin{array}{ c c} \hline 0 & 0 \\ \hline \end{array}$	1 neutrales Element
	$\begin{array}{ c c} \hline 1 & 0 \\ \hline \end{array}$	$\begin{array}{ c c} \hline 1 & 0 \\ \hline \end{array}$			$\begin{array}{ c c} \hline 0 & 1 \\ \hline \end{array}$	

Definition

Es sei (H, \star) eine Halbgruppe. Für festes $a \in H$ heißt die Abbildung

$\star_a: H \ni x \mapsto \underline{x \star a} \in H$ die **Rechtstranlation** mit a ,

${}_a\star: H \ni x \mapsto a \star x \in H$ die **Linkstranlation** mit a .

Beispiel

① $(\mathbb{R}, +)$ mit $a = \sqrt{2}$. Rechts- und Linkstranlationen stimmen überein und bedeuten: Addition von $\sqrt{2}$

② (\mathbb{R}^2, \circ) mit $g(x) := 2x$

$o_g: f \mapsto f \circ g$ mit $(f \circ g)(x) = f(g(x)) = f(2x)$

$g \circ: f \mapsto g \circ f$ mit $(g \circ f)(x) = g(f(x)) = 2f(x)$

invertierbares Element, inverses Element

Definition

Es sei (H, \star) eine Halbgruppe mit neutralem Element e .

Ein Element $a \in H$ heißt invertierbar oder eine Einheit von (H, \star) , wenn ein $b \in H$ existiert mit

$$a \star b = e \quad \text{und} \quad b \star a = e$$

In diesem Fall heißt b ein **inverses Element** oder ein **Inverses** zu a .

Beachte: b ist Inverses zu $a \Leftrightarrow a$ ist Inverses zu b !

Lemma

Es sei (H, \star) eine Halbgruppe mit neutralem Element e . Ist $a \in H$ invertierbar und sind b_1 und b_2 beides Inverse zu a , dann gilt $b_1 = b_2$.

Beweis.

$$\begin{aligned} b_1 &= b_1 \star e = b_1 \star (a \star b_2) \\ &= (b_1 \star a) \star b_2 = e \star b_2 = b_2 \end{aligned}$$

invertierbares Element, inverses Element

Beispiel

- 1 $(\mathbb{N}, +)$ hat kein neutrales Element, also auch keine invertierbaren Elemente.
- 2 In $(\mathbb{N}_0, +)$ ist nur das Element 0 invertierbar. Es ist zu sich selbst invers.
- 3 In $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ und $(\mathbb{C}, +)$ sind alle Elemente invertierbar. Das Inverse von a wird mit $-a$ bezeichnet.
- 4 In $(\{0, 1\}, +_2)$ sind beide Elemente invertierbar. Beide sind zu sich selbst invers.

$$\begin{aligned} 0 +_2 0 &= 0 \\ 1 +_2 1 &= 0 \end{aligned}$$

$+_2$		0	1
0		0	1
1		1	0

invertierbares Element, inverses Element

Beispiel

- 5 In (\mathbb{N}, \cdot) und (\mathbb{N}_0, \cdot) ist nur das Element 1 invertierbar. Es ist zu sich selbst invers.
- 6 In (\mathbb{Z}, \cdot) sind nur 1 und -1 invertierbar. Beide sind zu sich selbst invers.
- 7 In (\mathbb{Q}, \cdot) , (\mathbb{R}, \cdot) und (\mathbb{C}, \cdot) sind alle Elemente bis auf 0 invertierbar. Das Inverse von a wird mit a^{-1} oder $1/a$ bezeichnet.
- 8 In $(\{0, 1\}, \cdot_2)$ ist nur das Element 1 invertierbar. Es ist zu sich selbst invers.

\cdot_2		0	1
0		0	0
1		0	1

allgemeine Notation

- Wir bezeichnen eine allgemeine Halbgruppe oft mit (H, \star) .
- Das neutrale Element (wenn es existiert) heißt häufig e .
- Das Inverse von $a \in H$ wird (wenn es existiert) häufig mit a' bezeichnet.
- Das neutrale Element e (wenn es existiert) ist immer invertierbar und zu sich selbst invers: $e' = e$.

- Wir sprechen von einer **Halbgruppe in additiver Notation** $(H, +)$, wenn wir die Verknüpfung als „**Addition**“ bezeichnen und mit $+$ (oder ähnlich) notieren.
- Das neutrale Element (wenn es existiert) heißt dann häufig das **Nullelement** 0_H .
- Das Inverse von $a \in H$ wird dann (wenn es existiert) häufig mit $-a$ bezeichnet.
- Das neutrale Element 0_H (wenn es existiert) ist immer invertierbar und zu sich selbst invers: $-0_H = 0_H$.

additive Notation

- Für $n \in \mathbb{N}$ und $a \in H$ ist na eine Abkürzung für $a + \cdots + a$ (n -mal).
- Besitzt H das neutrale Element 0_H , so definieren wir auch $0a := 0_H$.
- Ist weiter $a \in H$ invertierbar, dann ist auch na invertierbar für $n \in \mathbb{N}_0$, und wir setzen $(-n)a := -(na)$.

- Es gilt

$$n(\underbrace{ma}_{\in H}) = (\underbrace{n \cdot m}_{\in \mathbb{Z}})a \quad \text{und} \quad (n+m)a = na + ma$$

Handwritten annotations:
- A squiggly line above $\in \mathbb{Z}$ with an arrow pointing to $n \cdot m$.
- An arrow from $\in \mathbb{Z}$ pointing to n in $(n+m)a$.
- An arrow from $\in \mathbb{Z}$ pointing to m in $(n+m)a$.
- An arrow from $\in H$ pointing to a in $na + ma$.

für alle $n, m \in \mathbb{Z}$, für die beide Ausdrücke in der jeweiligen Gleichung definiert sind.

multiplikative Notation

- Wir sprechen von einer **Halbgruppe in multiplikativer Notation** (H, \cdot) , wenn wir die Verknüpfung als „**Multiplikation**“ bezeichnen und mit \cdot (oder ähnlich) notieren.
- Das neutrale Element (wenn es existiert) heißt dann häufig das **Einselement** 1_H .
- Das Inverse von $a \in H$ wird dann (wenn es existiert) häufig mit a^{-1} bezeichnet.
- Das neutrale Element 1_H (wenn es existiert) ist immer invertierbar und zu sich selbst invers: $1_H^{-1} = 1_H$.

multiplikative Notation

- Für $n \in \mathbb{N}$ und $a \in H$ ist a^n eine Abkürzung für $a \cdot \dots \cdot a$ (n -mal).
- Besitzt H das neutrale Element 1_H , so definieren wir auch $a^0 := 1_H$.
- Ist weiter $a \in H$ invertierbar, dann ist auch a^n invertierbar für $n \in \mathbb{N}_0$, und wir setzen $a^{-n} = (a^n)^{-1}$.
- Es gilt

$$(a^n)^m = a^{n \cdot m} \quad \text{und} \quad a^{n+m} = a^n \cdot a^m$$

für alle $n, m \in \mathbb{Z}$, für die beide Ausdrücke in der jeweiligen Gleichung definiert sind.

Kompositionsnotation

- Wir sprechen von einer **Halbgruppe in Kompositionsnotation** (H, \circ) , wenn wir die Verknüpfung als „**Komposition**“ bezeichnen und mit \circ (oder ähnlich) notieren.
- Das neutrale Element (wenn es existiert) heißt dann häufig die **Identität** id .
- Das Inverse von $a \in H$ wird dann (wenn es existiert) häufig mit a^{-1} bezeichnet. $a \circ a^{-1} = \text{id}$
- Das neutrale Element id (wenn es existiert) ist immer invertierbar und zu sich selbst invers: $\text{id}^{-1} = \text{id}$.

Kompositionsnotation

- Für $n \in \mathbb{N}$ und $a \in H$ ist a^n eine Abkürzung für $a \circ \cdots \circ a$ (n -mal).
- Besitzt H das neutrale Element id , so definieren wir auch $a^0 := \text{id}$.
- Ist weiter $a \in H$ invertierbar, dann ist auch a^n invertierbar für $n \in \mathbb{N}_0$, und wir setzen $a^{-n} = (a^n)^{-1}$.

- Es gilt

$$(a^n)^m = a^{n \cdot m} \quad \text{und} \quad a^{n+m} = a^n \circ a^m$$

für alle $n, m \in \mathbb{Z}$, für die beide Ausdrücke in der jeweiligen Gleichung definiert sind.

Definition

Ein Monoid (H, \star) heißt eine **Gruppe**, wenn jedes Element aus H ein Inverses besitzt.

Inverse sind eindeutig

Beispiel

- 1 $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ und $(\mathbb{C}, +)$ sind Gruppen. ✓
- 2 $(\mathbb{Q}_{\neq 0}, \cdot)$, $(\mathbb{R}_{\neq 0}, \cdot)$ und $(\mathbb{C}_{\neq 0}, \cdot)$ sind Gruppen. ✓
- 3 In jedem Monoid (H, \star) ist die Menge der invertierbaren Elemente

$$E(H, \star) := \{a \in H \mid a \text{ ist invertierbar}\}$$

eine Gruppe, genannt die **Einheitengruppe** $E(H, \star)$ von (H, \star) .

Beispiel

- 4 Für $m \in \mathbb{N}$ bildet die Menge $\mathbb{Z}_m := \{0, 1, \dots, m-1\}$ mit der Verknüpfung $+_m$ (**Addition modulo m**) eine Gruppe.

Fall $m=2$ bereits bekannt

$+_m$	0	1	...	$m-1$
0	0	1	...	$m-1$
1	1	2	...	0
\vdots	\vdots	\vdots		\vdots
$m-1$	$m-1$	0	1	...

$\{f \mid f: X \rightarrow G\}$

- 5 Ist X eine Menge und (G, \star) eine Gruppe, dann ist (G^X, \star) eine Gruppe. Inverse zu f ist $f' : X \rightarrow G$ mit $f'(x) = f(x)^{-1}$, dann ist nämlich $(f \star f')(x) = f(x) \star f'(x) = e$.
- 6 (X^X, \circ) ist keine Gruppe, sobald X zwei oder mehr Elemente enthält. Die invertierbaren Elemente sind genau die bijektiven Funktionen $X \rightarrow X$.

Satz

Es sei (G, \star) eine Gruppe mit neutralem Element e .

1 Kürzungsregeln

$$a \star b_1 = a \star b_2 \quad \Rightarrow \quad b_1 = b_2$$

$$b_1 \star a = b_2 \star a \quad \Rightarrow \quad b_1 = b_2$$

Beweis. $a \star b_1 = a \star b_2$
 $\Rightarrow (a' \star a) \star b_1 = (a' \star a) \star b_2$
 $\Rightarrow e \star b_1 = e \star b_2$
 $\Rightarrow b_1 = b_2$

Rest analog

Rechenregeln für Inverse

Satz

Es sei (G, \star) eine Gruppe mit neutralem Element e .

- ② In einer Gruppe reicht es für den Nachweis, dass a und b Inverse voneinander sind, aus, diese in einer der beiden Reihenfolgen miteinander zu verknüpfen:

$$a \star b = e \Rightarrow b = a'$$

$$a \star b = e \Rightarrow a = b'$$

Beweis. Es seien $a, b \in G$ mit $a \star b = e$.

Andererseits ist a invertierbar, es gilt $a \star a' = e$.

Also: $a \star b = a \star a' \stackrel{\text{①}}{\Rightarrow} b = a'$.

Zweite Aussage genauso.

Rechenregeln für Inverse

Satz

Es sei (G, \star) eine Gruppe mit neutralem Element e .

- ③ Die Invertierung ist **involutorisch**, d. h., es gilt

$$(a')' = a$$

- ④ Für das inverse Element zu $a \star b$ gilt

$$(a \star b)' = b' \star a'$$

Beweis. ③ Ist a die Inverse von a' ?

$$a \star a' = e \quad \checkmark$$

$$a' \star a = e \quad \checkmark$$

$$\begin{aligned} \textcircled{4} \quad (a \star b) \star (b' \star a') &= a \star (b \star b') \star a' \\ &= a \star e \star a' = a \star a' = e \end{aligned}$$

Gruppenkriterium mit Translationen

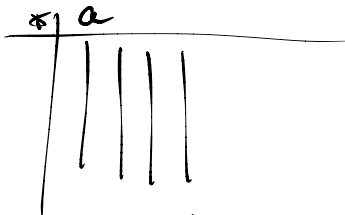
Lemma

notwendiges Kriterium

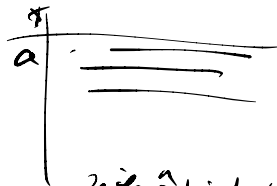
- 1 Ist (G, \star) eine Gruppe, so sind alle Rechtstranslationen \star_a und alle Linkstranslation ${}_a\star$ **bijektive** Abbildungen $G \rightarrow G$.

hinreichendes Kriterium

- 2 Ist (H, \star) eine nichtleere Halbgruppe und sind alle Rechtstranslationen \star_a und alle Linkstranslationen ${}_a\star$ **surjektive** Abbildungen, dann ist (H, \star) eine Gruppe.



Spalte $\hat{=}$ Rechtstranslation



Zeile $\hat{=}$ Linkstranslation

Gruppenkriterium mit Translationen

Beispiel *Sudoku-Kriterium*

Ist die Menge $\{\heartsuit, \boxtimes, \bullet, \otimes, \blacklozenge, \blacktriangleright\}$ mit den Verknüpfungen \star bzw. \square eine Gruppe? (Assoziativität wurde bereits geprüft und bestätigt.)

\star	\boxtimes	\bullet	\otimes	\blacklozenge	\heartsuit	\blacktriangleright
\blacklozenge	\bullet	\blacktriangleright	\heartsuit	\otimes	\blacklozenge	\boxtimes
\boxtimes	\heartsuit	\otimes	\bullet	\blacktriangleright	\boxtimes	\blacklozenge
\heartsuit	\boxtimes	\bullet	\otimes	\blacklozenge	\heartsuit	\blacktriangleright
\bullet	\blacklozenge	\heartsuit	\blacktriangleright	\boxtimes	\bullet	\otimes
\otimes	\blacktriangleright	\boxtimes	\blacklozenge	\heartsuit	\otimes	\bullet
\blacktriangleright	\otimes	\blacklozenge	\boxtimes	\bullet	\blacktriangleright	\heartsuit

Gruppe


\square	\boxtimes	\bullet	\otimes	\blacklozenge	\heartsuit	\blacktriangleright
\blacklozenge	\blacklozenge	\bullet	\heartsuit	\blacklozenge	\heartsuit	\bullet
\boxtimes	\boxtimes	\bullet	\otimes	\blacklozenge	\heartsuit	\blacktriangleright
\heartsuit	\heartsuit	\heartsuit	\heartsuit	\heartsuit	\heartsuit	\heartsuit
\bullet	\bullet	\blacklozenge	\heartsuit	\bullet	\heartsuit	\blacklozenge
\otimes	\otimes	\bullet	\boxtimes	\heartsuit	\heartsuit	\otimes
\blacktriangleright	\blacktriangleright	\blacklozenge	\otimes	\bullet	\heartsuit	\boxtimes

keine Gruppe

Gruppenkriterium mit Translationen

Beispiel

Assoziativität der Verknüpfung ist Voraussetzung für die Anwendung des Gruppenkriteriums! Die Menge $\{\heartsuit, \boxtimes, \bullet\}$ mit der Verknüpfung \star

\star	\heartsuit	\boxtimes	
\heartsuit	\bullet	\boxtimes	\heartsuit
\boxtimes	\heartsuit	\bullet	\boxtimes
\bullet	\boxtimes	\heartsuit	\bullet

ist **keine** Gruppe, da \star nicht assoziativ ist!

$$(\heartsuit \star \heartsuit) \star \boxtimes = \bullet \star \boxtimes = \heartsuit$$

$$\heartsuit \star (\heartsuit \star \boxtimes) = \heartsuit \star \boxtimes = \boxtimes$$

Kommutativität

Eigenschaft von $+$

Definition

Eine Halbgruppe bzw. ein Monoid bzw. eine Gruppe (H, \star) heißt **kommutativ** oder **abelsch**, wenn gilt:

$$x \star y = y \star x \quad \text{für alle } x, y \in H.$$

Beispiel

- ① $(\mathbb{N}, +)$, $(\mathbb{N}_0, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ und $(\mathbb{C}, +)$ sind kommutativ ✓
- ② (\mathbb{N}, \cdot) , (\mathbb{N}_0, \cdot) , (\mathbb{Z}, \cdot) , (\mathbb{Q}, \cdot) , (\mathbb{R}, \cdot) und (\mathbb{C}, \cdot) sind ebenfalls kommutativ ✓
- ③ $(\{0, 1\}, +_2)$ und $(\{0, 1\}, \cdot_2)$ ebenfalls ✓
 (X^X, \circ) ist nicht kommutativ

die symmetrische Gruppe

Definition

Es sei $X \neq \emptyset$ eine Menge und $S(X) := \{f: X \rightarrow X \mid f \text{ ist bijektiv}\}$.

- $(S(X), \circ)$ heißt die symmetrische Gruppe auf X .

Jedes Element von $S(X)$ heißt eine **Permutation** von X .

- Ist $X = \llbracket 1, n \rrbracket$ für $n \in \mathbb{N}$, so schreiben wir auch S_n und sprechen von der **symmetrischen Gruppe vom Grad n** .

Jedes $\sigma \in S_n$ heißt eine Permutation von $\llbracket 1, n \rrbracket$.

Darstellung einer Permutation $\sigma \in S_n$:

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

S_n hat $n!$ Elemente. $n! = 1 \cdot 2 \cdot \cdots \cdot n$ $0! = 1$

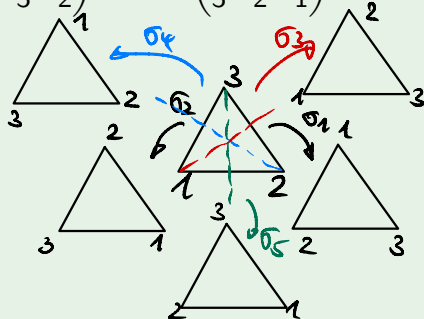
die symmetrische Gruppe vom Grad 3

Beispiel

Die symmetrische Gruppe S_3 hat $3! = 6$ Elemente:

$$\sigma_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \text{Drehungen}$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \text{Spiegelungen}$$



$$\sigma_4 \circ \sigma_3 = \sigma_2$$
$$\sigma_3 \circ \sigma_4 = \sigma_1$$

nicht kommutativ

Transposition

Definition

Eine Permutation $\sigma \in S_n$, $n \in \mathbb{N}$, heißt eine Transposition, wenn es Zahlen $i, j \in \llbracket 1, n \rrbracket$ mit $i \neq j$ gibt, sodass σ i und j vertauscht und den Rest von $\llbracket 1, n \rrbracket$ unverändert lässt. Wir schreiben dann $\sigma = \tau(i, j)$.

Es gibt $\binom{n}{2} = \frac{1}{2}n(n-1)$ verschiedene Transpositionen

Satz

Es sei $n \in \mathbb{N}$. Jede Permutation $\sigma \in S_n$ lässt sich als Komposition von $0 \leq r \leq n-1$ Transpositionen schreiben. *nicht evident!*

\uparrow \uparrow
Beweis durch vollständige Induktion.

Schwanken sind schief

Zerlegung in Transpositionen

Beispiel $n=4$, $r=n-1=3$ Transpos. werden gebraucht

$$\begin{array}{l} \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}}_{=\sigma} \xrightarrow{\tau(4,1)\circ} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & \mathbf{1} & \mathbf{4} \end{pmatrix} \\ \xrightarrow{\tau(3,1)\circ} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & \mathbf{1} & \mathbf{3} & 4 \end{pmatrix} \\ \xrightarrow{\tau(2,1)\circ} \begin{pmatrix} 1 & 2 & 3 & 4 \\ \mathbf{1} & \mathbf{2} & 3 & 4 \end{pmatrix} \end{array}$$

$$\tau(2,1)\circ\tau(3,1)\circ\tau(4,1)\circ\sigma = \text{id}$$

$$\Rightarrow \sigma = \tau(4,1)\circ\tau(3,1)\circ\tau(2,1)$$

Fehlstand und Signum einer Permutation

Definition

Es sei $n \in \mathbb{N}$ und σ eine Permutation in S_n .

- 1 Ein Indexpaar $(i, j) \in \llbracket 1, n \rrbracket^2$ heißt ein **Fehlstand** von σ , wenn $i < j$ und $\sigma(i) > \sigma(j)$ gilt.
- 2 Das **Signum** von σ ist

$$\operatorname{sgn} \sigma := \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

Beispiel 3 Fehlstände

$$\operatorname{sgn} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \frac{\overset{2-3}{\circlearrowleft}}{\underset{2-1}{\circlearrowright}} - \frac{\overset{1-3}{\circlearrowleft}}{\underset{3-1}{\circlearrowright}} + \frac{\overset{1-2}{\circlearrowleft}}{\underset{3-2}{\circlearrowright}} = (-1)^3 = -1$$

Eigenschaften von Signum

Definition

Es sei $n \in \mathbb{N}$ und σ eine Permutation in S_n .

σ heißt eine gerade Permutation im Fall $\text{sgn } \sigma = 1$.

σ heißt eine ungerade Permutation im Fall $\text{sgn } \sigma = -1$.

• $\text{sgn } \sigma = (-1)^{\text{Anzahl der Fehlstände von } \sigma}$ =: Parität von σ

• $\text{sgn id} = 1$ und $\text{sgn } \tau = -1$ für jede Transposition τ

• $\text{sgn}(\sigma_1 \circ \sigma_2) = (\text{sgn } \sigma_1) \cdot (\text{sgn } \sigma_2)$

*sgn ist verträglich mit
0 und \cdot !*

• $\sigma = \tau_1 \circ \dots \circ \tau_r$ (Komposition von $r \in \mathbb{N}$ Transpositionen in S_n)
impliziert $\text{sgn } \sigma = (-1)^r$