Lineare Algebra I

Woche 04

07.11.2023 und 09.11.2023

Algebraische Strukturen

Definition

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

Beispiel

- Halbgruppe
- Gruppe
- Ring
- Körper
- Vektorraum

Verknüpfung

Definition

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

$$\star\colon X \times X \to X.$$

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

Beispiel

$$+\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N} \qquad \text{Addition}$$

$$\cdot\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N} \qquad \text{Multiplikation}$$

Verknüpfung

Beispiel

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

$$\begin{array}{c|cc} +_2 & 0 & 1 \\ \hline 0 & & \\ 1 & & \end{array} \qquad \begin{array}{c|cc} \cdot_2 & 0 & 1 \\ \hline 0 & & \\ 1 & & \end{array}$$

2.

3.

Halbgruppe

Definition

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

Beispiel

1. $(\mathbb{N}, +)$, $(\mathbb{N}_0, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ und $(\mathbb{C}, +)$
2. $(\mathbb{N}, \cdot)$, $(\mathbb{N}_0, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$ und $(\mathbb{C}, \cdot)$
3. $(\{0, 1\}, +_2)$ und $(\{0, 1\}, \cdot_2)$

Halbgruppe

Beispiel

4.

5.

6. $(\mathcal{P}(X), \cap)$, $(\mathcal{P}(X), \cup)$ und $(\mathcal{P}(X), \triangle)$

neutrales Element

Definition

Es sei $(H, \star)$ eine Halbgruppe.

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

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.

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.

4.

$+_2$	0	1
0		
1		

$\cdot_2$	0	1
0		
1		

Translationen

Definition

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

$$\star_a \colon H \ni x \mapsto x \star a \in H \quad \text{die } \textbf{Rechtstranslation} \text{ mit } a,$$
$${}_a\star \colon H \ni x \mapsto a \star x \in H \quad \text{die } \textbf{Linkstranslation} \text{ mit } a.$$

Beispiel

1.
2.

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

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.

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.

$+_2$	0	1
0		
1		

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		
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: $e' = e$.

additive Notation

- 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 $n\, a$ eine Abkürzung für $a + \cdots + a$ (n-mal).

- Besitzt H das neutrale Element 0_H, so definieren wir auch $0\, a \coloneqq 0_H$.

- Ist weiter $a \in H$ invertierbar, dann ist auch $n\, a$ invertierbar für $n \in \mathbb{N}_0$, und wir setzen $(-n)\, a \coloneqq -(n\, a)$.

- Es gilt

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

  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.

- Das neutrale Element id (wenn es existiert) ist immer invertierbar und zu sich selbst invers: $\mathrm{id}^{-1} = \mathrm{id}$.

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 $a^0 \coloneqq \mathrm{id}$.
- 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.

Gruppe

Definition

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

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 $(H, \star)$.

Gruppe

Beispiel

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

$+_m$	0	1	$\cdots$	$m-1$
0				
1				
$\vdots$				
$m-1$				

5. Ist X eine Menge und $(G, \star)$ eine Gruppe, dann ist $(G^X, \star)$ eine Gruppe.

6. $(X^X, \circ)$ ist keine Gruppe, sobald X zwei oder mehr Elemente enthält.

Rechenregeln für Inverse

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.

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:

$$\begin{aligned} a \star b = e \quad &\Rightarrow \quad b = a' \\ a \star b = e \quad &\Rightarrow \quad a = b' \end{aligned}$$

Beweis.

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.

Gruppenkriterium mit Translationen

Lemma

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

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.

Gruppenkriterium mit Translationen

Beispiel

Ist die Menge {♡, ⊠, ◐, ⊗, ⬙, ⊳} mit den Verknüpfungen $\star$ bzw. $\Box$ eine Gruppe? (Assoziativität wurde bereits geprüft und bestätigt.)

$\star$	⊠	◐	⊗	⬙	♡	⊳
⬙	◐	⊳	♡	⊗	⬙	⊠
⊠	♡	⊗	◐	⊳	⊠	⬙
♡	⊠	◐	⊗	⬙	♡	⊳
◐	⬙	♡	⊳	⊠	◐	⊗
⊗	⊳	⊠	⬙	♡	⊗	◐
⊳	⊗	⬙	⊠	◐	⊳	♡

$\Box$	⊠	◐	⊗	⬙	♡	⊳
⬙	⬙	◐	♡	⬙	♡	◐
⊠	⊠	◐	⊗	⬙	♡	⊳
♡	♡	♡	♡	♡	♡	♡
◐	◐	⬙	♡	◐	♡	⬙
⊗	⊗	◐	⊠	♡	♡	⊗
⊳	⊳	⬙	⊗	◐	♡	⊠

Gruppenkriterium mit Translationen

Beispiel

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

$\star$	$\heartsuit$	$\boxtimes$	$\otimes$
$\heartsuit$	$\LEFTcircle$	$\boxtimes$	$\heartsuit$
$\boxtimes$	$\heartsuit$	$\LEFTcircle$	$\boxtimes$
$\LEFTcircle$	$\boxtimes$	$\heartsuit$	$\LEFTcircle$

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

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

Kommutativität

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 $(\mathbb{C}, +)$
2. $(\mathbb{N}, \cdot)$, $(\mathbb{N}_0, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$und $(\mathbb{C}, \cdot)$
3. $(\{0, 1\}, +_2)$ und $(\{0, 1\}, \cdot_2)$

Definition

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

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

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

- Ist $X = [\![1, n]\!]$ 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 $[\![1, n]\!]$.

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.

die symmetrische Gruppe vom Grad 3

Beispiel

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

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

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

Transposition

Definition

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

Satz

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

Beweis durch vollständige Induktion.

Zerlegung in Transpositionen

Beispiel

$$\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 4 & 1\end{pmatrix} \xrightarrow{\tau(4,1)\circ} \begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 1 & 4\end{pmatrix}$$

$$\xrightarrow{\tau(3,1)\circ} \begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 3 & 4\end{pmatrix}$$

$$\xrightarrow{\tau(2,1)\circ} \begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 2 & 3 & 4\end{pmatrix}$$

Fehlstand und Signum einer Permutation

Definition

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

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

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

Beispiel

$$\operatorname{sgn} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} =$$

Eigenschaften von Signum

Definition

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

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

- $\operatorname{sgn} \sigma = (-1)^{\text{Anzahl der Fehlstände von } \sigma} =:$ **Parität von σ**
- $\operatorname{sgn} \operatorname{id} = 1$ und $\operatorname{sgn} \tau = -1$ für jede Transposition τ
- $\operatorname{sgn}(\sigma_1 \circ \sigma_2) = (\operatorname{sgn} \sigma_1) \cdot (\operatorname{sgn} \sigma_2)$
- $\sigma = \tau_1 \circ \cdots \circ \tau_r$ (Komposition von $r \in \mathbb{N}$ Transpositionen in S_n) impliziert $\operatorname{sgn} \sigma = (-1)^r$