Lineare Algebra I

Woche 04

04.11.2025 und 06.11.2025

§ 6.2 Umkehrfunktion

Umkehrfunktion

Definition 6.22

Es sei $f\colon X \to Y$ eine Funktion.

f heißt **invertierbar**, wenn es eine Funktion $g\colon Y \to X$ gibt mit

$$g \circ f = \mathrm{id}_X \quad \text{und} \quad f \circ g = \mathrm{id}_Y.$$

In diesem Fall heißt g die **Umkehrfunktion** zu f.

Die Umkehrfunktion ist eindeutig bestimmt und wieder bijektiv.

Umkehrfunktion

Beispiel, siehe auch Beispiel 6.26

$$f(x) = \sin(x)$$

Umkehrfunktion der Komposition

Satz 6.28

Es seien $f\colon X \to Y$ und $g\colon Y \to Z$ bijektive Funktionen.

Dann ist auch $g \circ f$ bijektiv, und die Umkehrfunktion ist gegeben durch

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

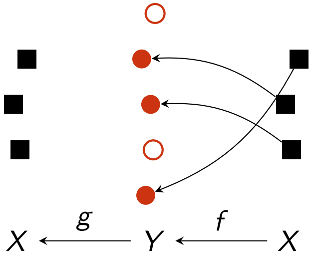
Beweis.

Satz 6.29

Es sei $f\colon X \to Y$ eine Funktion und $X \neq \emptyset$.

Dann sind äquivalent:

1. f ist injektiv.
2. Es existiert eine Abbildung $g\colon Y \to X$ mit der Eigenschaft $g \circ f = \mathrm{id}_X$. Eine solche Abbildung heißt eine **Linksinverse** von f. Sie ist notwendig surjektiv. Ihre Einschränkung $g|_{f(X)}$ auf das Bild von f ist eindeutig.



§ 6.3 Mächtigkeit von Mengen

Gleichmächtigkeit von Mengen

Definition 6.31

Zwei Mengen X und Y heißen **gleichmächtig**, wenn es eine bijektive Abbildung $f\colon X \to Y$ gibt. Wir schreiben in diesem Fall $X \sim Y$.

- Gleichmächtigkeit ist eine Äquivalenzrelation auf der Klasse aller Mengen.
- Die Äquivalenzklassen heißen **Kardinalzahlen**.

Endlichkeit, Abzählbarkeit, Überabzählbarkeit

Definition 6.32

Eine Menge X heißt

- **endlich**, wenn $X \sim [\![1, n]\!]$ für ein $n \in \mathbb{N}_0$ gilt.
  Die Zahl n heißt dann die **Mächtigkeit** oder **Kardinalität** von X.
  Wir schreiben: $\#X = n$.
- **unendlich**, wenn X nicht endlich ist.
- **abzählbar unendlich**, wenn $X \sim \mathbb{N}$ gilt.
- **abzählbar**, wenn X entweder endlich oder abzählbar unendlich ist.
- **überabzählbar**, wenn X nicht abzählbar ist.

Beispiel 6.33

1. Die Menge der ganzen Zahlen $\mathbb{Z}$ ist gleichmächtig zur Menge der geraden ganzen Zahlen $\{2\,n \mid n \in \mathbb{Z}\}$. Sie ist abzählbar unendlich.
2. Die Menge der rationalen Zahlen $\mathbb{Q}$ ist abzählbar unendlich.
3. Die Vereinigung abzählbar vieler abzählbarer Mengen ist wieder abzählbar.
4. Die Menge der reellen Zahlen $\mathbb{R}$ ist überabzählbar.

Injektivität, Surjektivität, Bijektivität für endliche Mengen

Satz 6.35

Es seien X und Y endliche, gleichmächtige Mengen und $f\colon X \to Y$ eine Funktion. Dann sind äquivalent:

1. f ist injektiv.
2. f ist surjektiv.
3. f ist bijektiv.

Vergleich von Mächtigkeiten

Definition 6.36

Es seien X und Y Mengen.

X ist **höchstens gleichmächtig** zu Y, wenn es eine injektive Abbildung $f: X \to Y$ gibt. Wir schreiben in diesem Fall $X \lesssim Y$ oder auch $Y \gtrsim X$.

Das ist eine Ordnungsrelation auf der Klasse aller Kardinalzahlen.

- Reflexivität:
- Transitivität:
- Antisymmetrie: Satz von Cantor-Bernstein-Schröder

§ 6.4 Familien und Folgen

Familie

Definition 6.38

Es seien I und Y Mengen.

1. Eine Abbildung
$$I \ni i \mapsto y(i) \coloneqq y_i \in Y$$
heißt eine **Familie (mit Werten) in Y** mit der **Indexmenge I**.
Kurz wird diese auch mit $(y_i)_{i \in I}$ bezeichnet.

2. Für $i \in I$ heißt y_i das **Mitglied** der Familie $(y_i)_{i \in I}$ zum Index i.

3. Ist $I_0 \subseteq I$, dann heißt $(y_i)_{i \in I_0}$ eine **Teilfamilie** von $(y_i)_{i \in I}$, und $(y_i)_{i \in I}$ heißt eine **Oberfamilie** von $(y_i)_{i \in I_0}$.
Die Teil- bzw. Oberfamilie heißt **echt** im Fall $I_0 \subsetneq I$.

Familie

Definition 6.38

Es seien I und Y Mengen.

4. Ist I endlich mit $\#I = n \in \mathbb{N}_0$, so heißt $(y_i)_{i \in I}$ eine **endliche Familie** mit n Mitgliedern.
5. Ist I unendlich, so heißt $(y_i)_{i \in I}$ eine **unendliche Familie**.
6. Ist I abzählbar unendlich, so heißt $(y_i)_{i \in I}$ eine **abzählbar unendliche Familie**.
7. Ist $I = \emptyset$, so heißt $(y_i)_{i \in I}$ die **leere Familie in Y**, kurz: $()$.
   Andernfalls heißt I eine **nichtleere Familie in Y**.
8. Zwei Familien $(y_i)_{i \in I}$ und $(z_j)_{j \in J}$ heißen **gleichmächtig**, wenn ihre Indexmengen gleichmächtig sind ($I \sim J$).

geordnete Familie, Folge, endliche Folge, Tupel

Definition 6.39

Es seien I und Y Mengen.

1. Ist I totalgeordnet, dann heißt eine Familie $(y_i)_{i \in I}$ in Y auch eine **geordnete Familie**.

2. Ist speziell $I = \mathbb{N}$ oder allgemeiner $I = \{n \in \mathbb{Z} \mid n \geqslant n_0\}$ mit einem Startindex $n_0 \in \mathbb{Z}$, so heißt $(y_i)_{i \in I}$ eine **Folge in Y**.
   Wir nennen die **Mitglieder einer Folge** auch **Glieder** der Folge oder **Folgenglieder**.

3. Ist speziell $I = [\![1, n]\!]$, so heißt $(y_i)_{i \in I}$ eine **endliche Folge in Y** mit n Mitgliedern oder der **Länge** n.

4. Wir können eine endliche Folge mit der Indexmenge $I = [\![1, n]\!]$ als **n-Tupel** $(y_1, y_2, \ldots, y_n)$ notieren.
   Insbesondere kann die leere Folge als () geschrieben werden.

Folge

Beispiel 6.41

§ 6.5 Das Auswahlaxiom

allgemeines kartesisches Produkt

Bisher hatten wir das **kartesische Produkt** von endlich vielen Mengen $A_1, \dots, A_n$ für $n \in \mathbb{N}$ definiert:

$$\bigtimes_{i=1}^{n} A_i := \Big\{ \underbrace{(a_1, \dots, a_n)}_{n\text{-}\mathbf{Tupel}} \,\Big|\, a_i \in A_i \text{ für } i = 1, \dots, n \Big\}$$

Definition 6.42

Allgemein ist das **kartesische Produkt** von Mengen A_i mit Indexmenge I definiert durch

$$\bigtimes_{i \in I} A_i := \Big\{ \underbrace{a \colon I \to \bigcup_{i \in I} A_i}_{\text{Funktion}} \,\Big|\, a(i) \in A_i \text{ für alle } i \in I \Big\}$$

Potenznotation von Funktionenmengen

Bemerkung 6.43

Es seien X und Y Mengen. Dann bezeichnet

$$Y^X := \{f \mid f\colon X \to Y \text{ ist eine Funktion}\}.$$

Beispiel

Auswahlaxiom

Kann man Elemente des kartesischen Produkts

$$\bigtimes_{i \in I} A_i := \Big\{ \underbrace{a \colon I \to \bigcup_{i \in I} A_i}_{\text{Funktion}} \;\Big|\; a(i) \in A_i \text{ für alle } i \in I \Big\}$$

überhaupt angeben?

Auswahlaxiom

Ist $\mathcal{A}$ eine Menge von nichtleeren Mengen, dann gibt es eine Funktion $F \colon \mathcal{A} \to \bigcup \mathcal{A}$, sodass gilt:

$$\forall A \in \mathcal{A} \; \big(F(A) \in A\big).$$

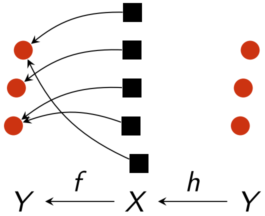
Eine solche Funktion F heißt **Auswahlfunktion** für $\mathcal{A}$, weil sie aus jedem Element A von $\mathcal{A}$ irgendein Element auswählt.

Auswirkungen des Auswahlaxioms

Satz 6.46

Folgende Aussagen sind in ZF zum Auswahlaxiom äquivalent:

1. Es sei I eine Menge, und weiter sei A_i eine nichtleere Menge für jedes $i \in I$. Dann ist das kartesische Produkt $\bigtimes_{i \in I} A_i$ nichtleer.
2. Es sei $f\colon X \to Y$ eine beliebige Funktion. Dann sind äquivalent:
   a. f ist surjektiv.
   b. Es existiert eine Abbildung $h\colon Y \to X$ mit der Eigenschaft $f \circ h = \mathrm{id}_Y$. Eine solche Abbildung heißt eine **Rechtsinverse** von f. Sie ist notwendig injektiv.
3. Es gilt das Lemma von Zorn 6.48.



Lemma 6.48

Es sei X mit der Relation $\preccurlyeq$ eine halbgeordnete Menge.

Weiter besitze jede totalgeordnete Teilmenge $A \subseteq X$ eine obere Schranke in X.

Dann existiert in X ein maximales Element.

Wir werden in der Vorlesung darauf hinweisen, wo Resultate vom Auswahlaxiom bzw. vom Lemma von Zorn abhängen.

§ 7 Halbgruppen und Gruppen

Definition 7.1

Es sei M eine Menge. Eine Abbildung $\star\colon M \times M \to M$ heißt eine **(innere) Verknüpfung** oder **(innere) Operation auf** M.

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

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

Beispiele

- Halbgruppe (§ 7)
- Gruppe (§ 7 und § 8)
- Ring (§ 9)
- Körper (§ 10)
- Vektorraum (§ 11)

Verknüpfung

Beispiel 7.2

Auf den natürlichen Zahlen $\mathbb{N}$ definieren wir die zwei Verknüpfungen

$$\begin{aligned} +\colon \mathbb{N} \times \mathbb{N} &\to \mathbb{N} && \text{Addition} \\ \cdot\colon \mathbb{N} \times \mathbb{N} &\to \mathbb{N} && \text{Multiplikation} \end{aligned}$$

Verknüpfung

Beispiel 7.2

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

$+_2$	0	1
0		
1		

$\cdot_2$	0	1
0		
1		

Verknüpfung

Beispiel 7.2

Es seien X und Y Mengen, und auf Y sei die Verknüpfung $\star$ definiert.

Verknüpfung

Beispiel 7.2

Es sei X eine Menge und $X^X = \{f \mid f\colon X \to X\}$.

§ 7.1 Halbgruppen

Halbgruppe

Definition 7.3

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

Beispiel 7.4

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 7.4

4.

5.

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

neutrales Element

Definition 7.6

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 7.7

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 7.8

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		

Halbgruppe mit/ohne neutralem/s Element

Beispiel 7.8

5. Es sei X eine Menge und $(H, \star)$ ein Monoid mit neutralem Element e. Dann ist $(H^X, \star)$ ein Monoid mit neutralem Element f, gegeben durch die konstante Funktion $f\colon X \to H$ mit $f(x) = e$ für alle $x \in X$.

6. $(\mathcal{P}(X), \cap)$ besitzt das neutrale Element X.

7. $(\mathcal{P}(X), \cup)$ besitzt das neutrale Element $\emptyset$.

8. $(\mathcal{P}(X), \triangle)$ besitzt das neutrale Element $\emptyset$.

Translationen

Definition 7.9

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

$$\begin{aligned} \star_a &: H \ni x \mapsto x \star a \in H \quad \text{die } \textbf{Rechtstranslation} \text{ mit } a, \\ {}_a\star &: H \ni x \mapsto a \star x \in H \quad \text{die } \textbf{Linkstranslation} \text{ mit } a. \end{aligned}$$

Beispiel 7.10

1. In $(\mathbb{R}, +)$ ist die Linkstranslation mit $b = \sqrt{2}$ gegeben durch die Abbildung $a \mapsto \sqrt{2} + a$. Sie ist wegen der Kommutativität von $+$ identisch zur Rechtstranslation mit b.
2. In $(\mathbb{R}^\mathbb{R}, \circ)$ sind die Links- und Rechtstranslationen mit g, definiert durch $g(x) = 2\,x$, gegeben durch

$$\begin{aligned} {}_g\circ &: \mathbb{R}^\mathbb{R} \ni f \mapsto g \circ f \in \mathbb{R}^\mathbb{R}, \quad \text{also } (g \circ f)(x) = 2\,f(x) \\ \circ_g &: \mathbb{R}^\mathbb{R} \ni f \mapsto f \circ g \in \mathbb{R}^\mathbb{R}, \quad \text{also } (f \circ g)(x) = f(2\,x). \end{aligned}$$

Unterhalbgruppe, Untermonoid

Definition 7.11

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

1. $U \subseteq H$ heißt **abgeschlossen** bzgl. $\star$, wenn $\star \colon H \times H \to H$ eingeschränkt werden kann zu $\star_U \colon U \times U \to U$. In diesem Fall heißt $\star_U$ die auf U **induzierte Verknüpfung**.

2. Eine bzgl. $\star$ abgeschlossene Teilmenge $U \subseteq H$ mit der Verknüpfung $\star_U$ heißt eine **Unterhalbgruppe von** $(H, \star)$. Manchmal schreibt man dies als $(U, \star_U) \leqslant (H, \star)$.

3. Ist $(H, \star)$ ein Monoid mit neutralem Element e, dann heißt eine bzgl. $\star$ abgeschlossene Teilmenge $U \subseteq H$, die auch das neutrale Element e enthält, ein **Untermonoid von** $(H, \star)$.

Beispiel 7.12

1. Die geraden Zahlen bilden ein Untermonoid von $(\mathbb{Z}, +)$ mit neutralem Element 0.

2. Es seien a, b, c paarweise verschieden.

   $(\mathcal{P}(\{a, b\}), \cap)$ bildet zwar eine Unterhalbgruppe des Monoids $(\mathcal{P}(\{a, b, c\}), \cap)$, aber kein Untermonoid, denn das neutrale Element $\{a, b, c\}$ fehlt in $\mathcal{P}(\{a, b\})$.

   Vielmehr ist $(\mathcal{P}(\{a, b\}), \cap)$ ein Monoid mit einem anderen neutralen Element, nämlich $\{a, b\}$, siehe Beispiel 7.8.

invertierbares Element, inverses Element

Definition 7.14

Es sei $(H, \star)$ ein Monoid mit neutralem Element e.

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

In diesem Fall heißt a' ein zu a **inverses Element** zu a.

a' ist Inverses zu a $\Leftrightarrow$ a ist Inverses zu a'

Lemma 7.15

Es sei $(H, \star)$ ein Monoid mit neutralem Element e. Ist $a \in H$ invertierbar und sind a_1' und a_2' beides Inverse zu a, dann gilt $a_1' = a_2'$.

Beweis.

invertierbare Elemente bilden ein Untermonoid

Lemma 7.16

Es sei $(H, \star)$ ein Monoid. Dann bilden die invertierbaren Elemente

$$E := \{a \in H \mid a \text{ ist invertierbar}\}$$

ein Untermonoid von $(H, \star)$.

Sind $a, b \in E$ und a', b' die zugehörigen inversen Elemente in H, dann gilt für das zu $a \star b$ inverse Element

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

Beweis.

invertierbares Element, inverses Element

Beispiel 7.17

1. $(\mathbb{N}, +)$ hat kein neutrales Element, also auch keine invertierbaren Elemente.
2. In $(\mathbb{N}_0, +)$ ist nur das neutrale 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		

invertierbares Element, inverses Element

Beispiel 7.17

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		

invertierbare Elemente können gekürzt werden

Lemma 7.18

Es sei $(H, \star)$ ein Monoid.
Für invertierbares $a \in H$ gelten die **Kürzungsregeln**

$$\begin{aligned} a \star b_1 = a \star b_2 \quad &\Rightarrow \quad b_1 = b_2 \\ b_1 \star a = b_2 \star a \quad &\Rightarrow \quad b_1 = b_2 \end{aligned}$$

für beliebige $b_1, b_2 \in H$.

Beweis.

Halbgruppen in allgemeiner Notation

Bemerkung 7.20

Verknüpfung	$\star$
neutrales Element	e
Inverse von a	a'

$a, b, c, e \in H \qquad A, B \subseteq H$

$$c \star A := \{c \star a \,|\, a \in A\}$$
$$A \star c := \{a \star c \,|\, a \in A\}$$
$$A \star B := \{a \star b \,|\, a \in A,\ b \in B\}$$
$$A' := \{a' \,|\, a \in A\}$$

Halbgruppen in additiver Notation

Bemerkung 7.20

Verknüpfung	$+$
neutrales Element	0_H
Inverse von a	$-a$

$a, b, c, 0_H \in H \qquad A, B \subseteq H$

$$c + A := \{c + a \,|\, a \in A\}$$
$$A + c := \{a + c \,|\, a \in A\}$$
$$A + B := \{a + b \,|\, a \in A,\ b \in B\}$$
$$-A := \{-a \,|\, a \in A\}$$

Für $n \in \mathbb{N}$ ist $n\, a$ eine Abkürzung für $a + \cdots + a$ (n-mal).

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

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

Es gilt $n\,(m\, a) = (n \cdot m)\, a$ und $(n + m)\, a = n\, a + m\, a$ für alle $n, m \in \mathbb{N}$ bzw. $n, m \in \mathbb{N}_0$ bzw. $n, m \in \mathbb{Z}$.

Halbgruppen in multiplikativer Notation

Bemerkung 7.20

Verknüpfung	$\cdot$
neutrales Element	1_H
Inverse von a	a^{-1}

$a, b, c, 1_H \in H \qquad A, B \subseteq H$

$$c \cdot A := \{c \cdot a \,|\, a \in A\}$$
$$A \cdot c := \{a \cdot c \,|\, a \in A\}$$
$$A \cdot B := \{a \cdot b \,|\, a \in A,\ b \in B\}$$
$$A^{-1} := \{a^{-1} \,|\, a \in A\}$$

Für $n \in \mathbb{N}$ ist a^n eine Abkürzung für $a \cdot \cdots \cdot a$ (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 $a^{-n} := (a^n)^{-1} = (a^{-1})^n$.

Es gilt $(a^n)^m = a^{n \cdot m}$ und $a^{n+m} = a^n \cdot a^m$ für alle $n, m \in \mathbb{N}$ bzw. $n, m \in \mathbb{N}_0$ bzw. $n, m \in \mathbb{Z}$.

Halbgruppen in Kompositionsnotation

Bemerkung 7.20

Verknüpfung	$\circ$
neutrales Element	id
Inverse von a	a^{-1}

$a, b, c, \mathrm{id} \in H \qquad A, B \subseteq H$

$$c \circ A := \{c \circ a \,|\, a \in A\}$$
$$A \circ c := \{a \circ c \,|\, a \in A\}$$
$$A \circ B := \{a \circ b \,|\, a \in A,\; b \in B\}$$
$$A^{-1} := \{a^{-1} \,|\, a \in A\}$$

Für $n \in \mathbb{N}$ ist a^n eine Abkürzung für $a \circ \cdots \circ a$ (n-mal).

Besitzt H das neutrale Element id, so definieren wir auch $a^0 := \mathrm{id}$.

Ist weiter $a \in H$ invertierbar, dann ist auch a^n invertierbar für $n \in \mathbb{N}_0$, und wir setzen $a^{-n} := (a^n)^{-1} = (a^{-1})^n$.

Es gilt $(a^n)^m = a^{n \cdot m}$ und $a^{n+m} = a^n \circ a^m$ für alle $n, m \in \mathbb{N}$ bzw. $n, m \in \mathbb{N}_0$ bzw. $n, m \in \mathbb{Z}$.