Lineare Algebra I

Woche 04

04.11.2025 und 06.11.2025

nächste Woche:
Vorlesung Mo, 10.11. um 14:15 !
Di, 11.11. um 9:20

§ 6.2 Umkehrfunktion

Umkehrfunktion

⟺ bijektiv

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
umkehrbar

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

inverse Funktion
In diesem Fall heißt g die **Umkehrfunktion** zu f. , geschrieben: f^{-1}.

Die Umkehrfunktion ist eindeutig bestimmt und wieder bijektiv.

$$g_1 = g_1 \circ \mathrm{id}_Y = g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2 = \mathrm{id}_X \circ g_2 = g_2$$

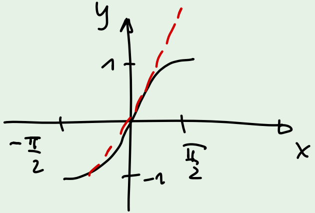
Unterscheide:

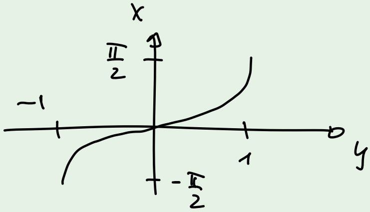
$f^{-1}(B)$	Urbild von $B \subseteq Y$ unter f
$f^{-1}(y)$	Wert der Umkehrfkt. f^{-1} bei $y \in Y$

Umkehrfunktion

Beispiel, siehe auch Beispiel 6.26

$X = [-\frac{\pi}{2}, \frac{\pi}{2}] \ni x \mapsto f(x) = \sin(x) \in [-1, 1]$ bijektiv





$f = \sin$

$f^{-1} = \arcsin$
$= „\sin^{-1}"$

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. $(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ \underbrace{(g^{-1} \circ g)}_{id_Y} \circ f = f^{-1} \circ f = id_X$

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ \underbrace{(f \circ f^{-1})}_{id_Y} \circ g^{-1} = g \circ g^{-1} = id_Z$$

$$Z \xleftarrow{g} Y \xleftarrow{f} X$$

$$Z \xrightarrow{g^{-1}} Y \xrightarrow{f^{-1}} X$$

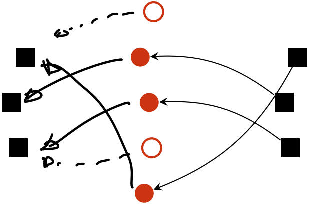
Charakterisierung der Injektivität

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.



$$X \xleftarrow{g} Y \xleftarrow{f} X$$

§ 6.3 Mächtigkeit von Mengen

Gleichmächtigkeit von Mengen

Definition 6.31

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

- Gleichmächtigkeit ist eine Äquivalenzrelation auf der Klasse aller Mengen.
- Die Äquivalenzklassen heißen **Kardinalzahlen**. enthalten $\mathbb{N}_0$

Die leere Menge ist nur zu sich selbst gleichmächtig.

Definition 6.32

n ist eindeutig!

Eine Menge X heißt

- **endlich**, wenn $X \sim \overbrace{[\![1, n]\!]}^{= \emptyset \text{ für } n=0}$ 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. Elemente sind nummerierbar
- **abzählbar**, wenn X entweder endlich oder abzählbar unendlich ist.
- **überabzählbar**, wenn X nicht abzählbar ist.

Endlichkeit, Abzählbarkeit, Überabzählbarkeit

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.

   $\mathbb{Z} \sim 2\mathbb{Z} \quad : \quad n \mapsto 2n$

   $\mathbb{Z} \sim \mathbb{N} \quad : \quad 0, 1, -1, 2, -2, \dots$

2. Die Menge der rationalen Zahlen $\mathbb{Q}$ ist abzählbar unendlich.

   $$\begin{array}{ccc} 1/1 & 2/1 & \cdots \\ 1/2 & 2/2 & \cdots \\ \vdots & \vdots & \end{array}$$

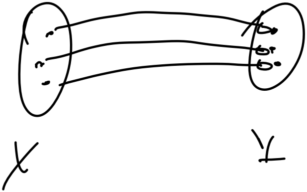
3. Die Vereinigung abzählbar vieler abzählbarer Mengen ist wieder abzählbar.

4. Die Menge der reellen Zahlen $\mathbb{R}$ ist **über**abzählbar.

Satz 6.35

Es seien X und Y endliche, gleichmächtige Mengen und $f : X \to Y$ 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.

Einbettung $f(X) \subseteq Y$

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

Das ist eine Ordnungsrelation auf der Klasse aller Kardinalzahlen.

- Reflexivität: $X \lesssim X$ wegen id_X
- Transitivität: $X \lesssim Y$, $Y \lesssim Z$
  $f\colon X \to Y$ inj, $g\colon Y \to Z$ inj $\Rightarrow$ $g \circ f\colon X \to Z$ inj.
  Lemma 6.19
- Antisymmetrie: Satz von Cantor-Bernstein-Schröder

Die Ordnung ist total $\Leftarrow$ Auswahlaxiom (AGT)

§ 6.4 Familien und Folgen

Familie

Definition 6.38

Es seien I und Y Mengen.

1. Eine Abbildung

$$I \ni i \mapsto y(i) := y_i \in Y$$

alle Mitglieder in derselben Menge 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 $I_0 \subsetneq I$.

Mengen

Elemente kommen nur einfach vor.

Familien

Mitglieder können mehrfach vorkommen.

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**.

   mit der üblichen Totalordnung $\leq$

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**.

   mit der üblichen Totalordnung $\leq$

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.

   kennen wir vom kart. Produkt $Y \times \cdots \times Y$

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

- $\mathbb{N} \ni n \mapsto y_n := \frac{1}{n} \in \mathbb{Q}_{\geq 0}$
- Fibonacci-Folge in $\mathbb{N}$

  $a_1 = 1, \; a_2 = 1$

  $a_{n+2} = a_{n+1} + a_n$ für $n \in \mathbb{N}$

§ 6.5 Das Auswahlaxiom

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

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

Abbildung
Funktion $\quad a \colon [\![1, n]\!] \to \bigcup_{i=1}^{n} A_i$

Definition 6.42

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

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

Analog zu $A^n = A^{[\![1,n]\!]} = \bigtimes_{i=1}^{n} A$ ist $A^I = \bigtimes_{i \in I} A$

Potenznotation von Funktionenmengen

Bemerkung 6.43

Es seien X und Y Mengen. Dann bezeichnet

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

Beispiel

- $\mathbb{R}^{\mathbb{N}}$ = Menge aller Folgen in $\mathbb{R}$
- $\{0,1\}^X$ = Menge aller „binärwertigen" Fkt.en auf X
  ist bijektiv zu $\mathcal{P}(X)$
- später: $\underline{Y}^X$ mit $\underline{Y}$ algebr. Struktur

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:

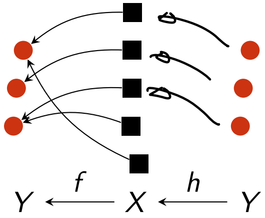
$$\forall A \in \mathcal{A} \,\big(F(A) \in A\big).$$

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

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.



Für solche endlichen Mengen brauchen wir das AoC nicht.

Lemma von Zorn

Lemma 6.48

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

Weiter besitze jede $\underbrace{\text{totalgeordnete Teilmenge}}_{\text{Kette}}$ $A \subseteq X$ 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

Algebraische Strukturen, Verknüpfungen

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	Woche	
Halbgruppe (§ 7)	4-6	eine Verknüpfung
Gruppe (§ 7 und § 8)		
Ring (§ 9)	7	zwei Verknüpfungen
Körper (§ 10)		
Vektorraum (§ 11)	8+	zwei Verknüpfungen (Kap. 3)

Verknüpfung

Beispiel 7.2

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

$$\left.\begin{aligned} +\colon \mathbb{N} \times \mathbb{N} &\to \mathbb{N} \qquad \text{Addition} \\ \cdot\colon \mathbb{N} \times \mathbb{N} &\to \mathbb{N} \qquad \text{Multiplikation} \end{aligned}\right\} \text{siehe Anhang A}$$

„$-$" ist keine Verknüpfung auf $\mathbb{N}$

Verknüpfungstafel

$*$ $\longrightarrow b$

Beispiel 7.2

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

$a \quad b$

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

Addition mod 2

$\cdot_2$	0	1
0	0	0
1	0	1

Multiplik. mod 2

Beispiel 7.2

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

Diese überträgt sich auf $Y^X = \{ f \mid f : X \to Y \}$ durch punktweise Anwendung:

$$* : Y^X \times Y^X \to Y^X$$

$$X \ni x \mapsto (f * g)(x) := f(x) * g(x) \in Y$$

für $f, g \in Y^X$

Beispiel 7.2

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

Dann ist die Komposition eine Verknüpfung auf X^X:

$$\circ : X^X \times X^X \to X^X$$

$$(f \circ g)(x) := f(g(x)) \in X$$

§ 7.1 Halbgruppen

Definition 7.3

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

$$(a \star b) \star c = a \star (b \star c) \quad \forall a, b, c \in H$$

Beispiel 7.4

1. $(\mathbb{N}, +)$, $(\mathbb{N}_0, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ und $(\mathbb{C}, +)$ Halbgruppen ✓

   „$-$" 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 $(\mathbb{C}, \cdot)$ Halbgruppen ✓

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

Halbgruppe (nicht immer nur auf „Zahlenmengen")

Beispiel 7.4

4. X eine Menge, $(H,*)$ eine Halbgruppe
   Dann ist $(H^X, *)$ eine Halbgruppe ✓
   $$\left.\begin{aligned}[(f*g)*h](x) &= (f*g)(x)*h(x) = [f(x)*g(x)]*h(x) \\ [f*(g*h)](x) &= \ldots = f(x)*[g(x)*h(x)]\end{aligned}\right\} =$$
   wegen Ass. in $(H,*)$
5. X eine Menge, $(X^X, \circ)$ ist Halbgruppe ✓
   Komposition $\circ$ ist assoziativ (Lemma 6.17)
6. $(\mathcal{P}(X), \cap)$, $(\mathcal{P}(X), \cup)$ und $(\mathcal{P}(X), \triangle)$ Halbgruppen ✓
   $\cap, \cup, \triangle$ sind assoziativ

Definition 7.6

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

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

$$e * a = a = a * e \qquad \forall a \in H$$

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. $e_1 = e_1 * e_2 = e_2$

e_2 ist neutral $\qquad$ e_1 ist neutral

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.

0 ist neutrales Element

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

1 ist neutrales Element

$\cdot_2$	0	1
0	0	0
1	0	1

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 $x \in X$.

   $(g * f)(x) = g(x) * f(x) = g(x) * e = g(x)$

   $(f * g)(x) = f(x) * g(x) = e * g(x) = g(x)$

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

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

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

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

Unterhalbgruppe, Untermonoid

Definition 7.11

also nicht nur in H

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** $(H, \star)$.

Unterhalbgruppe, Untermonoid

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.

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

$$a \star a' = e = a' \star a$$

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

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

e ist immer invertierbar und $e' = e$

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.

$$a_1' = a_1' \star e = a_1' \star (a \star a_2') = (a_1' \star a) \star a_2' = e \star a_2' = a_2'$$

invertierbare Elemente bilden ein Untermonoid

Lemma 7.16

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

$$E := \{a \in H \mid a \text{ ist invertierbar}\}$$ „Einheiten-Untermonoid"

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	0	1
1	1	0

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	0	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. $a * b_1 = a * b_2$

$$\Rightarrow (a' * a) * b_1 = (a' * a) * b_2$$

$$\Rightarrow e * b_1 = e * b_2$$

$$\Rightarrow b_1 = b_2$$

Bemerkung 7.20

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

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

$$c \star A := \{c \star a \mid a \in A\}$$

$$A \star c := \{a \star c \mid a \in A\}$$

$$A \star B := \{a \star b \mid a \in A,\ b \in B\}$$

$$A' := \{a' \mid a \in A\}$$

wenn alle invertierbar

Halbgruppen in additiver Notation

Bemerkung 7.20

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

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

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

wohldefiniert wegen der Assoziativität

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 $0\,a := 0_H$.

zu zeigen!

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

zu zeigen   zu zeigen

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 $a \cdot \dots \cdot a$ (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 $a^{-n} := (a^n)^{-1} = (a^{-1})^n$.

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. $n, m \in \mathbb{Z}$.