1 Grundstrukturen der Mathematik

Themen:

- Mathematische Logik
- Relationen
- Gruppen, Ringe, Körper

1.1 Mathematische Logik

Eine Formel oder ein Satz der Alltagssprache heißt *Aussage*, wenn sie wahr oder falsch sein kann.

1.1 Mathematische Logik

Eine Formel oder ein Satz der Alltagssprache heißt *Aussage*, wenn sie wahr oder falsch sein kann.

Beispiele: $2 < 5$, $3 = 5$, Sokrates hatte eine Glatze.

1.1 Mathematische Logik

Eine Formel oder ein Satz der Alltagssprache heißt *Aussage*, wenn sie wahr oder falsch sein kann.

Beispiele: $2 < 5$, $3 = 5$, Sokrates hatte eine Glatze.

In der Alltagssprache gibt es Aussagen (?), die wahr werden, indem man sie ausspricht. Welche?

Logische Konjunktionen

$$(A \textit{ oder } B) \text{ wahr} \quad \Leftrightarrow \quad A \text{ wahr oder } B \text{ wahr oder beide wahr,}$$

$$(A \textit{ und } B) \text{ wahr} \quad \Leftrightarrow \quad A \text{ wahr und } B \text{ wahr.}$$

Logische Konjunktionen

$(A \textit{ oder } B)$ wahr $\Leftrightarrow$ A wahr oder B wahr oder beide wahr,

$(A \textit{ und } B)$ wahr $\Leftrightarrow$ A wahr und B wahr.

Für *oder* und *und* schreiben wir

$\vee$ oder (nicht ausschließend) (von lat. vel)

$\wedge$ und

Logische Konjunktionen

$(A \textit{ oder } B)$ wahr $\Leftrightarrow$ A wahr oder B wahr oder beide wahr,

$(A \textit{ und } B)$ wahr $\Leftrightarrow$ A wahr und B wahr.

Für *oder* und *und* schreiben wir

- $\vee$ oder (nicht ausschließend) (von lat. vel)
- $\wedge$ und
- $\neg$ Verneinungszeichen

Wahrheitstafeln für die Konjunktionen

In Tafelform können wir die obigen Regeln so schreiben:

A\B	w	f
w	w	w
f	w	f

Tafel für $\vee$

A\B	w	f
w	w	f
f	f	f

Tafel für $\wedge$.

Verneinungsregeln

Es gelten die Verneinungsregeln für Aussagen A, B

$$\neg(A \vee B) \quad \Leftrightarrow \quad \neg A \wedge \neg B,$$

$$\neg(A \wedge B) \quad \Leftrightarrow \quad \neg A \vee \neg B,$$

Folgt direkt aus den Wahrheitstafeln.

Ein schwieriger Fall: Die Implikation

„Wenn es regnet, dann ist die Straße nass.“

Ein schwieriger Fall: Die Implikation

„Wenn es regnet, dann ist die Straße nass.“

„Wenn Albert Einstein den Nobelpreis nicht bekommen hätte,
dann wäre er an Hänschen Klein verliehen worden.“

Ein schwieriger Fall: Die Implikation

„Wenn es regnet, dann ist die Straße nass.“

„Wenn Albert Einstein den Nobelpreis nicht bekommen hätte,
dann wäre er an Hänschen Klein verliehen worden.“

Es gibt 2 heiße Kandidaten auf einen Preis, nämlich E und K.

„Wenn E den Preis nicht bekommen hätte,
dann wäre er an K verliehen worden.“

Wahrheitstafel der Implikation

Die Mathematik definiert die Wahrheit der Implikation durch die Wahrheitstafel

A\B	w	f
w	w	f
f	w	w

.

A=Voraussetzung, B=Behauptung

Wahrheitstafel der Implikation

Die Mathematik definiert die Wahrheit der Implikation durch die Wahrheitstafel

A\B	w	f
w	w	f
f	w	w

.

A=Voraussetzung, B=Behauptung

Eine Implikation ist daher immer wahr, wenn die Voraussetzung falsch ist. Damit sind alle Aussagen über mögliche Preisträger wahr.

Verneinung der Implikation

Aufgrund der Wahrheitstafeln ist

$$(A \Rightarrow B) \quad \Leftrightarrow \quad (\neg A \vee B)$$

Verneinung der Implikation

Aufgrund der Wahrheitstafeln ist

$$(A \Rightarrow B) \quad \Leftrightarrow \quad (\neg A \vee B)$$

Daraus folgt für die Verneinung der Implikation

$$\neg(A \Rightarrow B) \quad \Leftrightarrow \quad (A \wedge \neg B)$$

Der modus ponens

Ein mathematischer Beweis besteht aus einer Folge von Aussagen, die entweder von vorneherein als richtig angesehen werden oder aus der folgenden Schlussregel, dem *modus ponens*, abgeleitet werden können:

Der modus ponens

Ein mathematischer Beweis besteht aus einer Folge von Aussagen, die entweder von vorneherein als richtig angesehen werden oder aus der folgenden Schlussregel, dem *modus ponens*, abgeleitet werden können:

„Wenn es regnet, dann ist die Straße nass“	$A \Rightarrow B$
„Es regnet“	A
„Die Straße ist nass“	B

Die Antinomie des Epimenides

Wir nehmen an, es gibt nur Lügner, die immer lügen, und Wahrheitssprecher, die immer die Wahrheit sagen.

Die Antinomie des Epimenides

Wir nehmen an, es gibt nur Lügner, die immer lügen, und Wahrheitssprecher, die immer die Wahrheit sagen.

Ein Kreter sagt: „Alle Kreter lügen“.

Die Antinomie des Epimenides

Wir nehmen an, es gibt nur Lügner, die immer lügen, und Wahrheitssprecher, die immer die Wahrheit sagen.

Ein Kreter sagt: „Alle Kreter lügen“.

Ist das wahr, so behauptet er, dass er ein Lügner ist.
Ist das falsch, so behauptet er, dass er gar kein Lügner ist.

Die Antinomie des Epimenides

Wir nehmen an, es gibt nur Lügner, die immer lügen, und Wahrheitssprecher, die immer die Wahrheit sagen.

Ein Kreter sagt: „Alle Kreter lügen“.

Ist das wahr, so behauptet er, dass er ein Lügner ist.
Ist das falsch, so behauptet er, dass er gar kein Lügner ist.

Was ist an dieser Argumentation falsch?

Die Antinomie des Epimenides

Wir nehmen an, es gibt nur Lügner, die immer lügen, und Wahrheitssprecher, die immer die Wahrheit sagen.

Ein Kreter sagt: „Alle Kreter lügen“.

Ist das wahr, so behauptet er, dass er ein Lügner ist.
Ist das falsch, so behauptet er, dass er gar kein Lügner ist.

Was ist an dieser Argumentation falsch?

Richtig lautet die Antinomie:

„Der Satz, den ich jetzt ausspreche, ist falsch“.

Ein Klassiker der Unterhaltungsmathematik

Ein Urwaldforscher wird von einem einheimischen Stamm gefangengenommen. Es stellt sich heraus, dass dieser Stamm aus Kannibalen besteht, die ihn töten und verspeisen wollen. Sie sagen zu ihm:

Ein Klassiker der Unterhaltungsmathematik

Ein Urwaldforscher wird von einem einheimischen Stamm gefangengenommen. Es stellt sich heraus, dass dieser Stamm aus Kannibalen besteht, die ihn töten und verspeisen wollen. Sie sagen zu ihm:

> *„Von deiner nächsten Aussage machen wir abhängig, wie wir dich zubereiten: Entsprechen deine nächsten Worte der Wahrheit, so werden wir dich kochen. Solltest du allerdings lügen, dann wirst du gegrillt“.*

Ein Klassiker der Unterhaltungsmathematik

Ein Urwaldforscher wird von einem einheimischen Stamm gefangengenommen. Es stellt sich heraus, dass dieser Stamm aus Kannibalen besteht, die ihn töten und verspeisen wollen. Sie sagen zu ihm:

> *„Von deiner nächsten Aussage machen wir abhängig, wie wir dich zubereiten: Entsprechen deine nächsten Worte der Wahrheit, so werden wir dich kochen. Solltest du allerdings lügen, dann wirst du gegrillt“.*

Der Forscher sagt etwas, das ihm das Leben rettet. Was?

Ein Klassiker der Unterhaltungsmathematik

Ein Urwaldforscher wird von einem einheimischen Stamm gefangengenommen. Es stellt sich heraus, dass dieser Stamm aus Kannibalen besteht, die ihn töten und verspeisen wollen. Sie sagen zu ihm:

> *„Von deiner nächsten Aussage machen wir abhängig, wie wir dich zubereiten: Entsprechen deine nächsten Worte der Wahrheit, so werden wir dich kochen. Solltest du allerdings lügen, dann wirst du gegrillt“.*

Der Forscher sagt etwas, das ihm das Leben rettet. Was?

> *„Ich werde gegrillt werden“.*

Superspiel

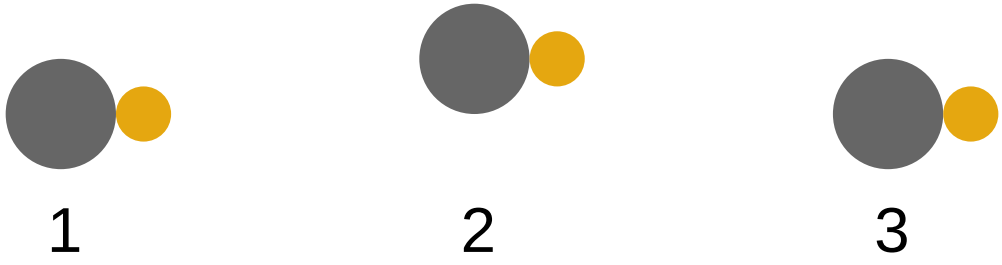
Ein Zweipersonenspiel heißt „normal“, wenn es nach endlich vielen Zügen zu Ende ist.

Superspiel

Ein Zweipersonenspiel heißt „normal“, wenn es nach endlich vielen Zügen zu Ende ist.

Das „Superspiel“ besteht darin, dass der anziehende Spieler ein beliebiges normales Spiel nennt, das dann mit dem anderen Spieler im Anzug gespielt wird. Existiert Superspiel?

Am Marterpfahl



Drei Forscher werden von einem Indianerstamm gefangen genommen und hintereinander an drei Marterpfähle gebunden.

Am Marterpfahl

1 2 3

Drei Forscher werden von einem Indianerstamm gefangen genommen und hintereinander an drei Marterpfähle gebunden.

Es gibt drei schwarze und zwei rote Marterpfähle.

1 sieht die Farben von 2 und 3, 2 sieht 3, 3 sieht nichts.

Am Marterpfahl

1 2 3

Drei Forscher werden von einem Indianerstamm gefangen genommen und hintereinander an drei Marterpfähle gebunden.

Es gibt drei schwarze und zwei rote Marterpfähle.

1 sieht die Farben von 2 und 3, 2 sieht 3, 3 sieht nichts.

Wer die Farbe seines Pfahls erkennt, wird freigelassen.

Am Marterpfahl

Drei Forscher werden von einem Indianerstamm gefangen genommen und hintereinander an drei Marterpfähle gebunden.

Es gibt drei schwarze und zwei rote Marterpfähle.

1 sieht die Farben von 2 und 3, 2 sieht 3, 3 sieht nichts.

Wer die Farbe seines Pfahls erkennt, wird freigelassen.

Nach einer Weile nennt Forscher 3 die Farbe seines Pfahls und kommt frei.

Wie konnte er das wissen?

Berühmte Aussagen

Wem werden die folgenden Aussagen zugeschrieben und was hat derjenige tatsächlich gesagt bzw. gemeint ?

a) Non scholae sed vitae discimus (Nicht für die Schule, sondern für's Leben lernen wir).

Berühmte Aussagen

Wem werden die folgenden Aussagen zugeschrieben und was hat derjenige tatsächlich gesagt bzw. gemeint ?

a) Non scholae sed vitae discimus (Nicht für die Schule, sondern für's Leben lernen wir).

b) Mens sana in corpore sana (Ein gesunder Geist in einem gesunden Körper).

Berühmte Aussagen

Wem werden die folgenden Aussagen zugeschrieben und was hat derjenige tatsächlich gesagt bzw. gemeint ?

a) Non scholae sed vitae discimus (Nicht für die Schule, sondern für's Leben lernen wir).

b) Mens sana in corpore sana (Ein gesunder Geist in einem gesunden Körper).

c) Auge um Auge, Zahn um Zahn.

Zurück zur Antinomie des Epimenides

Die Antinomie beruht darauf, dass in der Alltagslogik der Satz

„Alle Kreter lügen“.

verneint wir durch

„Alle Kreter lügen nicht“.

Zurück zur Antinomie des Epimenides

Die Antinomie beruht darauf, dass in der Alltagslogik der Satz

„Alle Kreter lügen“.

verneint wir durch

„Alle Kreter lügen nicht“.

Die Alltagslogik ist daher *Aussagenlogik*.
In Mathematik und Informatik verwenden wir dagegen die *Prädikatenlogik*.

Prädikate

sind Ausdrücke, die von einer oder mehrerer Variablen abhängen (=ein- bzw. mehrstellige Prädikate). Nachdem man für die Variablen Individuen eingesetzt hat, entsteht eine Aussage.

Prädikate

sind Ausdrücke, die von einer oder mehrerer Variablen abhängen (=ein- bzw. mehrstellige Prädikate). Nachdem man für die Variablen Individuen eingesetzt hat, entsteht eine Aussage.

In

„x ist ein Mensch“.

können wir beliebige Lebewesen für x einsetzen:

„Sokrates ist ein Mensch“.

„Der Hund Lupo ist ein Mensch“.

In jedem Fall entsteht eine Aussage.

Verneinungsregeln

Wir verwenden

$\forall$ „für alle“

$\exists$ „es existiert“

Verneinungsregeln

Wir verwenden

$\forall$ „für alle“
$\exists$ „es existiert“

Ist $A(x)$ ein einstelliges Prädikat, so gelten die Regeln

$$\neg\, \forall x\, A(x) \quad \Leftrightarrow \quad \exists x\, \neg A(x),$$

$$\neg\, \exists x\, A(x) \quad \Leftrightarrow \quad \forall x\, \neg A(x).$$

1.2 Satz und Beweis

Ein mathematischer Satz besteht aus einer Voraussetzung und einer Behauptung.

1.2 Satz und Beweis

Ein mathematischer Satz besteht aus einer Voraussetzung und einer Behauptung.

Der *Beweis* des Satzes besteht aus einer Folge von wahren Aussagen, deren letzte die Behauptung ist.

Beispiel

Man zeige für $a, b \geq 0$

$$\frac{a+b}{2} \geq \sqrt{ab}.$$

Beispiel

Man zeige für $a, b \geq 0$

$$\frac{a+b}{2} \geq \sqrt{ab}.$$

Das geschieht häufig so

$$\Rightarrow \quad a+b \geq 2\sqrt{ab} \quad \Rightarrow \quad (a+b)^2 \geq 4ab$$

$$\Rightarrow \quad a^2 - 2ab + b^2 \geq 0 \quad \Rightarrow \quad (a-b)^2 \geq 0.$$

Was ist daran falsch?

Beispiel

Man zeige für $a, b \geq 0$

$$\frac{a+b}{2} \geq \sqrt{ab}.$$

Das geschieht häufig so

$$\Rightarrow \quad a+b \geq 2\sqrt{ab} \quad \Rightarrow \quad (a+b)^2 \geq 4ab$$

$$\Rightarrow \quad a^2 - 2ab + b^2 \geq 0 \quad \Rightarrow \quad (a-b)^2 \geq 0.$$

Was ist daran falsch?

Korrekt ist natürlich die umgekehrte Reihenfolge.

Der indirekte Beweis

Aus den Wahrheitstafeln folgt

$$A \Rightarrow B \quad \Leftrightarrow \quad \neg A \vee B$$

und entsprechend

$$\neg(A \Rightarrow B) \quad \Leftrightarrow \quad A \wedge \neg B$$

Der indirekte Beweis

Aus den Wahrheitstafeln folgt

$$A \Rightarrow B \quad \Leftrightarrow \quad \neg A \vee B$$

und entsprechend

$$\neg(A \Rightarrow B) \quad \Leftrightarrow \quad A \wedge \neg B$$

Im indirekten Beweis zeigen wir daher, dass $A \wedge \neg B$ falsch ist. Dazu nehmen wir die Verneinung der Behauptung als wahr an und zeigen, dass nicht gleichzeitig die Voraussetzung wahr ist.

Beispiel

Man zeige für $a, b \geq 0$

$$\frac{a+b}{2} \geq \sqrt{ab}.$$

Beispiel

Man zeige für $a, b \geq 0$

$$\frac{a+b}{2} \geq \sqrt{ab}.$$

Als Voraussetzung können wir hier $(a-b)^2 \geq 0$ nehmen. Dann nehmen wir an

$$\frac{a+b}{2} < \sqrt{ab}.$$

Beispiel

$$\frac{a+b}{2} < \sqrt{ab}$$

$$\Rightarrow \quad a+b < 2\sqrt{ab} \quad \Rightarrow \quad (a+b)^2 < 4ab$$

$$\Rightarrow a^2 - 2ab + b^2 < 0 \quad \Rightarrow \quad (a-b)^2 < 0.$$

mit Widerspruch zur Voraussetzung.

Die Kontraposition

Aus der Wahrheitstafel für die Implikation folgt

$$(A \Rightarrow B) \quad \Leftrightarrow \quad (\neg B \Rightarrow \neg A).$$

Man nennt $\neg B \Rightarrow \neg A$ die *Kontraposition* zu $A \Rightarrow B$.

Beispiel

Man zeige:

Wenn n^2 gerade ist, so ist auch n gerade.

Kontraposition:

Wenn n ungerade ist, so ist auch n^2 ungerade.

Beispiel

Man zeige:

Wenn n^2 gerade ist, so ist auch n gerade.

Kontraposition:

Wenn n ungerade ist, so ist auch n^2 ungerade.

Beweis der Kontraposition:

$$n = 2k + 1 \quad \Rightarrow \quad n^2 = 4k^2 + 4k + 1.$$

1.3 Mengen, Relationen, Abbildungen

Eine Menge ist eine Zusammenfassung von Gegenständen. Schreibe

$$a \in A \;\Leftrightarrow\; a \text{ gehört zur Menge } A$$

$$a \notin A \;\Leftrightarrow\; a \text{ gehört nicht zur Menge } A$$

1.3 Mengen, Relationen, Abbildungen

Eine Menge ist eine Zusammenfassung von Gegenständen. Schreibe

$$a \in A \;\Leftrightarrow\; a \text{ gehört zur Menge } A$$

$$a \notin A \;\Leftrightarrow\; a \text{ gehört nicht zur Menge } A$$

Beispiel: Für die Menge $A_2 = \{1, 2\}$ gilt $1 \in A_2$ und $3 \notin A_2$.

1.3 Mengen, Relationen, Abbildungen

Eine Menge ist eine Zusammenfassung von Gegenständen. Schreibe

$$a \in A \;\Leftrightarrow\; a \text{ gehört zur Menge } A$$

$$a \notin A \;\Leftrightarrow\; a \text{ gehört nicht zur Menge } A$$

Beispiel: Für die Menge $A_2 = \{1, 2\}$ gilt $1 \in A_2$ und $3 \notin A_2$.

Die *natürlichen Zahlen* sind

$$\mathbb{N} = \{1, 2, 3, \ldots\}.$$

1.3 Mengen, Relationen, Abbildungen

Eine Menge ist eine Zusammenfassung von Gegenständen. Schreibe

$$a \in A \;\Leftrightarrow\; a \text{ gehört zur Menge } A$$

$$a \notin A \;\Leftrightarrow\; a \text{ gehört nicht zur Menge } A$$

Beispiel: Für die Menge $A_2 = \{1, 2\}$ gilt $1 \in A_2$ und $3 \notin A_2$.

Die *natürlichen Zahlen* sind

$$\mathbb{N} = \{1, 2, 3, \ldots\}.$$

Menge G der geraden natürlichen Zahlen lassen sich schreiben als

$$2\mathbb{N}, \quad G = \{2n : n \in \mathbb{N}\}, \quad G = \{n \in \mathbb{N} : n \text{ ist gerade}\}.$$

Die leere Menge

In der *leeren Menge*

$$\emptyset = \{\}$$

begegnet uns der horror vacui: Die Aussage $a \in \emptyset$ ist für jedes a falsch.

Mengenbeziehungen

$$
\begin{aligned}
A = B \quad &\Leftrightarrow \quad (x \in A \Leftrightarrow x \in B) \\
A \subset B \quad &\Leftrightarrow \quad (x \in A \Rightarrow x \in B) \quad (\textit{Teilmenge}), \\
A \cap B \quad &\Leftrightarrow \quad \{x : x \in A \wedge x \in B\} \quad (\textit{Schnittmenge}), \\
A \cup B \quad &\Leftrightarrow \quad \{x : x \in A \vee x \in B\} \quad (\textit{Vereinigungsmenge}),
\end{aligned}
$$

Mengenbeziehungen

$$
\begin{aligned}
A = B \quad &\Leftrightarrow \quad (x \in A \Leftrightarrow x \in B) \\
A \subset B \quad &\Leftrightarrow \quad (x \in A \Rightarrow x \in B) \quad (\textit{Teilmenge}), \\
A \cap B \quad &\Leftrightarrow \quad \{x : x \in A \wedge x \in B\} \quad (\textit{Schnittmenge}), \\
A \cup B \quad &\Leftrightarrow \quad \{x : x \in A \vee x \in B\} \quad (\textit{Vereinigungsmenge}), \\
A \setminus B \quad &\Leftrightarrow \quad \{x : x \in A,\ x \notin B) \quad (\textit{Komplement}).
\end{aligned}
$$

Teilmenge

$$A \subset B \quad \Leftrightarrow \quad (x \in A \Rightarrow x \in B) \quad (\textit{Teilmenge}).$$

Es gilt $B \subset B$ für alle Mengen B.

Teilmenge

$$A \subset B \quad \Leftrightarrow \quad (x \in A \Rightarrow x \in B) \quad (\textit{Teilmenge}).$$

Es gilt $B \subset B$ für alle Mengen B.

Es gilt $\emptyset \subset B$ für alle Mengen B.

Denn die Voraussetzung $x \in \emptyset$ ist immer falsch und daher ist $x \in \emptyset \Rightarrow x \in B$ immer wahr.

Komplement

$$A \setminus B \quad \Leftrightarrow \quad \{x : x \in A,\ x \notin B) \quad (\textit{Komplement}).$$

Komplement

$$A \setminus B \quad \Leftrightarrow \quad \{x : x \in A,\ x \notin B) \quad (\textit{Komplement}).$$

Sind die zu untersuchenden Mengen alle Teilmengen einer Menge M, so schreibt man auch A^c an Stelle von $M \setminus A$.

Beispiel

Man beachte den Unterschied zwischen $A = \{a\}$ und $A' = \{\{a\}\}$:

Beispiel

Man beachte den Unterschied zwischen $A = \{a\}$ und $A' = \{\{a\}\}$:

Es gilt $\{a\} \in A'$, aber $a \notin A'$.

Potenzmenge

Die *Potenzmenge* einer Menge A ist

$$\mathcal{P}(A) = 2^A = \{B : B \subset A\}.$$

Potenzmenge

Die *Potenzmenge* einer Menge A ist

$$\mathcal{P}(A) = 2^A = \{B : B \subset A\}.$$

Für die Menge $A_2 = \{1, 2\}$ gilt beispielsweise

$$\mathcal{P}(A_2) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}.$$

$\mathcal{P}(A_2)$ besteht daher aus 4 Elementen, die alle selber Mengen sind.

Durchschnitt und Vereinigung eines Mengensystems

Für eine nichtleere Menge I, die hier *Indexmenge* genannt wird, gebe es für jedes $i \in I$ eine Menge A_i.

Durchschnitt und Vereinigung eines Mengensystems

Für eine nichtleere Menge I, die hier *Indexmenge* genannt wird, gebe es für jedes $i \in I$ eine Menge A_i.

Dann:

$$\cap_{i \in I} A_i = \{x : \forall i \in I : x \in A_i\}, \quad \cup_{i \in I} A_i = \{x : \exists i \in I : x \in A_i\}.$$

Geordnetes Paar

Für zwei Elemente a, b heißt

$$(a, b) \textit{ geordnetes Paar.}$$

Geordnetes Paar

Für zwei Elemente a, b heißt

$$(a, b) \textit{ geordnetes Paar.}$$

Es gilt

$$(a, b) = (a', b') \Leftrightarrow a = a' \text{ und } b = b'$$

(Geordnetes) n-tupel, kartesische Produkt

Analog ist das (geordnete) n-tupel $(a_1, a_2, \ldots, a_n)$ definiert.

(Geordnetes) n-tupel, kartesische Produkt

Analog ist das (geordnete) n-tupel $(a_1, a_2, \ldots, a_n)$ definiert.

Für Mengen $A_1, \ldots, A_n$ ist das *kartesische Produkt*

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) : \ a_i \in A_i \text{ für } i = 1, 2, \ldots, n\}.$$

(Geordnetes) n-tupel, kartesische Produkt

Analog ist das (geordnete) n-tupel $(a_1, a_2, \ldots, a_n)$ definiert.

Für Mengen $A_1, \ldots, A_n$ ist das *kartesische Produkt*

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) : \ a_i \in A_i \text{ für } i = 1, 2, \ldots, n\}.$$

Wie viele Elemente besitzt $A \times B$?

Relation

Für eine Menge A heißt $R \subset A \times A$ *Relation*.

Relation

Für eine Menge A heißt $R \subset A \times A$ *Relation*.

Ist $(a, b) \in R$, so schreibe

aRb oder: a und b stehen in der Relation R.

Relation

Für eine Menge A heißt $R \subset A \times A$ *Relation*.

Ist $(a, b) \in R$, so schreibe

$$aRb \text{ oder: } a \text{ und } b \text{ stehen in der Relation } R.$$

Beispiel: Natürliche Zahlen $\mathbb{N}$, die nach Größe geordnet werden:

$$R = \{(a, b) \in \mathbb{N} \times \mathbb{N} : a \leq b\}.$$

Relation

Für eine Menge A heißt $R \subset A \times A$ *Relation*.

Ist $(a, b) \in R$, so schreibe

$$aRb \text{ oder: } a \text{ und } b \text{ stehen in der Relation } R.$$

Beispiel: Natürliche Zahlen $\mathbb{N}$, die nach Größe geordnet werden:

$$R = \{(a, b) \in \mathbb{N} \times \mathbb{N} : a \leq b\}.$$

Statt aRb schreibt man dann gleich $a \leq b$.

Spezielle Relationen

Eine Relation R heißt

(a) *reflexiv*, wenn aRa für alle $a \in A$,

Spezielle Relationen

Eine Relation R heißt

(a) *reflexiv*, wenn aRa für alle $a \in A$,

(b) *symmetrisch*, wenn mit aRb auch bRa gilt,

Spezielle Relationen

Eine Relation R heißt

(a) *reflexiv*, wenn aRa für alle $a \in A$,

(b) *symmetrisch*, wenn mit aRb auch bRa gilt,

(c) *antisymmetrisch*, wenn aus aRb und bRa folgt, dass $a = b$,

Spezielle Relationen

Eine Relation R heißt

(a) *reflexiv*, wenn aRa für alle $a \in A$,

(b) *symmetrisch*, wenn mit aRb auch bRa gilt,

(c) *antisymmetrisch*, wenn aus aRb und bRa folgt, dass $a = b$,

(d) *transitiv*, wenn aus aRb und bRc folgt, dass aRc.

Ordnungsrelation oder Halbordnung

Eine Relation R heißt *Ordnungsrelation* oder *Halbordnung*, wenn sie

reflexiv, antisymmetrisch und transitiv

ist.

Ordnungsrelation oder Halbordnung

Eine Relation R heißt *Ordnungsrelation* oder *Halbordnung*, wenn sie

reflexiv, antisymmetrisch und transitiv

ist.

Eine Ordnungsrelation heißt *total*, wenn zusätzlich gilt: Für alle $a, b \in A$ gilt aRb oder bRa.

Strenge Ordnungsrelation

Aus einer Ordnungsrelation $\leq$ erhält man eine *strenge Ordnungsrelation* durch:

$$a < b \;\Leftrightarrow\; a \leq b \text{ und } a \neq b.$$

Beispiel (i)

Sei B eine nichtleere Menge.

Auf der Potenzmenge $\mathcal{P}(B)$ ist die Teilmengenbeziehung $\subset$ eine Ordnungsrelation.

Beispiel (i)

Sei B eine nichtleere Menge.

Auf der Potenzmenge $\mathcal{P}(B)$ ist die Teilmengenbeziehung $\subset$ eine Ordnungsrelation.

Wenn B mehr als ein Element enthält, ist sie keine totale Ordnung.

Beispiel (ii)

Auf einer Menge A existiere eine totale Ordnung $\leq$. Wie kann man die n-tupel

$$(a_1, a_2, \ldots, a_n) \in A^n = A \times \ldots \times A$$

sinnvoll ordnen?

Beispiel (ii)

Auf einer Menge A existiere eine totale Ordnung $\leq$. Wie kann man die n-tupel

$$(a_1, a_2, \ldots, a_n) \in A^n = A \times \ldots \times A$$

sinnvoll ordnen?

Eine Möglichkeit ist die *komponentenweise Ordnung* $\leq_k$

$$(a_1, \ldots, a_n) \leq_k (b_1, \ldots, b_n) \;\Leftrightarrow\; a_i \leq b_i \text{ für } i = 1, \ldots, n.$$

Beispiel (ii)

Auf einer Menge A existiere eine totale Ordnung $\leq$. Wie kann man die n-tupel

$$(a_1, a_2, \ldots, a_n) \in A^n = A \times \ldots \times A$$

sinnvoll ordnen?

Eine Möglichkeit ist die *komponentenweise Ordnung* $\leq_k$

$$(a_1, \ldots, a_n) \leq_k (b_1, \ldots, b_n) \Leftrightarrow a_i \leq b_i \text{ für } i = 1, \ldots, n.$$

Für die Menge

$$A_2 = \{1, 2\} \text{ und } n = 2$$

ist die Ordnung nicht total, z.B. $(1, 2)$ und $(2, 1)$.

Beispiel (ii)

Eine totale Ordnung ist die *lexikographische* Ordnung

$$(a_1, \ldots, a_n) <_l (b_1, \ldots, b_n) \Leftrightarrow$$

$$\exists i_0 \; a_i = b_i \text{ für } i = 1, \ldots, i_0 - 1 \text{ und } a_{i_0} < b_{i_0},$$

Beispiel (ii)

Eine totale Ordnung ist die *lexikographische* Ordnung

$$(a_1, \ldots, a_n) <_l (b_1, \ldots, b_n) \Leftrightarrow$$

$$\exists i_0 \; a_i = b_i \text{ für } i = 1, \ldots, i_0 - 1 \text{ und } a_{i_0} < b_{i_0},$$

Wörterbücher!

Minimal und Minimum

Sei A mit einer Halbordnung $\leq$ versehen.

- $m \in A$ heißt *minimal*, wenn es kein $a \in A \setminus \{m\}$ gibt mit $a \leq m$

Minimal und Minimum

Sei A mit einer Halbordnung $\leq$ versehen.

- $m \in A$ heißt *minimal*, wenn es kein $a \in A \setminus \{m\}$ gibt mit $a \leq m$
- $m \in A$ heißt *Minimum* von A, wenn $m \leq a$ für alle $a \in A$ gilt. In diesem Fall schreiben wir $m = \min A$.

Minimal und Minimum

Sei A mit einer Halbordnung $\leq$ versehen.

- $m \in A$ heißt *minimal*, wenn es kein $a \in A \setminus \{m\}$ gibt mit $a \leq m$
- $m \in A$ heißt *Minimum* von A, wenn $m \leq a$ für alle $a \in A$ gilt. In diesem Fall schreiben wir $m = \min A$.

Das Minimum ist, falls es existiert, eindeutig bestimmt und minimal.

Minimal und Minimum

Sei A mit einer Halbordnung $\leq$ versehen.

- $m \in A$ heißt *minimal*, wenn es kein $a \in A \setminus \{m\}$ gibt mit $a \leq m$
- $m \in A$ heißt *Minimum* von A, wenn $m \leq a$ für alle $a \in A$ gilt. In diesem Fall schreiben wir $m = \min A$.

Das Minimum ist, falls es existiert, eindeutig bestimmt und minimal.

Jede endliche, total geordnete Menge A besitzt ein Minimum.

Nach unten beschränkt

$T \subset A$ heißt *nach unten beschränkt in* A, wenn

$$\exists u \in A \text{ mit } u \leq t \text{ für alle } t \in T.$$

Nach unten beschränkt

$T \subset A$ heißt *nach unten beschränkt in* A, wenn

$$\exists u \in A \text{ mit } u \leq t \text{ für alle } t \in T.$$

In diesem Fall heißt u *untere Schranke* von T.

Nach unten beschränkt

$T \subset A$ heißt *nach unten beschränkt in* A, wenn

$$\exists u \in A \text{ mit } u \leq t \text{ für alle } t \in T.$$

In diesem Fall heißt u *untere Schranke* von T.

Die ganzen Zahlen

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

mit der natürlichen Ordnung sind nach unten unbeschränkt.

Maximal, Maximum, obere Schranke

Die Begriffe maximal, Maximum, obere Schranke sind analog definiert.

Maximal, Maximum, obere Schranke

Die Begriffe maximal, Maximum, obere Schranke sind analog definiert.

Wenn T nach unten und nach oben beschränkt in A ist, so heißt T beschränkt in A.

Äquivalenzrelation

Ist R

- reflexiv,
- symmetrisch
- transitiv

so heißt R *Äquivalenzrelation*.

Äquivalenzrelation

Ist R

- reflexiv,
- symmetrisch
- transitiv

so heißt R *Äquivalenzrelation*.

Schreiben meist $\sim$ statt R.

Äquivalenzklasse

Jedem $a \in A$ ordnen wir die *Äquivalenzklasse*

$$\overline{a} = \{x \in A : a \sim x\}$$

zu.

Äquivalenzklasse

Jedem $a \in A$ ordnen wir die *Äquivalenzklasse*

$$\overline{a} = \{x \in A : a \sim x\}$$

zu.

Wegen der Reflexivität ist $a \in \overline{a}$.

Äquivalenzklasse

Jedem $a \in A$ ordnen wir die *Äquivalenzklasse*

$$\overline{a} = \{x \in A : a \sim x\}$$

zu.

Wegen der Reflexivität ist $a \in \overline{a}$.

Weiter folgt aus der Transitivität:

$$\overline{a} = \overline{b} \;\Leftrightarrow\; a \sim b.$$

Äquivalenzklasse

Jedem $a \in A$ ordnen wir die *Äquivalenzklasse*

$$\overline{a} = \{x \in A : a \sim x\}$$

zu.

Wegen der Reflexivität ist $a \in \overline{a}$.

Weiter folgt aus der Transitivität:

$$\overline{a} = \overline{b} \;\Leftrightarrow\; a \sim b.$$

Hier deutet sich schon an, dass A in Äquivalenzklassen zerfällt.

Disjunkte Zerlegung

Sei A nichtleer.

Eine Menge von Teilmengen $A_i \subset A$, $A_i \neq \emptyset$, $i \in I$, heißt *Partition* oder *disjunkte Zerlegung* von A, wenn

$$A_i \cap A_j = \emptyset \text{ für } i \neq j \text{ (disjunkt!) und } A = \cup_{i \in I} A_i \text{ (Zerlegung!).}$$

Äquivalenzrelation und disjunkte Zerlegung

Satz Die Begriffe „Äquivalenzrelation“ und „disjunkte Zerlegung“ sind im folgenden Sinne äquivalent:

Äquivalenzrelation und disjunkte Zerlegung

Satz Die Begriffe „Äquivalenzrelation“ und „disjunkte Zerlegung“ sind im folgenden Sinne äquivalent:

(a) Zu einer disjunkten Zerlegung $\{A_i : i \in I\}$ von A definiere

$$a \sim b \;\Leftrightarrow\; \exists i \in I \text{ mit } a, b \in A_i.$$

Äquivalenzrelation und disjunkte Zerlegung

Satz Die Begriffe „Äquivalenzrelation“ und „disjunkte Zerlegung“ sind im folgenden Sinne äquivalent:

(a) Zu einer disjunkten Zerlegung $\{A_i : i \in I\}$ von A definiere

$$a \sim b \;\Leftrightarrow\; \exists i \in I \text{ mit } a, b \in A_i.$$

Dann ist $\sim$ Äquivalenzrelation mit Äquivalenzklassen A_i.

Äquivalenzrelation und disjunkte Zerlegung

Satz Die Begriffe „Äquivalenzrelation“ und „disjunkte Zerlegung“ sind im folgenden Sinne äquivalent:

(a) Zu einer disjunkten Zerlegung $\{A_i : i \in I\}$ von A definiere

$$a \sim b \;\Leftrightarrow\; \exists i \in I \text{ mit } a, b \in A_i.$$

Dann ist $\sim$ Äquivalenzrelation mit Äquivalenzklassen A_i.

(b) Die Äquivalenzklassen bilden eine disjunkte Zerlegung von A.

Beweis (a)

(a) Zu einer disjunkten Zerlegung $\{A_i : i \in I\}$ definiere

$$a \sim b \;\Leftrightarrow\; \exists i \in I \text{ mit } a, b \in A_i.$$

Dann ist $\sim$ Äquivalenzrelation mit Äquivalenzklassen A_i.

Beweis (a)

(a) Zu einer disjunkten Zerlegung $\{A_i : i \in I\}$ definiere

$$a \sim b \;\Leftrightarrow\; \exists i \in I \text{ mit } a, b \in A_i.$$

Dann ist $\sim$ Äquivalenzrelation mit Äquivalenzklassen A_i.

$a \sim a$ gilt wegen $A = \cup_i A_i$, a muss daher zu einem A_i gehören.

Beweis (a)

(a) Zu einer disjunkten Zerlegung $\{A_i : i \in I\}$ definiere

$$a \sim b \;\Leftrightarrow\; \exists i \in I \text{ mit } a, b \in A_i.$$

Dann ist $\sim$ Äquivalenzrelation mit Äquivalenzklassen A_i.

$a \sim a$ gilt wegen $A = \cup_i A_i$, a muss daher zu einem A_i gehören.

$$a \sim b \;\Leftrightarrow\; b \sim a$$

ist offensichtlich.

Beweis (a)

(a) Zu einer disjunkten Zerlegung $\{A_i : i \in I\}$ definiere

$$a \sim b \;\Leftrightarrow\; \exists i \in I \text{ mit } a, b \in A_i.$$

Dann ist $\sim$ Äquivalenzrelation mit Äquivalenzklassen A_i.

$a \sim a$ gilt wegen $A = \cup_i A_i$, a muss daher zu einem A_i gehören.

$$a \sim b \;\Leftrightarrow\; b \sim a$$

ist offensichtlich.

Transitivität: $a \sim b$ bedeutet $a, b \in A_i$ und $b \sim c$ bedeutet $b, c \in A_j$.

Beweis (a)

(a) Zu einer disjunkten Zerlegung $\{A_i : i \in I\}$ definiere

$$a \sim b \;\Leftrightarrow\; \exists i \in I \text{ mit } a, b \in A_i.$$

Dann ist $\sim$ Äquivalenzrelation mit Äquivalenzklassen A_i.

$a \sim a$ gilt wegen $A = \cup_i A_i$, a muss daher zu einem A_i gehören.

$$a \sim b \;\Leftrightarrow\; b \sim a$$

ist offensichtlich.

Transitivität: $a \sim b$ bedeutet $a, b \in A_i$ und $b \sim c$ bedeutet $b, c \in A_j$.

Da die Mengen A_i und A_j disjunkt sind und b zu beiden Mengen gehört, muss $i = j$ gelten.

Beweis (b)

(b) Die Äquivalenzklassen bilden eine disjunkte Zerlegung von A.

Beweis (b)

(b) Die Äquivalenzklassen bilden eine disjunkte Zerlegung von A.

Wegen $a \in \overline{a}$ sind die Äquivalenzklassen nichtleer.

Beweis (b)

(b) Die Äquivalenzklassen bilden eine disjunkte Zerlegung von A.

Wegen $a \in \overline{a}$ sind die Äquivalenzklassen nichtleer.

$$\cup_{a \in A}\{a\} = A \;\Rightarrow\; \cup_{a \in A}\overline{a} = A$$

Beweis (b)

(b) Die Äquivalenzklassen bilden eine disjunkte Zerlegung von A.

Wegen $a \in \overline{a}$ sind die Äquivalenzklassen nichtleer.

$$\cup_{a \in A} \{a\} = A \;\Rightarrow\; \cup_{a \in A} \overline{a} = A$$

Disjunkt:

$$\overline{a} \cap \overline{b} \neq \emptyset \;\Rightarrow\; \exists c \text{ mit } c \in \overline{a},\, c \in \overline{b}.$$

Beweis (b)

(b) Die Äquivalenzklassen bilden eine disjunkte Zerlegung von A.

Wegen $a \in \overline{a}$ sind die Äquivalenzklassen nichtleer.

$$\cup_{a \in A} \{a\} = A \;\Rightarrow\; \cup_{a \in A} \overline{a} = A$$

Disjunkt:

$$\overline{a} \cap \overline{b} \neq \emptyset \;\Rightarrow\; \exists c \text{ mit } c \in \overline{a},\, c \in \overline{b}.$$

Damit folgt $a \sim c$ und $b \sim c$, mit der Transitivität auch $a \sim b$.

Allgemeinere Relationen

Man kann Relationen zwischen verschiedenen Mengen definieren, also $R \subset A \times B$.

Allgemeinere Relationen

Man kann Relationen zwischen verschiedenen Mengen definieren, also $R \subset A \times B$.

A könnte hier eine Menge von Personen sein und B eine Menge von Firmen.

Abbildung

Seien A und B nichtleere Mengen.

Abbildung

Seien A und B nichtleere Mengen.

Eine *Abbildung* f zwischen diesen Mengen ordnet jedem Element $a \in A$ genau ein Element $b \in B$ zu.

Abbildung

Seien A und B nichtleere Mengen.

Eine *Abbildung* f zwischen diesen Mengen ordnet jedem Element $a \in A$ genau ein Element $b \in B$ zu.

Wir schreiben für diese Zuordnung

$$f(a) = b, \quad a \mapsto b, \quad f : A \to B$$

Abbildung

Seien A und B nichtleere Mengen.

Eine *Abbildung* f zwischen diesen Mengen ordnet jedem Element $a \in A$ genau ein Element $b \in B$ zu.

Wir schreiben für diese Zuordnung

$$f(a) = b, \quad a \mapsto b, \quad f : A \to B$$

A heißt *Definitions-* und B *Werte- oder Zielbereich* der Abbildung f.

Graph einer Abbildung

Eine Abbildung ist eine spezielle Relation:

$$f(a) = b \;\Leftrightarrow\; (a, b) \in G_f \subset A \times B.$$

Graph einer Abbildung

Eine Abbildung ist eine spezielle Relation:

$$f(a) = b \;\Leftrightarrow\; (a, b) \in G_f \subset A \times B.$$

G_f heißt *Graph* von f.

Graph einer Abbildung

Eine Abbildung ist eine spezielle Relation:

$$f(a) = b \;\Leftrightarrow\; (a, b) \in G_f \subset A \times B.$$

G_f heißt *Graph* von f.

Abbildungen zwischen Zahlbereichen werden oft als *Funktionen* bezeichnet, was hauptsächlich historische Gründe hat.

Manchmal auch *Operatoren*.

Bild

Für $A' \subset A$ setzen wir

$$f(A') = \{f(a) : a \in A'\}.$$

Bild

Für $A' \subset A$ setzen wir

$$f(A') = \{f(a) : a \in A'\}.$$

$f(A')$ heißt *Bild von* A', auch $A' = A$.

Bild

Für $A' \subset A$ setzen wir

$$f(A') = \{f(a) : a \in A'\}.$$

$f(A')$ heißt *Bild von* A', auch $A' = A$.

Es gilt für $A_1, A_2 \subset A$

$$f(A_1 \cup A_2) = f(A_1) \cup f(A_2), \quad f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2).$$

Beweisbeispiel

$$f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2).$$

Solche Beziehungen beweist man durch Rückgriff auf die einzelnen Elemente.

Beweisbeispiel

$$f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2).$$

Solche Beziehungen beweist man durch Rückgriff auf die einzelnen Elemente.

$$b \in f(A_1 \cap A_2) \;\Rightarrow\; \exists a \in A_1 \cap A_2 \text{ mit } f(a) = b.$$

Beweisbeispiel

$$f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2).$$

Solche Beziehungen beweist man durch Rückgriff auf die einzelnen Elemente.

$$b \in f(A_1 \cap A_2) \;\Rightarrow\; \exists a \in A_1 \cap A_2 \text{ mit } f(a) = b.$$

Dann

$$b \in f(A_1) \text{ und } b \in f(A_2)$$

Beweisbeispiel

$$f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2).$$

Solche Beziehungen beweist man durch Rückgriff auf die einzelnen Elemente.

$$b \in f(A_1 \cap A_2) \;\Rightarrow\; \exists a \in A_1 \cap A_2 \text{ mit } f(a) = b.$$

Dann

$$b \in f(A_1) \text{ und } b \in f(A_2)$$

:Gegenbeispiel:

$$A_1 = \{a_1\}, \quad A_2 = \{a_2\}, \quad f(a_1) = f(a_2) = b$$

Urbild

Für $B' \subset B$ heißt

$$f^{-1}(B') = \{a \in A : f(a) \in B'\}$$

das *Urbild von* B'.

Urbild

Für $B' \subset B$ heißt

$$f^{-1}(B') = \{a \in A : f(a) \in B'\}$$

das *Urbild von* B'.

Für $B_1, B_2 \subset B$ gilt

$$f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2), \quad f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2).$$

Injektive und surjektive Abbildungen

Sei $f : A \to B$ eine Abbildung.

Injektive und surjektive Abbildungen

Sei $f : A \to B$ eine Abbildung.

- f heißt *surjektiv*, wenn $f(A) = B$.

Injektive und surjektive Abbildungen

Sei $f : A \to B$ eine Abbildung.

- f heißt *surjektiv*, wenn $f(A) = B$.
- f heißt *injektiv*, wenn aus $f(a_1) = f(a_2)$ folgt, dass $a_1 = a_2$.

Injektive und surjektive Abbildungen

Sei $f : A \to B$ eine Abbildung.

- f heißt *surjektiv*, wenn $f(A) = B$.
- f heißt *injektiv*, wenn aus $f(a_1) = f(a_2)$ folgt, dass $a_1 = a_2$.

Injektiv: Zwei verschiedene Elemente des Urbildbereichs werden auf verschiedene Elemente des Zielbereichs abgebildet.

Bijektive Abbildungen

Eine Abbildung heißt *bijektiv*, wenn sie injektiv und surjektiv ist.

Bijektive Abbildungen

Eine Abbildung heißt *bijektiv*, wenn sie injektiv und surjektiv ist.

Jedes Element $a \in A$ hat genau einen Partner $b = f(a) \in B$ und jedes $b \in B$ hat genau einen Partner $a \in A$.

Umkehrabbildung

Ist f bijektiv, existiert die *Umkehrabbildung* oder *Inverse* von f

$$f^{-1} : B \to A \text{ mit } f^{-1}(f(a)) = a \text{ und } f(f^{-1}(b)) = b.$$

Umkehrabbildung

Ist f bijektiv, existiert die *Umkehrabbildung* oder *Inverse* von f

$$f^{-1} : B \to A \text{ mit } f^{-1}(f(a)) = a \text{ und } f(f^{-1}(b)) = b.$$

Diese Umkehrabbildung unterscheidet sich in der Notation nicht von der Definition des Urbilds, im Gegensatz zu letzterer ist sie aber eine echte Abbildung.

Endliche Mengen

Bei endlichen Mengen A gilt für die Selbstabbildungen $f : A \to A$:

$$f \text{ ist surjektiv } \Leftrightarrow f \text{ ist injektiv } \Leftrightarrow f \text{ ist bijektiv.}$$

Hintereinanderausführung von Abbildungen

Ist $g : A \to B$ und $f : B \to C$, so ist die *Hintereinanderausführung* oder *Verkettung* definiert durch

$$f \circ g : A \to C, \quad a \mapsto f(g(a)).$$

lassen sich in der Form

$$\mathbb{S} = \{S, e_1, \ldots, e_l, f_1, \ldots, f_m, R_1, \ldots, R_n\}$$

schreiben

lassen sich in der Form

$$\mathbb{S} = \{S, e_1, \ldots, e_l, f_1, \ldots, f_m, R_1, \ldots, R_n\}$$

schreiben mit

- S Grundmenge
- e_i ausgezeichnete (meist neutrale) Elemente ,
- f_j Abbildungen (meist zweistellige Operationen wie $+$),
- R_k (meist zweistellige) Relationen.

lassen sich in der Form

$$\mathbb{S} = \{S, e_1, \ldots, e_l, f_1, \ldots, f_m, R_1, \ldots, R_n\}$$

schreiben mit

- S Grundmenge
- e_i ausgezeichnete (meist neutrale) Elemente ,
- f_j Abbildungen (meist zweistellige Operationen wie $+$),
- R_k (meist zweistellige) Relationen.

Dies ist redundant, weil man alle Abbildungen auch als Relationen schreiben kann.

1.5 Gruppen

Eine *Gruppe* $\mathbb{G} = (G, e, \circ)$ besteht

- aus einer Menge G,
- einer zweistelligen Operation $\circ$ mit $z = x \circ y \in G$,
- einem ausgezeichneten Element $e \in G$.

1.5 Gruppen

Eine *Gruppe* $\mathbb{G} = (G, e, \circ)$ besteht

- aus einer Menge G,
- einer zweistelligen Operation $\circ$ mit $z = x \circ y \in G$,
- einem ausgezeichneten Element $e \in G$.

Es gelten die Gruppenaxiome:

(G1) (Assoziativgesetz) Für alle $x, y, z \in G$ gilt

$$(x \circ y) \circ z = x \circ (y \circ z).$$

1.5 Gruppen

Eine *Gruppe* $\mathbb{G} = (G, e, \circ)$ besteht

- aus einer Menge G,
- einer zweistelligen Operation $\circ$ mit $z = x \circ y \in G$,
- einem ausgezeichneten Element $e \in G$.

Es gelten die Gruppenaxiome:

(G1) (Assoziativgesetz) Für alle $x, y, z \in G$ gilt

$$(x \circ y) \circ z = x \circ (y \circ z).$$

(G2) (Neutrales Element) Für alle $x \in G$ gilt

$$e \circ x = x \circ e = x.$$

1.5 Gruppen

Eine *Gruppe* $\mathbb{G} = (G, e, \circ)$ besteht

- aus einer Menge G,
- einer zweistelligen Operation $\circ$ mit $z = x \circ y \in G$,
- einem ausgezeichneten Element $e \in G$.

Es gelten die Gruppenaxiome:

(G1) (Assoziativgesetz) Für alle $x, y, z \in G$ gilt

$$(x \circ y) \circ z = x \circ (y \circ z).$$

(G2) (Neutrales Element) Für alle $x \in G$ gilt

$$e \circ x = x \circ e = x.$$

(G3) (Inverses Element) Zu jedem $x \in G$ gibt es ein $x^{-1} \in G$ mit

$$x^{-1} \circ x = x \circ x^{-1} = e.$$

Beispiele für Gruppen

Endliche Gruppen gibt man mit einer *Gruppentafel* an, in der die Ergebnisse von $x \circ y$ eingetragen werden.

Beispiele für Gruppen

Endliche Gruppen gibt man mit einer *Gruppentafel* an, in der die Ergebnisse von $x \circ y$ eingetragen werden.

Wir bezeichnen die Gruppenelemente mit $0, 1, 2, \ldots$, wobei 0 das neutrale Element ist.

Beispiele für Gruppen

Endliche Gruppen gibt man mit einer *Gruppentafel* an, in der die Ergebnisse von $x \circ y$ eingetragen werden.

Wir bezeichnen die Gruppenelemente mit $0, 1, 2, \ldots$, wobei 0 das neutrale Element ist.

Die Gruppe mit 3 Elementen ist eindeutig bestimmt:

$\circ$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

.

Beispiele für Gruppen

Vierelementige Gruppen gibt es schon mehrere:

$\circ$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\circ$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Beispiele für Gruppen

Gruppen mit unendlicher Grundmenge sind

$$\mathbb{G} = (\mathbb{Z}, 0, +), \quad \mathbb{G} = (\mathbb{Q}, 0, +), \quad \mathbb{G} = (\mathbb{Q} \setminus \{0\}, 1, \cdot).$$

Beispiele für Gruppen

Gruppen mit unendlicher Grundmenge sind

$$\mathbb{G} = (\mathbb{Z}, 0, +), \quad \mathbb{G} = (\mathbb{Q}, 0, +), \quad \mathbb{G} = (\mathbb{Q} \setminus \{0\}, 1, \cdot).$$

Also: Konkrete Gruppen können alles mögliche sein. Beweise streng aus den Axiomen folgern!

Lösbarkeit von Gleichungen

Satz In jeder Gruppe sind die Gleichungen $x \circ a = b$ und $a \circ x = b$ eindeutig nach x auflösbar.

Lösbarkeit von Gleichungen

Satz In jeder Gruppe sind die Gleichungen $x \circ a = b$ und $a \circ x = b$ eindeutig nach x auflösbar.

Das neutrale und das inverse Element sind daher eindeutig bestimmt.

Lösbarkeit von Gleichungen

Satz In jeder Gruppe sind die Gleichungen $x \circ a = b$ und $a \circ x = b$ eindeutig nach x auflösbar.

Das neutrale und das inverse Element sind daher eindeutig bestimmt.

Die Gruppentafeln sind *Lateinische Quadrate*, bei denen in jeder Zeile und in jeder Spalte jedes Element genau einmal vorkommt.

Beweis

Man muss hier vorsichtig sein, weil das Kommutativgesetz $x \circ y = y \circ x$ nicht unbedingt gelten muss.

Beweis

Man muss hier vorsichtig sein, weil das Kommutativgesetz $x \circ y = y \circ x$ nicht unbedingt gelten muss.

Als Lösung von $x \circ a = b$ vermuten wir $x = b \circ a^{-1}$,

$$x \circ a = (b \circ a^{-1}) \circ a \overset{(G1)}{=} b \circ (a^{-1} \circ a) \overset{(G3)}{=} b \circ e \overset{(G2)}{=} b.$$

Beweis

Man muss hier vorsichtig sein, weil das Kommutativgesetz $x \circ y = y \circ x$ nicht unbedingt gelten muss.

Als Lösung von $x \circ a = b$ vermuten wir $x = b \circ a^{-1}$,

$$x \circ a = (b \circ a^{-1}) \circ a \overset{(G1)}{=} b \circ (a^{-1} \circ a) \overset{(G3)}{=} b \circ e \overset{(G2)}{=} b.$$

Eindeutigkeit: Nehmen an, dass die Gleichung $x \circ a = b$ von zwei Gruppenelementen x, x' gelöst wird.

Beweis

Man muss hier vorsichtig sein, weil das Kommutativgesetz $x \circ y = y \circ x$ nicht unbedingt gelten muss.

Als Lösung von $x \circ a = b$ vermuten wir $x = b \circ a^{-1}$,

$$x \circ a = (b \circ a^{-1}) \circ a \overset{(G1)}{=} b \circ (a^{-1} \circ a) \overset{(G3)}{=} b \circ e \overset{(G2)}{=} b.$$

Eindeutigkeit: Nehmen an, dass die Gleichung $x \circ a = b$ von zwei Gruppenelementen x, x' gelöst wird.

Aus $x \circ a = x' \circ a$ folgt durch Multiplikation von rechts mit a^{-1}, dass $x = x'$.

Beweis

Man muss hier vorsichtig sein, weil das Kommutativgesetz $x \circ y = y \circ x$ nicht unbedingt gelten muss.

Als Lösung von $x \circ a = b$ vermuten wir $x = b \circ a^{-1}$,

$$x \circ a = (b \circ a^{-1}) \circ a \overset{(G1)}{=} b \circ (a^{-1} \circ a) \overset{(G3)}{=} b \circ e \overset{(G2)}{=} b.$$

Eindeutigkeit: Nehmen an, dass die Gleichung $x \circ a = b$ von zwei Gruppenelementen x, x' gelöst wird.

Aus $x \circ a = x' \circ a$ folgt durch Multiplikation von rechts mit a^{-1}, dass $x = x'$.

Die eindeutige Lösbarkeit von $a \circ x = b$ zeigt man ganz analog.

Kommutative Gruppen

Eine Gruppe heißt *abelsch* oder *kommutativ*, wenn zusätzlich das Kommutativgesetz gilt:

(G4) Für alle $x, y \in G$ gilt

$$x \circ y = y \circ x.$$

Kommutative Gruppen

Eine Gruppe heißt *abelsch* oder *kommutativ*, wenn zusätzlich das Kommutativgesetz gilt:

(G4) Für alle $x, y \in G$ gilt

$$x \circ y = y \circ x.$$

Bei einer kommutativen Gruppe schreibt man meist $+$ statt $\circ$ mit dem neutralen Element 0.

Kommutative Gruppen

Eine Gruppe heißt *abelsch* oder *kommutativ*, wenn zusätzlich das Kommutativgesetz gilt:

(G4) Für alle $x, y \in G$ gilt

$$x \circ y = y \circ x.$$

Bei einer kommutativen Gruppe schreibt man meist $+$ statt $\circ$ mit dem neutralen Element 0.

Erinnert an die ganzen Zahlen $\mathbb{Z} = (Z, 0, +)$, die ja eine kommutative Gruppe bilden.

Gruppe der bijektiven Selbstabbildungen

Satz Sei A eine nichtleere Menge. Dann bilden die bijektiven Selbstabbildungen $f : A \to A$ zusammen mit der Verkettung $f \circ g$ eine Gruppe.

Gruppe der bijektiven Selbstabbildungen

Satz Sei A eine nichtleere Menge. Dann bilden die bijektiven Selbstabbildungen $f : A \to A$ zusammen mit der Verkettung $f \circ g$ eine Gruppe.

Neutrales Element: Die Identität $id_A : A \to A$, $id_A(a) = a$.

Gruppe der bijektiven Selbstabbildungen

Satz Sei A eine nichtleere Menge. Dann bilden die bijektiven Selbstabbildungen $f : A \to A$ zusammen mit der Verkettung $f \circ g$ eine Gruppe.

Neutrales Element: Die Identität $id_A : A \to A$, $id_A(a) = a$.

Insbesondere ist mit f, g bijektiv auch $f \circ g$ bijektiv und

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

Beweis

$f \circ id_A = id_A \circ f = f$ ist klar.

Beweis

$f \circ id_A = id_A \circ f = f$ ist klar.

Das inverse Element zu f ist die von uns definierte Umkehrabbildung.

Beweis

$f \circ id_A = id_A \circ f = f$ ist klar.

Das inverse Element zu f ist die von uns definierte Umkehrabbildung.

Ist

$$a \overset{h}{\mapsto} b \overset{g}{\mapsto} c \overset{f}{\mapsto} d,$$

so gilt gleichgültig wie man klammert, immer $f(g(h(a))) = d$.

I.A. nicht kommutativ

Hat die Menge A drei Elemente oder mehr, so ist die Gruppe der bijektiven Selbstabbildungen nicht kommutativ.

I.A. nicht kommutativ

Hat die Menge A drei Elemente oder mehr, so ist die Gruppe der bijektiven Selbstabbildungen nicht kommutativ.

Als Beispiel nehmen wir für $A_3 = \{1, 2, 3\}$

$$f(1) = 2,\ f(2) = 3,\ g(1) = 2,\ g(2) = 1 \ \Rightarrow\ f \circ g(1) = 3,\ g \circ f(1) = 1.$$

1.6 Ringe und Körper

$$\mathbb{R} = (R, 0, 1, +, \cdot).$$

1.6 Ringe und Körper

$\mathbb{R} = (R, 0, 1, +, \cdot)$. $\mathbb{R}$ heißt *Ring*, wenn

(R1) $(R, 0, +)$ ist eine kommutative Grupppe.

1.6 Ringe und Körper

$\mathbb{R} = (R, 0, 1, +, \cdot)$. $\mathbb{R}$ heißt *Ring*, wenn

(R1) $(R, 0, +)$ ist eine kommutative Grupppe.

(R2) $(R, 1, \cdot)$ ist eine Halbgruppe mit neutralem Element 1, d.h. es gilt das Assoziativgesetz sowie $x \cdot 1 = 1 \cdot x = x$.

1.6 Ringe und Körper

$\mathbb{R} = (R, 0, 1, +, \cdot)$. $\mathbb{R}$ heißt *Ring*, wenn

(R1) $(R, 0, +)$ ist eine kommutative Grupppe.

(R2) $(R, 1, \cdot)$ ist eine Halbgruppe mit neutralem Element 1, d.h. es gilt das Assoziativgesetz sowie $x \cdot 1 = 1 \cdot x = x$.

(R3) Es gelten die Distributivgesetze

$$(x + y) \cdot z = x \cdot z + y \cdot z, \quad x \cdot (y + z) = x \cdot y + x \cdot z.$$

1.6 Ringe und Körper

$\mathbb{R} = (R, 0, 1, +, \cdot)$. $\mathbb{R}$ heißt *Ring*, wenn

(R1) $(R, 0, +)$ ist eine kommutative Grupppe.

(R2) $(R, 1, \cdot)$ ist eine Halbgruppe mit neutralem Element 1, d.h. es gilt das Assoziativgesetz sowie $x \cdot 1 = 1 \cdot x = x$.

(R3) Es gelten die Distributivgesetze

$$(x + y) \cdot z = x \cdot z + y \cdot z, \quad x \cdot (y + z) = x \cdot y + x \cdot z.$$

Ist die Operation „$\cdot$“ zusätzlich kommutativ, so heißt $\mathbb{R}$ *kommutativer Ring*.

$\mathbb{Z}$

Der bekannteste kommutative Ring sind die ganzen Zahlen

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

mit der üblichen Addition und Multiplikation.

Körper

Ein *Körper* $\mathbb{K} = (K, 0, 1, +, \cdot)$ ist ein kommutativer Ring, in dem zusätzlich gilt:

$(K \setminus \{0\}, 1, \cdot)$ ist eine kommutative Gruppe.

Körper

Ein *Körper* $\mathbb{K} = (K, 0, 1, +, \cdot)$ ist ein kommutativer Ring, in dem zusätzlich gilt:

$(K \setminus \{0\}, 1, \cdot)$ ist eine kommutative Gruppe.

D.h. es gilt zusätzlich:

Zu jedem $x \neq 0$ gibt es ein x^{-1} mit $xx^{-1} = 1$.

Der Körper Z_2

besteht nur aus den beiden neutralen Elementen 0 und 1.

0 ist neutral bezüglich der Addition:

$$0 + 0 = 0, \quad 0 + 1 = 1.$$

Der Körper Z_2

besteht nur aus den beiden neutralen Elementen 0 und 1.

0 ist neutral bezüglich der Addition:

$$0 + 0 = 0, \quad 0 + 1 = 1.$$

1 ist neutral bezüglich der Multiplikation:

$$0 \cdot 1 = 0, \quad 1 \cdot 1 = 1.$$

Der Körper Z_2

besteht nur aus den beiden neutralen Elementen 0 und 1.

0 ist neutral bezüglich der Addition:

$$0 + 0 = 0, \quad 0 + 1 = 1.$$

1 ist neutral bezüglich der Multiplikation:

$$0 \cdot 1 = 0, \quad 1 \cdot 1 = 1.$$

Zusätzlich setzt man

$$1 + 1 = 0, \quad 0 \cdot 0 = 0.$$