# Mathematik I WS 15/16

Thomas  $Dinges^1$  Jonas Wolf <sup>2</sup>

30. November 2015

Inoffizielles Skript für die Vorlesung Mathematik I im WS 15/16, bei Britta Dorn. Alle Angaben ohne Gewähr. Fehler können gerne via E-Mail gemeldet werden.

<sup>&</sup>lt;sup>1</sup>thomas.dinges@student.uni-tuebingen.de

<sup>&</sup>lt;sup>2</sup>mail@jonaswolf.de

# Inhaltsverzeichnis

1	Logi	k
	1.1	Negation
	1.2	Konjunktion
	1.3	Disjunktion
	1.4	XOR
	1.5	Implikation
	1.6	Äquivalenz
	1.7	Beispiel
	1.8	Definition
	1.9	Satz
	1.10	Bemerkung
	1.11	Bemerkung (Logisches Umformen)
		Definition
		Beispiel
		Definition
	1.15	Beispiel / Bemerkung
		Negation von All- und Existenzaussagen
2	Men	
	2.1	Definition (Georg Cantor, 1845-1918)
	2.2	Bemerkung
	2.3	Definition
	2.4	Beispiel
	2.5	Satz (Rechenregeln für Mengen)
3	Bewe	eismethoden 20
	3.1	Direkter Beweis
	3.2	Beweis durch Kontraposition
	3.3	Beweis durch Widerspruch, indirekter Beweis
	3.4	Vollständige Induktion
		3.4.1 Prinzip der vollständigen Induktion
		3.4.2 Bemerkung
		3.4.3 Verschärftes Induktionsprinzip
	3.5	Schubfachprinzip
		3.5.1 Idee
		3.5.2 Satz
		3.5.3 Beispiel
	3.6	Weitere Beweistechniken (Werkzeugkiste)

4	Abbi	ldungen 31
	4.1	Definition
	4.2	Beispiele
	4.3	Beispiele
	4.4	Definition
	4.5	Beispiel
	4.6	Definition
	4.7	Beispiele
	4.8	Definition
	4.9	Beispiel
	4.10	Bemerkung
	4.11	Definition
	4.12	Beispiel
		Satz
	4.14	Satz (Charakterisierung bijektiver Abbildungen)
		Bemerkung / Definition
	4.16	Satz (Wichtiger Satz für endliche Mengen)
	4.17	Das Prinzip der rekursiven Definition von Abbildungen 39
	4.18	Beispiel
		Bemerkung
	4.20	Beispiel (Fibonacci-Zahlen)
5	Rela	tionen 41
	5.1	Definition
	5.2	Beispiel
	5.3	Definition

## 1 Logik

### Aussagenlogik

Eine **logische Aussage** ist ein Satz, der entweder wahr oder falsch (also nie beides zugleich) ist. Wahre Aussagen haben den Wahrheitswert 1 (auch wahr, w, true, t), falsche den Wert 0 (auch falsch, f, false).

Notation: Aussagenvariablen  $A, B, C, ...A_1, A_2$ .

#### Beispiele:

- 2 ist eine gerade Zahl (1)
- Heute ist Montag (1)
- 2 ist eine Primzahl (1)
- 12 ist eine Primzahl (0)
- Es gibt unendlich viele Primzahlen (1)
- Es gibt unendlich viele Primzahlzwillinge (Aussage, aber unbekannt, ob 1 oder 0)
- 7 (keine Aussage)
- Ist 173 eine Primzahl? (keine Aussage)

Aus einfachen Aussagen kann man durch logische Verknüpfungen (**Junktoren**, z.B. und, oder, ...) kompliziertere bilden. Diese werden Ausdrücke genannt (auch Aussagen sind Ausdrücke). Durch sogenannte **Wahrheitstafeln** gibt man an, wie der Wahrheitswert der zusammengesetzten Aussage durch die Werte der Teilaussagen bedingt ist. Im folgenden seien A, B Aussagen.

Die wichtigsten Junktoren:

### 1.1 Negation

Verneinung von A:  $\neg A$  (auch  $\bar{A}$ ),  $nicht\ A$ , ist die Aussage, die genau dann wahr ist, wenn A falsch ist.

Wahrheitstafel:

A	$\neg A$
1	0
0	1

Beispiele:

• A: 6 ist durch 3 teilbar. (1)

•  $\neg A$ : 6 ist nicht durch 3 teilbar. (0)

• B: 4,5 ist eine gerade Zahl (0)

•  $\neg B$ : 4,5 ist keine gerade Zahl. (1)

### 1.2 Konjunktion

Verknüpfung von A und B durch  $und: A \wedge B$  ist genau dann wahr, wenn A und B gleichzeitig wahr sind.

Wahrheitstafel:

Α	В	$A \wedge B$
1	1	1
1	0	0
0	1	0
0	0	0

Beispiele:

•  $\underbrace{6 \text{ ist eine gerade Zahl}}_{A(1)}$  und  $\underbrace{\text{durch 3 teilbar}}_{B(1)}$ . (1)

•  $\underbrace{9 \text{ ist eine gerade Zahl}}_{A(0)}$  und  $\underbrace{\text{durch 3 teilbar}}_{B(1)}$ . (0)

## 1.3 Disjunktion

 $oder: A \vee B$ 

Wahrheitstafel:

Α	В	$A \lor B$
1	1	1
1	0	1
0	1	1
0	0	0

↑ Einschließendes oder, kein entweder...oder.

Beispiele:

• 6 ist gerade oder durch 3 teilbar. (1)

- 9 ist gerade oder durch 3 teilbar. (1)
- 7 ist gerade oder durch 3 teilbar. (0)

#### 1.4 XOR

entweder oder: A xor B,  $A \oplus B$  (ausschließendes oder, exclusive or).

Wahrheitstafel:

A	В	$A \oplus B$
1	1	0
1	0	1
0	1	1
0	0	0

### 1.5 Implikation

wenn, dann,  $A \Rightarrow B$ :

- wenn A gilt, dann auch B
- A impliziert B
- aus A folgt B
- A ist <u>hinreichend</u> für B,
- B ist notwendig für A

Wahrheitstafel:

Α	В	$A \Rightarrow B$
1	1	1
1	0	0
0	1	1
0	0	1

Merke: ex falso quodlibet: aus einer falschen Aussage kann man alles folgern!

(Die Implikation  $A\Rightarrow B$  sagt nur, dass B wahr sein muss, <u>falls</u> A wahr ist. Sie sagt nicht, dass B tatsächlich war ist.)

Beispiele:

• Wenn 1 = 0, bin ich der Papst. (1)

## 1.6 Äquivalenz

genau dann wenn,  $A \Leftrightarrow B$  (dann und nur dann wenn, g.d.w, äquivalent, if and only if, iff)

Wahrheitstafel:

Α	В	$A \Leftrightarrow B$
1	1	1
1	0	0
0	1	0
0	0	1

Beispiele:

- Heute ist Montag genau dann wenn morgen Dienstag ist. (1)
- Eine natürliche Zahl ist durch 6 teilbar g. d. w. sie durch 3 teilbar ist. (0)  $A \Rightarrow B \ (1)$   $B \Rightarrow A \ (0)$

### Festlegung

 $\neg$ bindet stärker als alle anderen Junktoren:  $(\neg A \land B)$ heißt  $(\neg A) \land B$ 

## 1.7 Beispiel

a)

Wann ist der Ausdruck  $(A \lor B) \land \neg (A \land B)$  wahr?

 $\rightarrow$  Wahrheitstafel

A	В	$(A \vee B)$	$(A \wedge B)$	$\neg (A \land B)$	$(A \vee B) \wedge \neg (A \wedge B)$
1	1	1	1	0	0
1	0	1	0	1	1
0	1	1	0	1	1
0	0	0	0	1	0

<u>∧</u> Klammerung relevant

Welche Wahrheitswerte ergeben sich für

•  $A \lor (B \land \neg A) \land B)$ ?

#### • $A \vee B \wedge \neg A \wedge B$ ?

 $(A \vee B) \wedge \neg (A \wedge B)$  und  $(A \oplus B)$  haben dieselben Wahrheitstafeln. Ausdrücke sehen unterschiedlich aus (Syntax), aber haben dieselbe Bedeutung (Semantik). Dies führt zu 1.8 Definition.

b)

Wann ist  $(A \wedge B) \Rightarrow \neg (C \vee A)$  falsch?

 $\rightarrow$  Wahrheitstafel: <u>alle</u> möglichen Belegungen von A, B, C mit 0/1

Α	В	С	$(A \wedge B)$	$\neg(C \lor A)$	$(A \land B) \Rightarrow \neg(C \lor A)$
1	1	1	1	0	0
1	1	0	1	0	0
1	0	1	0	0	1
1	0	0	0	0	1
0	1	1	0	0	1
0	1	0	0	1	1
0	0	1	0	0	1
0	0	0	0	1	1

oder überlegen:

$$(A \wedge B) \Rightarrow \neg (C \vee A)$$
 ist nur 0, wenn

$$(A \wedge B) = 1$$
, also  $A = 1$  und  $B = 1$ 

und

$$\neg (C \lor A) = 0 \text{ ist.}$$

(Wissen: A = 1), also  $\underline{C} = 0$  oder  $\underline{C} = 1$  möglich.

### 1.8 Definition

Haben zwei Ausdrücke  $\alpha$  und  $\beta$  bei jeder Kombination von Wahrheitswerten ihrer Aussagevariablen den gleichen Wahrheitswert, so heißen sie <u>logisch äquivalent</u>; man schreibt  $\alpha \equiv \beta$ . (' $\equiv$ ' ist kein Junktor, entspricht '=')

Es gilt: Falls  $\alpha \equiv \beta$  gilt, hat der Ausdruck  $\alpha \Leftrightarrow \beta$  immer den Wahrheitswert 1.

### 1.9 Satz

Seien  $A,\,B,\,C$  Aussagen. Es gelten folgende logische Äquivalenzen:

- a) Doppelte Negation:  $A \equiv \neg(\neg A)$
- b) Kommutativität von  $\land$ ,  $\lor$ ,  $\oplus$ ,  $\Leftrightarrow$ :
  - $(A \wedge B) \equiv (B \wedge A)$
  - $(A \lor B) \equiv (B \lor A)$
  - $(A \oplus B) \equiv (B \oplus A)$
  - $(A \Leftrightarrow B) \equiv (B \Leftrightarrow A)$

 $\wedge$  gilt nicht für ' $\Rightarrow$ ' !!  $(A \Rightarrow B \not\equiv B \Rightarrow A)$ 

- c) Assoziativität von  $\land$ ,  $\lor$ ,  $\oplus$ ,  $\Leftrightarrow$ :
  - $(A \wedge B) \wedge C \equiv A \wedge (B \wedge C)$
  - $(A \lor B) \lor C \equiv A \lor (B \lor C)$
  - $(A \oplus B) \oplus C \equiv A \oplus (B \oplus C)$
  - $(A \Leftrightarrow B) \Leftrightarrow C \equiv A \Leftrightarrow (B \Leftrightarrow C)$
- d) Distributivität:
  - $\bullet \ \ A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$
  - $\bullet \ \ A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$
- e) Regeln von DeMorgan:
- f)  $A \Rightarrow B \equiv \neg B \Rightarrow \neg A$
- $\mathbf{g)} \ A \Rightarrow B \equiv \neg A \vee B$
- **h)**  $A \Leftrightarrow B \equiv (A \Rightarrow B) \land (B \Rightarrow A)$

(Alle Äquivalenzen gelten auch, wenn die Aussagevariablen durch Ausdrücke ersetzt werden.)

Beweis: Jeweils mittels Wahrheitstafel (Übung!), zum Beispiel:

	A	$\neg A$	$\neg(\neg A)$
a)	1	0	1
	0	1	0

	Α	В	$(A \wedge B)$	$\neg (A \land B)$	$\neg A$	$\neg B$	$(\neg A \lor \neg B)$
	1	1	1	0	0	0	0
e)	1	0	0	1	0	1	1
	0	1	0	1	1	0	1
	0	0	0	1	1	1	1

#### 1.10 Bemerkung

$$(1.9 \text{ f}): (A \Rightarrow B) \equiv (\neg B \Rightarrow \neg A)$$

(1.9 f):  $(A \Rightarrow B) \equiv \underbrace{(\neg B \Rightarrow \neg A)}_{\text{wird } \underline{\text{Kontraposition}}}$  genannt, wichtig für Beweis. Wird im Sprachgebrauch oft falsch verwendet

**Beispiel:** Pit ist ein Dackel.  $\Rightarrow$  Pit ist ein Hund.

äquivalent zu:  $(\neg B) \Rightarrow (\neg A)$ 

Pit ist kein Hund.  $\Rightarrow$  Pit ist kein Dackel.

aber nicht zu:  $B \Rightarrow A$ 

Pit ist ein Hund.  $\Rightarrow$  Pit ist ein Dackel.

und nicht zu:  $\neg A \Rightarrow \neg B$ 

Pit ist kein Dackel.  $\Rightarrow$  Pit ist kein Hund.

**Beispiel:** Sohn des Logikers / bellende Hunde ( $\rightarrow$  Folien)

#### Bemerkung (Logisches Umformen) 1.11

Sei  $\alpha$  ein Ausdruck. Ersetzen von Teilausdrücken von  $\alpha$  durch logisch äquivalente Ausdrücke liefert einen zu  $\alpha$  äquivalenten Ausdruck. So erhält man eventuell kürzere/einfachere Ausdrücke, zum Beispiel:

$$\neg(A\Rightarrow B)\underset{1.9\text{ g})}{\equiv}\neg(\neg A\vee B)\underset{1.9\text{ e})}{\equiv}\neg(\neg A)\wedge(\neg B)\underset{1.9\text{ a})}{\equiv}A\wedge\neg B$$

#### 1.12 Definition

Ein Ausdruck heißt <u>Tautologie</u>, wenn er für jede Belegung seiner Aussagevariablen, immer den Wert 1 annimmt. Hat er immer Wert 0, heißt er <u>Kontradiktion</u>. Gibt es mindestens eine Belegung der Aussagevariablen, so dass der Ausdruck Wert 1 hat, heißt er erfüllbar.

### 1.13 Beispiel

- a)  $A \vee \neg A$  Tautologie  $A \wedge \neg A$  Kontradiktion
- b)  $\neg (A \Rightarrow B) \Leftrightarrow A \land \neg B$  Tautologie (vergleiche Beispiel in 1.11).  $(A \Rightarrow B) \Leftrightarrow (\neg A \lor B)$  Tautologie (vergleiche Beispiel in 1.9g).
- c)  $A \wedge \neg B$  ist erfüllbar (durch A = 1, B = 0).

### Prädikatenlogik

Eine <u>Aussageform</u> ist ein sprachliches Gebilde, dass formal wie eine Aussage aussieht, aber eine oder mehrere Variablen enthält.

Beispiel: 
$$P(x)$$
 :  $\underbrace{x}_{Variable} \leq \underbrace{10}_{Pr\ddot{a}dikat \; (Eigenschaft)}$ 

Q(x): x studiert Informatik R(y): y ist Primzahl und  $y^2 + 2$  ist Primzahl.

Eine AussageformP(x) wird zur Aussage, wenn man die Variable durch ein konkretes Objekt ersetzt. Diest ist nur dann sinnvoll, wenn klar ist, welche Werte für x erlaubt sind, daher wird oft die zugelassene Wertemenge mit angegeben. (hier Vorgriff auf Kapitel Mengen)

Im Beispiel:

- P(3) ist wahr, P(42) falsch.
- R(2) ist falsch, R(3) ist wahr.

Oft ist die Frage interessant, ob es wenigstens ein x gibt, für das P(x) wahr ist, oder ob P(x) sogar für alle zugelassenen x wahr ist.

#### 1.14 Definition

Sei P(x) eine Aussageform.

a) Die Aussage Für alle x (aus einer bestimmten Menge M) gilt P(x). ist wahr genau dann wenn P(x) für alle in Frage kommenden x wahr ist.

Schreibweise: 
$$\forall x \in M$$
 :  $P(x)$  für alle, für jedes aus der Menge M gilt Eigenschaft

auch 
$$\bigvee_{x \in M} P(x)$$
.

Das Symbol ∀ heißt All- Quantor, die Aussage All- Aussage.

b) Die Aussage Es gibt (mindestens) ein x aus M, das die Eigenschaft P(x) besitzt. ist wahr, g.d.w P(x) für mindestens eines der in Frage kommenden x wahr ist.

Schreibweise: 
$$\exists x \in M \quad \vdots \quad P(x)$$
.

∃ heißt Existenzquantor, die Aussage Existenzmenge.

### 1.15 Beispiel / Bemerkung

Übungsgruppe G: 
$$\underbrace{a}_{Anna}\underbrace{b}_{Bob}\underbrace{c}_{Clara}$$

$$B(x): x$$
 ist blond.  $W(x): x$  ist weiblich.

$$B(a) = 1, W(b) = 0$$

1. Alle Studenten der Gruppe sind blond. (1)

$$\forall x \in G$$
: x ist blond

$$\forall x \in G: B(x) (1)$$

Das bedeutet: a blond  $\wedge$  b blond  $\wedge$  c blond

$$\underbrace{B(a)}_{1} \wedge \underbrace{B(b)}_{1} \wedge \underbrace{B(c)}_{1}$$

∀ ist also eine Verallgemeinerung der Konjunktion.

2. Alle Studenten der Gruppe sind weiblich. (0)

$$\underbrace{W(a)}_{1} \wedge \underbrace{W(b)}_{0} \wedge \underbrace{W(c)}_{1}(0)$$

3. Es gibt einen Studenten der Gruppe, der weiblich ist. (1)

$$\exists x \in G: W(x) (1)$$

bedeutet: 
$$\underbrace{W(a)}_{1} \lor \underbrace{W(b)}_{0} \lor \underbrace{W(c)}_{1} = 1$$

 $\exists$  ist verallgemeinerte Disjunktion.

4. Aussage A: Alle Studenten der Gruppe sind weiblich. (0)

Verneinung von A?  $\neg A$ 

∧ Nicht korrekt wäre: Alle Studenten der Gruppe sind männlich. (Wahrheitswert ist auch 0)

Korrekt: Nicht alle Studenten der Gruppe sind weiblich (1) Es gibt (mindestens) einen Studenten der Gruppe, der nicht weiblich ist. (1)

allgemeiner:

#### 1.16 Negation von All- und Existenzaussagen

a)  $\neg(\forall x \in M : P(x)) \equiv \exists x \in M : \neg P(x)$ 

b) 
$$\neg(\exists x \in M : P(x)) \equiv \forall x \in M : \neg P(x)$$

(Verallgemeinerung der Regeln von DeMorgan) (vergleiche Beispiel 1.15, 4):

$$\neg(\forall x \in G : W(x))$$

$$\equiv \neg(W(a) \wedge W(b) \wedge W(c)$$

$$\underbrace{\equiv}_{DeMorgan} (\neg W(a)) \lor (\neg W(b)) \lor (\neg (W(c)))$$

$$\equiv \exists x \in G : \neg W(x)$$

### Bemerkung

Aussageformen können auch mehrere Variablen enthalten, Aussagen mit mehreren Quantoren sind möglich.

Zum Beispiel:

$$\exists x \in X \quad \exists y \in Y : P(x,y)$$
$$\exists x \in X \quad \forall y \in Y : P(x,y)$$

$$\forall x \in X \quad \exists y \in Y : P(x, y)$$
  
 $\forall x \in X \quad \forall y \in Y : P(x, y)$ 

Negation dann durch mehrfaches Anwenden von 1.16, zum Beispiel:

```
\neg(\forall x \in X \quad \forall y \in Y \quad \exists z \in Z : P(x, y, z))
\equiv \exists x \in X : \neg(\forall y \in Y \quad \exists z \in Z : P(x, y, z))
\equiv \exists x \in X \quad \exists y \in Y : \neg(\exists z \in Z : P(x, y, z))
\equiv \exists x \in X \quad \exists y \in Y \quad \forall z \in Z : \neg P(x, y, z))
```

#### Also:

ändere  $\exists$  in  $\forall$ ,  $\forall$  in  $\exists$ , verneine Prädikat.

### 2 Mengen

### 2.1 Definition (Georg Cantor, 1845-1918)

Eine  $\underline{\text{Menge}}$  ist eine Zusammenfassung von bestimmten wohlunterscheidbaren Objekten ( $\underline{\text{Elementen}}$ ) unserer Anschauung oder unseres Denkens zu einem Ganzen.

Im Folgenden seien A, B Mengen.

- a)  $x \in A : x$  ist Element der Menge A  $x \notin A : x$  ist nicht Element der Menge A oder auch:  $A \ni x : x$  ist Element der Menge A  $A \not\ni x : x$  ist nicht Element der Menge A
- b) Eine Menge kann beschrieben werden durch:

 $\mathbb{N} = \{1, 2, 3, 4, ...\}$  Menge der natürlichen Zahlen

 $\mathbb{N}_0=\{0,1,2,3,4,...\}$  Menge der natürlichen Zahlen mit der Null  $\mathbb{Z}=\{0,1,-1,2,-2,...\}$  Menge der ganzen Zahlen

• Charakterisierung ihrer Elemente:

 $A = \{x \mid x \text{ besitzt die Eigenschaft } E\}, \text{ z.B.:}$ 

$$A = \{ n \mid n \in \mathbb{N} \text{ und n ist gerade} \}$$

sprich: "mit der Eigenschaft"

$$= \{2, 4, 6, 8, ...\}$$

 $= \{x \mid \exists k \in \mathbb{N} \text{ mit } x = 2 \cdot k\} = \{2k \mid k \in \mathbb{N}\}\$ 

Bsp:  $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$  Menge der rationalen Zahlen

- c) Mit Ø bezeichnen wir die Menge ohne Elemente (leere Menge)
- d) Mit |A| bezeichnen wir die Anzahl der Elemente der Menge A (Kardinalität oder Mächtigkeit von A), zum Beispiel:

$$\left|\left\{1, a, \overline{*}\right\}\right| = 3, \quad \left|\emptyset\right| = 0, \quad \left|\mathbb{N}\right| = \infty, \quad \left|\left\{\mathbb{N}\right\}\right| = 1$$

e)  $A \cap B := \{x \mid x \in A \land x \in B\}$  heißt <u>Durchschnitt</u> oder <u>Schnittmenge</u> von A und B.

Grafische Veranschaulichung: Venn-Diagramm ( $\wedge$  gilt nicht als Beweis)



f)  $A \cup B := \{x \mid x \in A \lor x \in B\}$  heißt Vereinigung von A und B.



**Beispiele:**  $A = \{1, 2, 3\}, B = \{2, 3, 4\}, C = \{4\}$ 

$$A \cap B = \{2, 3\},\$$
  
$$A \cap C = \emptyset,$$

$$B \cap C = \{4\} = C$$
,

$$A \cup B = \{1, 2, 3, 4\}$$

g) A und B heißen disjunkt, falls gilt  $A \cap B = \emptyset$ 



h) A heißt Teilmenge von  $B, A \subseteq B$ , falls gilt:

$$x \in A \Rightarrow x \in B$$

Oder in Worten: Jedes Element von A ist auch Element von B.

Dasselbe bedeutet die Notation

$$B \supset A$$

(B ist Obermenge von A)

Beispiel:  $\{1,2\} \subseteq \{1,2,3\} \subseteq \mathbb{N} \subseteq \mathbb{N}_0 \subseteq \mathbb{Z} \subseteq \mathbb{R}$  (reelle Zahlen)

Es gilt:  $\emptyset \subseteq A$  für jede Menge A.

**Achtung:** Unterschied  $\subseteq, \in !$ 

Zum Beispiel:

 $A = \{1, \mathbb{N}\}\$  (hier ist die Menge  $\mathbb{N}$  ein Element von A, keine Teilmenge!)

$$1 \in A$$
,  $\mathbb{N} \in A$ ,  $\mathbb{N} \nsubseteq A$ ,  $2 \notin A$ ,  $\{1\} \subseteq A$ 

i) Zwei Mengen A, B heißen gleich  $(A=B, \text{ falls gilt: } A\subseteq B \text{ und } B\subseteq A \text{ (also } x\in A\Rightarrow/\Leftarrow/\Leftrightarrow x\in B.$ 

Darin liegt ein Beweisprinzip: Man zeigt A=B, indem man zeigt:

- $x \in A \Rightarrow x \in B$
- $x \in B \Rightarrow x \in A \text{ (mehr später)}$

Beispiel:  $A=2,3,4, \qquad B=\{x\in \mathbb{N}\mid x>1 \text{ und } x<5\}$  A=B

**j)**  $A \subsetneq B(A \subsetneq B)$  bedeutet  $A \subseteq B$ , aber  $A \neq B$ .

(d.h.  $\exists x \in B \text{ mit } x \notin A, \text{ aber } x \in B$ )

(A ist echte Teilmenge von B.)

k) Mit  $P(A) := \{B \mid B \text{ ist eine Teilmenge von A}\} = \{B \mid B \subseteq A\}$  bezeichnen wir die Menge aller (echten oder nicht echten) Teilmengen von A, die sogenannte Potenzmenge von A.  $(\emptyset \subseteq A \forall A, A \subseteq A \forall A)$ 

Beispiel:

$$A = \{1, \}, P(A) = \{\emptyset, \{\underbrace{1}_A\}\}$$

$$B = \{1, 2\}, P(B) = \{\emptyset, \{1\}, \{2\}, \{\underbrace{1, 2}\}\}\}$$

$$C = \{1, 2, 3\}, P(C) = \dots \text{ (8 Elemente)}$$

$$P(\emptyset) = \{\emptyset\}$$
Was ist  $P(P(A))$ ?
$$P(P(A)) = P(\{\emptyset, \{1\}\}) = \{\emptyset, \{\emptyset\}, \{1\}, \{\emptyset, \{1\}\}\}\}$$

1)  $A \setminus B := \{x \mid x \in A \text{ und } x \notin B\}$  heißt die <u>Differenz</u> (A ohne B).

Ist  $A \subseteq X$  mit einer Obermenge X, so heißt  $X \setminus A$  das Komplement von A (bezüglich X). Wir schreiben  $A_X^C$  oder kurz  $A^C$  (wenn X aus dem Kontext klar ist).

m)  $A \triangle B := (A \backslash B) \cup (B \backslash A)$  heißt die symmetrische Differenz von A und B.

### 2.2 Bemerkung

Verallgemeinerung der Vereinigung und des Durchschnitts:

$$A_1 \cap A_2 \cap \ldots \cap A_n = \{x \mid x \in A_1 \land x \in A_2 \land \ldots \land x \in A_n\}$$

$$=:\bigcap_{i=1}^n A_i$$

$$A_1 \cup \ldots \cup A_n = \{x \mid x \in A_1 \vee \ldots \vee x \in A_n\}$$

$$=: \bigcup_{i=1}^{n} A_i$$

Beziehungsweise noch allgemeiner:

Sei S eine Menge von Mengen (System von Mengen)

#### 2.3 Definition

Seien A, B Mengen.

$$A\underbrace{x}_{Kreuz}B := \{(a,b) \mid a \in A, b \in B\}$$

Die Menge aller geordneten Paare, heißt <u>kartesisches Produkt</u> von A und B (nach René Descartes, 1596 - 1650).

Dabei legen wir fest: (a, b) = (a', b') (mit  $a, a' \in A, b, b' \in B$ ):  $\Leftrightarrow a = a'$  und b = b'.

Allgemein sei für Mengen  $A_1, ...A_n (n \in \mathbb{N})$   $A_1xA_2x...xA_n := \{a_1, a_2, ..., a_n) \mid a_i \in A_i, \forall i = 1...n\}$ die Menge aller geordneten n-Tupel (mit analoger Gleichheitsdefinition).

$$(n = 2 : Paare, n = 3 : Tripel)$$

Schreibweise:

$$A_1 \times ... \times A : n =: \sum_{i=1}^n A_i$$

Ist eine der Mengen  $A_1, ... A_n$  leer, setzen wir  $A_1 \times ... \times A_n = \emptyset$ .

Statt  $A \times A$  schreiben wir auch  $A^2$ , statt  $\underbrace{A \times ... \times A}_{n-Faktoren} = A^n$ .

### 2.4 Beispiel

$$A = \{1, 2, 3\}, B = \{3, 4\}$$

$$(1, 3) \in A \times B, \underbrace{(3, 1)}_{B \times A} \notin A \times B,$$

$$\underbrace{(3, 1)}_{B \times A} \notin A \times B \in B \times A$$

$$(1,2) \in A \times B, \in A \times A$$
  
 $A \times B = \{(1,3), (1,4), (2,3), (2,4), (3,3), (3,4)\}$   
 $B \times A = \dots$   
 $B \times B = B^2 = \{(3,3), (3,4), (4,3), (4,4)\}$ 

## 2.5 Satz (Rechenregeln für Mengen)

Seien A, B, C, X Mengen. Dann gilt:

- a)  $A \cup B = B \cup A$   $A \cap B = B \cap A$ (Kommutativgesetz)
- b)  $(A \cup B) \cup C = A \cup (B \cup C)$   $(A \cap B) \cap C = A \cap (B \cap C)$ (Assoziativgesetz)
- c)  $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$   $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$ (Disbributivgesetz)
- d)  $A, B \subseteq X$ , dann  $(A \cap B)_X^C = A_X^C \cup B_X^C$   $(A \cup B)_X^C = A_X^C \cap B_X^C$  (Regeln von DeMorgan)
- e)  $A \subseteq X$ , dann  $(A_X^C)_X^C = A$
- f)  $A\Delta B = (A \cup B) \setminus (A \cap B)$  $(= \{x \mid x \in A \oplus x \in B\})$



g)  $A \cap B = A$  genau dann, wenn  $A \subseteq B$   $(A \cap B) = A \iff A \subseteq B$ )

h) 
$$A \cup B = A \Leftrightarrow B \subseteq A$$

**Beweis** 

a) 
$$A \cup B = \{x \mid x \in A \lor x \in B\}$$
  
=  $\{x \mid x \in B \lor x \in A\} = B \cup A$   
Kommutativgesetz 1.9 b)

 $A \cap B$  analog

b), c) Übung, wie a) benutze Assoziativgesetz (1.9 c) ) bzw. Distributivgesetz (1.9 d) ) für logische Äquivalenzen.

$$\begin{array}{l} \mathrm{d}) \ (A \cap B)_X^C \\ &= \{x \mid x \in X \setminus (A \cap B)\} \\ &= \{x \mid x \in X \wedge (x \notin (A \cap B))\} \\ &= \{x \mid x \in X \wedge \neg (x \in (A \cap B))\} \\ &= \{x \mid x \in X \wedge \neg (x \in A \wedge x \in B)\} \\ &= \{x \mid x \in X \wedge (x \notin A \vee x \notin B)\} \\ &= \{x \mid ((x \in X) \wedge (x \notin A)) \vee ((x \in X) \wedge (x \notin B))\} \\ &= A_X^C \cup B_X^C \end{array}$$

- 2. Regel analog
- e) ähnlich
- f) g) h) später

### 3 Beweismethoden

Ein mathematischer <u>Beweis</u> ist die Herleitung der Wahrheit (oder Falschheit) einer Aussage aus einer Menge von <u>Axiomen</u> (nicht beweisbare Grundtatsachen) oder bereits bewiesenen Aussagen nmittels logischen Folgerungen.

Bewiesene Aussagen werden Sätze genannt.

<u>Lemma</u> - Hilfssatz, der nur als Grundlage für wichtigeren Satz formuliert und bewiesen wird.

Theorem - wichtiger Satz

Korollar - einfache Folgerung aus Satz, z.B. Spezialfall

Definition - Benennung/Bestimmung eines Begriffs/Symbols

□ - Zeichen für Beweisende (■, q.e.d., wzbw...)

Mathematische Sätze haben oft die Form:

Wenn V (Voraussetzung) gilt, dann gilt auch B (Behauptung)

 $(V, B: Aussagen), kurz: V \Rightarrow B$ 

Zu zeigen ist also, dass  $V \Rightarrow B$  eine wahre Aussage ist.

### 3.1 Direkter Beweis

Gehe davon aus, dass V wahr ist, folgere daraus, dass B wahr ist.

 $[ \text{ Sei } V \text{ wahr}, \Rightarrow \dots \\ \Rightarrow \dots \\ \vdots \\ \Rightarrow B \text{ ist wahr } ]$ 

Beispiel: Sei  $n \in \mathbb{N}$ . Ist n gerade, so ist auch  $n^2$  gerade.

### 3.2 Beweis durch Kontraposition

vgl. Satz 1.9 f) 
$$A \Rightarrow B \equiv \neg B \Rightarrow \neg A$$

Statt  $V \Rightarrow B$  zu zeigen, können wir also auch  $\neg B \Rightarrow \neg V$  zeigen.

[ Es gelte  $\neg B \Rightarrow \dots$  $\Rightarrow \dots$  $\Rightarrow \dots$ 

$$\vdots \\ \Rightarrow \text{ es gilt } \neg V ]$$

Beispiel: Sei  $n \in \mathbb{N}$ .

$$\underbrace{\text{Ist } n^2 \text{ gerade}}_{V}, \underbrace{\text{so ist auch } n \text{ gerade}}_{B}.$$

#### Beweis durch Kontraposition:

### 3.3 Beweis durch Widerspruch, indirekter Beweis

Zu zeigen ist Aussage A. Wir gehen davon aus, dass A <u>nicht</u> gelte ( $\neg A$  ist wahr) und folgern durch logische Schlüsse eine zweite Aussage B, von der wir wissen, dass sie falsch ist. Wenn alle logischen Schlüsse korrekt waren, muss also  $\neg A$  falsch gewesen sein, also A wahr.

( 
$$((\neg A \Rightarrow B) \land (\neg B)) \Rightarrow A \text{ ist Tautologie})$$

**Beispiel:** [Euklid]  $\sqrt{2} \notin \mathbb{Q}$ 

Beweis: Wir nehmen an, dass die Aussage falsch ist, also  $\sqrt{2} \in \mathbb{Q}$  gilt, das heißt  $\sqrt{2} = \frac{p}{q}$  mit p. q.  $\in \mathbb{Z}(q \neq 0)$  teilerfremd (vollständig gekürzter Bruch)

$$\Rightarrow 2 = \frac{p^2}{q^2}$$

 $\Rightarrow p^2=2q^2,$ also ist  $p^2$  gerade, damit aber auch p<br/> gerade (Beispiel in 3.2), also p=2\*rmit <br/>  $r\in\mathbb{Z}.$ 

$$\Rightarrow p^2 = (2r)^2 = 2q^2$$

$$\Rightarrow 4r^2 = 2q^2$$

$$\Rightarrow \underline{2r^2 = q^2}$$

 $\Rightarrow q^2$  gerade

 $\Rightarrow q$  gerade

Also: p gerade, q gerade, Widerspruch zu p, q teilerfremd.

Also war die Annahme falsch, es muss  $\sqrt{2} \notin \mathbb{Q}$  gelten.  $\square$ 

### 3.4 Vollständige Induktion

Eine Methode, um Aussagen über natürliche Zahlen zu beweisen.

#### Beispiel: Gauß

$$1 + 2 + \dots + 100 = ?$$

$$1 \quad 2 \quad 3 \quad \dots \quad 50$$

$$+ 100 \quad 99 \quad 98 \quad \dots \quad 51$$

$$101 \quad 101 \quad 101 \quad \dots \quad 101$$

$$50 * 101 = 5050$$

$$(=\frac{100}{2}*101)$$

#### Allgemein:

$$\frac{1}{1+2+3} + \dots + n \underbrace{=}_{Vermutung} \frac{n(n+1)}{2}$$

$$(n \in \mathbb{N})$$

#### 3.4.1 Prinzip der vollständigen Induktion

Sei  $n_0 \in \mathbb{N}$  fest vorgegeben (oft  $n_0 = 1$ ).

Für jedes  $n \geq n_0, n \in \mathbb{N}$ , sei A(n) eine Aussage, die von n abhängt.

Es gelte:

1.  $A(n_0)$  ist wahr (Induktionsanfang)

2. 
$$\forall n \in \mathbb{N}, n \ge n_0$$
: Ist $A(n)$ wahr, so ist $A(n+1)$ wahr. (Induktionsschritt)

Induktionsvorraussetzung Induktionsbehauptung

Dann ist die Aussage A(n) für alle  $n \ge n_0$  wahr. (Dominoprinzip)

(Bemerkung: gilt auch für  $\mathbb{N}_0$  ( $n_0 = 0$  auch möglich) und für  $n_0 \in \mathbb{Z}$ , Behauptung gilt dann für alle  $n \in \mathbb{Z}$  mit  $n \geq n_0$ ).

Beispiel:

a) Kleiner Gauß  $1+2+...+n=\frac{n(n+1)}{2} \forall n \in \mathbb{N}$ 

Beweis:

$$A(n): 1+2+...+n = \frac{n(n+1)}{2}$$

- Induktionsan<br/>fang  $(n=1):A(1):1=\frac{1*(1+1)}{2}$
- Induktionsschritt:

Induktionsvorraussetzung: sei  $n \geq 1$ . Es gelte A(n), d.h.  $1 + ... + n = \frac{n(n+1)}{2}$ 

Induktionsbehauptung: Es gilt A(n+1), d.h.  $1 + ... + n + (n+1) = \frac{(n+1)(n+1+1)}{2}$ 

Beweis: 
$$\underbrace{1+2+...+n}_{Ind.vor.} + (n+1) = \underbrace{\frac{n(n+1)}{2}}_{Ind.vor.} + (n+1)$$

$$= \frac{n^2+n+2n+2}{2}$$

$$= \frac{(n+1)(n+2)}{2}$$

$$A(n+1)$$

- **b)**  $A(n): 2^n \ge n \forall n \in \mathbb{N}$ 
  - Induktionsanfang: (n = 1) : A(1) gilt:  $2^1 \ge 1$
  - Induktionsschritt:

Induktionsvorraussetzung: Sei  $n \ge 1$ . Es gelte A(n), d.h.  $2^n \ge n$ 

Induktionsbehauptung: (Zu zeigen!): Es gilt A(n+1), d.h.  $2^{2+1} \ge n+1$ .

Beweis: 
$$2^{n+1} = 2 * 2^n \ge 2 * n$$

$$= n + n$$

$$\ge n + 1,$$
also  $2^{n+1} \ge n + 1$ 

#### 3.4.2 Bemerkung

Für Formeln wie in Beispiel 3.4.1a) benutzen wir das Summenzeichen  $\Sigma$  (sigma, großes griechisches S)

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2} \ 1 + 2 + 3 + \dots + n \ k = 1 \\ k = 2k = 3k = n$$

weitere Bsp:

$$\sum_{k=1}^{n} 2k = 2 * 1 + 2 * 2 + ... 2 * n \sum_{k=4}^{n} 2k = 2 * 4 + 2 * 5 + .... 2 * n$$

$$\sum_{k=1}^{3} 7 = 7 + 7 + 7 = 21$$

allg. 
$$\sum_{k=m}^{n} a_k = a_m + a_{m+1} + a_n \ (a_m, a_{m+1}, ...a-n \in \mathbb{R})$$

h heißt Summationszeichen

$$\sum_{k=m}^{n} a_k = \sum_{i=m}^{n} a_i$$

Schreibweisen:

$$\sum_{k=1}^{n} a_k, \sum_{k=1}^{n} a_k, \sum_{k\in\mathbb{N}} a_k, \sum_{k=1, k\neq 2}^{4} a_k = a_1 + a_3 + a_4$$

Für n < m setzt man

$$\sum_{k=m}^{n} a_k = 0$$
 (leere Summe), z.B.  $\sum_{k=7}^{3} k = 0$ 

#### Produktzeichen $\Pi$

$$\prod_{k=m}^{n} a_k = a_m * a_{m+1}...a_n,$$

für 
$$n < m$$
 setze  $\prod_{k=m}^{n} a_k = 1$ 

Rechenregeln für Summen (zu beweisen z.B. durch vollständige Induktion)

**a**)

$$\sum_{k=m}^{n} a = (n - m + 1) * a$$
$$(\sum_{k=3}^{5} a = a + a + a = (5 - 3 + 1) * a)$$

b)

$$\sum_{k=m}^{n} (c * a_k) = c * \sum_{k=m}^{n} a_k$$

c) Indexverschiebung

$$\sum_{k=m}^{n} a_k = a_m + a_{m+1} + \dots a_n$$
  
=  $a_{(m+e)-e} + a_{(m+1+e)-e} + \dots + a_{(n+e)-e}$   
neuer Summations index  $j := k + e$ 

(k durchläuft Werte: 
$$m, m + 1..., n$$
, j durchläuft Werte:  $m + e, m + 1 + e, ... n + e$ ) also gilt  $\sum_{k=m}^{n} a_k = \sum_{j=m+e}^{n+e} a_{j-e}$  (Beispiel:  $\sum_{k=0}^{5} a_k * x^{k+2} = \sum_{j=2}^{7} a_{j-2} * x^j$ )

d) Addition von Summen gleicher Länge

$$\sum_{k=m}^{n} (a_k + b_k) = \sum_{k=m}^{n} a_k + \sum_{k=m}^{n} b_k$$

e) Aufspalten

$$\sum_{k=m}^{n} a_k = \sum_{k=m}^{l} a_k + \sum_{k=l+1}^{n} a_k$$
 für  $m < l < n$ 

f) Teleskopsumme

$$\sum_{k=m}^{n} (a_k - a_{k+1}) = a_m - a_{n+1}$$

$$\sum_{k=m}^{n} (a_k - a_{k+1}) = (a_m - a_{m+1} + (a_{m+1} - a_{m+2} + (a_{m+2}...) + (a_n - a_{m+1}))$$

g) Doppelsummen

$$\sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} = \sum_{i=1}^{n} (a_{i1} + a_{i2} + \dots + a_{im} = a_{11} + a_{12} + \dots + a_{1m} + a_{21} + a_{22} + a_{2m}$$

#### 3.4.3 Verschärftes Induktionsprinzip

 $A(n), n_0$  wie in 3.4.1

Es gelte:

- (1)  $A(n_0)$  ist wahr
- $(2) \ \forall n \ge n_0:$

Sind  $A(n_0)$ , ..., A(n) wahr, so ist A(n+1) wahr.

(d.h. 
$$A(n_0) \wedge A(n_0 + 1) \wedge ... \wedge A(n) \Rightarrow A(n + 1)$$
)

Dann ist A(n) wahr für <u>alle</u>  $n \in \mathbb{N}, n \ge n_0$ 

Beispiel: A(n): Jede natürliche Zahl n > 1 ist Primzahl oder Produkt von Primzahlen.

Beweis:

Induktionsanfang:  $(n_0 = 2)$ . n = 2 ist Primzahl  $\checkmark$ 

Induktionsschritt: Sei  $n \ge n_0$   $(n \ge 2)$ 

#### • Induktionsvoraussetzung:

Aussage gilt für 2, 3, 4, ..., n

$$(A(2), A(3), A(4), ..., A(n) \text{ wahr})$$

#### • Induktionsbehauptung:

A(n+1) gilt, d.h. n+1 ist Primzahl oder Produkt von Primzahlen.

Beweis:

- falls n+1 Primzahl, so gilt A(n+1)
- falls n+1 keine Primzahl, dann ist  $n+1=k \cdot l$ , für  $k,l \in \mathbb{N}$ , 1 < k < n+1, 1 < l < n+1 (k=l möglich).

Nach Induktionsvoraussetzung:

Aussage gilt für 
$$k$$
 und  $l \Rightarrow n+1$  ist Produkt von Primzahlen.  $(A(n+1) \text{ ist wahr})$ 

### 3.5 Schubfachprinzip

#### 3.5.1 Idee

In einem Schrank befinden sich n verschiedene Paar Schuhe. Wie viele Schuhe muss man maximal herausziehen, bis man sicher ein zusammenpassendes Paar hat?

(Antwort: n+1)

#### 3.5.2 Satz

(Schubfachprinzip, engl.: pigeon hole principle)

Seien  $k, n \in \mathbb{N}$ .

Verteilt man n Objekte auf k Fächer, so gibt es ein Fach, das mindestens  $\lceil \frac{n}{k} \rceil$  Objekte enthält.

(Dabei bezeichnet [x] die kleinste ganze Zahl z mit  $x \leq z$ .)

Beweis (durch Kontraposition):

$$(\underbrace{n \text{ Objekte}, k \text{ Fächer}}_{A} \Rightarrow \underbrace{\exists \text{ Fach mit mind. } \lceil \frac{n}{k} \rceil \text{ Objekten}}_{B}$$

statt  $A \Rightarrow B$  zeige  $\neg B \Rightarrow \neg A$ )

 $(\neg B)$  Jedes Fach enthalte höchstens  $\lceil \frac{n}{k} \rceil - 1$  Objekte.

Dann ist die Gesamtzahl von Objekten höchstens

$$k \cdot \underbrace{\left( \left\lceil \frac{n}{k} \right\rceil - 1 \right)}_{< \frac{n}{k}} < k \cdot \frac{n}{k} = n$$

 $(\neg A)$  es gibt also weniger als n Objekte

#### 3.5.3 Beispiel

a) Wieviele Menschen müssen auf einer Party sein, damit <u>sicher</u> 2 am selben Tag Geburtstag haben?

367

b) Auf jeder Party mit mindestens 2 Gästen gibt es 2 Personen, die dieselbe Anzahl <u>Freunde</u> auf der Party haben.

Beweis: Sei n die Anzahl der Partygäste. Jeder Gast kann mit 0, 1, 2, ..., n-1 Gästen befreundet sein (n Möglichkeiten).

Aber: Es kann nicht sein, dass ein Gast 0 Freunde hat und gleichzeitig ein Gast n-1 (=alle) Freunde hat.

 $\Rightarrow$ Es gibt n-1mögliche Werte für die Anzahl der Freunde, entspricht n-1 Fächern.

Jeder der n Gäste trägt sich in ein Fach ein  $\Rightarrow$  mindestens 2 Gäste sind im selben Fach.

c) In Berlin gibt es mindestens 2 Personen, die genau dieselbe Anzahl Haare auf dem Kopf haben.

Beweis: Anzahl Haare im Durchschnitt:

blond 150.000 braun 110.000 schwarz 100.000 rot 90.000 zur Sicherheit: maximal 1 Millionen Haare möglich entspricht 1 Mio Fächer.

Anzahl Einwohner in Berlin: 3,5 Millionen  $\Rightarrow$  Behauptung 3.5.2

### 3.6 Weitere Beweistechniken (Werkzeugkiste)

- a) Wichtigste Technik: Ersetzen eines mathematischen Begriffs durch seine Definition (und umgekehrt).  $A(\subset B = \{x \mid x \in A \lor x \in B\})$
- b) Aussagen der Form  $\forall a \in S$  gilt P(a): beginne mit: Sei  $a \in S$ , zeige P(a).
- c) Aussage der Form  $\exists a \in S \text{ mit } P(a)$  oft: finde/gebe konkretes Element a an, für dass P(a) gilt.
- d) Gleichheit von Mengen zeigt man oft mittels Inklusion (vgl. Definition 2.1(i))

Zu zeigen: 
$$A = B$$
  $(A, B \text{ Mengen})$  zeige:  $A \subseteq B$  (Sei  $a \in A \Rightarrow ... \Rightarrow ... \Rightarrow a \in B$ ) 2.1 (i)) und  $B \subseteq A$  (Sei  $b \in B \Rightarrow ... \Rightarrow ... \Rightarrow b \in A$ )

⊆ ...

Beispiel: 2.5f)

$$A\triangle B = (A \cup B) \setminus (A \cap B)$$

Beweis:

$$\subseteq$$
 Sei  $x \in A \triangle B = (A \backslash B) \cup (B \backslash A)$ 

1. Fall:

$$x \in A \backslash B$$
, dann gilt  $x \in A$ , also  $x \in A \cup B$ 

Außerdem  $x \notin B$ , also gilt auch  $x \notin A \cap B$ 

$$\Rightarrow x \in (A \cup B) \setminus (A \cap B)$$

2.Fall

Ist  $x \in B \setminus A$ , so argumentiere analog.

$$\supseteq$$
 sei  $x \in (A \cup B) \setminus (A \cap B)$   
 $\Rightarrow x \in A \text{ oder } x \in B.$ 

1.Fall

$$x \in A$$
, so ist  $x \notin B$ , da  $x \notin A \cap B$   
 $\Rightarrow x \in A \backslash B \subseteq (A \backslash B) \cup (B \backslash A)$   
 $= A \triangle B$ ,  
d.h.  $x \in A \triangle B$ .

2.Fall (1. Fall analog)

$$x \in B$$
, so  $x \notin A$ , da  $x \notin A \cap B$   
 $\Rightarrow x \in B \setminus A \subseteq A \triangle B$   
Also  $x \in A \triangle B$ 

e) Äquivalenzen  $(A \Leftrightarrow B, A, B \text{ Aussagen})$  werden meist in 2 Schritten bewiesen:

Hinrichtung zeigt 
$$A \Rightarrow B$$
,  
Rückrichtung zeigt  $B \Rightarrow A$ .

⇒: ...

*⇐: ...* 

(oft auch eine von beiden mittels Kontraposition)

Beispiel: 2.5g) 
$$A \cap B = A \Leftrightarrow A \subseteq B$$

Beweis:

$$\Rightarrow$$
: Sei  $A \cap B = A$ . Dann ist  $A = A \cap B \subseteq B$   
 $\Leftarrow$ : Sei  $A \subseteq B$ . Dann ist  $A \subseteq A$  und  $A \subseteq B$ ,  
also ist  $A \subseteq A \cap B$   
außerdem  $A \cap B \subseteq A$ 

$$\Rightarrow A = A \cap B$$

2.5h) analog.

 ${f f}$ ) Äquivalenzen der Form:

Sei ... . Dann sind folgende Aussagen äquivalent:

- a) ...
- b) ...
- c) ..
- d) ...

Zeigt man durch Ringschluss:

Zeige 
$$a$$
)  $\Rightarrow$   $b$ )  $\Rightarrow$   $c$ )  $\Rightarrow$   $d$ )  $\Rightarrow$   $a$ )

(oder andere Reihenfolge, soll Ring geben.)

# 4 Abbildungen

### 4.1 Definition

a) Eine Abbildung (oder <u>Funktion</u>)

$$f:A\to B$$

besteht aus

- zwei nicht-leeren Mengen:
   A, dem <u>Definitionsbereich</u> von f
   B, dem <u>Bildbereich</u> von f
- und einer Zuordnungsvorschrift, die jedem Element  $a \in A$  genau ein Element  $b \in B$  zuordnet

Wir schreiben dann b = f(a), nennen b das <u>Bild</u> oder den <u>Funktionswert</u> von a (unter f), und a (ein) <u>Urbild</u> von b (unter f).

Notation:

$$f: A \to B$$
  
 $a \mapsto f(a)$ 

b) Die Menge  $G_f := \{(a, f(a)) \mid a \in A\} \subseteq A \times B$  heißt der Graph von f.

### 4.2 Beispiele

Siehe Folien!

### 4.3 Beispiele

a) A Menge

$$id_A: A \to A$$
  
 $x \mapsto x$ 

identische Abbildung

b)  $f: \mathbb{R} \to \mathbb{R}$  $x \mapsto x^2$  ist Abbildung (aus der Schule bekannt als  $f(x) = x^2$ ) c)  $\wedge$  kann als Abbildung aufgefasst werden, + ebenso:

Allgemein bezeichnet man eine Abbildung  $\{0,1\}^n \to \{0,1\}^m \ (n,m\in\mathbb{N})$  als boolesche Funktion.

### 4.4 Definition

Zwei Abbildungen  $f:A\to B,\ g:C\to D$  heißen gleich (in Zeichen: f=g), wenn:

- $\bullet$  A = C
- $\bullet$  B=D
- f(a) = g(a)

$$\forall a \in A (= C)$$

## 4.5 Beispiel

$$f: \{0,1\} \to \{0,1\}, x \mapsto x$$
$$g: \{0,1\} \to \{0,1\}, x \mapsto x^2$$
$$f = g$$

### 4.6 Definition

Sei  $f: A \to B$ , seien  $A_1 \subseteq A, B_1 \subseteq B$  Teilmengen.

Dann heißt

a)  $f(A_1) := \{f(a) \mid a \in A_1\} \subseteq B \text{ das } \underline{\text{Bild}} \text{ von } A_1 \text{ (unter } f) \text{ (Bildmenge)}.$ 

(Beispiel: 
$$f: \mathbb{N} \to \mathbb{N}$$
  
 $x \mapsto 2x$   
 $A_1 = \{1, 3\}$   
 $f(A_1) = \{f(1), f(3)\} = \{2, 6\}$ )

b)  $f^{-1}(B_1) := \{ a \in A \mid f(a) \in B_1 \} \subseteq A$ das Urbild von  $B_1$  (unter f).

(Beispiel oben: 
$$B_1 = \{8, 14, 100\}, f^{-1}(B_1) = \{4, 7, 50\}$$
  
 $B_2 = \{3\}, f^{-1}(B_2) = \emptyset$ )

c) f surjektiv, falls gilt: f(a) = B

(d.h. 
$$\forall b \in B \exists a \in A : f(a) = b$$
)

[ alle Elemente von B werden getroffen ]

d) f injektiv, falls gilt:

$$\forall a_1, a_2 \in A \text{ mit } a_1 \neq a_2 \text{ gilt } f(a_1) \neq f(a_2)$$

(äquivalent: 
$$f(a_1) = f(a_2) \Rightarrow a_1 = a_2$$
)

[ kein Element von B wird doppelt getroffen ]

e) f bijektiv, falls f surjektiv und injektiv (f ist Bijektion).

[ jedes Element wird genau einmal getroffen ]

#### 4.7 Beispiele

siehe Folien

- a) f aus Beispiel in 4.6 a) ist injektiv, aber nicht surjektiv:
  - $f(\mathbb{N})$  ist Menge der geraden natürlichen Zahlen, nicht  $\mathbb{N}$ .

b) 
$$f: \mathbb{R} \to \mathbb{R}$$
  
 $x \mapsto x^2$ 

$$x \mapsto x^2$$

nicht surjektiv:

$$f(\mathbb{R}) = \mathbb{R}_0^+ = \{x \in \mathbb{R} \mid x \ge 0\} \ne \mathbb{R}$$

nicht injektiv:

$$f(1) = f(-1) = 1$$

$$f(2) = f(-2) = 4$$

$$g: \mathbb{R}_0^+ \to \mathbb{R}_0^+$$
$$x \mapsto x^2$$

injektiv, surjektiv, bijektiv

c) 
$$f: \mathbb{R} \to \mathbb{R}$$
  
 $x \mapsto 2x + 1$   
ist surjektiv:  
Sei  $y \in \mathbb{R}$ . Zeige:  $\exists x \in \mathbb{R}$  mit  $y = 2x + 1$  (vgl. 3.6 b) )  
Wähle  $x = \frac{y-1}{2}$   
 $f$  ist injektiv:  
angenommen, es gibt  $x_1, x_2 \in \mathbb{R}$   
mit  $f(x_1) = f(x_2)$ , d.h.  
 $2x_1 + 1 = 2x_2 + 1$ ,  
dann folgt  $x_1 = x_2$ .

### 4.8 Definition

Sei  $f: A \to B$  bijektiv. Dann definieren wir die <u>Umkehrfunktion</u>.

 $f^{-1}:B\to A,$ indem wir jedem  $b\in B$ dasjenige  $a\in A$ zuordnen, für das f(a)=b gilt.

### 4.9 Beispiel

$$A(a_1, a_2, a_3) \qquad B(b_1, b_2, b_3)$$

$$f: (A \to B) \text{ bijektiv}$$

$$a_1 \to b_2$$

$$a_2 \to b_3$$

$$a_3 \to b_1$$

$$f^{-1}: B \to A$$

$$b_1 \to a_3$$

$$b_2 \to a_1$$

$$b_3 \to a_2$$

### 4.10 Bemerkung

Man kann jedem  $b \in B$  wirklich ein  $a \in A$  zuordnen, das f(a) = b erfüllt, denn f ist surjektiv. Nur <u>ein</u> solches a, denn f ist injektiv.

#### 4.11 Definition

Seien  $g: A \to B$   $f: B \to C$ Abbildungen.

Dann heißt die Abbildung:  $f \circ g : A \to C$  $a \to (f \circ g)(a) :=$  $f(g(a)) \forall a \in A$ 

die Hintereinanderausführung oder Komposition von f mit g.

f nach g

$$A \underset{g}{\longrightarrow} B \underset{f}{\longrightarrow} C$$

### 4.12 Beispiel

 $A = B = C = \mathbb{R}$ 

$$\begin{array}{ll} f: \mathbb{R} \to \mathbb{R} & g: \mathbb{R} \to \mathbb{R} \\ x \to x+1 & x \to 2x \end{array}$$

$$(f \circ g)(x) = f(g(x)) = f(2x) = 2x + 1$$

$$(g \circ f)(x) = g(f(x)) = g(x+1) = 2 * (x+1)$$
  
= 2x + 2

hier also  $f \circ g \neq g \circ f!$ 

### 4.13 Satz

Die Komposition {inj., surj., bij} Abbildungen ist {inj., surj., bij}

Beweis: Pü / Ü

### 4.14 Satz (Charakterisierung bijektiver Abbildungen)

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

f ist bijektiv genau dann, wenn es eine Abbildung  $g: B \to A$  gibt mit  $g \circ f = id_A$  und  $f \circ g = id_B$ .

Diese Abbildung g ist eindeutig und genau die Umkehrfunktion von f, also  $g = f^{-1}$ .

 $f^{-1}$  ist ebenfalls bijektiv und es gilt  $(f^{-1})^{-1} = f$ 

#### Beweis:

" $\Rightarrow$ " Sei f bijektiv. Dann existiert für jedes  $b \in B$  genau ein  $a \in A$  mit b = f(a).

Definiere nun also  $g:B\to A$  mit  $g(b)=\underline{a},$  dann gilt die Aussage:

$$(g \circ f)(a) = g(\underline{f(a)}) = g(\underline{b}) = a = id_A(a)$$

$$(f \circ g)(b) = f(\underline{g(b)}) = f(\underline{a}) = b = id_B(b)$$

" $\Leftarrow$ " Es existiere Abbildung g wie angegeben (zu zeigen: f ist bijektiv)

- f surjektiv: Sei  $b \in B$ . Dann ist  $g(b) \in A$ ,  $f(\underline{g(b)}) = id_B(b) = b$ , d.h. g(b) ist Urbild von b unter f.
- f injektiv:

Sei 
$$f(a_1) = f(a_2)$$

Dann ist 
$$\underline{\underline{a_1}} = g(\underline{f(a_1)}) = g(f(a_2)) = \underline{\underline{a_2}}$$

• Eindeutigkeit von g:

Angenommen es gäbe Abbildungen  $g_1, g_2$  mit angegebenen Eigenschaften.

Sei  $b \in B$ . Dann gibt es genau ein  $a \in A$  mit f(a) = b.

Also 
$$g_1(b) = g_1(\underline{f(a)}) = a = g_2(\underline{f(a)}) = g_2(\underline{b}),$$
  
d.h.  $g_1 = g_2$ 

•  $f^{-1}$  bijektiv,  $(f^{-1})^{-1} = f$ :

folgt aus  $f \circ f^{-1} = id_B$ ,  $f^{-1} \circ f = id_A$ , wende Aussage des Satzes auf  $f^{-1}$  an.

### 4.15 Bemerkung / Definition

Bijektivität erlaubt präzise Definition der Endlichkeit / Unendlichkeit von Mengen:

a) Menge  $M \neq \emptyset$  heißt endlich  $\Leftrightarrow \exists n \in \mathbb{N} : \exists$  bijektive Abbildung  $f : \{1, ..., n\} \rightarrow M$ .

 $(\emptyset$  wird auch als endlich bezeichnet).

Andernfalls heißt M unendlich.

[Hilberts Hotel]

b) Zwei Mengen  $M_1, M_2$  heißen gleichmächtig, falls es eine bijektive Abbildung  $g: M_1 \to M_2$  gibt.

Beispiel: N, 2N (alle geraden natürlichen Zahlen) gleichmächtig:

$$g: \mathbb{N} \to 2\mathbb{N}$$

$$n \mapsto 2n$$

ist bijektiv.

c) Menge M heißt <u>abzählbar unendlich</u>, wenn M gleichmächtig ist wie  $\mathbb{N}$ , d.h.  $\exists$  bijektive Abbildung.

$$h: \mathbb{N} \to M$$
.

#### Beispiel:

- N abzählbar unendlich:  $h = id_N$
- $\mathbb{N}$  abzählbar unendlich:  $h: \mathbb{N} \to \mathbb{N}_0(x \to x 1)$  ist bijektiv.
- $\mathbb{Z}$  ist abzählbar unendlich: (Geschichte vom Teufel:  $h \to \mathbb{Z}$ 
  - $1 \to 0$
  - $2 \rightarrow 1$
  - $3 \rightarrow -1$
  - $4 \rightarrow 2$

$$\underbrace{5}_{Tag} \to \underbrace{-2}_{Zahl}$$

allgemein:

$$x \to \begin{cases} k & \text{falls } x = 2k + 1 (\text{für } k = 0, 1, 2, ...) \\ -k & \text{falls } x = 2k (\text{für } k = 1, 2, 3, ...) \end{cases}$$

• Q ist abzählbar unendlich:

$$\frac{1}{1}\frac{1}{2}\frac{1}{3}\frac{1}{4}\frac{1}{5}...$$

$$\frac{2}{1}\frac{2}{2}\frac{2}{3}\frac{2}{4}\frac{2}{5}...$$

$$\frac{3}{1}\frac{3}{2}\frac{3}{3}\frac{3}{4}\frac{3}{5}...$$
:

Cantorsches Diagonalverfahren.

- $\mathbb{R}$  ist <u>nicht</u> abzählbar unendlich! (Beweis von Cantor, 2. Diagonalisierungsargument)  $\rightarrow$  eventuell später
- $P(\mathbb{N} \text{ ist nicht abz\"{a}hlbar unendlich (allgemein: } | A | < | P(A) | Satz von Cantor.)$

## 4.16 Satz (Wichtiger Satz für endliche Mengen)

Seien  $A, B \neq \emptyset$  endliche Mengen, |A| = |B|, und  $f : A \rightarrow B$  eine Abbildung. Dann gilt f injektiv  $\Leftrightarrow f$  surjektiv  $\Leftrightarrow f$  bijektiv.

#### Beweis:

Wir setzen n: |A| = |B|. Es genügt zu zeigen f injektiv  $\Leftrightarrow f$  surjektiv.

 $\Rightarrow$  Sei f injektiv, d.h. falls  $a_1, a_2 \in A$  mit  $a_1 \neq a_2$ , dann gilt  $f(a_1) \neq f(a_2)$ .

D.h., verschiedene Elemente aus A werden auf verschiedene Elemente aus B abgebildet, die n Elemente aus A also auf n verschiedene Elemente aus B. Da B genau n Elemente besitzt, ist f surjektiv. (f(A) = B).

[formaler: d.h. 
$$| f(A) | = | A | = | B |$$
.  
Da  $f(A) \subseteq B$  endlich, folgt  $f(A) = B$ .

### 4.17 Das Prinzip der rekursiven Definition von Abbildungen

Sei  $B \neq \emptyset$  Menge,  $n_0 \in \mathbb{N}$ ,  $A = \{n \in \mathbb{N} \mid n \geq n_0\}$ .

Man kann eine Funktion  $f: A \to B$  definieren durch

- Angabe des Startwerts  $f(n_0)$
- Beschreibung, wie man für jedes  $n \in A$  den Funktionswert f(n+1) aus f(n) berechnet (Rekursionsschritt).

### 4.18 Beispiel

- a) Die Fakultätsfunktion:  $f: \mathbb{N}_0 \to \mathbb{N}$  mit f(0) = 0  $\underbrace{!}_{\text{Fakultät}} = 1$  (Startwert)  $f(n+1) = (n+1)! = n!(n+1) \text{ für alle } n \geq 0$  Also: f(1) = 1! = 0! \* 1 f(2) = 2! = 1! \* 2 = 1 \* 2 = 2 f(3) = 3! = 2! \* 3 = 1 \* 2 \* 3 f(4) = 4! = 3! \* 4 = 1 \* 2 \* 3 \* 4  $\vdots$   $f(70) = 70! \approx 1, 2 * 10^{100}$
- **b)** Potenzen: für festes  $x \in \mathbb{R}$  definiere  $x^0 = 1$   $x^{n+1} = x^n * x$  für alle  $n \ge 0$   $(Px : \mathbb{N}_0 \to \mathbb{R} \qquad n \to x^n)$
- c) Eine Pflanze verdopple jeden Tag die Anzahl ihrer Knospen und produziere eine zusätzliche.

 $f: \mathbb{N} \to \mathbb{N}$  beschreibe die Anzahl der Knospen nach n Tagen.

$$f(1) = 1$$

$$f(2) = 2 * 1 + 1 = 3$$

$$f(3) = 2 * 3 + 1 = 7$$

$$f(4) = 2 * 7 + 1 = 15$$

$$\vdots$$

$$f(n+1) = 2 * f(n) + 1$$

Wieviele Knospen gibt es nach 100 Tagen?  $\Rightarrow$  Geschlossene / explizite Form von f gefragt.

Vermutung:  $f(n) = 2^n - 1$ 

(Bemerkung: bessere Methoden (statt vermuten / raten) in der Vorlesung Algorithmen, dort z.B. auch mathematische Strukturen wie oben, diese werden  $B\ddot{a}ume$  (Graphen) genannt.

Beweis: vollständige Induktion

Induktionsanfang:

$$f(1) = 2^1 - 1 = 1$$

Induktionsschritt:

Indunktionsvorraussetzung:

sei 
$$f(n) = 2^n - 1 \forall n \ge 1$$

Induktionsbehauptung:

$$f(n+1) = 2^{n+1} - 1$$

Beweis:

$$f(n+1) = 2 * f(n) + 1$$

$$= 2(2^{n} - 1) + 1$$

$$= 2^{n+1} - 2 + 1$$

$$= 2^{n+1} - 1$$

### 4.19 Bemerkung

Die rekursive Definition kann verallgemeinert werden: benutze zur Definition von f(n+1) die vorigen  $k(k \in \mathbb{N}$  Werte von f, also  $\underbrace{f(n), f(n-1), ..., f(n-k+1)}_{\text{k Stück}}$ 

und gebe k Startwerte  $f(n_0), f(n_0 + 1), ..., f(n_0 + k - 1)$ 

# 4.20 Beispiel (Fibonacci-Zahlen)

k = 2

$$f(1) = 1$$

$$f(2) = 1$$

$$f(n+1) = f(n) + f(n+1)$$

$$(f(3) = f(2) + f(1) = 1 + 1 = 2,$$

$$f(4) = 2 + 1 = 3,$$

$$f(5) = 3 + 2 = 5,$$

$$f(6) = 8,$$

$$f(7) = 13...)$$

explizite Form:

$$f(n) = \frac{1}{\sqrt{5}} \left( \left( \frac{1 + \sqrt{5}}{2} \right)^n - \left( \frac{1 - \sqrt{5}}{2} \right)^n \right)$$

### 5 Relationen

### 5.1 Definition

Seien  $M_1, ..., M_n$ nicht leere Mengen  $(n \in \mathbb{N}).$ 

- a) Eine n-stellige Relation über  $M_1, ..., M_n$  ist eine Teilmenge von  $M_1x...xM_n$ . Ist  $M_1 = ... = M_n = M$ , d.h.  $R \supseteq M^n$ , so spricht man von einer n-stelligen Relation auf M.
- (speziell: n=2, zweistellige Relation auf M: Sei  $M \neq \emptyset$  Menge. Eine Teilmenge  $R_{\sim} \subseteq MxM$  heißt (zweistellige) Relation auf M. Statt  $(a,b) \in R_{\sim}$  (mit  $a,b \in M$ ) schreibt man kurz  $a\overline{R}_{\sim}b$  oder  $a \sim b$  (a steht in Relation zu b)

### 5.2 Beispiel

- a) Relationale Datenbanken ( $\rightarrow$  Folie)
- b)  $M = \{1, 2, 3\},$   $R_{\sim} = \{(1, 2), (1, 3), (2, 3)\}$  also:  $1 \sim 2, 1 \sim 3, 2 \sim 3$

Hierfür sind wir die Notation < gewohnt:

$$1 < 2, 1 < 3, 2 < 3$$
 (Kleiner-Relation)

Ähnlich: 
$$\geq$$
 auf  $M: R_{\geq} = \{(1,1), (2,1), (3,1), (2,2), (3,2), (3,3)\}$ 

allgemeiner: kleiner-Relation auf  $\mathbb{Z}$ :

$$\begin{array}{l} R_{<}\{(x,y) \mid x,y \in \mathbb{Z}, x < y\} \\ R_{\leq ...} \leq \end{array}$$

**c**)

Teiler-Relation R, auf  $\mathbb{Z}$ :

$$R_{|} = \{(x,y) \mid x,y \in \mathbb{Z} \text{ und } \exists k \in \mathbb{Z} \text{ mit } x \mid y \text{ } (x \text{ } teilt \text{ } y)$$

z.B. 
$$6|42$$
,  $3|-27$ ,  $7|0$ 

d) Sei M die Menge aller Menschen,  $R_m = \{(a, b) \mid a, b \in M \text{ und } a \text{ und } b \text{ haben dieselbe Mutter } \}$ 

Zwei wichtige Typen von Relationen auf einer Menge:

Ordnungsrelationen und Äquivalenzrelationen.

#### 5.3 Definition

Sei  $M \neq \emptyset, R_{\preceq}$  (oder  $\preceq) eine Relation auf <math display="inline">M$  mit folgenden Eigenschaften:

- 1.  $\forall x \in M : x \leq x \text{ (Reflexivität)}$
- 2.  $\forall x, y \in M : (x \leq y \land y \leq x) \Rightarrow x = y \text{ (Antisymmetrie)}$
- 3.  $\forall x, y, z \in M : (x \leq y \land y \leq z) \Rightarrow x \leq z$  (Transitivität)

Dann heißt  $\leq$  Ordnungsrelation oder (partielle) Ordnung auf M.

Gilt zusätzlich:

4.  $\forall x, y \in M : x \leq y$  oder  $y \leq y$ , so heißt  $\leq$  eine <u>totale</u> (oder <u>vollständige</u>, oder lineare) Ordnung.