User: diskrete
PW: fun

Vorlesung Diskrete Strukturen

1. Logik

Ziel: Sachverhalte sollen (mathematisch) exakt formuliert werden. Dazu sind Gedanken zu

- Aussagen
- Beweisen
- Mengen (später)

notwendig.

Die Logik entwickelte sich aus der Philosophie und wurde und ist heute die Grundlage aller Wissenschaften.

Die moderne Logik entwickelte sich durch G. Frege (1879, „Begriffsschrift"), A. Whitehead u. B. Russell (1910, „Principia Mathematica") und D. Hilbert (1920er, Hilbertprogramm, Widerspruchsfreiheit der Axiomensysteme der Mathematik) zu einem der wichtigsten Werkzeuge der Informatik

Es wird (streng) der deduktiven Methode, Schlussfolgerungen von gegebenen Prämissen auf zwingende Konsequenzen (Konklusion), gefolgt (vgl. Wissenschaftstheorie u. Erkenntnisgewinn).

1.1. Definitionen

Definition: Eine Aussage ist ein Satz, der entweder wahr oder falsch ist, aber nie beides gleichzeitig.

Eine wahre Aussage hat den Wahrheitswert w (oder „1" / „true") und falsche Aussagen f (oder „0" / „false").

Beispiele:

- Wiesbaden liegt in Hessen (w)
- 11 ist eine Primzahl (w)
- $\sqrt{2}$ kann durch einen (gekürzten) Bruch dargestellt werden (später)
- Ein Barbier ist einer, der genau alle die rasiert, die sich nicht selbst rasieren. (?)

Das letzte Beispiel ist bekannt als Russell-Paradoxon und hat 1918 eine Grundlagenkrise in der Mathematik ausgelöst.

Aussagen können auch verknüpft werden:

- 11 ist eine Primzahl und Wiesbaden liegt am Rhein

Dies ergibt wieder eine Aussage

Idee: Repräsentiere Aussagen durch Aussagenvariablen, die einen Wahrheitswert haben.

Bem: Die umgangssprachlichen Verknüpfungen „und", „oder", „nicht", „wenn ..., dann ..." und entweder oder können nun präzise aufgeschrieben werden.

Umgangssprache	Name i. d. Logik	Symbol
und	Konjunktion	$\wedge$
oder	Disjunktion	$\vee$
nicht	Negation	$\neg$
wenn ..., dann ...	Implikation	$\rightarrow$
entweder ..., oder	Kontravalenz	$\oplus$
genau dann wenn	Äquivalenz	$\leftrightarrow$

Def: Seien x und y Aussagenvariablen für zwei Aussagen, dann gilt

"Junktoren"

x	y	$(x \wedge y)$
0	0	0
0	1	0
1	0	0
1	1	1

"Konjunktion"

x	y	$(x \vee y)$
0	0	0
0	1	1
1	0	1
1	1	1

"Disjunktion"

x	y	$(x \to y)$
0	0	1
0	1	1
1	0	0
1	1	1

"Implikation"

x	y	$(x \oplus y)$
0	0	0
0	1	1
1	0	1
1	1	0

"Kontravalenz"

x	y	$(x \leftrightarrow y)$
0	0	1
0	1	0
1	0	0
1	1	1

"Äquivalenz"

x	$\neg x$
0	1
1	0

"Negation"

Bem: Schreibt man alle Kombinationen von Wahrheitswerten auf, um den Wahrheitswert einer zusammengesetzten Aussage fest zu legen, so spricht man von Wahrheitswertetabelle (Wahrheitswertetafel).

Bem: In der Umgangssprache wird die Kontravalenz oft mit der Disjunktion verwechselt.

Def: Einen „Verknüpfer" von Aussagen nennt man auch Junktor.

Mit Wahrheitswertetabellen können auch kompliziertere Aussagen überprüft werden:

Bsp: Seien x und y Aussagevariablen, dann ist die Aussage $(x \to y) \wedge (y \to x)$ gleichwertig zu $(x \leftrightarrow y)$.

x	y	$(x \to y)$	$(y \to x)$	$(x \to y) \wedge (y \to x)$	$x \leftrightarrow y$
0	0	1	1	1	1
0	1	1	0	0	0
1	0	0	1	0	0
1	1	1	1	1	1

Def: Eine Verknüpfung von Aussagenvariablen mit Junktoren heißt (aussagenlogische) Formel.

Bem: Jede Zeile einer Wahrheitswertetabelle enthält eine Belegung der Wahrheitswertevariablen mit Wahrheitswerten.

Eine Wahrheitswertetabelle enthält alle möglichen Kombinationen von Belegungen der Wahrheitswertevariablen.

Def: Eine Formel heißt Tautologie, wenn sie für jede Belegung wahr ist.

Eine Formel die nie wahr ist heißt Kontradiktion.

Bsp:

x	y	$(x \wedge y)$	$(x \wedge y) \to x$ (Tautologie)	$\neg(x \vee y)$	$\neg x$	$\neg(x \vee y) \to \neg x$ (Tautologie)
0	0	0	1	1	1	1
0	1	0	1	0	1	1
1	0	0	1	0	0	1
1	1	1	1	0	0	1

x	y	$\neg(x \wedge y)$	$\neg x$	$(x \wedge y) \wedge \neg x$ (Kontradiktion)
0	0	1	1	0
0	1	1	1	0
1	0	1	0	0
1	1	0	0	0

Def: Zwei Formeln H_1 und H_2 heißen logisch äquivalent (Schreibweise: $H_1 \equiv H_2$) genau dann, wenn $(H_1 \leftrightarrow H_2)$ eine Tautologie ist.

Bem: Mit dieser Definition haben zwei logisch äquivalente Formeln die gleiche Wahrheitswertetabelle.

Bem: Mit der Definition der logischen Äquivalenz kann man in einer Formel eine Teilformel ersetzen und erhält eine neue logisch äquivalente Formel

⇒ Aussagenlogische Formeln können umgeformt / vereinfacht werden

Umformungsregeln:

$$\left.\begin{aligned}(X \wedge y) &\equiv (y \wedge X)\\ (X \vee y) &\equiv (y \vee X)\end{aligned}\right\} \text{Kommutativität}$$

$$\left.\begin{aligned}(x \wedge (y \wedge z)) &\equiv ((x \wedge y) \wedge z)\\ (x \vee (y \vee z)) &\equiv ((x \vee y) \vee z)\end{aligned}\right\} \text{Assoziativität}$$

$$\left.\begin{aligned}(x \wedge (y \vee z)) &\equiv ((x \wedge y) \vee (x \wedge z))\\ (x \vee (y \wedge z)) &\equiv ((x \vee y) \wedge (x \vee z))\end{aligned}\right\} \text{Distributivität}$$

$$\left.\begin{aligned}x \wedge x &\equiv x\\ x \vee x &\equiv x\end{aligned}\right\} \text{Idempotenz}$$

$$\left.\neg\neg x \equiv x\right\} \text{Doppelte Negation}$$

$$\left.\begin{aligned}\neg(x \vee y) &\equiv \neg x \wedge \neg y\\ \neg(x \wedge y) &\equiv \neg x \vee \neg y\end{aligned}\right\} \text{De Morgans Regeln}$$

Sei H eine Tautologie, dann

$$(X \wedge H) \equiv X$$
$$(X \vee H) \equiv H$$

Wenn H' eine Kontradiktion ist, dann

$$(X \vee H') \equiv X$$
$$(X \wedge H') \equiv H'$$

Bsp: $\neg(\neg X \wedge y) \wedge (X \vee y)$

$\equiv (\neg(\neg x) \vee \neg y) \wedge (x \vee y)$ „De Morgan"

$\equiv (x \vee \neg y) \wedge (x \vee y)$ „doppelte Negation"

$\equiv (x \wedge x) \vee (x \wedge y) \vee (\neg y \wedge x) \vee (\neg y \wedge y)$ „Distributivität"

$\equiv x \vee (x \wedge y) \vee (\neg y \wedge x) \vee (\underbrace{\neg y \wedge y}_{\text{Kontradiktion}})$ „Idempotenz"

$\equiv x \vee (x \wedge y) \vee (\neg y \wedge x)$ „Kontradiktionsregel"

$\equiv x \vee (x \wedge (\underbrace{y \vee \neg y}_{\text{Tautologie}}))$ „Tautologieregel"

$\equiv x \vee x$ „Idempotenz"

$\equiv x$

1.2. Aussageformen und Quantoren

Bis jetzt hatten wir nur Aussagen über konkrete Objekte nun sollen diese Objekte durch Variablen ersetzt werden.

Aussage: „5 ist eine Primzahl"

Aussageform: $p(x)$: „x ist eine Primzahl"

$\Rightarrow$ $p(5)$ ist wahr und $p(4)$ ist falsch.

Die (freien) Variablen einer Aussageform können mit bel. Werten aus dem <u>Universum</u> belegt werden.

$\Rightarrow$ das Universum von $p(x)$ ist $\mathbb{N}$

Für $q(x)$: „x blüht rot" könnte das Universum die Menge aller Blumen sein.

<u>Def:</u> Eine <u>Aussageform</u> über den Universen $U_1, \dots, U_n$ ist ein Satz mit den Variablen $x_1, \dots, x_n$, der zu einer Aussage wird, wenn x_i mit einem Wert aus U_i belegt wird.

1.3 Quantoren

<u>Ziel:</u> Es soll ausgedrückt werden, dass eine Aussageform für alle Elemente (mindestens eines) eines Universums wahr wird.

<u>Def:</u> Sei $p(x)$ eine Aussageform über dem Universum U. $\exists x\, p(x)$ bezeichnet die Aussage „Es gibt ein $u \in U$, so dass $p(u)$ wahr ist"

$\forall x\, p(x)$ bezeichnet „Für alle $u \in U$ gilt $p(u)$"

Bem: Die Symbole $\exists$ und $\forall$ heißen Quantoren.. „$\exists$" ist der Existenzquantor und „$\forall$" heißt Allquantor.

Bsp: • Sei $p(x)$ die Aussageform $(x \leq x+1)$ über dem Universum $\mathbb{N}$, dann ist

- $\forall x\, p(x)$ wahr
- $\exists x\, p(x)$ wahr

• Sei $q(x)$ die Aussageform (x ist eine Primzahl), dann ist

- $\forall x\, q(x)$ falsch
- $\exists x\, q(x)$ wahr

Bem: Ist das Universum $U = \{u_1, \dots, u_n\}$ endlich, dann gilt

$$\exists x\, p(x) \equiv p(u_1) \vee p(u_2) \vee \dots \vee p(u_n) \quad \text{und}$$

$$\forall x\, p(x) \equiv p(u_1) \wedge p(u_2) \wedge \dots \wedge p(u_n).$$

Umformungsregeln:

$$\left.\begin{aligned} \neg \forall x\, p(x) &\equiv \exists x\, (\neg p(x)) \\ \neg \exists x\, p(x) &\equiv \forall x\, (\neg p(x)) \end{aligned}\right\} \text{ Negationsregeln}$$

Ausklammerregeln:

$$\begin{aligned} (\forall x\, p(x)) \wedge (\forall x\, q(x)) &\equiv \forall x\, (p(x) \wedge q(x)) \\ (\exists x\, p(x)) \vee (\exists x\, q(x)) &\equiv \exists x\, (p(x) \vee q(x)) \end{aligned}$$

$$\begin{aligned} \forall x \forall y\, p(x,y) &\equiv \forall y \forall x\, p(x,y) \\ \exists x \exists y\, p(x,y) &\equiv \exists y \exists x\, p(x,y) \end{aligned}$$

2. Mengen und Mengenoperationen

Der intuitive Mengenbegriff ist mathematisch extrem schwer / unmöglich zu definieren.
Für uns reicht die folgende Beschreibung:

Erklärung (Georg Cantor, 1895):

Eine Menge ist die Zusammenfassung bestimmter, wohlunterschiedener Objekte unserer Anschauung oder unseres Denkens, wobei eindeutig feststeht, ob ein Objekt zu einer Menge gehört oder nicht.
Die Objekte der Menge heißen Elemente.

Bem:
- Wir beschäftigen uns nur mit Mengen, die eindeutig und ohne Widersprüche definiert werden können.
- Mengen werden immer mit Großbuchstaben bezeichnet und Objekte mit Kleinbuchstaben.
- Ist a ein Element der Menge M, so schreiben wir $a \in M$, sonst $a \notin M$.

Def: Die Anzahl der Elemente in einer Menge M heißt **Mächtigkeit** oder **Kardinalität** von M (Schreibweise: $\#M$)
Ist $\#M$ endlich, so heißt M **endliche Menge**, sonst **unendliche Menge**.

Bem:
- Eine Menge enthält jedes Element maximal einmal: $\{I, N, F, O, R, M, A, T, K\}$
- Die Reihenfolge spielt keine Rolle: $\{I, N, F, O, R, M, A, T, K\} = \{A, F, I, K, M, N, O, R, T\}$

Bsp:
i) $M = \{1, 2, 3, 4, 5\}$ und $\#M = 5$
ii) $N = \{\square, \diamond, \triangle\}$ und $\#N = 3$

Bem: Manchmal ist es schwer / unmöglich eine Menge durch aufzählen zu beschreiben.
$\Rightarrow$ verwende eine geeignete Aussageform zur Beschreibung.

Bsp:
- $p(x)$: x ist größer als 10
  $M = \{x \in \mathbb{N} \mid p(x)\}$
- $N = \{x \in \mathbb{N} \mid 0 < x < 3\}$

Def: Zwei Mengen A und B sind gleich (Schreibweise: $A = B$), wenn jedes Element von A auch eines von B ist und umgekehrt. (Schreibweise: $A = B$).
Ist A nicht gleich B, so schreibt man $A \neq B$.

Bem: Gilt für zwei Aussageformen $q(x)$ und $q'(x)$, dass $q(x) \equiv q'(x)$ über dem Universum $\mathcal{U}$, dann $\{x \in \mathcal{U} \mid q(x)\} = \{x \in \mathcal{U} \mid q'(x)\}$.

Bsp: $p(x)$: „die Quersumme von x ist ein Vielfaches von 3"
$q(x)$: „x ist ohne Rest durch 3 teilbar"

$\{x \in \mathbb{N} \mid p(x)\} = \{x \in \mathbb{N} \mid q(x)\}$

Def: Sei $\mathcal{U}$ ein Universum, $p(x)$ eine Aussageform über $\mathcal{U}$ und $M = \{x \in \mathcal{U} \mid p(x)\}$.
Dann heißt $\overline{M} =_{def} \{x \in \mathcal{U} \mid \neg p(x)\}$ Komplement von M.

Bsp: Sei $p(x)$: x gerade und $M = \{x \in \mathbb{N} \mid p(x)\}$, dann ist $\overline{M}$ die Menge der ungeraden Zahlen.

Def: Sei $p(x) : x \neq x$ über einem beliebigen Universum $\mathcal{U}$, dann heißt

$$\emptyset_{\mathcal{U}} =_{def} \{x \in \mathcal{U} \mid p(x)\} = \{x \in \mathcal{U} \mid x \neq x\}$$

die leere Menge (in $\mathcal{U}$).

Bem: Die Konstruktion der leeren Menge ist unabhängig vom Universum $\mathcal{U}$.

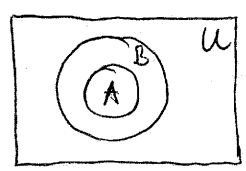
Es gilt sogar $\emptyset_{\mathcal{U}} = \emptyset_{\mathcal{U}'}$ für zwei unterschiedliche Universen $\mathcal{U}$ und $\mathcal{U}'$, denn für jedes Element (also keines) aus $\emptyset_{\mathcal{U}}$ ist in $\emptyset_{\mathcal{U}'}$ und umgekehrt.

$\Rightarrow$ ab jetzt reden wir von der leeren Menge.

Def: Seien A und B Mengen, dann heißt A Teilmenge von B (Schreibweise: $A \subseteq B$), wenn alle Elemente von A auch in B enthalten sind. Statt $A \subseteq B \wedge A \neq B$ schreiben wir $A \subset B$ (echte Teilmenge).

Bem:

- $(A \subseteq B)$ gdw $(\forall x \; x \in A \to x \in B)$
- $A = B$ gdw $(\forall x \; ((x \in A \to x \in B) \wedge (x \in B \to x \in A)))$
- graphisch:



„Venn-Diagramm"

2.1. Operationen auf Mengen

Def: Sei M eine Menge, dann heißt

$$\mathcal{P}(M) =_{def} \{ N \mid N \subseteq M \}$$

die Potenzmenge von M.

Bsp:

- für alle Mengen M gilt $\emptyset \in \mathcal{P}(M)$
- $\mathcal{P}(\{1,2\}) = \{ \emptyset, \{1\}, \{2\}, \{1,2\} \}$
- $\mathcal{P}(\{a,b,c\}) = \{ \emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\} \}$

Def: Sei M eine Menge und $A, B \in \mathcal{P}(M)$, dann heißt

$$(A,B) =_{def} \{ N \in \mathcal{P}(M) \mid A \subset N \subset B \}$$

(offenes) Intervall zwischen A und B. Weiterhin

$\langle A,B \rangle =_{def} \{ N \in \mathcal{P}(M) \mid A \subseteq N \subseteq B \}$ abgeschlossenes,

$\langle A,B) =_{def} \{ N \in \mathcal{P}(M) \mid A \subseteq N \subset B \}$ links und

$(A,B \rangle =_{def} \{ N \in \mathcal{P}(M) \mid A \subset N \subseteq B \}$ rechts

abgeschlossenes Intervall.

Def: Seien $A = \{x \in \mathcal{U} \mid p(x)\}$ und $B = \{x \in \mathcal{U} \mid q(x)\}$ mit Aussageformen $p(x)$ bzw $q(x)$, dann ist

- $A \cap B =_{def} \{x \in \mathcal{U} \mid p(x) \wedge q(x)\}$ „Schnitt"
- $A \cup B =_{def} \{x \in \mathcal{U} \mid p(x) \vee q(x)\}$ „Vereinigung"
- $\bar{A} =_{def} \{x \in \mathcal{U} \mid \neg p(x)\}$ „Komplement"
- $A \setminus B =_{def} \{x \in \mathcal{U} \mid p(x) \wedge \neg q(x)\}$

Bem: Mit dieser Definition gelten für $\cup, \cap, \bar{}$ die Regeln der Aussagenlogik, d.h. etwa $\overline{(A \cap B)} = \bar{A} \cup \bar{B}$ (de Morgan)

Def: Seien A und B Mengen, dann heißt

$A \times B =_{def} \{(a,b) \mid a \in A, b \in B\}$

Kreuzprodukt (kartesisches Produkt) von A und B.

Bem:

- $M \times \emptyset = \emptyset = \emptyset \times M$
- $A = \{a,b\}$ und $B = \{1,2\}$, dann $A \times B = \{(a,1), (a,2), (b,1), (b,2)\}$
- $I = \{x \in \mathbb{R} \mid 0 \leq x \leq 5\}$ und $J = \{x \in \mathbb{R} \mid 0 \leq y \leq 1\}$, dann ist $I \times J$ ein Rechteck der euklidischen Ebene.

- Statt $N = \underbrace{M \times M \times \dots \times M}_{t\text{-mal}}$ schreiben wir kurz M^t, die Elemente von N werden t-Tupel genannt.
- $M^* =_{df} \bigcup_{0 \leq i} M^i$

3. Mathematisches Beweisen

Ein mathematischer Beweis dient verschiedenen Zwecken

- ermöglicht die vollständige Überprüfung von Sachverhalten und Ideen
- hilft Kritik und Irrtümer auszuräumen
- ermöglicht die selbständige Einarbeitung in neue Wissensgebiete
- dient der Gewinnung von neuem Wissen

Beispiel: Sei $p \geq 5$ eine Primzahl, dann teilt 24 die Zahl $p^2 - 1$ ohne Rest.

Probieren: $p = 5 \Rightarrow 25 - 1$ ist durch 24 teilbar
$p = 7 \Rightarrow 49 - 1$ ——"——
$p = 11 \Rightarrow 121 - 1$ ——"——

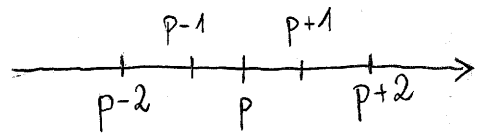
Überprüfung mit einem Rechner liefert immer korrektes Ergebnis

Aber:
- Ist das immer so?
- ⇒ Nichts gelernt!
- Status unklar

Suchen einen Beweis:

Wir wissen $p^2-1 = (p-1)(p+1)$ „Binomische Formel"

Da p eine ungerade Primzahl ist, sind $(p-1)$ und $(q-1)$ gerade. $(p \geq 5)$



Jede dritte Zahl ist durch 3 teilbar, d.h. entweder $p-1$ oder $p+1$ durch 3 teilbar, da p nicht durch 3 teilbar ist (Primzahl, $p \geq 5$).

Von zwei geraden Zahlen, die aufeinander folgen ist eine sogar durch 4 teilbar.

D.h. 2, 3 und 4 teilen p^2-1 und damit auch $2 \cdot 3 \cdot 4 = 24$ teilt p^2-1. #

Ein Beweis startet mit früheren Ergebnissen, Definitionen und einfachen gültigen Tatsachen, den Axiomen ($\hat{=}$ Fundament)

Bsp: Axiome der natürlichen Zahlen nach G. Peano

i) 0 ist eine natürliche Zahl

ii) Jede natürliche Zahl n hat einen Nachfolger $s(n)$

iii) Aus $s(n) = s(m)$ folgt $n = m$

iv) 0 ist nicht Nachfolger einer natürlichen Zahl

v) Jede Menge, die die 0 enthält und die für jedes n auch $s(n)$ enthält, umfasst alle natürlichen Zahlen

Bem: Zu beweisende Tatsachen werden oft Satz oder Theorem genannt.
Sachverhalte die man nur im Kontext eines Satzes verwendet nennt man Lemma oder Hilfssatz. Kleine Folgerungen aus einem Satz bezeichnet man mit Korollar.

3.1. Der direkte Beweis

Mathematische Aussagen haben oft die Form „Wenn p, dann q". Dabei heißt p Hypothese (Prämisse) und q Konklusion (Konsequenz).

Ziel: Beginnend bei der Hypothese wird in (kleinen) Schritten die Wahrheit von „Zwischenaussagen" belegt. Am Ende der Kette steht die Konsequenz.

Beispiel:

Satz: Wenn eine Zahl $a \in \mathbb{N}$ (Prämisse: ohne Rest durch 6 teilbar ist), (Konsequenz: „ist a gerade").

Beweis:

Wenn a ohne Rest durch 6 teilbar ist, dann gibt es ein $k \in \mathbb{N}$ mit $a = 6k$.

Also $a = 2 \cdot \underbrace{3 \cdot k}_{=k'} = 2 \cdot k'$.

D.h. a ist ohne Rest durch 2 teilbar, also gerade. #

3.2. Beweis durch Kontraposition

Wir wissen: $p \to q \equiv \neg q \to \neg p$

Manchmal ist es einfacher aus $\neg q$ die Folgerung $\neg p$ abzuleiten, als aus p die Konklusion q.

Beispiel:

Satz: Wenn $\overbrace{a^2 \in \mathbb{N} \text{ ungerade}}^{\triangleq p}$, dann ist $\underbrace{a \text{ ungerade}}_{\triangleq q}$.

Beweis:

Also zeigen wir:

Wenn a nicht ungerade, dann ist a^2 nicht ungerade.

Gleichwertig: Wenn a gerade, dann ist a^2 gerade.

Wenn a gerade, dann ex. ein $k \in \mathbb{N}$ mit $a = 2k$, also $a^2 = 4k^2 = 2 \cdot (2k^2)$, d.h. auch a^2 ist gerade. #

3.3. Beweis durch Widerspruch

Soll $p \to q$ gezeigt werden, so kann man auch wie folgt vorgehen:

i, Annahme: Die Hypothese p ist erfüllt und $\neg q$ ist richtig.

ii, ausgehend von $p \wedge \neg q$ zeigen wir einen Widerspruch, d.h. $(p \wedge \neg q) \to$ false.

iii, Wenn $(p \wedge \neg q) \to$ false wahr ist, muß $(p \wedge \neg q)$ falsch sein, was zeigt, dass $\neg q$ falsch ist, denn p ist ja wahr.

iv, da $\neg q$ falsch ist, muß q richtig sein.

Bsp:

Satz: Seien $a, b \in \mathbb{N}$ gerade, dann ist auch $a \cdot b$ gerade

Beweis: Angenommen $a \cdot b$ ist ungerade und a bzw b gerade. Dann gibt es ein k, so dass $a = 2k$ ist, also ist $a \cdot b = 2k \cdot b$ gerade. Aber $a \cdot b$ kann nicht gerade und ungerade sein $\Rightarrow$ Widerspruch, also $a \cdot b$ gerade #

3.4. Äquivalenzen

Oft sollen Aussagen der Form $p \to q$ („wenn p, dann q") gezeigt werden.

Allerdings treten auch oft Aussagen $p \leftrightarrow q$ („p genau dann, wenn q", kurz: p gdw q)

Wir machen uns die Äquivalenz $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$ zu Nutze:

Satz: Sei $a \in \mathbb{N}$. Die Zahl a ist gerade ($\hat{=} p$) genau dann, wenn a^2 gerade ($\hat{=} q$).

Beweis:

„$\Rightarrow$": Entspricht $p \to q$

Wenn a gerade, dann ex. (existiert) ein k, so dass $a = 2k$. Also $a^2 = (2k)^2 = 4k^2 = 2 \cdot (2k^2)$, d.h. auch a^2 ist gerade.

„$\Leftarrow$": Entspricht $q \to p$.

Es gilt $a^2 = a \cdot a$ ist gerade. Angenommen a wäre ungerade, dann gäbe es ein $k \in \mathbb{N}$, so dass $a = 2k+1$.
Also $a^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2+2k) + 1$.
D.h. a^2 ungerade. Widerspruch. Also a gerade #

3.5 Die Fallunterscheidung

Da $(q \to p) \wedge (\neg q \to p) \equiv (\neg q \vee p) \wedge (\neg\neg q \vee p)$

$\equiv (\neg q \wedge \neg\neg q) \vee p$

$\equiv p$ gilt, kann man eine Aussage p beweisen, indem man die Fälle q und $\neg q$ getrennt analysiert.

Satz: Sei $a \in \mathbb{N}$, dann entsteht bei dem Teilen von a^2 durch 4 entweder der Rest 1 oder 0.

Beweis: Hier ist $q \triangleq$ „a ist gerade"

Fall a gerade: Wenn a gerade ex. ein $k \in \mathbb{N}$, so dass $a = 2k$, also gilt $a^2 = 4k^2$, d.h. a^2 ist ein Vielfaches von 4 und damit bleibt der Rest 0 bei der Division durch 4.

Fall a ungerade: Wenn a ungerade ist, dann gilt $a = 2k+1$, $k \in \mathbb{N}$.

Also $a^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4(k^2+k)+1$.

Bei der Division von $4(k^2+k)+1$ durch 4 bleibt der Rest 1.

#

3.6 Das Taubenschlagprinzip

Das Taubenschlagprinzip von Dirichlet ist auch als Schubfachschluß bekannt und beruht auf einem simplen Abzählargument:

Dirichlets Taubenschlagprinzip

Halten sich $k+1$ Tauben in k Taubenschlägen auf, so gibt es mindestens einen Taubenschlag in dem zwei Tauben sitzen.

Dies kann man auch verallgemeinern:

Verallgemeinertes Taubenschlagprinzip

Werden n Tauben auf k Taubenschläge verteilt und ist $n > k$, dann gibt es mindestens einen Taubenschlag in dem $\lceil \frac{n}{k} \rceil$ Tauben sitzen.

Satz: In einer Gruppe von mindestens acht Leuten haben mindestens zwei am gleichen Wochentag Geburtstag.

Beweis: Da es nur sieben Wochentage gibt, müssen mindestens acht Leute in sieben Kategorien aufgeteilt werden. Damit gibt es mit dem Tauben-

Schlagprinzip mindestens einen Wochentag der zwei (oder mehr) Personen enthält. #

Satz: Sei $A \subseteq \mathbb{N}$ mit $\#A = 3$, dann gibt es in A stets zwei Zahlen, deren Summe gerade ist.

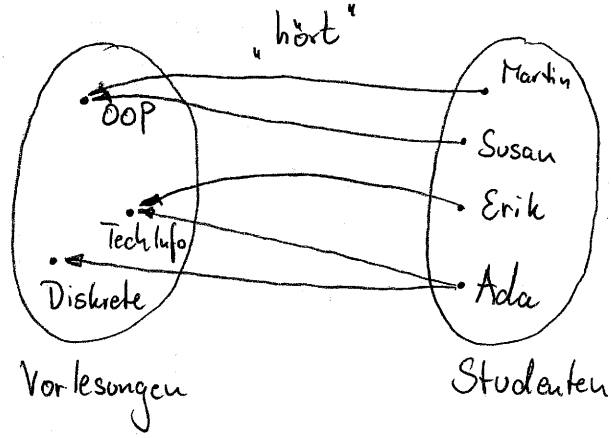
Beweis: Die Summe von zwei natürlichen Zahlen ist genau dann gerade, wenn entweder beide Zahlen gerade oder beide Zahlen ungerade sind (*).

Werden die Elemente von A den zwei Kategorien „gerade" / „ungerade" zugeordnet, so gibt es eine Kategorie die zwei Zahlen enthält (zwei gerade oder zwei ungerade).
Mit obiger Beobachtung (*) ergibt sich die Aussage. #

wir gehen davon aus, dass dies „klar" ist.

4. Relationen und Funktionen

Die Elemente von zwei Mengen stehen oft in einer Beziehung zueinander:



Um solche Beziehungen zu modelliert soll der Begriff der Relation eingeführt werden:

Bsp: $A = \{$ Martin, Ada, Charles $\}$ und $B = \{$ C++, Java, Ruby $\}$

Fakten: i) Martin beherrscht C++ und Java
ii) Ada und Charles sind Rubyprogrammierer

Die Relation, welche Mitarbeiter welche Programmiersprache beherrscht ist z.B. für die Personalabteilung und die Arbeitsplanung wichtig.

Wir kürzen sie durch R ab.

D.h. Martin R C++, Martin R Java, Ada R Ruby und Charles R Ruby, aber auch z.B. Ada ($\not R$) Java.

Kurzschreibweise: $R = \{$(Martin, C++), (Martin, Java), (Ada, Ruby), (Charles, Ruby)$\} \subseteq A \times B$

Def: Seien A und B beliebige Mengen. Eine (binäre) Relation R zwischen A und B ist eine Teilmenge $R \subseteq A \times B$.

Statt $(x,y) \in R$ schreibt man $R(x,y)$ oder xRy.
Sprechweise: x steht in Relation R zu y.
$(x,y) \notin R$ wird mit $x \not R y$ bezeichnet.

Bem: Sei $n \geq 1$, $A_1, \dots, A_n$ beliebige Mengen, dann heißt $R \subseteq A_1 \times A_2 \times \dots \times A_n$ n-stellige Relation.

Bsp: Sei A eine Menge, dann heißt

i) $R = A \times A$ Allrelation

ii) $R = \emptyset$ Nullrelation

iii) $R = \{(x,x) \mid x \in A\}$ Gleichheitsrelation

Bsp: Sei A die Menge alle Zeichenketten (Strings) der Länge 5 über dem binären Alphabet $\Sigma = \{a, b\}$

$R = \{(s,t) \mid$ der Anfangsbuchstabe von s und t ist gleich$\}$

D.h. xRx, $xyRxyy$, ...

Bsp: Sei A die Menge aller Länder der Erde, dann enthält die Relation „haben eine gemeinsame Grenze" z.B. $\{$(Deutschland, Polen), (Frankreich, Spanien), (Österreich, Italien)$\} \subseteq R$, aber (Spanien, Polen) $\notin R$

Bsp: Sei $R = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \mid a-b$ gerade$\}$

$1R3$, $1R5$ und $5R3$ aber z.B. $2(\neg R)3$

Bsp: Sei $R = \{(a,b) \in (\mathbb{Z} \setminus \{0\}) \times \mathbb{Z} \mid a$ teilt b ohne Rest$\}$

Statt aRb schreibt man $a \mid b$ (Sprechweise: a teilt b). Für $a(\neg R)b$ ist $a \nmid b$ üblich.

Bem: Relationen sind die Grundlage von (relationalen) Datenbanken.

4.1. Operationen auf Relationen

Def: Seien R und S Relationen, dann gilt $R = S$ (bzw. $R \subseteq S$), wenn R und S als Mengen gleich (bzw. R Teilmenge von S) ist.

Seien nun $S, R \subseteq A \times B$ zwei Relationen über den Mengen A und B, dann

- $x (\neg R)\, y$ gdw $(x,y) \notin R$
- $x (R \cup S)\, y$ gdw $x R y$ odw $x S y$
- $x (R \cap S)\, y$ gdw $x R y$ und $x S y$

Def: Sei $R \subseteq A \times B$ eine Relation zwischen A und B, dann heißt

$$R^{-1} = \{ (y,x) \in B \times A \mid (x,y) \in R \}$$

Umkehrrelation (von R).

Bsp: Sei $R = \{ (x,y) \in \mathbb{Z} \times \mathbb{N} \mid x^2 = y \}$, dann ist $R^{-1} = \{ (y,x) \in \mathbb{N} \times \mathbb{Z} \mid y = x^2 \}$

Def: Sei R eine Relation zwischen A und B, und S eine Relation zwischen C und D, dann heißt

$$R \otimes S = \{ ((a,c),(b,d)) \in (A \times C) \times (B \times D) \mid aRb \text{ und } cSd \}$$

inneres Produkt von R und S.

Sei T eine Relation zwischen B und C, dann heißt

$$R \circ T = \{ (a,c) \in A \times C \mid \exists b \in B \text{ mit } aRb \text{ und } bTc \}$$

Komposition von S und T.

Bsp: Sei $\Sigma = \{a, b, c, \dots, z\}$ die Menge aller Kleinbuchstaben und

$R = \{ (\alpha, \beta) \in \Sigma \times \Sigma \mid$ der Kleinbuchstabe α kommt im Alphabet vor $\beta \}$

$$R \otimes R = \{ ((\underbrace{\alpha, \gamma}_{\triangleq \text{„String“ der Länge 2}}), (\beta, \delta)) \in \Sigma^2 \times \Sigma^2 \mid \alpha R \beta \text{ und } \gamma R \delta \}$$

„Anordnung von Strings“

Bsp: Seien $x, y \in \mathbb{Z}$, dann schreiben wir $x \mid y$ (Sprechweise: x teilt y (ohne Rest)), wenn ein c existiert, sodass $y = c \cdot x$, d.h. y ist ein Vielfaches von x.

$$R = \{(x,y) \in \mathbb{Z}^2 \mid x \mid y\}$$

$$S = \{(y,z) \in \mathbb{Z}^2 \mid 2 \mid (y+z)\}$$

$$R \circ S = \{(x,z) \in \mathbb{Z}^2 \mid \exists y \; x \mid y \wedge 2 \mid (y+z)\}$$

$$= \underbrace{\{(x,z) \in \mathbb{Z}^2 \mid x \text{ ungerade oder } z \text{ gerade}\}}$$

Warum? $\Rightarrow$ selber rausbekommen!

4.2. Eigenschaften von Relation

Def: Sei R eine (binäre) Relation über A, dann heißt

i) R reflexiv, falls $\forall a \in A$ gilt aRa.

ii) R symmetrisch, falls $\forall a,b \in A$ aus aRb stets bRa folgt.

iii) R antisymmetrisch, falls $\forall a,b \in A$ aus $aRb \wedge bRa$ stets $a=b$ folgt.

iv) R transitiv, falls $\forall a,b,c \in A$ aus $aRb \wedge bRc$ stets aRc folgt.

Bsp: Sei $R = \{(x,y) \in \mathbb{R}^2 \mid x = y\}$.

R ist reflexiv, symmetrisch, antisymmetrisch und transitiv.

Bsp: Sei $T = \{(x,y) \in \mathbb{N} \mid x|y\}$

T ist reflexiv, antisymmetrisch und transitiv.

Bsp: Sei $\leq = \{(x,y) \in \mathbb{Z} \mid x \leq y\}$

$\leq$ ist reflexiv, antisymmetrisch und transitiv.

Satz: Eine Relation R ist genau dann symmetrisch, wenn $R^{-1} \subseteq R$. Es gilt dann sogar $R = R^{-1}$.

Beweis:

„$\Rightarrow$" Wenn R symmetrisch ist folgt aus aRb stets bRa.

Aus der Def. der Umkehrrelation folgt die Gleichwertigkeit von aRb und $bR^{-1}a$.

Sei $(b,a) \in R^{-1}$, d.h. aRb und damit $(a,b) \in R$ sowie $(b,a) \in R$ und $R^{-1} \subseteq R$. $= aRb$

„$\Leftarrow$" Gilt $R^{-1} \subseteq R$, dann ist $bR^{-1}a$ und bRa. D.h. aus aRb folgt bRa.

Da eine Relation R genau dann symmetrisch ist, wenn R^{-1} symmetrisch ist (vgl. Definition), ergibt sich $R = (R^{-1})^{-1} \subseteq R^{-1}$, d.h. $R \subseteq R^{-1}$ und $R^{-1} \subseteq R$.
Zusammen $R = R^{-1}$. #

Def: Sei R eine binäre Relation, die reflexiv, symmetrisch und transitiv ist. Dann heißt R Äquivalenzrelation.

Bsp: Sei A = „Menge aller Waren eines Supermarkts"
$R = \{(x,y) \in A \times A \mid x$ hat den gleichen Preis wie $y\}$

⇒ R ist eine Äquivalenzrelation

Bsp: Sei B = „Menge aller Menschen"
$S = \{(x,y) \in B \times B \mid x$ ist Freund $y\}$

⇒ S ist eine Äquivalenzrelation

Bsp: Sei $L = \{H \mid H$ ist aussagenlogische Formel$\}$
$\equiv = \{(H_1, H_2) \mid H_1$ ist logisch äquivalent $H_2\}$
⇒ $\equiv$ ist eine Äquivalenzrelation

Bsp: Sei $B = \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ und $\sim \subseteq \{((a,b),(c,d)) \in B^2 \mid a \cdot d = b \cdot c\}$, dann ist $\sim$ eine Äquivalenzrelation

reflexiv: $(a,b) \sim (a,b)$, da $a \cdot b = b \cdot a$

symmetrisch: $(a,b) \sim (c,d)$, dann $a \cdot d = b \cdot c$

$\Rightarrow c \cdot b = d \cdot a$

$\Rightarrow (c,d) = (a,b)$

transitiv: $(a,b) \sim (c,d)$ und $(c,d) \sim (e,f)$, dann $ad = bc$ und $cf = de$. Also gilt $adf = bcf$ und einsetzen ergibt $adf = bde$, damit $af = be$. D.h. $(a,b) \sim (e,f)$

$\Rightarrow$ „Bruchrechnen"

Def: Sei $\sim$ eine Äquivalenzrelation über A und $a \in A$. Dann heißt

$$[a]_\sim = \{b \in A \mid a \sim b\}$$

die Äquivalenzklasse von a (bzgl. $\sim$). Die Elemente in $[a]_\sim$ heißt Repräsentant von $[a]_\sim$.

Def: Sei $A \neq \emptyset$ eine beliebige Menge. Eine Zerlegung oder Partition von A ist eine Familie $\mathcal{Z} \subseteq \mathcal{P}(A)$ mit

i) $A = \bigcup_{X \in \mathcal{Z}} X$

ii) $\emptyset \notin \mathcal{Z}$

iii) Für $M_1, M_2 \in \mathcal{Z}$ mit $M_1 \neq M_2$ gilt $M_1 \cap M_2 = \emptyset$

Satz: Sei $A \neq \emptyset$. Eine bel. Äquivalenzrelation über A definiert ein Zerlegung $\mathcal{Z}$ von A und umgekehrt legt jede Zerlegung $\mathcal{Z}$ von A wieder eine Äquivalenzrelation R fest.

Beweis:

„$\Rightarrow$" Sei $A_a = \{ b \in A \mid a \sim b \}$ und $\mathcal{Z}$ sei die Mengen aller Mengen A_a, wobei $a \in A$.

Da $\sim$ reflexiv ist, kann A_a nicht leer sein und $\bigcup_{a \in A} A_a = \bigcup_{X \in \mathcal{Z}} X = A$.

Nun ist noch zu zeigen, dass für A_a und A_b mit $A_a \neq A_b$ gilt $A_a \cap A_b = \emptyset$.

Angenommen es gäbe $A_a \neq A_b$ mit $d \in A_a \cap A_b$, dann gilt $a \sim d$ und $b \sim d$. Wegen der Symmetrie auch $d \sim b$ und mit der Transitivität $a \sim b$. D.h. $A_a = A_b$. Widerspruch $\Rightarrow$ $A_a \cap A_b = \emptyset$

„$\Leftarrow$" Sei $\mathcal{Z}$ eine Zerlegung von A. $A_x \in \mathcal{Z}$ sei die Klasse von $\mathcal{Z}$, die das Element $x \in A$ enthält.

Es kann passieren, dass eine Klasse evtl. mehrere „Namen" hat, da ja mehr als ein Element in A_x vorkommen kann.

Sei $R = \{(a,b) \in A^2 \mid A_a = A_b\}$

Klar: R ist reflexiv, da $A_a = A_a$, d.h. $(a,a) \in R$
Ebenso ist R symmetrisch, da aus $A_a = A_b$ auch $A_b = A_a$ folgt, d.h. aus aRb folgt bRa.
Gilt aRb und bRc, dann bedeutet dies $A_a = A_b$ und $A_b = A_c$, d.h. $A_a = A_c$ und somit ist aRc, d.h. R ist transitiv.
$\Rightarrow$ R ist Äquivalenzrelation. #

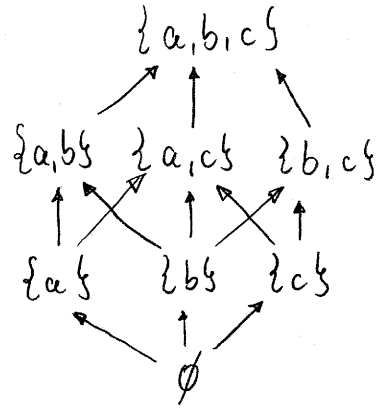
Def: Sei R ein Relation über A, die reflexiv, antisymmetrisch und transitiv ist, dann nennt man R eine

Halbordnung.

Gilt zusätzlich, dass für alle $a, b \in A$ aRb oder bRa gilt, dann heißt R Ordnung. Statt aRb schreibt man oft $a \leq b$.

Bsp: Die übliche „kleines-gleich" Relation auf den reellen Zahlen ist eine Ordnung.

Bsp Sei $A = \{a, b, c\}$, dann kann man $\mathcal{P}(A)$ graphisch wie folgt darstellen:



Dann ist „$\subseteq$" eine Halbordnung auf $\mathcal{P}(A)$, da

reflexiv: $\forall X \in \mathcal{P}(A)$ gilt $X \subseteq X$

antisymmetrisch: $\forall X, Y \in \mathcal{P}(A)$ mit $X \subseteq Y$ und $Y \subseteq X$ gilt $X = Y$

transitiv: $\forall X, Y, Z \in \mathcal{P}(A)$ mit $X \subseteq Y$ und $Y \subseteq Z$ gilt $X \subseteq Z$

4.3 Funktionen

Def: Sei $f \subseteq A \times B$ eine Relation zu A und B.

Gibt es für jedes $a \in A$ maximal ein $b \in B$, so dass $(a,b) \in f$, dann heißt f Abbildung oder Funktion

Schreibweise: $f: A \to B$

Gilt $(a,b) \in f$ schreibt man auch $f(a) = b$ oder $f: a \mapsto b$.

Gibt es für alle $a \in A$ genau ein $b \in B$, so dass $f(a) = b$, dann heißt f total.

Die Menge $D_f = \{ a \in A \mid$ es gibt ein $b \in B$ mit $f(a) = b \}$ heißt Definitionsbereich (engl. Domain) von f und $W_f = \{ b \in B \mid$ es gibt ein $a \in A$ mit $f(a) = b \}$ wird Wertebereich (engl. Range) genannt.

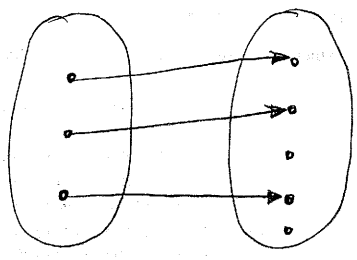
Die inverse Relation f^{-1} heißt Umkehrfunktion, wenn sie selbst eine Funktion ist. Dann heißt f invertierbar.

Die Menge $f^{-1}(N) = \{a \in A \mid f(a) \in N\}$ heißt Urbild von N. Statt $f^{-1}(\{b\})$ schreibt man kurz $f^{-1}(b)$.

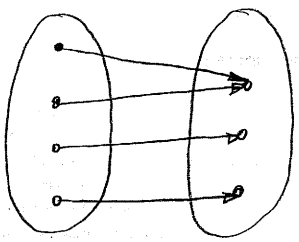
Bem: Diese Definition deckt auch mehrstellige Funktionen ab, da A ja das kartesische Produkt von Mengen sein kann.

Def: Eine Fkt $f: A \to B$ heißt

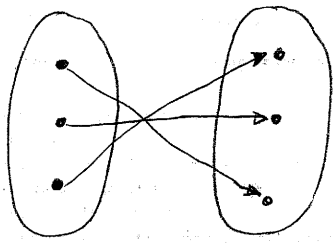
- surjektiv, wenn $W_f = B$
- injektiv, wenn $\forall a, a' \in A$ mit $a \neq a'$ gilt $f(a) \neq f(a')$
- bijektiv, wenn f surjektiv und injektiv ist.



injektiv und nicht surjektiv



surjektiv und nicht injektiv



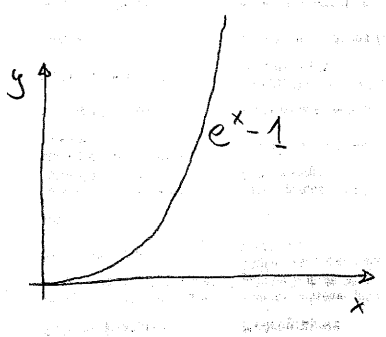
bijektiv

Bsp: • Die Fkt $f: \mathbb{R} \to \mathbb{R}$, $f(x) = 2x+3$ ist bijektiv.

- f ist surjektiv, da $\forall b \in \mathbb{R}$ gilt $f(\underbrace{\frac{b-3}{2}}_{\in \mathbb{R}}) = b$
- f ist injektiv, wenn aus $f(a) = f(a')$ folgt $a = a'$ (via Kontraposition)

Sei $f(a) = f(a')$ $\Rightarrow$ $2a+3 = 2a'+3$
$\Rightarrow$ $2a = 2a'$
$\Rightarrow$ $a = a'$

• Sei $g: \mathbb{R}^+ \to \mathbb{R}^+$, $g(x) = e^x - 1$, dann ist g bijektiv



Bem: Wenn f bijektiv ist, dann auch f^{-1} und $(f^{-1})^{-1} = f$.

5. Abzählbare und überabzählbare Mengen

Def: Zwei Mengen A und B heißen gleichmächtig, wenn eine bijektive Fkt f von A nach B existiert.

Def: Eine Menge A heißt <u>abzählbar</u>, wenn A entweder endlich oder A gleichmächtig $\mathbb{N}$.

Bsp:
- Jede endliche Teilmenge von $\mathbb{N}$ ist abzählbar
- $\mathbb{Z}$ ist abzählbar vermöge $f: \mathbb{N} \to \mathbb{Z}$

$$f(n) = \begin{cases} -\frac{n}{2}, & \text{falls } n \text{ gerade} \\ \frac{1+n}{2}, & \text{sonst} \end{cases}$$

$\mathbb{N}$ =	0	1	2	3	4	5	6	7	...
	↓	↓	↓	↓	↓	↓	↓	↓	
$\mathbb{Z}$ =	0	1	-1	2	-2	3	-3	4	...

- $\mathbb{Q}^+$ ist abzählbar

	1	2	3	4	5	...
1	1/1	2/1	3/1	4/1	5/1	
2	1/2	2/2	3/2	4/2	5/2	
3	1/3	2/3	3/3	4/3	5/3	
4	1/4	2/4	3/4	4/4	5/4	
5	1/5	2/5	3/5	4/5	5/5	

$$\tau(x,y) = \frac{1}{2}(x^2 + 2xy + y^2 + 3x + y)$$

$\mathbb{N}$ =	0	1	2	3	...
	↓	↓	↓	↓	
$\mathbb{Q}^+$ =	1/1	2/1	1/2	1/3	

„Cantor'sches Diagonalargument"

Def: Seien M und I beliebige Mengen, wobei $I \neq 0$. Eine Abbildung $f: I \to M$ heißt Indexfunktion (von I nach M) und I heißt Indexmenge.

Die Werte $f(i)$ werden oft mit m_i bezeichnet und i heißt Index von m_i.
Oft notiert man eine Indexfunktion mit $(m_i)_{i \in I}$ oder kurz (m_i).

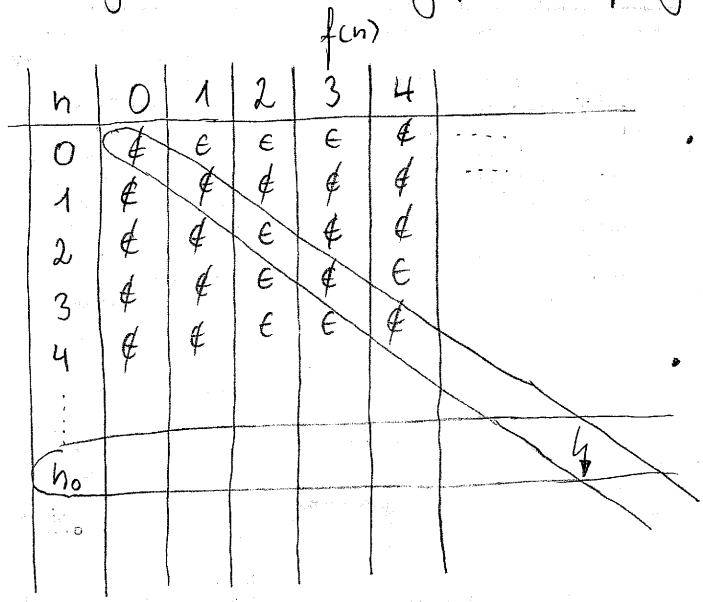
Bsp:
- Jedes Array stellt eine Indexfunktion dar
- Die Zuordnung von Personalausweis (nummer) zu einem Bürger ist eine Indexfunktion.

Frage: Gibt es verschiedene Unendlichkeitsbegriffe?

Satz: Die Potenzmenge $\mathcal{P}(\mathbb{N})$ der natürlichen Zahlen ist nicht abzählbar.

Beweis: Annahme: $\mathcal{P}(\mathbb{N})$ ist abzählbar. Da $\mathcal{P}(\mathbb{N})$ unendlich viele Elemente enthält, gibt es eine bijektive Abbildung $f: \mathbb{N} \to \mathcal{P}(\mathbb{N})$

Damit ergibt sich (ungefähr) folgende Tabelle



- In diesem Beispiel gilt $1,2,3 \in f(0)$, aber $0,4 \notin f(0)$
- Die genaue Tabelle ist nicht bekannt, da f nicht bekannt ist

Für die Diagonale D gilt $D = \{n \in \mathbb{N} \mid n \in f(n)\}$.
Sei $S = \{n \in \mathbb{N} \mid n \notin f(n)\}$ die negierte Diagonale.

Es gilt $S \subseteq \mathbb{N}$, d.h. $S \in \mathcal{P}(\mathbb{N})$, d.h. es gibt ein n_0 mit $S = f(n_0)$, da f bijektiv

Nun soll untersucht werden, ob $n_0 \in S$ gilt

$n_0 \in S$: Wenn $n_0 \in S$ wäre, dann gilt nach Def. von S $n_0 \notin f(n_0) = S$. Kann nicht sein.

$n_0 \notin S$: Wenn $n_0 \notin S$, dann gilt $n_0 \in S$, denn es gilt $n_0 \notin f(n_0) = S$. Kann nicht sein.

Dies führt zum Widerspruch $n_0 \in S \leftrightarrow n_0 \notin S$.
$\Rightarrow$ Annahme falsch, d.h. $\mathcal{P}(\mathbb{N})$ kann nicht abzählbar sein. #

Def: Eine Menge heißt überabzählbar, wenn sie nicht abzählbar ist.

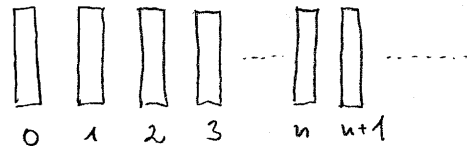
Folgerung: $\mathcal{P}(\mathbb{N})$ ist überabzählbar.

Bem:
- Stellt man die reellen Zahlen im Intervall $(0,1)$ als unendlich lange Bitstrings dar, so kann man zeigen, dass dieses Intervall überabzählbar ist.
- $\mathbb{R}$ und $\mathbb{C}$ sind überabzählbar
- Es gilt sogar $\mathcal{P}(\mathbb{N})$ mächtiger als $\mathbb{N}$, $\mathcal{P}(\mathcal{P}(\mathbb{N}))$ mächtiger als $\mathcal{P}(\mathbb{N})$, ..., d.h. es gibt mindestens abzählbar unendlich viele verschiedene Unendlich $\Rightarrow$ Theorie der Kardinalzahlen

6. Induktion und induktive Definitionen

Sei $p(x)$ eine beliebige Aussageform über dem Universum $\mathbb{N}$.
Für jedes $a \in \mathbb{N}$ kann man einen Beweis für $p(a)$ führen.
Aber: Wie zeigt man $\forall a \in \mathbb{N}\ p(a)$?

Anschaulich: „Domino-Tag" $p(n) \hat{=}$ der Dominostein der Nummer n fällt um.



Idee: i, Zeige Dominostein 0 fällt um

ii, Zeige, dass Dominostein $n+1$ fällt, wenn Stein n fällt (allgemein für $\forall n \in \mathbb{N}$)

Formal:

Induktionsanfang: Zeige, dass $p(0)$ gilt

Induktionsschritt: Zeige, dass $\forall n \in \mathbb{N}$ gilt

Wenn $p(n)$ wahr, dann auch $p(n+1)$ wahr

Die Voraussetzung $p(n)$ nennt man auch

Induktionsvoraussetzung.

Bsp „Summe der ungeraden Zahlen"

$$1 = 1$$
$$1 + 3 = 4$$
$$1 + 3 + 5 = 9$$
$$1 + 3 + 5 + 7 = 16$$

Dies führt zu folgender Vermutung: $\triangleq \forall n \in \mathbb{N}\ p(n)$

Satz: Sei $n \in \mathbb{N}$, $n > 0$, dann gilt $\sum_{i=1}^{n} 2i-1 = n^2$

Beweis:

(IA) $n=1$: $\sum_{i=1}^{1} 2i-1 = 1 = 1^2$ Ok

(IV) $\forall a \in \mathbb{N}\ \sum_{i=1}^{a} 2i-1 = a^2$

(IS) $n \to n+1$

$$\sum_{i=1}^{n+1} 2i-1 = \sum_{i=1}^{n} 2i-1 + 2(n+1)-1$$
$$\overset{(IV)}{=} n^2 + 2n + 1$$
$$= (n+1)^2$$

} dann $p(n+1)$

Wenn $p(n)$

#

An dieser Stelle zeigt sich ein direkter Zusammenhang mit rekursiven Programmen:

Pseudocode:

```
int Sum Odds (int i)      // summiere die ersten i ungeraden
                          // Zahlen

  if (i == 0) then
    return "error";
  endif;
  if (i == 1) then
    return 1;        // Abbruch der Rekursion
  else
    return (2i-1) + Sum Odds(i-1);
  endif
end Sum Odds.
```

Mathematisch:

$$\text{sum odds} : \mathbb{N} \to \mathbb{N} \quad \text{mit} \quad \text{sum odds}(i) = \begin{cases} \text{undefiniert, falls } i=0 \\ 1, \text{ falls } i=1 \\ 2i-1 + \text{sum odds}(i-1), \\ \qquad \text{sonst} \end{cases}$$

$\Rightarrow$ Induktion und Rekursion sind verwandt.

Ein weiteres Beispiel:

<u>Satz:</u> Sei M eine endliche Menge, dann gilt $\#\mathcal{P}(M) = 2^{\#M}$.

Beweis:

(IA) Sei $\#M = 1$, dann gibt es genau zwei Mengen in $\mathcal{P}(M)$, nämlich $\emptyset$ und M. Es gilt $2 = \#\mathcal{P}(M) = 2^1$, d.h. der Induktionsanfang gilt.

(IV) Sei $\#N = n$, dann gilt $\#\mathcal{P}(N) = 2^n$

(IS) $n \to n+1$

Sei $M = \{a_1, a_2, \dots, a_n, a_{n+1}\}$ eine Menge mit $n+1$ Elementen. Wählen nun $a_i \in M$ beliebig und $M' = M \setminus \{a_i\}$, d.h. $\#M' = n$.

Nach (IV) gibt es also 2^n Teilmengen von M', die auch alle Teilmengen von M sind.

Für jedes $X \in \mathcal{P}(M')$ gilt $X \cup \{a_i\} \subseteq M$, also gibt es weitere 2^n Teilmengen von M. Andere Teilmengen gibt es nicht.

Also $\#\mathcal{P}(M) = 2\#\mathcal{P}(M') = 2 \cdot 2^n = 2^{n+1}$. #

Bem: Wir haben bisher nur die Struktur

(IA) beweise $p(0)$

(IS) beweise $\forall a$ gilt $p(a) \to p(a+1)$

verwendet, man kann das auch verallgemeinern

(IA) beweise $p(0)$

(IS) beweise $\forall a$ gilt $(p(0) \wedge p(1) \wedge \dots \wedge p(a)) \to p(a+1)$

$\Rightarrow$ es ex. weitere Varianten von Induktions-beweisen.

Das Induktionsprinzip kann auch für Definitionen benutzt werden

6.1. Induktive Definitionen

Bsp: Wir definieren die Folge $(a_i)_{i \in \mathbb{N}}$ durch

(IA) $a_0 = 1$

(IS) $a_{n+1} = a_n \cdot (n+1)$

D.h.

i	0	1	2	3	4	5	...
a_i	1	1	2	6	24	120	...

Nun kann man leicht Induktionsbeweise führen:

Satz: Für jedes $n \in \mathbb{N}^{\wedge}_{n \geq 1}$ gilt $a_n = \prod_{i=1}^{n} i$

Beweis:

(IA) $n = 1$ $\quad 1 = a_0 = \prod_{i=1}^{1} i$, d.h. die Induktionsanfang ist erfüllt.

(IV) $\quad a_n = \prod_{i=1}^{n} i$

(IS) $n \to n+1$:

$$a_{n+1} = a_n \cdot (n+1) \overset{(IV)}{=} \prod_{i=1}^{n} i \cdot (n+1) = \prod_{i=1}^{n+1} i \qquad \#$$

Def: Die Menge L_{AL} der aussagenlogischen Formeln ist wie folgt definiert:

(IA) Jede Aussagenvariable $x_1, x_2, x_3, \ldots$ ist eine aussagenlogische Formel

(IS) Seien $H_1, H_2 \in L_{AL}$, dann auch

$(H_1 \wedge H_2)$, $(H_1 \vee H_2)$, $(H_1 \to H_2)$, $(H_1 \leftrightarrow H_2)$, $(H_1 \oplus H_2)$, $\neg H_1 \in L_{AL}$

Nichts sonst ist eine aussagenlogische Formel.

Def: Sei $H \in L_{AL}$, dann $\#_(H) =$ „Anzahl der öffnenden Klammern in H" und $\#_)(H) =$ „Anzahl der schliessenden Klammern in H"

Bsp: Sei $H = ((x \vee y) \wedge \neg z)$, dann $\#_(H) = 2$ und $\#_)(H) = 2$.

Satz: Sei $H \in L_{AL}$, dann gilt $\#_(H) = \#_)(H)$.

Beweis: via Induktion über den Aufbau der Formel #

In der Informatik nennt man eine endliche Menge Σ Alphabet und ihre Elemente Buchstaben. Σ^* ist dann die Menge aller Worte inkl. des leeren Worts, das$ aus keinem Buchstaben besteht.

Wir definieren eine Menge L von Worten ($\hat{=}$ Sprache):

Def: Sei $\Sigma = \{a, b\}$ dann

(IA) gehört das Wort ab zu L

(IS) gilt $x \in L$, dann gehört auch $a \times b$ zu L.

kein anderes Wort gehört zu L.

7. Graphentheorie

Def: Ein (gerichteter) Graph $G = (V, E)$ ist ein Paar aus einer Menge V, der Menge der Knoten und einer Relation $E \subseteq V \times V$, der Menge der Kanten.

Die Kante $e = (u, v) \in E$ verbindet den Startknoten u mit dem Endknoten v.

Zwei verbundene Knoten heißen auch adjazent (benachbart).

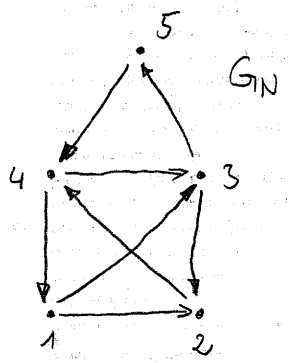
Ist die Menge der Knoten endlich, so heißt der Graph endlich.

Bsp:

- Nullgraph $G_0 = (V, \emptyset)$
- vollständiger Graph $G_V = (V, V \times V)$
- $V = \{1, 2, 3, 4, 5\}$

$E = \{(1,2), (2,4), (4,3), (3,5), (5,4), (4,1), (1,3), (3,2)\}$

$G_N = (V, E)$



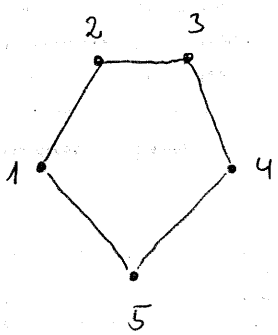
Def: Sei $G = (V, E)$ ein Graph. Ist E eine symmetrische Relation, dann heißt G ungerichtet.

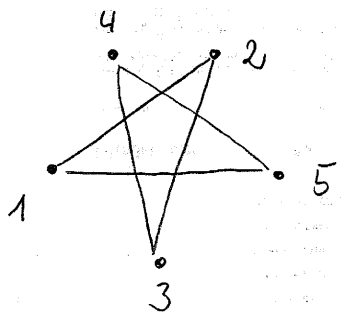
Bem: Bei einem ungerichteten Graphen $G = (V, E)$ schreibt man kurz nur $(a,b) \in E$ statt $(a,b) \in E$ und $(b,a) \in E$.

Da die Anordnung der Knoten keine Rolle spielt, wird (a,b) und (b,a) auch durch $\{a,b\}$ abgekürzt

Bem: Die graphische Darstellung ist nicht eindeutig:

$G_5 = (V, E)$, $V = \{1,2,3,4,5\}$ und $E = \{(1,2), (2,3), (3,4), (4,5), (5,1)\}$





Def: Ein Graph heißt planar, wenn er ohne Überkreuzung von Kanten gezeichnet werden kann.

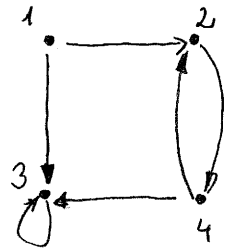
Bem: G_5 ist planar (Anwendung: Platinenentwicklung)

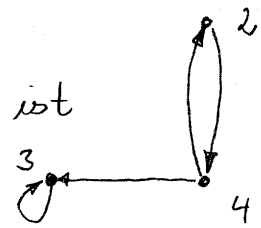
Def: Seien $G = (V_G, E_G)$ und $H = (V_H, E_H)$ Graphen. Gilt $V_H \subseteq V_G$ und $E_H \subseteq E_G$, dann heißt H Teilgraph oder Untergraph (von G).

Def: Sei $G = (V_G, E_G)$ ein Graph und $V' \subseteq V_G$. Der Graph

$$G_{V'} = (V', E') \text{ mit } E' = \{(u,v) \in V' \times V' \mid (u,v) \in E_G\}$$

heißt der von V' induzierte Teilgraph (von G).

Bsp: Sei 

, dann ist 

G $\qquad$ $G_{\{2,3,4\}}$

Nun kann man auch einfach Boolesche Operationen auf Graphen definieren:

Def Seien $G = (V, E)$ und $G' = (V', E')$ Graphen, dann

$$G \cup G' = (V \cup V', E \cup E') \quad \text{„Vereinigung“}$$

$G_1 \cap G_2 = (V_1 \cap V_2, E_1 \cap E_2)$ „Schnitt"

$\neg G_1 = (V_1, (V_1 \times V_1) \setminus E_1)$ „Komplementgraph"

Def: Sei $G_1 = (V_1, E_1)$ und $v \in V_1$. Der Ausgrad (engl. outdegree) von v ist die Anzahl der Kanten, die v als Startknoten haben. Analog ist der Ingrad (engl. indegree) von v die Anzahl der Kanten, die v als Endknoten haben.

Als Abkürzung verwenden wir $\text{outdeg}_{G_1}(v)$ und $\text{indeg}_{G_1}(v)$. Im ungerichteten Fall verwenden wir $\deg_{G_1}(v)$.

Ein Knoten v mit $\text{outdeg}_{G_1}(v) = \text{indeg}_{G_1}(v) = 0$ heißt isoliert.

Satz: Sei $G_1 = (\{v_1, \dots, v_n\}, E_1)$ ein gerichteter Graph, dann gilt

$$\sum_{i=1}^{n} \text{indeg}_{G_1}(v_i) = \sum_{i=1}^{n} \text{outdeg}_{G_1}(v_i) = \#E_1$$

Ist G_1 ungerichtet, dann gilt

$$\sum_{i=1}^{n} \deg_{G_1}(v_i) = 2 \cdot \#E_1$$

Beweis: Induktion über die Anzahl der Kanten.

(IA) $\#E = 0$, d.h. alle Knoten von G sind isoliert und G ist ungerichtet.

$$\sum_{i=1}^{n} \text{indeg}_G(v_i) = \sum_{i=1}^{n} \text{outdeg}_G(v_i) = 0 = \#E$$

und

$$\sum_{i=1}^{n} \deg_G(v_i) = 0 = 2 \cdot \#E,$$ d.h. der (IA) ist erfüllt.

(IV) Sei G ein Graph mit m Kanten und Knoten $\{v_1, \dots, v_n\}$, dann gilt

$$\sum_{i=1}^{n} \text{indeg}_G(v_i) = \sum_{i=1}^{n} \text{outdeg}_G(v_i) = \#E$$

Ist G ungerichtet, dann gilt sogar

$$\sum_{i=1}^{n} \deg_G(v_i) = 2 \cdot \#E.$$

(IS) $m \to m+1$: Sei G ein Graph mit $m+1$ Kanten und $e = (u, v) \in E$.

G' ist ein Graph, der entsteht, wenn man aus G die Kante e heraus nimmt.

Damit verringert sich für u der Ausgrad um genau 1 und für v der Eingrad auch.

$$\text{Also } \sum_{i=1}^{n} \text{indeg}_G(v_i) = \sum_{i=1}^{u} \text{indeg}_{G'}(v_i) + 1$$

$$\overset{(IV)}{=} \sum_{i=1}^{u} \text{outdeg}_{G'}(v_i) + 1$$

$$= \sum_{i=1}^{u} \text{outdeg}_G(v_i) = \#E$$

Entfernt man aus einem ungerichteten Graphen eine Kante (u,v), dann muß auch (v,u) entfernt werden, um die Kantenrelation symmetrisch zu halten.
Rest mit gleicher Argumentation. #

Folgerung: In einem ungerichteten Graphen ist die Zahl der Knoten mit ungeraden Grad gerade.

Beweis: Wäre dies nicht der Fall, so wäre $\sum_{i=1}^{u} \deg_G(v_i)$ ungerade. Widerspruch. #

Def: Ein ungerichteter Graph heißt regulär, wenn alle Knoten genau Grad k haben.

Korollar: Sei $G = (V,E)$ regulär, dann gilt

$$k \cdot \#V = 2 \cdot \#E.$$

Def: Sei $G = (\{v_1, \dots, v_n\}, \{e_1, \dots, e_m\})$ ein ungerichteter Graph. Eine Folge von Kanten $e_{i_1}, e_{i_2}, \dots, e_{i_k} \in \{e_1, \dots, e_m\}$ heißt Pfad / Weg (der Länge k) von u nach v, wenn für alle $e_{i_j} = (u_{i_j}, v_{i_j})$ mit $1 \leq j \leq k$ gilt:

i) $e_{i_1} = (u, v_{i_1})$ und $e_{i_k} = (u_{i_k}, v)$

ii) für $1 \leq j < k$ gilt $v_{i_j} = u_{i_{(j+1)}}$

G heißt zusammenhängend, wenn für alle Knoten u und v ein Pfad von u nach v existiert.

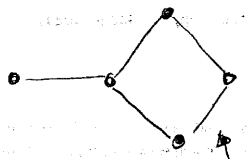
Ein Pfad von u nach v heißt geschlossen, Zyklus oder Kreis, wenn $u = v$ gilt.

Def:

- Ein Graph heißt zyklenfrei / kreisfrei, wenn er keinen Zyklus der Länge ≥ 1 hat. Ist der Graph gerichtet, so heißt er DAG (directed acyclic graph).
- Ein zyklenfreier Graph heißt Wald.
- Ein Wald heißt Baum, wenn er zusammenhängend ist.

Bsp:

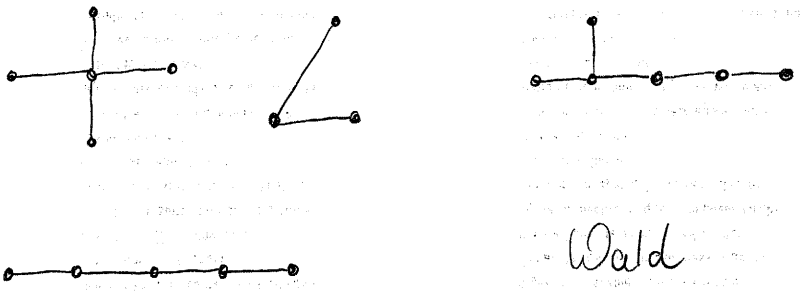
G_1



„Doppelbaum"

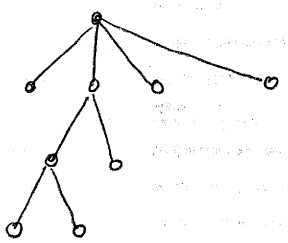
Kreis

G_2



Wald

G_3



Satz: Ist G ein zusammenhängender Graph mit n Knoten und $n-1$ Kanten, dann ist G ein Baum.

Beweis: z.B. Meinel, Mundhenk, Mathematische Grundlagen der Informatik. #

8. Algebraische Grundlagen

In der Algebra werden Strukturen von Mengen untersucht. Geschichtlich geht die Algebra aus dem Problem Gleichungen zu lösen hervor

ca. 825 „al-Kitab al-mukhtasar fi hisab al-dschabr wa-l-muqabala"
„Algebra"

„Das kurz gefasste Buch übo die Rechenverfahren zum Ergänzen und Ausgleichen"

von al-Chwarizmi aus Bagdad.
„Algorithmus"

Def: Ein Paar $(G, \circ)$ heißt Gruppe, wenn

i) $\circ$ ist eine Funktion der Form $\circ : G \times G \to G$

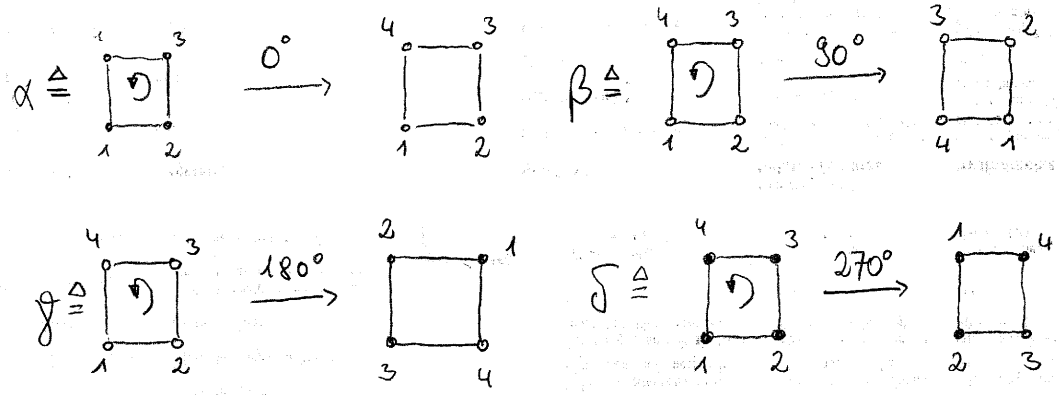
ii) $\circ$ ist assoziativ, d.h. $\forall a,b,c \in G$ gilt $a \circ (b \circ c) = (a \circ b) \circ c$

iii) Es gibt ein Element $e \in G$, sodass $\forall a \in G$ gilt $a \circ e = a = e \circ a$

e heißt neutrales Element.

- für jedes $a \in G$ gibt es ein $a' \in G$, so dass $a \circ a' = e = a' \circ a$. a' heißt inverses Element (von a)
- gilt $\forall a, b \in G$ zusätzlich $a \circ b = b \circ a$, dann heißt $(G, \circ)$ kommutative oder abelsche Gruppe.

Bsp:
- $(\mathbb{Z}, +)$ ist eine abelsche Gruppe
- $(\mathbb{R} \setminus \{0\}, \cdot)$ ——"——
- $(\mathbb{C} \setminus \{0\}, \cdot)$ ——"——
- $(\mathbb{N}, +)$ ist keine abelsche Gruppe
- „Drehung eines Vierecks"



Die Verknüpfung sei die Hintereinanderausführung von Drehungen. Darstellung als Verknüpfungstafel

$\circ$	α	β	γ	δ
α	α	β	γ	δ
β	β	γ	δ	α
γ	γ	δ	α	β
δ	δ	α	β	γ

Beh: $(\{\alpha, \beta, \gamma, \delta\}, \circ)$ ist eine Gruppe

Def: Sei $m \in \mathbb{N}$, $m \geq 2$. Zwei Zahlen $a, b \in \mathbb{Z}$ heißen kongruent modulo m, wenn $m \mid a-b$
Schreibweise: $a \equiv b \bmod m$

Bsp: Es gilt $-2 \equiv 19 \bmod 21$ oder $10 \equiv 0 \bmod 2$

Lemma: Die Kongruenz ist eine binäre Äquivalenzrelation.

Beweis: vgl. Übung #

Lemma: Die folgenden Aussagen sind äquivalent

i) $a \equiv b \bmod m$
ii) $a = b + km$ im $k \in \mathbb{Z}$
iii) a und b lassen bei der Division den gleichen Rest

Beweis: Wir führen einen Zirkelschluß durch

i) $\rightarrow$ ii): Wenn $a \equiv b \bmod m$, dann gilt $m \mid a-b$, d.h. $a - b = k \cdot m$ nach Def. von „|"

ii) $\rightarrow$ iii) Wenn $a = b + k \cdot m$, dann läßt a bei der Division durch m den Rest b. Da $b = a - k \cdot m$ gilt das auch für b.

iii → i, Wenn $a = b + km$, dann gilt $a - b = km$,
d.h. $m \mid a-b$ und somit $a \equiv b \bmod m$.

Def: Das Tripel $(R, \oplus, \odot)$ heißt Ring, wenn
i, $(R, \oplus)$ ist eine abelsche Gruppe
ii, $\odot$ ist vom Typ $\odot : R \times R \to R$ „Abgeschlossenheit"
iii, $\odot$ ist assoziativ
iv, $\forall a, b, c \in R$ gilt $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$
und $(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$
„Distributivität"

Def: Ist $(R, \oplus, \odot)$ ein Ring und zusätzlich $(R \setminus \{e_+\}, \odot)$ eine abelsche Gruppe, wobei e_+ das neutrale Element der Verknüpfung $\oplus$ ist, dann heißt $(R, \oplus, \odot)$ Körper (engl. Field).

Bsp: · $(\mathbb{Z}, +, \cdot)$ ist ein Ring aber kein Körper
· $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$ sind Körper

Lemma: Seien $a, b, c, d \in \mathbb{Z}$ und $m \in \mathbb{N}$, $m \geq 2$, dann gilt

i) $a + c \equiv b + d \mod m$

ii) $a \cdot c \equiv b \cdot d \mod m$

Beweis: Meinel / Mundhenk, Mathematische Grundlagen der Informatik. #

D.h. mit Kongruenzen kann man Umformungen vornehmen wie gewohnt, indem man auf beiden Seiten addiert oder multipliziert

Man kann mod m statt als Äquivalenzrelation als Modulo-Fkt verwenden, d.h.

$$(x + y) \bmod m = ((x \bmod m) + (y \bmod m)) \bmod m$$

(↓ Funktion)

So ist dies in den üblichen Programmiersprachen gelöst, z.B. Java kennt den %-Operator.

Bsp $(2370 + 5780) \bmod 100 = ((2370 \bmod 100) + (5780 \bmod 100)) \bmod 100$

$= (70 + 80) \bmod 100$

$= 150 \bmod 100$

$= 50 \bmod 100$

Probe $2370 + 5780 \equiv 8150 \equiv 50 \mod 100$

, wenn $a \equiv b \mod m$ und $c \equiv d \mod m$.

Def: Sei $m \in \mathbb{N}$, $m \geq 2$, dann ist $\mathbb{Z}_m = \{ a \mid 0 \leq a < m \}$.
Seien $a, b \in \mathbb{Z}_m$, dann definieren wir

i) $a \oplus b = (a+b) \bmod m$
ii) $a \odot b = (a \cdot b) \bmod m$

Bem: $(\mathbb{Z}_m, \oplus, \odot)$ ist ein Ring, wobei es sogar ein neutrales Element bzgl. $\odot$ gibt und zusätzlich ist $\odot$ kommutativ.

$(\mathbb{Z}_m, \oplus, \odot)$ heißt Restklassenring modulo m.

Def: Seien $a, b \in \mathbb{Z}$, dann bezeichnet $ggT(a,b)$ den größten gemeinsamen Teiler, d.h.

$T_a = \{ c \mid c \mid a \}$
$T_b = \{ c \mid c \mid b \}$
$\Rightarrow ggT(a,b) = \text{maximum}(T_a \cap T_b)$

Zwei Zahlen $a, b \in \mathbb{Z}$ heißen teilerfremd, wenn $ggT(a,b) = 1$

Wir legen fest: $ggT(0,0) = 0$

Bsp: $ggT(15,10) = 5$ und $ggT(3,7) = 1$, d.h. 3 und 7 sind teilerfremd.

Satz: Sei $m \in \mathbb{N}$, $m \geq 2$ und $a \in \mathbb{Z}_m$. Es gibt genau dann ein $a' \in \mathbb{Z}_m$ mit $a \circ a' = 1 \bmod m$, wenn $ggT(a, m) = 1$.

Beweis: später (erst. Security) #

Bsp: RSA nach Rivest - Shamir - Adleman

i) Wähle zwei verschiedene Primzahlen p und q
ii) berechne $n = p \cdot q$
iii) berechne $\phi = (p-1)(q-1)$
iv) wähle ein e, so dass $ggT(e, \phi) = 1$
v) suche ein d mit $e \cdot d \equiv 1 \bmod \phi$

Öffentlich: (n, e)
Geheim: d

Verschlüsseln mit $E(m) = m^e \bmod n$, $m \in \mathbb{Z}_n$
Entschlüsseln mit $D(m) = m^d \bmod n$, $m \in \mathbb{Z}_n$

Bsp $p = 7$, $q = 11$ $\Rightarrow$ $n = 77$ $\phi = 60$

$e = 17$, dann liefert Know-How oder probieren $d = 53$

Sei $m = 45$, dann $E(45) = 45^{17} \bmod 77$
$= 12$
$D(12) = 12^{53} \bmod 77$
$= 45$

- Welche Algorithmen brauchen wir dafür?
- Wie macht man das effizient? (In der Praxis werden Zahlen mit 1024 Bit (≈ 300 Dezimalstellen) verwendet (und mehr).
- Warum ist das sicher?

— Ende der Vorlesung —