

Übersichtsfolien zur Übung

Diskrete Strukturen im Wintersemester 2013/2014

Markus Kaiser

6. Februar 2014

- Markus Kaiser
 - Mail: tutor@zfix.org
 - Web: ds.zfix.org

- Vorlesung
 - Dienstag 13:45-15:15 in MI HS1
 - Donnerstag 10:15-11:45 in MI HS1

- Meine Tutorübungen
 - Dienstag 12:00-14:00 in 03.09.014
 - Dienstag 16:15-17:45 in 03.11.018
 - Offiziell müsst ihr in die angemeldete Übung!

■ Hausaufgaben

- Abgabedatum auf Übungsblatt
- Abgabe in Briefkästen, Rückgabe in Tutorübung
- Geheftet, Handschriftlich, Deckblatt
- Teams aus 3 oder 4 Studenten
- Teams nicht änderbar, nicht gruppenübergreifend
- Üblicherweise schwerer als Klausurstoff

■ Notenbonus

- „Bepunktung“ mit Ampelfarben
- Bei $\frac{2}{3}$ mindestens gelb
- 0.3 Notenstufen Bonus auf bestandene Klausur

■ Tutoresaufgaben

- Lösen wir zusammen in den Übungen
- Üblicherweise schwerer als Klausurstoff

- **Mathematische Grundlagen**
 - Mengen, Relationen, Funktionen
 - Logik
 - Beweise
- **Kombinatorik**
 - Zählkoeffizienten
 - Spaß mit Urnen
- **Graphentheorie**
 - Definition
 - Ein paar Algorithmen
- **Algebra**
 - Modulo
 - Algebren
 - Gruppen, vielleicht Körper

Definition (Menge)

Eine **Menge** ist eine **ungeordnete** Sammlung **unterscheidbarer** Objekte.

Mit **Mengenklammern** werden Objekte zusammengefasst.

$$A := \{a, b, \dots, z\}$$

Man nennt a ein **Element** von A , es gilt $a \in A$.

- Reihenfolge ist **egal**
- Elemente kommen **nicht** mehrfach vor

Beispiel

- $\{a, b, c, a, c\} = \{a, b, c\} = \{c, a, b\}$
- $\mathbb{N} := \{1, 2, 3, \dots\}$
- $\emptyset := \{\}$

Definition (Extensionale Schreibweise)

Die **extensionale Schreibweise** einer Menge zählt ihre Elemente auf.

$$M := \{x_1, x_2, x_3, \dots\}$$

Beispiel

- $A := \{2, 4, 6, \dots\}$
- $B := \{1, 2, 3, 4\} = [4]$
- $C := \{2, 3, 5, 7, 11, \dots\}$
- $D := \{\alpha, a, \odot, 8, \{1, 2\}, \mathbb{N}\}$

Definition (Intensionale Schreibweise)

Die **intensionale Schreibweise** beschreibt eine Menge durch charakteristische Eigenschaften.

$$M := \{x \in \Omega \mid P(x)\}$$

M enthält alle Elemente im **Universum** Ω mit der Eigenschaft P .

Beispiel

- $A := \{2, 4, 6, \dots\} = \{x \in \mathbb{N} \mid x \text{ gerade}\} = \{2x : x \in \mathbb{N}\}$
- $B := \{1, 2, 3, 4\} = \{x \in \mathbb{N} \mid x \leq 4\}$
- $C := \{2, 3, 5, 7, 11, \dots\} = \{x \in \mathbb{N} \mid x \text{ prim}\}$

Bezeichnungen

- Objekte in Mengen

$a \in A$ a ist Element von A

$b \notin A$ b ist kein Element von A

$|A|$ Anzahl der Elemente in A , Kardinalität

- Relationen zwischen Mengen

$B \subseteq A$ B ist Teilmenge von A , $x \in B \rightarrow x \in A$

$B \subset A$ B ist echte Teilmenge von A

$B = A$ $B \subseteq A$ und $A \subseteq B$

Beispiel

- $1 \in \{1, 2, 3, 4\}$, aber $9 \notin \{1, 2, 3, 4\}$

- $\{1, 2\} \subseteq \{1, 2, 3, 4\}$, aber $\{1, 5\} \not\subseteq \{1, 2\}$

- $\emptyset \subseteq [5] \subseteq \mathbb{N} \subseteq \mathbb{N}_0 \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

Operationen

$$\bar{A} := \{x \mid x \notin A\}$$

Komplement

$$A \cup B := \{x \mid x \in A \text{ oder } x \in B\}$$

Vereinigung

$$A \cap B := \{x \mid x \in A \text{ und } x \in B\}$$

Schnitt

$$A \setminus B := A \cap \bar{B}$$

Differenz

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

Symmetrische Differenz

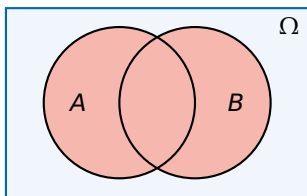
Für mehrere Mengen schreibt man

$$\bigcap_{i=1}^n A_i := A_1 \cap A_2 \cap \dots \cap A_n$$

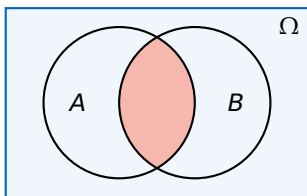
$$\bigcup_{i=1}^n A_i := A_1 \cup A_2 \cup \dots \cup A_n$$

Venn-Diagramme visualisieren Mengen A, B, \dots im Universum Ω .

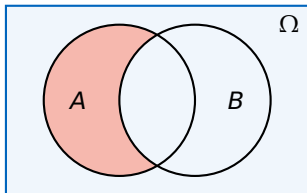
■ $A \cup B$



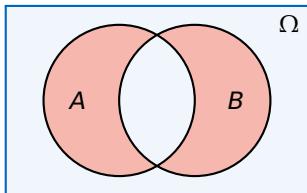
■ $A \cap B$



■ $A \setminus B$



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



Satz (De Morgansche Gesetze)

Sind A, B Mengen, dann gilt

$$\overline{A \cup B} = \bar{A} \cap \bar{B}$$

$$\overline{A \cap B} = \bar{A} \cup \bar{B}$$

Für Mengen A_i gilt

$$\overline{\bigcup_{i=1}^n A_i} = \bigcap_{i=1}^n \bar{A}_i$$

$$\overline{\bigcap_{i=1}^n A_i} = \bigcup_{i=1}^n \bar{A}_i$$

- Zusammen mit $\overline{\bar{A}} = A$ wichtigste Regel
- Gilt auch in der Aussagenlogik

Definition (Potenzmenge)

Die **Potenzmenge** $\mathcal{P}(M)$ zu einer Menge M ist die Menge all ihrer Teilmengen.

$$\mathcal{P}(M) := \{X \mid X \subseteq M\}$$

- $\mathcal{P}(M)$ enthält für endliche Mengen genau $2^{|M|}$ Elemente
- Man schreibt deshalb auch 2^M
- Es ist $M \in \mathcal{P}(M)$ und $\emptyset \in \mathcal{P}(M)$

Beispiel

Für $M = \{a, b, c\}$ ist

$$\mathcal{P}(M) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

mit $|\mathcal{P}(M)| = 2^3 = 8$

Definition (Tupel)

Ein n -Tupel ist eine **geordnete** Sammlung n **beliebiger** Objekte. Mit **Tupelklammern** werden Objekte zusammengefasst.

$$T := (t_1, t_2, \dots, t_n)$$

- Reihenfolge **nicht** egal
- Elemente **dürfen** mehrmals vorkommen

Beispiel

- $(a, b, c) \neq (c, a, b) \neq (a, b, c, a, c)$
- $(1, 2, 3) \neq \{3, 2, 1\} = \{1, 2, 3\}$
- $(\{\alpha, \beta\}, \emptyset, \mathbb{N})$

Definition (Kreuzprodukt)

Sind A, B Mengen, dann ist ihr **kartesisches Produkt** (Kreuzprodukt)

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

Für Mengen A_i ist

$$A_1 \times \dots \times A_n := \{(a_1, \dots, a_n) \mid a_1 \in A_1, \dots, a_n \in A_n\}$$

- Für endliche A_i ist $|A_1 \times \dots \times A_n| = |A_1| \cdot \dots \cdot |A_n|$
- Man schreibt $A^n := \underbrace{A \times \dots \times A}_{n \text{ mal}}$ mit $A^0 = \{\emptyset\}$

Beispiel

- $\{1, 2\} \times \{a, b\} = \{(1, a), (2, a), (1, b), (2, b)\}$
- $\{\alpha, \beta\}^2 = \{(\alpha, \alpha), (\alpha, \beta), (\beta, \alpha), (\beta, \beta)\}$

Definition (Relation)

Eine binäre **Relation** R verbindet Elemente zweier Mengen A und B .

$$R \subseteq A \times B$$

Ist $(a, b) \in R$, so schreibt man auch $a R b$.

- Eine Relation über $M \times M$ nennt man homogen
- Es gibt $|\mathcal{P}(A \times B)|$ Relationen über A, B

Beispiel

- Die **Gleichheitsrelation** über $\mathbb{N} \times \mathbb{N}$
 $\{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6), (7, 7), \dots\}$
- Die **Teilbarkeitsrelation** über \mathbb{N}
 $\{(1, 1), (1, 2), (1, 3), \dots, (2, 2), (2, 4), \dots, (3, 3), (3, 6), \dots\}$

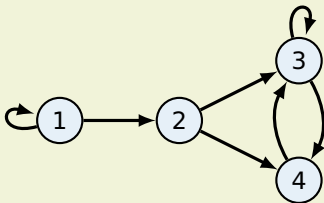
Grafische Darstellung von Relationen

Jede Relation $R \subseteq M \times M$ kann als **Graph** dargestellt werden. Die Elemente aus M werden zu **Knoten** und für jedes Tupel $(a, b) \in R$ wird ein **Pfeil** von a nach b eingefügt.

Beispiel

Sei $R \subseteq [4] \times [4]$ eine Relation über den natürlichen Zahlen.

$$R := \{(1, 1), (1, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 3)\}$$



Eigenschaften homogener Relationen

Sei $R \in M \times M$ eine homogene Relation. Man nennt R

reflexiv $\forall a \in M. (a, a) \in R$

total $\forall a, b \in M. (a, b) \in R \vee (b, a) \in R$

symmetrisch $\forall a, b \in M. (a, b) \in R \rightarrow (b, a) \in R$

asymmetrisch $\forall a, b \in M. (a, b) \in R \rightarrow (b, a) \notin R$

antisymmetrisch $\forall a, b \in M. (a, b) \in R \wedge (b, a) \in R \rightarrow a \equiv b$

transitiv $\forall a, b, c \in M. (a, b) \in R \wedge (b, c) \in R \rightarrow (a, c) \in R$

- Jede totale Relation ist reflexiv
- Jede asymmetrische Relation ist antisymmetrisch
- **Äquivalenzrelationen** sind reflexiv, symmetrisch und transitiv
- R^+ ist die **transitive Hülle**, R^* die **reflexive transitive Hülle**

Definition (Funktion)

Eine Relation $f \subseteq A \times B$ ist eine **Funktion von A nach B** wenn es für alle $a \in A$ genau ein Element $b \in B$ mit $a f b$ gibt.

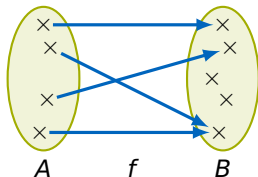
$$\forall a \in A. |\{(a, b) \mid b \in B\}| = 1$$

Man schreibt

$$f : A \rightarrow B$$

$$a \mapsto f(a) = b$$

$A \rightarrow B$ bezeichnet die Menge aller Funktionen von A nach B.



Definition (Bild)

Sei $f : A \rightarrow B$ eine Funktion, $X \subseteq A$, $Y \subseteq B$, $b \in B$. Dann ist

$$f(X) := \{f(x) \mid x \in X\}$$

das **Bild** der Menge X unter f . Außerdem ist

$$f^{-1}(b) := \{a \mid a \in A, f(a) = b\}$$

$$f^{-1}(Y) := \bigcup_{y \in Y} \{f^{-1}(y)\}$$

das **Urbild** des Elements b und der Menge Y unter f .

- Man nennt $A = f^{-1}(B)$ **Urbild** oder **Definitionsmenge** von f
- Man nennt $f(A) \subseteq B$ **Bild** oder **Wertemenge** von f

Definition (Funktionskomposition)

Seien $f : B \rightarrow C$ und $g : A \rightarrow B$ Funktionen. Dann ist

$$h : A \rightarrow C$$

$$a \mapsto (f \circ g)(a) = f(g(a))$$

die **Komposition** der Funktionen f und g .

Man liest $f \circ g$ als „f nach g“.

Man definiert die Potenzierung von Funktionen ähnlich der Mengentheorie.

$$f^0 := id$$

$$f^n := \underbrace{f \circ \dots \circ f}_{n \text{ mal}}$$

Dabei bezeichnet id die **Identität** mit $id(x) := x$.

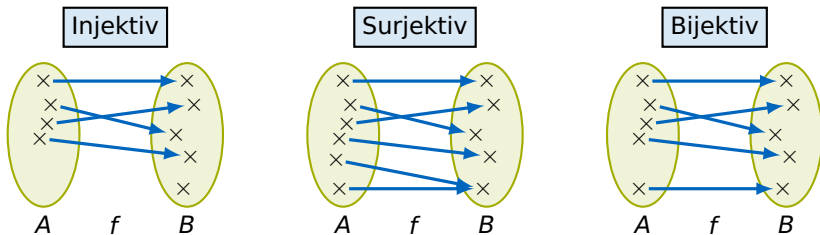
Eigenschaften von Funktionen

Sei $f : A \rightarrow B$ eine Funktion. Man nennt f

injektiv $\forall b \in B. |f^{-1}(b)| \leq 1$ (Kein b wird doppelt getroffen)

surjektiv $\forall b \in B. |f^{-1}(b)| \geq 1$ (Jedes b wird getroffen)

bijektiv $\forall b \in B. |f^{-1}(b)| = 1$ (Jedes b wird genau einmal getroffen)



Definition (Syntax der Aussagenlogik)

Aussagenlogische **Formeln** bestehen aus Konstanten, Variablen und Operatoren. Die Menge \mathcal{F} aller Formeln ist induktiv definiert.

■ $\text{false} = 0 = \perp \in \mathcal{F}$, $\text{true} = 1 = \top \in \mathcal{F}$ (Konstanten)

■ $V = \{a, b, c, \dots\} \subseteq \mathcal{F}$ (Variablen)

■ Ist $A \in \mathcal{F}$ eine aussagenlogische Formel, dann auch

$\neg A \in \mathcal{F}$ (Negation)

■ Sind $A, B \in \mathcal{F}$ aussagenlogische Formeln, dann auch

$(A \wedge B) \in \mathcal{F}$ (Konjunktion)

$(A \vee B) \in \mathcal{F}$ (Disjunktion)

$(A \rightarrow B) \in \mathcal{F}$ (Implikation)

Alle Formeln lassen sich so konstruieren.

Definition (Bindungsregeln)

Die **Bindungsstärke** der Operatoren in absteigender Reihenfolge ist

$$\neg \quad \wedge \quad \vee \quad \rightarrow \quad \leftrightarrow$$

Die Implikation ist **rechtsassoziativ**

$$a \rightarrow b \rightarrow c \rightarrow d \text{ steht für } (a \rightarrow (b \rightarrow (c \rightarrow d)))$$

- Üblicherweise klammert man \wedge und \vee

$$(a \wedge b) \vee c \text{ statt } a \wedge b \vee c$$

Beispiel

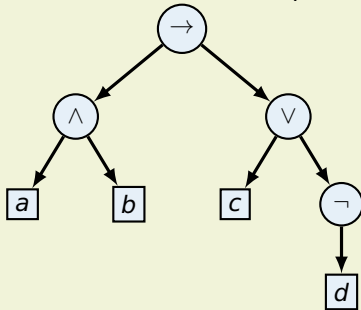
- $\neg a \wedge b$ steht für $((\neg a) \wedge b)$
- $a \wedge b \rightarrow c \vee \neg d$ steht für $((a \wedge b) \rightarrow (c \vee (\neg d)))$

Syntaxbaum

Syntaxbäume visualisieren in welcher Reihenfolge die Regeln zur induktiven Definition angewandt werden müssen, um eine Formel zu erzeugen.

Beispiel

Sei $F := a \wedge b \rightarrow c \vee \neg d$ dann ist der dazu passende Syntaxbaum



Definition (Belegung)

Eine passende **Belegung** β zu einer Formel F ordnet jeder Variable in V einen Wahrheitswert aus $\{0, 1\}$ zu. Es ist

$$\beta : V \rightarrow \{0, 1\}$$

- Belegungen formalisieren Einsetzen
- Für n Variablen existieren 2^n Belegungen

Beispiel

Sei $F := \neg(a \wedge b)$ mit $V = \{a, b\}$ und

$$\beta : \{a, b\} \rightarrow \{0, 1\}$$

$$a \mapsto 1$$

$$b \mapsto 0$$

Dann ist β eine zu F passende **Belegung**.

Definition (Semantik einer Formel)

Die **Semantik** $[F]$ einer aussagenlogischen Formel F ist eine Funktion, die jeder passenden Belegung β einen Wahrheitswert zuordnet. Sei $\mathcal{B} = \{\beta_0, \beta_1, \dots\}$ die Menge aller Belegungen zu F . Dann ist

$$[F] : \mathcal{B} \rightarrow \{0, 1\}$$

- Die Semantik löst eingesetzte Formeln auf
- Wird anhand der induktiven Syntax definiert
- Es gibt **syntaktisch verschiedene** Formeln gleicher **Semantik**

Beispiel

Sei $F := (G \rightarrow H)$ mit G, H Formeln. Dann ist

$$[F](\beta) = \begin{cases} 0 & \text{falls } [G](\beta) = 1 \text{ und } [H](\beta) = 0 \\ 1 & \text{sonst} \end{cases}$$

Wahrheitstabelle

Die Semantik einer Formel kann mit Hilfe einer **Wahrheitstabelle** visualisiert werden. Die Tabelle gibt den Wahrheitswert der Formel für jede mögliche Belegung an.

Beispiel

Sei $F := a \vee b \rightarrow \neg c \wedge b$. Die zu $[F]$ gehörige Wahrheitstabelle ist

a	b	c	$a \vee b$	\rightarrow	$\neg c$	\wedge	b
0	0	0	0	1	1	0	
0	0	1	0	1	0	0	
0	1	0	1	1	1	1	
0	1	1	1	0	0	0	
1	0	0	1	0	1	0	
1	0	1	1	0	0	0	
1	1	0	1	1	1	1	
1	1	1	1	0	0	0	

Wahrheitstabelle

Die Semantik einer Formel kann mit Hilfe einer **Wahrheitstabelle** visualisiert werden. Die Tabelle gibt den Wahrheitswert der Formel für jede mögliche Belegung an.

Beispiel

Sei $F := a \vee b \rightarrow \neg c \wedge b$. Die zu $[F]$ gehörige Wahrheitstabelle ist

a	b	c	$a \vee b$	\rightarrow	$\neg c$	\wedge	b
0	0	0	0	1	1	0	
0	0	1	0	1	0	0	
0	1	0	1	1	1	1	
0	1	1	1	0	0	0	
1	0	0	1	0	1	0	
1	0	1	1	0	0	0	
1	1	0	1	1	1	1	
1	1	1	1	0	0	0	

Wahrheitstabelle

Die Semantik einer Formel kann mit Hilfe einer **Wahrheitstabelle** visualisiert werden. Die Tabelle gibt den Wahrheitswert der Formel für jede mögliche Belegung an.

Beispiel

Sei $F := a \vee b \rightarrow \neg c \wedge b$. Die zu $[F]$ gehörige Wahrheitstabelle ist

a	b	c	$a \vee b$	\rightarrow	$\neg c$	\wedge	b
0	0	0	0	1	1	0	
0	0	1	0	1	0	0	
0	1	0	1	1	1	1	
0	1	1	1	0	0	0	
1	0	0	1	0	1	0	
1	0	1	1	0	0	0	
1	1	0	1	1	1	1	
1	1	1	1	0	0	0	

Definition (Äquivalente Formeln)

Man nennt zwei Formeln **äquivalent**, wenn sie dieselbe Semantik besitzen.

Seien F, G Formeln mit Belegungen $\mathcal{B} = \mathcal{B}_F = \mathcal{B}_G$. F und G sind äquivalent wenn

$$\forall \beta \in \mathcal{B}. [F](\beta) = [G](\beta)$$

Man schreibt $F \equiv G$ oder $F \leftrightarrow G$.

Beispiel

Für $F := a \rightarrow b$ und $G := \neg a \vee b$ gilt $F \equiv G$.

a	b	$a \rightarrow b$	$\neg a$	\vee	b
0	0	1	1	1	0
0	1	1	1	1	1
1	0	0	0	0	0
1	1	1	0	1	1

Eigenschaften aussagenlogischer Formeln

Sei F eine aussagenlogische Formel mit Variablen V und der Menge der passenden Belegungen \mathcal{B} . Man nennt F

erfüllbar $\exists \beta \in \mathcal{B}. [F](\beta) = 1$ (F kann wahr sein)

unerfüllbar $\forall \beta \in \mathcal{B}. [F](\beta) = 0$ (F ist nie wahr)

gültig $\forall \beta \in \mathcal{B}. [F](\beta) = 1$ (F ist immer wahr)

- Eine unerfüllbare Formel nennt man **Widerspruch**
- Eine gültige Formel nennt man **Tautologie**

Identität $F \wedge \text{true} \equiv F$

$F \vee \text{false} \equiv F$

Dominanz $F \vee \text{true} \equiv \text{true}$

$F \wedge \text{false} \equiv \text{false}$

Idempotenz $F \vee F \equiv F$

$F \wedge F \equiv F$

Doppelte Negation $\neg\neg F \equiv F$

Triviale Tautologie $F \vee \neg F \equiv \text{true}$

Triviale Kontradiktion $F \wedge \neg F \equiv \text{false}$

Kommutativität $F \vee G \equiv G \vee F$
 $F \wedge G \equiv G \wedge F$

Assoziativität $(F \vee G) \vee H \equiv F \vee (G \vee H)$
 $(F \wedge G) \wedge H \equiv F \wedge (G \wedge H)$

Distributivität $F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$
 $F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$

De Morgan $\neg(F \wedge G) \equiv \neg F \vee \neg G$
 $\neg(F \vee G) \equiv \neg F \wedge \neg G$

Implikation $F \rightarrow G \equiv \neg F \vee G$

Bikonditional $F \leftrightarrow G \equiv \neg(F \otimes G) [\equiv (F \rightarrow G) \wedge (G \rightarrow F)]$

Definition (Literal)

Ein **Literal** ist eine Variable $v \in V$ oder die Negation $\neg v$ einer Variable.

Definition (Klausel)

Eine **Klausel** verknüpft mehrere Literale mit einem assoziativen Operator.

Beispiel

Seien $a, \neg b, c$ Literale. Dann sind

- $a \wedge \neg b \wedge c$

- $a \vee \neg b \vee c$

Klauseln.

Definition (Disjunktive Normalform)

Eine **DNF-Klausel** ist eine Konjunktion von Literalen L_i .
Eine Formel F , ist in **Disjunktiver Normalform**, wenn sie eine Disjunktion von DNF-Klauseln ist.

$$F := \bigvee_i \bigwedge L_i$$

- Ausnahme: false ist auch in DNF

Beispiel

F ist in DNF.

$$F := \underbrace{(a \wedge b \wedge \neg c)}_{\text{DNF-Klausel}} \vee \underbrace{(\neg b \wedge c)}_{\text{DNF-Klausel}} \vee \underbrace{(\neg a \wedge b \wedge \neg c)}_{\text{DNF-Klausel}}$$

Definition (Konjunktive Normalform)

Eine **KNF-Klausel** ist eine Disjunktion von Literalen L_i .
Eine Formel F , ist in **Konjunktiver Normalform**, wenn sie eine Konjunktion von KNF-Klauseln ist.

$$F := \bigwedge_i \bigvee L_i$$

- Ausnahme: true ist auch in KNF

Beispiel

F ist in KNF.

$$F := \underbrace{(\neg a \vee b)}_{\text{KNF-Klausel}} \wedge \underbrace{(\neg b \vee c)}_{\text{KNF-Klausel}} \wedge \underbrace{(a \vee b \vee \neg c)}_{\text{KNF-Klausel}}$$

- Jede nicht-triviale Formel ist in DNF und KNF umwandelbar
- Durch Äquivalenzumformungen berechenbar (exponentiell groß!)
- Oder: Konstruktion mit Wahrheitstabellen

Normalformen aus Wahrheitstabellen

Gegeben eine Formel F und ihre Wahrheitstabelle

■ DNF

- 1 Betrachte Zeilen mit Eintrag 1
- 2 Bilde **Konjunktion** aus der **Belegung**
- 3 Bilde **Disjunktion** aller erhaltenen Klauseln

■ KNF

- 1 Betrachte Zeilen mit Eintrag 0
- 2 Bilde **Disjunktion** aus der **Negation** der Belegung
- 3 Bilde **Konjunktion** aller erhaltenen Klauseln

Beispiel

Gegeben eine Formel F mit folgender Semantik

a	b	c	F
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	0

F dargestellt in

■ DNF

$$(\neg a \wedge b \wedge c) \vee (a \wedge \neg b) \vee (a \wedge b \wedge \neg c)$$

■ KNF

$$(a \vee b) \wedge (\neg a \vee b \vee \neg c) \wedge (\neg a \vee \neg b \vee \neg c)$$

Mengendarstellung der KNF

Eine Formel $F = \bigwedge \bigvee L_i$ in KNF kann in einer Mengendarstellung repräsentiert werden.

- Klauseln werden durch Mengen von Literalen dargestellt

$$\{a, \neg b, c\} \text{ steht für } (a \vee \neg b \vee c)$$

- KNF-Formeln sind Mengen von Klauseln

$$\{\{\neg a\}, \{a, \neg b, c\}\} \text{ steht für } \neg a \wedge (a \vee \neg b \vee c)$$

- \emptyset steht für true, $\{\emptyset\}$ für false

Beispiel

Gegeben $F := (a \vee b) \wedge (\neg a \vee b \vee \neg c) \wedge (\neg a \vee \neg b \vee \neg c)$ in KNF.

$$\{\{a, b\}, \{\neg a, b, \neg c\}, \{\neg a, \neg b, \neg c\}\}$$

Idee

Erzeuge die KNF aus dem Syntaxbaum

- 1 Weise jedem **inneren Knoten** eine Variable zu
- 2 Variablen sind **abhängig** von ihren Kindern
- 3 Berechne **kleine** KNFs und führe diese **zusammen**

$$(x \wedge y) \vee z \equiv$$

$$\wedge (A_V \leftrightarrow A_\wedge \vee z)$$

$$\wedge (A_\wedge \leftrightarrow x \wedge y)$$

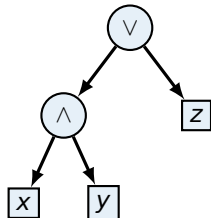
$$\equiv$$

$$\wedge (A_V \vee \neg A_\wedge) \wedge (A_V \vee \neg z)$$

$$\wedge (\neg A_V \vee A_\wedge \vee z)$$

$$\wedge (\neg A_\wedge \vee x) \wedge (\neg A_\wedge \vee y)$$

$$\wedge (A_\wedge \vee \neg x \vee \neg y)$$



Idee

Erzeuge die KNF aus dem Syntaxbaum

- 1 Weise jedem **inneren Knoten** eine Variable zu
- 2 Variablen sind **abhängig** von ihren Kindern
- 3 Berechne **kleine KNFs** und führe diese **zusammen**

$$(x \wedge y) \vee z \equiv$$

$$\wedge (A_V \leftrightarrow A_\wedge \vee z)$$

$$\wedge (A_\wedge \leftrightarrow x \wedge y)$$

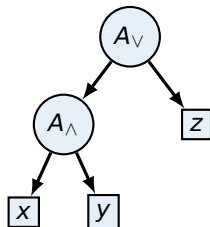
$$\equiv$$

$$\wedge (A_V \vee \neg A_\wedge) \wedge (A_V \vee \neg z)$$

$$\wedge (\neg A_V \vee A_\wedge \vee z)$$

$$\wedge (\neg A_\wedge \vee x) \wedge (\neg A_\wedge \vee y)$$

$$\wedge (A_\wedge \vee \neg x \vee \neg y)$$

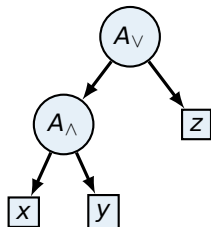


Idee

Erzeuge die KNF aus dem Syntaxbaum

- 1 Weise jedem **inneren Knoten** eine Variable zu
- 2 Variablen sind **abhängig** von ihren Kindern
- 3 Berechne **kleine KNFs** und führe diese **zusammen**

$$\begin{aligned}
 (x \wedge y) \vee z &\equiv A_V \\
 &\wedge (A_V \leftrightarrow A_\wedge \vee z) \\
 &\wedge (A_\wedge \leftrightarrow x \wedge y) \\
 &\equiv \\
 &\wedge (A_V \vee \neg A_\wedge) \wedge (A_V \vee \neg z) \\
 &\quad \wedge (\neg A_V \vee A_\wedge \vee z) \\
 &\wedge (\neg A_\wedge \vee x) \wedge (\neg A_\wedge \vee y) \\
 &\quad \wedge (A_\wedge \vee \neg x \vee \neg y)
 \end{aligned}$$

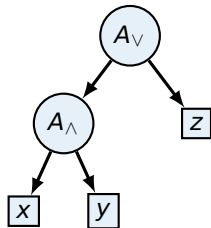


Idee

Erzeuge die KNF aus dem Syntaxbaum

- 1 Weise jedem **inneren Knoten** eine Variable zu
- 2 Variablen sind **abhängig** von ihren Kindern
- 3 Berechne **kleine** KNFs und führe diese **zusammen**

$$\begin{aligned}
 (x \wedge y) \vee z &\equiv A_V \\
 &\wedge (A_V \leftrightarrow A_\wedge \vee z) \\
 &\wedge (A_\wedge \leftrightarrow x \wedge y) \\
 &\equiv A_V \\
 &\wedge (A_V \vee \neg A_\wedge) \wedge (A_V \vee \neg z) \\
 &\quad \wedge (\neg A_V \vee A_\wedge \vee z) \\
 &\wedge (\neg A_\wedge \vee x) \wedge (\neg A_\wedge \vee y) \\
 &\quad \wedge (A_\wedge \vee \neg x \vee \neg y)
 \end{aligned}$$



Definition (DPLL-Belegung)

Sei F eine Formel in KNF und p eine Variable von F .
Dann bezeichnet $F[p \setminus \text{true}]$ die Formel, die entsteht, wenn jedes Vorkommen von p in F durch true ersetzt und vereinfacht wird.

DPLL

Gegeben eine Formel F in KNF

- Wenn $F = \text{true}$ dann antworte **erfüllbar**
- Wenn $F = \text{false}$ dann antworte **unerfüllbar**
- Sonst
 - 1 Wähle eine Variable p in F
 - 2 Prüfe ob $F[p \setminus \text{true}]$ oder $F[p \setminus \text{false}]$ erfüllbar

- Schlaue Wahl der Variable beschleunigt Ausführung
- Wähle Variablen die einzeln stehen (**One-Literal-Rule**)

Definition (Resolvent)

Seien K_1 , K_2 und R Klauseln in Mengendarstellung. Dann heißt R **Resolvent** von K_1 und K_2 wenn $L \in K_1$, $\neg L \in K_2$ und

$$R = (K_1 \setminus \{L\}) \cup (K_2 \setminus \{\neg L\})$$

Resolution

Gegeben eine Formel F in KNF in Mengendarstellung.

```
while  $\square = \emptyset \notin F$  do  
   $R \leftarrow$  Resolvent aus  $F$  mit  $R \notin F$   
  if  $R$  existiert then  
     $F \leftarrow F \cup R$   
  else  
    return erfüllbar  
return unerfüllbar
```

Definition (Kalkül)

Ein **Logikkalkül** stellt **Inferenzregeln** bereit, mit denen Formeln **syntaktisch** umgeformt werden können.

Definition (Folgerung)

F **folgt aus** A , wenn mit Hilfe der **Semantik** der **Aussagenlogik** F unter der Annahme dass A gilt zu true ausgewertet wird. Wir schreiben

$$A \models F$$

Definition (Ableitung)

F kann aus A **abgeleitet** werden, wenn mit Hilfe **syntaktischer** Umformungen in einem **Logikkalkül** F unter der Annahme A bewiesen werden kann. Wir schreiben

$$A \vdash F$$

Eigenschaften von Kalkülen

korrekt (sound) Es können **nur** semantisch gültige Formeln abgeleitet werden.

Aus $A \vdash F$ folgt $A \models F$

vollständig (complete) **Alle** semantisch gültigen Formeln können abgeleitet werden.

Aus $A \models F$ folgt $A \vdash F$

- Für uns nur korrekte vollständige Kalküle
- Beispiel für die Aussagenlogik: **Natürliches Schließen**
- Es gibt keine solchen Kalküle für die
 - Prädikatenlogik
 - Arithmetik
- Deshalb sind nicht alle Sätze der Mathematik beweisbar

	Introduktion	Elimination
\wedge	$\frac{\tau \quad \varphi}{\tau \wedge \varphi} +\wedge$	$\frac{\tau \wedge \varphi}{\tau} -\wedge_1 \quad \frac{\tau \wedge \varphi}{\varphi} -\wedge_2$
\vee	$\frac{\tau}{\tau \vee \varphi} +\vee_1 \quad \frac{\varphi}{\tau \vee \varphi} +\vee_2$	$\frac{\tau \vee \varphi \quad \boxed{\begin{array}{c} \tau \\ \vdots \\ \chi \end{array}} \quad \boxed{\begin{array}{c} \varphi \\ \vdots \\ \chi \end{array}}}{\chi} -\vee$
\rightarrow	$\frac{\boxed{\begin{array}{c} \tau \\ \vdots \\ \varphi \end{array}}}{\tau \rightarrow \varphi} +\rightarrow$	$\frac{\tau \quad \tau \rightarrow \varphi}{\varphi} -\rightarrow, \text{MP}$
\neg	$\frac{\boxed{\begin{array}{c} \tau \\ \vdots \\ \perp \end{array}}}{\neg \tau} +\neg$	$\frac{\tau \quad \neg \tau}{\perp} -\neg$

	Introduktion	Elimination
\perp		$\frac{\perp}{\tau} \text{ -- } \perp$
$\neg\neg$	$\frac{\tau}{\neg\neg\tau} \text{ ++}$	$\frac{\neg\neg\tau}{\tau} \text{ --}\neg$

■ Praktische abgeleitete Regeln

$$\frac{}{\tau \vee \neg\tau} \text{ LEM}$$

$$\frac{\boxed{\begin{array}{c} \neg\tau \\ \vdots \\ \perp \end{array}}}{\tau} \text{ --}\neg, \text{ PBC}$$

$$\frac{\neg\varphi \quad \tau \rightarrow \varphi}{\neg\tau} \text{ MT}$$

Definition (Term)

Die Menge \mathcal{T} aller **Terme** ist induktiv definiert.

- Jede Konstante ist in \mathcal{T}
- Jede Variable ist in \mathcal{T}
- Sind f eine Funktion und t_1, \dots, t_n Terme, dann auch

$$f(t_1, \dots, t_n)$$

Funktionen wandeln Terme in **Terme** um. Wir beschreiben sie mit Kleinbuchstaben.

Definition (Prädikat)

Prädikate P wandeln Terme in **Wahrheitswerte** um. Wir beschreiben sie mit Großbuchstaben.

Die Menge \mathcal{P} enthält alle **Prädikate**.

Definition (Syntax der Prädikatenlogik)

Die Menge \mathcal{L} aller **prädikatenlogischen Formeln** ist induktiv definiert. Seien $A, B \in \mathcal{L}$, $t_i \in \mathcal{T}$ und $P \in \mathcal{P}$. Dann sind alle Formeln

■ Grundbausteine

$$V = \{a, b, \dots\} \subseteq \mathcal{L} \quad (\text{Variablen})$$

$$P(t_1, \dots, t_n) \in \mathcal{L} \quad (\text{Prädikate, Konstanten})$$

$$t_i = t_j \in \mathcal{L} \quad (\text{Gleichheit})$$

■ Verknüpfungen der Aussagenlogik

$$\neg A \in \mathcal{L} \quad (\text{Negation})$$

$$(A \wedge B), (A \vee B) \in \mathcal{L} \quad (\text{Konjunktion, Disjunktion})$$

$$(A \rightarrow B) \in \mathcal{L} \quad (\text{Implikation})$$

■ Quantoren

$$\exists x.A \in \mathcal{L} \quad (\text{Existenzquantor})$$

$$\forall x.A \in \mathcal{L} \quad (\text{Allquantor})$$

Definition (Bindungsregeln)

Die **Bindungsstärke** der Operatoren in absteigender Reihenfolge ist

$$\forall \exists \neg \wedge \vee \rightarrow \leftrightarrow$$

Die Implikation ist **rechtsassoziativ**.

- Üblicherweise klammert man wieder \wedge und \vee
- Genauso klammert man Quantoren

$$(\forall x.F) \rightarrow G \quad \text{statt} \quad \forall x.F \rightarrow G$$

- **Achtung!** Äußere Quantoren werden öfter anders interpretiert

$$\forall x \forall y.F \wedge G \leftrightarrow H$$

Bindet formal **nur an das F!**

Definition (Struktur)

Eine passende **Struktur** $S = (U_S, I_S)$ zu einer Formel F besteht aus einem **Universum** U_S und einer **Interpretation** I_S .

- Alle Terme werten zu einem Wert im **Universum** U_S aus
- Die **Interpretation** I_S weist den Atomen der Formel Werte zu. Sie spezifiziert

- **Variablen** x mit

$$x_S \in U_S$$

- **Konstanten** a mit

$$a_S \in U_S$$

- **k-stellige Prädikate** P mit

$$P_S \subseteq U_S^k$$

- **Funktionen** f mit

$$f_S : U_S^k \rightarrow U_S$$

Definition (Ersetzung)

Sei φ eine Formel und a eine Konstante.

Mit $\varphi[x/a]$ bezeichnen wir die Formel die man erhält, wenn man alle **freien** Vorkommnisse von x in φ durch a ersetzt.

	Introduktion	Elimination
\exists	$\frac{\tau[x/a]}{\exists x.\tau} \quad +\exists$	$\frac{\exists x.\tau \quad \boxed{\begin{array}{c} a.\tau[x/a] \\ \vdots \\ \chi \end{array}}}{\chi} \quad -\exists$
\forall	$\frac{\boxed{\begin{array}{c} a \\ \vdots \\ \tau[x/a] \end{array}}}{\forall x.\tau} \quad +\forall$	$\frac{\forall x.\tau}{\tau[x/a]} \quad -\forall$

- Man muss ein **unbenutztes** a in $+\forall$ und $-\exists$ wählen

Vollständige Induktion

Die **vollständige Induktion** ist eine Beweistechnik, um zu zeigen, dass alle natürlichen Zahlen ein Prädikat P erfüllen.

$$\forall n \in \mathbb{N}_0. P(x)$$

Ein solcher Beweis besteht aus

Induktionsanfang Man zeigt, dass $P(0)$ gilt.

Induktionsschritt Man zeigt für ein beliebiges k , dass wenn $P(k)$ gilt (**Induktionshypothese**), dann auch $P(k+1)$.

Zusammen beweisen die Teile, dass das Prädikat für alle $n \in \mathbb{N}_0$ gilt.

In Prädikatenlogik formuliert gilt in \mathbb{N}_0

$$P(0) \wedge \forall k. (P(k) \rightarrow P(k+1)) \rightarrow \forall n. P(n)$$

- Kann verallgemeinert werden, z.B. auf \mathbb{Z}
- Aber nicht auf \mathbb{R} (Warum?)

Definition (Wohlfundierte Relation)

Eine Relation $\prec \subseteq A \times A$ heißt **wohlfundiert**, wenn keine **unendlichen Folgen** von Elementen $a_1, a_2, a_3, \dots \in A$ existieren, sodass

$$a_1 \succ a_2 \succ a_3 \succ \dots$$

Jede Kette hat ein **unteres Ende**.

Beispiel

- $\prec_1 := \{(a, b) \in \mathbb{N}^2 \mid a < b\}$ ist wohlfundiert.
- $\prec_2 := \{(a, b) \in \mathbb{N}^2 \mid a > b\}$ ist **nicht** wohlfundiert.
- $\prec_3 := \{(a, b) \in \mathbb{Z}^2 \mid a < b\}$ ist **nicht** wohlfundiert.
- $\prec_4 := \{(a, b) \in \mathbb{N}^2 \mid \exists x. x \text{ teilt } a \wedge x \text{ teilt } b\}$ ist **nicht** wohlfundiert.
- $\prec_5 := \emptyset$ ist wohlfundiert.

Wohlfundierte Induktion

Die **wohlfundierte Induktion** verallgemeinert die vollständige Induktion.

Um für eine Menge A mit wohlfundierter Relation \prec ein Prädikat

$$\forall a \in A. P(a)$$

zu zeigen, beweist man

Induktionsanfang Man zeigt, dass für alle bezüglich \prec **minimalen** Elemente m_i das Prädikat gilt.

Induktionsschritt Man zeigt, dass wenn **alle kleineren** Elemente als n das Prädikat erfüllen, so auch n .

In Prädikatenlogik formuliert gilt

$$\forall a \in A. (\forall b \prec a. P(b) \rightarrow P(a)) \quad \text{gdw.} \quad \forall a \in A. P(a)$$

- Wo ist der Induktionsanfang?

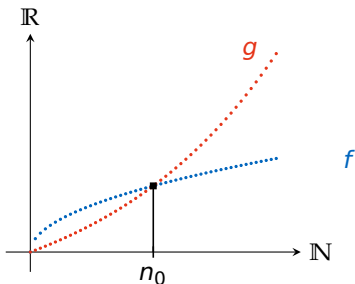
Definition (Asymptotisches Verhalten)

Eine Funktion g ist **asymptotisch größer** (wächst asymptotisch **schneller**) als eine andere Funktion f , wenn gilt

$$\exists n_0 > 0 \forall n \geq n_0. |f(n)| < |g(n)|$$

- Der Einfachheit halber betrachten wir **strikt positive** Funktionen
- Dann sind die Beträge egal

- Oftmals sind **Vorfaktoren** nicht interessant



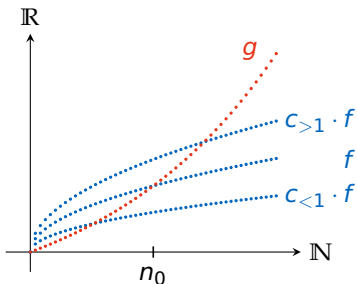
Definition (Asymptotisches Verhalten)

Eine Funktion g ist **asymptotisch größer** (wächst asymptotisch **schneller**) als eine andere Funktion f , wenn gilt

$$\exists n_0 > 0 \forall n \geq n_0. |f(n)| < |g(n)|$$

- Der Einfachheit halber betrachten wir **strikt positive** Funktionen
- Dann sind die Beträge egal

- Oftmals sind **Vorfaktoren** nicht interessant



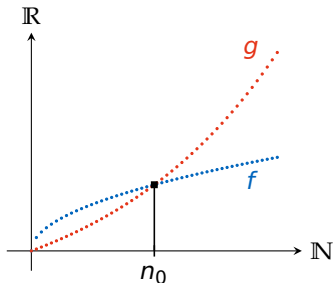
Definition (Asymptotische obere Schranke)

Seien f, g **strikt positiv**. Eine Funktion f wächst **asymptotisch maximal so schnell** wie eine Funktion g , wenn gilt

$$\exists c > 0 \exists n_0 > 0 \forall n \geq n_0. f(n) \leq c \cdot g(n)$$

wir schreiben dann

$$f \in \mathcal{O}(g)$$



- $\mathcal{O}(g)$ ist eine Menge von Funktionen ...
- ... die maximal so schnell wachsen wie g

Definition (Landausymbole)

Seien f, g **strikt positiv**. Analog zu $\mathcal{O}(g)$ definiert man weitere Mengen von Funktionen.

$$o(g) := \{f \mid \forall c > 0 \exists n_0 > 0 \forall n \geq n_0. f(n) < c \cdot g(n)\} \quad (\text{langsamer})$$

$$\mathcal{O}(g) := \{f \mid \exists c > 0 \exists n_0 > 0 \forall n \geq n_0. f(n) \leq c \cdot g(n)\} \quad (\text{nicht schneller})$$

$$\Theta(g) := \mathcal{O}(g) \cap \Omega(g) \quad (\text{gleich schnell})$$

$$\Omega(g) := \{f \mid \exists c > 0 \exists n_0 > 0 \forall n \geq n_0. f(n) \geq c \cdot g(n)\} \quad (\text{nicht langsamer})$$

$$\omega(g) := \{f \mid \forall c > 0 \exists n_0 > 0 \forall n \geq n_0. f(n) > c \cdot g(n)\} \quad (\text{schneller})$$

Es ist

$$o(g) \subseteq \mathcal{O}(g)$$

$$o(g) \cap \Omega(g) = \emptyset$$

$$\omega(g) \subseteq \Omega(g)$$

$$\omega(g) \cap \mathcal{O}(g) = \emptyset$$

Satz (Landausymbole mit Grenzwerten)

Existiert der Grenzwert $\lim_{n \rightarrow \infty} \left| \frac{f(n)}{g(n)} \right|$, dann gilt

$f \in o(g)$	gdw.	$\lim_{n \rightarrow \infty} \left \frac{f(n)}{g(n)} \right = 0$
$f \in \mathcal{O}(g)$	gdw.	$0 \leq \lim_{n \rightarrow \infty} \left \frac{f(n)}{g(n)} \right < \infty$
$f \in \Theta(g)$	gdw.	$0 < \lim_{n \rightarrow \infty} \left \frac{f(n)}{g(n)} \right < \infty$
$f \in \Omega(g)$	gdw.	$0 < \lim_{n \rightarrow \infty} \left \frac{f(n)}{g(n)} \right \leq \infty$
$f \in \omega(g)$	gdw.	$\lim_{n \rightarrow \infty} \left \frac{f(n)}{g(n)} \right = \infty$

Definition (Fakultät)

Die **Fakultät** $n!$ einer natürlichen Zahl $n \in \mathbb{N}_0$ ist

$$n! := \prod_{i=1}^n i = n \cdot (n-1) \cdot \dots \cdot 1$$

mit $0! := 1$.

Definition (Steigende und fallende Faktorielle)

Für $n, m \in \mathbb{N}_0$ mit $m \leq n$ ist

$$\begin{aligned} n^{\underline{m}} &:= \frac{n!}{(n-m)!} && \text{(fallende Faktorielle)} \\ &= n \cdot (n-1) \cdot \dots \cdot (n-m+1) \end{aligned}$$

$$\begin{aligned} n^{\overline{m}} &:= \frac{(n+m-1)!}{(n-1)!} && \text{(steigende Faktorielle)} \\ &= n \cdot (n+1) \cdot \dots \cdot (n+m-1) \end{aligned}$$

Definition (Binomialkoeffizient)

Der **Binomialkoeffizient** $\binom{n}{k}$ gibt die Anzahl der k -elementigen Teilmengen einer n -elementigen Menge an.

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n^{\underline{k}}}{k!}$$

Man sagt n über k oder k aus n .

- $\binom{n}{k}$ viele Möglichkeiten, k Elemente aus n Elementen zu wählen

Satz (Pascalsche Identität)

Die *Pascalsche Identität* liefert eine rekursive Definition des Binomialkoeffizienten.

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

Definition (Multimenge)

Multimengen sind eine Verallgemeinerung gewöhnlicher Mengen. Elemente können nun mehrfach vorkommen, die Reihenfolge spielt weiterhin keine Rolle.

Sie werden meist auch mit $\{\cdot\}$ notiert, alternativ $\{\cdot\}$.

Satz (Anzahl von Multiteilmengen)

Eine *k -Multiteilmenge* von M mit $|M| = n$ ist eine Multimenge, die k (nicht unbedingt verschiedene) Elemente aus M enthält.

Es gibt

$$\binom{k+n-1}{k} = \binom{k+n-1}{n-1}$$

solche Multiteilmengen.

Beispiel

■ $M := \{1, 2, 2, 2, 3\} = \{2, 1, 2, 3, 2\} \quad |M| = 5$

Doppeltes Abzählen

Ermittelt man die **Mächtigkeit** einer Menge auf zwei Arten, so müssen beide Ergebnisse **übereinstimmen**.

Eine so ermittelte Gleichung kann die gesuchte Mächtigkeit festlegen.

Beispiel (Matrizen)

In einer Matrix müssen die Summen von Zeilensummen und Spaltensummen übereinstimmen.

Beispiel (Studenten)

In einer Vorlesung sitzen **64 Studenten** und **n Studentinnen**. Jeder Student kennt genau **5 Studentinnen** und jede Studentin **8 Studenten**. Wenn „bekannt sein“ symmetrisch ist, wie viele Studentinnen besuchen die Vorlesung?

$$64 \cdot 5 = n \cdot 8$$

$$n = \frac{64 \cdot 5}{8} = 40$$

Definition (Schubfachprinzip)

Sei $f : X \rightarrow Y$ eine Abbildung und $|X| > |Y|$.
Dann gilt

$$\exists y \in Y. |f^{-1}(y)| \geq 2$$

Wenn man n Elemente auf $m < n$ Fächer verteilt, dann gibt es **mindestens ein Fach**, das mindestens **2** Elemente enthält.

Definition (Verallgemeinertes Schubfachprinzip)

Sei $f : X \rightarrow Y$ eine Abbildung und $|X| > |Y|$.
Dann gilt

$$\exists y \in Y. |f^{-1}(y)| \geq \left\lceil \frac{|X|}{|Y|} \right\rceil$$

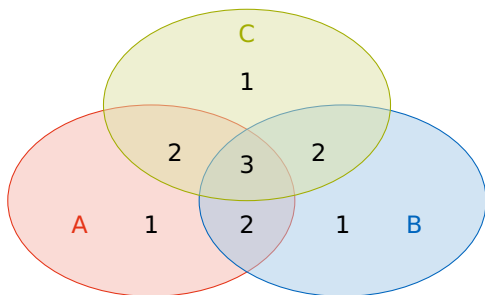
Wenn man n Elemente auf $m < n$ Fächer verteilt, dann gibt es **mindestens ein Fach**, das mindestens $\left\lceil \frac{|X|}{|Y|} \right\rceil$ Elemente enthält.

Inklusion und Exklusion

Das Prinzip der **Inklusion und Exklusion** erweitert die Summenregel um **nicht disjunkte** Mengen.

Für drei Mengen A, B, C gilt

$$\begin{aligned} |A \cup B \cup C| &= |A| + |B| + |C| \\ &\quad - |A \cap B| - |A \cap C| - |B \cap C| \\ &\quad + |A \cap B \cap C| \end{aligned}$$



Definition (k -Partition)

Eine k -Partition einer Menge A ist eine Zerlegung von A in k **disjunkte, nichtleere Teilmengen** A_1, \dots, A_k mit

$$\bigsqcup_{i=1}^k A_i = A$$

Dabei bezeichnet \sqcup die disjunkte Vereinigung.

Beispiel

Einige mögliche 3 -Partitionen von $[5]$ sind

$$\begin{array}{ll} \{\{1, 2\}, \{3, 4\}, \{5\}\} & \{\{1\}, \{3, 4\}, \{2, 5\}\} \\ \{\{1, 2, 3\}, \{4\}, \{5\}\} & \{\{1, 5\}, \{2, 4\}, \{3\}\} \end{array}$$

Es existieren genau 25 solche 3 -Partitionen.

Definition (Stirlingzahlen zweiter Art)

Die **Stirlingzahl zweiter Art** $S_{n,k}$ gibt die Anzahl der k -Partitionen einer n -elementigen Menge an. Wir schreiben

$$\left\{ \begin{matrix} n \\ k \end{matrix} \right\} := S_{n,k}$$

Es ist

$$\left\{ \begin{matrix} n \\ k \end{matrix} \right\} = \left\{ \begin{matrix} n-1 \\ k-1 \end{matrix} \right\} + k \cdot \left\{ \begin{matrix} n-1 \\ k \end{matrix} \right\}$$

- $\left\{ \begin{matrix} n \\ k \end{matrix} \right\}$ viele Möglichkeiten, n unterscheidbare Objekte in k gleiche Fächer zu verteilen, sodass jedes Fach ein Objekt bekommt

Beispiel

- Es gibt $\left\{ \begin{matrix} 5 \\ 3 \end{matrix} \right\} = 25$ 3-Partitionen von $[5]$.

Definition (Permutation)

Eine **Permutation** einer Menge $A = \{a_1, \dots, a_n\}$ ist eine **bijektive Abbildung** $\pi : A \rightarrow A$.

Wir notieren Permutationen in zweizeiligen Vektoren.

$$\pi = \begin{pmatrix} a_1 & \dots & a_n \\ \pi(a_1) & \dots & \pi(a_n) \end{pmatrix}$$

- Weist jedem Element in A ein neues, eindeutiges Element in A zu.
- „Mischt“ die Elemente einer Menge

Beispiel

π ist eine Permutation auf $[9]$.

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 4 & 7 & 2 & 6 & 1 & 9 & 8 \end{pmatrix}$$

Es ist $\pi(1) = 3$, $\pi(4) = 7$.

Definition (k -Zyklus)

Ein k -Zyklus ist eine Permutation π , die k verschiedene Zahlen i_1, \dots, i_k im Kreis vertauscht.

$$\pi = \begin{pmatrix} i_1 & i_2 & \dots & i_k \\ i_2 & i_3 & \dots & i_1 \end{pmatrix}$$

Wir schreiben auch

$$\pi = (i_1 \ i_2 \ \dots \ i_k)$$

Jede Permutation ist eine Verkettung disjunkter Zyklen.

Beispiel

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 4 & 7 & 2 & 6 & 1 & 9 & 8 \end{pmatrix}$$

π enthält vier Zyklen.

$$\pi = (1 \ 3 \ 4 \ 7) (2 \ 5) (6) (8 \ 9)$$

Definition (Stirlingzahlen erster Art)

Die **Stirlingzahl erster Art** $s_{n,k}$ gibt die Anzahl der Permutationen mit n Elementen und k **Zyklen** an. Wir schreiben

$$\begin{bmatrix} n \\ k \end{bmatrix} := s_{n,k}$$

Es ist

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + (n-1) \cdot \begin{bmatrix} n-1 \\ k \end{bmatrix}$$

- Es gilt $\sum_{k=1}^n \begin{bmatrix} n \\ k \end{bmatrix} = n!$

Beispiel

- Es gibt $\begin{bmatrix} 9 \\ 4 \end{bmatrix} = 67284$ Permutationen über $[9]$ mit **vier Zyklen**.

Definition (Graph)

Ein (einfacher, ungerichteter) Graph $G = (V, E)$ ist ein Zweitupel aus Knotenmenge V und Kantenmenge $E \subseteq \binom{V}{2}$.

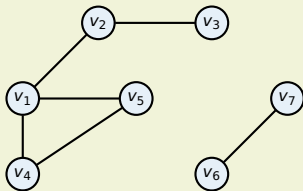
- $\binom{V}{2}$ ist Notation für alle zweielementigen Teilmengen.
- V für Vertices, E für Edges

Beispiel

$$G = (V, E)$$

$$V = \{v_1, v_2, v_3, v_4, v_5, v_6, v_7\}$$

$$E = \{\{v_1, v_2\}, \{v_1, v_4\}, \\ \{v_1, v_5\}, \{v_2, v_3\}, \\ \{v_4, v_5\}, \{v_6, v_7\}\}$$



Definition (Vollständiger Graph)

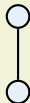
Im **vollständigen Graphen** K_n mit n Knoten sind alle Knoten durch Kanten verbunden.

- Er enthält $\binom{n}{2} = \frac{n(n-1)}{2}$ Kanten.

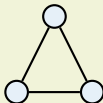
Beispiel



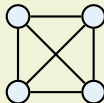
K_1



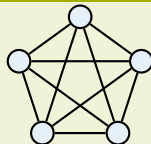
K_2



K_3



K_4



K_5

Definition (k -Weg)

Ein k -Weg in einem Graphen $G = (V, E)$ ist eine nichtleere Folge von Knoten $(v_0, \dots, v_k) \in V^{k+1}$ von $k + 1$ Knoten, sodass zwischen aufeinanderfolgenden Knoten Kanten existieren.

$$\forall i \in \mathbb{Z}_k. \{v_i, v_{i+1}\} \in E$$

(v_0) bezeichnet einen 0-Weg.

Definition (k -Pfad)

Ein k -Pfad in G ist ein k -Weg in G , in dem kein Knoten mehrfach vorkommt.

Definition (k -Kreis)

Ein k -Kreis ($k \geq 3$) in G ist ein k -Weg (v_0, \dots, v_k) in G , wobei v_0, \dots, v_{k-1} paarweise verschieden sind und $v_0 = v_k$ gilt.

Sei $G = (V, E)$ ein Graph und $v \in V$.

Definition (Nachbarschaft)

Die **Nachbarschaft** $\Gamma(v)$ eines Knotens v ist die Menge aller Knoten, die mit v über eine Kante verbunden sind.

$$\Gamma(v) = \{u \in V \mid \{v, u\} \in E\}$$

Definition (Grad)

Der **Grad** $\deg(v)$ bezeichnet die Anzahl der Nachbarn von v .

$$\deg(v) = |\Gamma(v)|$$

Aus v führen genau $\deg(v)$ Kanten heraus.

Definition (k -regulär)

Haben alle Knoten in G den Grad k , so nennen wir G **k -regulär**.

Sei $G = (V, E)$ ein Graph.

Definition (Erreichbarkeit)

Ein Knoten $u \in V$ ist von $v \in V$ **erreichbar**, wenn es in G einen Pfad von u nach v gibt.

Definition (Zusammenhangskomponente)

Eine **Zusammenhangskomponente** ist eine **maximale** Teilmenge von Knoten in der sich alle Knoten erreichen.

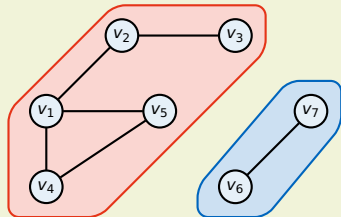
G heißt **zusammenhängend**, wenn nur eine solche Komponente existiert.

Beispiel

- G hat zwei Komponenten

$$\{v_1, v_2, v_3, v_4, v_5\}, \\ \{v_6, v_7\}$$

- G ist nicht zusammenhängend



Definition (Baum)

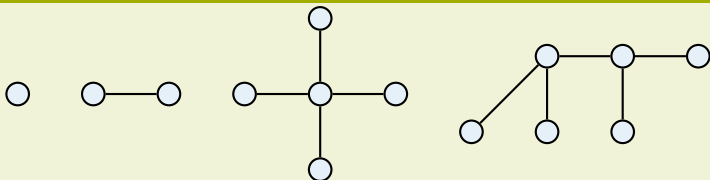
Ein ungerichteter Graph heißt **Baum**, falls er zusammenhängend und kreisfrei ist.

Definition (Wald)

Ein ungerichteter Graph heißt **Wald**, wenn seine Zusammenhangskomponenten Bäume sind.

- Wir nennen Knoten von Grad 1 **Blätter**
- Alle anderen Knoten heißen **innere Knoten**

Beispiel



Prüfercode

Der **Prüfer-Code** zu einem Baum $T = (V, E)$ mit Knotenmenge $V = [n]$ ist ein $(n - 2)$ -Tupel mit Elementen aus V .

Es gilt

- Jedem Baum kann genau ein Prüfer-Code zugeordnet werden
- Jeder Prüfer-Code stellt genau einen Baum dar

Damit wird eine Bijektion zwischen Tupeln und Bäumen definiert.

Satz (Satz von Cayley)

Es gibt genau n^{n-2} Bäume mit n Knoten.

Baum \rightarrow Code

Gegeben ein Baum $T = (V, E)$ mit $|V| = n$, finde Code (c_1, \dots, c_{n-2}) .

for $i \leftarrow 1, n-2$ **do**

$m \leftarrow \min \{v \in V \mid v \text{ ist Blatt}\}$

$V \leftarrow V \setminus \{m\}$

$c_i \leftarrow \text{parent}(m)$

Finde kleinstes Blatt

Entferne es aus T

Addiere seinen Vater zum Code

Code \rightarrow Baum

Gegeben ein Code (c_1, \dots, c_{n-2}) , finde Baum $T = (V, E)$.

$V \leftarrow [n]$

n Knoten

$E \leftarrow \emptyset$

Keine Kanten

$M \leftarrow \emptyset$

Keine markierten Knoten

for $i \leftarrow 1, n-2$ **do**

$X_i \leftarrow \{c_i, \dots, c_{n-2}\} \cup M$

Finde unmögliche Knoten

$v_i \leftarrow \min([n] \setminus X_i)$

Finde kleinsten möglichen Knoten

$E \leftarrow E \cup \{c_i, v_i\}$

Füge Kante $\{c_i, v_i\}$ hinzu

$M \leftarrow M \cup \{v_i\}$

Markiere v_i

$E \leftarrow E \cup (V \setminus M)$

Verbinde die 2 unmarkierten Knoten

Definition (Gradfolge)

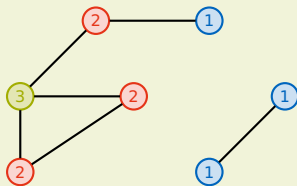
Sei $G = (V, E)$ ein ungerichteter einfacher Graph mit $|V| = n$.
Seine **Gradfolge** ist ein n -Tupel, das seine Grade enthält.

$$(\deg(v_1), \deg(v_2), \dots, \deg(v_n))$$

Üblicherweise werden Gradfolgen **aufsteigend** sortiert.

Beispiel

- $|V| = 7$
- Gradfolge $(1, 1, 1, 2, 2, 2, 3)$



Definition (Teilgraph)

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

Zu G heißt G'

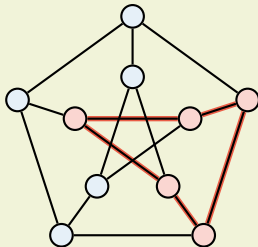
Teilgraph wenn $V' \subseteq V$ und $E' \subseteq E$.

Induzierter Teilgraph wenn $V' \subseteq V$ und $E' = \binom{V'}{2} \cap E$.

- Der induzierte Teilgraph ist der zu einer Knotenmenge kantenmaximale Teilgraph.

Beispiel

- Petersen-Graph G
- Induzierter Teilgraph G'

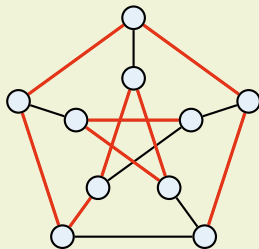
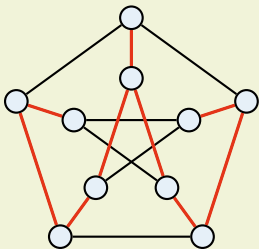


Definition (Spannbaum)

Ein Teilgraph $T' = (V', E')$ heißt **Spannbaum** von $G = (V, E)$ wenn T' ein **Baum** ist und $|V'| = |V|$ gilt.

- Spannäume sind nicht eindeutig
- Jeder zusammenhängende Graph hat mindestens einen Spannbaum

Beispiel



Definition (Euler-Tour)

Eine **Euler-Tour** in einem Graphen ist ein Weg, der jede Kante **genau einmal** enthält und dessen Anfangs- und Endknoten identisch sind. Ein Graph, der eine Euler-Tour besitzt, heißt **eulersch**.

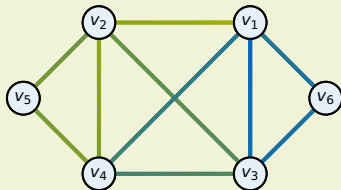
Satz (Euler)

*Ein zusammenhängender Graph besitzt genau dann eine **Euler-Tour**, wenn alle Knoten des Graphen **geraden Grad** haben.*

Beispiel

■ Eulertour

$(v_1, v_2, v_4, v_5, v_2, v_3,$
 $v_4, v_1, v_6, v_3, v_1)$



Definition (Gerichteter Graph)

Ein (einfacher) **gerichteter Graph** $G = (V, E)$ ist ein Zweitupel aus **Knotenmenge** V und **Kantenmenge** $E \subseteq V \times V$.

Dabei bezeichnet ein Tupel $(v_1, v_2) \in E$ eine Kante von v_1 nach v_2 .

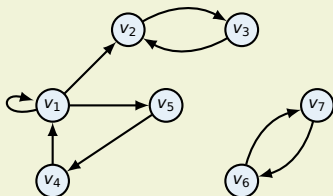
- Schleifen sind erlaubt
- Kanten in beide Richtungen sind erlaubt

Beispiel

$$G = (V, E)$$

$$V = \{v_1, v_2, v_3, v_4, v_5, v_6, v_7\}$$

$$E = \{(1, 1), (1, 2), (2, 3), (2, 3), (3, 2), (1, 5), (4, 1), (5, 4), (6, 7), (7, 6)\}$$



Definition (k -Färbbarkeit)

Ein Graph $G = (V, E)$ heißt k -färbbar, wenn es eine Abbildung $f : V \rightarrow [k]$ gibt, sodass

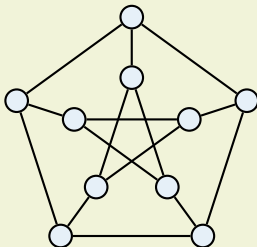
$$\forall v \in V \forall w \in \Gamma(v). f(v) \neq f(w)$$

Die **chromatische Zahl** $\chi(G)$ ist das kleinste k , sodass G k -färbbar ist.

- Ordne jedem Knoten eine Farbe zu
- Benachbarte Knoten haben unterschiedliche Farben

Beispiel

- G ist 3-färbbar
- G ist auch 4-färbbar
- $\chi(G) = 3$



Definition (k -Färbbarkeit)

Ein Graph $G = (V, E)$ heißt k -färbbar, wenn es eine Abbildung $f : V \rightarrow [k]$ gibt, sodass

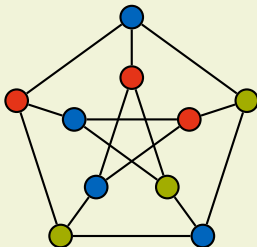
$$\forall v \in V \forall w \in \Gamma(v). f(v) \neq f(w)$$

Die **chromatische Zahl** $\chi(G)$ ist das kleinste k , sodass G k -färbbar ist.

- Ordne jedem Knoten eine Farbe zu
- Benachbarte Knoten haben unterschiedliche Farben

Beispiel

- G ist 3-färbbar
- G ist auch 4-färbbar
- $\chi(G) = 3$



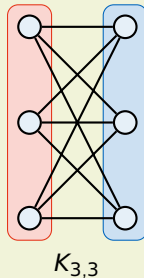
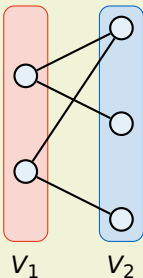
Definition (Bipartiter Graph)

Ein Graph $G = (V, E)$ heißt **bipartit** gdw. es eine Partitionierung $V = V_1 \uplus V_2$ gibt, sodass jede Kante zwei Knoten in **unterschiedlichen Klassen** verbindet.

$$\forall \{v_1, v_2\} \in E. v_1 \in V_1 \wedge v_2 \in V_2$$

- G ist bipartit gdw. $\chi(G) = 2$

Beispiel



Definition (Planarität)

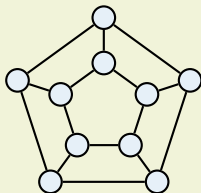
Ein Graph heißt **planar**, wenn er so in eine Ebene gezeichnet werden kann, dass sich keine Kanten schneiden.

Satz (Kuratowski)

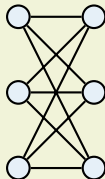
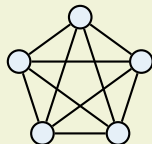
Ein Graph ist genau dann **nicht planar**, wenn er einen Teilgraphen enthält, der eine **Unterteilung** des K_5 oder des $K_{3,3}$ ist.

Beispiel

Planar



Nicht planar

 $K_{3,3}$  K_5

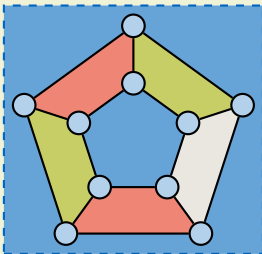
Satz (Eulersche Polyederformel)

Für einen zusammenhängenden planaren Graphen $G = (V, E)$ gilt

$$|F| - |E| + |V| - 2 = 0$$

Dabei ist $|F|$ die Anzahl von Flächen inklusive der äußeren Fläche.

Beispiel



- $|V| = 10$
- $|E| = 15$
- $|F| = 7$

Definition (Modulo-Kongruenz)

Zwei Zahlen $a, b \in \mathbb{Z}$ heißen **kongruent Modulo** $n \in \mathbb{N}$, falls

$$\exists k \in \mathbb{Z}. a = k \cdot n + b$$

Wir schreiben dann $a \equiv b \pmod{n}$ oder $a \equiv_n b$.
Durch \equiv_n wird eine **Äquivalenzrelation** definiert.

Definition (Modulo-Operator)

Der **Modulo-Operator** ordnet jeder Zahl $a \in \mathbb{Z}$ seine Äquivalenzklasse (**Restklasse**) Modulo $n \in \mathbb{N}$ zu. Es gilt

$$a \bmod n = r \quad \text{gdw.} \quad \exists q \in \mathbb{Z}. a = q \cdot n + r \quad \text{mit} \quad 0 \leq r < n$$

Modulo gibt den **Rest** bei einer **Ganzzahldivision** zurück.

Beispiel

$$5 \bmod 3 = 2$$

$$6 \bmod 3 = 0$$

$$-5 \bmod 3 = 1$$

Definition (Algebra)

Eine **Algebra** $\langle M, (\circ_i)_{i \in I} \rangle$ besteht aus einer Menge von Operanden und einer oder mehrerer innerer Verknüpfungen.

Eine **innere Verknüpfung** auf M ist eine Abbildung

$$\circ : M \times M \rightarrow M$$

Eine Verknüpfung heißt

assoziativ wenn $(a \circ b) \circ c = a \circ (b \circ c)$

kommutativ wenn $a \circ b = b \circ a$

für alle $a, b, c \in M$.

Beispiel

Einige Beispiele für Algebren sind (mit üblichen Verknüpfungen)

- $\langle \mathbb{Z}, +, \cdot \rangle$ die ganzen Zahlen
- $\langle \mathbb{Z}_{11}, +_{11} \rangle$ die Restklassen Modulo 11
- $\langle \mathbb{R}^3, +, \cdot \rangle$ der 3-Dimensionale \mathbb{R} -Vektorraum

Definition (Gruppe)

Eine Algebra $\langle G, \circ, e \rangle$ heißt **Gruppe**, wenn für alle $a, b, c \in G$ gilt

Assoziativität $(a \circ b) \circ c = a \circ (b \circ c)$

Neutrales Element Für e gilt $a \circ e = e \circ a = a$

Inverse Elemente Es gibt a^{-1} mit $a \circ a^{-1} = a^{-1} \circ a = e$

Wir schreiben auch kurz G .

Wir nennen G **abelsch (oder kommutativ)**, wenn \circ kommutativ ist.

Beispiel

Die Menge $[4]$ zusammen mit der Multiplikation modulo 5 beschreibt die Gruppe $\langle [4], \cdot_5, 1 \rangle = \mathbb{Z}_5^*$.

\cdot_5	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

- Erfüllt „Sudokuprinzip“
- Multiplikation ist assoziativ
- 1 ist neutrales Element
- Inverse existieren
- Kommutativ da symmetrisch

Definition (Untergruppe)

Sei G eine Gruppe und $H \subseteq G$ eine Teilmenge.
 H heißt **Untergruppe** von G , wenn für $a, b \in H$ gilt

Abgeschlossenheit $a \circ b \in H$

Inverse $a^{-1} \in H$

Wir schreiben $H < G$.

- Um zu zeigen dass $H < G$ gilt, reicht es zu zeigen dass

$$a, b \in H \rightarrow ab^{-1} \in H$$

- Jede Gruppe enthält $\{e\}$ und sich selbst als Untergruppe

Beispiel

Betrachte $G = \langle \mathbb{Z}_{10}, +_{10}, 0 \rangle$ die Restklassen Modulo 10.

Dann ist $H = \langle \{0, 2, 4, 6, 8\}, +_{10}, 0 \rangle$ eine Untergruppe von G , da die Summe zweier gerader Zahlen gerade ist und für $a \in H$ gilt, dass $a^{-1} = 10 - a \in H$.

Sei $\langle G, \circ, e \rangle$ eine Gruppe.

Definition (Ordnung)

Die **Ordnung** eines Elements $a \in G$ ist die kleinste Potenz k , sodass $a^k = e$.

$$\text{ord}(a) := \min \{k \in \mathbb{N} \setminus \{0\} \mid a^k = e\}$$

Existiert kein solches k , so ist $\text{ord}(a) := \infty$.

Definition (Erzeugnis)

Das **Erzeugnis** $\langle a \rangle$ von a in G ist die Menge aller Elemente, die durch Potenzierung von a und a^{-1} erhalten werden können.

$$\langle a \rangle := \{a^k \mid k \in \mathbb{Z}\}$$

Es gilt $\langle a \rangle < G$.

Definition (Zyklische Gruppe)

Man nennt eine Gruppe G **zyklisch**, wenn ein Element $a \in G$ existiert, sodass a die gesamte Gruppe erzeugt.

$$\langle a \rangle = G$$

Man nennt a einen **Generator (oder Erzeuger)**.

- Alle Untergruppen einer zyklischen Gruppe sind **zyklisch**
- Zyklische Gruppen sind isomorph zu einer \mathbb{Z}_i oder \mathbb{Z}

Beispiel

Die ganzen Zahlen \mathbb{Z} und alle Gruppen der Form $\langle \mathbb{Z}_i, +_i, 0 \rangle$ sind zyklisch mit dem Generator 1.

Betrachte $\langle \mathbb{Z}_7, +_7, 0 \rangle$. Es ist

- $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$
- $\langle 2 \rangle = \{2, 4, 6, 1, 3, 5, 0\} = \langle 1 \rangle = \mathbb{Z}_7$

Seien $\langle G, \circ, e \rangle$ und $\langle G', \bullet, e' \rangle$ Gruppen.

Definition (Homomorphismus)

Eine Abbildung $\varphi : G \rightarrow G'$ heißt **Homomorphismus**, wenn gilt

$$\varphi(a \circ b) = \varphi(a) \bullet \varphi(b)$$

Ist φ bijektiv, so nennt man sie einen **Isomorphismus**.

- Homomorphismen sind **strukturerhaltend**
- Sie betten eine Gruppe in eine andere ein

Satz

Ist $\varphi : G \rightarrow G'$ ein Homomorphismus, so gilt

- $\varphi(e) = e'$
- Für alle $a \in G$ gilt $\varphi(a)^{-1} = \varphi(a^{-1})$
- Ist $H < G$, dann auch $\varphi(H) < G'$

Sei $\langle G, \circ, e \rangle$ eine Gruppe und $H < G$.

Definition (Nebenklasse)

Zu einem Element $a \in G$ nennen wir

$$aH := \{ax \mid x \in H\}$$

$$Ha := \{xa \mid x \in H\}$$

die **linke/rechte Nebenklasse** von a bezüglich H .

Die Anzahl der Nebenklassen zu H nennt man ihren **Index** $\text{ind}(G : H)$.

- Die Nebenklassen zu H sind eine **Partition** von G

Satz (Satz von Lagrange)

Ist G eine endliche Gruppe, so gilt

$$\text{ord}(G) = \text{ord}(H) \cdot \text{ind}(G : H)$$

Daraus folgt direkt $\text{ord}(a) \mid \text{ord}(G)$ für alle $a \in G$.

Definition (Eulersche φ -Funktion)

Die Funktion $\varphi : \mathbb{N} \setminus \{0\} \rightarrow \mathbb{N}$ heißt **Eulersche φ -Funktion**. Sie ist definiert durch die Anzahl der zu n **teilerfremden** Zahlen.

$$\varphi(n) := |\{x \mid x \in [n], \text{ggT}(x, n) = 1\}|$$

Es gilt für

$$\text{ggT}(m, n) = 1 \quad \varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$$

$$p \text{ prim} \quad \varphi(p) = p - 1$$

$$p \text{ prim}, k > 0 \quad \varphi(p^k) = p^{k-1}(p - 1)$$

Satz (Euler-Fermat)

Für $m \in \mathbb{N}$ mit $m \geq 2$ und $k \in \mathbb{Z}$ mit $\text{ggT}(k, m) = 1$ gilt

$$k^{\varphi(m)} \equiv 1 \pmod{m}$$

ist p prim, so gilt im speziellen

$$k^{p-1} \equiv 1 \pmod{p}$$

Erweiterter Euklidischer Algorithmus

Der **erweiterte Euklidische Algorithmus** berechnet für zwei Zahlen $a, b \in \mathbb{N}$ ganze Zahlen $x, y \in \mathbb{Z}$, sodass gilt

$$a \cdot x + b \cdot y = \text{ggT}(x, y)$$

Beispiel

Seien $a = 99$, $b = 78$ mit $\text{ggT}(99, 78) = 3$.

$$99 = 1 \cdot 78 + 21 \quad \longrightarrow \quad 21 = 99 - 1 \cdot 78$$

$$78 = 3 \cdot 21 + 15 \quad \longrightarrow \quad 15 = 78 - 3 \cdot 21$$

$$21 = 1 \cdot 15 + 6 \quad \longrightarrow \quad 6 = 21 - 1 \cdot 15$$

$$15 = 2 \cdot 6 + 3 \quad \longrightarrow \quad 3 = 15 - 2 \cdot 6$$

$$6 = 2 \cdot 3 + 0$$

$$\begin{aligned} 3 &= 1 \cdot 15 - 2 \cdot 6 \\ &= 1 \cdot 15 - 2 \cdot (21 - 1 \cdot 15) = (-2) \cdot 21 + 3 \cdot 15 \\ &= (-2) \cdot 21 + 3 \cdot (78 - 3 \cdot 21) = 3 \cdot 78 - 11 \cdot 21 \\ &= 3 \cdot 78 - 11 \cdot (99 - 1 \cdot 78) = (-11) \cdot 99 + 14 \cdot 78 \end{aligned}$$