1) Menge

-- Menge mit Zeichen { } definieren

a) explizite/ extensionale Definition -> $M : \{a, 2, \$\}$

b) implizite/ intensionale Definition -> $\{x \mid$ "x **ist deutscher Staatsbürger mit Wohnsitz in München"**$\}$

-- oft vorkommende Abkürzung für Mengen

$\mathbb{N} = \{1, 2, 3, \ldots\}$ **-> Menge der natürlichen (= positiven ganzen) Zahlen**

$\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$ **-> natürliche Zahlen inkl. 0**

$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ **-> positive und negative ganze Zahlen**

$\mathbb{Q} = \{p/q \mid p \in \mathbb{Z}, q \in \mathbb{N}\}$ **-> rationale Zahlen**

$\mathbb{R}$ **-> reelle Zahlen**

$\mathbb{C}$

-- oft vorkommende Schreibweisen

$x \in M$ **-> Objekt** x **ist in der Menge** M **enthalten/** x **(ist) Element von** M

$x \notin M$ **-> Objekt** x **ist nicht in der Menge** M **enthalten/** x **(ist) kein Element von** M

$M_1 = M_2$ **->** M_1 **und** M_2 **werden als identisch angesehen**

$M_1 \neq M_2$ **->** M_1 **und** M_2 **sind verschieden**

$M_2 \setminus M_1$ **-> Differenz von** M_2 **und** M_1

$M_1 \Delta M_2$ **-> symmetrische Differenz von** M_1, M_2

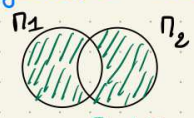
$M_1 \subseteq M_2$ **->** M_1 **ist eine Teilmenge von** M_2

$M_1 \nsubseteq M_2$ **->** M_1 **ist keine Teilmenge von** M_2

$M_1 \subsetneq M_2$ **-> falls zwar** $M_1 \in M_2$ **, jedoch auch** $M_2 \setminus M_1$ **mindestens ein Element besitzt**

Symmetrische Differenz: $\Pi_1 \Delta \Pi_2$

"Menge der Objekte, die Element genau einer der beiden Mengen sind"



$\Pi_1 \Delta \Pi_2 = (\Pi_1 \cup \Pi_2) \setminus (\Pi_1 \cap \Pi_2)$

$\Pi_1 \Delta \Pi_2 = \Pi_2 \Delta \Pi_1$ gilt stets, aber im Allgemein $\Pi_2 \setminus \Pi_1 \neq \Pi_1 \setminus \Pi_2$

$|M| < \infty$ **-> Eine Menge** M **ist endlich**

$|M| = \infty$ **-> Eine Menge** M **ist unendlich**

$M_1 \cap M_2$ **-> Schintt von** M_1 **und** M_2

$M_1 \cap M_2 = \emptyset$ **->** M_1 **und** M_2 **sind disjunkt (= besitzt kein gemeinsames Element)**

$M_1 \cup M_2$ **-> Vereinigung von** M_1 **und** M_2

$\cap S := \cap_{M \in S} M := \{x \mid$ "**Für jedes** $M \in S$ **gilt** $x \in M$"$\}$

$\cup S := \cup_{M \in S} M := \{x \mid$ "**es gibt mindestens ein** $M \in S$ **mit** $x \in M$"$\}$

Ω **-> Universum/ Grundmenge -> "alle existierende Elemente"**

$\bar{A} = (\Omega \setminus A)$ **-> Komplement(Gegenteil) von A (bzgl.** Ω**) -> "alles nicht in A liegt"**

$P(M) := 2^M := \{A \mid A \subseteq M\}$ -> Potenzmenge von Menge M mit k Elemente hat Kardinalität/ Mächtigkeit 2^k

$M = \cup P$ -> Partition einer Menge M -> Elemente von P überdecken M (Zerlegung von M in paarweise disjunkte nichtleere Teilmengen)

$(a_i)_{i \in \mathbb{N}}$ -> Sequenz/ Folge = unendliche Auflistung von Objekten nach ansteigenden Index

$(a_i)_{i \in [k]} = (a_1, a_2, \ldots, a_k)$ mit $(a_i)_{i \in [0]} = ()$ -> Tupel = endliche Sequenz/ Folge

$|t|$ -> Länge eines Tupels oder $\#t$ -> Anzahl der Komponenten

$A \times B = \{(a, b) \mid a \in A, b \in B\}$ -> -> Kartesische Produkt von A und B

$\{1, 2, 3\} \times \{a, b\} = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$ $|A \times B| = |A| \cdot |B|$

$A^k = \underbrace{A \times \ldots \times A}_{k \text{ mal}} = \{(a_1, \ldots, a_k) \mid a_1 \in A, a_2 \in A, \ldots, a_k \in A\}$ -> für alle k-Tupel mit Komponenten aus A

Σ oder L -> Alaphabet = Menge von Grundzeichen

$\Sigma^* := \bigcup_{k \in \mathbb{N}_0} \Sigma^k = \cup \{\Sigma^k \mid k \in \mathbb{N}_0\}$ -> Menge alller endlichen Wörter übers Alphabet Σ

ϵ oder λ -> leere Wort fürs leere Tupel

"Menge aller endlichen Tupel mit Einträgen aus einem Alphabet Σ"

Teilmenge $L \subseteq \Sigma^*$ -> als Sprache über Σ

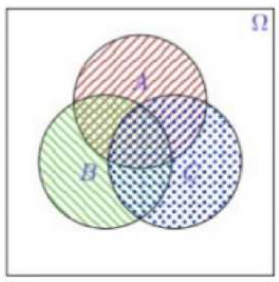
$uv := u_1 \ldots u_k v_1 \ldots v_l$ -> Konkatenation ("Verkettung") von zweier Wörter uv

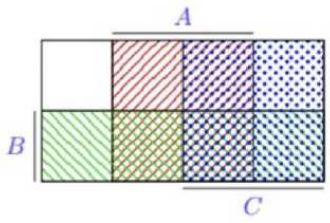
$w \in A_0 \cap A_1$: w hat an Stelle 0 und 1 ein "a"

$w \in A_0 \cup A_1$: w hat an Stelle 0 oder 1 ein "a"

$\bigcap_{k \in \mathbb{N}_0} A_k$ "immer a" ← "$\cap$" für alle ← "$\cup$" es gibt mindestens → $\bigcup_{k \in \mathbb{N}_0} A_k$ "irgendwo a"

Venn-Diagramm (links) und Karnaugh-Veitch-Diagramm (rechts)





Mengen: ohne Beachtung von Anordnung oder Vielfachheiten

$\{\emptyset, c, c, \{a, b\}\} = \{\emptyset, c, \{b, a\}\}$

Tupel: Beachtung der Anordnung und Vielfachheiten

$(a, b, c, c) \neq (a, b, c)$

$\Omega \setminus \Omega = \emptyset$

-- Standard-Äquivalenzumformungen

$\bar{\bar{A}} = A$
$A \cup A = A$
$A \cap A = A$
$A \cup \emptyset = A$
$A \cap \emptyset = \emptyset$

$A \cap \bar{A} = \emptyset$
$A \cup \bar{A} = \Omega$
$A \setminus B = A \cap \bar{B}$
$\overline{A \cup B} = \bar{A} \cap \bar{B}$
$\overline{A \cap B} = \bar{A} \cup \bar{B}$

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

$A \Delta B = (A \setminus B) \cup (B \setminus A)$

$A \cup (B \cup C) = (A \cup B) \cup C$
$A \cap (B \cap C) = (A \cap B) \cap C$

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

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

2) Relation

$R \subseteq A_1 \times A_2 \times \ldots \times A_k$ -> **eine k-stellige Relation**

Join: $R \bowtie_{i=j} S$ konkatiniert jedes Tupel $(r_1 \ldots r_k) \in R$ mit jedem Tupel $(s_1 \ldots s_\ell) \in S$ soweit $r_i = s_j$

Projektion: $\Pi_{i_1, i_2 \ldots i_j} R$: reduziert jedes Tupel $(r_1 \ldots r_k) \in R$ auf die Einträge an den Positionen $1 \leq i_1, i_2 \ldots i_j \leq k$

A_{Id}	$A_{Nachname}$	$A_{Vorname}$
1	Man	Spider
2	Brot	Bernd
3	Woman	Wonder
4	Gaga	Lady

R

A_{Id}	$A_{Matrikelnummer}$
1	3141
2	271828
3	1701
4	3694

S

A_{Id}	$A_{Geschlecht}$
1	m
2	b
3	w
4	w

T

$\Pi_3 (R \bowtie_{1=1} (T \bowtie_{2=1} \{(w)\}))$

3 Woman Wonder 3 w w
4 Gaga Lady 4 w w

Binäre (2-stellige) Relation R **zwischen Mengen** A **und** B **ist eine Teilmenge** $R \subseteq A \times B$

homogene binäre Relation $R \subseteq A \times A$ **(A -> Grundmenge von R)**

Umkehrrealtion (inverse Relation) $R^{-1} := \{(b, a) \mid (a, b) \in R\}$

-> Veranschaulichung von binären Relation durch gerichteten Graph $G = (V, E)$

Knotenmenge V **-> Elemente von** V **= Knoten von** G

Kantenrelation/ -menge $E \subseteq V \times V$ **-> Elemente von** E **= Kanten von G**

Weg/ Pfad $(v_0, v_1, \ldots, r_l)$ **= ein Tupel von Knoten** $v_i \in V$

Länge eines Pfades $(v_0, v_1, \ldots, r_l)$ **ist** l

;) Relationales Produkt:

$R \subseteq A \times B$; $S \subseteq C \times D$

Relationale Produkt von R und S: die binäre Relation $RS \subseteq A \times D$

$RS = \{(a, d) \mid$ es gibt $x \in B \cap C$ mit $(a, x) \in R$ und $(x, d) \in S\}$

$RS = \Pi_{1,4} (R \bowtie_{2=1} S)$

R: $1 \to 2$; S: $2 \to 4$ $\Rightarrow RS = \Pi_{1,4} (R \bowtie_{2=1} S) = 1 \to 4$

im Graph: RS enthält (u, v) $\Leftrightarrow$ es gibt einen Verbindungsknoten w und eine Kante (u, w) in R und eine Kante (w, v) in S.

über eine beliebigen nichtleeren Menge A

	ref	sym	asy	ant	tot	tra
$\emptyset$	✗	✓	✓	✓	✗	✓
id_A	✓	✓	✗	✓	✗	✓
$A \times A$	✓	✓	✗	✗	✓	✓

über ganze Zahlen

	ref	sym	asy	ant	tot	tra
$=$	✓	✓	✗	✓	✗	✓
$\neq$	✗	✓	✗	✗	✗	✗
$\leq$	✓	✗	✗	✓	✓	✓
$<$	✗	✗	✓	✓	✗	✓

über Potenzmenge einer beliebigen Menge

	ref	sym	asy	ant	tot	tra
$=$	✓	✓	✗	✓	✗	✓
$\neq$	✗	✓	✗	✗	✗	✗
$\subseteq$	✓	✗	✗	✓	✗	✓
$\not\subseteq$	✗	✗	✗	✗	✗	✗
$\subset$	✗	✗	✓	✓	✗	✓
$\not\subset$	✓	✗	✗	✗	✓	✗

binäre Relation $R \subseteq A \times A$ **- auf eine Menge A definiert**

$R^0 := \mathrm{ld}_A := \{(a, a) \mid a \in A\}$

$R^1 := R = R^0 R$ -> **1-Schritt-Pfade -> Weg der Länge 1**

$R^2 := RR = R^1 R$ -> **2-Schritte-Pfade -> Weg der Länge 2**

$R^{k+1} := R^k R = RR^k = \underbrace{RR \ldots R}_{k+1 \text{ mal}}$ **für beliebiges** $k \in \mathbb{N}_0$ **-> k-Schritt-Pfade -> Weg der Länge k**

$R^+ := \bigcup_{k \in \mathbb{N}} R^k$ -> **transitive Hülle einer binären Relation** $R \subseteq A \times A$ **("alle Pfade, mindestens einen Schritt machen")**

$R^* := \bigcup_{k \in \mathbb{N}_0} R^k = R^0 \cup R^+$ -> **Reflexiv-transitive Hülle einer binären Relation** $R \subseteq A \times A$

$R^{\leq k} := \bigcup_{i=0}^{k} R^i = R^0 \cup R^1 \cup \cdots \cup R^k$ -> **Erreichbarkeit in höchstens k Schritten**

R^{-1} -> **(inverse) Umdrehensrelation ("alle Pfeile umdrehen")**

Eigenschaften einer binären Relation $R \subseteq A \times A$

- **Reflexivität:** $\forall a \in A : (a, a) \in R$ { irreflexiv = gar keine Schleifen; nicht reflexiv = gibts Schleifen, aber nicht alle

-> Jeder Knoten hat eine Schleife (Jedes Element steht in Relation mit sich selber)

- **Symmetrie:** $\forall a, b \in A : (a, b) \in R \Rightarrow (b, a) \in R$

-> Zwischen je zwei Knoten entweder beide Kanten oder gar keine Kante (beliebige Schleifen)

- **Asymmetrie:** $\forall a, b \in A : (a, b) \in R \Rightarrow (b, a) \notin R$ (weder Doppelpfeile noch Schleife)

-> Keine Schleifen und zwischen je zwei verschiedenen Knoten höchstens eine Kante

- **Antisymmetrie:** $\forall a, b \in A : (a, b) \in R \wedge (b, a) \in R \Rightarrow a = b$ (Doppelpfeile nein, aber Schleife ja)

-> Zwischen zwei verschiedenen Knoten existiert höchstens eine Kante

- **Transitivität:** $\forall a, b, c \in A : (a, b) \in R \wedge (b, c) \in R \Rightarrow (a, c) \in R$ entweder Transivität zwischen alle Knoten oder Transivität für Graph mit gar keine Kanten

-> Man kann mit genau zwei Schritten von a nach c kommen, dann auch mit genau einem Schritt

Relation auf Operationen

$=\mathbb{Z}$ -> reflexiv; symmetrisch; transitiv; antisymmetrisch

$\leq \mathbb{Z}$ -> reflexiv; antisymmetrisch; transitiv

$< \mathbb{Z}$ -> nicht reflexiv; asymmetrisch; transitiv

$\neq \mathbb{Z}$ -> nicht reflexiv; symmetrisch; nicht transitiv

$|_{\mathbb{Z}} \subseteq \mathbb{Z} \times \mathbb{Z}$ -> nicht reflexiv; nicht symmetrisch; nicht asymmetrisch; nicht antisymmetrisch; transitiv

$|_{\mathbb{N}} \subseteq \mathbb{N} \times \mathbb{N}$ -> reflexiv; antisymmetrisch; transitiv

$\equiv m \subseteq \mathbb{Z} \times \mathbb{Z}$ -> reflexiv; symmetrisch; transitiv

$\subseteq$ auf $\mathcal{P}(\mathbb{Z})$ -> reflexiv; antisymmetrisch; transitiv

Kongruenzbegriff auf Dreiecken -> reflexiv; symmetrisch; transitiv

Relation auf Wörter $u, v \in \Sigma^*$

$u \preceq_p v$ (u ist ein Präfix von v, falls es ein $w \in \Sigma^*$ mit $uw = v$ gibt) -> reflexiv; antisymmetrisch; transitiv

$u \preceq_s v$ (u ist ein Suffix von v, falls es ein $w \in \Sigma^*$ mit $wu = v$ gibt)) -> reflexiv; antisymmetrisch; transitiv

$u \preceq_i v$ (u ist ein Infix bzw. Faktor von v, falls es $w, w' \in \Sigma^*$ mit $wuw' = v$ gibt) -> reflexiv; antisymmetrisch; transitiv

$u \cong_c v$ (u und v sind konjugiert, falls es $w, w' \in \Sigma^*$ mit $u = ww'$ und $v = w'w$ gibt) -> reflexiv; symmetrisch; transitiv

xRy Person mit Blutgruppe x kann einer Person mit Blutgruppe y Blut spenden -> reflexiv; antisymmetrisch; transitiv

Äquivalenzrelationen: reflexiv, symmetrisch, transitiv

- Für $R \subseteq A \times A$ eine Äquivalenzrelation definiert man:

  Äquivalenzklasse eines Objekts a bzgl R:

  $$[a]_R = \{b \in A \mid a R b\}$$

- es gilt: • $a \in [a]_R$
  • $[a]_R = [b]_R$ für $a R b$
  • $[a]_R \cap [b]_R = \emptyset$ für $(a,b) \notin R$

verschiedenen "Äquivalenzbegriffen" $=_z$, $\equiv_m$, $\widetilde{=}_c$ ...

$a =_z b$ -> "a und b dieselbe/identische Zahl"

$a \equiv_m b$ -> "a und b derselbe Rest bei Division durch m"

bsp: $[1]_{=_{\mathbb{Z}}} = \{1\}$; $[-5]_{\equiv_3} = 3\mathbb{Z}+1$

Quotient von A bzgl. R als die Menge aller Äquivalenzklassen:

$A/R = \{[a]_R \mid a \in A\}$ "eine Partition von A"

bsp: $\mathbb{Z}/_{\equiv_3} = \{3\mathbb{Z}, 3\mathbb{Z}+1, 3\mathbb{Z}+2\}$

Ordnungsrelationen:

$R \subseteq A \times A$ ist eine partielle Ordnung (Halbordnung) auf A, falls:

R reflexiv, antisymmetrisch und transitiv

zb: $|_{\mathbb{N}}$

$R \subseteq A \times A$ ist eine totale Ordnung auf A, falls:

1. R eine partielle Ordnung auf A ist
2. es gilt mindestens $a R b$ oder $b R a$

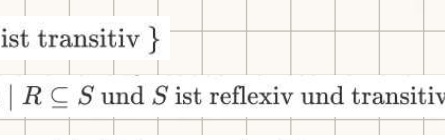
zb: $\leqslant_{\mathbb{Z}}$

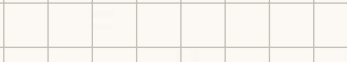
- Hasse Diagramme: Visualisierung einer partiellen Ordnung $R \subseteq A \times A$:
  man stellt nur eine möglichst kleine Relation $S \subseteq R$ dar, für die $S^* = R$ gilt. G_S heißt dann Hasse Diagramm von R.

"was ich weiß aufgrund der Transitivität und Reflexivität brauche ich nicht mehr darzustellen"

bsp: $\leqslant_{\mathbb{N}_0}$

ohne Schleifen
ohne Transivität

Statt: 

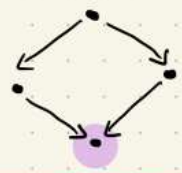
nur: 

R — Hasse Diagramm (*) $S^* = R$ — S

- m ∈ A ist ein maximales Element bzgl R:

  Falls $m R a$, dann auch $a R m$ und $a = m$

  "keine Kanten zu einem anderen Element"

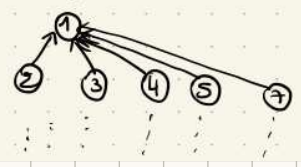


- m ist das größte Element bzgl R, falls
  $a R m$ für jedes $a \in A$ gilt

  "keine Kanten zu einem anderen Element, aber von jedem anderen Element eine Kante"

  eindeutiges maximales

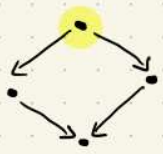
bzgl $|_{\mathbb{N}}^{-1}$ ("ist Vielfaches") ist 1 das größte Element



- m ∈ A ist ein minimales Element bzgl R:

  Falls es kein $a \neq m$ gibt sodass $a R m$ gilt

  "keine Kanten von einem anderen Element"

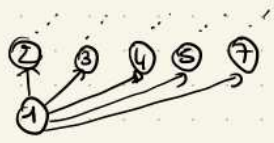


- m ist das kleinste Element bzgl R, falls
  $m R a$ für jedes $a \in A$ gilt:

  "keine Kanten von einem anderen Element aber eine Kante zu jedem anderen"

  eindeutiges minimales

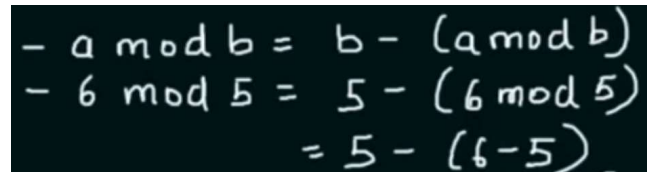
bzgl $|_{\mathbb{N}}$ ist 1 das kleinste Element



transitive Hülle R^+ ist das kleinste Element in $\{S \subseteq A \times A \mid R \subseteq S \text{ und } S \text{ ist transitiv}\}$

reflexiv-transitive Hülle R^* ist das kleinste Element in $\{S \subseteq A \times A \mid R \subseteq S \text{ und } S \text{ ist reflexiv und transitiv}\}$

Bei einer Umdrehung von R zu R^{-1} -> minimales und maximales tauschen sich, kleinste und größte tauschen sich



3) Funktionen

Zuordnung von zwei Mengen A und B: für jedes $a \in A$ gibt es genau ein $b \in B$ mit $(a, b) \in R$

Menge aller Funtktionen von A nach B -> $B^A := \{f : A \to B\}$

k-äre Funktion -> $f : \chi_{i=1}^{k} A_i \to B$

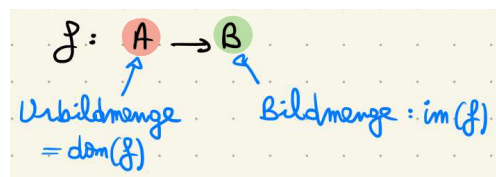
$|B^A| = |B|^{|A|}$

bsp: $A = \{a, b, c\}$; $B = \{0, 1\}$

$|B^A| = 2^3 = 8$: 8 mögliche Funktionen von A nach B

Urbildmenge $dom(f)$ -> $f^{-1}(Y) = \{a \in A \mid f(a) \in Y\} \subseteq \mathrm{dom}(f)$ (->"Urbilder von Y")

Bildmenge $im(f)$ -> $f(X) = \{f(a) \mid a \in X\} \subseteq \mathrm{im}(f)$ (->"Bilder von X")



$f : A \to B$ (totale) Funktion: $\mathrm{dom}(f) = A$ ("Für jedes a genau ein b")

$f : A \hookrightarrow B$ partielle Funktion: $\mathrm{dom}(f) \subseteq A$ ("Für jedes a höchstens ein b")

$f : A^k \to A$ -> k-stellige Operationen auf A

für eine binäre Operation $\odot : A \times A \to A$

-> assoziativ falls $(a \odot b) \odot c = a \odot (b \odot c)$ für alle $a, b, c \in A$

-> kommutativ falls $a \odot b = b \odot a$ für alle $a, b \in A$

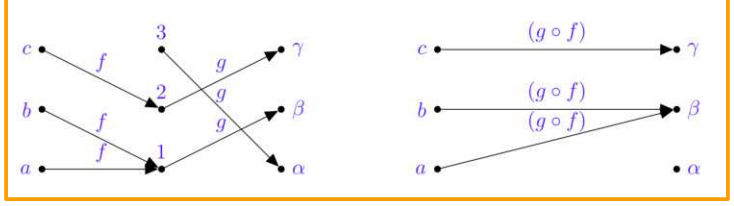
-> idempotent falls $a \odot a = a$ für alle $a \in A$

Komposition (Nacheinanderausführung) $g \circ f$ ("g nach f")

Komposition ist assoziativ, aber nicht kommutativ

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

Relationales Produkt $fg = \{(a, g(f(a))) \mid a \in A\}$ = Komposition $(g \circ f)$



Eigenschaften für eine Funktion $f : A \to B$

a) injektiv, falls aus $f(a) = f(a')$ stets $a = a'$ folgt

-> Äquivalent: $\left|f^{-1}(\{b\})\right| \leq 1$ für jedes $b \in B$ ("jedes Element B wird maximal 1 mal von A getroffen") "für jedes $b \in B$ gibt es höchstens ein Urbild"

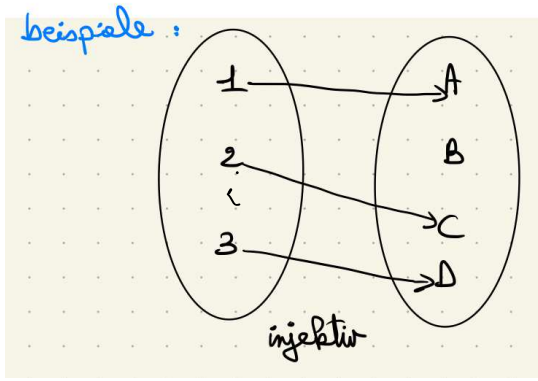
b) surjektiv, falls für jedes $b \in B$ ein $a \in A$ mit $f(a) = b$ gibt

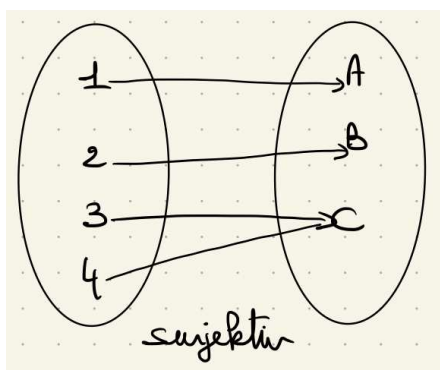
-> Äquivalent: $f(A) = B, \mathrm{im}(f) = B, \left|f^{-1}(\{b\})\right| \geq 1$ für jedes $b \in B$ ("jedes Element B wird mindestens 1 mal von A getroffen") "mindestens ein Urbild"

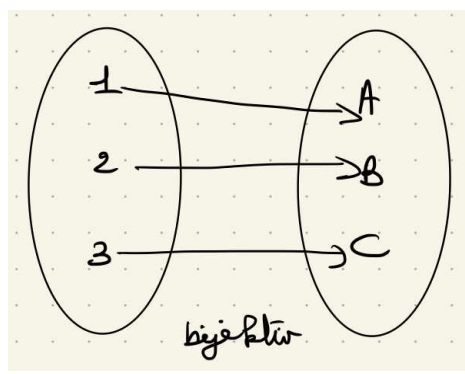
c) bijektiv, falls sie sowohl injektiv als auch surjektiv ist "genau ein Urbild"

-> Äquivalent: $\left|f^{-1}(\{b\})\right| = 1$ für jedes $b \in B$ ("jedes Element B wird genau 1 mal von A getroffen")

***Eine bijektive Funktion $f : A \to A$ -> Permutation (Ursprungsmenge = Zielmenge)**







Einige Eigenschaften

-- Ist f injektiv, dann ist $g : A \to f(A), a \mapsto f(a)$ bijektiv

-- Ist $f : A \to A$ injektiv und A endlich, dann ist f bijektiv

-- Ist $f : A \to A$ surjektiv und A endlich, dann ist f bijektiv

-- Ist $f : A \to B$ eine bijektive Funktion, dann ist f^{-1} injektiv

-- Ist $f : A \to B$ eine bijektive Funktion, dann auch f^{-1} eine bijektive Funktion

-- Ist $(g \circ f)$ surjektiv, dann auch g surjektiv

-- Ist $(g \circ f)$ surjektiv, dann auch f surjektiv

-- Sind $f : A \to B$ und $g : B \to C$ injektiv/ surjektiv, dann auch $(g \circ f)$ injektiv/ surjektiv

-- Sei $f : A \to B$ eine bijektive Funktion. Dann ist f^{-1} die einzige Funktion g aus A^B mit der Eigenschaft $(g \circ f) = \mathrm{ld}_A$ und $(f \circ g) = \mathrm{Id}_B$

Sind $f : A \to B$ und $g : B \to A$ injektiv, dann gibt es $h : A \to B$ bijektiv Satz von Cantor

-- Für $f : A \to B$ und $g : B \to A$ gelte $(g \circ f) = \mathrm{ld}_A$ und $(f \circ g) = \mathrm{Id}_B$. Dann sind f, g bijektiv mit $f^{-1} = g$ und $g^{-1} = f$

-- Sind $f : A \to B$ und $g : B \to C$ bijektiv, dann auch $(g \circ f) : A \to C$ und es gilt $(g \circ f)^{-1} = \left(f^{-1} \circ g^{-1}\right)$

-- Ist $(g \circ f) : A \to C$ bijektiv, dann ist $f : A \to B$ injektiv und $g : B \to C$ surjektiv

-- $f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y)$ und $f^{-1}(X \cap Y) = f^{-1}(X) \cap f^{-1}(Y)$

-- $f(X \cup Y) = f(X) \cup f(Y)$, aber $f(X \cap Y) \subseteq f(X) \cap f(Y)$

-> f ist dann injektiv, wenn stets $f(X \cap Y) = f(X) \cap f(Y)$ gilt

1. Seien f und g injektiv. Wir untersuchen $g \circ f$:

   Injektivität: Seien $a, a' \in A$ beliebig und es gelte $a \neq a'$. Nach Definition der Komposition gilt $(g \circ f)(a) = g(f(a))$ und analog $(g \circ f)(a') = g(f(a'))$. Da f injektiv ist, gilt nach Definition der Injektivität $f(a) \neq f(a')$. Da auch g injektiv ist, folgt $g(f(a)) \neq g(f(a'))$. Somit ist $g \circ f$ injektiv.

   Surjektivität: Sei $A = \{0\}$, $B = \{0\}$ und $C = \{0, 1\}$. Sei $f = \{(0, 0)\}$ und $g = \{(0, 0)\}$. Offensichtlich sind f und g injektiv. Dann gilt $g \circ f = \{(0, 0)\}$. Somit ist $g \circ f$ nicht surjektiv, da $1 \in C$ und $\nexists\, a \in A$. $(g \circ f)(a) = 1$.

   Bijektivität: Da $g \circ f$ nicht surjektiv ist, ist $g \circ f$ auch nicht bijektiv.

2. Sei f injektiv und sei g surjektiv. Wir untersuchen $g \circ f$:

   Injektivität: Sei $A = \{0, 1\}$, $B = \{0, 1, 2\}$ und $C = \{0, 1\}$, $f = \{(0, 0), (1, 1)\}$ und $g = \{(0, 0), (1, 0), (2, 1)\}$. Offensichtlich ist f injektiv und g surjektiv. Dann gilt $g \circ f = \{(0, 0), (1, 0)\}$. Da $(g \circ f)(0) = (g \circ f)(1)$, ist $g \circ f$ nicht injektiv.

   Surjektivität: Mit dem gleichen Gegenbeispiel wie für die Injektivität folgt, dass $g \circ f$ nicht surjektiv ist, da $1 \in C$ und $\nexists\, a \in A$. $(g \circ f)(a) = 1$.

   Bijektivität: Da $g \circ f$ weder injektiv noch surjektiv ist, ist $g \circ f$ auch nicht bijektiv.

3. Sei f injektiv und g bijektiv. Wir untersuchen $g \circ f$:

   Injektivität: Da g bijektiv ist, ist g insbesondere auch injektiv und daher folgt mit 1., dass $g \circ f$ injektiv ist.
   Surjektivität: Sei $A = \{0\}$, $B = \{0, 1\}$ und $C = \{0, 1\}$. Sei $f = \{(0, 0)\}$ und $g = \{(0, 0), (1, 1)\}$. Offensichtlich ist f injektiv und g bijektiv. Dann gilt $g \circ f = \{(0, 0)\}$. Somit ist $g \circ f$ nicht surjektiv, da $1 \in C$ und $\nexists\, a \in A$. $(g \circ f)(a) = 1$.

   Bijektivität: Da $g \circ f$ nicht surjektiv ist, ist $g \circ f$ auch nicht bijektiv.

4. Sei f surjektiv und g injektiv. Wir untersuchen $g \circ f$:

   Injektivität: Sei $A = \{0, 1\}$, $B = \{0\}$ und $C = \{0, 1\}$. Sei $f = \{(0, 0), (1, 0)\}$ und $g = \{(0, 0)\}$. Offensichtlich ist f surjektiv und g injektiv. Dann gilt $g \circ f = \{(0, 0), (1, 0)\}$. Da $(g \circ f)(0) = (g \circ f)(1) = 0$, ist $g \circ f$ nicht injektiv.
   Surjektivität: Mit dem gleichen Gegenbeispiel wie für die Injektivität folgt, dass $g \circ f$ nicht surjektiv ist, da $1 \in C$ und $\nexists\, a \in A$. $(g \circ f)(a) = 1$.

   Bijektivität: Da $g \circ f$ weder injektiv noch surjektiv ist, ist $g \circ f$ auch nicht bijektiv.

5. Seien f und g surjektiv. Wir untersuchen $g \circ f$:

   Injektivität: Sei $A = \{0, 1\}$, $B = \{0\}$ und $C = \{0\}$. Sei $f = \{(0, 0), (1, 0)\}$ und sei $g = \{(0, 0)\}$. Offensichtlich sind f und g surjektiv. Dann gilt $g \circ f = \{(0, 0), (1, 0)\}$. Da $(g \circ f)(0) = (g \circ f)(1) = 0$, ist $g \circ f$ nicht injektiv.

   Surjektivität: Sei $c \in C$ beliebig. Da g nach Annahme surjektiv ist, existiert ein $b \in B$, sodass $g(b) = c$. Da auch f nach Annahme surjektiv ist, existiert auch ein $a \in A$, sodass $f(a) = b$. Also gilt $g(f(a)) = c$ und daher nach Definition der Komposition $(g \circ f)(a) = c$. Somit ist $g \circ f$ surjektiv.

   Bijektivität: Da $g \circ f$ nicht injektiv ist, ist $g \circ f$ auch nicht bijektiv.

6. Sei f surjektiv und sei g bijektiv. Wir untersuchen $g \circ f$:

   Injektivität: Sei $A = \{0, 1\}$, $B = \{0\}$ und $C = \{0\}$. Sei $f = \{(0, 0), (1, 0)\}$ und sei $g = \{(0, 0)\}$. Offensichtlich ist f surjektiv und g bijektiv. Dann gilt $g \circ f = \{(0, 0), (1, 0)\}$. Da $(g \circ f)(0) = (g \circ f)(1) = 0$, ist $g \circ f$ nicht injektiv.

   Surjektivität: Da g bijektiv ist, ist g insbesondere auch surjektiv und somit folgt die Surjektivität von $g \circ f$ mit 5.

   Bijektivität: Da $g \circ f$ nicht injektiv ist, ist $g \circ f$ auch nicht bijektiv.

7. Sei f bijektiv und g injektiv. Wir untersuchen $g \circ f$:

   Injektivität: Da f bijektiv ist, ist f insbesondere auch injektiv und somit folgt mit 1. die Injektivität von $g \circ f$.
   Surjektivität: Sei $A = \{0\}$, $B = \{0\}$ und $C = \{0, 1\}$. Sei $f = \{(0, 0)\}$ und $g = \{(0, 0)\}$. Offensichtlich ist f bijektiv und g injektiv. Dann gilt $g \circ f = \{(0, 0)\}$. Somit ist $g \circ f$ nicht surjektiv, da $1 \in C$ und $\nexists\, a \in A$. $(g \circ f)(a) = 1$.

   Bijektivität: Da $g \circ f$ nicht surjektiv ist, ist $g \circ f$ auch nicht bijektiv.

8. Sei f bijektiv und sei g surjektiv. Wir untersuchen $g \circ f$:

   Injektivität: Sei $A = \{0, 1\}$, $B = \{0, 1\}$ und $C = \{0\}$. Sei $f = \{(0, 0), (1, 1)\}$ und $g = \{(0, 0), (1, 0)\}$. Offensichtlich ist f bijektiv und g surjektiv. Dann gilt $g \circ f = \{(0, 0), (1, 0)\}$. Da $(g \circ f)(0) = (g \circ f)(1) = 0$, ist $g \circ f$ nicht injektiv.

   Surjektivität: Da f bijektiv ist, ist f insbesondere auch surjektiv und somit folgt mit 5., dass $g \circ f$ surjektiv ist.

   Bijektivität: Da $g \circ f$ nicht injektiv ist, ist $g \circ f$ auch nicht bijektiv.

9. Seien f und g bijektiv. Wir untersuchen $g \circ f$:

   Injektivität: Da f und g nach Annahme bijektiv sind, sind sie insbesondere auch injektiv. Daher folgt die Injektivität von $g \circ f$ mit 1.

   Surjektivität: Da f und g nach Annahme bijektiv sind, sind sie insbesondere auch surjektiv. Daher folgt die Surjektivität von $g \circ f$ mit 5.

   Bijektivität: Da $g \circ f$ injektiv und surjektiv ist, ist $g \circ f$ auch bijektiv.

Kardinalität von Mengen:

- $|A| \leq |B|$ (B mindestens so mächtig wie A):

  falls es eine injektive Funktion $f: A \to B$ gibt

"Eine Injektion $f: A \to B$ erlaubt es jedes Element aus $a \in A$ eindeutig mit $f(a) \in B$ zu identifizieren. B hat damit „mindestens so viele Elemente" wie A.

- $|A| = |B|$ (A und B gleichmächtig):

  falls es eine bijektive Funktion $f: A \to B$ gibt

"eine Bijektion $f: A \to B$ erlaubt es die Elemente von A und B eindeutig zu paaren. B hat damit „genau so" viele Elemente wie A"

- $|A| < |B|$ (echt mächtiger): falls es eine Injektion $f: A \to B$, aber keine Bijektion $g: A \to B$ gibt.

Satz von Cantor-Bernstein-Schröder:

- Sind $f: A \to B$ und $g: B \to A$ injektiv, dann gibt es $h: A \to B$ bijektiv

⇒ • $|A| = |B|$ wenn es injektive Funktionen $f: A \to B$ und $g: B \to A$ gibt

• $|A| < |B|$ wenn es eine injektive Funktion $f: A \to B$ aber keine injektive Funktion $g: B \to A$ gibt

- falls $|A| \leq |\mathbb{N}|$ ist die Menge A abzählbar, ansonsten überabzählbar

"A ist abzählbar wenn es möglich ist, jedes Element von A mit einer eindeutigen Nummer aus $\mathbb{N}$ zu versehen"

- es gilt stets $|A| < |\mathcal{P}(A)|$

- Multimengen:

Mengen: ohne Beachtung von Vielfachheiten und Reihenfolge	Multimenge: ohne Beachtung der Reihenfolge, aber unter Beachtung von Vielfachheiten
$\{a,a,b,c\} = \{a,b,c\}$	$\{a,b,c,a\}_{\Pi} = \{a,a,b,c\}_{\Pi} \neq \{b,a,c\}_{\Pi}$

- $\Omega = \{a,b,c,d\}$, Multimengen lassen sich mittels Zählfunktionen $m \in \mathbb{N}_0^{\Omega}$ darstellen

$$\{a,b,c,a\}_{\Pi} = \{(a,2),(b,1),(c,1),(d,0)\}$$

Vereinigung zweier Multimengen = die punktweise Addition der Zählfunktionen

Schnitt zweier Multimengen = das punktweise Minimum der Zählfunktionen

Graphen

Digraph: gerichteter Graph $G = (V, E)$ (Knoten / Menge; Kantenmenge: $E \subseteq V \times V$)

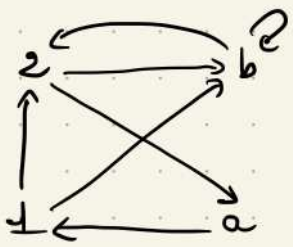
- ein Digraph ist bipartit falls $V = A \cup B$ mit $A \cap B = \emptyset$ $(V = A \dot\cup B)$ und $E \subseteq A \times B \cup B \times A$

Pfade:
- Folge von Knoten $v_0, v_1 \dots v_\ell$; $v_i \in V$ und $(v_{i-1}, v_i) \in E$ für jedes $i \in [\ell]$
  - die Länge eines Pfades ist die Anzahl der Kanten von v_0 bis v_ℓ
  - ein Pfad heißt einfach, falls kein Knoten mehrmals in dem Pfad vorkommt.
  - in einem endlichen Digraphen hat ein einfacher Pfad maximal länge $|V| - 1$

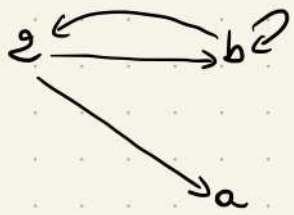
Teilgraphen: Für $U \subseteq V$ schreibt man:

$G[U]$ für $(U, E \cap (U \times U))$: von U induzierter Teilgraph

bsp:



$U = \{a, 2, b\}$



Zusammenhang für $G = (V, E)$

G ist zusammenhängend - falls $u\left(E \cup E^{-1}\right)^* v$ für alle $u, v \in V$ gilt

-> Es gibt Graphen zwischen allen zusammenhängenden Knoten

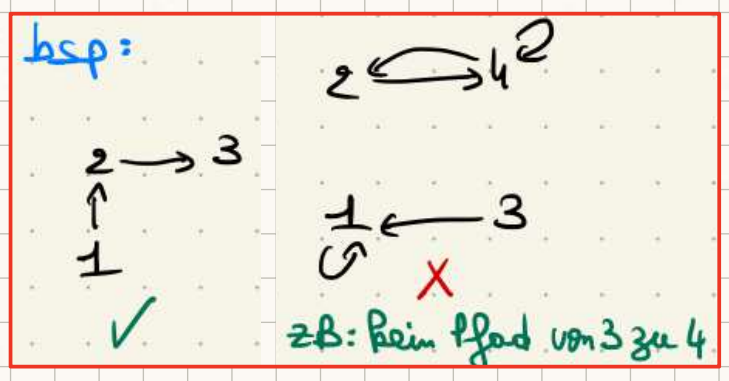
G ist stark zusammenhängend - falls sowohl uE^*v als auch vE^*u für alle $u, v \in V$ gilt

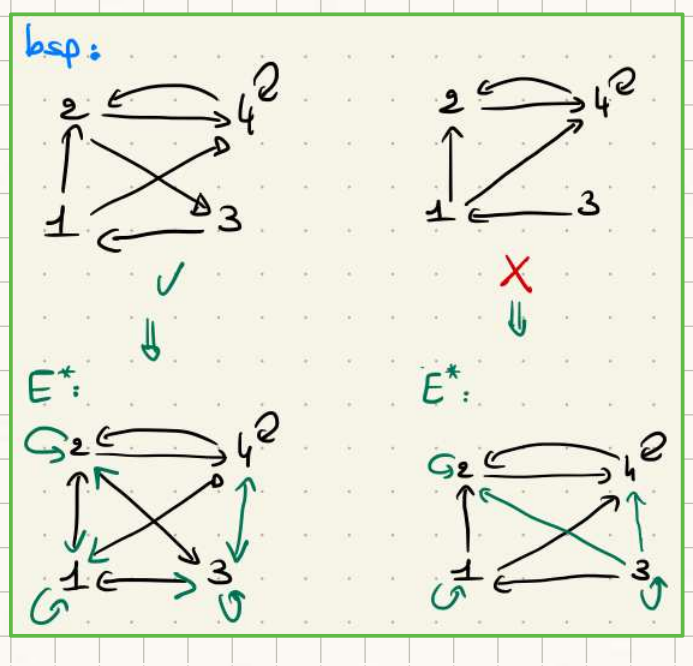
-> Es gibt Digraphen zwischen allen stark zusammenhängenden Knoten (Graph besitzt genau eine Zusammenhangskomonenete $U \subseteq V$)

U ist eine maximale (starke) Zusammenhangskomponente, falls es kein $U\prime$ mit $U \subsetneq U' \subseteq V$ gibt, so dass $G[U\prime]$ selbst eine (starke) Zusammenhangskomponente ist

zusammenhängend $\Rightarrow |V| \leq |E| + 1$

bsp:





- Kreise: . ein Kreis ist ein Pfad $v_0, v_1 \dots v_\ell$ mit $\ell \geq 1$ und $v_0 = v_\ell$

  . ein Kreis ist einfach falls alle Knoten $v_0 \dots v_{\ell-1}$ paarweise verschieden sind.

- Nachfolger von u: $uE = \{v \in V \mid uEv\}$

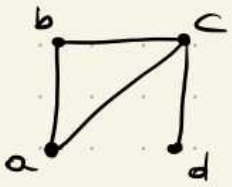
  Vorgänger von v: $Ev = \{u \in V \mid uEv\}$

Ungerichtete Graphen: ein Digraph G ist ungerichtet falls E symmetrisch ist

Einfache Graphen: ein endlicher Digraph ist ein einfacher Graph, falls E symmetrisch (ungerichtet) und irreflexiv ist (ohne Schleifen)

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

Knotengrad: $\deg(u) := |\Gamma(u)|$



$\Gamma(b) = \{c, a\}$

$\deg(b) = 2$

- in ungerichteten Graphen ist ein Pfad $v_0 \dots v_\ell$ mit $\ell \geq 3$, $v_0 = v_\ell$ ein Kreis.

Satz: Ein einfacher Graph ist bipartit genau dann, wenn er keinen Kreis ungerader Länge enthält

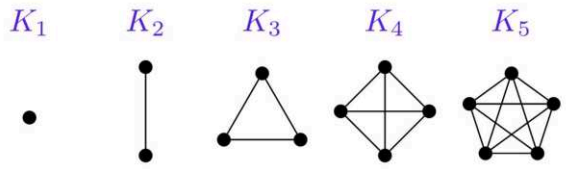
$\binom{V}{2} := \{\{u, v\} \subseteq V \mid u \neq v\}$ (Menge aller 2-elementigen Teilmengen) $\left|\binom{V}{2}\right| = \binom{|V|}{2}$

Spezielle einfache Graphen

- Vollständiger Graph $K_n := \left([n], \binom{[n]}{2}\right)$ $(n \geq 1)$ $(n-1)$-regulär

$|V| = n$

$|E| = \frac{n(n-1)}{2}$

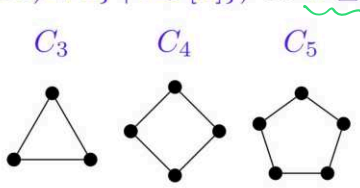


- Kreisgraph $C_n := ([n], \{\{i, (i \bmod n) + 1\} \mid i \in [n]\})$ für $n \geq 3$

2-regulär

$|V| = n$

$|E| = n$

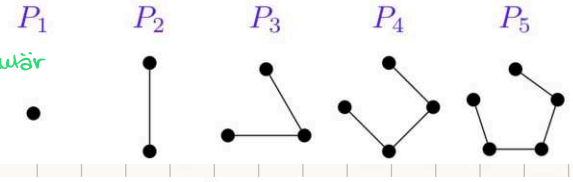


- Pfadgraph $P_n := ([n], \{\{i, i+1\} \mid i \in [n-1]\})$

$n=1$ 0-regulär
$n=2$ 1-regulär
$n \geq 3$ nicht k-regulär

$|V| = n$

$|E| = n-1$

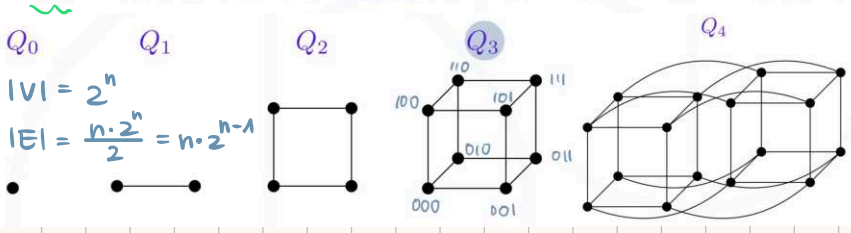


- Hyperwürfel der Dimension n n-regulär (für alle $n \geq 0$)

$Q_n := (\{0,1\}^n, \{\{u, v\} \mid \sum_{i=1}^n |u_i - v_i| = 1\})$ mit $Q_0 := (\{\varepsilon\}, \emptyset)$

$|V| = 2^n$

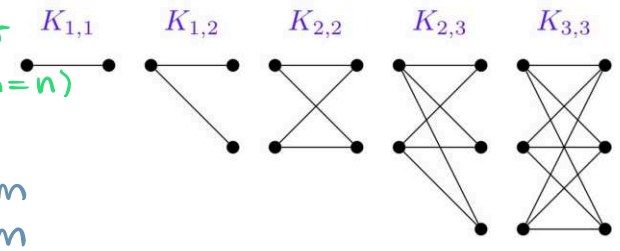
$|E| = \frac{n \cdot 2^n}{2} = n \cdot 2^{n-1}$



- Vollständiger bipartiter Graph

$K_{m,n} := ([m+n], \{\{i, j\} \mid i \in [m], j \in [m+n] \setminus [m]\})$ $(m \leq n)$

k-regulär (falls $k = m = n$)

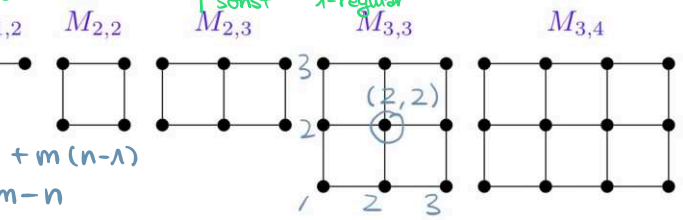


$|V| = n + m$

$|E| = n \cdot m$

- Gittergraph $M_{m,n} := ([m] \times [n], \{\{(i,j),(k,l)\} \mid |i-k| + |j-l| = 1\})$ $(m \leq n)$

k-regulär, wenn $m, n \leq 2$ { $m = n = 2$ 2-regulär; $m = n = 1$ 0-regulär; sonst 1-regulär



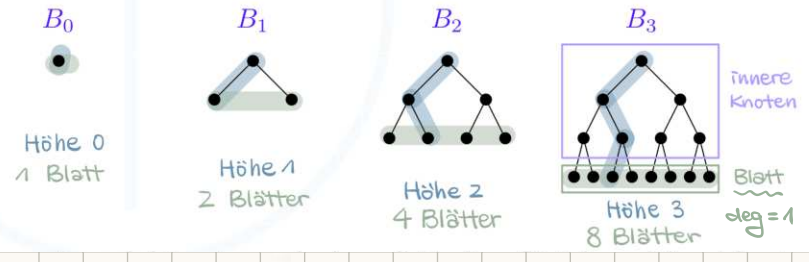
$|V| = n \cdot m$

$|E| = n(m-1) + m(n-1)$
$= 2mn - m - n$

- Perfekter Binärbaum der Höhe h

$B_h := (\{0,1\}^{\leq h}, \{\{u, ux\} \mid u \in \{0,1\}^{<h}, x \in \{0,1\}\})$

B^h { 2^h Blätter; $2^{h+1} - 1$ Knoten; $2^{h+1} - 2$ Kanten



Behauptung mit Induktionsbeweis

1) jede einfache zusammenhängend Graph mit $n \geq 1$ Knoten hat mindestens $n-1$ Kanten.

2) jeder endliche einfache zusammenhangende Graph mit $n \geq 3$ Knoten und mindestens n Kanten besitzt einen Kreis.

Die max. Zshgskomponenten von G' seien G1,...,Gr.

$1 \leq r \leq \deg(u)$

$|V| = 1 + \sum_{i \in [r]} |V_i|$

$|E| = \deg(u) + \sum_{i \in [r]} |E_i|$

Induktionsbeweis mit Beispielaufgabe

Zeigen Sie die folgenden Behauptungen mittels vollständiger Induktion.

Gliedern Sie den jeweiligen Beweis korrekt in Induktionsbasis, -schritt, -annahme und -behauptung.

a) zz: für jedes $n \in \mathbb{N}_0$ gilt: $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$

Beweis mittels Induktion nach $n \in \mathbb{N}_0$:

- Induktionbasis: für $n=0$ gilt: $\sum_{k=0}^{0} k = 0 = \frac{0(0+1)}{2}$ ✓
- Induktionsschritt: Sei $n \in \mathbb{N}_0$ beliebig gewählt, aber im Weiteren fest.
  - Induktionsannahme: für das fixierte n gilt: $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$
  - Induktionsbehauptung: für das fixierte n gilt: $\sum_{k=0}^{n+1} k = \frac{(n+1)(n+2)}{2}$ (⇒ für $n+1$ gilt)

Beweis der Induktionsbehauptung:

$$\sum_{k=0}^{n+1} k = n+1 + \sum_{k=0}^{n} k$$

$$= n+1 + \frac{n(n+1)}{2} \quad \text{(nach IA)}$$

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

⇒ damit gilt die Behauptung für jedes $n \in \mathbb{N}_0$

1) Gradfolge: $G(V,E)$ für $V = \{v_1, v_2 \dots v_n\}$ ⟶ $(\deg(v_1), \deg(v_2) \dots \deg(v_n))$

Ein Graph heißt k-regulär wenn für alle $v \in V$ gilt, dass $\deg(v) = k$

Handschlaglemma: Für jeden Graphen $G = (V, E)$ gilt:

$$2|E| = \sum_{i \in [n]} \deg(v_i)$$

⇒

1) ein Graph kann höchstens dann existieren, falls $\sum_{i \in [n]} d_i$ gerade ist
2) ein einfacher Graph muss eine gerade Anzahl an Knoten von ungeradem Grad besitzen.
3) ein einfacher Graph mit $|V| > \frac{1}{2} \sum_{i \in [n]} d_i + 1$ kann nicht zshg. sein.

"weil sonst ist: $|V| > |E| + 1$ und der Graph hat nicht genug Kanten"

d.h.:
- falls $|V| > \frac{1}{2} \sum_{i \in [n]} d_i + 1$ ⇒ Graph nicht zshg.
- $|V| \leq \frac{1}{2} \sum_{i \in \mathbb{N}} d_i + 1$ ⇏ Graph zshg.

bsp:



$|V| = 5$
$|E| = 6 = \frac{1}{2} \sum \deg$
$|V| \leq \frac{1}{2} \sum \deg + 1$ aber Graph nicht zsh.

Realisierbarkeit von Gradfolge

-> Die neue Gradfolge wird aus $(d_1, \ldots, d_n)$ gewonnen, indem man (i) d_n entfernt, (ii) die letzten d_n Komponenten um 1 verkleinert und (iii) aufsteigend sortiert.

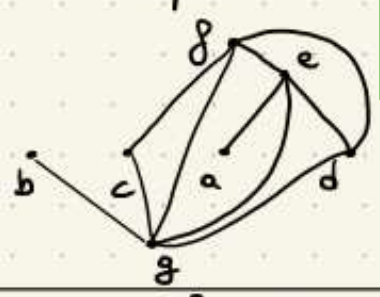
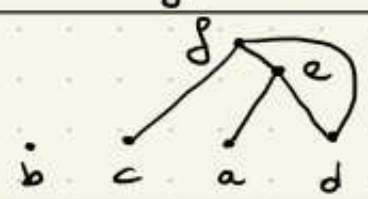
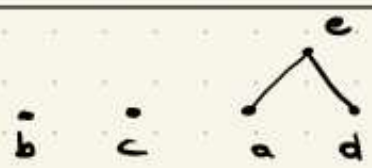
(⇒ Top down): Ist in G der Knoten mit maximalem Grad d_n genau mit Knoten der Grade $d_{n-1}, d_{n-2}, \ldots, d_{n-dn}$ verbunden, dann erhält man durch Entfernen dieses Knotens einen Graphen G' mit der (unsortierten) Gradfolge $(d_1, \ldots, d_{n-dn-1}, d_{n-dn} - 1, \ldots, d_{n-1} - 1)$.

(⇐ Bottom up): Hat man andererseits einen einfachen Graphen G' zu der unsortierten Gradfolge $(d_1, \ldots, d_{n-dn-1}, d_{n-dn} - 1, \ldots, d_{n-1} - 1)$ bereits gefunden, dann fügt man einfach einen neuen Knoten hinzu und verbindet diesen mit Knoten der Grade $d_{n-dn} - 1, \ldots, d_{n-1} - 1$.

Algorithmus von Havel Hakimi: "Havel Hakimi verbindet immer Knoten höchsten Grad"

Bsp: (1, 1, 2, 3, 4, 4, 5)

2 Phasen: Top down Reduktion der Gradfolge + bottom-up Konstruktion der Gradfolge

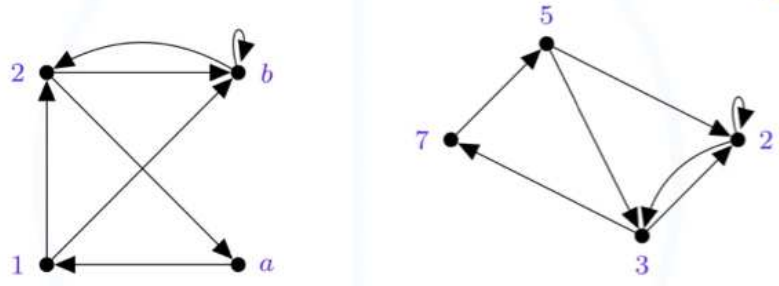
akt. Gradfolge	sort. Gradfolge	Graph
(1, 1, 2, 3, 4, 4, 5) a b c d e f g	(1, 1, 2, 3, 4, 4, 5) a b c d e f g	
(1, 0, 1, 2, 3, 3) a b c d e g	(0, 1, 1, 2, 3, 3) b a c d e g	
(0, 1, 0, 1, 2) b a c d e	(0, 0, 1, 1, 2) b c a d e	
(0, 0, 0, 0) b c a d	(0, 0, 0, 0) b c a d	

negativ
(0, -1, -1)
-> nicht realisierbar

Isomorphie:

- Zwei Digraphen G, H sind isomorph („strukturgleich"), kurz $G \cong H$, falls es eine Bijektion („Knotenumbenennung") $\beta\colon V_G \to V_H$ gibt, die die Kanten respektiert/erhält, d.h. uE_Gv gdw $\beta(u)E_H\beta(v)$
- ▷ Beispiel: $\beta(1) = 5, \beta(2) = 3, \beta(a) = 7, \beta(b) = 2$

1 → 2, 1 → b → $\beta(1) = 5$ → $\beta(2) = 3$, $\beta(b) = 2$



3) Bäume

jede Pfadgraphen ist ein Baum

Definition: Ein einfacher Graph $G = (V, E)$, der sowohl zusammenhängend als auch kreisfrei ist

Blatt: Ein Knoten $u \in V$ mit $\deg(u) = 1$

innere Knoten: alle anderen Knoten

Eigenschaften

- Ist $G = (V, E)$ ein Baum, dann gilt $|E| = |V| - 1$
- Jeder Baum $G = (V, E)$ mit $|V| \geq 2$ hat mindestens zwei Blätter
- Jeder einfache Graph $G = (V, E)$ mit $|E| \geq |V|$ enthält einen Kreis
- Jeder zushgd. einfache Graph $G = (V, E)$ besitzt aber mindestens $|E| \geq |V| - 1$ Kanten
- Jeder zusammenhängende Graph $G = (V, E)$ hat mindestens einen Spannbaum (Spannbaum -> Ein Teilgraph $T = (V, E')$ mit $E' \subseteq E$, der selbst ein Baum ist) -> "man entfernt einfache jede Kante die nicht für den Zusammenhang notwendig ist"

für einen einfachen Graph $G = (V, E)$

äquivalente Aussagen

(1) G ist ein Baum.

(2) G ist zushgd. und $|V| = |E| + 1$

(3) G ist kreisfrei und $|V| = |E| + 1$

(4) Zwei beliebige Knoten u, v sind durch genau einen einfachen Pfad in G verbunden

Für jeden Graph $G = (V, E)$ gilt:

- Es gibt eine Zusammenhangskomponente in G mit mindestens $\Delta(G) + 1$ Knoten.
- Jede Zusammenhangskomponente in G besitzt mindestens $\delta(G) + 1$ Knoten.

Für jeden Graph $G = (V, E)$ gilt:

G zusammenhängend	$\Longrightarrow$	$\lvert V\rvert \leq \lvert E\rvert + 1$	
G kreisfrei	$\Longrightarrow$	$\lvert V\rvert \geq \lvert E\rvert + 1$	
G kreisfrei	$\Longrightarrow$	$\lvert\{v \in V \mid \deg(v) = 1\}\rvert \geq 2$	(falls $\lvert V\rvert \geq 2$)
G kreisfrei	$\Longrightarrow$	G bipartit	(falls $\lvert E\rvert \geq 1$)
G bipartit	$\Longrightarrow$	$4\lvert E\rvert \leq \lvert V\rvert^2$	
$\Delta(G) + \delta(G) + 1 \geq \lvert V\rvert$	$\Longrightarrow$	G zusammenhängend	(folgt aus 3.)

Wurzelbäume $G = (V, E, r)$

Definition: ein Baum $G = (V, E)$ mit fest gewählter Wurzel $r \in V$

Höhe $h_G(v)$: der maximale Abstand (Länge des kürzestens Pfades) von der Wurzel zu einem Blatt

alle Kanten von der Wurzel weggerichtet: uEv für $\{u, v\} \in E$ und $h_G(v) = h_G(u) + 1''$
$h_G(v) = h_G(u) + 1$

im Fall uEv: u (Vater von v); v (Kind von u)

im Fall uE^*v : v (Nachfahre von u); u (Vorfahre von v)

Teilbaum T_u (durch die Nachfahre von u induziert)

- Höhe eines Knotens u in T -> Höhe von T_u
- Tiefe eines Knotens u in T -> Abstand von r zu u
- Level d Knoten -> Menge der Knoten mit Tiefe d

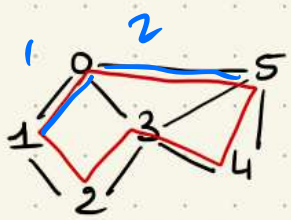
Eulertouren und Hamiltonkreise:

Sei $G = (V, E)$ ein einfacher zshg. Graph. Ein Pfad $v_0, v_1 \dots v_e$ mit $v_0 = v_e$ (geschlossener Pfad) heißt:

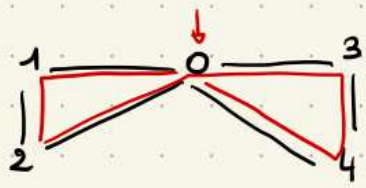
Eulertour, falls er jede Kante genau einmal besucht:

Hamiltonkreis, falls er jeden Knoten genau einmal besucht.

Beispiele:



Hamiltonkreis

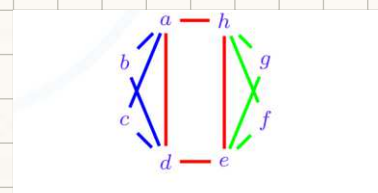


Eulertour

Kriterien:

Eulertouren: Existenz: ein zshg. einfacher Graph $G(V,E)$ besitzt eine Eulertour gdw jeder Knoten geraden (positiven) Knotengrad hat.

Beweis: Ein zusammenhängender einfacher Graph $G = (V, E)$, in dem jeder Knoten geraden Grad hat, besitzt eine Eulertour.



$\kappa = adeha$, $\kappa_1 = abdca$, $\kappa_2 = eghfe$

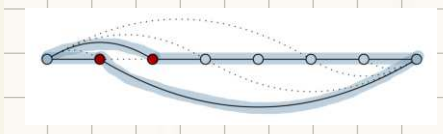
Eulertour: $(abdca)d(eghfe)ha$

äquivalent zu adeha

Hamiltonkreise: hinreichende Bedingung: für $K_{m,n}$ falls $m=n$ => Hamiltonkreis

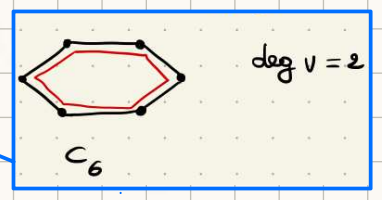
ein einfacher Graph $G=(V,E)$ mit $|V|>3$ besitzt einen Hamiltonkreis,

wenn in G jeder Knoten mindestens Knotengrad $\frac{|V|}{2}$ hat



Beweis: Ein einfacher Graph $G = (V, E)$, in dem jeder Knoten mindestens Grad $\frac{|V|}{2}$ hat, enthält einen Hamiltonkreis

Aus der Bedingung folgt die Existenz einen Hamiltonkreis aber es gibt Graphen mit Hamiltonkreise wo diese Bedingung nicht erfüllt ist.

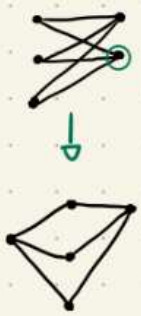


Planare Graphen und Knotenfärbungen: { Kantenanzahl $m \times n$ / Knotenanzahl $m+n$

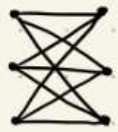
- ein einfacher Graph $G=(V,E)$ ist planar, falls man ihn in der zwei-dimensionalen Zeichenebene ohne Kantenüberschneidungen zeichnen kann.

Beispiele:

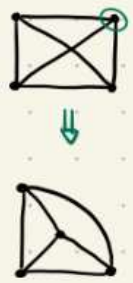
$K_{3,2}$: planar



$K_{3,3}$: nicht planar



K_4: planar



K_5: nicht planar

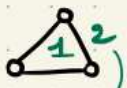


Eulersche Polyederformel (EPF):

- Sei $G=(V,E)$ ein zusammenhängender planarer Graph. Sei f die Anzahl der Flächen in die G bei überschneidungsfreier Darstellung die Zeichenebene zerschneidet, dann:

$$f - |E| + |V| = 2$$

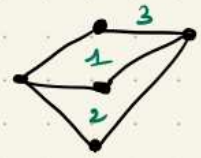
bsp:



$f=2$; $|E|=3$; $|V|=3$

$2-3+3=2$ ✓

Δ die umschließende Fläche wird mitgezählt



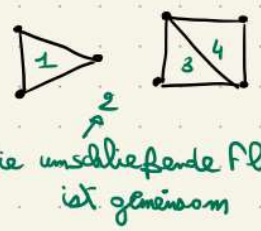
$f=3$; $|E|=6$; $|V|=5$

$3-6+5=2$ ✓

EPF für planare Graphen mit k max. zhgs. Komponenten:

$$f - |E| + |V| = 1 + k$$

bsp:



die umschließende Fläche ist gemeinsam

$f = 4$; $|E| = 8$; $|V| = 7$; $k = 2$

$4 - 8 + 7 \overset{?}{=} 1 + 2$ ✓

$= 3 \qquad = 3$

P_n ist für alle $n \geq 1$ planar.
C_n ist für alle $n \geq 3$ planar.
K_n ist nur für $n \leq 4$ planar.
$K_{m,n}$ ist nur für $m, n \leq 2$ planar.
$M_{m,n}$ ist für alle $m, n \geq 1$ planar.

Konsequenzen: Für jeden planaren Graphen $G = (V, E)$ gilt

- $f - |E| + |V| \geq 2$
- falls $|V| \geq 3$: $|E| \leq 3|V| - 6$ "Anzahl der Kanten muss begrenzt sein"
- es gibt mind. einen Knoten $u \in V$ mit $\deg(u) \leq 5$

Begründung:

jede Fläche wird durch mind. 3 Kanten definiert, dabei wird jede Kante doppelt gezählt:

$$f \leq \frac{2|E|}{3}$$

$$2 \leq f - |E| + |V| \leq \frac{2|E|}{3} - |E| + |V|$$

$$\Rightarrow \quad 2 \leq -\frac{1}{3}|E| + |V|$$

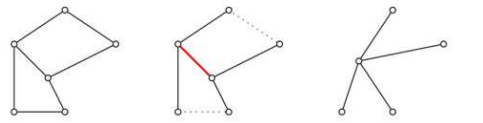
$$\overset{\times(-3)}{\Rightarrow} \quad -6 \geq |E| - 3|V|$$

$$\Rightarrow \quad \boxed{3|V| - 6 \geq |E|}$$

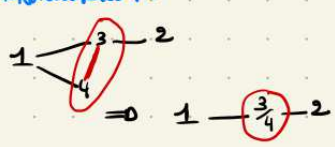
Minoren und Satz von Kuratowski

- Definition: Für zwei gegebene einfache Graphen $H = (V_H, E_H)$ und $G = (V_G, E_G)$ sagt man, dass „H ein Minor von G" ist, falls man aus G schrittweise mittels
  - ▷ Entfernen von Kanten,
  - ▷ Entfernen von Knoten vom Grad 0 und
  - ▷ Kantenkontraktion

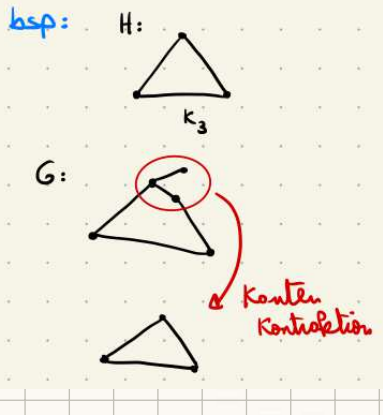
  einen zu H isomorphen Graphen erzeugen kann.



Kanten Kontraktion:



bsp:



▷ Satz von Kuratowski:

Ein einfacher Graph $G = (V, E)$ ist genau dann planar, wenn weder der $K_{3,3}$ noch der K_5 ein Minor von G ist.

$|\{v \in V \mid \deg(v) \geq 4\}| < 5$ und $|\{v \in V \mid \deg(v) \geq 3\}| < 6 \implies G$ planar

Anzahl der Knoten mit mindestens Grad 4 — Anzahl der Knoten mit mindestens Grad 3

Knotenfärbungen

$$\chi(G) \leq \frac{1}{2} + \sqrt{2\,|E| + \frac{1}{4}}$$

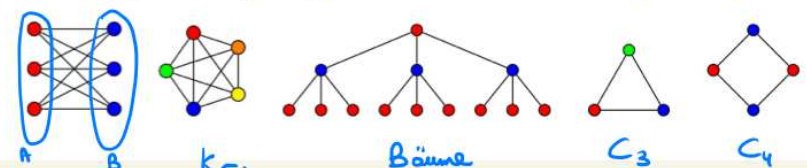
- Definition: Sei $G = (V, E)$ ein einfacher Graph.

  Eine Abbildung $c\colon V \to \mathbb{N}$ ist eine Knotenfärbung von G, falls $c(u) \neq c(w)$ für jede Kante $\{u, w\} \in E$ gilt.

  Die Anzahl der von c verwendeten Farben ist $|c(V)|$.

  Die chromatische Zahl $\chi(G)$ von G ist die minimale Anzahl von Farben, für die es eine Knotenfärbung von G gibt, d.h.

$$\chi(G) := \min\{|c(V)| \mid c\colon V \to \mathbb{N} \text{ Knotenfärbung von } G\}$$



Kanten nur zw. A und B

$\chi = 2$

- Beobachtungen:
  - $\chi(G) \leq |V|$ für jeden einfachen Graphen $G = (V, E)$.
  - $\chi(G) \leq 2$ genau dann, wenn G bipartit ist.
  - $\chi(G) > 1$, sobald $E \neq \emptyset$.
  - $\chi(K_n) = n$, $\chi(K_{m,n}) = 2$, $\chi(C_{2k}) = 2$, $\chi(C_{2k+1}) = 3$.
  - Für jeden einfachen Graphen $G = (V, E)$ gilt $\chi(G) \leq 1 + \max_{v \in V} \deg(v)$.

Jeder Graph mit maximalem Kontengrad D lässt sich mit $1 + D$ Farben färben

Vier-Farben-Satz: Für jeden einfachen planaren Graphen $G = (V, E)$ gilt $\chi(G) \leq 4$.

4-färbbar

Adjazenzmatrix eines Graphen

Matrizen

$M \in D^{m \times n}$ -> $m \times n$ Matrix über einer Menge D

-> eine Tabelle von Elementen von D mit m Zeilen und n Spalten

$M \in \mathbb{N}^{3\times 4}$ „3 Zeilen, 4 Spalten"

$$M = \begin{pmatrix} 0 & 2 & 3 & 1 \\ 0 & 1 & 2 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

Summe $C = A + B \in \mathbb{R}^{m \times n}$ definiert durch $C_{i,j} := A_{i,j} + B_{i,j}$

$$\begin{pmatrix} 1 & 2 & 0 \\ 3 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 1 \\ -2 & 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

Matrix Multiplikation nicht kommutativ

Produkt $C = A \cdot B \in \mathbb{R}^{k \times n}$ definiert durch $C_{i,j} := \sum_{t \in [m]} A_{i,t} \cdot B_{t,j}$

$A \times B$ „Zeilen von A mit Spalten von B multiplizieren"

„Spaltenzahl von A = Zeilenzahl von B"

$$\begin{pmatrix} 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 3 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 6 & 1 \\ 1 & -2 \end{pmatrix}$$

2×3-Matrix $\quad 3\times 2$-Matrix $\quad 2\times 2$ Matrix

$1\cdot 0 + 2\cdot 3 + 0\cdot 1 = 6$

) $A \in \mathbb{N}^{n\times n} \Rightarrow A^0$ ist die Einheitsmatrix E_n

bsp: $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \Rightarrow A^0 = E_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ $\quad A^3 \cdot A^0 = A^3$

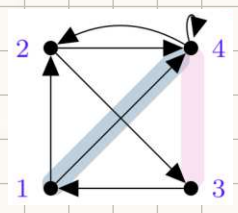
Adjazenzmatrix, Pfade zählen

$A_G = (a_{i,j})_{i,j\in[n]} \in \{0,1\}^{n\times n}$ mit ${}_n a_{i,j} = 1$ gdw. $v_i E v_j$

1 -> ja, der gerichtete Graph taucht auf

0 -> nein, der gerichtete Graph taucht nicht auf

$$A_G = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} \\ a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} \\ a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

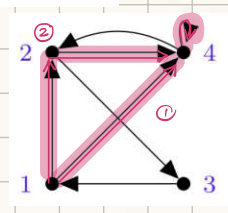


-> Anwendung: Random-Surfer-Modell

Für $k \in \mathbb{N}$ ist $\left(A_G^k\right)_{i,j}$ die Anzahl der verschiedenen k-Schritt-Pfade von v_i nach v_j

Summe 2

$$A_G^1 = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \quad A_G^2 = \begin{pmatrix} 0 & 1 & 1 & 2 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix} \quad A_G^3 = \begin{pmatrix} 1 & 2 & 1 & 3 \\ 0 & 2 & 1 & 3 \\ 0 & 1 & 1 & 2 \\ 1 & 2 & 1 & 3 \end{pmatrix}$$

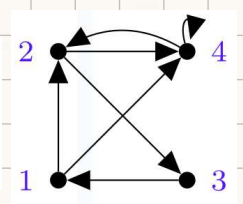


Übergangsmatrix

$\left(P_G^k\right)_{i,j}$ ist die Wahrscheinlichkeit von v_i nach v_j in genau k Schritten zu kommen

V: Webpages; E: Links; User klickt mit W'keit $p_{i,j} = \frac{1}{|v_i E|}$ auf Webpage v_i auf Link zu v_j (falls $v_i E v_j$; sonst $p_{i,j} = 0$).

$$P_G^1 = \begin{pmatrix} 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 0 & \frac{1}{2} & \frac{1}{2} \\ 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix} \quad P_G^2 = \begin{pmatrix} 0 & \frac{1}{4} & \frac{1}{4} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{4} & 0 & \frac{1}{4} \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & \frac{1}{4} & \frac{1}{4} & \frac{1}{2} \end{pmatrix} \quad P_G^3 = \begin{pmatrix} \frac{1}{4} & \frac{1}{4} & \frac{1}{8} & \frac{3}{8} \\ 0 & \frac{3}{8} & \frac{1}{8} & \frac{1}{2} \\ 0 & \frac{1}{4} & \frac{1}{4} & \frac{1}{2} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{8} & \frac{3}{8} \end{pmatrix}$$

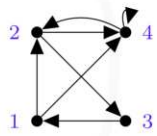


$P_G^n = P_G^{n-1} \cdot P_G$ z.B. $P_G^3 = P_G^2 \cdot P_G$

Dann verbringt der User im Mittel im Zeitraum $[0, T)$ beginnend in i auf j die Zeit $Q := \left(\frac{1}{T}\sum_{k=0}^{T-1} P_G^k\right)_{i,j}$

$T \to \infty$

▷ Beispiel: „Stark zusammenhängender" Graph



$$\frac{1}{100}\sum_{n=0}^{99} P_G^n \approx \begin{pmatrix} 0,1494 & 0,2845 & 0,1408 & 0,4253 \\ 0,1422 & 0,2902 & 0,1437 & 0,4239 \\ 0,1480 & 0,2816 & 0,1494 & 0,4210 \\ 0,1394 & 0,2845 & 0,1408 & 0,4353 \end{pmatrix} \xrightarrow{T\to\infty} \begin{pmatrix} \frac{1}{7} & \frac{2}{7} & \frac{1}{7} & \frac{3}{7} \\ \frac{1}{7} & \frac{2}{7} & \frac{1}{7} & \frac{3}{7} \\ \frac{1}{7} & \frac{2}{7} & \frac{1}{7} & \frac{3}{7} \\ \frac{1}{7} & \frac{2}{7} & \frac{1}{7} & \frac{3}{7} \end{pmatrix}$$

▷ Unabhängig, auf welcher Webpage User startet, er verbringt im Mittel $3/7$ seiner Zeit auf Webpage 4, $2/7$ auf Webpage 2 und je $1/7$ der Zeit auf den beiden restlichen.

Matchings mit Präferenz

Matching immer injektiv

Gesucht ist eine bijektive Abbildung $f : A \to B$ (mit $|A| = |B| = n$)

- **jede Frau $a \in A$ besitzt eine totale Präferenzordnung $\prec_a \subseteq B \times B$**
- **jeder Mann $b \in B$ besitzt entsprechend $_b \subseteq A \times A$**

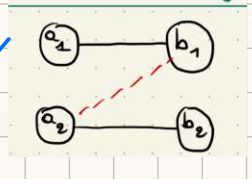
f ist instabil, falls es $a, a\prime \in A$ gibt mit
- $f(a) \prec_a f(a')$ **("a bevorzugt den Partner von a")**
- $a' \prec_{f(a')} a$ **("Der Partner von a' bevorzugt a")**

Personen: $A = \{a_1, a_2\}, B = \{b_1, b_2\}$

Präferenzen: $b_1 \prec_{a_1} b_2, \quad b_2 \prec_{a_2} b_1, \quad a_1 \prec_{b_1} a_2, \quad a_1 \prec_{b_2} a_2$

Instabiles Matching ("Ehe"): a_2 **präferiert** b_1, b_1 **präferiert** a_2

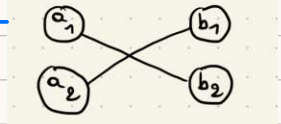
Instabiles Matching



Wenn zwei knoten beide lieber mit einander verbunden wären als mit dem knoten mit dem sie jeweils aktuell verbunden sind - instabil

Stabiles Matching ("Ehe"): a_1 **präferiert** b_2, a_2 **präferiert** b_1; b_1 **und** b_2 **präferieren** a_2; b_1 **hat seinen präferierten Partner,** b_2 **muss sich mit** a_1 **abfinden**

Stabiles Matching



Stabil heißt nicht, dass jeder seinen am meist präferierten Partner bekommt

Heiratssatz

Heiratssatz von Hall. Für einen bipartiten Graphen $G = (V_1, V_2, E)$ gibt es genau dann ein Matching M der Kardinalität $|V_1|$, wenn gilt:

$$\forall X \subseteq V_1 : |\Gamma(X)| \geq |X|.$$

Eine sehr sehr wichtige Folgerung von diesem Satz ist, dass jeder bipartite, k-reguläre Graph G ein perfektes Matching hat. D.h.:

$G = (V_1, V_2, E)$

G bipartit und k-regulär $\implies$ G hat perfektes Matching → $|V|$ ist gerade, $|V_1| = |V_2|$

perfektes Matching $|M| = \frac{|V|}{2}$

Gale-Shapley "Deferred Acceptance" Algorithmus

Solange es noch einen nicht verlobten Mann $b \notin \mathrm{im}(f)$ gibt:

- **b macht der Frau, die er unter denjenigen, die ihn noch nicht zurückgewiesen haben, am meisten begehrt (a) einen Antrag (größtes Element bzgl. $\prec b$)**
- **Wenn a noch nicht verlobt ist, verloben sich a und b ($f(a) := b$)**
- **Wenn a bereits verlobt ist und sie b ihrem aktuellen Partner $f(a)$ bevorzugt ($f(a) \prec_a b$), wird die Verlobung mit $f(a)$ aufgelöst und sie verlobt sich mit b ($f(a) := b$). Ansonsten lehnt sie b's Antrag ab.**

▷ Beispiel: $A = \{a_1, a_2, a_3, a_4\}$ und $B = \{b_1, b_2, b_3, b_4\}$

Frauen A verbessern

a_1 :	b_4	$\succ$	$\boxed{b_3}$	$\succ$	$b_1 \succ b_2$
a_2 :	$\boxed{b_2}$	$\succ$	b_4	$\succ$	$b_1 \succ b_3$
a_3 :	b_4	$\succ$	$\boxed{b_1}$	$\succ$	$b_2 \succ b_3$
a_4 :	b_3	$\succ$	b_2	$\succ$	$\boxed{b_4}$

verschlechtern B Männer

b_1 :	a_1	$\succ$	$\boxed{a_3}$	$\succ$	$a_4 \succ a_2$
b_2 :	a_1	$\succ$	a_3	$\succ$	$\boxed{a_2} \succ a_4$
b_3 :	a_2	$\succ$	$\boxed{a_1}$	$\succ$	$a_3 \succ a_4$
b_4 :	a_2	$\succ$	$\boxed{a_4}$	$\succ$	$a_1 \succ a_3$

$$(\neg A \vee B) \wedge (A \vee \neg B)$$
$$\equiv ((\neg A \vee B) \wedge A) \vee ((\neg A \vee B) \wedge \neg B)$$
$$\equiv ((\neg A \wedge A) \vee (B \wedge A)) \vee ((\neg A \wedge \neg B) \vee (B \wedge \neg B))$$
$$\equiv \underbrace{(\neg A \wedge A)}_{\text{false}} \vee (B \wedge A) \vee (\neg A \wedge \neg B) \vee \underbrace{(B \wedge \neg B)}_{\text{false}}$$
$$\equiv (A \wedge B) \vee (\neg A \vee \neg B)$$

Beobachtungen

Der Algorithmus terminiert also nach höchstens n^2 Runden

Keine zwei $a, a\prime \in A$ sind mit demselben $b \in B$ gematcht: Eine Frau verlobt sich nur mit einem alleinstehenden Mann

Die Zahl $|dom(f)|$ der gematchten $a \in A$ kann nicht abnehmen: Sobald eine Frau verlobt ist, wird die Verlobung nur aufgelöst, wenn sie einen neuen Partner gefunden hat.

Am Ende des Algorithmus ist $im(f) = B$: Jede Frau erhält irgendwann einen Antrag

Nach Terminierung: f ist ein ~~stabiles~~ perfekt Matching

-> f optimal für die Menge, die die Anträge macht (hier B)

Aussagenlogik

identisch — "genau dann ... wenn"

F	G	Konjunktion AND $F \wedge G$	NAND $\overline{F \wedge G}$	Disjunktion OR $F \vee G$	NOR $\overline{F \vee G}$	ExklusivOder XOR $F \oplus G$	"äquivalent" XNOR $F \equiv G$	bikonditional $F \leftrightarrow G$	Implikation $F \Rightarrow G$	Implikation $G \Rightarrow F$
0	0	0	1	0	1	0	1	1	1	1
0	1	0	1	1	0	1	0	0	1	0
1	0	0	1	1	0	1	0	0	0	1
1	1	1	0	1	0	0	1	1	1	1

Gültige Formel (Tautologie)

Lemma: Eine Formel F ist gültig genau dann, wenn für jede minimale Belegung β, die zu F passt, gilt: $[F](\beta) = 1$

Intuitiv: eine Formel ist gültig, wenn sie überall ("in allen Welten") wahr ist.

Widersprüchliche Formel (Widerspruch)

Lemma: Eine Formel F ist widersprüchlich (oder unerfüllbar), wenn für jede minimale Belegung β, die zu F passt, gilt: $[F](\beta) = 0$

Intuitiv: eine Formel ist widersprüchlich, wenn sie überall ("in allen Welten") falsch ist.

If-Then-Else-Operator

"wenn F, dann G, sonst H"

F	G	H	ITE(F,G,H)
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

$\text{ITE}(p,q,r) := ((p \to q) \wedge (\neg p \to r))$

- (allgemein) gültig: wenn für jede Belegung β, die zu F passt gilt $[F](\beta) = 1$
  (automatisch erfüllbar)
  ($F \equiv$ true) „in der Hauptspalte nur 1"
- erfüllbar: wenn für mind eine passende Belegung β gilt $[F](\beta) = 1$
  (aber nicht gültig)
  „wenn Hauptspalte mind eine 1 hat"
- unerfüllbar: wenn für jede passende Belegung β gilt $[F](\beta) = 0$
  ($F \equiv$ false) „in der Hauptspalte nur 0"

- $\neg F$ ist ein Widerspruch
- $F \equiv$ true
- true $\models F$

- $\neg F$ ist gültig
- $F \equiv$ false
- $F \models$ false

Logische Inferenz

Eine logische Inferenz ist eine Formel der Gestalt $F \to G$. Dabei ist F die Annahme und G die Konklusion.

"F impliziert G" bezeichnet die Formel $F \to G$

$F \models G$ (in Worten: "G folgt aus F") bezeichnet, dass die Formel $F \to G$ gültig ist

obwohl in Alltagssprache "G folgt aus F" und "F impliziert G" oft dieselbe Bedeutung

$\neg$	bindet stärker als	$\wedge$
$\wedge$	bindet stärker als	$\vee$
$\vee$	bindet stärker als	$\to$

$\neg\forall P \equiv \exists\neg P$
$\neg\exists P \equiv \forall\neg P$

& { unterschiedliche Syntax, gleiche Wahrheitstabelle } ⇒ semantisch äquivalent

Standardäquivalenzen

$(F \wedge F)$	$\equiv$	F	(Idempotenz)
$(F \vee F)$	$\equiv$	F	
$(F \wedge G)$	$\equiv$	$(G \wedge F)$	(Kommutativität)
$(F \vee G)$	$\equiv$	$(G \vee F)$	
$((F \wedge G) \wedge H)$	$\equiv$	$(F \wedge (G \wedge H))$	(Assoziativität)
$((F \vee G) \vee H)$	$\equiv$	$(F \vee (G \vee H))$	
$(F \wedge (F \vee G))$	$\equiv$	F	(Absorption)
$(F \vee (F \wedge G))$	$\equiv$	F	
$(F \wedge (G \vee H))$	$\equiv$	$((F \wedge G) \vee (F \wedge H))$	(Distributivität)
$(F \vee (G \wedge H))$	$\equiv$	$((F \vee G) \wedge (F \vee H))$	
$\neg\neg F$	$\equiv$	F	(Doppelnegation)
$\neg(F \wedge G)$	$\equiv$	$(\neg F \vee \neg G)$	(deMorgan)
$\neg(F \vee G)$	$\equiv$	$(\neg F \wedge \neg G)$	
$(F \wedge \neg F)$	$\equiv$	false	(Triviale Kontradiktion)
$(F \vee \neg F)$	$\equiv$	true	(Triviale Tautologie)
$(F \wedge \text{false})$	$\equiv$	false	(Dominanz)
$(F \vee \text{true})$	$\equiv$	true	
$(F \wedge \text{true})$	$\equiv$	F	(Identität)
$(F \vee \text{false})$	$\equiv$	F	
$(F \to G)$	$\equiv$	$(\neg F \vee G)$	(Implikation)
$(F \leftrightarrow G)$	$\equiv$	$((F \to G) \wedge (G \to F))$	(Bikonditional)
	$\equiv$	$\neg(F \oplus G)$	
$(F \oplus G)$	$\equiv$	$((F \vee G) \wedge (\neg F \vee \neg G))$	(XOR)
	$\equiv$	$((F \wedge \neg G) \vee (\neg F \wedge G))$	

Disjunktive Normalform (DNF)

$$\bigvee_{i=1}^{m}\left(\bigwedge_{j=1}^{m_i} L_{i,j}\right)$$

Eine Formel in DNF: $(p \wedge \neg q) \vee (\neg p \wedge \neg q \wedge r) \vee q$

Kanonische DNF

Disjunktion über alle Konjunktionen (aller minimalen erfüllenden Belegungen)

$D_F = (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (p \wedge q \wedge r)$

p	q	r	$((p$	$\rightarrow$	$q)$	$\wedge$	$(\neg$	p	$\rightarrow$	$r))$
0	0	0		1		0	1		0	
0	0	1		1		1	1		1	
0	1	0		1		0	1		0	
0	1	1		1		1	1		1	
1	0	0		0		0	0		1	
1	0	1		0		0	0		1	
1	1	0		1		1	0		1	
1	1	1		1		1	0		1	

Konjunktive Normalform (KNF)

$$\bigwedge_{i=1}^{m}\left(\bigvee_{j=1}^{m_i} L_{i,j}\right)$$

Eine Formel in KNF: $(p \vee \neg q) \wedge (\neg p \vee \neg q \vee r) \wedge q$

Kanonische KNF

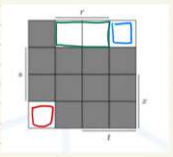
Konjunktion über alle Disjunktionen (aller minimalen nicht-erfüllenden Belegungen)

① $DNF_{\neg F} = (\neg p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge \neg r) \vee (p \wedge \neg q \wedge r)$

② $K_F = (p \vee q \vee r) \wedge (p \vee \neg q \vee r) \wedge (\neg p \vee q \vee r) \wedge (\neg p \vee q \vee \neg r)$

alles negieren

KV-Diagramm lesen und in KNF darstellen



c)

KNF?

Idee: DNF für $\neg K$ ablesen und dann negieren

$\neg K = (r \wedge \neg s \wedge \neg x) \vee (\neg r \wedge \neg s \wedge \neg x \wedge t) \vee (\neg r \wedge \neg s \wedge \neg t \wedge x)$

$\Rightarrow$ KNF: $K \equiv \neg\neg K \equiv \neg\left((r \wedge \neg s \wedge \neg x) \vee (\neg r \wedge \neg s \wedge \neg x \wedge t) \vee (\neg r \wedge \neg s \wedge \neg t \wedge x)\right)$

$\overset{\text{(De Morgan)}}{\equiv} \left(\neg(r \wedge \neg s \wedge \neg x) \wedge \neg(\neg r \wedge \neg s \wedge \neg x \wedge t) \wedge \neg(\neg r \wedge \neg s \wedge \neg t \wedge x)\right)$

$\equiv (\neg r \vee s \vee x) \wedge (r \vee s \vee x \vee \neg t) \wedge (r \vee s \vee t \vee \neg x)$

$\Rightarrow \{\{\neg r, s, x\}, \{r, s, x, \neg t\}, \{s, t, r, \neg x\}\}$

„Erfüllbarkeitsäquivalenz":

„$F \equiv_e G$" für erfüllbarkeitsäquivalent, dh es gibt eine erfüllende Belegung β_F für F gdw es eine erfüllende Belegung β_G für G gibt.

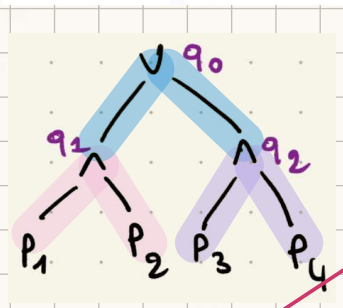
„β_F muss nicht zu G passen und β_G nicht zu F"

⚠ ▷ Jede erfüllende Belegung von E_F ist erfüllende Belegung von F; jede erfüllende Belegung von F lässt sich zu erfüllender, aber auch unerfüllender Belegung von E_F erweitern: $F \equiv_e E_F$, $F \not\equiv E_F$!

Problem: $F \equiv (p_1 \wedge p_2) \vee (p_3 \wedge p_4) \vee \ldots \vee (p_{2k-1} \wedge p_{2k})$ $\xrightarrow{\text{KNF?}}$ $(p_1 \vee \ldots) \wedge (p_2 \vee \ldots) \wedge \ldots$

→ Lösung: finde eine erfüllbarkeitsäquivalente KNF.

$F = (p_1 \wedge p_2) \vee (p_3 \wedge p_4)$



① Syntaxbaum aufstellen + zusätzliche Hilfsvariable für jeden Knoten einfügen

② Teilformel mit Hilfsvariable $q_0 \wedge (q_0 \leftrightarrow (q_1 \vee q_2)) \wedge (q_1 \leftrightarrow (p_1 \wedge p_2)) \wedge (q_2 \leftrightarrow (p_3 \wedge p_4))$

"Hilfsvariablen sind erfüllt genau dann, wenn ihre repräsentierte Teilformel erfüllt ist"

③ jede einzelne Teilformel muss in KNF überführt werden

$$E_F := q_0 \wedge (\neg q_0 \vee q_1 \vee q_2) \wedge (q_0 \vee \neg q_1) \wedge (q_0 \vee \neg q_2) \wedge (q_1 \vee \neg p_1 \vee \neg p_2) \wedge (\neg q_1 \vee p_1) \wedge (\neg q_1 \vee p_2) \wedge (q_2 \vee \neg p_3 \vee \neg p_4) \wedge (\neg q_2 \vee p_3) \wedge (\neg q_2 \vee p_4)$$

⇒ Klauseldarstellung von KNF-Formel

Hilfstabelle

(a) $(A \leftrightarrow (B \wedge C)) \equiv (A \vee \neg B \vee \neg C) \wedge (\neg A \vee B) \wedge (\neg A \vee C)$

(b) $(A \leftrightarrow (B \vee C)) \equiv (\neg A \vee B \vee C) \wedge (A \vee \neg B) \wedge (A \vee \neg C)$

(c) $(A \leftrightarrow \neg B) \equiv (A \vee B) \wedge (\neg A \vee \neg B)$

(d) $(A \leftrightarrow (B \leftrightarrow C)) \equiv (\neg A \vee \neg B \vee C) \wedge (\neg A \vee B \vee \neg C) \wedge (A \vee B \vee C) \wedge (A \vee \neg B \vee \neg C)$

(e) $(A \leftrightarrow (B \oplus C)) \equiv (\neg A \vee B \vee C) \wedge (\neg A \vee \neg B \vee \neg C) \wedge (A \vee \neg B \vee C) \wedge (A \vee B \vee \neg C)$

(f) $(A \leftrightarrow (B \rightarrow C)) \equiv (\neg A \vee \neg B \vee C) \wedge (A \vee B) \wedge (A \vee \neg C)$

$\{\{q_0\},$
$\{\neg q_0, q_1, q_2\}, \{q_0, q_1\}, \{q_0, \neg q_2\},$
$\{q_1, \neg p_1, \neg p_2\}, \{\neg q_1, p_1\}, \{\neg q_1, p_2\},$
$\{q_2, \neg p_3, \neg p_4\}, \{\neg q_2, p_3\}, \{\neg q_2, p_4\}\}$

DPLL: Davis-Putnam-Logemann-Loveland

Ziel: „eine erfüllende Belegung zu finden auch wenn es mehrere gäben"

Klauseldarstellung von KNF:

$\{\{\neg p\}, \{p, \neg q, r\}\}$ stellt $\neg p \wedge (p \vee \neg q \vee r)$ dar

$\neg p \vee \text{false} \equiv \neg p$ dh: $\{\neg p\} = \{\neg p, \text{false}\}$

$\neg p \wedge (p \vee \neg q \vee r) \wedge \text{True} \equiv \neg p \wedge (p \vee \neg q \vee r)$ dh:

$\{\{\neg p\}, \{p, \neg q, r\}\} = \{\{\neg p\}, \{p, \neg q, r\}, \text{true}\}$

$$\begin{aligned} \text{true} \vee G &\equiv \text{true} \\ \text{false} \vee G &\equiv G \end{aligned}$$

$$\begin{aligned} \text{true} \wedge G &\equiv G \\ \text{false} \wedge G &\equiv \text{false} \end{aligned}$$

$$\begin{aligned} \neg\text{true} &\equiv \text{false} \\ \neg\text{false} &\equiv \text{true} \end{aligned}$$

true $\{\}$ (leere Klauselmenge, nichts zu erfüllen, trivial erfüllt) Falls $\mathcal{K} = \emptyset$,

false $\{\{\}\}$ (Klauselmenge mit leerer Klausel, unerfüllbar) Falls $\{\} \in \mathcal{K}$

→ Basisversion: DPLL macht sehr viele unnötige Fallunterscheidungen

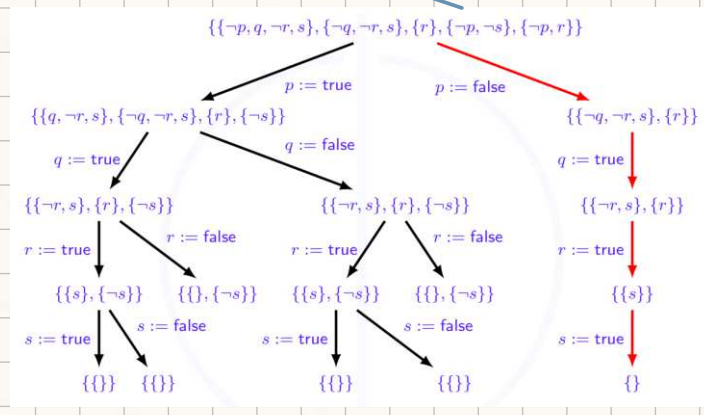
Gegeben Klauselmenge $\mathcal{K}$, totale Ordnung auf den Variablen $\prec$

- Falls $\{\} \in \mathcal{K}$, gib unerfüllbar zurück.
- Falls $\mathcal{K} = \emptyset$, gib erfüllbar zurück.
- Ansonsten fixiere die bzgl. $\prec$ erste in $\mathcal{K}$ vorkommende Variable x.

  Prüfe rekursiv, ob $\{C \setminus \{\neg x\} \mid C \in \mathcal{K}, x \notin C\}$ erfüllbar ist;

  falls ja, gib erfüllbar zurück;

  ansonsten gib Ergebnis der Rekursion zu $\{C \setminus \{x\} \mid C \in \mathcal{K}, \neg x \notin C\}$ zurück



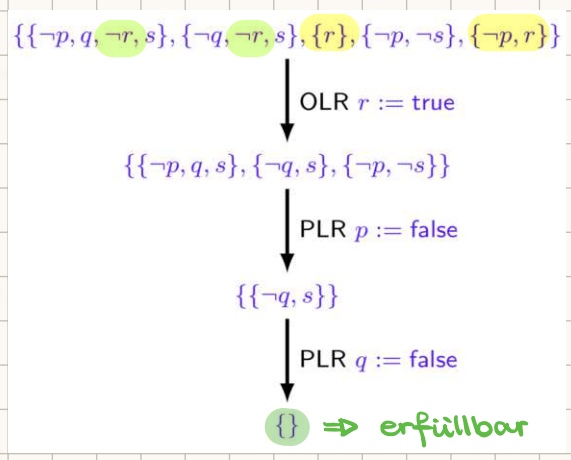
Erweiterte DPLL (um unnötige Fallunterscheidungen zu vermeiden)

1. **OLR (one-literal rule): falls eine Klausel nur aus einem Literal besteht -> setze dieses wahr**
2. **PLR (pure-literal rule): falls nur L in den Klauseln vorkommt, aber $\bar{L}$ nicht -> setze L wahr**
3. **erst dann Fallunterscheidung**

$$A \prec \neg A \prec B \prec \neg B \prec C \prec \neg C \prec D \prec \neg D$$

Literal = true -> diese ganze Klausel löschen

Literal = false -> nur dieses Literal löschen



Resolution (muss nicht alle Klausel / Variable benutzt, kann mehrfach benutzt)

Ziel: die leere Klausel aus der ursprünglichen Klauselmenge resolvieren -> nicht Erfüllbarkeit

Grundidee: füge iterativ neue Klauseln zur Formel hinzu, die logische Konsequenzen der ursprünglichen Klauseln sind

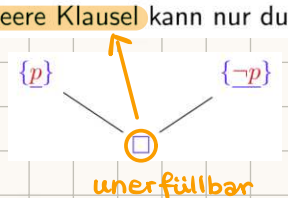
resolvent zwei Klausel k_1, k_2

$$K_1, K_2 \models \underbrace{(K_1 \setminus \{L\}) \cup (K_2 \setminus \{\bar{L}\})}_{\text{Resolvent}}$$

bsp. $\{\neg p, q, r\}$ und $\{\neg r, s, t\}$ ⇒ $\{\neg p, q, s, t\}$

⚠ immer genau ein Literal

Die leere Klausel kann nur durch



Warum dürfen wir das machen?

$(\neg p \vee q \vee r)$ | $(\neg r \vee s \vee t)$

$\equiv (\neg p \vee q) \vee r$ | $\equiv \neg r \vee (s \vee t)$

$\equiv (p \wedge \neg q) \rightarrow r$ | $\equiv r \rightarrow (s \vee t)$

Transitivität der Implikation

$(p \wedge \neg q) \rightarrow (s \vee t) \equiv \neg p \vee q \vee s \vee t$

$\{\neg p, q, s, t\}$

Kombinatorische Grundprinzipien

Summenregel: $\left|\dot{\bigcup}_{i\in[n]} A_i\right| = |A_1| + |A_2| + \cdots + |A_n|$

↑ disjunkte Vereinigung

Siebformel: $\left|\bigcup_{i\in[n]} A_i\right| = \sum_{I\subseteq[n]:I\neq\emptyset} (-1)^{|I|+1} \left|\bigcap_{i\in I} A_i\right|$

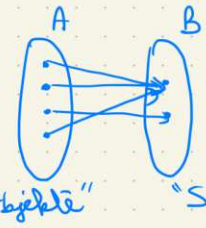
bsp: $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$

Produktregel: $|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdot \ldots \cdot |A_n|$

Schubfachprinzip:

Für jedes $f: A \to B$ gibt es ein $b \in B$ sodass $|f^{-1}(b)| \geq \lceil |A|/|B| \rceil$

bsp:



"Objekte" "Schubfächer"

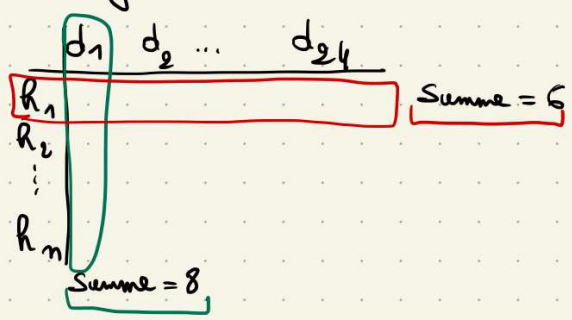
Doppeltes Abzählen Für jedes $R \subseteq S \times T$ gilt $\sum_{s\in S} |\{t \in T \mid (s,t) \in R\}| = \sum_{t\in T} |\{s \in S \mid (s,t) \in R\}|$

Summe der Spaltensummen $\sum_{j\in[n]} \sum_{i\in[m]} m_{i,j}$ = Summe der Zeilensummen $\sum_{i\in[m]} \sum_{j\in[n]} m_{i,j}$

Bsp: In einem Tanzkurs gibt es 24 Damen und n Herren. Nach der Tanzstunde hat jede Dame mit genau 8 Herren getanzt, jeder Herr mit genau 6 Damen.

$n = ?$

→ Modellierung als Tabelle:



Σ Zeilensumme $= \Sigma$ Spaltensumme

$\Rightarrow 6 \cdot n = 24 \cdot 8$

$n = \frac{24 \cdot 8}{6} = 32$

Urnenmodell

Wir ziehen k Elemente aus einer n-elementigen Menge.

	mit Zurücklegen	ohne Zurücklegen
mit Reihenfolge	n^k	$A_{n,k} = \{(s_1,\ldots,s_k) \in [n]^k \mid \lvert\{s_1 \ldots s_k\}\rvert = k\} = \frac{n!}{(n-k)!}$ (k verschiedene Elemente)
ohne Reihenfolge	$C_{n,k} = \{(s_1,\ldots,s_k) \in [n]^k \mid s_1 \leq s_2 \leq \cdots \leq s_k\} = \binom{n+k-1}{k}$	$B_{n,k} = \{(s_1,\ldots,s_k) \in [n]^k \mid s_1 < s_2 < \cdots < s_k\} = \binom{n}{k} = \frac{n!}{(n-k)!\,k!}$ ("k-elementigen Teilmengen von [n]")

. Binomialkoeffizient:

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

bsp:

$$\binom{4}{2} = \frac{4!}{2!} = 6 \Rightarrow \text{es gibt 6 2-elementige Teilmengen von } [4]$$

$$\{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}$$

. die Binomial Formel: $\forall x, y \in \mathbb{R}\ ; n \in \mathbb{N}_0$

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

$$(x+1)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$$

Anwendung ↓

die Vandermondesche Identität:

$$\binom{m+n}{k} = \sum_{i=0}^{k} \binom{m}{i}\binom{n}{k-i}$$

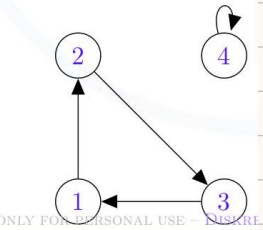
Stirling-Zahlen 1.Art $S_{n,k}$ → Die Anzahl der Permutationen von $[n]$ mit genau k Zykeln

$= S_{n+1,k}$

$$\begin{bmatrix} n+1 \\ k \end{bmatrix} = \begin{bmatrix} n \\ k-1 \end{bmatrix} + n \cdot \begin{bmatrix} n \\ k \end{bmatrix} \text{ mit } \begin{bmatrix} n \\ n \end{bmatrix} = 1, \begin{bmatrix} n+1 \\ 0 \end{bmatrix} = 0$$

innerhalb des Zykels → darf zyklisch rotiert
außerhalb des Zykels → darf nicht vertauscht

$(231)(4) =$
$(123)(4) =$
$(312)(4) =$



CHEN GEBRAUCH/ONLY FOR PERSONAL USE – DISKRE

↳ **Zykelschreibweise** $f = (x_0^{(1)} x_1^{(1)} \dots x_{l_1-1}^{(1)})(x_0^{(2)} x_1^{(2)} \dots x_{l_2-1}^{(2)}) \dots (x_0^{(k)} x_1^{(k)} \dots x_{l_k-1}^{(k)})$

(l_1 = Länge)

Anzahl Permutationen von $[n]$ in gegebene Zykelgrößen $(\lambda_1, \dots, \lambda_n)$ $(\sum_{i=1}^{n} i\lambda_i = n)$

$$\frac{n!}{1^{\lambda_1} \cdots n^{\lambda_n} \cdot \lambda_1! \cdots \lambda_n!}$$

Stirling-Zahlen 2.Art $S_{n,k}$ → Die Anzahl der Partitionen von n Elementen in k (nicht leere) Klassen

n nicht unterscheidbar
k nicht unterscheidbar

$$|F_{n,k}| = \left|\{(s_1, \dots, s_k) \in [n]^k \mid |\{s_1, s_2, \dots, s_k\}| = n\}\right| = n! S_{k,n}$$

mit $= S_{n+1,k}$

$$\left\{ n+1 \atop k \right\} = \left\{ n \atop k-1 \right\} + k \cdot \left\{ n \atop k \right\} \text{ mit } \left\{ n \atop n \right\} = 1, \left\{ n+1 \atop 0 \right\} = 0$$

n nicht unterscheidbar
k unterscheidbar

In $F_{n,k}$ bezeichnet n die Anzahl der Klassen und k die Anzahl der Objekte.

In $S_{n,k}$ bezeichnet n die Anzahl der Objekte und k die Anzahl der Klassen.

Anzahl Partitionen von $[n]$ in gegebene Klassengrößen $(\lambda_1, \dots, \lambda_n)$ $(\sum_{i=1}^{n} i\lambda_i = n)$

$$\frac{n!}{(1!)^{\lambda_1} \cdots (n!)^{\lambda_n} \cdot \lambda_1! \cdots \lambda_n!}$$

▷ Für jede Partition von n Elementen in k (nicht leere) Klassen gibt es genau $k!$ geordnete Partitionen. Z.B. für $n = 4, k = 3$ haben wir

$$\{\{2\},\{1,4\},\{3\}\} \mapsto \left\{ \begin{array}{ll} (\{2\},\{1,4\},\{3\}) & , \ (\{2\},\{3\},\{1,4\}) \\ (\{1,4\},\{2\},\{3\}) & , \ (\{1,4\},\{3\},\{2\}) \\ (\{3\},\{1,4\},\{2\}) & , \ (\{3\},\{2\},\{1,4\}) \end{array} \right\}$$

geordnete Zahlpartition

:) Zählvektoren mit K-Einträgen und Summe n: { n nicht unterscheidbar, K unterscheidbar

$$D_{n,K} = \{(s_1, \dots, s_K) \in \mathbb{N}_0^K \mid s_1 + s_2 + \dots + s_K = n\}$$

$$= \binom{n+K-1}{n} = C_{K,n}$$

Warum? Analogie: Striche und Kommas:

Bsp: teile 7 in 3 Summanden

1 + 2 + 4 oder 3 + 0 + 4

|, ||, |||| ||| , , ||||

diese String hat immer Länge $n + K - 1$ (n Striche, K − 1 Kommas)

String ist eindeutig durch Positionen der Kommas definiert.

$$\Rightarrow |D_{n,K}| = \binom{n+K-1}{K-1} = \binom{n+K-1}{n}$$

$$\binom{n}{K} = \binom{n}{n-K}$$

:) $k-1$ Plus-Zeichen aus den insgesamt $n-1$ Plus-Zeichen auszuwählen

$$|G_{n,k}| = |\{(s_1, \dots, s_k) \in \mathbb{N}^k \mid s_1 + s_2 + \dots + s_k = n\}| = \binom{n-1}{k-1}$$

{ n nicht unterscheidbar, K unterscheidbar

(Ungeordnete) Zahlpartition

:) Zählvektoren mit K Einträgen und Summe höchstens n

$$E_{n,K} = \{(s_1, \dots, s_K) \in \mathbb{N}_0^K \mid s_1 + \dots + s_K \leq n\}$$

$$|D_{n,K+1}| = |E_{n,K}| = \binom{n+K}{n}$$

Wieviele Möglichkeiten gibt es, n Euro in k Päckchen aufzuteilen, wenn Päckchen auch 0 Euro enthalten dürfen?

$$H_{n,k} = \{(s_1, \dots, s_k) \in \mathbb{N}_0^k \mid s_1 + \dots + s_k = n, s_1 \leq \dots \leq s_k\}$$

$$|H_{n,K}| = |P_{n+K,K}|$$

:) Partition von n → Anzahl Zahlpartitionen von n in k positive Summanden

$$P_{n,k} := \{(s_1, \dots, s_k) \in \mathbb{N}^k \mid s_1 + \dots + s_k = n, s_1 \leq s_2 \leq \dots \leq s_k\}$$

▷ Es folgt somit für $0 \leq k, n$

$$\begin{aligned} |P_{n,k}| &= |P_{n-1,k-1}| + |P_{n-k,k}| && \text{für } k > 0 \\ |P_{n,0}| &= 0 && \text{für } n > 0 \\ |P_{n,k}| &= 0 && \text{für } k > n \\ |P_{n,n}| &= 1 \end{aligned}$$

{ n Euros nicht unterscheidbar, K Kinder nicht unterscheidbar

Kombinatorik Formelsammlung

Urnenmodell

Ziehen von k Kugeln aus insgesamt n Kugeln

- ohne Zurücklegen, mit Beachtung der Reihenfolge:
  $|\{(s_1,\ldots,s_k) \in [n]^k : |\{s_1,s_2,\ldots,s_k\}| = k\}| = |A_{n,k}| = \frac{n!}{(n-k)!}$
- ohne Zurücklegen, ohne Beachtung der Reihenfolge:
  $|\{(s_1,\ldots,s_k) \in [n]^k : s_1 < s_2 < \ldots < s_k\}| = |B_{n,k}| = \binom{n}{k} = \frac{n!}{(n-k)!k!}$
- mit Zurücklegen, mit Beachtung der Reihenfolge:
  $|\{(s_1,\ldots,s_k) \in [n]^k\}| = n^k$
- mit Zurücklegen, ohne Beachtung der Reihenfolge:
  $|\{(s_1,\ldots,s_k) \in [n]^k : s_1 \leq s_2 \leq \ldots \leq s_k\}| = |C_{n,k}| = \binom{n+k-1}{k}$

Zählvektoren

- $|\{(s_1,\ldots,s_k) \in \mathbb{N}_0^k : s_1+s_2+\ldots+s_k = n\}| = |D_{n,k}| = \binom{n+k-1}{n} = |C_{k,n}|$
- $|\{(s_1,\ldots,s_k) \in \mathbb{N}_0^k : s_1+s_2+\ldots+s_k \leq n\}| = |D_{n,k+1}| = \binom{n+k}{n}$
- $|\{(s_1,\ldots,s_k) \in \mathbb{N}^k : s_1+s_2+\ldots+s_k = n\}| = |G_{n,k}| = |D_{n-k,k}| = \binom{n-1}{k-1}$
- $|\{(s_1,\ldots,s_k) \in \mathbb{N}^k : s_1+s_2+\ldots+s_k = n, s_1 \leq \ldots \leq s_k\}| = |P_{n,k}|$
  (Anzahl Zahlpartitionen von n in k Summanden > 0)
- $|\{(s_1,\ldots,s_k) \in \mathbb{N}_0^k : s_1+s_2+\ldots+s_k = n, s_1 \leq \ldots \leq s_k\}| = |H_{n,k}| = |P_{n+k,k}|$
  (Anzahl Zahlpartitionen von n in k Summanden ≥ 0)

Stirlingszahlen

- Stirlingzahlen 1. Art: Anzahl Permutationen von $[n]$ in k Zyklen: $s_{n,k} = \begin{bmatrix} n \\ k \end{bmatrix}$
  - Anzahl Permutationen von $[n]$ in gegebene Zykelgrößen $(\lambda_1,\ldots,\lambda_n)$ $(\sum_{i=1}^n i\lambda_i = n)$

$$\frac{n!}{1^{\lambda_1}\cdots n^{\lambda_n}\cdot\lambda_1!\cdots\lambda_n!}$$

- Stirlingzahlen 2. Art: Anzahl Partitionen von $[n]$ in k Klassen: $S_{n,k} = \left\{ n \atop k \right\}$
  - Anzahl Partitionen von $[n]$ in gegebene Klassengrößen $(\lambda_1,\ldots,\lambda_n)$ $(\sum_{i=1}^n i\lambda_i = n)$

$$\frac{n!}{(1!)^{\lambda_1}\cdots(n!)^{\lambda_n}\cdot\lambda_1!\cdots\lambda_n!}$$

Jede Gruppe min. ein Objekt enthält

- Aufteilen von n Objekten in k Gruppen, sodass jede Gruppe mind. ein Objekt enthält
  - Objekte und Gruppen unterscheidbar: $k! \cdot S_{n,k}$
    (Anzahl surjektiver Funktionen von $[n]$ auf $[k]$)
  - Objekte unterscheidbar, Gruppen nicht unterscheidbar: $S_{n,k}$
    (Anzahl Äquivalenzrelationen über $[n]$ mit genau k Klassen)
  - Objekte nicht unterscheidbar, Gruppen unterscheidbar:
    $|\{(s_1,\ldots,s_k) \in \mathbb{N}^k : s_1+s_2+\ldots+s_k = n\}| = |G_{n,k}| = \binom{n-1}{k-1}$
  - Objekte und Gruppen nicht unterscheidbar:
    $|\{(s_1,\ldots,s_k) \in \mathbb{N}^k : s_1+s_2+\ldots+s_k = n, s_1 \leq \ldots \leq s_k\}| = |P_{n,k}|$

Darf ein beliebiges Element aus dieser Menge mit
1. mehreren
2. Null

Elementen aus der anderen Menge in Verbindung stehen?

1. Frage	*ja*	*nein*	*ja*	*nein*
2. Frage	*ja*	*ja*	*nein*	*nein*
Verteilung	beliebig	injektiv	surjektiv	bijektiv

Funktion
$[n] \to [k]$

genaue Menge

Anzahl der abgebildeten Knoten

n Objekte auf k Gruppe	beliebig viele Objekte pro Gruppe („beliebig")	höchstens ein Objekt pro Gruppe („injektiv")	mindestens ein Objekt pro Gruppe („surjektiv")	genau ein Objekt pro Gruppe („bijektiv")
Objekte unterscheidbar Gruppe unterscheidbar	+ Zurücklegen + Reihenfolge k^n	− Zurücklegen + Reihenfolge $k^{\underline{n}} = \frac{k!}{(k-n)!}$	$k! \cdot S_{n,k}$	$n!$
Objekte nicht unterscheidbar Gruppe unterscheidbar	+ Zurücklegen − Reihenfolge $\binom{n+k-1}{n}$	− Zurücklegen − Reihenfolge $\binom{k}{n}$	$\binom{n-1}{k-1}$	1
Objekte unterscheidbar Gruppe nicht unterscheidbar	$\sum_{i=0}^k S_{n,i}$	1	$S_{n,k}$	1
Objekte nicht unterscheidbar Gruppe nicht unterscheidbar	$\sum_{i=0}^k P_{n,i}$	1	$P_{n,k}$	1

Teilbarkeitsproblem

Siebformel

Bestimmen Sie mit Hilfe des Prinzips von Inklusion und Exklusion die Anzahl der Zahlen ≤ 1000, die weder durch 3 noch durch 5 noch durch 7 teilbar sind.

$\Omega = \{0 \dots 1000\}$

Sei $A_K = \{n \in \{0 \dots 1000\} \mid K \text{ teilt } n\}$ „Zahlen ≤ 1000 die durch K teilbar sind"

$|A_K| = \left\lfloor \frac{1000}{K} \right\rfloor + 1$ wenn man 0 mitzählt

$\Rightarrow |\Omega \setminus \{A_3 \cup A_5 \cup A_7\}| = ?$

- $|A_3 \cup A_5 \cup A_7| = |A_3| + |A_5| + |A_7| - \underbrace{|A_3 \cap A_5|}_{A_{15}} - \underbrace{|A_3 \cap A_7|}_{A_{21}} - \underbrace{|A_5 \cap A_7|}_{A_{35}} + \underbrace{|A_3 \cap A_5 \cap A_7|}_{A_{105}}$

$= 334 + 201 + 143 - 67 - 48 - 29 + 10$

$= 544$

$\Rightarrow |\Omega \setminus \{A_3 \cup A_5 \cup A_7\}| = |\Omega| - |A_3 \cup A_5 \cup A_7|$

$= 1001 - 544 = 457$

$a \mid b \Rightarrow \frac{b}{a}$ "a teilt b" (b geteilt durch a ohne Rest)

EEA (euklidischer Algorithmus)

a	b=n	$K = \lfloor \frac{b}{a} \rfloor$	α	β
935	1491	1	716	−449
556	935	1	−449	267
379	556	1	267	−182
~~177~~	379	2	−182	85
25	~~177~~	7	85	−12
2	25	12	−12	1
1	2	2	1	0
(0	1	–	0	1)

ggT → 1

runter:

$a_{new} = b_{alt} - k_{alt} \cdot a_{alt}$

$b_{new} = a_{alt}$

hoch:

$\beta_{new} = \alpha_{alt}$

$\alpha_{new} = \beta_{alt} - K_{new} \cdot \alpha_{alt}$

α init = 0
β init = 1 immer!

$ggT(1491, 935) = 716 \cdot 935 + (-449) \cdot 1491 = 1$

Grundlagen - Modulare Arithmetik

Sei $n \in \mathbb{N}$

- $\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$
- $a \bmod n := a - \left\lfloor \frac{a}{n} \right\rfloor \cdot n \in \mathbb{Z}_n$
- Man schreibt $a \equiv_n b$ falls $a \bmod n = b \bmod n$
- $\equiv_n$ ist Äquivalenzrelation auf $\mathbb{Z}$
  - Äquivalenzklasse von $a \in \mathbb{Z}$ ist $[a]_n = \{a + nz \mid z \in \mathbb{Z}\} =: a + n\mathbb{Z}$
- $\equiv_n$ ist mit $+$ und $\cdot$ verträglich (Kongruenz)
  - Falls $a \equiv_n a'$ und $b \equiv_n b'$, dann $a + b \equiv_n a' + b'$ und $a \cdot b \equiv_n a' \cdot b'$

Beispiele und Probleme

- $(231 + 435) \bmod 4 = ((231 \bmod 4) + (435 \bmod 4)) \bmod 4 = (3 + 3) \bmod 4 = 2$
- $(231 \cdot 435) \bmod 4 = ((231 \bmod 4) \cdot (435 \bmod 4)) \bmod 4 = (3 \cdot 3) \bmod 4 = 1$
- $5^6 \bmod 4 = (5 \bmod 4)^6 \bmod 4 = 1^6 \bmod 4 = 1$

Aber Vorsicht!

- $4^6 \bmod 5 = 16^3 \bmod 5 = (16 \bmod 5)^3 \bmod 5 = 1 \neq 4^{6 \bmod 5} \bmod 5 = 4$
- Aus $3 \cdot 7 \equiv_9 3 \cdot 1$ folgt nicht $7 \equiv_9 1$

Gruppen Definition

(multiplikativ) $\mathbb{G} \hat{=} \langle \mathbb{G}, \bullet, 1 \rangle$ (additiv/abelsch) $\mathbb{G} \hat{=} \langle \mathbb{G}, +, 0 \rangle$

ist eine Gruppe, falls

0		$\bullet : \mathbb{G} \times \mathbb{G} \to \mathbb{G}$	$+ : \mathbb{G} \times \mathbb{G} \to \mathbb{G}$	(abgeschlossen)
1	$\forall a, b, c:$	$(a \bullet b) \bullet c = a \bullet (b \bullet c)$	$(a + b) + c = a + (b + c)$	(assoziativ)
2	$\forall a:$	$a \bullet 1 = 1 \bullet a = a$	$a + 0 = 0 + a = a$	(Neutrales)
3	$\forall a \exists b:$	$a \bullet b = b \bullet a = 1$	$a + b = b + a = 0$	(Inverses)

$\mathbb{G}$ ist kommutativ, falls noch

4	$\forall a, b:$	$a \bullet b = b \bullet a$	$a + b = b + a$	(kommutativ)

$\mathbb{G}$ ist endlich, falls $|\mathbb{G}| < \infty$. Ordnung der Gruppe

Gruppen Eigenschaften

Sei $\mathbb{G} \hat{=} \langle \mathbb{G}, \cdot, 1 \rangle$ eine Gruppe. Dann gilt immer (ab für $a \cdot b$):

- Das Neutrale ist eindeutig
- Das Inverse ist eindeutig
  - Notation: Für das eindeutige Inverse von a schreibt man in multiplikativen Gruppen a^{-1}; in additiven Gruppen entsprechend $-a$
- $(a^{-1})^{-1} = a$ und $(ab)^{-1} = b^{-1}a^{-1}$
  (bzw. $-(-a) = a$ und $-(a + b) = (-b) + (-a)$)
- Kürzungsregel: Falls $ab = ac$, dann $b = c$, bzw. falls $ba = ca$, dann auch $b = c$
  - $a^{-1}b$ ist die eindeutige Lösung von $ax = b$;
    ba^{-1} die eindeutige Lösung von $xa = b$
  - Für jedes $a \in \mathbb{G}$ sind $l_a(x) := ax$ und $r_a(x) := xa$ Permutationen von $\mathbb{G}$

wichtige Gruppen

$\langle \mathbb{Z}_n, +_n, 0 \rangle$ additive Gruppe modulo $n \in \mathbb{N}$

- Grundmenge: $\mathbb{Z}_n = \{0, 1, \ldots n-1\}$ (Reste modulo $n \in \mathbb{N}$)
- Gruppenoperation: $a +_n b := (a + b) \bmod n$
- Neutrales: 0
- Inverse: 0 für 0, sonst $n - a$ für $a \in \mathbb{Z}_n \setminus \{0\}$

$\varphi(400) = 2^{4-1} \cdot (2-1) \cdot 5^{2-1} \cdot (5-1) = 8 \cdot 20 = 160.$
$2^4 \cdot 5^2$

$\langle \mathbb{Z}_n^*, \cdot_n, 1 \rangle$ multiplikative Gruppe modulo $n \geq 2$

- Grundmenge: $\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n \mid \mathrm{ggT}(x, n) = 1\}$; $|\mathbb{Z}_n^*| =: \varphi(n) = n \prod_{p \in \mathbb{P}: p|n} \left(1 - \frac{1}{p}\right)$
  (alle zu n teilerfremde Reste modulo n)
- Gruppenoperation: $a \cdot_n b := (a \cdot b) \bmod n$
- Neutrales: 1
- Inverse: α mod n invers zu a (α ist Teil des Ergebnis von EEA(a, n))

$|\mathbb{Z}_n^*| = \varphi(n) = n \cdot \prod_{p \in P_n} (1 - p^{-1})$

Faktorisierung von n: $1491 = 3 \cdot 7 \cdot 71$

$\Rightarrow \varphi(n) = 1491 \cdot \left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{7}\right)\left(1 - \frac{1}{71}\right)$
$= 840$

$x = a^k \cdot b \quad \varphi(x) = x \cdot (1 - \frac{1}{a}) \cdot (1 - \frac{1}{b})$
obwohl a kommt beliebig k mal vor

$\langle S_A, \circ, \mathrm{Id}_a \rangle$ symmetrische Gruppe über A

- Grundmenge: $S_A = \{f : A \to A \mid f \text{ bijektiv}\}$
  (Menge aller Permutationen einer Menge A)
- Gruppenoperation: $f \circ g : A \to A : a \mapsto f(g(a))$ (Funktionskomposition)
- Neutrales: Identität $\mathrm{Id}_A : A \to A : a \mapsto a$
- Inverse: Umkehrabbildung

Während die additiven bzw. multiplikativen Gruppen modulo n immer kommutativ sind, sind die symmetrischen Gruppen im Allgemeinen nicht kommutativ

- **Beispiel**: $\langle S_3, \circ, \mathrm{Id} \rangle$ das neutrale Element

	$\mathrm{Id}_{[3]}$	$(1,2)$	$(1,3)$	$(2,3)$	$(1,2,3)$	$(1,3,2)$
$\mathrm{Id}_{[3]}$	$\mathrm{Id}_{[3]}$	$(1,2)$	$(1,3)$	$(2,3)$	$(1,2,3)$	$(1,3,2)$
$(1,2)$	$(1,2)$	$\mathrm{Id}_{[3]}$	$(1,3,2)$	$(1,2,3)$	$(2,3)$	$(1,3)$
$(1,3)$	$(1,3)$	$(1,2,3)$	$\mathrm{Id}_{[3]}$	$(1,3,2)$	$(1,2)$	$(2,3)$
$(2,3)$	$(2,3)$	$(1,3,2)$	$(1,2,3)$	$\mathrm{Id}_{[3]}$	$(1,3)$	$(1,2)$
$(1,2,3)$	$(1,2,3)$	$(1,3)$	$(2,3)$	$(1,2)$	$(1,3,2)$	$\mathrm{Id}_{[3]}$
$(1,3,2)$	$(1,3,2)$	$(2,3)$	$(1,2)$	$(1,3)$	$\mathrm{Id}_{[3]}$	$(1,2,3)$

$(1,2,3) \circ (2,4,6,5,3)$
meine 的可以省略
$\equiv (1,2,3)(4)(5)(6) \circ (1)(2,4,6,5,3)$

1	→ 1	→ 2
2	→ 4	→ 4
4	→ 6	→ 6
6	→ 5	→ 5
5	→ 3	→ 1
3	→ 2	→ 3

$\equiv (1,2,4,6,5)(3)$

für jede Funktion (Relation): $R^\circ = \mathrm{Id}$

$(1,2) \circ (2,3) = (3,1,2) = (1,2,3)$
die Elemente in einem Zyklus können zyklisch rotiert werden

$(2,3) \circ (1,2) = (1,3,2)$

$\Rightarrow \mathrm{ord}((1,2,3)) = 3$

$(1,2,3) \circ (1,2,3) \circ (1,2,3) = (1,3,2) \circ (1,2,3) = (1)(2)(3) = \mathrm{Id}$

Ordnung eines Elements

Definition: Für $\mathbb{G} \hat{=} \langle \mathbb{G}, \bullet, 1 \rangle$ eine Gruppe, $a \in \mathbb{G}$ und $k \in \mathbb{N}_0$:

$$a^0 := 1 \qquad a^{k+1} := a \bullet (a^k) \qquad a^{-(k+1)} := (a^{-1}) \bullet (a^{-k})$$

Setze dann $\langle a \rangle := \{a^k \mid k \in \mathbb{Z}\} = \{\ldots, (a^{-1})^3, (a^{-1})^2, a^{-1}, 1, a, a^2, a^3, \ldots\}$ (Erzeugnis von a)

und $\text{ord}(a) := \min\{k \in \mathbb{N} \mid a^k = 1\}$ (mit $\min \emptyset := \infty$).

- $\text{ord}(a)$ heißt Ordnung von a und ist die kleinste positive Zahl mit $a^k = 1$.
- a wird ein Erzeuger von $\mathbb{G}$ genannt, falls $\langle a \rangle = \mathbb{G}$.

- a ist ein Erzeuger von G gdw $a^{|G|/p} \neq 1$ für jeden Primfaktor p von $|G|$

Sei $\mathbb{G} \hat{=} \langle \mathbb{G}, \cdot, 1 \rangle$ eine Gruppe und $a \in \mathbb{G}$ mit $\text{ord}(a) < \infty$. Dann gilt

- $a^k = a^{k \bmod \text{ord}(a)} = 1$ gdw. $k \bmod \text{ord}(a) = 0$ gdw. $\text{ord}(a) | k$

Sonderfall Permutationen: ist $\pi \in S_n$ eine Permutation, dann ist die Ordnung von π das kleinste gemeinsame Vielfache der Längen der Zykel in π

Eigenschaften:
- $|S_n| = n!$
- Die Ordnung einer Permutation ist das kgV seiner Zykellänge
- Der Gruppenexponent ist das kgV aller möglichen Zykellängen.

- $a^{-1} = a^{\text{ord}(a)-1}$
- $a^k = a^{k \bmod \text{ord}(a)}$ für jedes $k \in \mathbb{Z}$
- $\langle a \rangle = \{1, a, a^2, \ldots, a^{\text{ord}(a)-1}\}$
- $|\langle a \rangle| = \text{ord}(a)$

Gruppenexponent

Sei $\mathbb{G} \hat{=} \langle \mathbb{G}, \cdot, 1 \rangle$ eine endliche Gruppe. Dann gilt

- für jedes $a \in \mathbb{G}$: $|\mathbb{G}| \bmod \text{ord}(a) = 0$, also $a^{|\mathbb{G}|} = 1$ (Ordnung jedes Elements teilt die Gruppengröße)
- $\lambda_{\mathbb{G}} := \text{kgV}(\{\text{ord}(a) \mid a \in \mathbb{G}\})$ teilt $|\mathbb{G}|$ ohne Rest (Gruppenexponent)
- $\lambda_{\mathbb{G}} = \min\{\lambda \in \mathbb{N} \mid \forall a \in \mathbb{G} : a^\lambda = 1\}$

$a^{\text{ord}(a)} = 1$
$a^{|G|} = 1 \quad \forall a \in G$
$a^{\lambda_G} = 1 \quad \forall a \in G$

Somit gilt für jedes $a \in \mathbb{G}$ und jedes $k \in \mathbb{Z}$: $a^k = a^{k \bmod \text{ord}(a)} = a^{k \bmod \lambda_{\mathbb{G}}} = a^{k \bmod |\mathbb{G}|}$

nicht zyklische Gruppe ⇒ kein Erzeuger

zyklische Gruppen

Gruppe hat mindestens einen Erzeuger

Eine Gruppe $\langle \mathbb{G}, \cdot, 1 \rangle$ heißt zyklisch, falls es ein $a \in \mathbb{G}$ gibt mit $\langle a \rangle = \mathbb{G}$; a heißt dann Erzeuger/Generator von $\mathbb{G}$

- Jede zyklische Gruppe ist kommutativ
- $\langle \mathbb{Z}_n, +_n, 0 \rangle$ ist zyklisch; Erzeuger $\mathbb{Z}_n^*$
- $\langle S_A, \circ, \text{Id}_a \rangle$ ist nicht zyklisch im Allgemeinen, da nicht kommutativ für $n \geq 3$
- $\langle \mathbb{Z}_n^*, \cdot_n, 1 \rangle$ zyklisch gdw. $n \in \{2, 4, p^r, 2p^r \mid p \in \mathbb{P}, r \in \mathbb{N}\}$

Sei $\langle \mathbb{G}, \cdot, 1 \rangle$ zyklisch und endlich mit $N := |\mathbb{G}|$. Dann gilt für $a \in \mathbb{G}$:

$$\langle a \rangle = \mathbb{G} \text{ gdw. } \forall p \in \{p \in P : p | N\} : a^{N/p} \neq 1$$

(Gibt uns einen Test, ob ein Element $a \in \mathbb{G}$ Erzeuger ist)

(a) Bestimmen Sie die Ordnung von 3 in $\langle \mathbb{Z}_{20}^*, \cdot_{20}, 1 \rangle$.

a) ord(3) in $\langle \mathbb{Z}_{20}^*, \cdot_{20}, 1 \rangle$ = ?
ord(3) muss Teiler von $|\mathbb{Z}_{20}^*|$ sein
$|\mathbb{Z}_{20}^*| = \varphi(20) = \varphi(4) \cdot \varphi(5) = 2 \cdot 4 = 8$
$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$ für $\text{ggT}(m,n) = 1$
⇒ damit kann 3 nur die Ordnungen 2, 4 oder 8 haben
(1 ist das einzige Element mit Ordnung 1)
- $\mathbb{Z}_{20}^*$ ist nicht zyklisch (nach VL)
bleiben nur noch 2 oder 4
$3^2 \equiv_{20} 9 \neq 1$ also ord(3) = 4

$3^1 \equiv_{20} 3$
$3^2 \equiv_{20} 9$
$3^3 \equiv_{20} 7$
$3^4 \equiv_{20} 81 \equiv_{20} 1$
⇒ ord(3) = 4

(b) Bestimmen Sie die Ordnung von 3 in $\langle \mathbb{Z}_{34}^*, \cdot_{34}, 1 \rangle$.

b) $\varphi(34) = \varphi(2)\varphi(17) = 16$ → 2 Primzahlen ⇒ zyklisch
3 kann nur die Ordnungen 2, 4, 8, 16 haben.
$3^2 \equiv_{34} 9$
$3^4 \equiv_{34} 81 \equiv_{34} 13$
$3^8 \equiv_{34} 33$
$3^{16} \equiv_{34} 1$ weil $a^{|G|} = 1$
⇒ ord(3) = 16 ⇒ 3 ist ein Erzeuger von $\mathbb{Z}_{34}^*$

(a) Entscheiden Sie, ob 3 ein Erzeuger der $\langle \mathbb{Z}_{89}^*, \cdot_{89}, 1 \rangle$ ist.

a) $|\mathbb{Z}_{89}^*| = \varphi(89) = 88 = 2^3 \cdot 11$
Erinnerung: a ist ein Erzeuger von G gdw $a^{|G|/p} \neq 1$ für jeden Primfaktor p von $|G|$

$3^{88/11} = 3^8 = (3^4)^2 = 81^2 \equiv_{89} (-8)^2 = 64 \neq 1$
$3^{88/2} = 3^{44} = (3^4)^{11} = 81^{11} \equiv_{89} (-8)^{11} = (-2)^{33} = -(2^{11})^3 \cdot 2^3 = -(1024)^3 \cdot 8 \equiv_{89} -(45)^3 \cdot 8$
$\equiv_{89} -3^6 \cdot 5^3 \cdot 2^3 \equiv_{89} -81 \cdot 3 \cdot 125 \cdot 8 \equiv_{89} 8 \cdot 3 \cdot 36 \cdot 8 \equiv_{89} -1 \neq 1$
Also ist 3 ein Erzeuger der Gruppe $\langle \mathbb{Z}_{89}^*, \cdot_{89}, 1 \rangle$

(b) Entscheiden Sie, ob 5 ein Erzeuger der $\langle \mathbb{Z}_{89}^*, \cdot_{89}, 1 \rangle$ ist.

b) $5^{88/2} = 5^{44} = (5^4)^{11} = (125 \cdot 5)^{11} \equiv_{89} (36 \cdot 5)^{11} \equiv_{89} 2^{11} = 2048 \equiv_{89} 1$
⇒ 5 ist kein Erzeuger der $\langle \mathbb{Z}_{89}^*, \cdot_{89}, 1 \rangle$

$\mathbb{Z}_n^* = \{1, 3, 5, 7, 9, 11, 13, 15\}$ n = 16
Gruppenoperation von $\langle \mathbb{Z}_n^*, \cdot_n, 1 \rangle$

$\langle 1 \rangle = \{1\}$ ⇒ ord(1) = 1
$\langle 3 \rangle = \{3, 9, 11, 1\}$ ⇒ ord(3) = 4
$\langle 5 \rangle = \{5, 9, 13, 1\}$ ⇒ ord(5) = 4
$\langle 7 \rangle = \{7, 1\}$ ⇒ ord(7) = 2
$\langle 9 \rangle = \{9, 1\}$ ⇒ ord(9) = 2
$\langle 11 \rangle = \{11, 9, 3, 1\}$ ⇒ ord(11) = 4
$\langle 13 \rangle = \{13, 9, 5, 1\}$ ⇒ ord(13) = 4
$\langle 15 \rangle = \{15, 1\}$ ⇒ ord(15) = 2
⇒ Gruppenexponent: $\lambda = \text{KgV}\{1, 4, 2\} = 4$

(d) Bestimmen Sie den Gruppenexponent $\lambda_{\mathbb{Z}_{20}^*} = \min\{\lambda \in \mathbb{N} : \forall x \in \mathbb{Z}_{20}^* : x^\lambda = 1\}$ von $\langle \mathbb{Z}_{20}^*, \cdot_{20}, 1 \rangle$.
(e) Bestimmen Sie den Gruppenexponent $\lambda_{\mathbb{Z}_{34}^*} = \min\{\lambda \in \mathbb{N} : \forall x \in \mathbb{Z}_{34}^* : x^\lambda = 1\}$ von $\langle \mathbb{Z}_{34}^*, \cdot_{34}, 1 \rangle$.
(f) Bestimmen Sie den Gruppenexponent $\lambda_{S_5} = \min\{k \in \mathbb{N} : \forall x \in S_5^* : x^\lambda = \text{Id}_{[5]}\}$ von $\langle S_5, \circ, \text{Id}_{[5]} \rangle$

d) Gruppenexponent = KgV alle Elementordnungen
nach a) sind die mögliche Elementordnungen 1, 2, 4 (28 : mod(3) = 4)
⇒ Gruppenexponent = $\text{KgV}\{1, 2, 4\} = 4$

e) $\langle \mathbb{Z}_{34}^*, \cdot_{34}, 1 \rangle$ ist zyklisch, da $34 = 2 \cdot 17$
⇒ Gruppenexponent = Gruppenordnung = 16

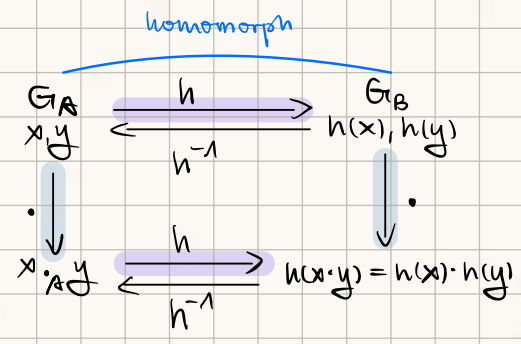
f) Die Ordnung einer Permutation ist das KgV seiner Zykellängen. Damit ist der Gruppenexponent das KgV alle möglichen Zykellängen,
⇒ $\text{KgV}(\{1, 2, 3, 4, 5\}) = 60$

wie viel Elemente der Ordnung G gibt es? (zyklische Gruppe)

⇒ Anzahl der Erzeuger = $\varphi(\varphi(n)) = \varphi(G)$

- **Definition**: Seien $\langle \mathbb{G}_A, \bullet_A, 1_A \rangle$ und $\langle \mathbb{G}_B, \bullet_B, 1_B \rangle$ Gruppen.

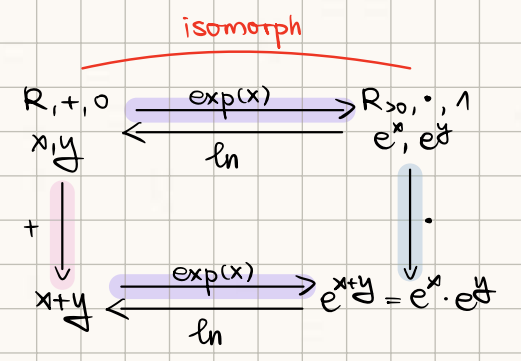
$h\colon \mathbb{G}_A \to \mathbb{G}_B$ heißt Homomorphismus, falls für alle $a, b \in \mathbb{G}_A$ $h(a \bullet_A b) = h(a) \bullet_B h(b)$



Beispiele: Homomorphien („von ähnlicher Gestalt“)

- $h\colon \langle \mathbb{Z}, +, 0 \rangle \to \langle \mathbb{Z}/n\mathbb{Z}, +, [0]_n \rangle\colon z \mapsto [z]_n$
- $h\colon \langle \mathbb{R}, +, 0 \rangle \to \langle \{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}, \oplus, (0,1) \rangle\colon x \mapsto (\sin x, \cos x)$

Isomorphismus $\mathbb{G}_A \cong \mathbb{G}_B$ isomorph = Homomorphismus + bijektiv



Beispiele: Isomorphien („von gleicher Gestalt“)

- $\langle \mathbb{Z}/n\mathbb{Z}, +, [0]_n \rangle \cong \langle \mathbb{Z}_n, +_n, 0 \rangle$ und
  $\langle (\mathbb{Z}/n\mathbb{Z})^*, \bullet, [1]_n \rangle \cong \langle \mathbb{Z}_n^*, \bullet_n, 1 \rangle$
  mittels $h([k]_n) = k \bmod n$ und $h^{-1}(k) = [k]_n$.
- $\langle \mathbb{R}, +, 0 \rangle \cong \langle \mathbb{R}_{>0}, \bullet, 1 \rangle$ mittels $h(x) = e^x$ und $h^{-1}(x) = \log x$.

- **Lemma**: Ist $h\colon \mathbb{G}_A \to \mathbb{G}_B$ ein Homomorphismus von Gruppen, dann gilt:
  1. $h(1_A) = 1_B$ da: $1_B \bullet_B h(1_A) = h(1_A) = h(1_A \bullet_A 1_A) = h(1_A) \bullet_B h(1_A)$.
  2. $h(a^{-1}) = h(a)^{-1}$ da: $h(a) \bullet_B h(a)^{-1} = 1_b = h(a \bullet_A a^{-1}) = h(a) \bullet_B h(a^{-1})$.
  3. $h(\langle a \rangle) = \langle h(a) \rangle$ da: $h(\langle a \rangle) = \{h(a^k) \mid k \in \mathbb{Z}\} = \{h(a)^k \mid k \in \mathbb{Z}\} = \langle h(a) \rangle$.
  4. $\operatorname{ord}(a) \geq \operatorname{ord}(h(a))$ (falls h Isomorphismus, dann $\operatorname{ord}(a) = \operatorname{ord}(h(a))$.
     da: $\operatorname{ord}(a) = |\langle a \rangle| \geq |h(\langle a \rangle)| = |\langle h(a) \rangle| = \operatorname{ord}(h(a))$.
  5. $h(\mathbb{G}_A) \leq \mathbb{G}_B$ da: $h(x) \bullet_B h(y)^{-1} = h(x \bullet_A y^{-1}) \in h(\mathbb{G}_A)$.
  6. $h^{-1}(1_B) \leq \mathbb{G}_A$ da: $h(x \bullet_A y^{-1}) = h(x) \bullet_B h(y)^{-1} = 1_B \bullet 1_B = 1_B$.
  7. Ist h Isomorphismus, dann auch die Umkehrabbildung h^{-1}
     da: $h^{-1}(h(x) \bullet_B h(y)) = h^{-1}(h(x \bullet_A y)) = x \bullet_A y = h^{-1}(h(x)) \bullet_A h^{-1}(h(y))$.
  8. Ist h Isomorphismus, dann $\langle a \rangle = \mathbb{G}_A$ gdw. $\langle h(a) \rangle = \mathbb{G}_B$ da: 4 .

Beispielaufgabe

Die Erzeugnistafeln beider Gruppen sind:

$\mathbb{Z}_6$:

a	$\langle a \rangle$	ord(a)
0	{0}	1
1	{1, 2, 3, 4, 5, 0}	6
2	{2, 4, 0}	3
3	{3, 0}	2
4	{4, 2, 0}	3
5	{5, 4, 3, 2, 1, 0}	6

$\mathbb{Z}_9^*$:

a	$\langle a \rangle$	ord(a)
1	{1}	1
2	{2, 4, 8, 7, 5, 1}	6
4	{4, 7, 1}	3
5	{5, 7, 8, 4, 2, 1}	6
7	{7, 4, 1}	3
8	{8, 1}	2

Dies ergibt, analog zum Beispiel auf Folie 1128, folgende Isomorphismen $h_1, h_2 : \mathbb{Z}_6 \to \mathbb{Z}_9^*$:

$$h_1(0) = 1, h_1(1) = 2, h_1(2) = 4, h_1(3) = 8, h_1(4) = 7, h_1(5) = 5.$$

und

$$h_2(0) = 1, h_2(1) = 5, h_2(2) = 7, h_2(3) = 8, h_2(4) = 4, h_2(5) = 2.$$

Wichtige Aussagen zur Isomoprhie von Gruppen

1. Jede zyklische Gruppe $(G, \circ)$ mit $|G| = \infty$ ist isomorph zu $(\mathbb{Z}, +)$.
2. Jede zyklische Gruppe $(G, \circ)$ mit $|G| = n$ ist isomorph zu $(\mathbb{Z}_n, +_n)$.
3. Zwei zyklische Gruppen mit gleich vielen Elementen sind isomorph zueinander.
4. Alle zyklischen Gruppen sind automatisch auch kommutativ, da $(\mathbb{Z}, +)$ und $(\mathbb{Z}_n, +_n)$ beide abelsch (kommutativ) sind.
5. Sind $(G, \circ)$ und $(H, \bullet)$ zwei isomorphe Gruppen und $h : G \to H$ ein Isomorphismus, dann gilt:

$$\begin{array}{lcl} h(a) = b & \Longrightarrow & \operatorname{ord}(a) = \operatorname{ord}(b), \\ h(a) = b & \Longrightarrow & h(a^{-1}) = b^{-1}, \\ (G, \circ) \text{ abelsch} & \Longrightarrow & (H, \bullet) \text{ abelsch, (kommutativ)} \\ (G, \circ) \text{ zyklisch} & \Longrightarrow & (H, \bullet) \text{ zyklisch.} \end{array}$$

- Aus der Sicht der Gruppentheorie sind isomorphe Gruppen äquivalent – kennt man einen Isomorphismus $h\colon \mathbb{G}_1 \to \mathbb{G}_2$, so kann man sich prinzipiell aussuchen, in welcher der beiden Gruppen man rechnen möchte:

$$a \bullet_1 b = h^{-1}(h(a)) \bullet_1 h^{-1}(h(b)) = h^{-1}(h(a) \bullet_2 h(b))$$

- Beispiele:
  - $[5 \bullet_{13} 12]_{13} = [5]_{13} \bullet [12]_{13} = [8]_{13}$
    also $5 \bullet_{13} 12 = 8$
    oder kürzer: $5 \bullet 12 \equiv_{13} 5 \bullet (-1) \equiv_{13} -5 \equiv_{13} 8$
  - $[\underbrace{995 \bullet_{997} \ldots \bullet_{997} 995}_{1000 \text{ Faktoren}}]_{997} = [995]_{997}^{1000} = [-2]_{997}^4 = [16]_{997}$
    also $995^{1000} \bmod 997 = 16$
    oder kürzer: $995^{1000} \equiv_{997} (-2)^4 \equiv_{997} 16$

- reflexiv: jede Knoten hat Schleifen
- irreflexiv: gar keine Schleifen
- nicht reflexiv: gibts mindestens eine Schleife, aber nicht alle

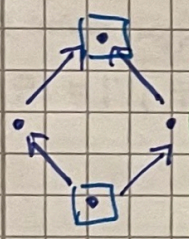
- symmetrisch: entweder Doppelkante oder gar keine Kante (beliebige Schleifen)
- asymmetrisch: weder Doppelkante noch Schleifen
- antisymmetrisch: höchstens eine Kante (Doppelkante nein, Schleifen ja)

transivität: entweder Transivität ~~für~~ zwischen alle Knoten oder für gar keine Kanten
- ✓ wenn mit genau 2 Schritten, dann auch mit genau 1 Schritt
- ✓ wenn mit genau 2 Schritten → geht nicht ⇒ dann auch transitiv

Äquivalenzklasse: reflexiv, symmetrisch, transitiv
Ordnungsrelation (partielle Ordnung): reflexiv, antisymmetrisch, transitiv
Hasse-Diagramm: ohne Schleifen, ohne Transivität

$\bigcap_{k \in \mathbb{N}_0} A_k$ "immer a" da "∩" für "alle"

$\bigcup_{k \in \mathbb{N}_0} A_k$ "irgendwo a" da "∪" für "es gibt mindestens"

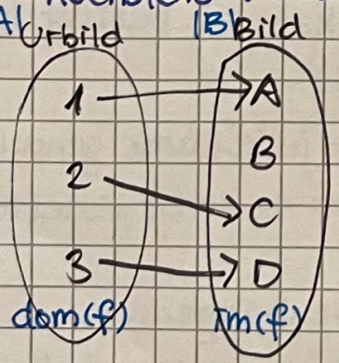


maximales Element (keine Kanten zu einem anderen Element)
größtes Element // + aber vom jeden anderen Element 1 Kante
Umdrehung von R zu R^{-1}
minimales Element (keine Kante von einem anderen Element)
kleinstes Element // + aber 1 Kante zu jedem anderen Element)

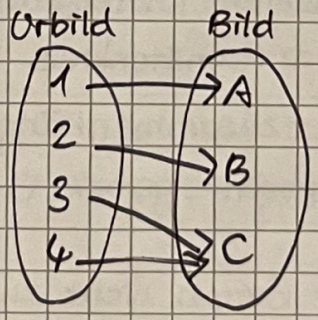
Satz von Cantor

$f: A \xrightarrow{inj} B$
$g: B \xrightarrow{inj} A$
$\hookrightarrow h: A \xrightarrow{\text{bijektiv}} B$

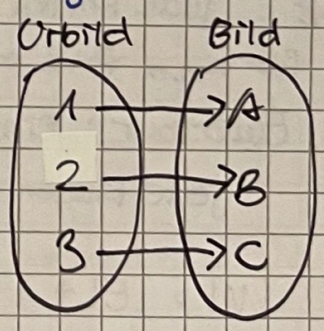
injektiv $|A| \leq |B|$
höchstens 1 Urbild



surjektiv
mindestens 1 Urbild



bijektiv $|A| = |B|$
genau 1 Urbild



$R^0 = Id$ (alle Schleifen)
$R^+ = \bigcup_{k \in \mathbb{N}} R^k$ transitive Hülle (alle Pfade, mindestens 1 Schritt machen)
$R^* = R_0 \cup R^+$ reflexiv-transitive Hülle (bis vollständig transitiv)

Eulersche Polyederformel (EPF-Formel)
zsmhg + planar ⇒ $|f| - |E| + |V| = 2$
k Zshgkomponente + planar ⇒ $|f| - |E| + |V| = 1 + k$

für planare Graph
- $f - |E| + |V| \geq 2$
- $|E| \leq 3|V| - 6$ $(|V| \geq 3)$
- mindestens 1 Knote $\deg(u) \leq 5$

5 Knoten

K_5 $(4,4,4,4,4)$ jede Knoten besitzt 4 Kanten

$K_{3,3}$ $(3,3,3,3,3,3)$ jede der 6 Knoten besitzt 3 Knoten

Satz von Kuratowski: einfache Graph ist planar, wenn weder K_5 noch $K_{3,3}$ ein Mirror von G ist

Vier-Farben-Satz: für jede einfache planare Graphen gilt $\chi(G) \leq 4$ (4-färbbar)

maximal 4 Farbe (oberschranke)

$\chi(G) \leq \max \deg(u) + 1$

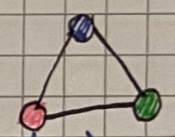
$\chi(G) \leq \frac{1}{2} + \sqrt{2|E| + \frac{1}{4}}$

jede Graph mit $(1,1,2,2,4,4)$ ist zusammenhängend

Sei v der Knoten von Grad 4. Die 4 Nachbarn von v sind mit v direkt verbunden. Der noch übrig bleibende Knoten hat die Knotengrad ≥ 1 und ist deshalb mit einem Nachbarn von v auch direkt verbunden. somit ist Graph zusammenhängend

kreisfrei $\Rightarrow |V| \geq |E| + 1$

$|E| \geq |V|$ $(|V| \geq 3)$ $\Rightarrow$ enthält einen Kreis (nicht kreisfrei)

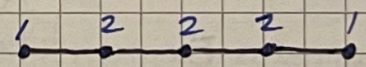


bipartit: einfache Graph enthält keinen Kreis ungerade Länge

einfach Graph: symmetrisch (ungerichtete Kanten) + irreflexiv (gar keine Kanten)

Baum = einfache Graph + zusammenhängend + kreisfrei + $|V| = |E| + 1$

jede Pfadgraph ist ein Baum



jede Baum hat mindestens 2 Blätter $(1,1,2,2,2)$

$\deg(u) = 1$

Hamiltonkreis: einfach + zusammenhängend (jede Knoten genau 1 mal besucht)

jede Knoten mindestens Knotengrad $\frac{|V|}{2}$ hat $\Rightarrow$ besitzt Hamiltonkreis

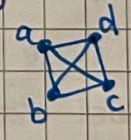
für $K_{m,n}$ falls $m=n$ $\Rightarrow$ Hamiltonkreis $(|V| > 3)$

Eulertour: einfach + zusammenhängend + jede Kante genau 1 mal besucht

jede Knoten hat positive gerade Grad $\Rightarrow$ besitzt Eulertour

$|V| > |E| + 1$ $\Rightarrow$ Graph nicht zusammenhängend

$|V| \leq |E| + 1$ $\not\Rightarrow$ Graph zusammenhängend



$|V| = 5$
$|E| = 6$
$|V| \leq |E| + 1$
aber nicht zsmhg.

perfektes Matching $G = (V_1, V_2, E)$ $|V| = |V_1| + |V_2|$

bipartit + k-regulär $\Rightarrow$ perfektes Matching $\Rightarrow$ { $|V|$ ist gerade; $|V_1| = |V_2|$; Matching-Anzahl $= \frac{|V|}{2}$

(alle Knoten haben Knotengrad k)

Graph-Automorphismus (Isomorphismus von G nach G)

wann darf man ankreuzen

1) haben den gleichen Knotengrad
2) haben die gleichen Nachbarn

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

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

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

$A \setminus (B \cup C) = (A \setminus B) \cup (A \setminus C)$

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

$F \wedge (F \vee G) = F \vee (F \wedge G) = F$

$F \leftrightarrow G = (F \rightarrow G) \wedge (G \rightarrow F) = \neg(F \oplus G)$

$F \oplus G = (F \vee G) \wedge (\neg F \vee \neg G)$

$= ((F \vee G) \wedge \neg F) \vee ((F \vee G) \wedge \neg G)$

$= (\underbrace{F \wedge \neg F}_{\text{false}}) \vee (G \wedge \neg F) \vee (F \wedge \neg G) \vee (\underbrace{G \wedge \neg G}_{\text{false}})$

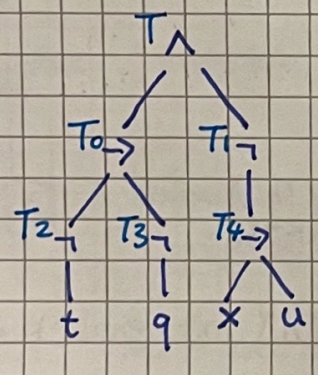
$= (\neg F \wedge G) \vee (F \wedge \neg G)$

DPLL

1) OLR $\{r\}$ $r := \text{true}$
2) PLR $\{\neg p, s\}, \{\neg p, t\}$ $p := \text{false}$
3) Fallunterscheidung
   - $p := \text{true}$
   - $p := \text{false}$

Erfüllbarkeitsäquivalenz

$H = ((\neg t \rightarrow \neg q) \wedge \neg(x \rightarrow u))$



T

$\wedge (T \leftrightarrow (T_0 \wedge T_1))$

$\wedge (T_0 \leftrightarrow (T_2 \rightarrow T_3))$

$\wedge (T_2 \leftrightarrow \neg t)$

$\wedge (T_3 \leftrightarrow \neg q)$

$\wedge (T_1 \leftrightarrow \neg T_4)$

$\wedge (T_4 \leftrightarrow (x \rightarrow u))$

$(A \leftrightarrow (B \wedge C)) = (A \vee \neg B \vee \neg C) \wedge (\neg A \vee B) \wedge (\neg A \vee C)$

$(A \leftrightarrow (B \vee C)) = (\neg A \vee B \vee C) \wedge (A \vee \neg B) \wedge (A \vee \neg C)$

$(A \leftrightarrow \neg B) = (A \vee B) \wedge (\neg A \vee \neg B)$

$(A \leftrightarrow (B \leftrightarrow C)) = (\neg A \vee \neg B \vee \neg C) \wedge (\neg A \vee B \vee \neg C) \wedge (A \vee B \vee C) \wedge (A \vee \neg B \vee \neg C)$

$(A \leftrightarrow (B \oplus C)) = (\neg A \vee B \vee C) \wedge (\neg A \vee \neg B \vee \neg C) \wedge (A \vee \neg B \vee C) \wedge (A \vee B \vee \neg C)$

$(A \leftrightarrow (B \rightarrow C)) = (\neg A \vee \neg B \vee C) \wedge (A \vee B) \wedge (A \vee \neg C)$

zyklische Gruppe hat mindestens einen Erzeuger

falls kein Erzeuger => nicht zyklische Gruppe

wie viel Elemente der Ordnung $|G|$ gibt es? (für zyklische Gruppe)

=> Anzahl der Erzeuger = $\varphi(\varphi(n)) = \varphi(G)$

$\varphi(71) = 71 - 1 = 70$ $22 \nmid 70$ => Ordnung 22 hat 0 Element

$\varphi(29) = 29 - 1 = 28$ alle mögliche Ordnung $\{1, 28, 2, 14, 4, 7\}$

	normale Funktion $[n] \to [k]$	"injektiv"	"surjektiv"	"bijektiv"
n Objekte auf k Gruppen	beliebig viele	höchstens eins	mindestens ein	genau eins
genaue Menge: n u. k unterscheidbar	mit Zü mit Re n^k	ohne Zü mit Re $\frac{k!}{(k-n)!}$	$k! \cdot S_{n,k}$	$n!$
Anzahl der abgeordnete Knoten: n gleich k unterscheidbar	mit Zü ohne Re $\binom{n+k-1}{n}$	ohne Zü ohne Re $\binom{k}{n}$	$\binom{n-1}{k-1}$	1
n unterscheidbar k gleich	$\sum_{i=0}^{k} S_{n,i}$	1	$S_{n,k}$	1
n u. k nicht unterscheidbar	$\sum_{i=0}^{k} P_{n,i} = P_{n+k,k}$	1	$P_{n,k}$	1

Binomial Formel $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$

Vandemondesche Identität $\binom{m+n}{k} = \sum_{i=0}^{k} \binom{m}{i}\binom{n}{k-i}$

Stirling 1. Art Anzahl der Permutation von $[n]$ mit genau k Zyklen

$$\frac{n!}{1^{\lambda_1} \cdots n^{\lambda_n} \cdots \lambda_1! \cdots \lambda_n!}$$

Stirling 2. Art Anzahl der Partitionen von n Elementen in k nicht leere Klassen

Elemente unterscheidbar, Klassen nicht unterscheidbar $\frac{n!}{(1!)^{\lambda_1} \cdots (n!)^{\lambda_n} \cdots \lambda_1! \cdots \lambda_n!}$

Siebformel ungerade + gerade − $A_k = \frac{n}{k} + (1)$ (falls 0 gezählt)

$$|A_3 \cup A_5 \cup A_7| = |A_3| + |A_5| + |A_7| - |A_3 \cap A_5| - |A_5 \cap A_7| - |A_3 \cap A_7| + |A_3 \cap A_5 \cap A_7|$$

DNF alle "1" $(\dots \wedge \dots) \vee (\dots \wedge \dots)$ KV-Diagramm ⇒ DNF-Darstellung

KNF alle "0" $(\dots \vee \dots) \wedge (\dots \vee \dots)$ Klausel ⇒ KNF-Darstellung

erst in DNF-Form und dann in KNF negieren

gültig: nur "1"
erfüllbar: mindestens eine "1"
unerfüllbar: nur "0"

$\{\{S\}\} \to \{\}$ leere Klauselmenge → erfüllbar $(K = \emptyset)$

$\{\{S\}, \{\neg S\}\} \to \{\{\}\}$ Klauselmenge mit leerer Klausel → unerfüllbar $(\{\} \in K)$

$F \models G$ (G folgt aus F) ⇒ $F \to G$ ist gültig

Siebformel (Prinzip von Inklusiv und Exklusiv)

$$|A_3 \cup A_5 \cup A_7| = \underbrace{|A_3| + |A_5| + |A_7|}_{\text{ungerade addieren}} \underbrace{- |A_3 \cap A_5| - |A_3 \cap A_7| - |A_5 \cap A_7|}_{\text{gerade subtrahieren}} + |A_3 \cap A_5 \cap A_7|$$

$$(231 + 435) \bmod 4 = ((231 \bmod 4) + (435 \bmod 4)) \bmod 4$$

$$(231 \cdot 435) \bmod 4 = ((231 \bmod 4) \cdot (435 \bmod 4)) \bmod 4$$

$$5^6 \bmod 4 = (5 \bmod 4)^6 \bmod 4$$

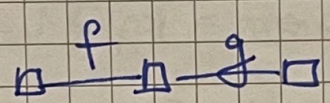
zyklisch $\langle Z_n, +_n, 0 \rangle$ additive Gruppe $a +_n b := (a+b) \bmod n$

2, 4, p^r, $2p^r$ $\langle Z_n^*, \cdot_n, 1 \rangle$ multiplikative Gruppe $a \cdot_n b := (a \cdot b) \bmod n$

$\langle S_A, \circ, Id_A \rangle$ symmetrische Gruppe ~~$f \circ g: A \to A$, $a \mapsto f(g(a))$~~ $g \circ f$

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

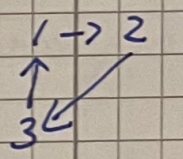
$g \circ f$



$(2,3)$ => 23 32 11

$(1,2)$ => 12 21 33

12 31 23



$(1,2,3)$

~~Ordnung von 3 in $\langle Z_{20}^*, \cdot_{20}, 1 \rangle$~~

$$|Z_n^*| = \varphi(n) = n \cdot \prod_{p \in P} \left(1 - \frac{1}{p}\right)$$

$1491 = 3 \cdot 7 \cdot 71$

$\varphi(1491) = 1491 \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{7}\right) \cdot \left(1 - \frac{1}{71}\right)$

或者 $= (3-1) \cdot (7-1) \cdot (71-1)$

n 本身就是Primzahl $\varphi(83) = 83 - 1 = 82$

$a^{-1} = a^{ord(a)-1}$

$a^k = a^{k \bmod ord(a)}$

$a^{ord(a)} = 1$

$a^{|G|} = 1$

$a^{\lambda_G} = 1$

Bestimmen die Ordnung von 3 in $\langle Z_{20}^*, \cdot_{20}, 1 \rangle$

$|Z_{20}^*| = \varphi(20) = \varphi(4) \cdot \varphi(5) = 2 \cdot (2-1)^{(2-1)} \cdot (5-1) = 8$

3 kann nur die Ordnung 2, 4, 8 haben (wer 1 hat Ordnung 1)

$3^1 \equiv_{20} 3 \neq 1$ $3^2 \equiv_{20} 9 \neq 1$ $3^3 \equiv_{20} 7 \neq 1$ $3^4 \equiv_{20} 81 \equiv_{20} 1$

$ord(3) = 4$

Ordnung einer Permutation $\langle S_5, \circ, Id_{[5]} \rangle$

$\pi(1)=2$, $\pi(2)=4$, $\pi(3)=5$, $\pi(4)=1$, $\pi(5)=3$

$\pi = (1,2,4)(3,5)$ => $ord(\pi) = KgV(3,2) = 6$

Zykellänge 3 2

entscheiden ob 3 ein Erzeuger von $\langle \mathbb{Z}_{89}^*, \cdot_{89}, 1 \rangle$

$|\mathbb{Z}_{89}^*| = \varphi(89) = 89-1 = 88 = 2^3 \cdot 11$

$3^{88/11} = 3^8 = (3^4)^2 = 81^2 \equiv_{89} (-8)^2 = 64 \neq 1$

$3^{88/2} = 3^{44} = (3^4)^{11} = 81^{11} \equiv_{89} (-8)^{11} = (-2)^{3\cdot 11} = ((-2)^{10})^3 \cdot (-2)^3 = -1024^3 \cdot 8$

$\equiv_{89} -(45)^3 \cdot 8 \equiv_{89} -3^6 \cdot 5^3 \cdot 2^3 \equiv_{89} -81 \cdot 9 \cdot 125 \cdot 8 \equiv_{89} 89 \cdot 9 \cdot 36 \cdot 8 \equiv_{89} -1 \neq 1$

3 ist Erzeuger von $\langle \mathbb{Z}_{89}^*, \cdot_{89}, 1 \rangle$

a ist Erzeuger von G gdw $a^{|G|/p} \neq 1$ für jeden Primfaktoren p von $|G|$

$k = \text{ord}(a)$ → Ordnung von a falls $a^k = 1$ (k ist kleinste positive Zahl)

Gruppenexponent

für nicht zyklisch → Gruppenexponent = KgV aller Elementordnungen

$\langle \mathbb{Z}_{20}^*, \cdot_{20}, 1 \rangle$ Elementordnung 1, 2, 4

Gruppenexponent = $\text{kgV}\{1,2,4\} = 4$

für zyklisch → Gruppenexponent = Gruppenordnung

$\langle \mathbb{Z}_{34}^*, \cdot_{34}, 1 \rangle$ $\varphi(34) = \varphi(2) \cdot (17) = (2-1) \cdot (17-1) = 16$

Gruppenexponent = 16

für Permutation → Gruppenexponent = KgV aller möglichen Zykellängen

Gruppenexponent = $\text{kgV}\{1,2,3,4,5\} = 60$

π^{785} für $\pi = (1,2,3)(4,5) \in S_6$ $\text{ord}(\pi) = 6$

$a^k = a^{k \bmod \text{ord}(a)}$

$\pi^{785} = \pi^{785 \bmod 6} = \pi^5 = (1,2,3)^5 (4,5)^5$

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

$= (1,2,3)^2 (4,5)^1$

$= (1,3,2)(4,5)$

Isomorphismus = Homomorphismus + bijektiv

zyklische Gruppe mit gleich viele Elementen (Gruppenordnung) ⇒ isomorph

Alle zyklisch Gruppen sind automatisch kommunikativ

Isomorphismus $h: G_1 \to G_2$

$a \cdot_1 b = h^{-1}(h(a)) \cdot_1 h^{-1}(h(b)) = h^{-1}(h(a) \cdot_2 h(b))$