

Diskrete Strukturen

Daniel

October 2024

Contents

1 Mengen	5
	5
1.0.1 Quantoren	5
1.0.2 Die Kardinalität einer Menge	6
1.1 Mengen durch Aussonderung	7
1.2 Mengenoperationen	7
1.3 Rechenregeln	8
1.4 Mengenkomplement	9
1.4.1 De-Morgansche Regeln	10
1.5 Paare und Produkte	10
1.5.1 Kartesisches Produkt	10
1.5.2 Potenzmengen	11
1.6 Doppeltes Abzählen	11
1.6.1 Beispiel: Handschlaglemma	12
1.7 Binomialkoeffizient	13
1.7.1 Fakultät	13
1.7.2 Das Pascalsche Dreieck	16
2 Abbildungen	17
	18
2.0.1 Eigenschaften von Abbildungen	18
2.0.2 Umkehrabbildung	19
2.0.3 Komposition von Abbildungen	19
2.0.4 Identität von Abbildungen	20
2.1 Größenvergleich von Mengen	20
2.2 Der Satz von Cantor-Schröder-Bernstein	21

2.3	Das Auswahlaxiom	21
2.4	Die Kontinuumshypothese	21
2.5	Permutationen	22
2.5.1	Komposition von Zyklen	23
2.5.2	Stirlingsche Formel	24
3	Boolesche Funktionen und Aussagenlogik	25
3.1	Boolesche Funktionen	25
3.2	Rechengesetze	25
3.3	Aussagenlogik	26
3.3.1	Syntax	26
3.3.2	Ausdrücke	26
3.3.3	Semantik	26
3.3.4	Auswertungsfunktion	27
3.3.5	Belegung eines ausdrucks	27
3.3.6	Darstellungssatz	28
3.3.7	Disjunkte Normalform	29
3.4	Erfüllbarkeitsproblem	29
3.4.1	konjunkte Normalform	30
3.5	Horn-SAT	31
3.5.1	Horn-Ausdrücke	31
3.5.2	Lösungsalgorithmus	31
4	Die natürlichen Zahlen	32
		32
4.0.1	Wohlordnung der natürlichen Zahlen	32
4.0.2	Rechenoperationen	32
4.0.3	Ordnungen	33
4.1	Vollständige Induktion	34
4.2	Teilbarkeit	35
4.3	Primzahlen	36
4.3.1	Fundamentalsatz der Arithmetik	37
4.4	Der euklidische Algorithmus	38
4.4.1	Lemma von Bézout	39
4.4.2	Erweiterter Euklidischer Algorithmus	40
4.4.3	Euklids Lemma	40
4.4.4	Chinesischer Restsatz	42

5	Modulare Arithmetik	42
5.1	Modulorechnung	42
5.2	Homomorphieregel	43
5.2.1	Al Kashi's Trick	43
5.3	Entscheidungsprobleme	44
6	Gruppen	45
6.1	Die multiplikative Gruppe \mathbb{Z}_n	45
6.1.1	Nullteiler	46
6.1.2	Einheiten	46
6.1.3	Die eulersche φ -Funktion	47
6.2	Zyklische Gruppen	47
6.2.1	Permutationsgruppen	47
6.2.2	Abelsche Gruppen	48
6.2.3	Erzeuger	48
6.2.4	Isomorphismen	48
6.3	Der diskrete Logarithmus	50
6.3.1	Beispiel: Diffie-Hellmann-Merkle-Verfahren	50
6.4	Untergruppen	51
6.4.1	Ordnungen	51
6.4.2	Nebenklassen	52
6.4.3	Index von Nebenklassen	53
6.5	Satz von Lagrange	53
6.6	Das RSA-Verfahren	54
7	Graphen	56
		56
7.0.1	Wichtige Beispiele für Graphen	56
7.0.2	Adjazente Knoten	57
7.0.3	isomorphe Graphen	57
7.0.4	Subgraphen	57
7.0.5	Kantenzüge	58
7.1	Zusammenhängende Knoten	58
7.1.1	Die disjunkte Vereinigung	58
7.1.2	Zusammenhangskomponenten	59
7.2	Färbbarkeit	60
7.2.1	Entscheidungsproblem Färbbarkeit	60

7.3	Bäume	61
7.4	Zweifacher Zusammenhang	63
7.5	Blockgraphen	63
7.6	Ohrendekomposition	65
7.7	Satz von Menger	67

1 Mengen

Definition:

Eine **Menge** ist eine Zusammenfassung von bestimmten, wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen, die dann die Elemente der Menge genannt werden.

Symbolik Bedeutung

$e \in M$	Das Element e ist Element der Menge M
$e \notin M$	Das Element e ist kein Element der Menge M
\emptyset oder $\{\}$	Leere Menge
$A \subseteq B$	A ist <i>Teilmenge</i> von B , d.h. jedes Element von A ist auch Element von B
$A \subset B$	A ist <i>echte Teilmenge</i> von B , d.h. jedes Element von A ist auch Element von B , aber $A \neq B$ ($A \subset B \implies A \subseteq B$)

Beispiel: Es ist eine Menge $M = \{1, 2, 3\}$ gegeben. Dann gilt:

- $M = \{3, 1, 2\} = \{1, 1, 2, 3, 3, 3, 3\}$
- $1 \in M$ und $4 \notin M$
- $\emptyset \subset M$
- $\{1\} \notin M$, aber $\{1\} \subset M$

Bemerkung:

Keine Menge kann Element von sich selbst sein! $\rightarrow M \notin M$

1.0.1 Quantoren

Bemerkung:

Um (Teil-)Mengen zu beschreiben oder Aussagen zu formulieren, werden oft Quantoren benutzt

Bemerkung:

Mengenbeziehungen können auch durch Quantoren dargestellt werden:

$$\begin{aligned} A \subseteq B &\iff \forall e \in A \mid e \in B \\ &\iff \nexists e \in A \mid e \notin B \\ &\iff \forall e_1 \in A \exists e_2 \in B \mid e_1 = e_2 \\ A = B &\iff (A \subseteq B) \wedge (B \subseteq A) \\ &\iff (\forall e \in A \mid e \in B) \wedge (\forall e \in B \mid e \in A) \end{aligned}$$

Quantor	Bedeutung
Allquantor \forall	"für alle" bzw. "für jedes"
Existenzquantor \exists	"es gibt (mindestens) ein" bzw. "es existiert (mindestens) ein"
Eindeutigkeitsquantor $\exists!$	"es gibt genau ein" bzw. "es existiert genau ein"
\nexists	"es gibt kein" bzw. "es existiert kein" (Negation des Existenzquantors)

Beispiel: Im Folgenden sind einige Mengen aufgelistet

- natürliche Zahlen $\mathbb{N} = \{0, 1, 2, 3, 4, 5, \dots\}$
 $\forall x \in \mathbb{N} \exists! y \in \mathbb{N} \mid y = x + 1$
 $\exists! x \in \mathbb{N} \mid x - 1 \notin \mathbb{N}$
 Sei $A \subseteq \mathbb{N}$ mit $0 \in A$ und $\forall x \in A \mid x + 1 \in A$. Dann gilt $A = \mathbb{N}$ (Péano-Axiome, axiomatische Definition der natürlichen Zahlen)
- ganze Zahlen $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
- rationale Zahlen $\mathbb{Q} = \{\frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{Z}, b \neq 0\}$

Mengen können auch andere Mengen als Elemente enthalten:

Beispiel: $N = \{0, \{1, 2\}\}$

- $\{1, 2\} \in N$
- $\{\{1, 2\}\} \subset N$
- $\{1\} \notin N$
- $\{1, 2\} \not\subseteq N$

1.0.2 Die Kardinalität einer Menge

Definition:

Die **Kardinalität** $|M|$, auch Mächtigkeit, einer Menge M beschreibt die Anzahl der Elemente in M .

Beispiel:

- $|\{0, 1, 2\}| = |\{0, 0, 0, 1, 2, 2\}| = 3$
- $|\{0, \{1, 2\}\}| = 2$
- $|\emptyset| = |\{\}| = 0$
- $|\{\emptyset\}| = |\{\{\}\}| = 1$
- $|\mathbb{N}| = |\mathbb{Q}| = \infty$

1.1 Mengen durch Aussonderung


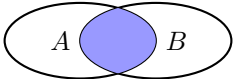
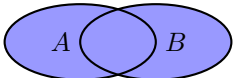


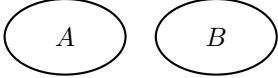
Bemerkung:

Mengen können geschrieben werden, indem Bedingungen an ihre Elemente geknüpft werden

Beispiel:

- $\{x \mid x \text{ erfüllt die Bedingung } *\}$
- $\{x \in M \mid x \text{ erfüllt die Bedingung } *\}$
- $\mathbb{Q} = \{\frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{Z}, b \neq 0\}$
- $\{x \in \mathbb{N} \mid x \leq 2\} = \{0, 1, 2\}$
- $\{x \in \mathbb{Z} \mid \exists y \in \mathbb{Z} \mid x = 3y\} = \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\}$

1.2 Mengenoperationen

Schreibweise	Mengen-Diagramm
$B \subset A$	
$Schnitt : A \cap B = \{x \mid x \in A \wedge x \in B\}$ $= \{x \in A \mid x \in B\}$ $= \{x \in B \mid x \in A\}$	
$Vereinigung : A \cup B = \{x \mid x \in A \vee x \in B\}$	
$Differenz : A \setminus B = \{x \in A \mid x \notin B\}$	
$symmetrische Differenz :$ $A \Delta B = \{x \in A \cup B \mid x \notin A \cap B\}$	
$Disjunktion : A \perp B \iff A \cap B = \emptyset$ $\iff \forall x \in A \mid x \notin B$	

1.3 Rechenregeln

- Schnitt und Vereinigung von Mengen sind **idempotent**:

$$\begin{aligned}A \cap A &= A \\ A \cup A &= A\end{aligned}$$

- Schnitt und Vereinigung von Mengen sind **kommutativ**:

$$\begin{aligned}A \cap B &= B \cap A \\ A \cup B &= B \cup A\end{aligned}$$

- Schnitt und Vereinigung von Mengen sind **assoziativ**:

$$\begin{aligned}A \cap (B \cap C) &= (A \cap B) \cap C \\ A \cup (B \cup C) &= (A \cup B) \cup C\end{aligned}$$

- Schnitt ist **distributiv** über Vereinigung:

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

- Vereinigung ist **distributiv** über Schnitt:

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

Bemerkung:

Vereinigung und Schnitt können auch über beliebig viele Mengen gebildet werden:

- Sei I eine Menge ("Indexmenge", die alle Mengen markiert, die vereinigt werden) und für jedes $i \in I$ sei M_i eine Menge, so gilt für die **Vereinigung** dieser Mengen:

$$\bigcup_{i \in I} M_i := \{x \mid \exists i \in I \mid x \in M_i\}$$

Bedeutung: Die Vereinigung der Mengen M_i ist die Menge aller Elemente x , die in mindestens einer der Mengen M_i enthalten sind.

- Sei I eine Menge und für jedes $i \in I$ sei M_i eine Menge, so gilt für den **Schnitt** dieser Mengen:

$$\bigcap_{i \in I} M_i := \{x \mid \forall i \in I \mid x \in M_i\}$$

Bedeutung: Der Schnitt der Mengen M_i ist die Menge aller Elemente x , die in allen Mengen M_i enthalten sind.

Exkursion: Definieren

Definition:

Das Symbol $:=$ bedeutet so viel wie "wird an dieser Stelle definiert als". Dabei wird einem Objekt, welches noch keine Bedeutung hat, auf der linken Seite des Operators die Bedeutung eines Ausdrucks auf der rechten Seite des Operators zugewiesen

Nehme an, dass $|K| < \infty$, d.h. die Menge $I = \{i_1, i_2, i_3, \dots, i_n\}$ hat endlich viele Elemente

- Die Summe ist dann definiert als

$$\sum_{i \in I} x_i := x_{i_1} + x_{i_2} + x_{i_3} + \dots + x_{i_n} \quad \text{mit} \quad \sum_{i \in \emptyset} x_i := 0$$

- Das Produkt ist dann definiert als

$$\prod_{i \in I} x_i := x_{i_1} \cdot x_{i_2} \cdot x_{i_3} \cdot \dots \cdot x_{i_n} \quad \text{mit} \quad \prod_{i \in \emptyset} x_i := 1$$

- Praktisch wird dabei meistens $I = \{0, 1, 2, \dots, n\}$ verwendet, sodass gilt

$$\sum_{i=0}^n x_i := x_0 + x_1 + x_2 + \dots + x_n$$
$$\prod_{i=0}^n x_i := x_0 \cdot x_1 \cdot x_2 \cdot \dots \cdot x_n$$

Beispiel:

$$\sum_{i=0}^3 i^2 = 0^2 + 1^2 + 2^2 + 3^2 = 0 + 1 + 4 + 9 = 14$$
$$\prod_{i=0}^3 i^2 = 0^2 \cdot 1^2 \cdot 2^2 \cdot 3^2 = 0 \cdot 1 \cdot 4 \cdot 9 = 0$$

1.4 Mengenkompement

Definition:

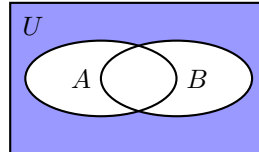
Sei U eine Menge ("Universum") und $A, B \subseteq U$, so schreiben wir das **Komplement**, auch Mengenkompement, von A als $\overline{A} := U \setminus A$.

1.4.1 De-Morgansche Regeln

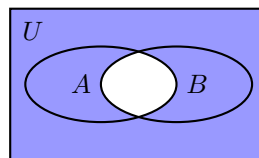
Bemerkung:

Für Komplementärmengen gelten die De-Morgan'schen Regeln:

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



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



1.5 Paare und Produkte

Definition:

Ein **geordnetes Paar** (a, b) ist eine Zusammenfassung von zwei Objekten a und b zu einem Ganzen, wobei die Reihenfolge der Objekte eine Rolle spielt:

Seien A, B Mengen. Sei $a \in A$ und $b \in B$. So schreiben wir:

$$(a, b) := \{\{a\}, \{a, b\}\}$$

Dabei stellt a in der Menge das erste Objekt des Paares dar.

1.5.1 Kartesisches Produkt

Definition:

Das **Kartesische Produkt** $A \times B$ zweier Mengen A und B ist die Menge aller geordneten Paare (a, b) aus Elementen der Mengen, wobei $a \in A$ und $b \in B$:

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

Beispiel: Seien $A = \{1, 2\}$ und $B = \{3, 4\}$. Dann gilt:

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

Bemerkung:

Wenn A und B endlich sind, also $|A| < \infty$ und $|B| < \infty$, so gilt:

$$|A \times B| = |A| \cdot |B|$$

Beispiel: Auf \mathbb{Z} (im Bereich der ganzen Zahlen) ist \leq folgendermaßen definiert:

$$\begin{aligned} x \leq y &:= \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid y - x \in \mathbb{N}\} \\ &:= \{(x, y) \in \mathbb{Z}^2 \mid \exists! z \in \mathbb{N} : x + z = y\} \end{aligned}$$

Es existiert (nach der zweiten Definition) also genau eine Zahl z in \mathbb{N} , sodass $x + z = y$.

1.5.2 Potenzmengen

Definition:

Die **Potenzmenge** $P(M)$ einer Menge M ist die Menge aller Teilmengen der Menge M

Beispiel: Sei M die Menge $\{0, 1, 2\}$, so gilt für die Potenzmenge $P(M)$ der Menge M :

$$P(M) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}\}$$

Bemerkung:

Für eine Menge M mit $|M| < \infty$ gilt:

$$|P(M)| = 2^{|M|}$$

Um eine Teilmenge $M_{Teil} \subseteq M$ auszuwählen gibt es für jedes Element $e \in M$ die zwei Möglichkeiten $e \in M_{Teil}$ und $e \notin M_{Teil}$. Somit ergibt sich aus der Kombinatorik die Anzahl der möglichen Teilmengen aus M als $2^{|M|}$.

1.6 Doppeltes Abzählen

Definition:

Das **Doppelte Abzählen** ist eine Beweisstrategie um zu zeigen, dass zwei Sachen X und Y identisch sind. Dazu finden wir ein Objekt, dass wir auf 2 unterschiedliche Weisen beschreiben können (Art X und Art Y), sodass wir eine Aussage über X und Y erhalten.

1.6.1 Beispiel: Handschlaglemma

Lemma:

Auf einer Konferenz ist die Anzahl der Teilnehmenden, die einer ungeraden Teilnehmerzahl die Hand gibt, immer gerade.

Beweis:

Sei $T = \{t_1, t_2, \dots, t_n\}$ die Menge aller Teilnehmenden der Konferenz, so definieren wir

$$H := \{(t_i, t_j) \in T^2 \mid t_i \text{ gibt } t_j \text{ die Hand}\}$$

H enthält die Paare aller Teilnehmenden, die sich die Hand gegeben haben.

Dabei können wir folgendes beobachten:

- Da teilnehmende sich nicht selbst die Hand geben können, gilt:

$$\forall i \in \{1, 2, \dots\} \mid \{t_i, t_i\} \notin H$$

- Da das Händegeben symmetrisch ist, gilt:

$$\text{Falls } (t_i, t_j) \in H, \text{ dann ist auch } (t_j, t_i) \in H$$

Somit geht jeder Handschlag doppelt in H ein und es muss gelten:

$$|H| = 2 \cdot y, \text{ für } y \in \mathbb{N} \text{ und } y \text{ die Anzahl der Handschläge ist}$$

Sei nun $x_i := |\{t_j \mid (t_i, t_j) \in H\}|$, so ist x_i die Anzahl der Teilnehmenden, denen t_i die Hand gibt.

Zählen wir nun die Handschläge aller Teilnehmenden zusammen, so erhalten wir:

$$x_1 + x_2 + \dots + x_n = \sum_{i=1}^n x_i = |H| = 2 \cdot y$$

Die Kardinalität von H ist die Summe aller Handschläge, also genau, was wir oben stehen haben.

Da $|H|$ gerade ist, muss auch die Summe der x_i gerade sein. Da die x_i die Anzahl der Handschläge sind, ist die Anzahl der Teilnehmenden, die einer ungeraden Anzahl an Teilnehmenden die Hand geben, gerade.

□

1.7 Binomialkoeffizient

Definition:

Der **Binomialkoeffizient** $\binom{n}{k}$ ist die Anzahl der Möglichkeiten, k Elemente aus einer Menge von n Elementen auszuwählen. Wenn $n, k \in \mathbb{N}$, dann wird der Binomialkoeffizient folgendermaßen definiert:

$$\begin{aligned}\binom{n}{k} &:= |\{K \subseteq \{1, 2, \dots, n\} \mid |K| = k\}| \\ &:= |\{K \in P(\{1, 2, \dots, n\}) \mid |K| = k\}| \end{aligned}$$

Da die Potenzmenge $P(A)$ alle möglichen Mengen $A_{Teil} \subseteq A$ enthält, gilt $A_{Teil} \subseteq A \iff A_{Teil} \in P(A)$

Gemäß der Definition gibt der Binomialkoeffizient die Anzahl der Möglichkeiten zu einer n -elementigen Menge eine k -elementige Teilmenge zu finden.

Beispiel: Einige Beispiele für Binomialkoeffizienten sind

- $\binom{n}{k} = 0$, falls $k > n$
- $\binom{n}{0} = 1$, da es nur eine Möglichkeit gibt, keine Elemente auszuwählen: \emptyset
- $\binom{n}{n} = 1$, da es nur eine Möglichkeit gibt, alle Elemente auszuwählen
- $\binom{n}{1} = n$, da es für jedes Element die Möglichkeit gibt, dieses auszuwählen
- $\binom{n}{n-1} = n$, da es für jedes Element die Möglichkeit gibt, dieses nicht auszuwählen
- Etwas abstrakter: $\binom{5}{2} = 10$, da es folgende Möglichkeiten für Teilmengen gibt: $\{1, 2\}, \{1, 3\}, \{1, 4\}, \{1, 5\}, \{2, 3\}, \{2, 4\}, \{2, 5\}, \{3, 4\}, \{3, 5\}, \{4, 5\}$

Um herauszufinden, wie sich der Binomialkoeffizient $\binom{n}{k}$ berechnen lässt, müssen wir zuerst die Fakultät $n!$ definieren.

1.7.1 Fakultät

Definition:

Die **Fakultät** $n!$ gibt die Anzahl der Möglichkeiten an, auf n Elementen eine Reihenfolge zu bilden:

$$\begin{aligned}n! &:= \prod_{i=1}^n i = 1 \cdot 2 \cdot 3 \cdot \dots \cdot n \\ 0! &:= 1 \end{aligned}$$

Proposition:

Sei $n, k \in \mathbb{N}$. Dann gilt $\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}$

Eine Proposition ist eine formale Aussage in der Mathematik, die entweder wahr oder falsch ist und bewiesen oder widerlegt werden kann.

Beweis:

Sei M eine Menge mit $|M| = n$ so gilt:

n	Möglichkeiten das erste Element auszuwählen
$n - 1$	Möglichkeiten das zweite Element auszuwählen
$n - 2$	Möglichkeiten das dritte Element auszuwählen
\vdots	\vdots
$n - k + 1$	Möglichkeiten das letzte Element auszuwählen

Dabei kommt es allerdings zur Mehrfachzählung aller Elemente, da sie in alle Möglichkeiten Elemente auszuzählen einfließen. So wird eine k -elementige Teilmenge $k!$ -mal ausgezählt. So gibt es insgesamt

$$\frac{n \cdot (n-1) \cdot \dots \cdot (n-k+2) \cdot (n-k+1)}{k!} = \frac{n!}{k! \cdot (n-k)!}$$

Möglichkeiten, eine k -elementige Teilmenge aus M auszuwählen.

□

Proposition:

Sei $n, k \in \mathbb{N}$. Dann gilt $\binom{n}{k} = \binom{n}{n-k}$

Beweis:

1. Algebraisch:

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

2. Kombinatorisch:

Es gibt gleich viele Möglichkeiten, eine k -elementige Teilmenge, wie ein $(n-k)$ -elementiges Mengenkomplement, zu wählen.

Beispiel: $\binom{n}{1} = \binom{n}{n-1} = n$ funktioniert aufgrund dieses Prinzips

□

Proposition:

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k} \text{ bzw. } \binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

Beweis:

Sei M eine Menge mit $|M| = n + 1$ mit $x \in M$, so ist die sind alle möglichen Teilmengen aus M :

$$P(M) = \{K \subseteq M \mid x \in K\} \cup \{K \subseteq M \mid x \notin K\}$$

Die Menge $\{K \subseteq M \mid x \in K\}$ enthält alle Teilmengen von M , in denen x als Element enthalten ist.

Die Menge $\{K \subseteq M \mid x \notin K\}$ enthält alle Teilmengen von M , in denen x nicht als Element enthalten ist.

Die Anzahl dieser Mengen lässt sich folgendermaßen als Binomialkoeffizient darstellen:

$$|\{K \subseteq M \mid x \in K\}| = |\{K \subseteq M \setminus \{x\} \mid |K| = k - 1\}| = \binom{n}{k-1}$$

Da festgelegt ist, dass x bereits in K enthalten ist, werden zusätzlich $k - 1$ beliebige Elemente aus $M \setminus \{x\}$ ausgewählt, sodass K insgesamt k Elemente enthält.

$$|\{K \subseteq M \mid x \notin K\}| = |\{K \subseteq M \setminus \{x\} \mid |K| = k\}| = \binom{n}{k}$$

Da festgelegt ist, dass x nicht in K enthalten ist, werden k beliebige Elemente aus $M \setminus \{x\}$ ausgewählt, sodass K k Elemente enthält, was dem normalen Binomialkoeffizienten entspricht.

Nach der Definition des Binomialkoeffizienten gilt für die Menge M :

$$|P(M)| = \binom{n+1}{k}$$

Damit gilt durch gleichsetzen:

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

□

1.7.2 Das Pascalsche Dreieck

Definition:

Das Pascal'sche Dreieck ist eine Form der grafischen Darstellung der Binomialkoeffizienten $\binom{n}{k}$, die auch eine einfache Berechnung dieser erlaubt. Sie sind im Dreieck derart angeordnet, dass jeder Eintrag die Summe der zwei darüberstehenden Einträge ist.

$$\begin{array}{ccccccc}
 & & \binom{0}{0} & & & & 1 \\
 & & & & & & \\
 & \binom{1}{0} & & \binom{1}{1} & & & 1 & 1 \\
 & & & & & & \\
 \binom{2}{0} & \binom{2}{1} & \binom{2}{2} & \iff & 1 & 2 & 1 \\
 & & & & & & \\
 \binom{3}{0} & \binom{3}{1} & \binom{3}{2} & \binom{3}{3} & & 1 & 3 & 3 & 1 \\
 & & & & & & \\
 \binom{4}{0} & \binom{4}{1} & \binom{4}{2} & \binom{4}{3} & \binom{4}{4} & 1 & 4 & 6 & 4 & 1
 \end{array}$$

$\binom{n}{k}$ ist die k+1-te Zahl in der n+1-ten Zeile des Pascalschen Dreiecks

2 Abbildungen

Definition:

Seien A, B Mengen, so ist eine **Abbildung** oder **Funktion** ein Paar (G_f, B) mit $G_f \subseteq A \times B$ mit $\forall a \in A \exists! b \in B : (a, b) \in G_f$. Wir schreiben:

$$f : A \rightarrow B, a \mapsto f(a)$$

Der Ausdruck bedeutet generell, dass A auf B zeigt, also Elemente abbildet (vor dem Komma) und wie diese abgebildet werden (nach dem Komma)

- G_f ist der "Graph" von f
- A ist der Definitionsbereich (DB) von f
- B ist der Wertebereich (WB) von f
- $f(a)$ ist das Bild von a unter f

Es gilt:

$$b = f(a) \iff (a, b) \in G_f$$

Das Paar (a, b) ist genau dann in G_f , wenn die Abbildung von a auf B bzw $f(a)$ b ergibt

Bemerkung:

Es handelt sich nicht um eine Abbildung, wenn ein $a \in A$ auf:

- kein Element in B abgebildet wird
- mehrere Elemente in B abgebildet wird

Definition:

Für $A' \subseteq A$ schreiben wir $f[A'] := \{f(a') \mid a' \in A'\} \subseteq B$ das **Bild von A' unter f** oder **Bild von f** .

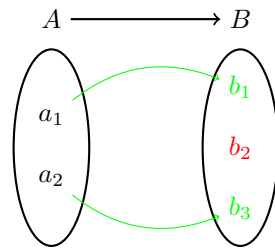
Oft wird für $f[A']$ auch $f(A')$ geschrieben. $f[A']$ enthält alle Bilder von a' und somit alle $b \in B$, die tatsächlich von einem $a \in A$ abgebildet werden

2.0.1 Eigenschaften von Abbildungen

Definition:

Eine Abbildung $f : A \rightarrow B$ heißt

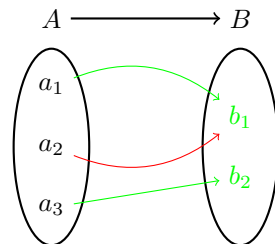
- **injektiv**, falls $\forall b \in B$ existiert höchstens ein $a \in A : f(a) = b$,
oder $f(a_1) = f(a_2) \implies a_1 = a_2$ für $a_1, a_2 \in A$



Die Abbildung
ist **injektiv**,
aber **nicht surjektiv**

"Höchstens ein Pfeil zeigt auf jedes Element in B" \implies injektiv

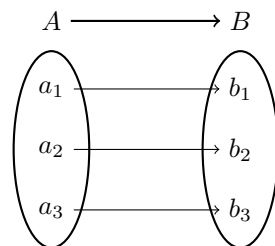
- **surjektiv**, falls $\forall b \in B \exists a \in A : b = f(a)$, d.h. $f[A] = B$



Die Abbildung
ist **surjektiv**,
aber **nicht injektiv**

"Zu jedem Element in B geht ein Pfeil" \implies surjektiv

- **bijektiv**, falls $\forall b \in B \exists! a \in A : b = f(a)$



Die Abbildung ist
bijektiv, also sowohl
injektiv als auch surjektiv

Beispiel: $f : \mathbb{R} \rightarrow \mathbb{R}, x \mapsto x^2$

- f ist nicht injektiv, da $f(-1) = f(1) = 1$
Somit zeigen zwei Elemente $x \in A$ auf das gleiche Element $y \in B$
- f ist nicht surjektiv, da $f(x) \geq 0 \forall x \in \mathbb{R}$
Negative Werte in B werden nicht abgebildet \implies nicht surjektiv

2.0.2 Umkehrabbildung

Definition:

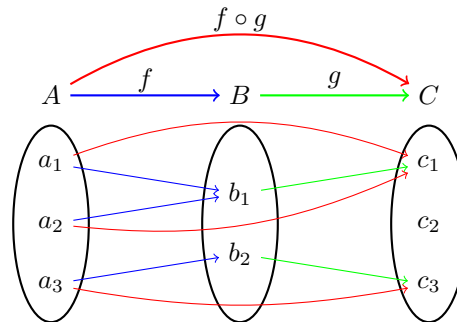
Die **Umkehrabbildung** einer Abbildung ist

- $f^{-1} : B \rightarrow A$, falls die Abbildung **bijektiv** ist
- $f^{-1} : f[A] \rightarrow A, b \mapsto a$ mit $f(a) = b$, falls die Abbildung **injektiv** ist
- allgemein für $B' \subseteq B$: $f^{-1}[B'] := \{a \in A \mid f(a) \in B'\} \subseteq A$
In B' sind alle Elemente aus B , die durch maximal ein Element in A abgebildet werden.

2.0.3 Komposition von Abbildungen

Definition:

Seien $f : A \rightarrow B$ und $g : B \rightarrow C$ Abbildungen, so ist die **Komposition** von f und g als die Abbildung $g \circ f : A \rightarrow C$, $a \mapsto g(f(a))$ definiert



Bei der Mehrfachanwendung einer Abbildung gilt:

Die Potenz gibt an, wie oft die Abbildung angewendet wird

- $f^0 : a \rightarrow A, a \mapsto a$
- $f^1 : A \rightarrow A, f^1 \mapsto a$
- $f^2 := f \circ f$
- $f^3 := f \circ f \circ f$
- $f^n := f^{n-1} \circ f = f \circ f^{n-1}$ für $n \geq 1$

2.0.4 Identität von Abbildungen

Definition:

Die Funktion $id_A : A \rightarrow A, a \mapsto a$ heißt **Identität von A**. Sie ist bijektiv und hat als einzige Abbildung die Eigenschaft, dass für jede Abbildung

- $f : A \rightarrow B$ gilt: $f \circ id_A = f$
- $g : B \rightarrow A$ gilt: $id_A \circ g = g$

Die Identität ist das neutrale Element der Komposition und verändert nichts am Ergebnis: $f \circ id_A = id_A \circ f = f$

Proposition:

Sei A endlich und $f : A \rightarrow A$, Dann sind die folgenden äquivalent:

- f ist injektiv
- f ist surjektiv
- f ist bijektiv

Dies gilt nicht, wenn A unendlich ist. Zum Beispiel ist $f : \mathbb{N} \rightarrow \mathbb{N}, n \mapsto n + 1$ injektiv, nicht surjektiv, da es kein $n \in \mathbb{N}$ gibt, sodass $f(n) = 0$.

$f : \mathbb{N} \rightarrow \mathbb{N}, x \mapsto \begin{cases} x & \text{falls } x = 0 \\ x - 1 & \text{falls } x > 0 \end{cases}$ ist surjektiv, nicht injektiv, da $f(0) = f(1)$

2.1 Größenvergleich von Mengen

Definition:

Seien A, B Mengen, so gilt

- $|A| = |B|$, falls es eine bijektive Abbildung $f : B \rightarrow A$ gibt
- $|A| \leq |B|$, falls es eine injektive Abbildung $f : A \rightarrow B$ gibt
- $|A| < |B|$, falls $|A| \leq |B|$ und $|A| \neq |B|$

Beispiel:

- $|\{1, 2, 3\}| = |\{*, \star, x\}|$
- $|\mathbb{N}| = |\mathbb{Z}|$, denn $f : \mathbb{N} \rightarrow \mathbb{Z}, x \mapsto \begin{cases} \frac{x}{2} & , \text{ falls } x \text{ gerade} \\ -\frac{x+1}{2} & , \text{ falls } x \text{ ungerade} \end{cases}$

0	-1	1
↓	↓	↓
0	1	2
		...
- $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$, denn $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}, f(x, y) = \frac{(x+y)^2 + 3 \cdot x + y}{2}$

2.2 Der Satz von Cantor-Schröder-Bernstein

Definition:

Der **Satz von Cantor** besagt, dass eine Menge A immer weniger Elemente als ihre Potenzmenge $P(A)$ enthält.

$$|A| < |P(A)|$$

Beweis:

Spezialfall: $A = \emptyset$ Dann ist $|A| = 0$ und $|P(A)| = |\emptyset| = 1$

Sei $A \neq \emptyset$: Wir zeigen zuerst " \leq ". Sei $f : A \rightarrow P(A)$, $a \mapsto \{a\}$, dann ist f injektiv, also $|A| \leq |P(A)|$

Da $P(A)$ für jedes Element $a \in A$ eine Menge $\{a\} \in P(A)$ enthält, kann hier das Element $a \in A$ auf $\{a\} \in P(A)$ abgebildet werden.

Jetzt zeigen wir " \neq ": Wir müssen zeigen, dass eine injektive Abbildung $f : A \rightarrow P(A)$ niemals surjektiv ist.

Sei $M := \{a \in A \mid a \notin f(a)\} \in P(A)$. Wir zeigen: $M \notin f[A]$

Widerspruchsannahme: Sei $a \in A$ mit $f(a) = M$.

Dann gilt, falls $a \in M$, dann $a \notin f(a) = M$ und falls $a \notin M$, dann $a \in f(a) = M$

□

2.3 Das Auswahlaxiom

Definition:

Das **Auswahlaxiom** besagt, dass es zu jeder nicht-leeren Menge S eine Auswahlabbildung f gibt, die jeder Menge $X \in S$ ein Element $f(X) \in X$ zuordnet.

Somit schafft das Auswahlaxiom die Möglichkeit "wähle eins aus", was innerhalb der ZF-Axiome nicht definiert ist.

Definition:

Der **Unvollständigkeitssatz** besagt, dass mit ZF nicht gezeigt werden kann, dass ZF widerspruchsfrei ist.

2.4 Die Kontinuumshypothese

Definition:

Die **Kontinuumshypothese** besagt, dass es keine Menge M gibt, so dass $|\mathbb{N}| < |M| < |P(\mathbb{N})|$ gilt.

Die Kontinuumshypothese lässt sich weder beweisen, noch widerlegen.

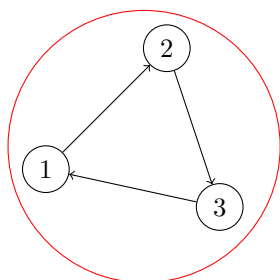
2.5 Permutationen

Definition:

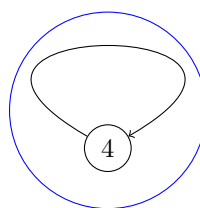
Eine **Permutation** ist eine bijektive Abbildung $\pi : X \rightarrow X$ einer endlichen Menge X . Die Menge aller Permutationen einer Menge mit n Elementen heißt S_n .

Es gibt zwei gebräuchliche Schreibweisen für Permutationen:

- $\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}$ z.B. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$
- Zykelschreibweise: $\pi = (1\ 2\ 3)(4)$, wobei Zyklen disjunkt sind



Zyklus



Fixpunkt

Allgemein:

Sei $\{x_{11}, x_{12}, \dots, x_{1j}, x_{21}, x_{22}, \dots, x_{2j}, \dots, x_{i1}, x_{i2}, \dots, x_{ij}\} \subseteq \{1, \dots, n\}$ mit allen x_{ij} verschieden. Dann ist die Permutation π definiert als:

$$\pi = \{x_{11}, x_{12}, \dots, x_{1j}\} \circ \{x_{21}, x_{22}, \dots, x_{2j}\} \circ \dots \circ \{x_{i1}, x_{i2}, \dots, x_{ij}\}$$

bedeutet:

$$\begin{array}{lll} \pi(x_{11}) = x_{12} & \pi(x_{12}) = x_{13} & \dots \\ \pi(x_{21}) = x_{22} & \pi(x_{22}) = x_{23} & \dots \end{array}$$

Diese Schreibweise ist nicht eindeutig, da

- Zyklen vertauscht werden können:

$$(1\ 2)(3\ 4) = (3\ 4)(1\ 2)$$

- Zyklen rotiert werden können, sodass ein beliebiges Element an erster Stelle steht:

$$(1\ 2\ 3\ 4) = (2\ 3\ 4\ 1) = (3\ 4\ 1\ 2) = (4\ 1\ 2\ 3)$$

- Zyklen der Länge, also Fixpunkte, ausgelassen werden können:

$$(1\ 2\ 3)(4) = (1\ 2\ 3)$$

2.5.1 Komposition von Zyklen

Es gibt 2 besondere Arten von Zyklen in Permutationen:

- zyklische Permutationen: ein Zyklus der Länge n in S_n
- Transposition: Zyklus der Länge 2 $(ij) = (ji)$ mit $i \neq j$

Bei der Komposition von Zyklen gibt es mehrere Rechenregeln:

- $(x_1 x_2 \dots x_i)^i = (1) = id_{\{1,2,\dots,n\}}$
Wenn also auf ein Element x_i der Zyklus i -mal angewendet wird, ist das Ergebnis wieder das Element x_i
- $(x_1 x_2 \dots x_i) (x_i x_{i+1} \dots x_j) = (x_1 x_2 \dots x_j)$ mit $\{x_1, x_2, \dots, x_j\} \subseteq \{1, 2, \dots, n\}$
Beispiel: $(1\ 2\ 3) \circ (3\ 4\ 5) = (1\ 2\ 3\ 4\ 5)$

Bemerkung:

Wenn $(x_1 x_2 \dots x_k)$ und $(y_1 y_2 \dots y_l)$ disjunkte Zyklen sind, dann gilt:

$$(x_1 x_2 \dots x_k) \circ (y_1 y_2 \dots y_l) = (x_1 x_2 \dots x_k)(y_1 y_2 \dots y_l)$$

Wenn die Zyklen nicht disjunkt sind, dann ist der zweite Ausdruck formal nicht korrekt, wird meist jedoch als Komposition angenommen.

Lemma:

Sei $(x_1 x_2 \dots x_k) \in S_n$ ein Zykel und $\pi \in S_n$. Dann gilt:

$$\pi \circ (x_1 x_2 \dots x_k) \circ \pi^{-1} = (\pi(x_1) \pi(x_2) \dots \pi(x_k))$$

Beweis:

Sei $\pi_i \in \{1, 2, \dots, n\}$. Jedes $j \in \{1, 2, \dots, n\}$ kann eindeutig so dargestellt werden:

$$\begin{aligned} \pi \circ \{x_1, \dots, x_k\} \circ \pi^{-1}(\pi(i)) &= \pi \circ \{x_1, \dots, x_k\} \circ (i) \\ &= \begin{cases} \pi(x_{j+1}), & i \notin \{x_1, \dots, x_k\} \\ \pi(x_l + 1), & i = x_l \\ \pi(x_1), & i = x_k \end{cases} \end{aligned}$$

□

Beispiel:

$$\begin{aligned}(1\ 2)(3\ 4\ 5) \circ (2\ 3)(1\ 5) &= (1\ 2)(3\ 4\ 5) \circ (5\ 1)(2\ 3) \\ &= (1\ 2) \circ (3\ 4\ 5\ 1) \circ (2\ 3) \\ &= (2\ 1\ 3\ 4\ 5) \circ (2\ 3) \\ &= (4\ 5\ 2) \circ (2\ 1\ 3) \circ (2\ 3) \\ &= (4\ 5\ 2)(1\ 3) \circ (3\ 2) \circ (3\ 2) \\ &= (4\ 5\ 2)(1\ 3)\end{aligned}$$

Proposition:

Jedes Element aus S_n ist eine Komposition aus Zyklen.

Beweis:

Sei $(x_1 \dots x_k)$ ein Zyklus, dann gilt:

$$(x_1 \dots x_k) = (x_1\ x_2) \circ (x_2\ x_3) \circ \dots \circ (x_{k-1}\ x_k)$$

Jedes $\pi \in S_n$ kann also als Komposition von Zyklen dargestellt werden.

□

Satz:

$$|S_n| = n!$$

Beweis:

- n Möglichkeiten für $\pi(1)$
- $n - 1$ Möglichkeiten für $\pi(2)$
- ...
- 1 Möglichkeit für $\pi(n)$

□

2.5.2 Stirlingsche Formel

Satz:

Stirlingsche Formel: $\forall n \in \mathbb{N} : \sqrt{2\pi n} \cdot \left(\frac{n}{e}\right)^n < n! < \sqrt{2\pi n} \cdot \left(\frac{n}{e}\right)^n \cdot e^{\frac{1}{12n}}$
 $e = \text{Eulersche Zahl} = \sum_{k=0}^{\infty} \frac{1}{k!} = 2,71728\dots$

Anwendung: Wie viele Stellen hat 1000!?

Sei lg der 10er-Logarithmus: $10^{lg(x)} = x$

$$\lg(\sqrt{1\pi n} \cdot n^n \cdot \left(\frac{1}{e}\right)^n) = \frac{1}{2} \cdot \lg(2\pi n) + n \cdot \lg(n) - n \cdot \lg(e)$$

Für $n = 1000$: $\approx 1,8991 + 3000 - 434,9448 = 2566,9543$

Der "Fehlerterm", also die maximale Abweichung, beträgt $\lg\left(\frac{1}{e^{12n}}\right) \approx 0.00036$
 $\Rightarrow 1000!$ hat 2567 Stellen

3 Boolesche Funktionen und Aussagenlogik

3.1 Boolesche Funktionen

Definition:

Sei $n \in \mathbb{N}$. Eine (n-stellige) **Boolesche Funktion** ist eine Abbildung $f : \{0, 1\}^n \rightarrow \{0, 1\}$

Bemerkung:

0 wird aufgefasst als "falsch", \perp , F, F
1 wird aufgefasst als "wahr", \top , T, W

Beispiel:

- Negationsfunktion: $\neg : \{0, 1\} \rightarrow \{0, 1\}, \begin{cases} \neg 0 = 1 \\ \neg 1 = 0 \end{cases}$
- Konjunktion / UND: $\wedge : \{0, 1\}^2 \rightarrow \{0, 1\}, \begin{cases} 0 \wedge 0 = 0 \\ 0 \wedge 1 = 0 \\ 1 \wedge 0 = 0 \\ 1 \wedge 1 = 1 \end{cases}$
- Disjunktion / ODER: $\vee : \{0, 1\}^2 \rightarrow \{0, 1\}, \begin{cases} 0 \vee 0 = 0 \\ 0 \vee 1 = 1 \\ 1 \vee 0 = 1 \\ 1 \vee 1 = 1 \end{cases}$

3.2 Rechengesetze

$\forall x, y, z \in \{0, 1\}$ gilt:

Idempotenz	$x \wedge x = x$	$x \vee x = x$
Kommutativität	$x \wedge y = y \wedge x$	$x \vee y = y \vee x$
Assoziativität	$(x \wedge y) \wedge z = x \wedge (y \wedge z)$	$(x \vee y) \vee z = x \vee (y \vee z)$
De-Morgansche Gesetze	$\neg(x \wedge y) = \neg x \vee \neg y$	$\neg(x \vee y) = \neg x \wedge \neg y$

Wir schreiben:

$$\begin{aligned} x_1 \wedge x_2 \wedge \cdots \wedge x_n &= \bigwedge_{i=1}^n x_i \\ x_1 \vee x_2 \vee \cdots \vee x_n &= \bigvee_{i=1}^n x_i \end{aligned}$$

3.3 Aussagenlogik

3.3.1 Syntax

Definition:

Die **Syntax** behandelt Symbole und Regeln und wie sich diese Symbole zu Ausdrücken zusammenfügen lassen.

3.3.2 Ausdrücke

Definition:

Ein **Ausdruck** besteht aus Variablensymbolen (z.B. X, Y, Z, X_1, X_2), Konnektoren (z.B. \wedge, \vee, \neg), \perp , \top und Klammern. Klammern zeigen dabei nur eine Reihenfolge an.

Beispiel: $X \wedge (\overline{Y} \vee X) \wedge \top$

Ein **Ausdruck in den Variablen S** , wobei S eine Menge ist, kann folgendermaßen rekursiv definiert werden:

- Falls $X \in S_i$, dann ist X ein Ausdruck
- \top und \perp sind Ausdrücke
- Falls A ein Ausdruck ist, ist \overline{A} ein Ausdruck
- Falls A_1 und A_2 Ausdrücke sind, dann sind auch $(A_1 \wedge A_2)$ und $(A_1 \vee A_2)$ Ausdrücke

Beispiel: X könnte stehen für:

- $3 \cdot 2 = 6$ (wahr)
- $\emptyset \in \emptyset$ (falsch)
- $(3 \cdot 2 = 6) \wedge (\overline{\emptyset \notin \emptyset})$ (falsch)
- $(3 \cdot 2 = 6) \vee (\emptyset \in \emptyset)$ (wahr)

3.3.3 Semantik

Definition:

Die **Semantik** behandelt die Bedeutung der Ausdrücke.

3.3.4 Auswertungsfunktion

Definition:

Sei A ein Ausdruck in den Variablen x_1, \dots, x_n , dann ist die **Auswertungsfunktion** die n -stellige boolesche Operation $f_A : \{0, 1\}^n \rightarrow \{0, 1\}$ wie folgt:

Sei $(a_1, \dots, a_n) \in \{0, 1\}^n$, falls A die Gestalt

- X_i mit $i \in \{1, \dots, n\}$ hat, dann ist $f_A(a_1, \dots, a_n) := a_i$
- \top hat, dann ist $f_A(a_1, \dots, a_n) := 1$
- \perp hat, dann ist $f_A(a_1, \dots, a_n) := 0$
- \overline{B} hat, dann ist $f_A(a_1, \dots, a_n) = \overline{f_B(a_1, \dots, a_n)}$
- $A_1 \wedge A_2$ für Ausdrücke A_1, A_2 hat, ist
 $f_A(a_1, \dots, a_n) = f_{A_1}(a_1, \dots, a_n) \wedge f_{A_2}(a_1, \dots, a_n)$
- $A_1 \vee A_2$ für Ausdrücke A_1, A_2 hat, ist
 $f_A(a_1, \dots, a_n) = f_{A_1}(a_1, \dots, a_n) \vee f_{A_2}(a_1, \dots, a_n)$

3.3.5 Belegung eines ausdrucks

Definition:

Eine Abbildung $\beta : S \rightarrow \{0, 1\}$ ist die **Belegung** der Variablen von S . Wir sagen: **β erfüllt A** , falls $f_A(\beta(x_1), \dots, \beta(x_n)) = 1$

Falls es eine Belegung gibt, die A erfüllt, heißt A erfüllbar, sonst unerfüllbar oder Kontradiktion.

Falls jedes $\beta : S \rightarrow \{0, 1\}$ den Ausdruck A erfüllt, heißt A **Tautologie**

Beispiel:

- Der Ausdruck $X \wedge (\overline{Y} \wedge Z)$ in den Variablen X, Y, Z hat eine Belegung $(1, 0, 1)$
- Der Ausdruck \top in den Variablen X, Y ist eine Tautologie
- Der Ausdruck $X \vee \overline{X}$ in den Variablen X, Y ist eine Tautologie
- Der Ausdruck $X \wedge \overline{X}$ in den Variablen X, Y ist eine Kontradiktion

Bemerkung:

Wir schreiben auch:

$$\begin{aligned} \implies & : \{0, 1\}^2 \rightarrow \{0, 1\} X \implies Y := \overline{X} \vee Y \\ \iff & : \{0, 1\}^2 \rightarrow \{0, 1\} X \iff Y := (X \implies Y) \wedge (Y \implies X) \end{aligned}$$

Über S definierte Ausdrücke A und B heißen äquivalent, wenn $A \iff B$ eine Tautologie ist. Das gilt genau dann, wenn $f_A = f_B$ gilt.

Beispiel:

- $X \wedge (\overline{Y} \vee X)$ ist äquivalent zu X .
Dies lässt sich mit dem Absorptionsgesetz zeigen: $X \wedge (X \vee \dots) = X$
- $X \implies Y$ ist äquivalent zu $\overline{y} \implies \overline{X}$

$$\begin{aligned} X \implies Y &\iff \overline{X} \vee Y \\ &\iff \overline{\overline{Y}} \vee \overline{X} \\ &\iff \overline{Y} \implies \overline{X} \end{aligned}$$

3.3.6 Darstellungssatz

Satz:

Darstellungssatz: Sei $f : \{0, 1\}^n \rightarrow \{0, 1\}$ eine boolesche Operation, dann gibt es einen aussagenlogischen Ausdruck A mit $f = f_A$

Beweis:

Definiere die Menge $f^{-1}(1)$ als die Menge aller Tupel $(b_1, \dots, b_n) \in \{0, 1\}^n$, für die $f(b_1, \dots, b_n) = 1$ gilt:

$$f^{-1}(1) = \{(b_1, \dots, b_n) \in \{0, 1\}^n \mid f(b_1, \dots, b_n) = 1\}.$$

Da f genau dann den Wert 1 annimmt, wenn eine der Belegungen in $f^{-1}(1)$ vorliegt, können wir $f(a_1, \dots, a_n)$ als eine Disjunktion über alle Elemente in $f^{-1}(1)$ darstellen:

$$\begin{aligned} f(a_1, \dots, a_n) &= \bigvee_{(b_1, \dots, b_n) \in f^{-1}(1)} \left(\bigwedge_{b_i=1} a_i \wedge \bigwedge_{b_i=0} \overline{a_i} \right). \\ (a_1, \dots, a_n) &= \bigwedge_{(b_1, \dots, b_n) \in f^{-1}(1)} \left(\bigwedge_{b_i=1} (a_i) \wedge \bigwedge_{b_i=0} (\overline{a_i}) \right) \end{aligned}$$

Hierbei gilt:

- Für jede Kombination $(b_1, \dots, b_n) \in f^{-1}(1)$ konstruieren wir einen Konjunktionsterm, der a_i enthält, wenn $b_i = 1$, und $\overline{a_i}$, wenn $b_i = 0$.
- Diese Konjunktionsterme sind genau dann wahr, wenn die Belegung der Variablen $(a_1, \dots, a_n) \iff$ Kombination (b_1, \dots, b_n) .

□

Beispiel: $(0\ 0)\ (1\ 0)\ (1\ 1) = \underbrace{(\bar{X} \wedge \bar{Y})}_{(0\ 0)} \vee \underbrace{(X \wedge \bar{Y})}_{(1\ 0)} \vee \underbrace{(X \wedge Y)}_{(1\ 1)}$

3.3.7 Disjunkte Normalform

Folgerung: Jeder Ausdruck ist zu einem Ausdruck in **disjunkter Normalform (DNF)** äquivalent:

$$\bigvee_i \bigwedge_j l_{ij}, \text{ wobei } l_{ij} \begin{cases} \text{eine Variable } (X_i) \rightarrow \text{”positives Literal”} \\ \text{eine negierte Variable } (\bar{X}_i) \rightarrow \text{”negatives Literal”} \end{cases}$$

$$\bigvee_{\emptyset} = \perp \quad A \vee \bigvee_{\emptyset} \iff A$$

Eine Disjunktion ist genau dann wahr, wenn mindestens eine der vereinigten Aussagen wahr ist.

$$\bigwedge_{\emptyset} = \top \quad A \wedge \bigwedge_{\emptyset} \iff A$$

Eine Konjunktion ist genau dann falsch, wenn mindestens eine der konjugierten Aussagen falsch ist

Bemerkung:

In der Praxis benutzen wir oft:

- Ringschluss:

$$(X_1 \implies X_2) \wedge (X_2 \implies X_3) \wedge \dots \wedge (X_n \implies X_1)$$

ist äquivalent zu:

$$\bigwedge_{(i,j) \in \{1, \dots, n\}^2} (X_i \iff X_j)$$

Da sich alle Aussagen gegenseitig implizieren, sind alle Aussagen äquivalent, wenn der Ringschluss korrekt ist.

- Kontraposition: $X \implies Y$ ist äquivalent zu $\bar{Y} \implies \bar{X}$
- Widerspruchsbeweis: $(X \implies Y) \iff ((X \wedge \bar{Y}) \implies \perp)$

3.4 Erfüllbarkeitsproblem

Das **Erfüllbarkeitsproblem** ist ein wichtiges Beispiel für ein Berechnungsproblem, bei dem ein aussagenlogischer Ausdruck gegeben und die Erfüllbarkeit von A herausgefunden werden soll.

Falls man alle Möglichkeiten für eine Belegung ausprobieren will, kommt man schon ab 185 Variablen auf mehr Fälle, als es Atome im beobachtbaren Universum gibt, da die Fälle exponentiell (2^n) steigen.

Es ist kein Verfahren bekannt, welches dieses Problem in polynomieller Zeit löst. Als "P-NP-Problem" ist es eines der sieben Millennium-Probleme, für dessen Lösung eine Million Dollar Preisgeld ausgestellt werden.

Ein Spezialfall des Erfüllbarkeitsproblems ist die DNF:

Sei A ein DNF: $A_1 \vee A_2 \vee \dots \vee A_k$

- A ist genau dann erfüllt, wenn eines der $A_i \in \{1, \dots, k\}$ erfüllbar ist
- $A_i = l_{i1} \wedge \dots \wedge l_{ij}$ ist genau dann erfüllbar, wenn es keine zwei Literale l_{ij}, l_{ik} gibt, sodass $l_{ij} = \overline{l_{ik}}$

Dieses Problem ist in polynomieller Zeit lösbar, allerdings ist es sehr ineffizient einen Ausdruck in DNF umzurechnen.

3.4.1 konjunkte Normalform

Ein anderer Spezialfall ist die Konjunktive Normalform (KNF):

Ein Ausdruck ist in KNF, falls er die Form

$$\bigwedge_i \underbrace{\bigvee_j \underbrace{l_{ij}}_{\text{Literal}}}_{\text{Klausel}}$$

Wir betrachten Klauseln als Menge von Literalen.

Lemma:

Jeder Ausdruck ist zu einem Ausdruck in konjunkter Normalform äquivalent.

Beweis:

Sei A ein Ausdruck und \overline{A} in DNF: $\bigvee_i \bigwedge_j l_{ij}$.

Dann ist $A \iff \overline{\overline{A}} \iff \overline{\bigvee_i \bigwedge_j l_{ij}}$

Durch Umformung mit den De-Morganschen Gesetzen lässt sich der Ausdruck in KNF darstellen.

Man erhält $\bigwedge_i \bigvee_j \overline{l_{ij}}$, was KNF ist.

□

Beweis:

Ein alternativer Beweisansatz funktioniert mithilfe des Distributivgesetzes:

Beispiel:

$$\begin{aligned} & ((X_1 \wedge Y_1) \vee (x_2 \wedge Y_2) \vee \dots \vee (X_n \wedge Y_n)) \text{ (DNF)} \\ \rightsquigarrow & ((X_1 \wedge Y_1) \vee \dots \vee (X_n \wedge Y_n) \vee X_n) \wedge ((X_1 \wedge Y_1) \vee \dots \vee (X_n \wedge Y_n) \vee Y_n) \\ & \vdots \end{aligned}$$

2^n Konjunkte, d.h. 2^n Klauseln.

Es gilt: Wenn es für das Erfüllbarkeitsproblem in KNF einen polynomiellen Algorithmus gibt, dann auch für das allgemeine Erfüllbarkeitsproblem!

□

3.5 Horn-SAT

3.5.1 Horn-Ausdrücke

Definition:

Ein Ausdruck heißt **Horn**, falls jede Klausel höchstens ein positives Literal hat.

Beispiel: $\underline{X} \wedge \underline{U} \wedge \underline{Z} \wedge (\overline{X} \vee Y) \wedge (\overline{U} \vee \overline{Y} \vee Z)$

Umformuliert: $X \wedge U \wedge Z \wedge (X \implies Y) \wedge ((U \wedge Y) \implies Z)$

$$\begin{array}{llll} X = 1 & & & \\ U = 1 & Z = 0 & Y = 1 & \textcolor{red}{Z = 1} \end{array}$$

Nicht erfüllbar!

3.5.2 Lösungsalgorithmus

Algorithmus für Horn-SAT (SAT = Erfüllbarkeitsproblem):

1. Suche alle Klauseln der Gestalt $\{X\}$ und lösche \overline{X} in allen Klauseln
2. Falls es jetzt eine LEERE Klausel gibt: nicht erfüllbar
3. Gehe zu 1, bis keine Klausel der Form $\{X\}$ vorhanden ist
4. ERFÜLLBAR!

Erfüllende Belegung: Alle Variablen mit Klausel $\{X\}$ auf 1, alle anderen auf 0

Beispiel:

- $\{\underline{X}\}, \{\underline{U}\}, \{\underline{Z}\}, \{\overline{X}, \underline{Y}\}, \{\overline{U}, \overline{Y}, \underline{Z}\}$

Da die zweite Klausel leer ist, ist es nicht erfüllbar.

Falls β eine Erfüllende Bedingung von A ist, dann auch vom Ausdruck nach Schritt 1.

Umgekehrt: Die Belegung in Schritt 4 ist erfüllend, denn:

- Alle Klauseln der Form $\{X\}$ sind wahr nach Konstruktion
- Alle anderen haben mindestens ein \overline{Y} , und sind deshalb wahr

Bemerkung:

Schritte 1 und 2 werden höchstens so oft durchlaufen, wie es Variablen gibt.

Die Laufzeit ist "polynomiell", d.h. "effizient"

4 Die natürlichen Zahlen

4.0.1 Wohlordnung der natürlichen Zahlen

Definition:

Für eine Menge M sei $M^+ := M \cup \{M\} \supset M$

$$\begin{aligned}
 0 &:= \emptyset \\
 1 &:= 0^+ = \emptyset \cup \{\emptyset\} = \{\emptyset\} \\
 2 &:= 1^+ = \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\} \\
 3 &:= 2^+ = \{\emptyset, \{\emptyset\}\} \cup \{\{\emptyset, \{\emptyset\}\}\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \\
 n+1 &:= n^+
 \end{aligned}$$

4.0.2 Rechenoperationen

Addition ist folgendermaßen induktiv definiert:

$$+ : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}, n + 0 = n \text{ und } n + m^+ = (n + m)^+$$

Subtraktion ist nur eine partielle Funktion:

$$- := \{(n, m) \in \mathbb{N} \times \mathbb{N} \mid n \geq m\} \rightarrow \mathbb{N}, n - m := d \text{ mit } m + d = n$$

Multiplikation:

$$\cdot : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}, n \cdot 0 = 0 \text{ und } n \cdot m^+ = n \cdot m + n$$

Es gelten die bekannten Kommutativitäts-, Assoziativitäts- und Distributivitätsgesetze.

$$\mathbb{N} = \{0, 1, 2, 3, \dots\}$$

Es gilt: Sei A eine Menge mit $0 \in A$. Falls $\forall a \in A, a^+ \in A$, dann ist $\mathbb{N} \subset A$. Dabei ist \mathbb{N} das kleinste solche A .

Auf \mathbb{N} gibt es eine Ordnung:

$$\begin{aligned} n < m & \quad \text{falls} \quad n \in m \text{ oder } n \subset m \\ n \leq m & \quad \text{falls} \quad n \subseteq m \end{aligned}$$

4.0.3 Ordnungen

Definition:

Sei A eine Menge. Eine **Ordnung** ist $R \subseteq A \times A$ mit

1. $\forall a \in A : (a, a) \in R$
2. $((a, b) \in R \wedge (b, c) \in R) \implies (a, c) \in R$
3. $((a, b) \in R \wedge (b, a) \in R) \implies a = b$

Dieses \leq ist eine Ordnung:

- reflexiv: $\forall n \in \mathbb{N} : n \leq n$
- transitiv: $\forall n_1, n_2, n_3 \in \mathbb{N} : n_1 \leq n_2 \wedge n_2 \leq n_3 \implies n_1 \leq n_3$
- anti-symmetrisch:
 $\forall n_1, n_2 \in \mathbb{N} : n_1 \leq n_2 \wedge n_2 \leq n_1 \implies n_1 = n_2$

Diese Ordnung ist **total**: $\forall n_1, n_2 \in \mathbb{N} : n_1 \leq n_2 \vee n_2 \leq n_1$
 und eine **Wohlordnung**:

$\forall T \subseteq \mathbb{N}$ mit $T \neq \emptyset, \exists! \min(T) \in T : \forall n \in T : \min(T) \leq n$

Jede nicht-leere Teilmenge T von \mathbb{N} hat ein kleinstes Element $\min(T)$

Statt $(3, 5) \in \leq$ schreiben wir $3 \leq 5$

Beispiel: \leq auf \mathbb{Z} ist keine Wohlordnung, da \mathbb{Z} kein kleinstes Element hat.

4.1 Vollständige Induktion

Seien A_0, A_1, \dots Aussagen.

Wir zeigen: $\forall n \in \mathbb{N} : A_n$ ist wahr.

Wir gehen wie folgt vor:

1. Induktionsanfang (IA): A_0 gilt
2. Induktionsschritt (IS): $\forall n \in \mathbb{N} : A_n \implies A_{n+1}$
3. Induktionsschluss: $\forall n \in \mathbb{N} : A_n$ ist wahr

Warum funktioniert das?

Sei $T = \{n \in \mathbb{N} \mid A_n \text{ wahr}\}$

IA: $0 \in T$

IS: $\forall n \in T : n^+ \in T$

Daher: $T = \mathbb{N}$

Beispiel: Zu zeigen: $\forall n \in \mathbb{N} : \sum_{i=0}^n i = 0 + 1 + \dots + n = \frac{n \cdot (n+1)}{2}$
 A_n ist die Aussage $\sum_{i=0}^n i = \frac{n \cdot (n+1)}{2}$

1. IA: A_0 ist wahr:

$$\sum_{i=0}^0 i = 0 = \frac{0 \cdot (0+1)}{2} \quad \checkmark$$

Induktionsvoraussetzung (IV):

$$\sum_{i=0}^n i = \frac{n \cdot (n+1)}{2}$$

2. IS:

$$\sum_{i=0}^{n+1} i = (n+1) + \sum_{i=0}^n i \stackrel{IV}{=} (n+1) + \frac{n \cdot (n+1)}{2} = \frac{(n+1) \cdot (n+2)}{2}$$

- 3.

□

Behauptung:

Jede ungerade Zhl ist gerade.

Beweis:

IV: A_n : die n-te ungerade Zahl $2n+1$ ist gerade.

IS: die (n+1)-te ungerade Zahl $2(n+1)+1 = (2n+1)+2$

$2n+1$ ist nach IV gerade, also ist der gesamte Term gerade.

□

Problem: Der Induktionsanfang fehlt! Wir hätten nachweisen müssen, dass 1 gerade ist.

Satz:

Seien A, B Mengen mit $|A| = |B| < \infty$ und sei $f : A \rightarrow B$ eine Abbildung, dann gilt:

$$f \text{ ist injektiv} \iff f \text{ ist surjektiv} \iff f \text{ ist bijektiv}$$

Beweis:

Vollständige Induktion:

A_n : Seien A, B Mengen mit $|A| = |B| = n$, dann ist jedes injektive $f : A \rightarrow B$ auch surjektiv.

A: $n = 0$, $A = B = \emptyset$ und die leere Funktion $\emptyset \rightarrow \emptyset$ ist surjektiv.

IV: $f' : A \setminus \{a\} \rightarrow B \setminus \{f(a)\}$, $f'(a') = f(a')$ ist bijektiv.

IS: Seien A, B Mengen mit $|A| = |B| = n + 1 > 0$ und $f : A \rightarrow B$ injektiv.

Sei $a \in A$. Ein solches a existiert, da $A \neq \emptyset$

f injektiv $\implies \forall a' \in A$ mit $a' \neq a : f(a') \neq f(a)$,

Zwei Elemente aus A zeigen nicht auf das gleiche Element in B , da die Abbildung injektiv ist

d.h. $f' : A \setminus \{a\} \rightarrow B \setminus \{f(a)\}$, $f'(a') = f(a')$ ist eine injektive Abbildung.

Wir definieren eine neue Abbildung, über alle Element von A und B , bis auf a und $f(a)$

$$|A \setminus \{a\}| = |B \setminus \{f(a)\}| = n$$

Die Mächtigkeit der Mengen A, B ist von $n + 1$ um 1 gesunken, da wir ein Element ausschließen

$$\text{Dann: } f[A] = f'[A \setminus \{a\}] \cup f[\{a\}] = B \setminus \{f(a)\} \cup f[\{a\}] = B$$

□

4.2 Teilbarkeit

Definition:

Seien $a, b \in \mathbb{N}$. Wir sagen **a teilt b**, oder a ist ein **Teiler** von b , oder b ist ein **Vielfaches von a** und schreiben $a \mid b$, falls $\exists k \in \mathbb{N} : b = a \cdot k$

Beispiel:

- $\forall n \in \mathbb{N} : n \mid 0$
- Falls $0 \mid n$, dann $n = 0$
Teilbarkeit ist etwas anderes als Division. Obwohl Teilbarkeit durch 0 definiert ist, ist Division durch 0 nicht definiert.
- $\forall n \in \mathbb{N} : 1 \mid n$

Falls $a \mid b$, dann $\frac{b}{a} = k$ mit $a \cdot k = b$

Bemerkung:

$|$ ist eine Ordnung. Sie ist reflexiv, transitiv und anti-symmetrisch.
Sie ist nicht total, da z.B. $2 \nmid 3$ und $3 \nmid 2$

Lemma:

Sei $a, b_1, b_2 \in \mathbb{N}$ und $a \mid b_1$ und $a \mid b_2$, $b_1 \geq b_2$.

Dann: $a \mid (b_1 + b_2)$ und $a \mid (b_1 - b_2)$

Beweis:

Sei $k_1, k_2 \in \mathbb{N}$ mit $b_i = ak_i$; für $i = 1, 2$.

Dann gilt nach dem Distributivgesetz:

$$\begin{aligned}(b_1 + b_2) &= a \cdot k_1 + a \cdot k_2 = a \cdot (k_1 + k_2) \\(b_1 - b_2) &= a \cdot k_1 - a \cdot k_2 = a \cdot (k_1 - k_2)\end{aligned}$$

□

4.3 Primzahlen

Definition:

Eine Zahl $p \in \mathbb{N}$ heißt **Primzahl**, falls $p \neq 1$ und
 $(a \mid p \wedge a \neq 1) \implies a = p$

Beispiel: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ...

Satz:

Euklid: Es gibt unendlich viele Primzahlen

Beweis:

Nehme an, es gäbe nur endlich viele Primzahlen p_1, \dots, p_k .

Sei $n := \prod_{i=1}^k p_i + 1$

Lemma:

$\exists i \in \{1, \dots, k\}$ mit $p_i \mid n$

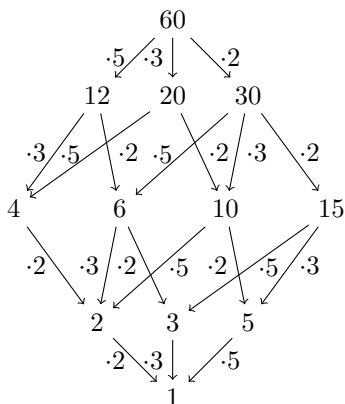
Lemma:

$p_i \mid (n - \prod_{i=1}^k p_i)$, d.h. $p_i \mid n$

Widerspruch!

□

Beispiel: Teilbarkeitsdiagramm für 60:



Bemerkung:

Sei $\pi(n)$ die Anzahl der Primzahlen $\leq n$. Es gibt eine "asymptotische Abschätzung" für $\pi(n)$, der Primzahlsatz:

$$\pi(n) \sim \frac{n}{\ln(n)}$$

d.h.

$$\forall \varepsilon > 0, \exists n_0 \in \mathbb{N} : \forall n > n_0 : \left| \frac{\pi(n) \cdot \ln(n)}{n} - 1 \right| < \varepsilon$$

Offene Frage: Gibt es unendlich viele Primzahlen p , für die $p+2$ eine Primzahl ist?

Primzahlen sind die "Elementarbausteine" der natürlichen Zahlen.

4.3.1 Fundamentalsatz der Arithmetik

Fundamentalsatz der Arithmetik:

Sei $n \in \mathbb{N}$, $n > 0$.

Dann $\exists! k \in \mathbb{N}$ und $\exists! p_1, \dots, p_k \in \mathbb{N}$ Primzahlen mit $p_1 < \dots < p_k$ und $\exists! \alpha_1, \dots, \alpha_k \in \mathbb{N} \setminus \{0\} : n = \prod_{i=1}^k p_i^{\alpha_i} = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$

Beispiel:

- $n = 60; k = 3; p_1 = 2, p_2 = 3, p_3 = 5; \alpha_1 = 2, \alpha_2 = 1, \alpha_3 = 1$
 $60 = 2^2 \cdot 3^1 \cdot 5^1$
- $n = 1; k = 0; 1 = \prod_{i=1}^0 p_i^{\alpha_i}$ "leeres Produkt"

Definition:

Die ganzen Zahlen \mathbb{Z} sind folgendermaßen definiert:

$$\mathbb{Z} := \{0, 1, -1, 2, -2, 3, -3, \dots\}$$

d.h.

$$z \in \mathbb{Z} : |z| := \begin{cases} z & \text{falls } z \in \mathbb{N} \\ -z & \text{falls } z \notin \mathbb{N} \end{cases}$$

Außerdem: $a \mid b$ falls $\exists k \in \mathbb{Z}, a \cdot k = b$

Beispiel: $-3 \mid 6$ da $-3 \cdot (-2) = 6$

4.4 Der euklidische Algorithmus

Definition:

Seien $a, b \in \mathbb{N}$. Der **größte gemeinsame Teiler** (ggT) von a und b ist die größte Zahl $d \in \mathbb{N}$ mit $d \mid a$ und $d \mid b$, geschrieben $d = \text{ggT}(a, b)$ und $\text{ggT}(0, 0) := 0$

Lemma:

Division mit Rest: Seien $a, b \in \mathbb{Z}, b \neq 0$.

Dann $\exists! q, r \in \mathbb{Z}$ mit $a = q \cdot b + r$ und $0 \leq r < b$

Beweis:

Falls $b > 0$:

Beweis für die Existenz:

Sei $q \in \mathbb{Z}$ größtmöglich mit $b \cdot q \leq a$

Setze $r := a - b \cdot q$, dann ist $r \geq 0$

Außerdem ist $b \cdot (q + 1) > 0$, also:

$$r = a - b \cdot q < b \cdot (q + 1) - b \cdot q < b$$

Eindeutigkeit: Sei $a = q \cdot b + r = q' \cdot b + r'$ mit $q, q' \in \mathbb{Z}$ und $0 \leq r, r' < b$

Ohne Beschränkung der Allgemeinheit (O.B.d.A.): $q' \geq q$

Dann: $b \cdot (q - q') = r' - r$, also $b \cdot \underbrace{(q' - q)}_{\geq 0} + r' = r < b$

Falls $q' > q$ ist $b \cdot (q' - q) + r' \geq b$ **Widerspruch!**

Also gilt $q = q'$ und $r = r'$

Falls $b < 0$ müssen einige Vorzeichen vertauscht werden, allerdings bleibt die Beweismethode gleich.

□

Notation: Wir schreiben $a \bmod b = r$

Proposition:

Seien $a, b \in \mathbb{N}$ mit $b > 0$.

Dann: $ggT(a, b) = ggT(a, a \bmod b)$

Beweis:

Sei $a = q \cdot b + r$. Sei $d := ggT(a, b)$ und $d' := ggT(b, r)$

$d \mid a$ und $d \mid b \implies d \mid \underbrace{(a - b \cdot q)}_r$, also $d \leq d'$

Da d Teiler von b und r und d' der ggT von b und r , muss $d \leq d'$

$d' \mid b$ und $d' \mid r \implies d' \mid \underbrace{(b \cdot q + r)}_a$, also $d' \leq d$

Wie oben folgt hieraus analog $d' \leq d$

$\implies d' = d$

□

Euklidischer Algorithmus: $EUKLID(m, n)$

Eingabe: $m, n \in \mathbb{N}$ mit $m \leq n$

Falls $m = 0$: Gebe n aus.

Sonst: Gebe $EUKLID(n \bmod m, m)$ aus.

Ausgabe ist $ggT(m, n)$

4.4.1 Lemma von Bézout

Korollar:

Lemma von Bézout: Sei $m, n \in \mathbb{N}$. Dann gibt es $a, b \in \mathbb{Z}$ mit $ggT(m, n) = a \cdot m + b \cdot n$

Beweis:

Mit vollständiger Induktion:

A_k : $\forall m, n \in \{0, \dots, k\} \exists a, b \in \mathbb{Z} : ggT(m, n) = a \cdot m + b \cdot n$

IA : $k = 0, m = n = 0, 0 = 0 \cdot 0 + 0 \cdot 0$

IS : Seien $m, n \in \{0, \dots, k+1\}$

Falls $m = n$: $m = n = ggT(m, n)$ und $m = 1 \cdot m + 0 \cdot n$

Falls $m \neq n$, O.B.d.A. $m < n$

Seien $q, r \in \mathbb{N}$ mit $r < m$ und $n = q \cdot m + r$

Dann: $ggT(m, n) = ggT(r, m) \stackrel{IV}{=} (\exists a', b' \in \mathbb{Z} :) a' \cdot r + b' \cdot m$

Dann setze: $a := b' - a' \cdot q$ und $b := a'$
Dann gilt: $a \cdot m + b \cdot n = (b' - a' \cdot q) \cdot m + a' \cdot (q \cdot m + r) = a' \cdot r + b' \cdot m = \text{ggT}(m, n)$

□

4.4.2 Erweiterter Euklidischer Algorithmus

Erweiterter Euklidischer Algorithmus: E-EUKLID(m, n)

Eingabe: $m, n \in \mathbb{N}$ mit $m \leq n$

Ausgabe: $a, b \in \mathbb{Z}$ mit $\text{ggT}(m, n) = a \cdot m + b \cdot n$

Falls $m \mid n$: Gebe $(1, 0)$ aus.

Sonst: Berechne $q, r \in \mathbb{N}$ mit $r < m$ und $n = q \cdot m + r$

Sei (a', b') die Ausgabe von E-EUKLID(r, m).

Gebe $(b' - a' \cdot q, b')$ aus.

4.4.3 Euklids Lemma

Lemma:

Euklids Lemma

Sei p eine Primzahl. Dann gilt: $p \mid a \cdot b \implies p \mid a \vee p \mid b$

Beweis:

Angenommen $p \mid mn$, aber $p \nmid m$.

Es ist zu zeigen, dass $p \mid n$:

$\text{ggT}(n, p) = 1$.

Nach Bezout:

$\exists a, b \in \mathbb{Z} : a \cdot p + b \cdot n = 1 \mid \cdot m$

$p \cdot (am) + (nm) \cdot b = m$

Es gilt: $p \mid p(am)$ und nach Voraussetzung/Implikation $p \mid mn$

Analog für $p \nmid n$

□

Lemma:

Jede natürliche Zahl, außer Null, hat eine Primfaktorzerlegung: Sei $n \in \mathbb{N}$, $n \neq 1$. Dann $\exists p \in \mathbb{N}$, p prim mit $p \mid n$

Beweis:

Sei $A \subseteq \mathbb{N} : A := \{n \in \mathbb{N} \mid n > 1 \wedge \nexists p \text{ prim} : p \mid n\}$

Wir leiten einen Widerspruchsbeweis ein.

Annahme: $A \neq \emptyset$.

Dann hat A ein kleinstes Element a . a ist keine Primzahl, denn $a \mid a$.

Das ist so, da es dann nicht in der Menge A enthalten wäre.

Also $\exists b \in \mathbb{N}$ mit $1 < b < a$ und $b \mid a$.

Jede Zahl, die keine Primzahl ist, hat einen Teiler.

a minimal $\implies \exists$ Primzahl $p : p \mid a$.

Dann gilt: $p \mid a$ - **Widerspruch!**

Gegenteilig zu den Voraussetzungen durch die Menge. Somit muss die Menge leer sein.

□

Die Primfaktorzerlegung ist eindeutig:

$n \in \mathbb{N} \setminus \{0\}$

Primfaktorzerlegung von n : $\prod_{i=1}^r p_i^{a_i} \quad p_1 < \dots < p_r, p_1, \dots, p_r$ sind Primzahlen

Primfaktorzerlegung von 1: $\prod_{i=1}^0 p_i^{a_i} = 1$ (leeres Produkt)

Beweis:

(Widerspruchsbeweis)

Angenommen es gibt ein $n \in \mathbb{N} \setminus \{0\}$ mit zwei verschiedenen Primfaktorzerlegungen Z_1, Z_2 . Wähle n kleinstmöglich.

Nach dem Lemma von Euklid teilt jeder Primfaktor p von Z_1 auch einen Primfaktor q von Z_2

Entweder p teilt q oder p teilt Z_2/q , in welchem Falls das ganze für Z_2/q getestet werden kann.

Deshalb gilt: $p = q$

Da p und q beides Primzahlen sind, müssen sie gleich sein.

Dann: Z_1/p und Z_2/p sind zwei verschiedene Primfaktorzerlegungen von n/p .

Dies würde bedeuten, dass $n/p = n/q$ zwei verschiedene Primfaktorzerlegungen hat, was jedoch ein Widerspruch zur Minimalität von n nach der Annahme ist.

Also gilt: $Z_1 = Z_2$

□

4.4.4 Chinesischer Restsatz

Satz:

Seien m, n teilerfremd mit $k, l \in \mathbb{N}$.
 Dann gibt es genau ein $x \in \{0, \dots, m \cdot n - 1\}$
 mit

1. $x \bmod m = k \bmod m$ bzw. $x \equiv k \bmod m$
2. $x \bmod n = l \bmod n$ bzw. $x \equiv l \bmod n$

Beweis:

Nach Bezout: $\exists a, b \in \mathbb{Z} : am + bn = 1$

$$x := l \cdot am + k \cdot bn$$

$$\begin{aligned} lam + kbn &\equiv kbn \pmod{m} && \text{Da } lam \text{ ein Vielfaches von } m \text{ ist} \\ &\equiv (1 - am) \cdot k \pmod{m} && \text{Umstellen obere Gleichung} \\ &\equiv k \pmod{m} && \text{Da } -amk \text{ ein Vielfaches von } m \text{ ist} \end{aligned}$$

Analog für n :

$$lam + kbn \equiv l \cdot am \equiv (1 - bn) \cdot l \equiv l \pmod{n}$$

□

5 Modulare Arithmetik

5.1 Modulorechnung

Definition:

Sei A eine Menge.

Eine Operation A^k nach A heißt (k -stellige) **Operation auf A**

$\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ Definierte auf \mathbb{Z}_n eine zweistellige Operation \oplus und eine zweistellige Operation \odot :

$$\begin{aligned} a \oplus b &:= (a + b) \bmod n \\ a \odot b &:= (a \cdot b) \bmod n \end{aligned}$$

Für $n = 3$:

\oplus	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

\odot	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

5.2 Homomorphieregel

$$\begin{aligned}(a + b) \bmod n &= (a \bmod n) \oplus (b \bmod n) \\ (a \cdot b) \bmod n &= (a \bmod n) \odot (b \bmod n)\end{aligned}$$

5.2.1 Al Kashi's Trick

Bemerkung:

Wie lässt sich $a^b \bmod c$ berechnen?

1. Binäre Exponentiation
2. Homomorphieregel

Beispiel:

- $x^4 = x \cdot x \cdot x \cdot x = (x^2)^2$
- $x^{11} = \left((x^2)^2\right)^2 \cdot x^2 \cdot x$

”Quadrieren und Multiplizieren”

1. Schreibe den Exponenten in Binär:
 $n = 11 = 1 \cdot 8 + 0 \cdot 4 + 1 \cdot 2 + 1 \cdot 1 \implies 1011$
2. Starte mit x
3. Falls nächste Ziffer 0: Quadrieren
4. Falls nächste Ziffer 1: Quadrieren und mit x multiplizieren

Warum funktioniert das?

$$\forall b \in \mathbb{N} \exists q \in \mathbb{N} : a^b = a^{2q+r} = a^{2q} \cdot a^r \text{ mit } r \in \{0, 1\}$$

lässt sich rekursiv mit $b = 2q$ anwenden

Beispiel: $2^{100000} \bmod 100001$

$$100000 = 2^{16} + 2^{15} + 2^{10} + 2^9 + 2^7 + 2^5$$

Binär: 1100001101010000

$$(2^2 \cdot 2)^{(2 \cdot 2 \cdot 2 \cdot 2) \cdot 2} \dots$$

Zwischenergebnisse Modulo 100001 berechnen

5.3 Entscheidungsprobleme

- $a, b \in \mathbb{N}$. Was ist $a \cdot b$?
Mit Schulmathematik polynomiell lösbar.
- Division mit Rest (Modulo):
 $a, b \in \mathbb{N}$ mit $b \neq 0$. Was ist $a \bmod b$?
Mit Schulmathematik polynomiell lösbar.
- Primzahltest:
 $n \in \mathbb{N}$. Ist n eine Primzahl?
2002: "Primes is in P" \implies polynomiell lösbar
- geg: $n \in \mathbb{N}$ und $i \in \mathbb{N}$. Ist das i -te Bit des größten Primfaktors von n eine 1?
Kein polynomielles Verfahren bekannt
- geg: aussagenlogische Formel. Ist die Formel erfüllbar?
Vermutlich existiert kein polynomielles Verfahren

6 Gruppen

Definition:

Eine **Gruppe** besteht aus

- einer Menge G von Elementen
- einer zweistellige Operation auf G , d.h.: $f : G^2 \rightarrow G$ ("Gruppenoperation")
- einer einstelligen Operation $^{-1} : G \rightarrow G$ ("Inversenbildung")
- dem neutralen Element $e \in G$

mit den folgenden Eigenschaften:

- Assoziativität: $\forall a, b, c \in G : a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- neutrales Element: $\forall a \in G : a \cdot e = e \cdot a = a$
- Inversenbildung: $\forall a \in G : a \cdot a^{-1} = a^{-1} \cdot a = e$

Beispiel:

- $(\mathbb{Z}, +, -, 0)$
- \mathbb{Q}
- \mathbb{R}
- \mathbb{C}
- $(\mathbb{Z}_n, \oplus, \ominus, 0)$

6.1 Die multiplikative Gruppe \mathbb{Z}_n

$$\mathbb{Z}_n = \{0, \dots, n-1\} \subseteq \mathbb{Z}$$

mit $\cdot : \mathbb{Z}_n^2 \rightarrow \mathbb{Z}_n : (x, y) \mapsto (x \cdot y) \bmod n$

- ist assoziativ ✓
- neutrales Element 1
- Inverses Element: $x \cdot x^{-1} \equiv x^{-1} \cdot x \equiv 1 \pmod{n}$

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$$

Angenommen, 2 hat Inverses: $2 \cdot x \equiv 1 \pmod{6}$

$$2 \cdot i \equiv 1 \pmod{6}$$

$$3 \equiv 3 \cdot 1 \equiv 3 \cdot (2 \cdot i) \equiv \frac{3 \cdot 2}{0} \pmod{6} \text{ Widerspruch!}$$

6.1.1 Nullteiler

Definition:

Mann nennt $a \in \mathbb{Z}_n \setminus \{0\}$ **Nullteiler**, wenn es ein $b \in \mathbb{Z}_n \setminus \{0\}$ gibt, mit $a \cdot b = 0$

Beispiel: 2 ist ein Nullteiler in \mathbb{Z}_6 , da $2 \cdot 3 = 0 \pmod{6}$

6.1.2 Einheiten

Definition:

Ein Element $a \in \mathbb{Z}_n$ heißt **Einheit**, falls es ein $b \in \mathbb{Z}_n$ gibt mit $a \cdot b = 1$

Definition:

Die Menge aller Einheiten in \mathbb{Z}_n ist die **Einheitsgruppe** \mathbb{Z}_n^*

Beispiel: Einheiten in \mathbb{Z}_6 sind 5, 1.

Lemma:

Sei $m \in \mathbb{Z}_n \setminus \{0\}$. Dann sind äquivalent:

- m ist Einheit in \mathbb{Z}_n .
- m ist kein Nullteiler
- m, n sind teilerfremd: $\text{ggT}(m, n) = 1$

Beweis:

1 \implies 2 Widerspruchsbeweis:

Sei m ein Nullteiler in $\mathbb{Z}_n \setminus \{0\}$, d.h. $\exists b \in \mathbb{Z}_n \setminus \{0\} : m \cdot b = 0$

Angenommen, m ist eine Einheit, d.h. $\exists i \in \mathbb{Z}_n : m \cdot i = 1$

$$0 = i \cdot 0 = i \cdot (m \cdot b) = (i \cdot m) \cdot b = b \quad \text{Widerspruch!}$$

2 \implies 3 Beweis der Kontraposition: $\bar{3} \implies \bar{2}$:

Angenommen, $\text{ggT}(m, n) > 1$

Zu zeigen: m ist Nullteiler:

$$m' := \frac{n}{\text{ggT}(m, n)} \in \mathbb{Z}_n \setminus \{0\}$$

$m \cdot m'$ ist ein Vielfaches von n , also $m \cdot m' \equiv 0 \pmod{n}$

Zu zeigen bleibt: $\forall a, b \in \mathbb{Z}_n$ ist $a \cdot b \in \mathbb{Z}$:

das Inverse von $a \cdot b$ ist $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$

□

6.1.3 Die eulersche φ -Funktion

Definition:

Die **eulersche φ -Funktion** $\varphi(n)$ beschreibt die Anzahl der Einheiten der multiplikativen Gruppe:

$$\varphi(n) = |\mathbb{Z}_n^*|$$

Falls n eine Primzahl ist, so gilt: $\varphi(n) = n - 1$.

Falls n die Potenz einer Primzahl p^k ist, so gilt: $\varphi(n) = p^{k-1} \cdot (p-1)$

Alle Zahlen, die nicht teilerfremd zu p^k sind:

p, p^2, \dots, p^k ($\frac{p^k}{k}$ Zahlen)

Lemma:

Seien n, m Primzahlen. Dann gilt: $\varphi(m \cdot n) = \varphi(n) \cdot \varphi(m)$

Beweis:

Sei $f : \mathbb{Z}_{nm} \rightarrow \mathbb{Z}_n \times \mathbb{Z}_m : f(a) = (a \bmod n, a \bmod m)$.

Diese Abbildung ist nach dem chinesischen Restsatz bijektiv.

Es gilt: $\text{ggT}(a, nm) = 1 \iff \text{ggT}(a, m) = 1$

(Beweis analog mit $\text{ggT}(a, n) = 1$)

Deshalb gibt es eine Umkehrfunktion $\mathbb{Z}_{mn}^* = f^{-1}(\mathbb{Z}_n^* \cdot \mathbb{Z}_m^*)$ und es gilt:

$$\varphi(nm) = |\mathbb{Z}_n^* \cdot \mathbb{Z}_m^*| = |\mathbb{Z}_n^*| \cdot |\mathbb{Z}_m^*| = \varphi(n) \cdot \varphi(m)$$

□

Korollar:

Sei $n = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$ in Primfaktorzerlegung.

Dann gilt: $\varphi(n) = \varphi(p_1^{\alpha_1}) \cdot \dots \cdot \varphi(p_k^{\alpha_k})$

6.2 Zyklische Gruppen

6.2.1 Permutationsgruppen

Definition:

Permutationsgruppen: Sei X eine Menge. $\text{Sym}(X)$ ist die Menge aller Permutationen auf X . Es wird eine Gruppe bezüglich

- der Komposition \circ als Gruppenoperation.
- dem neutralen Element id_X für alle $\pi \in \text{Sym}(X)$: $\pi \circ id_X = id_X \circ \pi = \pi$
- dem Inversen Element, die Umkehrfunktion π^{-1}

6.2.2 Abelsche Gruppen

Definition:

Alle diese Gruppen sind **abelsch**, d.h. die Gruppenoperation ist kommutativ: $\forall a, b \in G : a \cdot b = b \cdot a$

Schreibweise: $(G, \cdot, ^{-1}, e)$

Häufig auch: (G, \cdot)

e und g^{-1} sind ($\forall g \in G$) bereits eindeutig durch \cdot festgelegt.

$$\pi_1 \circ \pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$|x| > 2$, dann ist $\text{Sym}(x)$ nicht abelsch:

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3)$$

$$\pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\ 2)(3)$$

6.2.3 Erzeuger

Definition:

Eine Gruppe $(G; *)$ heißt **zyklisch**, wenn es ein $g \in G$ gibt, sodass

$$G = \{e, g^1, g^{-1}, g \circ g, (g \circ g)^{-2}, \dots\} = \{g^n \mid n \in \mathbb{Z}\}$$

Die Zahl g heißt **Erzeuger** von G .

Beispiel:

- Erzeuger von $(\mathbb{Z}; +)$ ist 1
- Erzeuger von $(\mathbb{Z}_n; +)$ ist 1

6.2.4 Isomorphismen

Definition:

Gruppen $(G, *)$ und (H, \cdot) heißen **isomorph**, falls es eine Bijektion $f : G \rightarrow H$ gibt, sodass gilt:

$$f(a \circ b) = f(a) \cdot f(b)$$

Diese Abbildung ist ein **Gruppenisomorphismus**.

Proposition:

Sei $(G; *)$ eine zyklische Gruppe mit dem Erzeuger g .

Wenn G unendlich ist, dann ist: $f : \mathbb{Z} \rightarrow G : k \mapsto g^k$ ein Gruppensomorphismus.

Sonst sei $|G| = n \in \mathbb{N}$. Dann ist $f : \mathbb{Z}_n \rightarrow G : k \mapsto g^k$ ein Gruppensomorphismus.

Beweis:

$f(k+l) = g^{k+l} = g^k \cdot g^l$ in beiden Fällen.

Beweis der Injektivität, Surjektivität folgt in beiden Fällen:

1. Fall: G ist unendlich.

Falls $k-l = n \neq 0$, dann ist $g^m = g^{m \bmod n}$ **Widerspruch!**
 g^m kann sich nicht wiederholen, da die Menge unendlich ist

2. Fall: G ist endlich. Es gibt ein kleinstes $g^m = e$.

Damit hat $G = \{e, g, g^2, \dots, g^{m-1}\}$ die Kardinalität m .

□

Proposition:

Jede Primzahl $p < n$ ist ein Erzeuger in \mathbb{Z}_n . Somit ist die Anzahl der Erzeuger $= \varphi(n)$

Beweis:

Falls $d = \text{ggT}(a, n) > 1$, dann ist $a, 2a, \dots$ immer durch d teilbar, also ist $1 \notin \{a, 2a, \dots\}$ und ist kein Erzeuger von \mathbb{Z}_n .

Falls $\text{ggT}(a, n) = 1$, dann gibt es nach dem Lemma von Bézout:

$$k, l \in \mathbb{Z} : 1 = ka + ln$$
$$\text{Für } b \in \mathbb{Z}_n : b = b \cdot ka + \underbrace{b \cdot ln}_{\bmod n=0} \quad \text{und} \quad \underbrace{b = a + a + \dots + a}_{b \cdot k - Mal}$$

□

Definition:

Falls (\mathbb{Z}_n^*) zyklisch ist, dann heißt ein Erzeuger von \mathbb{Z}_n^* **Primitivwurzel**.

Bemerkung:

Wenn n eine Primzahl ist, dann ist \mathbb{Z}_n^* zyklisch ist, und es gibt $\varphi(\varphi(n))$ Primitivwurzeln.

Beispiel: $T_{12}^* = \{1, 3, 7, 11\}$ ist nicht zyklisch:

- $1 \cdot 1 \equiv 1 \pmod{12}$
- $5 \cdot 5 \equiv 25 \equiv 1 \pmod{12}$
- $7 \cdot 7 \equiv 49 \equiv 1 \pmod{12}$
- $11 \cdot 11 \equiv 121 \equiv 1 \pmod{12}$

6.3 Der diskrete Logarithmus

Sei p eine Primzahl und g eine Primitivwurzel von \mathbb{Z}_p^* , also \mathbb{Z}_p^* zyklisch. Dann ist $\exp_g : \mathbb{Z}_{p-1} \rightarrow \mathbb{Z}_p^* : k \mapsto g^k$ ein Isomorphismus.

Definition:

Der **diskrete Logarithmus** zur Basis g ist definiert als die Umkehrfunktion von \exp_g :

$$\log_g : \mathbb{Z}_p^* \rightarrow \mathbb{Z}_{p-1} : a \mapsto k \text{ mit } g^k \equiv a \pmod{p}$$

Zur Lösung des diskreten Logarithmus ist kein Algorithmus in polynomieller Laufzeit bekannt:

Eingabe: Primzahl p , Primitivwurzel g , $a \in \mathbb{Z}_p^*$

Ausgabe: $\log_x(a) \in \mathbb{Z}_{p-1}$

Deshalb wird \exp_p auch Einbahnfunktion genannt.

Eine weitere Einbahnfunktion ist die Faktorisierung von $n = p \cdot q$ mit Primzahlen p, q .

Beides sind Grundlagen für Verschlüsselungstechniken.

6.3.1 Beispiel: Diffie-Hellmann-Merkle-Verfahren

Es wird öffentlich eine Primzahl p und eine Primitivwurzel g aus \mathbb{Z}_p^* gewählt.

Person 1 wählt eine zufällige Zahl $a \in \mathbb{Z}_{p-1}$ und berechnet $a' = g^a \pmod{p}$

Person 2 wählt eine zufällige Zahl $b \in \mathbb{Z}_{p-1}$ und berechnet $b' = g^b \pmod{p}$

a' und b' werden öffentlich ausgetauscht.

Person 1 berechnet $c \equiv (b')^a \equiv g^{b \cdot a} \pmod{p}$

Person 2 berechnet $c \equiv (a')^b \equiv g^{a \cdot b} \pmod{p}$

Mithilfe von c können jetzt Nachrichten verschlüsselt werden:

Sei $m = \{m_1, \dots, m_l\}$ eine Nachricht mit $m_i \in \mathbb{Z}_2$ (Binärdarstellung)

Sei c_1, \dots, c_k die Binärschreibweise von c , wobei $k \geq l$ (sonst teile m in mehrere Nachrichten)

Die verschlüsselte Nachricht hat die Form

$$V := (c_1 + m_1 \pmod{2}, \dots, c_l + m_l \pmod{2})$$

Die entschlüsselte Nachricht hat die Form

$$(m_1, \dots, m_l) = (c_1 + (c_1 + m_1 \pmod{2}), \dots, c_l + (c_l + m_l \pmod{2}))$$

6.4 Untergruppen

Definition:

Sei $(G; *)$ eine Gruppe. Eine **Untergruppe** U von G ist eine Teilmenge $U \subseteq G$, sodass $(U, *)$ eine Gruppe ist.

explizit: $e \in U$ und $\forall g, h \in U : g \cdot h, g^{-1} \in U$

Beispiel:

- $\{x \in \mathbb{Z} \mid x \text{ gerade}\}$ ist Untergruppe von $(\mathbb{Z}; +)$
- \mathbb{Z}, \mathbb{Q} sind Untergruppen von \mathbb{R}
- $\{(1 \ 2), id\}$ ist Untergruppe von S_n

Definition:

Sei $(G; *)$ eine Gruppe und $g \in G$. Dann ist die von g erzeugte Untergruppen die kleinste Untergruppe $\langle g \rangle$ von G , die g enthält.

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

Beispiel: $\langle \emptyset \rangle = \{e\}$ ist die triviale Untergruppe

6.4.1 Ordnungen

Definition:

Sei $(G; *)$ eine Gruppe. Die **Ordnung** von G ist $|G|$.

Sei $g \in G$. Die Ordnung von g ist $|\langle g \rangle|$

Beispiel:

- Wenn $(x_1 \ \dots \ x_n)$ ein k -Zyklus in S_n ist, dann ist die Ordnung von $(x_1 \ \dots \ x_k)$ gleich k
- Die Ordnung von 2 in \mathbb{Z} ist unendlich
- Wenn g eine Primitivwurzel mod p prim ist, dann ist die Ordnung von g gleich $p - 1$
- Sei ein Element von S_n : $\sigma = (x_1 \ \dots \ x_k) (y_1 \ \dots \ y_l)$ in Zykelschreibweise, dann ist die Ordnung von σ das kleinste gemeinsame Vielfache von k und l

Bemerkung:

Sei G eine Gruppe mit $g \in G$. Dann gilt:

$$|\langle g \rangle| = \min\{n \in \mathbb{N} \setminus \{0\} \mid g^n = e\}$$

Denn: $g^k = g^{k \bmod \text{ord}(g)}$ $\text{ord}(g)$ ist die Ordnung von g

6.4.2 Nebenklassen

Definition:

Sei G eine Gruppe und U eine Untergruppe von G . Sei $g \in G$.
Dann ist $g \circ U := \{g \circ u \mid u \in U\}$ die **Linksnebenklasse**.
Analog ist $U \circ g := \{u \circ g \mid u \in U\}$ die **Rechtsnebenklasse**.

Beispiel: $(\mathbb{R}^n; +)$, $v \in \mathbb{R}^n$, $U \in \mathbb{R}^n$ ist UVR. Dann ist $v + U$ der affine Teilraum von \mathbb{R}^n ; Nebenklassen sind genau affine Teilräume.

Bemerkung:

Jedes $g \in G$ ist in einer Nebenklasse enthalten, nämlich in $g \circ U$, denn $e \in U$.
Mit jedem $g \in G$ lässt sich mit U eine Nebenklasse bilden, da $e \in U$.
Siehe affine Teilräume

Bemerkung:

Die Abbildung $U \rightarrow g \circ U : u \mapsto g \circ u$ ist bijektiv.

Beweis:

Surjektiv nach Definition von $g \circ U$.
Seien $u_1, u_2 \in U$ mit $g \circ u_1 = g \circ u_2 \implies u_1 = u_2$, also injektiv.

□

Besonders: $|U| = |g \circ U| = |U \circ g|$

Lemma:

Zwei Nebenklassen $g \circ U$ und $h \circ U$ sind entweder gleich oder disjunkt.

Beweis:

1. Falls $x \in c \circ U$, dann gilt: $x \circ U \subseteq c \circ U$
Sei $u \in U$ und $a = g \circ u$. Dann gilt:

$$g \circ u = (a \circ u^{-1}) \circ u = a \circ (u^{-1} \circ u) = a \circ e = a \in a \circ U$$

2. Falls $x \circ U \subseteq c \circ U$, dann gilt: $x \circ U = c \circ U$

Angenommen $g \circ U \cap h \circ U \neq \emptyset$:

Sei $a \in g \circ U \cap h \circ U$, dann ist $a \in g \circ U$ und $a \in h \circ U$.

Nach 1. und 2. gilt deshalb: $a \circ U = g \circ U$ und $a \circ U = h \circ U$.

Somit gilt $g \circ U = h \circ U$

□

6.4.3 Index von Nebenklassen

Definition:

Sei G eine Gruppe und U eine Untergruppe von G . Der **Index** von U in G ist die Anzahl der Nebenklassen von U in G und wird mit $[G : U] = |\{g \circ U \mid g \in G\}|$ bezeichnet.

”Nebenklassen” bezieht sich hier auf Links- oder Rechtsnebenklassen, aber nicht auf alle zusammen

6.5 Satz von Lagrange

Definition:

Sei G eine endliche Gruppe, U eine UG von G . Dann gilt:

$$[G : U] = \frac{|G|}{|U|}$$

Insbesondere: $|U|$ teilt $|G|$

Beweis:

$$G = \bigcup_{g \in G} g \circ U$$

Das sind $[G : U]$ -viele Nebenklassen der Kardinalität $|U| = |g \circ U|$

□

Korollar:

Sei G endlich mit $g \in G$.

Dann ist die Ordnung von g ein Teiler von $|G|$ und $g^{|G|} = e$

Beweis:

$|\langle g \rangle| = |G|$ wegen Lagrange. Sei $|\langle g \rangle| = k$ und $k \cdot l = |G|$:

$$g^{|G|} = g^{k \cdot l} = (g^k)^l = e^l = e$$

□

Beispiel:

- $G \in \mathbb{Z}$, $n \in \mathbb{N}_+$. Dann ist $n \cdot \mathbb{Z} = \{n \cdot a \mid a \in \mathbb{Z}\}$ eine UG.
Sei $b \in \mathbb{Z}$. Dann ist $b + n \cdot \mathbb{Z} = \{b + n \cdot a \mid a \in \mathbb{Z}\}$ eine Nebenklasse, d.h die Nebenklassen sind genau die Restklassen.
Das ist die ”übliche Definition von \mathbb{Z}_n :

$$\mathbb{Z}_n = \mathbb{Z} \setminus \{n \cdot \mathbb{Z}\} = \{a + n \cdot \mathbb{Z}\}$$

- $G = D_4$, $u = \langle r \rangle$ r ist die Rotation um 90°
 $|U| = 4$. Es gibt zwei Nebenklassen: Die Menge der Rotationen und die Menge der Spiegelungen.

Beispiel:

1. "Kleiner Satz von Fermat": $a \in \mathbb{Z}_p$, p teilt nicht a .
Dann gilt: $a^{p-1} \equiv 1 \pmod{p}$

Beweis:

$$a \bmod p \text{ ist Einheit in } \mathbb{Z}_p^* \text{ und } |\mathbb{Z}_p^*| = p - 1 \\ \implies a^{p-1} \equiv 1 \pmod{p}$$

□

2. "Satz von Euler-Fernand": Sei $n \in \mathbb{N}$, $a \in \mathbb{Z}$ mit $\text{ggT}(a, n) = 1$.
Dann gilt: $a^{\varphi(n)} \equiv 1 \pmod{n}$ **Beweis:**

Analog zu oben mit $\varphi(n)$ statt $p - 1$

□

6.6 Das RSA-Verfahren

Bob:

1. Wählt zufällig zwei (große) Primzahlen p, q .
2. Berechnet $n = p \cdot q$
3. Wählt zufällig d mit $\text{ggT}(d, \varphi(n)) = 1$
4. Berechnet $i = d^{-1} \in \mathbb{Z}_{\varphi(n)}^*$ (mit E-Euklid)

Der öffentliche Schlüssel ist (n, d) , er wird übertragen.

Alice:

1. Berechnet $c := m^i \bmod n$ für die Nachricht mit $m \leq n - 1$

Die Nachricht m wird öffentlich übertragen.

$$\text{Dann: } c^d \equiv m^{i \cdot d} \equiv m^{1+k \cdot \varphi(n)} \equiv m \cdot (m^{\varphi(n)})^k \equiv m \pmod{n}$$

Angriffsmöglichkeiten:

- Wenn man $n = p \cdot q$ faktorisieren kann, lässt sich $\varphi(n)$ und damit auch d/i berechnen.
- Durch geschicktes Erraten der Nachrichten (z.B. "Ja") und deren Verschlüsselung kann der private Schlüssel herausgefunden werden.
In der Praxis werden allerdings Zufallsbits angehängt, wodurch die Nachrichten nicht erraten werden können.

Beispiel: RSA-Anwendung: Signieren

Damit Bob weiß, dass die Nachricht m tatsächlich von Alice kommt, kann Alice diese signieren.

Sei (m_A, i_A) der öffentliche Schlüssel und d_A der private Schlüssel von Bob.

Alice verschickt m_A und $s := m^{d_A} \bmod n_A$.

Bob berechnet $s^{i_A} \bmod n_A$

Dabei muss gelten: $s^{i_A} \equiv m^{d_A i_A} \equiv m \bmod n_A$

Das lässt sich kombinieren: erst verschlüsseln und dann signieren.

Beispiel: Alice möchte Bob "I LOVE YOU" schicken.

1. Schlüsselerstellung: B wählt $p = 59$ und $q = 71$.
Dann berechnet er $n = 59 \cdot 71 = 4189$ und $\varphi(n) = (p - 1) \cdot (q - 1) = 58 \cdot 70 = 4060$
B wählt d teilerfremd zu 4060, z.B $d = 13$ (**privater Schlüssel**)
Er berechnet $i \equiv 13^{-1} \pmod{4060}$ mit dem erweiterten euklidischen Algorithmus: $1 = -3 \cdot 4060 + 937 \cdot 13 \implies i = 937$
2. Schlüsselübermittlung: B schickt $(n, i) = (4189, 937)$ an A.
3. Verschlüsselung: zuerst codiert A ihre Nachricht: Leer = 00, A = 01, B = 02, ..., J = 10, ...
Aus "I LOVE YOU" wird "09001215220500251521". Dies ist größer als n , also muss es in Pakete geteilt werden.
Für jedes Paket (z.B "090") berechnet A: $C := 90^{937} \bmod 4189 = 998$ mit Al-Kashi.
4. Nachrichtenübermittlung: A schickt 998 und die anderen verschlüsselten Pakete an B.
5. Entschlüsselung: B berechnet für alle Pakete: $998^{13} \equiv 90 \pmod{4189}$ und hat somit "I LOVE YOU" entschlüsselt.

7 Graphen

Bemerkung:

Schleifen sind nicht erlaubt und Knoten dürfen nicht doppelt verbunden werden.

Bemerkung:

Für eine Menge M schreiben wir $\binom{M}{2} := \{A \subseteq M \mid |A| = 2\}$, die Menge aller zweielementigen Teilmengen von M .

Falls M endlich ist: $|\binom{M}{2}| = \binom{|M|}{2} = \frac{|M| \cdot (|M|-1)}{2}$

Definition:

Ein Graph ist ein Paar $G = (V(G), E(G))$ mit

- $V(G)$ eine Menge ("Knotenmenge")
- $E(G) \subseteq \binom{V(G)}{2}$ ("Kantenmenge")

Wenn der Graph aus dem Kontext geschlossen werden kann, schreiben wir auch nur $G = (V, E)$.

Diese Graphen heißen schlicht bzw. einfach und ungerichtet.

Beispiel:

- Knoten: Facebookprofile
Kanten: $\{a, b\} \in E$, falls a, b befreundet sind
- Knoten: Schauspieler
Kanten: $\{a, b\} \in E$, falls es einen film gibt, in dem beide mitspielen

7.0.1 Wichtige Beispiele für Graphen

- $n \in \mathbb{N}, K_n := (V, E)$, wobei $V = \{1, \dots, n\}$ und $E = \binom{V}{2}$, heißt **n -elementige Clique** oder **n -elementiger vollständiger Graph**
- $I_n := (\{1, \dots, n\}, \emptyset)$ ist die **stabile Menge** der Größe n
- $P_n := (\{1, \dots, n\}, \{\{1, 2\}, \{2, 3\}, \dots, \{n-1, n\}\})$ ist der **Pfad** der Länge $n \geq 2$
- $C_n := (\{1, \dots, n\}, \{\{1, 2\}, \{2, 3\}, \dots, \{n-1, n\}, \{n, 1\}\})$ ist der **Kreis** der Länge $n \geq 3$

7.0.2 Adjazente Knoten

Bemerkung:

Wenn $\{u, v\} \in E$, dann heißen u, w **benachbart** oder **adjazent**.
Der **Grad** von v ist die Anzahl seiner Nachbarn.

Beispiel: In P_5 haben 1, 5 den Grad 1 und 2, 3, 4 den Grad 2.

Definition:

Sei $G = (V, E)$ ein Graph. Der **Komplementärgraph** von G ist

$$\overline{G} := (V, \binom{V}{2} \setminus \{E\})$$

Bemerkung:

$$\overline{\overline{G}} = G \text{ und } \overline{K_n} = I_n$$

7.0.3 isomorphe Graphen

Definition:

Seien G, H Graphen. ein **Isomorphismus** von G nach H ist eine Bijektion $f : V(G) \rightarrow V(H)$ mit
 $\{u, v\} \in E(G) \iff \{f(u), f(v)\} \in E(H)$.
Dann sind G, H isomorph.

Beispiel: Ein Isomorphismus von C_5 nach $\overline{C_5}$ lautet:

$$f \in S_n, f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 2 & 4 \end{pmatrix}$$

7.0.4 Subgraphen

Definition:

Seien G, H Graphen. H heißt

- **Supgraph** von G , falls $V(H) \subseteq V(G)$ und $E(H) \subseteq E(G)$
- **induzierter Subgraph** von G , falls $V(H) \subseteq V(G)$
und $E(H) = \binom{V(H)}{2} \cap E(G)$ Dann ist H durch G und $V(H)$
eindeutig definiert und wir schreiben $H = G[V(H)]$

Beispiel:

- P_3, C_3 sind Subgraphen von K_5
- C_3 ist induzierter Subgraph von K_5
- K_4 ist induzierter Subgraph von K_5
- P_5 ist Subgraph von C_5 , aber kein induzierter Subgraph

7.0.5 Kantenzüge

Definition:

Sei $G = (V, E)$ ein Graph. Ein **Kantenzug** von u_1 nach u_l , wobei $u_1, u_l \in V$, ist eine Kantenfolge (u_1, \dots, u_l) mit $\{u_i, u_{i+1}\} \in E$ für alle $i \in \{1, \dots, l-1\}$

Ein Kantenzug heißt **geschlossen**, falls $u_1 = u_l$, sonst heißt er **offen**

Ein Kantenzug heißt **Weg** oder **Pfad**, falls alle Knoten des Kantenzuges verschieden sind

Ein Kantenzug heißt **Kreis**, falls er geschlossen ist und (u_1, \dots, u_{l-1}) ein Weg ist

7.1 Zusammenhängende Knoten

Definition:

Ein Graph $G = (V, E)$ heißt **zusammenhängend**, falls es für je zwei $s, t \in V$ einen Kantenzug von s nach t gibt.

Bemerkung:

Wenn es einen Kantenzug von s nach t gibt, dann auch einen Pfad:

$$(s, u_1, \dots, u_l, t)$$

ist ein Kantenzug. Für alle $u_i = u_j$ im Kantenzug, existiert dann ein Pfad:

$$(s, u_1, \dots, u_i, u_{j+1}, \dots, u_l, t)$$

7.1.1 Die disjunkte Vereinigung

Definition:

Seien G, H Graphen mit $V(G) \cap V(H) = \emptyset$. Die **disjunkte Vereinigung** von G, H ist:

$$G \uplus H := (V(G) \cup V(H), E(G) \cup E(H))$$

Proposition:

Ein Graph $G = (V, E)$ mit $V \neq \emptyset$ ist genau dann zusammenhängend, falls er nicht als disjunkte Vereinigungen zweier nicht leerer Graphen geschrieben werden kann, d.h:

$$\forall V_1, v_2 \subseteq V; V_1, V_2 \neq \emptyset; V_1 \cap V_2 = \emptyset : G \neq G[V_1] \uplus G[V_2]$$

Beweis:

Richtung \implies : Seien $V_1, V_2 \subseteq V; V_1, V_2 \neq \emptyset; V_1 \cap V_2 = \emptyset$
Angenommen $G = G[V_1] \uplus G[V_2]$:

Dann ist G zusammenhängend und es gibt einen Kantenzug (u, u_1, \dots, u_l, v)

Sei i der Index des ersten Elements mit $u_i \in V_2$.

Dann ist $\{u_{i-1}, u_i\} \in U(G)$, aber $\{u_{i-1}, u_i\} \notin G[V_1] \uplus G[V_2]$.

Widerspruch!

Richtung \impliedby : Angenommen G ist nicht zusammenhängend.

Sei $v \in V$ und $V' = \{u \in V \mid \exists \text{ Kantenzug von } v \text{ nach } u\}$

Proposition:

$$V \setminus V' \neq \emptyset$$

Beweis:

Sonst: $\forall u, u' \in V$ gibt es einen Kantenzug v nach u und v nach u' . Dann ist u nach v nach u' ein Kantenzug von u nach u' . Da u, u' beliebig, wäre G zusammenhängend.

Widerspruch!

□

Dann ist $G = G[V'] \uplus G[V \setminus V']$, sonst gäbe es $v_1 \in V'$ und $u_1 \in V \setminus V'$ mit $\{u_1, v_1\} \in E$ und dann existiert ein Kantenzug v_1 nach u_1 . Das ist ein **Widerspruch** zur Definition von u

□

7.1.2 Zusammenhangskomponenten

Definition:

Eine **Zusammenhangskomponente** (ZK) eines Graphen G ist ein maximal zusammenhängender Subgraph H von G .

Maximal bedeutet: Für jedes $v \in V(G) \setminus V(H)$ gibt es keinen Kantenzug von einem Knoten in H nach v

Bemerkung:

Jede ZK ist ein induzierter Subgraph.

Bemerkung:

Wenn H_1, H_2 zwei ZK sind, dann gilt: $H_1 = H_2$ oder $V(H_1) \cap V(H_2) = \emptyset$

Jeder Graph ist die disjunkte Vereinigung seiner ZK.

7.2 Färbbarkeit

Definition:

Ein Graph $G = (V, E)$ heißt **k -färbbar**, mit $k \in \mathbb{N}$, falls es ein $f : V \rightarrow \{1, \dots, k\}$ gibt mit $\forall \{u, v\} \in E : f(u) \neq f(v)$

Benachbarte Knoten haben also eine andere Farbe.

Beispiel:

- C_6 ist 2-färbbar
- G ist 1-färbbar $\iff E = \emptyset \iff I_n$ mit $n = |V(G)|$
- C_5 ist 3-färbbar, aber nicht 2-färbbar
- K_n ist n -färbbar, aber nicht $n - 1$ -färbbar

Bemerkung:

Falls G n -färbbar ist, dann ist G auch $n + 1$ -färbbar

7.2.1 Entscheidungsproblem Färbbarkeit

Eingabe: endlicher Graph G

Ausgabe: Ist G k -färbbar?

Für $k \geq 3$ ist kein Algorithmus in polynomieller Laufzeit bekannt.

Einen solchen gibt es genau dann, wenn es einen Algorithmus für andere Erfüllbarkeitsprobleme, wie zum Beispiel in der Aussagenlogik, gibt.

Proposition:

Ein endlicher Graph ist genau dann 2-färbbar, wenn er keine Kreise ungerader Länge enthält.

Beweis:

Richtung \implies : Wenn G einen Subgraphen enthält, der zu C_n mit n ungerade isomorph ist, dann gäbe es eine Zweifärbung von G und eine Zweifärbung von C_n . Das ist ein Widerspruch, wie zum Beispiel bei C_5 .

Richtung \impliedby : Wir geben einen Algorithmus an, der entweder eine 2-Färbung berechnet oder einen Kreis ungerader Länge findet.

1. Wähle $v_0 \in V$ und definiere $f(v_0) = 0$
2. $\forall u \in V$ mit $f(u) = i$ bereits definiert. Für jeden Nachbarn v von u :
 - Falls $f(v)$ definiert und $f(v) \neq f(u)$ mache nichts
 - Falls $f(v)$ nicht definiert, definiere $f(v)$ ungleich $f(u)$
 - Sonst gilt $f(v) = f(u)$ und wir haben einen ungeraden Kreis gefunden
3. Fahre fort mit Schritt 2 bis f für alle Knoten der ZK von v_0 definiert ist
4. Fahre fort mit Schritt 1 bis f für alle Knoten von G definiert ist

□

Bemerkung:

2-färbbare Graphen heißen **bipartit**.

7.3 Bäume

Definition:

Ein **Baum** ist ein zusammenhängender Graph ohne Kreise.

Ein **Wald** ist ein Graph ohne Kreise, d.h. eine disjunkte Vereinigung von Bäumen.

Bemerkung:

Jeder Wald (und damit auch jeder Baum) ist 2-färbbar.

Definition:

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

- Falls v den Grad 0 hat, dann heißt v **isoliert**.
- Falls v den Grad 1 hat, dann heißt v **Blatt**.

Lemma:

Jeder endliche Baum mit mindestens zwei Knoten hat ein Blatt.

Beweis:

Sei $v_0 \in V$. Da G mindestens 2 Knoten hat, hat v_0 einen Nachbarn v_1 . Entweder ist v_1 ein Blatt und wir sind fertig oder v_1 hat einen Nachbarn $v_2 \neq v_0$.

Das gleiche Argument: v_2 ist Blatt oder hat Nachbarn $v_3 \neq v_1$.

Da der Baum endlich ist: Falls wir nie ein Blatt finden muss sich irgendwann ein Knoten wiederholen und wir haben einen Kreis gefunden. **Widerspruch** zur Definition eines Baumes.

□

Lemma:

Sei $G = (V, E)$ ein zusammenhängender endlicher Graph und $V \neq \emptyset$.
Es sind äquivalent:

1. G ist ein Baum
2. $|E| = |V| - 1$
3. $|E| \leq |V| - 1$

Beweis:

Mittels Ringschluss: $1 \implies 2 \implies 3 \implies 1$

2. \implies 3. Da $=$ gilt, gilt auch \leq .

1. \implies 2. Mit vollständiger Induktion:

A_n : Jeder Baum mit n Knoten hat genau $n - 1$ Kanten.

IA : Sei $|V| = 1$. Dann ist $|E| = 0$ und es gilt $|E| = |V| - 1$

IS : Sei $n \geq 1$ mit A_n wahr. Sei G ein Baum mit $n + 1$ Knoten.

Dann ist $1 \leq 2$ und G hat ein Blatt v . Deshalb ist $G[V \setminus \{v\}]$ ein Baum mit n Knoten.

Nach IV hat $G[V \setminus \{v\}]$ genau $n - 1$ Knoten.

Dann hat G genau n Kanten, nämlich die aus $G[V \setminus \{v\}]$ und zusätzlich $\{v, w\}$, wobei w der einzige Nachbar von v ist.

3. \implies 1. Sei G zusammenhängend mit $|E| \leq |V| - 1$.

Falls G einen Kreis enthält, können wir aus diesem eine Kante entfernen und erhalten einen zusammenhängenden Subgraphen.

Wir wiederholen dies, bis ein Subgraph G' von G entsteht, der keine Kreise enthält.

Dann ist $G' = (V, E')$ ein Baum und wir gilt 1. \implies 2., gilt $|E| = |V| - 1$.

Es gilt somit: $|E| \geq |E'| = |V| - 1$. Da $|E| \leq |V| - 1$ bekommen wir $|E| = |E'|$ und G ist bereits ein Baum.

□

Bemerkung:

In einem Baum gibt es zwischen zwei Knoten v, w genau einen Weg von v nach w .

7.4 Zweifacher Zusammenhang**Definition:**

Ein Graph G heißt zweifach zusammenhängend, falls $|V| \geq 3$ und falls $\forall v \in V : G - v$ zusammenhängend.

Bemerkung:

I_2 ist nicht 2-fach zusammenhängend

Beispiel:

- C_k für $k \geq 3$
- Falls (V, E) zweifach zusammenhängend ist, dann auch (V, E') für jedes E' mit $E \subseteq E' \subseteq \binom{V}{2}$
- Petersengraph

7.5 Blockgraphen**Definition:**

Sei $G = (V, E)$ ein Graph, $u \in V$ und H die ZK von G die u enthält. Dann heißt u **Gelenkpunkt** von G , falls $H - u$ nicht zusammenhängend ist.

Ein maximal zusammenhängender Subgraph B von G ohne Gelenkpunkte in B heißt **Block** von G .

Beispiel: Sei B ein Block von G :

- $|V(B)| = 1$. Dann besteht B nur aus einem isolierten Knoten
- $|V(B)| = 2$. Dann ist B isomorph zu P_2 und $(V, E \setminus E(B))$ hat mehr ZK als G
- $|V(B)| \geq 3$. Dann ist B maximaler zweifach zusammenhängender Subgraph von G

Lemma:

Sei $G = (V, E)$ ein Graph, B_1 und B_2 Blöcke und $B_1 \neq B_2$.
Dann ist $|V(B_1) \cap V(B_2)| \leq 1$. Falls $v \in V(B_1) \cap V(B_2)$, dann ist v ein Gelenkpunkt in G .
Zwei unterschiedliche Blöcke teilen also maximal einen Knoten, der dann ein Gelenkpunkt ist.

Beweis:

Da B_1 und B_2 beide 2-zusammenhängend sind und v, w in beiden Blöcken liegen, gibt es zwischen v und w in B_1 sowie in B_2 jeweils zwei disjunkte Wege. Damit existieren auch in der Vereinigung der Teilgraphen B_1 und B_2 mindestens zwei disjunkte Wege zwischen v und w . Die Vereinigung $(V(B_1) \cup V(B_2), E(B_1) \cup E(B_2))$ ist daher ebenfalls 2-zusammenhängend. Das widerspricht der Annahme, dass B_1 und B_2 maximal sind. Also gilt $|V(B_1) \cap V(B_2)| \leq 1$.

Angenommen, $V(B_1) \cap V(B_2) = \{v\}$, und v ist kein Gelenkpunkt. Dann würde $G - v$ weiterhin zusammenhängend bleiben, und es existiert ein Weg zwischen zwei Knoten aus $B_1 \setminus \{v\}$ und $B_2 \setminus \{v\}$ über v . Da B_1 und B_2 beide 2-zusammenhängend sind, würde die Vereinigung der Knoten- und Kantenmengen von B_1 und B_2 erneut einen 2-zusammenhängenden Teilgraphen bilden, was wieder der Maximalität der Blöcke widerspricht.

□

Sei $G = (V, E)$ ein endlicher Graph. Der **Blockgraph** ist der Graph $G_B = (V_B, E_B)$ mit

- $V(G_B) = A \cup B$, wobei $A \subseteq V$ die Menge der Gelenkpunkte und B die Menge der Blöcke von G
 $V(G_B)$ ist also eine Vereinigung von Knoten und Knotenmengen
- $E(G_B) = \{\{a, B'\} \mid a \in A, B' \in B, a \in V(B')\}$

Bemerkung:

G_B ist 2-färbbar

Proposition:

Sei G ein endlicher Graph, dann ist G_B ein Wald.
Falls G zusammenhängend ist, dann ist G_B ein Baum.

Beweis:

Angenommen, G_B enthält einen Kreis $(a_0, B_0, a_1, B_1, \dots, B_k, a_0)$.
Es gilt: $V(B_i) \cap V(B_j) \subseteq \{a_i\}$, d.h., zwei Blöcke teilen höchstens einen Knoten, nämlich einen Gelenkpunkt.

Da G_B einen Kreis enthält, gibt es einen geschlossenen Pfad im ursprünglichen Graphen G , der durch die Blöcke B_0, B_1, \dots, B_k läuft.

Konkret gibt es in jedem B_i einen Weg von a_i nach $a_{(i+1) \bmod k}$. Indem diese Wege aneinandergefügt werden, ergibt sich ein Kreis in G .

Das ist ein Widerspruch zur Definition eines Gelenkpunktes: Gelenkpunkte trennen G , sodass es nach ihrem Entfernen keine Kreise geben kann, die über mehrere Blöcke hinweg verlaufen. Also ist G_B kreisfrei und damit ein Wald.

Ist G zusammenhängend, so gibt es zwischen jedem Paar von Blöcken B_i und B_j einen Weg in G , der über Gelenkpunkte führt. Da G_B die Blöcke als Knoten und die Gelenkpunkte als Kanten repräsentiert, ist G_B ebenfalls zusammenhängend.

Da G_B ein kreisfreier und zusammenhängender Graph ist, ist G_B ein Baum.

□

7.6 Ohrendekomposition

Definition:

Sei $G(V, E)$ ein Graph und a_0, \dots, a_n, a_{n+1} paarweise verschieden mit $V \cap \{a_0, \dots, a_{n+1}\} = \{a_0, a_{n+1}\}$.
Dann erhalten wir einen neuen Graphen mit der

- Knotenmenge $V \cup \{a_1, \dots, a_n\}$
- Kantenmenge $E \cup \{\{a_0, a_1\}, \dots, \{a_n, a_{n+1}\}\}$

Dieser Graph entstand aus G durch Anhängen des Weges (a_0, \dots, a_{n+1}) .

Der angehängte Graph wird **Ohr** genannt.

Für einen endlichen Graphen ist eine **Ohrendekomposition** ein Subgraph $C \subseteq H$, der isomorph zu einem C_n für $n \geq 3$, sodass durch Anhängen der Wege w_1, \dots, w_k in Reihenfolge der Graph H entsteht.

Proposition:

Ein endlicher Graph ist genau dann 2-fach zusammenhängend, wenn er eine Ohrendekomposition hat.

Beweis:

Richtung \Leftarrow : Vollständige Induktion nach der Anzahl der Ohren in einer Ohrendekomposition.

A_n ist die Aussage

”Jeder Graph, der aus einem zu einem C_n isomorphen Graphen durch Anhängen von n Ohren entsteht, ist 2-fach zusammenhängend”

IA: $n = 0 \rightarrow$ Dann ist der Graph isomorph zu C_m für $m \geq 3$ und ist damit 2-fach zusammenhängend.

IS: Sei $n \geq 0$, sodass A_n gilt: Wir zeigen A_{n+1} .

Sei a_0, \dots, a_{n+1} das letzte angehängte Ohr und G_n der Subgraph, an den es angehängt wird, um G zu erhalten.

Es ist zu zeigen, dass G 2-fach zusammenhängend ist, also $\forall v \in V : G - v$ zusammenhängend:

Fall 1 $v \in \{a_0, \dots, a_n\} : G - v$ ist G_n und zwei angehängte Pfade, also zusammenhängend

Fall 2 $v \in V \setminus \{G_n\} : G - v$ ist $G_n - v$ und ein angehängter Weg. $G_n - v$ ist nach IV zusammenhängend, also ist $G - v$ zusammenhängend.

Richtung \Rightarrow : Sei G ein 2-fach zusammenhängender Graph.

Sei H ein Subgraph von G , der eine Ohrendekomposition hat, sodass es keinen Subgraphen von G gibt, der größer als H und auch eine Ohrendekomposition hat.

Solch ein H existiert, da G endlich und einen Kreis enthält. Insbesondere gilt: $|V(H)| \geq 3$

H ist ein induzierter Subgraph, da es sonst ein Ohr gäbe, dass an H angehängt werden könnte, was ein Widerspruch zur Maximalität wäre.

Falls $H \neq G$, dann gibt es eine Kante $\{u, v\} \in E(G)$ mit $u \in V(H)$ und $v \notin V(H)$.

Da G 2-fach zusammenhängend ist, gibt es in $G - u$ einen Pfad (v, u_1, \dots, u_n, w) mit $w \in V(H)$ und $u_1, \dots, u_n \notin V(H)$.

Dann ist dieser Pfad ein Ohr, dass an H angehängt werden kann, was ein Widerspruch zur Maximalität ist.

□

7.7 Satz von Menger

Definition:

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

- Zwei Pfade $\{u_1, \dots, u_k\}$ und $\{v_1, \dots, v_n\}$ heißen **disjunkt**, falls $\{u_1, \dots, u_k\} \cap \{v_1, \dots, v_n\} = \emptyset$
- Zwei Pfade $\{a, u_1, \dots, u_k, b\}$ und $\{a, v_1, \dots, v_n, b\}$ heißen **unabhängig**, falls $\{u_1, \dots, u_k\}$ und $\{v_1, \dots, v_n\}$ disjunkt sind
- Seien $A, B \subseteq V$. Ein **A-B-Pfad** ist ein Pfad (v_1, \dots, v_n) mit $A \cap \{v_1, \dots, v_n\} = \{v_1\}$ und $B \cap \{v_1, \dots, v_n\} = \{v_n\}$
- Seien $A, B, X \subseteq V$. Wir sagen: X **trennt** A von B , falls jeder A-B-Pfad einen Knoten aus X enthält

Bemerkung:

- Ein A-A-Pfad muss der Form $\{a\}$ sein
- A trennt A von B
- Falls $A \cap B \neq \emptyset$ und X trennt A von B , dann $A \cap B \subseteq X$

Satz:

Satz von Menger

Sei $G = (V, E)$ ein endlicher Graph und seien $a, b \in U$.

Dann ist die maximale Anzahl paarweise disjunkter A-B-Pfade gleich der kleinsten Zahl $k_{G,A-B}$, sodass es in G eine Menge $X \subseteq U$ der Kardinalität $K_{G,A-B}$ gibt, die A von B trennt.

Korollar:

Sei $G = (V, E)$ ein endlicher Graph und $a, b \in U$ mit $\{a, b\} \notin E$.

Dann ist die maximale Anzahl paarweise unabhängiger Pfade von a nach b gleich der Größe der kleinsten Teilmenge $V \setminus \{a, b\}$, die $\{a\}$ von $\{b\}$ in G trennt.