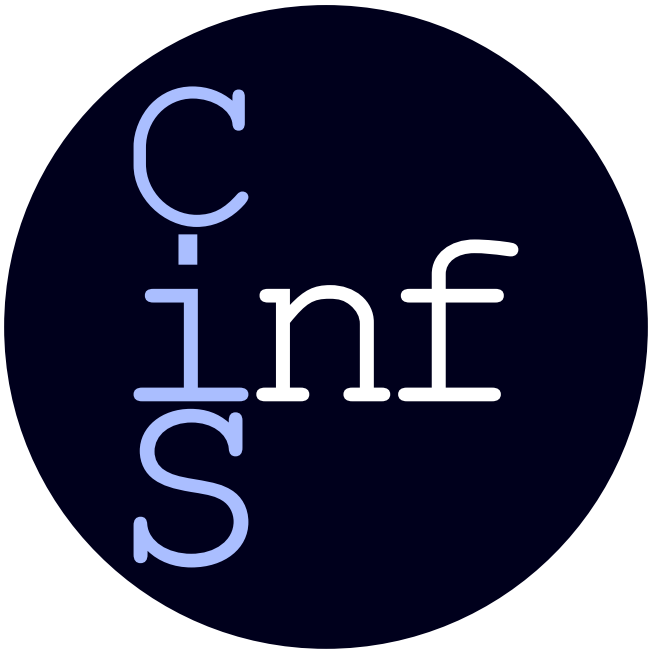
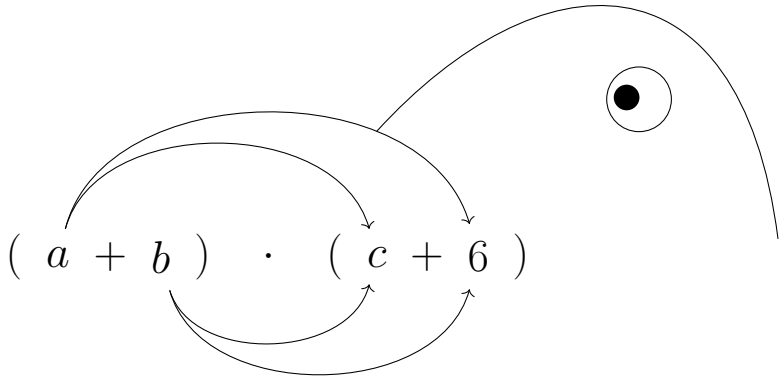


Diskrete Mathematik für Studierende der Informatik 1



Alan Kniep, Livi Franke

19. Februar 2021

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Inhaltsverzeichnis

1. Mathematische Grundlagen und Logik

1.1 Mengen

Definition 1.1.1: Mengen

"Eine Menge ist eine Zusammenfassung bestimmter, wohlunterschiedener Objekte unserer Anschauung oder unseres Denkens zu einem Ganzen; diese Objekte heißen Elemente der Menge."

Cantor

Die Reihenfolge in der die Elemente in einer Menge aufgeführt werden spielt keine Rolle. In einer Menge können keine Elemente mehrfach vorkommen bzw. werden Duplikate ignoriert. Mengen sind durch ihre Elemente eindeutig bestimmt. Seien L und M zwei Mengen so gilt $L = M$ gdw. L und M dieselben Elemente haben.

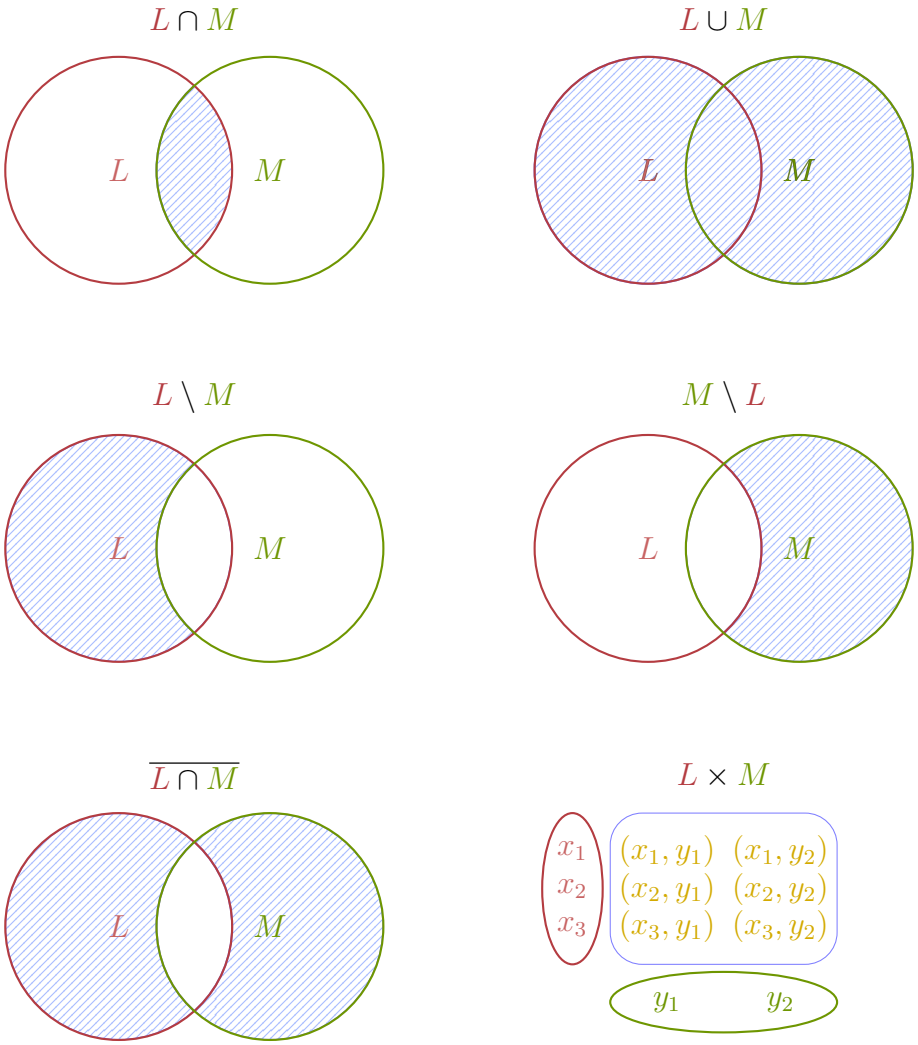
Definition 1.1.2: Mengensyntax

Element von	$\in$	Sei x ein Element der Menge M, so gilt: $x \in M$.
Nicht Element von	$\notin$	Sei x kein Element der Menge M so gilt: $x \notin M$
Teilmenge von	$\subseteq$	$\forall x \in L : x \in M \rightarrow L \subseteq M$
Nicht Teilmenge von	$\not\subseteq$	$\exists x \in L : x \notin M \rightarrow L \not\subseteq M$
Leere Menge	$\emptyset$, $\{\}$	die Menge, die keine Elemente hat

Die leere Menge $\emptyset$ ist Teilmenge jeder Menge, da sie keine Elemente besitzt und somit alle ihre Elemente Teilmenge aller anderen Mengen sind. Ist sie explizit aufgelistet als Element einer Menge M, so gilt auch: $\emptyset \in M$.

1.1.1 Mengenoperationen

Vereinigung	$L \cup M$	$:=$	$\{x \mid x \in L \vee x \in M\}$
Schnitt	$L \cap M$	$:=$	$\{x \mid x \in L \wedge x \in M\}$
Differenz	$L \setminus M$	$:=$	$\{x \in L \mid x \notin M\}$
Potenzmenge	$\mathcal{P}(M)$	$:=$	$\{L \mid L \subseteq M\}$
Kartesisches Produkt	$L \times M$	$:=$	$\{(x, y) \mid x \in L \wedge y \in M\}$



Die Anzahl der Eelemente in der Potenzmenge der Menge M entspricht 2 hoch der Anzahl von Elementen von M:

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

Abgeschlossenheit der Potenzmenge

$$\forall X, Y \in \mathcal{P}(M) : \Big(X \cap Y \in \mathcal{P}(M) \wedge X \cup Y \in \mathcal{P}(M) \wedge \overline{X} \in \mathcal{P}(M) \wedge \overline{Y} \in \mathcal{P}(M)\Big)$$

Satz 1.1.1

Sind L, M und N Mengen, so ist $L \cap (M \cup N)$ äquivalent zu $(L \cap M) \cup (L \cap N)$.

Die Anzahl der Elemente der Menge des kartesischen Produktes der Mengen L und M ist gleich der Anzahl der Elemente der Menge L multipliziert mit der Anzahl der Elemente der Menge M:

$$|M \times L| = |M| \cdot |L|$$

Definition 1.1.3

Ein n-Tupel ist eine geordnete Liste von n Elementen: $(x_1, x_2, \ldots, x_n)$
Ein 2-Tupel nennet man geordnetes Paar, ein 3-Tupel Tripel.

1.2 Logik

Definition 1.2.1: Aussagen

Eine Aussage a ist ein Satz, dem eindeutig der Wahrheits "wahr" (1) oder "falsch" (0) zugeordnet werden kann.

Sollten Sie unseren exzellenten ETI-Cheatsheet [1] bereits gelesen haben, was wir Ihnen sehr empfehlen, dann sehen Sie ja sofort, dass Aussagen eigentlich mit Großbuchstaben benannt werden.

Definition 1.2.2: Junktoren

Konjunktion	$a \wedge b$	"a und b"
Disjunktion	$a \vee b$	"a oder b"
Implikation	$a \to b$	"a impliziert b"
Äquivalenz	$a \leftrightarrow b$	"a gdw. b"
Kontravalenz	a xor b	"entweder a oder b"

Tabelle 1.1: Wahrheitstafel Junktoren

a	b	$\neg a$	$a \wedge b$	$a \vee b$	$a \to b$	$a \leftrightarrow b$	a xor b
0	0	1	0	0	1	1	0
0	1	1	0	1	0	0	1
1	0	0	0	1	1	0	1
1	1	0	1	1	1	1	0

Satz 1.2.1

Sind a, b und c Aussagen, so ist $a \wedge (b \vee c)$ äquivalent zu $(a \wedge b) \vee (a \wedge c)$.

Satz 1.2.2: Kontraposition

Seien a und b Aussagen. Dann ist die Aussage $a \to b$ äquivalent zu $\neg b \to \neg a$.

Definition 1.2.3: Aussageform

Eine Aussage, in der anstelle einer Konstante eine Variable steht nennt man Aussageform. Eine Aussage a lautet als Aussageform $a(x)$.

[1] https://cis-exzellenz.de/files/eti-cheatsheet

Definition 1.2.4: Quantoren

Sei $a(x)$ eine Aussageform und M eine Menge.

Existenzquantor $\exists$
Der Aussage $(\exists x \in M)a(x)$ kann der Wahrheitswert wahr (1) zugeordnet werden, wenn (mindestens) ein Element x der Menge M $a(x)$ erfüllt.
$(\exists x \in M)a(x)$ meint umgangssprachlich "es gibt ein x in M mit $a(x)$."

Allquantor $\forall$
Der Aussage $(\forall x \in M)a(x)$ kann der Wahrheitswert wahr (1) zugeordnet werden, wenn alle Elemente x der Menge M $a(x)$ erfüllen.
$(\forall x \in M)a(x)$ meint umgangssprachlich "für alle x in M gilt $a(x)$."

Existenzaussage

$$\underbrace{\exists x \in \mathbb{N}}_{Quantor}\underbrace{x + 24 = 42}_{Aussageform}$$

Allaussage

$$\underbrace{\forall x \in \mathbb{N}}_{Quantor}\underbrace{(x + 42 > 0)}_{Aussageform}$$

Negation von Quantorenaussagen

$$\neg(\exists x \in \mathbb{N}(x + 24 = 42)) \longleftrightarrow \forall x \in \mathbb{N}(x + 24 \neq 42)$$
$$\neg(\forall x \in \mathbb{N}(x + 42 > 0)) \longleftrightarrow \exists x \in \mathbb{N}(x + 42 \leq 0)$$

1.3 Abbildungen

Definition 1.3.1

Eine **Abbildung** ist eine **Zuordnung**, welche **jedem** Element einer Menge L (mindestens) ein Element einer Menge M zuordnet, man schreibt

$$f : L \to M$$

wobei L der **Definitionsbereich** (auch Vorbereich) und M der **Wertevorrat** (auch Wertebereich) von f ist.

f bildet also jedes $x \in L$ auf genau ein $y \in M$ ab. Hierbei wird y als der Wert von f an der Stelle x bezeichnet.

$$\forall x \in L : f(x) = y,\ y \in M$$

Anstelle von $f(x) = y$ schreibt man auch $x \mapsto y$.

Das **Bild** von f ist die Menge aller Elemente aus dem Wertebereich, welche Elementen aus dem Definitionsbereich zugeordnet sind:

$$\{f(x) : x \in L\} \subseteq M$$

Beispiele:

$$f : \mathbb{N} \to \mathbb{N},\ f(n) = 2 \cdot n + 3$$
$$f : \mathbb{N} \to \mathbb{N};\ n \mapsto 2 \cdot n + 3$$

$$L = \{x_1, x_2, x_3\}, M = \{y_1, y_2\}$$
$$f : L \to M; x_1 \mapsto y_1; x_2 \mapsto y_2; x_3 \mapsto y_1$$
$$\leftrightarrow\ f : L \to M, f(x_1) = y_1, f(x_2) = y_2, f(x_3) = y_1$$

Definition 1.3.2: Injektivität

Eine Abbildung heißt **injektiv**, wenn jedem Element des Wertevorrats maximal ein Element des Definitionsbereich zugeordnet wird:

$$\forall x_1, x_2 \in L : (x_1 \neq x_2 \to f(x_1) \neq f(x_2))$$
$$\forall x_1, x_2 \in L : f(x_1) = f(x_2) \to x_1 = x_2$$
$$\forall y \in f(L)\ \exists! x \in L : f(x) = y$$

Eine Abbildung $f : L \to M$ kann nicht injektiv sein, wenn die Menge M weniger Elemente besitzt als L.

Definition 1.3.3: Surjektivität

Eine Abbildung heißt **surjektiv**, wenn jedem Element des Wertevorrats mindestens ein Element des Definitionsbereichs zugeordnet wird:

$$\forall y \in M \; \exists x \in L : f(x) = y$$

Eine Abbildung $f : L \to M$ kann nicht surjektiv sein, wenn die Menge M mehr Elemente besitzt als L.

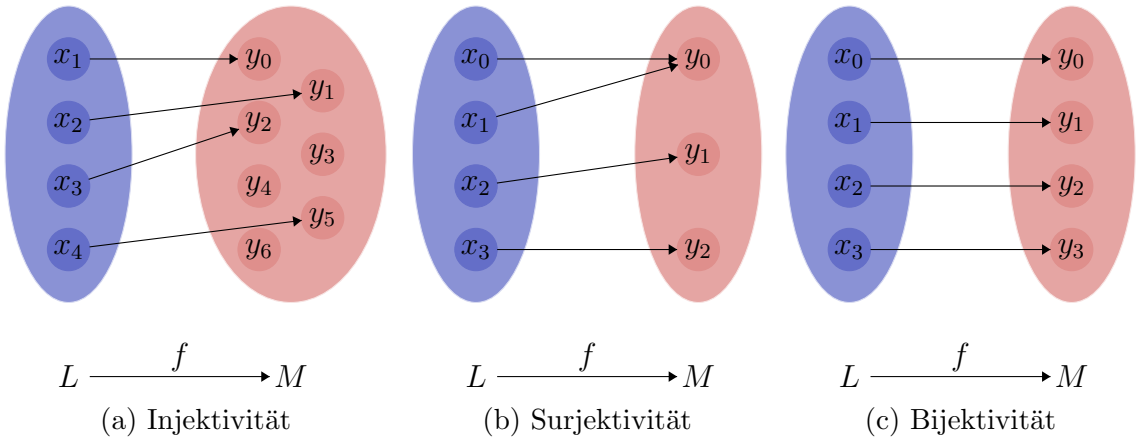
Definition 1.3.4: Bijektivität

Eine Abbildung heißt **bijektiv**, wenn sie sowohl injektiv, als auch surjektiv ist, also jedem Element des Wertevorrats genau einem Element des Definitionsbereichs zugeordnet ist:

$$\forall y \in M \; \exists! x \in L : f(x) = y$$

Eine Abbildung $f : L \to M$ kann nur bijektiv sein, wenn die Menge M genau gleich viele Elemente besitzt wie L.

Abbildung 1.1: $L \longrightarrow M, \quad f(x) = y$



(a) Injektivität (b) Surjektivität (c) Bijektivität

Definition 1.3.5: Verknüpfung

Eine n-stellige **Verknüpfung** (auch Operation) auf einer Menge L ist eine Abbildung

$$f : L^n \to M$$

Eine 2-stellige Verknüpfung nennt man **binäre** Verknüpfung, Beispiele hierfür sind Addition und Multiplikation:

$$f : \mathbb{N}^2 \to \mathbb{N}; (x_1, x_2) \mapsto x_1 + x_2$$

Definition 1.3.6: Bild und Urbild

Seien M und L Mengen, $f : M \to L$ eine Abbildung und $M' \subseteq M$ sowie $L' \subseteq L$. So ist das Bild von M' unter f die Menge

$$f[M'] = \{y \in L : \exists x \in M' \, (f(x) = y)\} = \{f(x) : x \in M'\}$$

und das Urbild von L' unter f die Menge

$$f^{-1}[L'] = \{x \in M : f(x) \in L'\}$$

Satz 1.3.1

Seien M und L Mengen und $f : M \to L$. Für alle $M_1, M_2 \subseteq M$ und $L_1, L_2 \subseteq L$ gilt:

(1) $f[M_1 \cap M_2] \subseteq f[M_1] \cap f[M_2]$
(2) $f[M_1 \cup M_2] = f[M_1] \cup f[M_2]$
(3) $f^{-1}[L_1 \cap L_2] = f^{-1}[L_1] \cap f^{-1}[L_2]$
(4) $f^{-1}[L_1 \cup L_2] = f^{-1}[L_1] \cup f^{-1}[L_2]$
(5) $f^{-1}[M_1] \supseteq M_1$
(6) $f[f^{-1}[L_1]] \subseteq L_1$

Definition 1.3.7: Komposition

Die Komposition zweier Funktion f und g, mit $f : M \to L$ und $g : L \to N$ ist gegeben durch:

$$g \circ f : M \to N; m \mapsto g(f(a))$$

und wird als g nach f oder g Kringel[1] f gelesen.

Die Komposition von Abbildungen erfüllt das Assoziativgesetz.

Satz 1.3.2

$$f : M \to L, \; g : L \to N$$
$$h \circ (g \circ f) = (h \circ g) \circ f$$

Definition 1.3.8: Einschränkung

Unter Einschränkung (auch Restriktion) einer Funktion $f : M \to L$ auf eine Menge $M' \subseteq M$ versteht man die Funktion $g : M' \to L; x \mapsto f(x)$. Man schreibt $f \restriction M'$ oder $f \mid_{M'}$.

[1] Der Österreicher sagt auch g Knödel f

Definition 1.3.9: Umkehrfunktion

Gegeben sei die injektive Funktion $f : M \to L$, so lässt sich die Funktion $g : f[A] \to A$ so definieren, dass für alle $l \in f[M]$ und $m \in M$ die Gleichung $g(l) = m$ genau dann gilt, wenn $f(a) = b$ gilt. So wird g auch als Umkehrfunktion von f bezeichnet und als f^{-1} geschrieben.

Wenn eine Abbildung $f : M \to L$ eine Bijektion ist, so überschneiden sich die Notationen für das Urbild $(f^{-1}[L'])$ mit der Notation des Bildes von L' der Umkehrfunktion f^{-1}. Beide Mengen sind allerdings identisch, weshalb dies unproblematisch ist. Es gilt:

$$\{x \in M : f(x) \in L'\} = \{f^{-1}(y) : y \in L'\}$$

1.4 Boolesche Algebra

Dieser Abschnitt wurde im WiSe 20/21 aufgrund des verkürzten Semesters übersprungen.

1.5 Summen- und Produktzeichen

Definition 1.5.1: Summenzeichen

Das **Summenzeichen** $\sum$ ist eine Möglichkeit um mithilfe eines **Laufindex** i eine Rechnung wiederholt auszuführen und dabei einen Wert x_i zu erhöhen und jedes Zwischenergebnis von einer **untere Summationsgrenze** $k \in \mathbb{N}_0$ bis zu einer **oberen Summationsgrenze** $n \in \mathbb{N}_0$ aufzusummieren.

$$\sum_{i=k}^{n} x_i = x_k + ... + x_n$$

Sei $k > n$, so handelt es sich um die **leere Summe**, welche als 0 definiert ist.

Aus dem **Distributivgesetz** sowie dem **Kommutativgesetz** folgt:

$$\left(\sum_{i=k}^{m} a_i\right) \cdot \left(\sum_{j=h}^{n} b_j\right) = \sum_{i=k}^{m}\sum_{j=h}^{n} (a_i \cdot b_j) = \sum_{j=h}^{n}\sum_{i=k}^{m} (a_i \cdot b_j)$$

$$\sum_{i=k}^{n} (a_i + b_i) = \sum_{i=k}^{n} a_i + \sum_{i=k}^{n} b_i$$

Definition 1.5.2: Produktzeichen

Das **Produktzeichen** $\prod$ verhält sich wie das Summenzeichen, nur multiplikativ statt additiv.

$$\prod_{i=k}^{n} x_i = x_k \cdot ... \cdot x_n$$

Sei $k > n$, so handelt es sich um das **leere Produkt**, welches als 1 definiert ist.

2. Natürliche Zahlen und vollständige Induktion

2.1 Natürliche Zahlen

Definition 2.1.1: Assoziativgesetz

Das **Assoziativgesetz** für die natürlichen Zahlen x, y und z lautet:

$$x + (y + z) = (x + y) + z$$
$$x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

Definition 2.1.2: Kommutativgesetz

Das **Kommutativgesetz** für die natürlichen Zahlen x und y lautet:

$$x + y = y + x$$

Definition 2.1.3: Distributivgesetz

Das **Distributivgesetz** für die natürlichen Zahlen x, y und z lautet:

$$x \cdot (y + z) = x \cdot y + x \cdot z$$
$$y \cdot (x + z) = y \cdot x + y \cdot z$$
$$z \cdot (x + y) = z \cdot x + z \cdot y$$

Definition 2.1.4: Neutrales Element der Addition

Es existiert das **neutrale Element der Addition**:

$$a + 0 = a = 0 + a$$

Definition 2.1.5: Neutrales Element der Multiplikation

Es existiert das **neutrale Element der Multiplikation**:

$$a \cdot 1 = a = 1 \cdot a$$

2.2 Vollständige Induktion

Grundprinzip: Zu beweisen ist, dass eine Aussageform $A(n)$ für alle natürlichen Zahlen n (möglicherweise mit Bedinung, bspw. $n > 3$) gilt.

Zuerst wird der **Induktionsanfang (IA)** gezeigt, also dass die Aussageform für die kleinste zu zeigene Zahl (s) gilt.

Anschließend muss der **Induktionsschritt (IS)** gezeigt werden, also wenn die Aussageform für eine beliebige Zahl n gilt, sie auch für den Nachfolger $n + 1$ gilt.

$$\forall n, s \in \mathbb{N}(n \geq s)\Big(\big(A(s) \wedge \big(A(n) \to A(n+1)\big)\big) \to \big(A(n)\big)\Big)$$

Satz 2.2.1

$$\forall n \in \mathbb{N}\left(\sum_{i=1}^{n} i = \frac{n(n+1)}{2}\right)$$

Für den Fall, dass $k \neq 1$ gilt folgende Gleichung:

$$\forall n, k \in \mathbb{N}\left(\sum_{i=k}^{n} i = \frac{n(n+1) - (k-1)(k)}{2}\right)$$

Satz 2.2.2

$$\forall n \in \mathbb{Z}\Big(3 \mid (n^3 - n)\Big)$$

$$\begin{aligned}
\sum_{i=0}^{n} q^i &= 1 + \sum_{i=1}^{n} q^i, \quad q \in \mathbb{N} \setminus \{1\} \\
&= 1 + q \cdot \sum_{i=1}^{n} q^{i-1} \\
&= 1 + q \cdot \sum_{i=0}^{n-1} q^i \\
&= 1 + q \cdot \sum_{i=0}^{n-1} q^i + q^{n+1} - q^{n+1} \\
&= 1 + q \cdot \left(\sum_{i=0}^{n-1} q^i + q^n \right) - q^{n+1} \\
&= 1 + q \cdot \sum_{i=0}^{n} q^i - q^{n+1}
\end{aligned}$$

$$\begin{aligned}
\sum_{i=0}^{n} q^i &= 1 + q \cdot \sum_{i=0}^{n} q^i - q^{n+1} \qquad \left| - \left(q \cdot \sum_{i=0}^{n} q^i \right) \right. \\
(1-q) \cdot \sum_{i=0}^{n} q^i &= 1 - q^{n+1} \\
q \neq 1 \rightarrow \sum_{i=0}^{n} q^i &= \frac{1 - q^{n+1}}{1 - q}
\end{aligned}$$

Satz 2.2.3: Geometrische Summenformel

$$\sum_{i=0}^{n} q^i = \frac{1 - q^{n+1}}{1 - q}, \quad q \in \mathbb{R} \setminus \{1\}$$

2.2.1 Vollständige Induktion mit mehreren Vorgängern

Die Aussageform $A(n)$ gilt für alle $n \in \mathbb{N}$ gdw. folgende Aussage wahr ist.

$$A(1) \wedge \left(\bigwedge_{i=1}^{n} A(i) \rightarrow A(n+1) \right)$$

Hierbei verhält sich $\bigwedge$ wie das Summen- oder Produktzeichen nur für Konjunktionen, also durch logische Und ($\wedge$) verknüpfte Aussagen:

$$\bigwedge_{i=1}^{n} A(i) \leftrightarrow A(1) \wedge \ldots \wedge A(n)$$

2.2.2 Rekursive Definition

$$
\begin{aligned}
&(1)\ \text{Startwert} && a_1 = 1 = 1! \\
&(2)\ \text{Definition} && a_{n+1} = a_n \cdot (n+1) = (n+1)!
\end{aligned}
$$

$$
\begin{aligned}
\text{für } n = 2: \quad a_{2+1} &= a_2 \cdot (2+1) \\
&= a_{1+1} \cdot (2+1) \\
&= a_1 \cdot (1+1) \cdot (2+1) \\
&= 1 \cdot 2 \cdot 3 \\
&= 6
\end{aligned}
$$

Definition 2.2.1: Fibonacci-Zahlen

$$f_0 = 0 \quad , \quad f_1 = 1$$
$$\forall n \in \mathbb{N} : f_{n+1} = f_{n-1} + f_n$$

Satz 2.2.4

Für alle $n \in \mathbb{N}_0$ gilt:

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

2.3 Peano (Geschke) Axiome

Die Eigenschaften der natürlichen Zahlen lassen sich durch die folgenden Peano Axiome (benannt nach Peano, 1981) ableiten. (Peano hat diese allerdings einschließlich der 0 definiert.)

Definition 2.3.1

(1) $1 \in \mathbb{N}$
(2) $n \in \mathbb{N} \to n' \in \mathbb{N}$
(3) $n \in \mathbb{N} \to n' \neq 1$
(4) $m, n \in \mathbb{N} \to (m' = n' \to m = n)$ (injektiv)
(5) $\big(1 \in S \wedge \forall n \in \mathbb{N}\ (n \in S \to n' \in S)\big) \to \mathbb{N} \subseteq S$

Hierbei steht n' für den Nachfolger von n in den natürlichen Zahlen, also für $n + 1$. Ein Zahlenbereich, der den Pianoaxiomen genügt, wird als Bereich der natrülichen Zahlen $\mathbb{N}$ bezeichnet.

Satz 2.3.1

Jede nichtleere Menge natürlicher Zahlen hat ein kleinstes Element:

$$(M \subseteq \mathbb{N} \wedge M \neq \emptyset) : \exists! x \in M\ \forall y \in M : x \leq y$$

3. Elementare Zahlentheorie

3.1 Relationen

Definition 3.1.1: Relation

Eine Relation R von der Menge L nach M ist eine Teilmenge von $L \times M$, eine Relation R von M ist eine Teilmenge von $M \times M$. Die Elemente von R sind Tupel, man schreibt:

$$(x, y) \in R \leftrightarrow aRb$$

Die **leere Relation** gegeben durch die leere Menge $\emptyset$ ist eine Relation von jeder Menge.

Eine **Funktion** ist eine spezielle Relation. Sei F eine Relation von der Menge L nach der Menge M, dann ist F eine Funktion, genau dann wenn F jedem Element von L genau einem Element von M zuordnet.

$$\begin{aligned} &\forall l \in L\ \exists m \in M\ \Big((l, m) \in F\Big) \\ \wedge\ &\forall l \in L\ \forall m_1, m_2 \in M\ \Big(\big((l, m_1) \in F \wedge (l, m_2) \in F\big) \rightarrow m_1 = m_2\Big) \end{aligned}$$

$$\leftrightarrow$$

$$\forall l \in L\ \exists! m \in M\ \Big((l, m) \in F\Big)$$

Für Relationen auf einer Menge L gilt:

Begriff	Quantoren	Tupel
Reflexivität	$\forall x \in L : xRx$	$x \in L \rightarrow (x, x) \in R$
Irreflexivität	$\forall x \in L : \neg(xRx)$	$x \in L \rightarrow (x, x) \notin R$
Symmetrie	$\forall x, y : xRy \rightarrow yRx$	$(x, y) \in R \rightarrow (y, x) \in R$
Asymmetrie	$\forall x, y : xRy \rightarrow \neg(yRx)$	$(x, y) \in R \rightarrow (y, x) \notin R$
Antisymmetrie	$\forall x, y : xRy \wedge yRx \rightarrow x = y$	$(x, y), (y, x) \in R \rightarrow x = y$
Transitivität	$\forall x, y, z : xRy \wedge yRz \rightarrow xRz$	$(x, y), (y, z) \in R \rightarrow (x, z) \in R$

Definition 3.1.2: Äquivalenzrelation

Eine Relation R auf eine Menge M welche sowohl reflexiv, transitiv als auch symmetrisch ist, heißt Äquivalenzrelation.

Für jedes $x \in M$, wobei gilt $R \subseteq M$, gibt es eine Menge, welche **Äquivalenzklasse** von x genannt wird. Man schreibt:

$$[x]_R = \{y \in M : (x, y) \in R\}$$

Satz 3.1.1

Wenn $R \subseteq M$, dann gilt:

$$\forall x, y \in M : [a]_R \cap [b]_R = \emptyset \text{ xor } [a]_R = [b]_R$$

Letzteres gilt gdw. aRb.

Definition 3.1.3: Partition

Sei M eine Menge, I eine Indexmenge und es gilt:

$$\forall i \in I : K_i \subseteq M$$

Dann ist $P = \{K_i : i \in I\}$ eine Partition von M, wenn:

$$\Big(\forall i, j \in I, i \neq j : K_i \cap K_j = \emptyset\Big) \wedge \Big(\bigcup_{i \in I} K_i = M\Big)$$

Einer Partition $P = \{K_i : i \in I\}$ von M kann man eine Äquivalenzrelation von M zuordnen, deren Äquivalenzklasse die Menge K_i ist:

$$R := \{(x, y) \in M \times M \mid \exists i \in I : x, y \in K_i\}$$

Daraus folgt, dass zwei Elemente $x, y \in M$ äquivalent sind, wenn diese in der gleichen Menge K_i sind.

Satz 3.1.2

Für jede Äquivalenzrelation auf die Menge M bilden die Äquivalenzklassen eine Partition von M. Außerdem gibt es für jede Partition von M eine Äquivalenzrelation, deren Äquivalenzklassen die Menge in der Partition sind.

Definition 3.1.4: Ordnungsrelationen

Eine Relation R auf eine Menge M welche sowohl reflexiv, transitiv als auch antisymmetrisch ist, heißt **Ordnungsrelation** oder auch Halbordnung bzw. partielle Ordnung. Das Tupel (M, R) ist eine partiell- bzw. halbgeordnete Menge.

Verwendet wird oftmals $\leqslant$ als Zeichen, wobei $x \leqslant y$ eine abkürzende Schreibweise für $(x, y) \in \leqslant$ ist. Dies meint aber nicht zwangsläufig die bekannte "kleinergleich"-Relation.

Definition 3.1.5: Lineare Ordnung

Eine **lineare Ordnung** (auch totale Ordnung) ist eine Ordnungsrelationen R auf einer Menge M für die gilt:

$$\forall x, y \in M, x \neq y : xRy \text{ xor } yRx$$

3.2 Ganze und rationale Zahlen

Die Menge der **ganzen Zahlen** ist definiert als $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, hinzu kommt die Menge der **raitonalen Zahlen** als Menge aller Brüche ganzer Zahlen, welche definiert ist als $\mathbb{Q} = \{\frac{m}{n} : m, n \in \mathbb{Z},\ n \neq 0\}$.

3.2.1 Bruchrechnung

Addition

$$\frac{x}{y} + \frac{x'}{y'} = \frac{x \cdot y'}{y \cdot y'} + \frac{x' \cdot y}{y' \cdot y} = \frac{x \cdot y' + x' \cdot y}{y \cdot y' + y' \cdot y}$$

Multiplikation

$$\frac{x}{y} \cdot \frac{x'}{y'} = \frac{x \cdot x'}{y \cdot y'}$$

Division

$$\frac{x}{y} \div \frac{x'}{y'} = \frac{x}{y} \cdot \frac{y'}{x'} = \frac{x \cdot y'}{y \cdot x'}$$

3.2.2 Ordnungsrelationen der rationalen Zahlen

Für alle $x, y, z \in \mathbb{Q}$ gilt:

(1)	$x < y \wedge y < z$	$\to x < z$	(Transitivität)
(2)	$x < y$	$\to x + z < y + z$	(Monotonie)
(3)	$x < y$	$\to x \cdot z < y \cdot z,$ für $z > 0$	
(4)	$x < y$	$\to x \cdot z > y \cdot z,$ für $z < 0$	
(5)	$x \leq y \wedge y \leq z$	$\to x \leq z$	(Transitivität)
(6)	$x \leq y$	$\to x + z \leq y + z$	(Monotonie)
(7)	$x \leq y$	$\to x \cdot z \leq y \cdot z,$ für $z > 0$	
(8)	$x \leq y$	$\to x \cdot z \leq y \cdot z,$ für $z < 0$	

3.3 Körper

Definition 3.3.1: Körper

Ein **Körper** ist eine Menge über die folgende Abbildungen definiert sind:

$$+ : K \times K \to K$$
$$\cdot : K \times K \to K$$

und die Körperaxiome (K1) bis (K5) erfüllt sind.

Per Definition bilden daher zwar die rationalen und die reellen Zahlen Körper, die natürlichen und ganzen Zahlen aber nicht.

Für die rationalen bzw. reellen Zahlen schreibt man daher

$$K_{\mathbb{Q}} = (\mathbb{Q}, +, \cdot, 0, 1)$$
$$K_{\mathbb{R}} = (\mathbb{R}, +, \cdot, 0, 1)$$

3.3.1 Körperaxiome

(K1): Assoziativgesetze:

$$x + (y + z) = (x + y) + z$$
$$x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

(K2): Kommutativgesetze

$$x + y = y + x$$
$$x \cdot y = y \cdot x$$

(K3): Distributivgesetze

$$x \cdot (x + z) = xa \cdot y + x \cdot z$$

(K4): Neutrale Elemente

$$x + 0 = x$$
$$x \cdot 1 = x$$

(K5): Inverse Elemente

$$x + (-x) = 0$$
$$x \cdot x^{-1} = 1, \ x \neq 0$$

3.4 Reelle Zahlen

Satz 3.4.1

Für alle $x \in \mathbb{Z}$ gilt, ist das Quadrat von x gerade, so ist auch x gerade:

$$\forall x \in \mathbb{Z} : 2 \mid m^2 \to 2 \mid m$$

Satz 3.4.2: Wurzel von 2

Es gibt keine rationale Zahl x mit $x^2 = 2$, bzw. ist $\sqrt{2}$ nicht rational.

3.5 Abzählbarkeit von $\mathbb{Q}$ und $\mathbb{R}$

Definition 3.5.1: Gleichmächtigkeit

Seien die Mengen L und M gleichmächtig, so gibt es eine Bijektion f der Form:

$$f : L \to M$$

Definition 3.5.2: Abzählbar und Überabzählbar

Eine Menge M heißt **abzählbar**, gdw. sie endlich ist oder wenn es eine **Bijektion** von den natürlichen Zahlen auf die Menge M gibt:

$$\mathbb{N} \to M$$

Ist eine Menge M unendlich aber abzählbar, so ist M abzählbar unendlich.

Eine Menge, welche nicht abzählbar ist, wird **überabzählbar** oder überabzählbar unendlich genannt.

Eine **surjektive Abbildung** von $\mathbb{N}$ auf eine Menge M heißt **Aufzählung** von M.

Satz 3.5.1: Abzählbarkeit der ganzen und rationalen Zahlen

Die Menge der ganzen Zahlen $\mathbb{Z}$ ist abzählbar (unendlich), ebenso wie die Menge der rationalen Zahlen $\mathbb{Q}$ abzählbar (unendlich) ist.

Aufzählung von $\mathbb{Z}$:

$$\mathbb{Z} = \{f(1), f(2), f(3), \ldots\} = \{\underbrace{0}_{1}, \underbrace{1}_{2}, \underbrace{-1}_{3}, \underbrace{2}_{4}, \underbrace{-2}_{5}, \ldots\}$$

Die Aufzählung von $\mathbb{Q}$ erfolgt auf einem ähnlichen Prinzip, Bilder dazu finden sich schnell im Internet oder im Skript auf Seite 32 (Satz 3.20).

Satz 3.5.2: Überabzählbarkeit der reellen Zahlen

Die Menge der reellen Zahlen $\mathbb{R}$ ist überabzählbar (unendlich).

Beweis durch Widerspruch:

Angenommen, wir könnten alle reellen Zahlen zwischen 0 und 1 aufzählen, so könnten wir eine bijektive Abbildung zwischen den natürlichen Zahlen und den reellen Zahlen aufstellen. Folglich müssten wir eine Menge M definieren, welche alle reellen Zahlen zwischen 0 und 1 durch als Elemente enthält: $M = \{s_1, s_2, s_3, \ldots\}$.

M könnten wir wie folgt definieren:

$_i{}^j$		s_{i1}	s_{i2}	s_{i3}	$\cdots$
s_{1j}	0.	s_{11}	s_{12}	s_{13}	$\cdots$
s_{2j}	0.	s_{21}	s_{22}	s_{23}	$\cdots$
s_{3j}	0.	s_{31}	s_{32}	s_{33}	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Dabei sind S_{ij} Ziffern aus der Menge $0, 1, 2, \ldots, 9$.

So lässt sich eine Zahl a mit folgender Form definieren:

$$a = 0.a_1a_2a_3\ldots$$

Wobei $a_i \in \{0, 1, 2, \ldots, 9\}$ gilt. Weiter definieren wir:

$$a_i := \begin{cases} 1, & \text{wenn } s_{ii} \neq 1 \\ 2, & \text{sonst} \end{cases}$$

Durch die Definition von a lassen dich unabhängig von den Elementen von M neue reelle Zahlen zwischen 0 und 1 definieren, welche noch kein Element von M sind. Dies steht im Widerspruch, dazu das M bereits alle reellen Zahlen zwischen 0 und 1 enthält. □

3.6 Teilbarkeitsrelation und Primzahlen

3.6.1 Teilbarkeit

Definition 3.6.1: Teilbarkeit

Die Teilbarkeit drückt aus, dass eine ganze Zahl durch eine andere ohne Rest geteilt wird. Man schreibt:

$$x \mid y \leftrightarrow x \cdot q = y,\ q \in \mathbb{Z}$$

$x \mid y$ wird als x teilt y gelesen.

Satz 3.6.1: Eigenschaften der Teilbarkeitsrelation

$$\begin{array}{lll}
(1) & x \mid x \wedge y \mid z & \rightarrow \quad x \mid z \\
(2) & x_1 \mid y_1 \wedge x_2 \mid y_2 & \rightarrow \quad x_1 \cdot x_2 \mid y_1 \cdot y_2 \\
(3) & x \cdot y \mid x \cdot c \wedge x \neq 0 & \rightarrow \quad y \mid z \\
(4) & x \mid y_1 \wedge x \mid y_2 & \rightarrow \quad \forall z_1, z_2 \in \mathbb{Z} : x \mid y_1 \cdot z_1 + y_2 \cdot z_2
\end{array}$$

$$x \mid y \ \leftrightarrow \ -x \mid y \ \leftrightarrow \ -x \mid -y \ \leftrightarrow \ x \mid -y$$

$$\forall x \in \mathbb{Z} : x \mid 0$$

$$\forall x \neq 0 \in \mathbb{Z} : 0 \not\mid x$$

3.6.2 Primzahlen

Definition 3.6.2: Primzahlen

Sei n eine natürliche Zahl mit $n \geq 2$, welche sich nur von ihren **trivialen Teilern** teilen, so ist n eine Primzahl.

Satz 3.6.2: Der Satz von Euklid

Es gibt unendlich viele Primzahlen.

Satz 3.6.3

Jede natürliche Zahl $n \geq 2$ lässt sich als Produkt von Primzahlpotenzen der Form $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots p_k^{\alpha_k}$ darstellen. Dabei ist k eine natürliche Zahl ≥ 1 und alle Primzahlen $p_1, p_2, \ldots, p_k$ sind voneinander verschieden. $\alpha_1, \alpha_2, \ldots \alpha_k$ sind ebenfalls natürliche Zahlen.

Zudem gilt, dass bis auf die Reihenfolge der Faktoren die Produktdarstellung von n eindeutig ist.

Satz 3.6.4

$$p \mid x \cdot y \quad \rightarrow \quad p \mid x \vee p \mid y, \qquad y \in \mathbb{N}, p \in \mathcal{P}$$

Dabei sei $\mathcal{P}$ die Menge aller Primzahlen.

3.7 Größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches

Definition 3.7.1: Größter gemeinsamer Teiler (ggT)

Der größte gemeinsame Teiler von zwei natürlichen Zahlen x und y ist die größte natürliche Zahl z, welche sowohl x als y teilt. Dafür schreibt man:

$$\text{ggT}(x, y) = z$$

Wird der größte gemeinsame Teiler von zwei Zahlen gesucht, so kann man wie folgt vorgehen:

$$x = 12 = 2^2 \cdot 3, \quad y = 18 = 2 \cdot 3^2$$
$$\text{ggT}(12, 18) = 2 \cdot 3 = 6$$

Man schreibt die Zahlen in ihrer Primfaktorenzerlegung auf und multipliziert alle Primzahlen, welche sowohl in der Primfaktorzerlegung der einen Zahl als auch in der Zerlegung der anderen Zahl vorkommen, mit dem jeweils kleinsten Exponten, dann ist das Produkt der ggT von beiden Zahlen.

Definition 3.7.2: Kleinstes gemeinsames Vielfaches (kgV)

Das kleinste gemeinsame Vielfache von zwei natürlichen Zahlen x und y ist die kleinste natürliche Zahl z, für die gilt: $x \mid z$ und $y \mid z$. Dafür schreibt man:

$$\text{kgV}(x, y) = z$$

Wird das kleinste gemeinsame Vielfache von zwei Zahlen gesucht, so kann man wie folgt vorgehen:

$$x = 12 = 2^2 \cdot 3, \quad y = 18 = 2 \cdot 3^2$$
$$\text{kgV}(12, 18) = 2^2 \cdot 3^2 = 36$$

Man schreibt die Zahlen in ihrer Primfaktorenzerlegung auf und multipliziert alle Primzahlen mit dem jeweils größten Exponten, dann ist das Produkt das kgV von beiden Zahlen.

Da im ggT nur die kleinsten Primzahlpotenzen und in kgV die höchsten Primzahlpotenzen vorkommen, ergibt sich:

$$\text{ggT}(x, y) \cdot \text{kgV}(x, y) = x \cdot y$$

Definition 3.7.3: Absolutbetrag

$$\forall x \in \mathbb{R} : |x| = \begin{cases} x, & \text{wenn } x \geq 0 \\ -x, & \text{wenn } x < 0 \end{cases}$$

$$\forall x, y \in \mathbb{Z} \setminus \{0\} :$$
$$\text{kgV}(x, y) = \text{kgV}(|x|, |y|)$$
$$\text{ggT}(x, y) = \text{ggT}(|x|, |y|)$$

Satz 3.7.1: Division mit Rest

$$\forall m \in \mathbb{Z},\ n \in \mathbb{N}, q, r \in \mathbb{Z} : (0 \leq r < n) \wedge (m = q \cdot n + r)$$
$$m = (m \text{ div } n) \cdot n + (m \text{ mod } n)$$

Ganzzahl Division: $q = m \text{div} n$
Modulo: $r = m \mod n$

Seien $m, n \in \mathbb{N}_0,\ m > n$;
(1) Falls $n = 0$; gib m als größten gemeinsamen Teiler aus
(2) Falls $n \neq 0$; bestimme q und r mit $0 \leq r < n$ und $m = q \cdot n + r$
(3) Setze $m := n$ und $n := r$; gehe zurück zu (1)

```java
public int ggT(int m, int n) {
    int r;
    while(n != 0) {
        r = m % n;
        m = n;
        n = r;
    }
    return m;
}

java.lang.System.out.print(ggT(70, 60)); // 10
```

3.8 Modulare Arithmetik

Definition 3.8.1: Kongruenz

Seien $x, y \in \mathbb{Z}$ und $m \in \mathbb{N}$, so sind diese kongruent modulo m, falls a und b den gleichen Divisionsrest haben. Man schreibt:

$$\begin{aligned}\big(x \equiv y \pmod m\big) &\leftrightarrow (x \bmod m = y \bmod m) \\ &\leftrightarrow \big((m \mid x - y) \leftrightarrow (m \mid y - x)\big)\end{aligned}$$

$$\begin{aligned}x - y &= (q_x \cdot m + r_x) - (q_y \cdot m + r_y) \\ &= (q_x - q_y) \cdot m + (r_x - r_y)\end{aligned}$$

Des weiteren gelten folgende Aussagen für $x, y, z, w \in \mathbb{Z}$:

(1) $x \equiv x \pmod m$
(2) $x \equiv y \pmod m \to y \equiv x \pmod m$
(3) $x \equiv y \pmod m \wedge y \equiv z \pmod m \to x \equiv z \pmod m$
(4) $x \equiv y \pmod m \to -x \equiv -y \pmod m$
(5) $x \equiv y \pmod m \wedge z \equiv w \pmod m \to x + z \equiv y + w \pmod m$
(6) $\mathrm{ggT}(z, m) = 1 \to \big(z \cdot x \equiv z \cdot y \pmod m \to x \equiv y \pmod m\big)$

Definition 3.8.2: Restklassen

Für alle $m \in \mathbb{N}$ und $x \in \mathbb{Z}$ ist die **Restklasse** von a mod m definiert als

$$[x]_m := \{y \in \mathbb{Z} : y \bmod m = x \bmod m\}$$

Für alle $m \in \mathbb{N}$ gibt es genau m verschiedene Restklassen modulo m, welche **paarweise disjunkt** sind. Die Restklassen modulo m bilden eine Partition von $\mathbb{Z}$, da ihre Vereinigung die Menge $\mathbb{Z}$ bildet und sie paarweise disjunkt sind.

Definition 3.8.3: Gaußklammern

Die Gaußklammern dienen zum gezielten Runden von (reellen) Zahlen, dabei meint die untere Gaußklammer $\lfloor x \rfloor$ die größte ganze Zahl kleiner gleich x und die obere Gaußklammer $\lceil x \rceil$ die kleinste ganze Zahl größer gleich x:

$$\begin{aligned}\lfloor x \rfloor \leq x,\ \lfloor x \rfloor \in \mathbb{Z} \\ \lceil x \rceil \geq x,\ \lceil x \rceil \in \mathbb{Z}\end{aligned}$$

4. Elementare Kombinatorik

4.1 Fakultät, Faktorielle, Binomialkoeffizienten

Definition 4.1.1: Mächtigkeit

Die **Mächtigkeit** einer Menge M (geschrieben: $|M|$) gibt die Anzahl der Elemente der Menge M an.

Satz 4.1.1: Mächtigkeitsregeln

Die **Additionsregel** besagt, dass für eine endliche Menge M mit disjunkten Teilmengen $M_1, \ldots, M_n$ mit $M = \bigcup_{i=1}^{n} M_i$ gilt:

$$|M| = \sum_{i=1}^{n} |M_i|$$

Die **Multiplikationsregel** besagt, dass für endliche Mengen $M_1, \ldots, M_n$ folgendes gilt:

$$|M_1 \times \ldots \times M_n| = |M_1| \cdot \ldots \cdot |M_n| = \prod_{i=1}^{n} = |M_i|$$

Die **Gleichheitsregel** besagt, dass für zwei endliche Mengen L und M gilt: Gdw. es eine Bijektion $f : L \to M$ gibt, gilt $|L| = |M|$.

Definition 4.1.2: Mengenpotenzen

Sei M eine beliebige Menge, so meint M^n die Menge aller n-Tupel, welche sich aus den Elementen der Menge M erstellen lassen. Dabei ist $M^0 := \{\emptyset\}$.

Grundaufgabe 1 - Ziehen mit Zurücklegen und mit Berücksichtigung der Reihenfolge:

Wieviele verschiedene k-Tupel lassen sich aus einer n-elementigen Menge bilden? Dabei seien $n, k \in \mathbb{N}_0$.

Aus der Multiplikationsregel ergibt sich n^k.

Grundaufgabe 2 - Ziehen ohne Zurücklegen und mit Berücksichtigung der Reihenfolge:

Wieviele verschiedene k-Tupel, wobei in keinem Tupel ein Element doppelt vorkommt, lassen sich aus einer n-elementigen Menge bilden? Dabei seien $n, k \in \mathbb{N}_0$.

Aus der Multiplikationsregel für $k \geq 1$ ergibt sich $n \cdot (n-1) \cdot \ldots \cdot (n-(k-1))$ und 1 für $k = 0$. Für den Fall $k = n$ kann man stattdessen auch $k!$ schreiben.

Definition 4.1.3: Fallende Faktorielle

$$n^{\underline{k}} = \begin{cases} n \cdot (n-1) \cdot \ldots \cdot (n-k+1), & \text{falls } k \geq 1 \\ 1, & \text{sonst} \end{cases}$$

Definition 4.1.4: Permutationen

Eine Permutation ist eine bijektive Abbildung π von einer Menge M auf sich selbst:

$$\pi : M \to M$$

Ist die Menge M paarweise verschieden und beträgt ihre Mächtigkeit n, so kann die Permutation π wie folgt notiert werden:

$$\pi = \begin{pmatrix} m_1 & m_2 & \cdots & m_n \\ \pi(m_1) & \pi(m_2) & \cdots & \pi(m_n) \end{pmatrix}$$

Definition 4.1.5: Fakultät

Die Fakultät einer Zahl n (geschrieben $n!$) ist definiert als das fallende Faktorielle $n^{\underline{n}}$.

$n!$ gibt die Anzahl an Möglichkeiten n Objekte anzuordnen

Grundaufgabe 3 - Ziehen ohne Zurücklegen und ohne Berücksichtigung der Reihenfolge:

Wieviele verschiedene k-elementige Teilmengen einer n-elementigen Menge M gibt es? Dabei sei $0 \leq k \leq n$.

Die Antwort lässt sich aus Grundaufgabe 2 herleiten, indem wir aus jedem k-Tupel $(m_1, \ldots, m_k)$ eine k-elementige Menge $\{m_1, \ldots, m_k\}$ bilden. Da bei Mengen die Reihenfolge keine Rolle spielt, haben wir weniger unterschiedliche k-elementige Mengen als k-Tupel; für jede dieser Mengen gibt es $k!$ k-Tupel, welche die gleichen Elemente haben und die in der Berechnung gekürzt werden müssen. Daraus folgt als Lösung:

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

Definition 4.1.6: Binomialkoeffizient

Man nennt $\frac{n^{\underline{k}}}{k!} = \binom{n}{k}$ einen **Binomialkoeffizienten** für $n, k \in \mathbb{N}_0$ mit $0 \leq k \leq n$.

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

Satz 4.1.2

$$\forall n, k \in \mathbb{N},\ n \geq 2,\ 1 \leq k \leq n-1 : \binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

$$\begin{array}{ccccccccccccc}
 & & & & \binom{0}{0} & & & & & & & & \\
 & & & \binom{1}{0} & & \binom{1}{1} & & & & & & & \\
 & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & & & \\
 & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & & & & \\
\binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & & & & \\
\ddots & & & & \vdots & & & & & & \ddots & &
\end{array}$$

Pascalsches Dreieck:

$$\begin{array}{ccccccccccccc}
 & & & & 1 & & & & & & & & \\
 & & & 1 & & 1 & & & & & & & \\
 & & 1 & & 2 & & 1 & & & & & & \\
 & 1 & & 3 & & 3 & & 1 & & & & & \\
1 & & 4 & & 6 & & 4 & & 1 & & & & \\
\ddots & & & & \vdots & & & & & & \ddots & &
\end{array}$$

Satz 4.1.3: Binomischer Lehrsatz

$$\forall n \in \mathbb{N}_0 : (a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i = a^n + \binom{n}{1} a^{n-1} b + \ldots + b^n,\ a, b \in \mathbb{R}$$

Satz 4.1.4

$$\forall n \in \mathbb{N}_0 : 2^n = \sum_{i=0}^{n} \binom{n}{i}$$

$$\forall n, k \in \mathbb{N}_0,\ n \geq k : \binom{n}{k} = \binom{n}{n-k}$$

Grundaufgabe 4 - Ziehen mit Zurücklegen und ohne Berücksichtigung der Reihenfolge:

Wieviele verschiedene Möglichkeiten gibt es, k ununterscheidbare Kugeln auf n Gefäße $K_1, \ldots, K_n$ zu verteilen? Dabei sei $n \in \mathbb{N}$ und $k \in \mathbb{N}_0$.

Die Antwort ist $\binom{k+n-1}{k} = \binom{k+n-1}{n-1}$ Möglichkeiten.

Grundaufgabe 5:

Wie viele verschiedene n-lange Zeichenfolgen lassen sich aus den Zeichen $Z_1, \ldots, Z_r$ mit einer jeweiligen Zeichenhäufigkeit $n_1, \ldots, n_r$ bilden? Dabei seien $r, n \in \mathbb{N}$.

Die Antwort ist $\frac{(n_1+\ldots+n_r)!}{n_1!\cdot\ldots\cdot n_r!} = \frac{n!}{n_1!\cdot\ldots\cdot n_r!}$, sodass jedes Zeichen Z_i mit $i \in \{1, \ldots, r\}$ genau n_i-mal vorkommt.

Definition 4.1.7: Multinomialkoeffizient

Seien $n_1, \ldots, n_r \in \mathbb{N}_0$ mit $n = n_1 + \ldots + n_r$. Dann nennt man

$$\binom{n}{n_1, \ldots, n_r} = \frac{n!}{n_1! \cdot \ldots \cdot n_r!}, \; r \geq 2$$

einen Multinomialkoeffizienten.

Satz 4.1.5: Ziehen von Elementen einer Menge

Ziehen mit Zurücklegen und mit Berücksichtigung der Reihenfolge:

$$n^k$$

Ziehen ohne Zurücklegen und mit Berücksichtigung der Reihenfolge:

$$n^{\underline{k}} = \frac{n!}{(n-k)!} = \begin{cases} n \cdot (n-1) \cdot \ldots \cdot (n-k+1), & \text{falls } k \geq 1 \\ 1, & \text{sonst} \end{cases}$$

Ziehen ohne Zurücklegen und ohne Berücksichtigung der Reihenfolge:

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

Ziehen mit Zurücklegen und ohne Berücksichtigung der Reihenfolge:

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

Satz 4.1.6: Multinomialsatz

$$\forall x_1, \ldots, x_r \in \mathbb{R} : (x_1 + \ldots + x_r)^n = \sum_{x_1+\ldots+x_r=n} \binom{n}{x_1, \ldots, x_r} \cdot x_1^{n_1} \cdot \ldots \cdot x_r^{n_r}$$

Satz 4.1.7: Schubfachprinzip

Wenn m Objekte auf n Fächer verteilt werden, so gibt es mindestens ein Fach mit mindestens $\lceil \frac{m}{n} \rceil$ Objekten, wobei $m, n \in \mathbb{N}$.
Ist $m > n$, so gibt es mindestens ein Fach mit mindestens zwei Objekten. Es gibt also eine injektive Abbildung $f : \{1, \ldots, m\} \to \{1, \ldots, n\}$ mit $n, m \in \mathbb{N}$.

Satz 4.1.8

Für Teilmengen $M_1, \ldots, M_n$ mit $n \in \mathbb{N}$ und $M = \bigcup_{i=1}^{n} M_i$ eine unendliche Menge, so ist eine der Teilmengen M_i ebenfalls unendlich.

4.2 Inklusion und Exklusion (Siebformel)

Satz 4.2.1: Siebformel

Seien $A_1, \ldots, A_n$ mit $n \in \mathbb{N}$ endliche Mengen, so gilt:

$$|A_1 \cup \ldots \cup A_n| = \sum_{k=1}^{n} \left((-1)^{k-1} \cdot \sum_{i \leq n_1 < \ldots < n_k \leq n} |A_{n_1} \cap \ldots \cap A_{n_k}| \right)$$

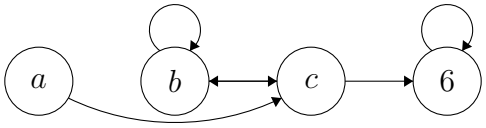
Satz 4.2.2

Jede nichtleere endliche Menge M hat genauso viele Teilmengen gerader Mächtigkeit wie ungerader.

4.3 Graphen von Relationen

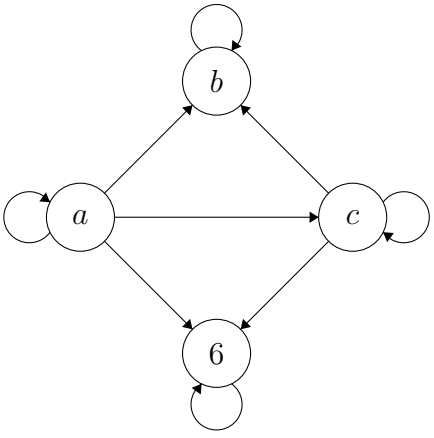
Relationen können in Form von **gerichteten Graphen** graphisch dargestellt werden. Hierbei wird jedes Element von M durch einen mit dem Element beschrifteten **Knoten** als Punkt oder Kreis dargestellt und jedes Paar (x, y) mit $x, y \in M$ der Relation R durch eine **gerichtete Kante**, also einen Pfeil von x nach y dargestellt. Eine Kante von einem Knoten auf sich selbst nennt man auch **Schlinge**.

Der gerichtete Graph (M, R), gebildet aus der Menge $M = \{a, b, c, 6\}$ und der Relation $R = \{(a, c), (b, b), (b, c), (c, b), (c, 6), (6, 6)\}$ würde wie folgt aussehen:

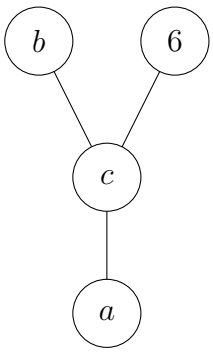


(1) R ist reflexiv, wenn jeder Knoten im gerichteten Graphen eine Schlinge hat
(2) R ist irreflexiv, wenn das für keinen Knoten gilt
(3) R ist symmetrisch, wenn es für jede gerichtete Kante x nach y auch eine gerichtete Kante von x nach y gibt
(4) R ist antisymmetrisch, wenn für zwei verschiedene Knoten maximal eine gerichtete Kante zwischen diesen existiert
(5) R ist transitiv, wenn für alle Knoten x, y, z gilt, dass wenn es eine gerichtete Kante von x nach y und eine gerichtete Kante y nach z gibt, so gibt es auch eine gerichtete Kante von x nach z.

Für die Darstellungen von **Ordnungsrelationen** (also Relationen, welche Reflexiv, Transitiv und Antisymmetrisch sind) gibt es zusätzlich zur obigen auch eine simplifizierte Darstellung, sogenannte **Hassediagramme**. Hierbei werden Schlingen sowie Kanten, die sich aus der Transitivität ergeben, weggelassen. Außerdem werden Kanten nicht gerichtet dargestellt, da alle Kanten nur in eine Richtung zeigen können (Antisymmetrie) und per Vereinbarung daher immer nach oben (auch diagonal) gezeichnet werden:



a) gerichteter Graph



b) Hassediagramm

4.4 Hüllenbildungen

Definition 4.4.1: Reflexive Hülle

Sei R eine Relation auf einer Menge M. So ist

$$R' := R \cup \{(x, x) : x \in M\}$$

die reflexive Hülle von R und die kleineste reflexive Relation für die gilt, dass $R \subseteq R'$.

Definition 4.4.2: Transitive Hülle

Sei R eine Relation auf einer Menge M. so ist

$$\begin{aligned} R^+ := R \cup \{\ (x, y) : \exists n \geq 2 \wedge x_1, \ldots, x_n \in M \\ \text{mit} \quad x = x_1,\ y = x_n \\ \wedge\, (x_1, x_2), \ldots, (x_{n-1}, x_n) \in R\} \end{aligned}$$

die transitive Hülle von R und die kleinste transitive Relation für die gilt, dass $R \subseteq R^+$.

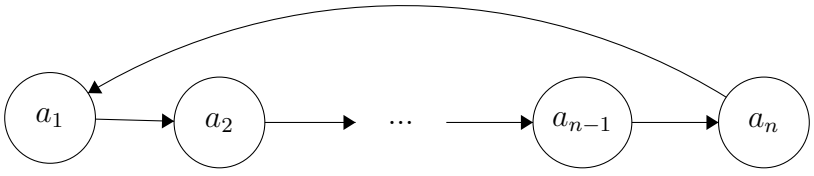
Definition 4.4.3: Reflexive transitive Hüllenbildungen

Sei R eine Relation auf eine Menge M. So ist

$$R^* := R^+ \cup R'$$

die reflexive, transitive Hülle von R und die kleinste reflexive, transitive Relation für die gilt, dass $R \subseteq R^*$.

Eine reflexive, transitive Relation heißt **Quasiordnung**. Weiter ist R^* eine Ordnungsrelation, gdw. es in R keine Schleifen über mindestens zwei Knoten, also der folgenden Art (für $n \geq 2$) gibt:



Definition 4.4.4: Mehrstellige Relationen

Seien $M_1, \ldots, M_n$ Mengen mit $n \geq 1$, so ist eine n-Stellige Relation über die Mengen $M_1, \ldots, M_n$ eine Teilmenge des kartesischen Produkts der Mengen $M_1, \ldots, M_n$:

$$M_1 \times, \cdots, M_n = \{(m_1, \ldots, m_n) : m_1 \in M_1 \wedge, \cdots, \wedge m_n \in M_n\}$$

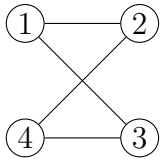
5. Graphentheorie

5.1 Grundlegende Definitionen

Definition 5.1.1: Ungerichteter Graph

Ein ungerichteter Graph $G = (V, E)$ ist ein Paar aus der Menge V der Ecken und E der Kanten, wobei $V(G)$ die Ecken von G und $E(G)$ die Kanten von G meint. Im Rahmen der Vorlesung ist die Menge der Ecken V als endlich definiert.
In einem ungerichteten Graphen sind Kanten nicht gerichtet (Mengen, statt Paare); dies bedeutet, dass es auch keine Schleifen geben kann, da eine Menge keine Doppelungen haben kann.

$$
\begin{aligned}
G &= (V, E) \\
V &= \{1, 2, 3, 4\} \\
E &= \{\{1, 2\}, \{1, 3\}, \{2, 4\}, \{3, 4\}\}
\end{aligned}
$$



Satz 5.1.1: Vollständiger Graph

Ein Graph heißt vollständig, wenn es zwischen je zwei verschiedenen Ecken in V eine Kante gibt. Ein vollständiger Graph muss also $\binom{|V|}{2}$ Kanten haben.
Für jede Eckenanzahl $n \in \mathbb{N}$ mit der Eckenmenge $\{1, 2, \ldots, n\}$ hat genau einen vollständigen Graphen, dieser wird mit K_n bezeichnet.

Satz 5.1.2: Weglänge

Ein Weg der Länge $n \in \mathbb{N}_0$ ist ein ununterbrochener Pfad durch $n + 1$ verschiedene Ecken.

Ein wichtiger Unterschied ist, ob ein Graph G ein Weg ist, oder ob es einen Teilgraph $G' \neq G$ von G gibt, welcher ein Weg ist, denn dann ist G nicht automatisch ein Weg, sondern hat einen Weg.

Satz 5.1.3: Kreise

Man nennt einen (Teil-)Graphen mit $n \in \mathbb{N} \setminus \{1, 2\}$ Ecken einen Kreis der Länge n, wenn es einen Weg durch $n - 1$ verschiedene Ecken gibt und eine weitere Kante vom Wegende zum Weganfang existiert.

Definition 5.1.2: Teilgraph

Ein Graph G' heißt Teilgraph, für einen Graphen G (geschrieben $G' \subseteq G$), falls:

$$\begin{aligned} V(G') &\subseteq V(G) \text{ und} \\ E(G') &\subseteq E(G) \end{aligned}$$

Definition 5.1.3: Zusammenhängender Graph

Wenn es für zwei verschiedene Knoten $v, w \in V(G)$ eines Graphen G einen Weg gibt, der bei v anfängt und bei w aufhört, so heißt G zusammenhängender Graph.

Definition 5.1.4: Zusammenhangskomponente

Sei G' ein zusammenhängender Teilgraph des Graphen G, so heißt G' Zusammenhangskomponente von G, wenn es keinen anderen Teilgraphen F von G mit $G' \neq F$ gibt, für den gilt: $G' \subseteq F$.

Man schreibt $c(G)$ für die Anzahl der Zusammenhangskomponenten des Graphen G.

Definition 5.1.5: Baum

Sei G ein zusammenhängender Graph. Man nennt G einen Baum, falls G keine Kreise enthält.

Definition 5.1.6: Grad

Sei G ein Graph und $v \in V(G)$ eine Ecke. Der Grad von v (geschrieben $d(v)$) ist die Anzahl der Kanten von v und anderen Ecken.

Satz 5.1.4: Handshake Lemma

Sei G ein Graph mit $V(G) = \{v_1, \ldots, v_n\}$, wobei alle v_i paarweise verschieden sind. Es gilt, dass die Summe der Grade aller v_i die doppelte Mächtigkeit von $E(G)$ ist:

$$\sum_{i=1}^{n} d(v_i) = 2 \cdot |E(G)|$$

Satz 5.1.5

In einem Graphen ist die Anzahl der Ecken von ungeradem Grad immer gerade.

Definition 5.1.7: Endknoten

Eine Ecke v eines Graphen G mit $d(v) = 1$ nennt man Endknoten.

Satz 5.1.6

Ein Baum mit mindestens zwei Ecken hat auch mindestens zwei Endknoten.

Satz 5.1.7

Ein Baum mit n Ecken hat genau $n - 1$ Kanten.

Definition 5.1.8: Isomorphismus

Zwei Graphen G und H, mit einer Bijektion $f : V(G) \to V(H)$, der Form:

$$\forall x, y \in V(G), x \neq y : \quad \{x, y\} \in E(G) \leftrightarrow \{f(x), f(y)\} \in E(H)$$

heißen isomorph und die Bijektion, welche obige Bedingung erfüllt heißt Isomorphismus.

Damit zwei Graphen isomorph sind, müssen sie dieselbe Anzahl an Ecken und Kanten haben. Ferner müssen isomorphe Graphen gleich viele Ecken mit jeweils demselben Grad haben.

Weiter sind vollständige Graphen isomorph, wenn sie dieselbe Anzahl an Ecken haben.

Außerdem sind Graphen derselben Länge isomorph, wenn sie Kreise oder Wege sind.

Definition 5.1.9: Komplementgraph

Der Komplementgraph $\overline{G}$ eines Graphen $G = (V, E)$ ist wie folgt definiert:

$$V(\overline{G}) = V(G)$$
$$E(\overline{G}) = \{\{x, y\} : x, y \in V(G),\ x \neq y,\ \{x, y\} \notin E(G)\}$$

Sind zwei Graphen isomorph, so sind auch ihre Komplementgraphen isomorph.

Definition 5.1.10: Gradfolge

Sei $G = (\{v_1, \ldots, v_n\}, E)$ ein Graph mit n Ecken und $d(v_1) \geq \ldots \geq d(v_n)$ so heißt das n-Tupel $(d(v_1), \ldots, d(v_n))$ Gradfolge von G.

Sind zwei Graphen isomorph, so müssen sie dieselbe Gradfolge haben, anders herum müssen zwei Graphen mit derselben Gradfolge aber nicht isomorph sein.

Definition 5.1.11: Multigraph

Ein Multigraph, im Gegensatz zu einem normalen Graphen, ist ein Tripel $G = (V, E, f)$, wobei V weiterhin die Menge von Ecken ist, E die Menge von Kanten (nicht als zweielementige Mengen, sondern als Kantenbezeichnung) und f als Abbildung der Kanten auf die Ecken. Dabei kann jeder Kante eine ein- oder zweielementige Teilmenge von V zugeordnet werden. Die Kanten, denen eine einelementige Teilmenge von V zugeordnet wird, nennt man Schlingen.
Gibt es zwei oder mehr Kanten, denen dieselbe zweielementige Teilmenge von Ecken zugeordnet wurde, so sind diese Mehrfachkanten.
Wenn es für je zwei Ecken eines Multigraphen einen Weg gibt, der diese verbindet, dann heißt der Multigraph zusammenhängend.

Der Grad von einem Knoten eines Mutligraphen wird wie bisher bestimmt, mit dem Unterschied, dass Schlingen doppelt gezählt werden.

Definition 5.1.12: Kantenfolge, Kantenzug und Weg

Sei $G = (V, E, f)$ ein Multigraph und sei $v_0, e_1, v_1, \ldots, v_{l-1}, e_l, v_l$ eine Folge mit $v_i \in V,\ i = 0, \ldots, l$ und $e_i \in E,\ i = 1, \ldots, l$.

(1) Die Folge heißt Kantenfolge der Länge l, falls jedes e_i eine Kante ist, deren Endpunkte die Ecken v_{i-1} und v_i sind.
(2) Eine Kantenfolge, in der keine Kante mehr als einmal vorkommt, nennt man Kantenzug.
(3) Ein Kantenzug, in dem keine Ecke mehr als einmal vorkommt, ist ein Weg von v_0 nach v_l.
(4) Eine Kantenfolge heißt geschlossen, falls $v_0 = v_l$.

5.2 Eulersche Linien und Hamiltonsche Kreise

Definition 5.2.1: Eulersche Linie/Kreis

Ein Kantenzug in einem Multigraph G wird Erulersche Linie oder Eulerscher Kreis genannt, falls er geschlossen ist und alle Kanten von G durchläuft.

Satz 5.2.1

Ein Graph G hat genau dann eine Eulersche Linie, wenn alle Knoten von G geraden Grad sind.

Definition 5.2.2: Hamiltonscher Kreis

Sei C ein Kreis in einem Graphen G, so heißt C ein Hamiltonscher Kreis, wenn C alle Knoten von G enthält.

Satz 5.2.2

Sei G ein Graph mit einem Hamiltonschen Kreis, so gilt:

$$c(G \setminus A) \leq |A|, \quad \forall A \subseteq V(G) : A \neq \emptyset$$

Dabei sei $c(H)$ die Anzahl der Zusammenhangskomponenten von H für einen beliebigen Graphen H.

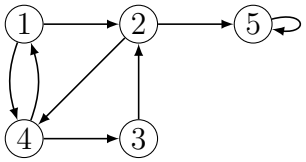
5.3 Gerichtete Graphen

Definition 5.3.1: Gerichteter Graph/Digraph

Ein gerichteter Graph $G = (V, E)$, dabei ist V eine beliebige Menge und E eine Teilmenge von (V^2).
Eine Kante der Form (v, v) mit $v \in V$ heißt Schlinge.
$V(G)$ ist die Eckenmenge des Graphen G und $E(G)$ ist die Kantenmenge.

Ein gerichteter Graph lässt sich auch mithilfe der **Adjazenzmatrix**, oder über (mindestens) eine der beiden **Nachbarschaftslisten** beschreiben:

Graph G



Adjazenzmatrix von G

	v_1	v_2	v_3	v_4	v_5
v_1	0	1	0	1	0
v_2	0	0	0	1	1
v_3	0	1	0	0	0
v_4	1	0	1	0	0
v_5	0	0	0	0	1

$$\rightarrow \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Nachbarschaftslisten:

Nachbarschaftsliste 1 von G

v_1	2	4
v_2	4	5
v_3	2	
v_4	1	3
v_5	5	

Nachbarschaftsliste 2 von G

v_1	4	
v_2	1	3
v_3	4	
v_4	1	2
v_5	2	5

Die **Adjazenzmatrix** wird gebildet, in dem eine 1 in die i-te Zeile und j-te Spalte geschrieben wird, wenn das Paar (v_i, v_j) in $E(G)$ ist.

Die **1. Nachbarschaftsliste** wird gebildet, in dem in die Zeile von V_i alle Knoten geschrieben werden, zu denen von v_i eine Kante führt.

Die **2. Nachbarschaftsliste** wird gebildet, in dem in die Zeile von V_i alle Knoten geschrieben werden, von denen man zu v_i über eine gerichtete Kante kommt.

Definition 5.3.2: Außen- und Innengrad

Der Außengrad (out degree) der Ecke v ($d^+(v)$) eines Graphen G ist die Anzahl der Kanten die von v wegführen.
Der Innengrad (in degree) der Ecke v ($d^-(v)$) eines Graphen G ist die Anzahl der Kanten die zu v hinführen.

Definition 5.3.3: gerichtete Kantenfolge, Kantenzug, Weg, geschlossene Kantenfolge

Für den gerichteten Graphen $G = (V, E)$ ist die Folge:

$$v_0, e_0, v_1, \ldots, v_{\ell-1}, v_\ell, e_\ell$$

mit $v_i \in V \forall i \in \{0, ..., \ell\}$ und $e_i \in E \forall i \in \{1, ..., \ell\}$.

(1) Wenn für alle Kanten e_i der Folge $e_i = (v_{i-1}, v_i)$ gilt, so wird die Folge **Kantenfolge** genannt.

(2) Sind alle Kanten der Kantenfolge paarweise verschieden, so wird sie als **Kantenzug** bezeichnet.

(3) Sind zudem alle Knoten paarweise verschieden, so wird von einem **gerichteten Weg** gesprochen.

(4) Um eine **geschlossene, gerichtete Kantenfolge** handelt es sich, wenn $v_0 = v_\ell$ gilt.

Definition 5.3.4: zugrunde liegender ungerichteter Graph

Zu jedem gerichteten Graphen $G = (V, E)$ gibt es einen, diesem zugrunde liegenden, ungerichteten Graphen G_u mit der Eckenmenge V und der Kantenmenge $E(G_u)$ mit

$$E(G_u) = \big\{\{v, w\} : (v, w) \in E \wedge v \neq w\big\}$$

Definition 5.3.5: schwach und stark zusammenhängend

Gegeben sei der gerichtete Graph G:

(1) Wenn G_u zusammenhängend ist, so ist G **schwach zusammenhängend**.

(2) Wenn für je zwei verschiedene Ecken v und w des Graphen G ein gerichteter Weg von v nach w existiert, so heißt G **stark zusammenhängend**.

(3) Als **schwache Zusammenhangskomponente** bezeichnet man einen Teilgraph $G' \subseteq G$, wenn G' schwach zusammenhängend ist und es keinen echt größeren Teilgraphen $F \subseteq G$ gibt, welcher schwach zusammenhängend ist.

(4) Als **starke Zusammenhangskomponente** bezeichnet man einen Teilgraph $G' \subseteq G$, wenn G' stark zusammenhängend ist und es keinen echt größeren Teilgraphen $F \subseteq G$ gibt, welcher stark zusammenhängend ist.

5.4 Bäume

Aus einem ungerichteten Baum, also ein zusammenhängender Graph ohne Kreise, lässt sich ein gerichteter Graph konstruieren, welcher denselben Baum darstellt indem jede Kante von der Wurzel weggerichtet wird.

Dabei ist der Knoten 0 die **Wurzel (root)** des Baumes. Geht bei diesem gerichteten Graphen eine Kante vom Knoten v zum Knoten w, so wird v **Vater (parent)** und w **Kind (child)** genannt. Jeder Knoten ohne Kind wird **Blatt** genannt. Ein Knoten, welcher kein Blatt ist heißt **innerer Knoten**.

Als **Höhe** des Baumes B wird die maximale Länge eines Weges von der Wurzel zu einem Blatt bezeichnet.

Als **Grad** eines Baumes B wird die maximale Anzahl der Kinder (Außengrad) eines Kontens von B bezeichnet

Definition 5.4.1: Binärer Baum

Ein Baum ist ein **binärer Baum**, falls er vom Grad 2 ist.

Ein Baum heißt regulär, falls alle inneren Knoten gleich viele Kinder haben.

Satz 5.4.1

Sei B ein regulärer binärer Baum mit n Knoten, so hat B:

Blätter	innere Knoten
$\frac{n+1}{2}$	$\frac{n-1}{2}$

Satz 5.4.2

Gegeben sei der Baum B der Höhe h mit einem Grad $s > 1$. So ist die Anzahl der Knoten in B höchstens:

$$|V(B)| \leq \frac{s^{h+1} - 1}{s - 1}$$

5.5 Breiten- und Tiefensuche

Definition 5.5.1: Tiefensuche/depth first search (DFS)

Gegeben sei ein gerichteter Graph $G = (V, E)$, so lässt sich ein gerichteter Baum B mit der Wurzel v konstruieren.
Dabei ist B ein Teilgraph von G und enthält alle Knoten von G, welche von dem Knoten v aus erreichbar sind.

Die Tiefensuche, ist ein Algorithmus und funktioniert wie folgt:

(1) Markiere v (die Wurzel von B) und setze $a = v$. B ist nun ein Baum, welcher nur aus der Wurzel v besteht.

(2) **(Vorwärtsschritt/advance step)** Falls ein unmarkierter Knoten $u \in V$ mit $(a, u) \in E$ existiert, füge sowohl den Knoten u, als auch die Kante (a, u) zu B hinzu, markiere u und setze $a = u$.

(3) **(Rückwärtsschritt/back-tracking step)** Falls es keinen wie in (2) beschriebenen Knoten gibt und $a \neq v$ (also a nicht die Wurzel von B ist), so sei w der Vater von a in B, setze $a = w$ und fahre mit (2) fort.

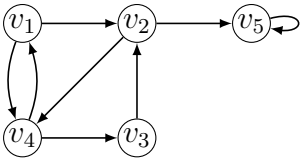
(4) Falls es keinen wie in (2) beschriebenen Knoten gibt und $a = v$ (also a die Wurzel von B ist), so endet der Algorithmus.

Der so erzeugte Baum B wird auch als **DFS-Baum** bezeichnet und enthält alle von v aus erreichbaren Knoten von G (diese entsprechen den markierten Knoten). Der DFS-Baum ist ggf. von den in (2) getroffenen Entscheidungen abhängig und deshalb nicht immer eindeutig.

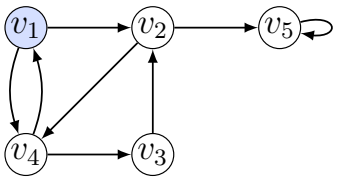
Der Tiefensuchen-Algorithmus lässt sich gut mithilfe eines Stacks implementieren: In den Schritten (1) und (2) wird der neue Knoten auf den Stack gepusht, in Schritt (3) wird der oberste Knoten vom Stack genommen.

Beispiel: Sei die Wurzel $v = v_1$ und das Entscheidungskriterium im Falle mehrerer Optionen der kleinste Index zuerst.

Gegebener Graph: G

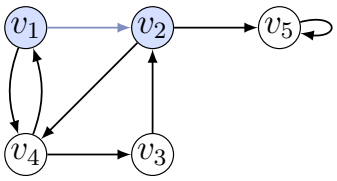


Schritt: (1)

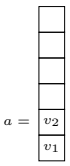


Stack

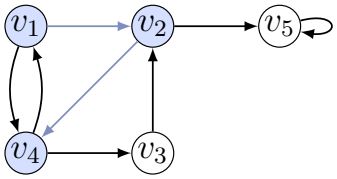
Schritt: (2)



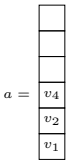
Stack



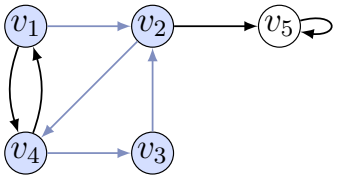
Schritt: (2)



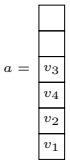
Stack



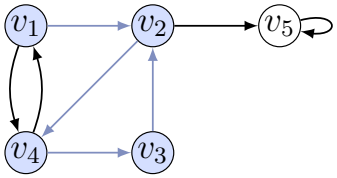
Schritt: (2)



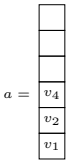
Stack



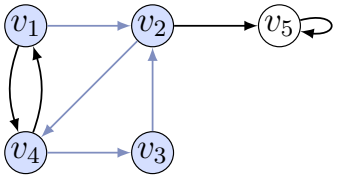
Schritt: (3)



Stack

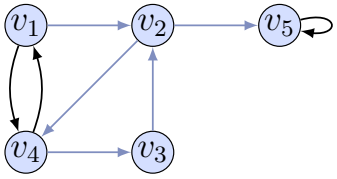


Schritt: (3)

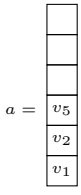


Stack

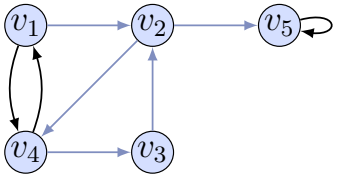
Schritt: (2)



Stack

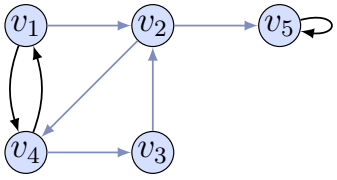


Schritt: (3)



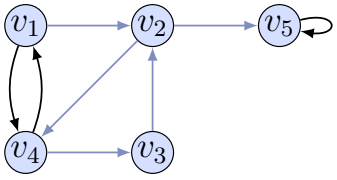
Stack

Schritt: (3)



Stack

Schritt: (3)



Stack

Satz 5.5.1

Von einem Knoten $v \in V(G)$ gibt es genau dann einen gerichteten Weg $v_0, v_1, \ldots, v_\ell$ zu einem anderen Knoten $w \in V(G)$, wenn der Knoten $w \in B$ ist, wobei B der DFS-Baum von G ist.

Definition 5.5.2: Breitensuche/breadth first search (BFS)

Gegeben sei ein gerichteter Graph $G = (V, E)$, so lässt sich ein gerichteter Baum B mit der Wurzel v konstruieren.
Dabei ist B ein Teilgraph von G und enthält alle Knoten von G, welche von dem Knoten v aus erreichbar sind.

Die Breitensuche ist ein Algorithmus und funktioniert wie folgt:

(1) Markiere v (die Wurzel von B) und setze $a = v$. B ist nun ein Baum, welcher nur aus der Wurzel v besteht.

(2) Falls ein unmarkierter Knoten $u \in V$ mit $(a, u) \in E$ existiert, füge sowohl den Knoten u, als auch die Kante (a, u) zu B hinzu und markiere u.

(3) Falls es keinen wie in (2) beschriebenen Knoten gibt und ein Knoten $b \in B$ existiert von dem es eine Kante $(b, u) \in E(G)$ gibt, wobei u ein noch unmarkierter Knoten ist. So wähle aus allen b den, welcher zu erst zu B hinzugefügt wurde und setze $a = b$. Fahre mit Schritt (2) fort.

(4) Falls es keinen wie in (2) beschriebenen Knoten gibt und kein wie in (3) beschriebenes b gibt, so endet der Algorithmus.

Der so erzeugte Baum B wird auch als **BFS-Baum** bezeichnet, aber ist durch G und v nicht eindeutig bestimmt.

Die Breitensuche lässt sich analog zur Tiefensuche implementieren, mit dem Unterschied, dass statt einem Stack eine Warteschlange (Queue) nach dem last in last out (lilo) Prinzip verwendet wird.

Satz 5.5.2

Von einem Knoten $v \in V(G)$ gibt es genau dann einen, gerichteten Weg $v_0, v_1, \ldots, v_\ell$, zu einem anderen Knoten $w \in V(G)$, wenn der Knoten $w \in B$ ist, wobei B der BFS-Baum von G ist.

6. Restklasenringe und RSA-Verschlüsselung

6.1 Restklassenringe

Definition 6.1.1: Restklassen modulo m

$\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z} := \{[0]_m, \ldots, [m-1]_m\}$ meint die Menge der Restklassen modulo m. Weiter ist $x \in K$ ein **Repräsentant (auch Vertreter)** für eine Restklasse K modulo m, es gilt $K = [x]_m$. Dabei sind die **Standardrepräsentanten** für die Restklassen in $\mathbb{Z}_m$ die Zahlen $0, \ldots, m-1$.

Definition 6.1.2: Rechenoperationen zwischen Restklassen modulo m

Seien $x, y \in \mathbb{Z}$ so definieren wir:

$$[x]_m \oplus [y]_m := [x+y]_m$$
$$[x]_m \odot [y]_m := [x \cdot y]_m$$

Dabei sind $\oplus$ und $\odot$ wohldefiniert und nicht abhängig von der Wahl der Repräsentanten x und y, sondern lediglich von den Restklassen $[x]_m$ und $[y]_m$.

Satz 6.1.1: Rechengesetze zwischen Restklassen modulo m

(1) Kommutativgesetz:

$$[x]_m \oplus [y]_m = [y]_m \oplus [x]_m$$
$$[x]_m \odot [y]_m = [y]_m \odot [x]_m$$

(2) Assoziativgesetz:

$$([x]_m \oplus [y]_m) \oplus [z]_m = [x]_m \oplus ([y]_m \oplus [z]_m)$$
$$([x]_m \odot [y]_m) \odot [z]_m = [x]_m \odot ([y]_m \odot [z]_m)$$

(3) Existenz neutraler Elemente:

$$[x]_m \oplus [0]_m = [x]_m$$
$$[x]_m \odot [0]_m = [x]_m$$

(4) Distributivgesetz:

$$[x]_m \odot ([y]_m \oplus [z]_m) = ([x]_m \odot [y]_m) \oplus ([x]_m \odot [z]_m)$$

(5) Existenz additiver Inverser:

$$[x]_m \oplus [-x]_m) = [0]_m$$

Definition 6.1.3: Multiplikatives Inverses

Es sei $[x]_m \in \mathbb{Z}_m$. So gibt es ein **multiplikatives Inverses** $[y]_m$ von $[x]_m$, wenn gilt:

$$[x]_m \odot [y]_m = [1]_m$$

Gibt es ein solches $[b]_m$, so ist $[x]_m$ invertierbar.
Nicht jedes $[x]_m$ hat ein multiplikatives Inverses und höchstens eins.

Satz 6.1.2

$[x]_m \in \mathbb{Z}_m$ ist invertierbar gdw. x und m teilerfremd sind.

Aus dem obigen Satz folgt, sei p eine Primzahl, so ist jedes Element $[x]_p \in \mathbb{Z}_p \setminus \{[0]_p\}$ invertierbar. Dies bedeutet, dass $\mathbb{Z}_p$ ein endlicher Körper ist.

Berechnen des multiplikativen Inverses von $[x]_m \in \mathbb{Z}_m$ passiert mit dem (erweiterten) euklidischen Algorithmus. Sei der $\text{ggT}(x, m) = d = 1$, so ist $[x]_m$ invertierbar und es gibt $\lambda, \mu \in \mathbb{Z}$ mit $d = \mu m + \lambda x$. So ist das multiplikative Inverse von $[x]_m$ $[\lambda]_m$ mit dem Standardrepräsentanten $[\lambda \bmod m]_m$.

Definition 6.1.4: Eulersche φ-Funktion

Sei $\varphi(n),\ n \in \mathbb{N}$ die Anzahl der zu n teilerfremden natürlichen Zahlen kleiner-gleich n.

Sei p eine Primzahl, so ist $\varphi(p) = p - 1$, da alle natürlichen Zahlen, die kleiner als p sind, zu p teilerfremd sind.

Seien p, q verschiedene Primzahlen, so gilt $\varphi(pq) = (p-1) \cdot (q-1) = pq - p - q + 1$.

Definition 6.1.5: Satz von Fermat-Euler

Für zwei teilerfremde, natürliche Zahlen m, n gilt:

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

Sei p eine Primzahl und $n \in \mathbb{N}$. Aus dem obigen Satz und $\varphi(p)$ folgt der **kleine Satz von Fermat**:

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

6.2 RSA-Verschlüsselung

Beim RSA-Verschlüsselungsverfahren gibt es Schlüsselpaar bestehend aus einem privaten und einem öffentlichen Schlüssel. Der öffentliche Schlüssel dient dabei zur Verschlüsselung einer Nachricht m. Eine auf die Art verschlüsselte Nachricht kann allerdings nur mit dem privaten Schlüssel wieder entschlüsselt werden.

Der öffentliche Schlüssel ist dabei ein Zahlenpaar (e, N), der private ein Zahlenpaar (d, N), wobei N das RSA-Modul ist und in beiden Schlüsseln gleich ist.

Um die Schlüssel zu generieren benötigt man zwei möglichst große, verschiedene Primzahlen p und q, dabei ist $N = p \cdot q$. Wichtig ist, dass N größer ist als die Nachricht m, wobei die Größen der Primzahlen natürlich auch einen höheren Sicherheitsfaktor bieten.

Mithilfe der Eulerschen φ-Funktion lässt sich anschließend e errechnen, wobei e eine zu $\varphi(N)$ teilerfremde Zahl ist mit $1 < e < \varphi(N)$.

Der Wert d des privaten Schlüssels lässt sich anschließend errechnen durch das multiplikative Inverse $[d]_{\varphi(N)}$ von $[e]_{\varphi(N)}$.

Die Primzahlen p, q und der Wert $\varphi(N)$ werden nach Generierung der Schlüssel nicht mehr benötigt und können gelöscht werden.

Zum Verschlüsseln einer Nachricht m wird diese mit e potenziert und modulo N gerechnet; zum Entschlüsseln wird die verschlüsselte Nachricht mit d potenziert, sodass $(m^e)^d \equiv m \pmod{N}$.

7. Algebraische Strukturen

7.1 Einfache Strukturen

Definition 7.1.1: Algebraische Struktur

Als **algebraische Struktur** bezeichnet man einen $k+1$-Tupel der Form $\mathcal{M} = (M, f_1, \ldots, f_k)$, wobei M eine Menge ist und $f_i,\ i = 1, \ldots, k$ endlich viele endlichstellige Operationen auf M sind. Man bezeichnet $\mathcal{M}$ auch als **unterliegende Menge**, aber unterscheidet nicht immer zwischen $\mathcal{M}$ und M.

Ein Körper ist nichts anderes als eine Menge K mit den zweistelligen Operationen $+$ und $\cdot$, wobei die Körperaxiome (K1) bis (K5) erfüllt sind, was einen Körper zu einer algebraischen Struktur macht. (Bspw. $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$)

Auch $(\mathbb{N}, +, \cdot)$ und $(\mathbb{Z}, +, \cdot)$ sind algebraischen Strukturen.

Sei $F(M)$ die Menge der Funktionen von einer Menge M auf M, so ist $(F(M), \circ)$ ebenfalls eine algebraische Struktur.

Sei $\mathcal{S}(M)$ die Menge der Bijektionen von M auf M, dann ist auch $(\mathcal{S}(A), \circ)$ eine algebraische Struktur.

Definition 7.1.2: Neutrales Element bezüglich $*$

Sei $*$ eine zweistellige Operation einer algebraischen Struktur $(M, *)$, so heißt ein Element $e \in M$ neutrales Element bezüglich $*$, wenn gilt:

$$\forall x \in M : e * x = x * e = x$$

Ein neutrales Element bezüglich $+$ in $\mathbb{R}$, $\mathbb{Q}$ und $\mathbb{Z}$ ist die 0 und die 1 bezüglich $\cdot$.

Bezüglich $\circ$ ist die identische Abbildung (Identität) $id_M : M \to M; x \mapsto x$ ein neutrales Element in $F(M)$ und $\mathcal{S}(M)$.

So wie wir die natürlichen Zahlen $\mathbb{N}$ definiert haben (> 0) gibt es kein neutrales Element bezüglich $+$, obwohl es sich um eine algebraische Struktur handelt.

Satz 7.1.1

Es gibt höchstens ein neutrales Element e bezüglich einer zweistelligen Operation $*$ auf M.

Definition 7.1.3: Inverses bezüglich $*$

Seien $x, y \in M$, so heißt y zu x invers bezüglich einer zweistelligen Operation $*$ auf M, sofern $x * y = y * x = e$ gilt. Existiert ein solches y, so heißt x invertierbar.

Definition 7.1.4: Halbgruppe und Monoid

Sei $(M, *)$ eine algebraische Struktur und $*$ eine zweistellige Verknüpfung. Gilt nun:

$$\forall x, y, z \in M : x * (y * z) = (x * y) * z$$

also das Assoziativgesetz, so nennt man $(M, *)$ **Halbgruppe**. Hat sie nun auch noch ein neutrales Element, so nennt man sie auch **Monoid**.

Satz 7.1.2

Ein Monoid $(M, *)$ besitzt höchstens ein Inverses bezüglich $*$.

7.2 Gruppentheorie

Definition 7.2.1: Gruppe

Ein Monoid, in dem jedes Element invertierbar ist, nennt man **Gruppe**.

Satz 7.2.1

Für eine Gruppe $\mathcal{G} = (G, *)$ gilt: Seien $x, y, z \in G$ und gilt $x * y = x * z$, so gilt auch $y = z$ und dass aus $y * x = z * x$ folgt $y = z$.
Außerdem sind die Gleichungen $x * y = z$ und $y * x = z$ mit der Unbekannten x eindeutig lösbar.

Oftmals werden $\mathcal{G}$ und G synonym genutzt, da die linke Schreibweise oftmals nur genutzt wird zur expliziten Angabe der Operation $*$ oder der Einschränkung der Menge G.

7.2.1 Die Ordnung eines Gruppenelements

Definition 7.2.2: Ordnung eines Gruppenelements

Sei $\mathcal{G} = (G, *)$ eine Gruppe, so ist a^n definiert durch:

$$a^{n+1} := a^n * a$$
$$a^0 := e$$

Weiter definieren wir für Potenzen mit negativen Exponten:

$$a^{-n} := (a^{-1})^n$$

Für Potenzen in $\mathbb{R}$ gilt für alle $a \in G$ und alle $m, n \in \mathbb{Z}$:

$$a^m a^n = a^{m+n}$$
$$(a^m)^n = a^{mn}$$

Satz 7.2.2

In einer endlichen Gruppe $\mathcal{G}$ hat jedes Element eine endliche Ordnung.

Satz 7.2.3

Für eine Gruppe $\mathcal{G} = (G, *)$ sei $x \in G$ ein Element von endlicher Ordnung m. Es gilt $x^n = e$ für alle ganzen Zahlen $n \in \mathbb{Z}$ gdw. $m \mid n$.

7.2.2 Isomorphie von Gruppen

Definition 7.2.3: Gruppenisomorphismus

Seien $\mathcal{G}$ und $\mathcal{H}$ die Gruppen $\mathcal{G} = (G, *_\mathcal{G})$ und $\mathcal{H} = (H, *_\mathcal{H})$. Man nennt eine Bijektion

$$f : G \to H$$

Isomorphismus von Gruppen, falls gilt:

$$\forall x, y \in G : f(x *_\mathcal{G} y) = f(x) *_\mathcal{H} f(y)$$

Gibt es einen Isomorphismus zwischen zwei Gruppen $\mathcal{G}$ und $\mathcal{H}$, so nennt man sie isomorph und schreibt $\mathcal{G} \cong \mathcal{H}$ (Äquivalenzrelation $\cong$).

Satz 7.2.4

Sei $f : G \to H$ ein Gruppenisomorphismus; so trifft dies auch auf $f^{-1} : H \to G$ zu.

Seien sowohl $f : F \to G$ als auch $g : G \to H$ Gruppenisomorphismen, so handelt es sich auch bei der Verkettung $g \circ f : F \to H$ um einen Gruppenisomorphismus.

Sei wieder $f : G \to H$ ein Gruppenisomorphismus und seien zusätzlich e_G und e_H die neutralen Elemente von G und H, so ist $f(e_G) = e_H$ und $\forall x \in G : f(x^{-1}) = (f(x))^{-1}$

7.2.3 Zyklische Gruppen

Definition 7.2.4: Zyklische Gruppe

Sei G eine Gruppe. G heißt **zyklisch**, wenn es ein $x \in G$ mit $G = \{x^n : n \in \mathbb{Z}\}$ gibt. Das bedeutet, dass x die Gruppe G erzeugt.

Satz 7.2.5

Sei G eine zyklische Gruppe. Es gilt entweder $G \cong (\mathbb{Z}, +)$ oder $G \cong (\mathbb{Z}_m, +)$, $m \in \mathbb{Z}$.

Definition 7.2.5: Kommutative / abelsche Gruppen

Sei G eine Gruppe. Sie heißt kommutativ (auch abelsch), falls in G das Kommutativgesetz gilt, also:

$$\forall x, y \in G : xy = yx$$

Alle zyklischen Gruppen sind abelsch.

7.2.4 Untergruppen und Nebenklassen

Definition 7.2.6: Untergruppe

Sei $\mathcal{G} = (G, *)$ eine Gruppe. $\mathcal{U} = (U, *_{\mathcal{U}})$ heißt Untergruppe von $\mathcal{G}$, falls $U \subseteq G$ gilt und $\mathcal{U}$ zusammen mit der eingeschränkten Operation $*_{\mathcal{U}}$ eine Gruppe bildet, wobei $*_{\mathcal{U}} = * \restriction U \times U$.

Satz 7.2.6

Sei G eine Gruppe und $U \subseteq G$. U ist eine Untergruppe von G gdw. U nicht leer ist und gilt:

$$\forall x, y \in U : e, x^{-1}, xy, xy^{-1} \in U$$

Ist U endlich, so ist ausreichend, dass U nicht leer ist und $\forall x, y \in U : xy \in U$ gilt.

Definition 7.2.7: Links- und Rechtsnebenklassen

Sei G eine Gruppe und $U \subseteq G$ eine Untergruppe von G, so schreibt man $xU = \{xu : u \in U\}$ für ein $x \in G$ und nennt dies **Linksnebenklassen von x von U**; analog schreibt man für die **Rechtsnebenklassen von x von U** $Ux = \{ux : u \in U\}$.

Der Unterschied ist wichtig; ist eine Gruppe abelsch, sind die Links- und Rechtsnebenklassen identisch; ist sie nicht abelsch, kann man keine direkte Aussage treffen.

Beispiel: Die Rechtsnebenklasse von 4 von $\mathcal{U} = (6\mathbb{Z}, +)$ über $\mathcal{G} = (\mathbb{Z}, +)$ entspricht der Menge $\{u + 4 : u \in 6\mathbb{Z}\} = \{6m + 4 : m \in \mathbb{Z}\} = \{\ldots, -2, 4, 10, 16, \ldots\} = [4]_6$. In diesem Fall entspricht sie also der Restklasse von 4 modulo 6 und, da diese Gruppe sogar abelsch ist, sind die Links- äquivalent zu den Rechtsnebenklassen.

Satz 7.2.7

Sei G eine Gruppe und $U \subseteq G$ eine Untergruppe von G, so gilt:

$$\begin{aligned}
\forall x \in G &: x \in xU \wedge x \in Ux \\
\forall u \in U &: uU = U = Uu \\
\forall x, y \in G &: (y \in xU \to xU = yU) \wedge (y \in Ux \to Ux = Uy) \\
\forall x, y \in G &: \text{Entweder } xU = yU \text{ oder sie sind disjunkt,} \\
&\quad \text{Entweder } Ux = Uy \text{ oder sie sind disjunkt} \\
\forall x \in G &: xU, U, Ux \text{ sind gleichmächtig}
\end{aligned}$$

Sei G eine Gruppe; für eine Untergruppe $U \subseteq G$, welche von $x \in G$ erzeugt wird, schreibt man auch $\langle x \rangle := \{x^n : n \in \mathbb{Z}\}$ statt U. Dies Ordnung von $\langle x \rangle$ ist dabei genau die Ordnung von x.

Satz 7.2.8: Satz von Lagrange

Es sei G eine endliche Gruppe und $U \subseteq G$ eine Untergruppe von G. Die Ordnung von U ist ein Teiler der Ordnung von G.

Definition 7.2.8: Index einer Untergruppe

Sei G eine Gruppe. Wir bezeichnen die Anzahl der Rechtsnebenklassen von einer Untergruppe $U \subseteq G$ als Index von U in G und schreiben $[G : U]$.
Dabei ist die Anzahl der Rechtsnebenklassen immer identisch zur Anzahl der Linksnebenklassen.

Für eine endliche Gruppe G und jede Untergruppe $U \subseteq G$ gilt:

$$|G| = [G : U] \cdot |U|$$

Satz 7.2.9

Die Untergruppe einer zyklischen Gruppe ist zyklisch.

Satz 7.2.10

Eine Gruppe G deren Ordnung eine Primzahl ist, ist zyklisch und hat lediglich die Untergruppen G und $\{e\}$ (e ist das neutrale Elemente).

7.3 Permutationen

Eine Permutation der Menge M ist eine Bijektion von M nach M. Dabei ist $S(M)$ die Gruppe aller Permutationen auf der Menge M mit der Verknüpfung $\circ$ (Verkettung) und der Identität ID_M als neutrales Element.

Sei $M = \{x_1, \ldots, x_n\}$, $n \in \mathbb{N}$ eine Menge und $\pi : M \to M$ eine Permutation, man schreibt:

$$\pi = \begin{pmatrix} x_1 & \ldots & x_n \\ \pi(x_1) & \ldots & \pi(x_n) \end{pmatrix}$$

Wir schreiben außerdem π^m, $m \in \mathbb{N}$, wenn wir die Permutation mehrmals anwenden.

Satz 7.3.1

Sei M eine endliche Menge. Sei weiter $\pi \in S(M)$. Es existiert für jedes $x \in M$ ein $n \in \mathbb{N}$, sodass $\pi^n(x) = x$.

Gibt es ein $n \in \mathbb{N}$, sodass für alle $x \in M$ gilt, dass $\pi^n(x) = x$, so ist $\pi^n = Id_M$ und n die Ordnung von π.

Definition 7.3.1: Zyklus der Länge n

Sei M eine Menge und $x_1, \ldots, x_n \in M$ mit $n \geq 2$ paarweise verschieden. Man bezeichnen mit $(x_1 \ldots x_n)$ die wie folgt definierte Permutation π von M:

$$\pi(x) = \begin{cases} x, & \text{falls } x \in M \setminus \{x_1, \ldots, x_n\} \\ x_{i+1}, & \text{falls } x = x_i,\ i \in \{1, \ldots, n-1\} \\ x_1, & \text{falls } x = x_n \end{cases}$$

Diese Permutation nennt man einen **Zyklus der Länge** n. Zwei Zyklen $(x_1 \ldots x_n)$ und $(y_1 \ldots y_m)$ mit $n, m \in \mathbb{N}$ heißen **disjunkt**, falls die Mengen $\{x_1, \ldots, x_n\}$ und $\{y_1 \ldots y_m\}$ disjunkt sind. Ein Zyklus der Länge 2 heißt **Transposition**.

Satz 7.3.2

Sei M eine endliche Menge. Jede Permutation $\pi \in S(M)$ ist ein Produkt paarweise disjunkter Zyklen. Dabei nennt man die Darstellung von π als Produkt disjunkter Zyklen **Zyklenzerlegung**, welche bis auf die Reihenfolge eindeutig ist.

Jeder Zyklus sowie jede Permutation von M ist ein Produkt von Transpositionen.