Übung 0: Mathematische Grundlagen

Vor dem Beginn der Vorlesung und Übung wollen wir kurz einige Dinge aus der Mathematik wiederholen, die wir in ALD benötigen. Eine ausführliche Behandlung dieser Themen finden Sie unter anderem in dem Buch: *Eine Einführung in die Mathematik an Beispielen aus der Informatik – Logik, Zahlen, Graphen, Analysis und Lineare Algebra. St.J. Goebbels, J. Rethmann. Springer Verlag, 2023.*

In ALD soll es natürlich um *Algorithmen und Datenstrukturen* gehen, nicht um Mathematik. Aber wir benötigen Mathematik als „Handwerkszeug". Zum einen, um die Probleme, die wir lösen wollen, sauber zu definieren, zum anderen, um die Korrektheit der Algorithmen zeigen und die Laufzeiten herleiten zu können. Die benötigte Mathematik ist nicht schwer und wir benötigen auch nicht sehr viel Mathematik.

Mengen Schauen wir uns zunächst einige Notationen aus dem Bereich Mengenlehre an. Unter einer *Menge M* verstehen wir eine gedankliche Zusammenfassung von unterscheidbaren Dingen. Die „Dinge" sind die Elemente von M. Diese einfache „Definition" einer Menge soll für uns genügen, obwohl wir nicht formal festlegen, was „Dinge" oder eine „gedankliche Zusammenfassung" ist. Korrekt müsste man eine Menge axiomatisch definieren[1], was hier aber viel zu weit führen würde.

- Die Menge $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$ bezeichne die Menge der natürlichen Zahlen, die Menge $\mathbb{N}_0 = \{0, 1, 2, 3, , \ldots\}$ enthält auch die Zahl Null.
- Die Menge der ganzen Zahlen $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ bezeichnen wir mit $\mathbb{Z}$.

Um auszudrücken, dass x ein Element der Menge M ist, schreiben wir $x \in M$. Um auszudrücken, dass x kein Element der Menge M ist, schreiben wir $x \notin M$. Beispielsweise gehört die Zahl -2 zur Menge $\mathbb{Z}$, sie ist ein Element der Menge der ganzen Zahlen, also schreiben wir $-2 \in \mathbb{Z}$. Allerdings gehört -2 nicht zur Menge der natürlichen Zahlen, sie ist kein Element von $\mathbb{N}$, also schreiben wir $-2 \notin \mathbb{N}$.

Die obigen Mengen $\mathbb{N}$ und $\mathbb{Z}$ konnten leicht mittels einer Aufzählung angegeben werden, bei den rationalen Zahlen $\mathbb{Q}$ ist das nicht mehr so einfach möglich, bei den reellen Zahlen $\mathbb{R}$ ist es gar nicht möglich. Daher werden Mengen auch oft durch Angabe von Bedingungen beschrieben.

- Die Menge $\mathbb{Q}$ der rationalen Zahlen wird durch $\mathbb{Q} := \{\frac{a}{b} \mid a \in \mathbb{Z},\ b \in \mathbb{N}\}$ beschrieben. Es ist die Menge aller Brüche $\frac{a}{b}$, wobei der Zähler $a \in \mathbb{Z}$ eine ganze Zahl und der Nenner $b \in \mathbb{N}$ eine natürliche Zahl sind. Damit ist $b = 0$ automatisch ausgeschlossen.
- Mit $\mathbb{R}$ bezeichnen wir die Menge der reellen Zahlen; die Menge der positiven, reellen Zahlen bezeichnen wir mit $\mathbb{R}^+$; soll auch die Null enthalten sein, dann schreiben wir $\mathbb{R}_0^+$.

Zwei Mengen X und Y heißen *gleich* genau dann, wenn sie die gleichen Elemente besitzen, d.h., jedes Element der einen Menge ist auch in der anderen Menge enthalten und umgekehrt. Wir schreiben dann $X = Y$. Gilt dies nicht, dann schreiben wir $X \neq Y$. Beispielsweise sind die Mengen $X = \{1, 2, 3\}$ und $Y = \{2, 3, 1\}$ gleich, sie enthalten dieselben Elemente, also dürfen

[1] `https://de.wikipedia.org/wiki/Zermelo-Fraenkel-Mengenlehre`

wir $X = Y$ schreiben. Die Reihenfolge, in der wir die Elemente einer Menge aufzählen, spielt also keine Rolle.

Eine Menge X heißt *Teilmenge* von Y genau dann, wenn jedes Element von X auch Element von Y ist. Dann schreiben wir $X \subseteq Y$. Die leere Menge $\emptyset$ und die Menge X selber sind immer Teilmengen von X, es gilt also $\emptyset \subseteq X$ und $X \subseteq X$.

Ist X keine Teilmenge von Y, so schreiben wir $X \not\subseteq Y$. Um auszudrücken, dass eine Menge X eine echte Teilmenge von Y ist, schreiben wir $X \subset Y$ oder $X \subsetneq Y$. In diesem Fall gibt es (mindestens) ein Element $e \in Y$, das nicht in X enthalten ist, also $e \notin X$ gilt.

Achtung: Diese Schreibweisen $\subseteq$ und $\subset$ werden in der Mathematik und Informatik nicht einheitlich benutzt, im Gegensatz zu den Vergleichen $\leq$ und $<$ auf Zahlen. Wenn Sie also in Büchern oder auf Web-Seiten etwas über Mathematik lesen, dann müssen Sie sich dort zunächst über die Begriffsbildungen informieren, um die Texte auch wirklich verstehen zu können.

Mengenoperationen Oft müssen wir Operationen auf Mengen durchführen können, so wie wir bspw. die Operationen Addition, Subtraktion, Multiplikation oder Division auf Zahlen durchführen können. Ohne auf Mengen definierte Operationen wäre die Mengenlehre sehr langweilig. Im Folgenden seien X und Y zwei Mengen.

- *Schnitt* bzw. Schnittmenge: $X \cap Y := \{e \in X \mid e \in Y\}$
- *Vereinigung* bzw. Vereinigungsmenge: $X \cup Y := \{e \mid e \in X \text{ oder } e \in Y\}$
- *Differenz* bzw. Differenzmenge: $X \setminus Y := \{e \in X \mid e \notin Y\}$
- Sind die Elemente einer Menge der Größe nach vergleichbar, dann liefert $\max X$ das größte Element von X, falls es existiert, und $\min Y$ liefert das kleinste Element von Y, sofern vorhanden.

  Beispiel: $\min\{1, 2, 3, 4, 5\} = 1$ und $\max\{1, 2, 3, 4, 5\} = 5$.
- Das *kartesische Produkt* $X \times Y = \{(x, y) \mid x \in X, y \in Y\}$ zweier Mengen X und Y ist definiert als die Menge aller geordneten Paare, deren erstes Element aus X und deren zweites Element aus Y ist.

  Beispiel: Für die Mengen $X = \{2, 4, 8\}$ und $Y = \{3, 5, 7\}$ gilt:

  $$X \times Y = \{(2, 3), (2, 5), (2, 7), (4, 3), (4, 5), (4, 7), (8, 3), (8, 5), (8, 7)\}$$

- Um das Komplement $\overline{X}$ einer Menge X definieren zu können, benötigen wir zunächst eine Grundmenge G. Sei daher $X \subseteq G$ eine Menge über der Grundmenge G. Dann ist das *Komplement* $\overline{X}$ von X die Menge mit den Elementen von G, die nicht in X enthalten sind, also $\overline{X} := \{e \in G \mid e \notin X\}$.

  Beispiel: Für die Grundmenge $G = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ und die Menge $X = \{2, 3, 5, 7\}$ ist $\overline{X} = \{1, 4, 6, 8, 9\}$.

Zwei Mengen A und B heißen *disjunkt* (oder auch elementfremd), wenn sie kein Element gemeinsam haben, also wenn $A \cap B = \emptyset$ gilt. Beispielsweise gilt für die Mengen $A = \{2, 3, 5\}$, $B = \{1, 2, 4\}$ und $C = \{3, 5, 7\}$:

- A und B sind nicht disjunkt, denn $A \cap B = \{2\} \neq \emptyset$.
- A und C sind nicht disjunkt, denn $A \cap C = \{3, 5\} \neq \emptyset$.

- B und C sind disjunkt, denn $B \cap C = \emptyset$.

Mehrere Mengen $M_1, \ldots, M_k$ heißen *paarweise disjunkt*, genau dann wenn beliebige zwei der Mengen disjunkt sind, also $M_i \cap M_j = \emptyset$ für $1 \leq i, j \leq k$ und $i \neq j$ gilt. So sind bspw. die Mengen $X = \{2, 4, 8\}$, $Y = \{3, 9, 27\}$ und $Z = \{5, 25, 125\}$ paarweise disjunkt.

Mächtigkeit einer Menge Bei einer endlichen Menge M bezeichnen wir die Anzahl der Elemente auch als *Mächtigkeit* oder *Kardinalität* und schreiben dafür $|M|$. So gilt für die obigen Mengen unter anderem $|A| = |B| = |C| = 3$, $|A \cap B| = 1$, $|A \cap C| = 2$, $|B \cap C| = 0$ und $|X \times Y| = |X| \cdot |Y| = 3 \cdot 3 = 9$.

Zu einer Menge M bezeichnet die *Potenzmenge* $\mathcal{P}(M)$ die Menge aller Teilmengen von M. Die Mächtigkeit der Potenzmenge ist $|\mathcal{P}(M)| = 2^{|M|}$. Für die obige Menge $A = \{2, 3, 5\}$ gilt

$$\mathcal{P}(A) = \big\{\emptyset, \{2\}, \{3\}, \{5\}, \{2, 3\}, \{2, 5\}, \{3, 5\}, \{2, 3, 5\}\big\}$$

und daher $|\mathcal{P}(A)| = 8 = 2^3 = 2^{|A|}$.

Bei unendlichen Mengen wie $\mathbb{N}$ oder $\mathbb{R}$ ist die Kardinalität nicht so einfach zu definieren. Man definiert daher zunächst den Begriff der Gleichmächtigkeit zweier beliebiger Mengen A und B. Eine Menge A heißt *gleichmächtig* zu einer Menge B, wenn es eine bijektive Funktion $f\colon A \to B$ gibt, siehe Seite 9. Man schreibt dann $|A| = |B|$.

Eine Menge, die gleichmächtig zur unendlichen Menge $\mathbb{N}$ ist, heißt *abzählbar*, da die Elemente abgezählt werden können. Beispielsweise sind $\mathbb{N}$, $\mathbb{Z}$ und $\mathbb{Q}$ abzählbar, wohingegen die Menge der reellen Zahlen $\mathbb{R}$, die Menge der komplexen Zahlen $\mathbb{C}$ oder auch das Intervall $]0, 1[$ mächtiger als $\mathbb{N}$ sind und daher *überabzählbar* genannt werden.

Eigenschaften von Mengen Im Folgenden seien X, Y und Z drei Mengen.

- Transitiv: Aus $X \subseteq Y$ und $Y \subseteq Z$ folgt $X \subseteq Z$.
- Kommutativ: $X \cup Y = Y \cup X$ und $X \cap Y = Y \cap X$
- Assoziativ: $X \cup (Y \cup Z) = (X \cup Y) \cup Z$ und $X \cap (Y \cap Z) = (X \cap Y) \cap Z$
- Distributiv: $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$ und $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$

  Achtung: Das Distributivgesetz gilt für beide Operationen, der Vereinigung $\cup$ und der Schnittmengenbildung $\cap$. Bei Zahlen gilt das Distributivgesetz nicht in beiden Ausprägungen für die Operationen Addition und Multiplikation. Es gilt zwar

  $$3 \cdot (4 + 5) = 3 \cdot 9 = 27 = (3 \cdot 4) + (3 \cdot 5) = 12 + 15,$$

  aber werden die Operationen Addition und Multiplikation vertauscht, dann gilt es nicht:

  $$3 + (4 \cdot 5) = 3 + 20 = 23 \neq (3 + 4) \cdot (3 + 5) = 7 \cdot 8 = 56$$

- de Morgan: $\overline{X \cup Y} = \overline{X} \cap \overline{Y}$ und $\overline{X \cap Y} = \overline{X} \cup \overline{Y}$ bezüglich einer gemeinsamen Grundmenge G, also $X, Y \subseteq G$.

Aussagenlogik Unter einer *Aussage* versteht man in der Mathematik einen Satz, der entweder wahr oder falsch ist, wie bspw. der Satz „Krefeld liegt an der Elbe“, der offensichtlich eine falsche Aussage ist. In der Mathematik handeln die Aussagen von mathematischen Objekten wie Zahlen, Mengen, Relationen oder Funktionen, wie bspw. die Aussage „es gibt unendlich viele Primzahlen“ oder „die Summe zweier ungerader natürlicher Zahlen ist ungerade“.

Oft wollen wir Aussagen verknüpfen, wie bspw. in dem Satz „es regnet und die Sonne scheint“ oder „wenn es regnet und die Sonne scheint, dann ist ein Regenbogen am Himmel“. Im Folgenden definieren wir einige logische Operationen wie Und, Oder, Nicht, Implikation und Äquivalenz mittels Wahrheitstafeln.

- Die Negation $\neg X$ oder auch $\overline{X}$ (logisches Nicht) ist genau dann wahr, wenn X falsch ist.

X	$\neg X$
0	1
1	0

- Die Konjunktion $X \wedge Y$ (logisches Und) ist genau dann wahr, wenn beide Aussagen X und Y wahr sind.

X	Y	$X \wedge Y$
0	0	0
0	1	0
1	0	0
1	1	1

- Die Disjunktion $X \vee Y$ (logisches Oder) ist genau dann wahr, wenn (mindestens) eine der Aussagen X oder Y wahr ist.

X	Y	$X \vee Y$
0	0	0
0	1	1
1	0	1
1	1	1

- Die Implikation $X \Rightarrow Y$ (wenn X dann Y bzw. aus X folgt Y) ist genau dann wahr, wenn X falsch oder Y wahr ist.

X	Y	$X \Rightarrow Y$
0	0	1
0	1	1
1	0	0
1	1	1

- Die Äquivalenz $X \iff Y$ (X genau dann wenn Y) ist genau dann wahr, wenn X und Y denselben Wahrheitswert haben.

X	Y	$X \iff Y$
0	0	1
0	1	0
1	0	0
1	1	1

Diese einfachen logischen Operationen können kombiniert und verschachtelt werden, sodass beliebig komplexe Aussagen entstehen können. Auch deren Wahrheitswert kann mittels Wahrheitstafeln bestimmt werden. Beispiel:

$$((P \Rightarrow Q) \wedge P) \Rightarrow Q$$

Oder in Worten: Wenn ((*P* impliziert *Q*) und (*P* gilt), dann gilt auch *Q*. Hier die dazu passende Wahrheitstafel:

P	Q	$P \Rightarrow Q$	$(P \Rightarrow Q) \wedge P$	$((P \Rightarrow Q) \wedge P) \Rightarrow Q$
0	0	1	0	1
0	1	1	0	1
1	0	0	0	1
1	1	1	1	1

Diese (komplexe) Aussage ist offensichtlich für alle möglichen Kombinationen von Wahrheitswerten wahr. Eine solche Aussage nennt man *Tautologie*. Eine (komplexe) Aussage, die immer falsch ist, nennt man *Kontradiktion* oder *unerfüllbar*. Die folgende Liste enthält einige sehr wichtige Tautologien.

- Modus Ponens: $((P \Rightarrow Q) \wedge P) \;\Rightarrow\; Q$
- Modus Tollens: $((P \Rightarrow Q) \wedge \neg Q) \;\Rightarrow\; \neg P$
- Implikation ist transitiv: $((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \;\Rightarrow\; (P \Rightarrow R)$
- $(P \iff Q) \iff ((P \Rightarrow Q) \wedge (Q \Rightarrow P))$

Syntaktisch unterschiedliche Formeln können dasselbe aussagen. So bedeuten die beiden Aussagen $F \wedge G$ und $G \wedge F$ dasselbe, obwohl es syntaktisch zwei verschiedene Objekte sind. Auch $\neg(F \vee G)$ und $(\neg F \wedge \neg G)$ sagen dasselbe aus, wie man an den Wahrheitstafeln erkennen kann.

F	G	$\neg(F \vee G)$	$\neg F \wedge \neg G$
0	0	1	1
0	1	0	0
1	0	0	0
1	1	0	0

und

F	G	$\neg(F \wedge G)$	$\neg F \vee \neg G$
0	0	1	1
0	1	1	1
1	0	1	1
1	1	0	0

Soll eine mathematische Aussage bewiesen werden, dann ist es oft einfacher, eine andere Aussage zu beweisen, die aber „dieselbe Bedeutung“ hat wie die ursprüngliche Aussage. Dies ist genau dann der Fall, wenn beide Aussagen denselben Wahrheitswert in jeder Zeile der zugehörigen Wahrheitstafel haben:

> Zwei Aussagen P und Q heißen *äquivalent*, wenn $P \iff Q$ eine Tautologie ist. Wir schreiben in diesem Fall $P \equiv Q$.

Die folgende Liste enthält einige wichtige Äquivalenzen.

$$
\begin{array}{rcll}
(F \wedge F) & \equiv & F & \text{Idempotenz} \\
(F \vee F) & \equiv & F & \\
(F \wedge G) & \equiv & (G \wedge F) & \text{Kommutativität} \\
(F \vee G) & \equiv & (G \vee F) & \\
((F \wedge G) \wedge H) & \equiv & (F \wedge (G \wedge H)) & \text{Assoziativität} \\
((F \vee G) \vee H) & \equiv & (F \vee (G \vee H)) & \\
(F \wedge (F \vee G)) & \equiv & F & \text{Absorption} \\
(F \vee (F \wedge G)) & \equiv & F &
\end{array}
$$

$$
\begin{array}{rcll}
(F \wedge (G \vee H)) & \equiv & ((F \wedge G) \vee (F \wedge H)) & \text{Distributivität} \\
(F \vee (G \wedge H)) & \equiv & ((F \vee G) \wedge (F \vee H)) & \\
\neg\neg F & \equiv & F & \text{Doppelnegation} \\
\neg(F \wedge G) & \equiv & (\neg F \vee \neg G) & \text{de-Morgansche-Regeln} \\
\neg(F \vee G) & \equiv & (\neg F \wedge \neg G) & \\
(F \vee G) & \equiv & F, \text{ falls } F \text{ Tautologie} & \text{Tautologieregeln} \\
(F \wedge G) & \equiv & G, \text{ falls } F \text{ Tautologie} & \\
(F \vee G) & \equiv & G, \text{ falls } F \text{ unerfüllbar} & \text{Unerfüllbarkeitsregeln} \\
(F \wedge G) & \equiv & F, \text{ falls } F \text{ unerfüllbar} &
\end{array}
$$

Nur so am Rande, obwohl das eigentlich mit Logik gar nichts zu tun hat, sehr wohl allerdings mit Aussagen: Bestimmte Aussagen bekommen in der Mathematik einen Namen.

- Definition: Eine Namensgebung für einen Sachverhalt.
- Satz bzw. Theorem: Eine wichtige Aussage.
- Lemma: Ein Hilfssatz, zur Hinführung auf einen Satz
- Korollar: Eine direkte Folgerung aus einem Satz.

Prädikatenlogik Wenn wir in einer Aussage wie „3 ist eine Primzahl“ oder „3 ist größer als 4“ einen Wert durch eine Variable ersetzen, dann nennen wir einen Satz wie „x ist eine Primzahl“ oder „x ist größer als y“ eine *Aussageform*. Eine Aussageform ist selbst keine Aussage, kann aber durch das Einsetzen entsprechender Werte zu einer Aussage gemacht werden. Ob durch das Einsetzen der Werte eine wahre oder falsche Aussage entsteht, hängt vom eingesetzten Wert ab.

Aussageformen werden wir mittels großer Buchstaben gefolgt von einer „Parameterliste“ schreiben, also bspw. $P(x)$ für eine Aussageform, die von einer Variablen x abhängt, oder $Q(x, y)$ für eine Aussageform, die von zwei Variablen x und y abhängt. Beispiele:

- Sei $P(x)$ die Aussageform „x ist eine Primzahl“. Dann ist $P(7)$ die Aussage „7 ist eine Primzahl“ und daher wahr.
- Sei $Q(x, y)$ die Aussageform „$x \geq y$“. Dann ist $Q(3, 4)$ die falsche Aussage $3 \geq 4$.

Auch Aussageformen können über die logischen Operationen Und, Oder, Nicht usw. verknüpft werden. So können wir obige Aussageformen $P(x)$ und $Q(x, y)$ verknüpfen zu $P(x) \wedge Q(x, y)$, was für $x = 5$ und $y = 4$ zu einer wahren Aussage wird.

Beispiel: Sei „x ist durch 3 teilbar“ die Aussageform $P(x)$ und sei „x ist kleiner als 14“ die Aussageform $Q(x)$.

- Für $x \in \mathbb{N}$ ist $P(x) \wedge Q(x)$ wahr für die Zahlen 3, 6, 9 und 12.
- Für $x \in \mathbb{Z}$ ist $P(x) \wedge Q(x)$ wahr für die Zahlen …, -6, -3, 0, 3, 6, 9 und 12.
- Für $x \in \mathbb{N}$ ist $\neg P(x)$ für die Zahlen 1, 2, 4, 5, 7, 8, … wahr.

Hier haben wir die Werte, für die die Aussageform gilt, explizit angegeben. Oft werden solche Werte nicht explizit angegeben, sondern *quantifiziert*. Dabei werden zwei *Quantoren* unterschieden:

- Der Existenzquantor $\exists$: Die Aussageform $\exists x\, P(x)$ steht für die Aussage „es existiert mindestens ein Wert x (aus einer gegebenen Grundmenge), für den $P(x)$ eine wahre Aussage ist“.
- Der Allquantor $\forall$: Die Aussageform $\forall x\, Q(x)$ steht für die Aussage „für alle Werte (einer gegebenen Grundmenge) ist die Aussage $Q(x)$ wahr“.

Beispiel: Sei $P(x)$ wieder die Aussageform „x ist eine Primzahl“. Dann ist $\exists x \in \mathbb{N} : P(x)$ wahr, denn $P(5)$ ist wahr. Man liest den Doppelpunkt als „sodass gilt“, hier also „Es existiert ein x aus $\mathbb{N}$ sodass $P(x)$ gilt“. Für den Allquantor ist $\forall x \in \mathbb{N} : P(x)$ falsch. Schränken wir die Grundmenge ein, dann wäre bspw. $\forall x \in \{2, 3, 5, 7\} : P(x)$ wahr.

Relationen und Abbildungen Seien A und B Mengen. Eine Teilmenge $R \subseteq A \times B$ heißt *Relation*. Eine Relation ist also eine Menge von Paaren. Oft wird anstelle von Paaren die Schreibweise

$$xRy \iff (x, y) \in R$$

genutzt, die aussagt, dass x in Relation zu y steht. Seien $A = \{x, y, z\}$ und $B = \{a, b, c, d, e\}$ zwei Mengen und $R = \{(x, a), (x, b), (x, c), (z, d), (z, e)\} \subseteq A \times B$ eine Relation. Dann kann uRv bspw. die Bedeutung „u ist Vater von v“ haben. In diesem Fall hätte x drei Kinder, y wäre kinderlos und z hätte zwei Kinder. Da jedes Kind genau einen (leiblichen) Vater hat, ist jedes Element von B genau einmal in den Paaren aus $A \times B$ enthalten.

Betrachten wir einige Eigenschaften von Relationen. Sei dazu $R \subseteq M \times M$ eine Relation.

- R heißt *reflexiv* genau dann, wenn für alle $x \in M$ gilt: xRx.

  Sei $R \subseteq \mathbb{N} \times \mathbb{N}$ mit $xRy :\iff x \leq y$. Dann ist R reflexiv, denn für jedes $n \in \mathbb{N}$ gilt $n \leq n$. Die Relation $<$ hingegen ist nicht reflexiv.

- R heißt *transitiv* genau dann, wenn für alle $x, y, z \in M$ gilt: Aus xRy und yRz folgt xRz.

  Die Relation $\leq$ ist transitiv, denn aus $x \leq y$ und $y \leq z$ folgt $x \leq z$. Auch die Relation $<$ ist transitiv.

- R heißt *symmetrisch* genau dann, wenn für alle $x, y \in M$ gilt: Aus xRy folgt yRx.

  Die Relationen $\leq$ und $<$ sind beide nicht symmetrisch, denn aus $x < y$ folgt nicht $y < x$. Die Relation $=$ ist symmetrisch, denn falls $x = y$ gilt, dann gilt auch $y = x$.

- R heißt *anti-symmetrisch* genau dann, wenn für alle $x, y \in M$ gilt: Aus xRy und yRx folgt $x = y$. **Achtung:** Anti-symmetrisch ist nicht das Gegenteil von symmetrisch. Die Relation $=$ ist symmetrisch und anti-symmetrisch.

  Die Relation $\leq$ ist anti-symmetrisch, denn wenn $x \leq y$ und $y \leq x$ gilt, dann ist $x = y$.

- Ist eine Relation reflexiv, symmetrisch und transitiv, so heißt sie eine *Äquivalenzrelation*. Der Name leitet sich von der Äquivalenz ab, die die gleichen Eigenschaften hat.

- Die *transitive, reflexive Hülle* R^* von R ist definiert als die kleinste Menge mit den Eigenschaften $R \subseteq R^*$ sowie R^* ist reflexiv und transitiv.

Der Begriff „transitiv“ kann als Transitionsschritt bei einem Automaten oder einer Turingmaschine interpretiert werden und spielt daher im Bereich Berechenbarkeit und Komplexitätstheorie eine wichtige Rolle.

Eine Relation $R \subseteq A \times B$ heißt

- *linkstotal*, wenn gilt: $\forall a \in A \; \exists b \in B : aRb$
- *rechtstotal*, wenn gilt: $\forall b \in B \; \exists a \in A : aRb$
- *linkseindeutig*, wenn gilt: $\forall a, b, c : (aRb \wedge cRb) \Rightarrow a = c$
- *rechtseindeutig*, wenn gilt: $\forall a, b, c : (aRb \wedge aRc) \Rightarrow b = c$

Die obige ist-Vater-von-Relation ist nicht linkstotal, da y nicht auf der linken Position eines Paares aus R vorkommt: y ist kinderlos. Sie ist rechtstotal, da alle Elemente aus B in mindestens einem Paar aus R auf der rechten Position vorkommt: Alle Kinder haben (mindestens) einen Vater. Außerdem ist sie linkseindeutig, denn jedes Kind hat genau einen leiblichen Vater. Aber sie ist nicht rechtseindeutig: Zwei der Väter haben mehr als ein Kind.

Kommen wir nun zu dem Begriff der Funktion.

- Eine rechtseindeutige Relation $f \subseteq A \times B$ heißt *partielle Funktion* oder funktionale Relation oder Abbildung von A nach B.
- Eine linkstotale partielle Funktion $f \subseteq A \times B$ heißt *(totale) Funktion* von A nach B.

Aufgrund der Rechtseindeutigkeit schreibt man anstelle von $(a, b) \in f \subseteq A \times B$ bei Funktionen üblicherweise $f : A \to B$ und $b = f(a)$ oder auch $a \mapsto f(a)$.

- Der Wert $b = f(a) \in B$ heißt das *Bild* von a unter f.
- Für alle $b \in B$ ist $f^{-1}(b) = \{a \in A \mid f(a) = b\}$ die Menge der *Urbilder* von b unter f. Die Menge $f^{-1}(b)$ kann leer sein.

Wir haben den Begriff der Funktion so gewählt, wie es in der Theoretischen Informatik üblich ist. Hier wird zwischen partieller und totaler Funktion unterschieden, die Mathematik kennt in der Regel nur Funktionen, die immer linkstotal sind. Es kann aber schwierig bis unmöglich sein, herauszufinden, für welche Eingaben ein Algorithmus terminiert (Halteproblem[2]) und damit einen Funktionswert berechnet[3]. Daher meinen wir oft nur eine partielle Funktion, wenn wir von Funktionen sprechen.

Die folgenden Begriffe sind in der Abbildung 1 auch grafisch veranschaulicht. Sei $f : A \to B$ eine partielle Funktion.

- Die Menge A wird als *Quellmenge* oder Grundmenge bezeichnet und die Menge B heißt *Zielmenge*.
- Bei einer totalen Funktion $f : A \to B$ nennt man A auch den *Definitionsbereich* oder den Argumentbereich der Funktion.

[2] `https://de.wikipedia.org/wiki/Halteproblem`
[3] `https://de.wikipedia.org/wiki/Partielle_Funktion#Anwendungen`

- Bei einer partiellen Funktion muss nicht jedes $a \in A$ ein Bild $f(a) \in B$ besitzen. Der (eventuell nicht explizit angebbare) Definitionsbereich $D(f)$ ist hier die Menge der Urbilder $a \in A$, für die ein Bild $f(a)$ erklärt ist. Der Definitionsbereich ist die Einschränkung von A auf die Urbilder.

- Die Menge $W(f)$ der Elemente aus B, die als Werte der Abbildung tatsächlich auftreten, also
$$W(f) := \{b \in B \mid \text{ es existiert ein } a \in A \text{ mit } b = f(a)\}$$
heißt der *Wertebereich*, die *Wertemenge* oder die *Bildmenge* von f. Die Bildmenge ist die Einschränkung der Zielmenge B auf die Bilder.

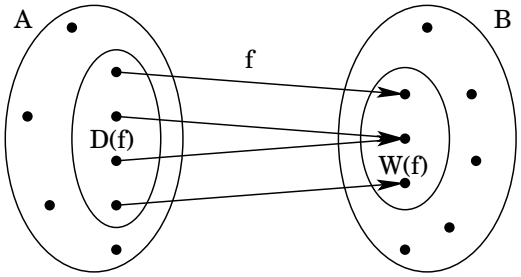

Abbildung 1: Definitionsbereich und Wertebereich einer Funktion.

Sei $f \subseteq A \times B$ eine totale Funktion, d.h., sie ist rechtseindeutig und linkstotal.

- Eine linkseindeutige Funktion heißt *injektiv*.
- Eine rechtstotale Funktion heißt *surjektiv*.
- Eine surjektive und injektive Funktion heißt *bijektiv*.

Bei injektiven Funktionen ist das Urbild von b eindeutig, man identifiziert das eine Element a mit $f(a) = b$ dann mit der Menge $f^{-1}(b)$ und spricht bei f^{-1} von *Umkehrfunktion*.

Beispiel: Die Funktion $f : \mathbb{N} \to \mathbb{N}$ mit $f(x) = x^2$ ist injektiv. Zu jedem Bild y gibt es ein eindeutiges Urbild $f^{-1}(y) = \sqrt{y}$. Aber die Funktion ist nicht surjektiv, da bspw. der Wert $2 \in \mathbb{N}$ nicht das Quadrat einer natürlichen Zahl ist, denn $\sqrt{2} \notin \mathbb{N}$.

Durch Einschränkung der Zielmenge auf die Bildmenge kann allerdings jede Abbildung „surjektiv gemacht werden“, in diesem Fall etwa so: Die Funktion $f' : \mathbb{N} \to \{1, 4, 9, 16, 25, \ldots\}$ mit $f'(x) = x^2$ ist surjektiv. Damit ist diese Funktion injektiv und surjektiv, also auch bijektiv.

Mit der Definition der Gleichmachtigkeit zweier Mengen von Seite 3 heißt das also, dass die Mengen $\mathbb{N}$ und $\{1, 4, 9, 16, 25, \ldots\}$ gleich mächtig sind. Obwohl in der zweiten Menge viele natürliche Zahlen „fehlen“, sind die Mengen gleich mächtig, denn von beiden Mengen können die Elemente aufgezählt werden.

Die Funktion $g : \mathbb{Z} \to \mathbb{N}$ mit $g(x) = x^2$ ist nicht injektiv, also linkseindeutig, denn sowohl $g(-2) = 4$ als auch $g(2) = 4$ werden auf denselben Wert abgebildet. Das Urbild ist also nicht eindeutig, denn $f^{-1}(4) = \{-2, 2\}$ enthält zwei Elemente.

Kombinatorik In der Kombinatorik beschäftigt man sich mit Abzählproblemen, wie sie bspw. bei der Wahrscheinlichkeitsanalyse von Glücksspielen auftreten. Dabei soll eine Anzahl möglicher Anordnungen oder Auswahlen von Objekten bestimmt werden. Ein bekanntes Beispiel ist Lotto, das bei uns in Deutschland auch 6-aus-49 genannt wird. Wie viele Möglichkeiten

gibt es, 6 Kugeln aus einer Urne mit 49 verschiedenen Kugel auszuwählen, wobei die Kugeln nach einem Zug nicht zurückgelegt werden?

Sei $[n] := \{1, 2, 3, \ldots, n\}$ die Menge der ersten n natürlichen Zahlen. Wie viele Möglichkeiten gibt es, diese Zahlen (ohne Wiederholung) hintereinander zu schreiben? Für 4 Zahlen gibt es die folgenden Reihenfolgen:

$1,2,3,4$	$2,1,3,4$	$3,1,2,4$	$4,1,2,3$
$1,2,4,3$	$2,1,4,3$	$3,1,4,2$	$4,1,3,2$
$1,3,2,4$	$2,3,1,4$	$3,2,1,4$	$4,2,1,3$
$1,3,4,2$	$2,3,4,1$	$3,2,4,1$	$4,2,3,1$
$1,4,2,3$	$2,4,1,3$	$3,4,1,2$	$4,3,1,2$
$1,4,3,2$	$2,4,3,1$	$3,4,2,1$	$4,3,2,1$

Die erste Zahl kann auf n Positionen stehen, die zweite Zahl kann dann noch auf $n-1$ Positionen stehen, für die dritte Zahl verbleiben noch $n-2$ Positionen und so weiter. Es gibt also

$$n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 3 \cdot 2 \cdot 1 = n!$$

viele mögliche Reihenfolgen, die Zahlen aus $[n]$ ohne Wiederholung aufzuschreiben, für $n = 4$ also $4! = 24$ verschiedene Möglichkeiten.

Wie viele Möglichkeiten gibt es, k Zahlen aus $[n]$ auszuwählen und (ohne Wiederholung) hintereinander zu schreiben? Für $k = 2$ und $n = 4$ ergeben sich folgende Möglichkeiten:

$1,2$	$1,3$	$1,4$	$2,3$	$2,4$	$3,4$
$2,1$	$3,1$	$4,1$	$3,2$	$4,2$	$4,3$

Für die erste Zahl stehen n Zahlen zur Verfügung, für die zweite Zahl stehen nur noch $n-1$ Zahlen zur Verfügung, für die dritte Zahl nur noch $n-2$ Zahlen und so weiter. Wenn also k viele verschiedene Zahlen ausgewählt werden, gibt es

$$\begin{aligned} n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot (n-k+1) &= \frac{n \cdot (n-1) \cdots (n-k+1) \cdot \cancel{(n-k) \cdots 3 \cdot 2 \cdot 1}}{\cancel{(n-k) \cdots 3 \cdot 2 \cdot 1}} \\ &= \frac{n!}{(n-k)!} \end{aligned}$$

viele Möglichkeiten, k aus n Zahlen (ohne Wiederholung) hintereinander zu schreiben. Dies nennt man *Variationen ohne Wiederholung*. Im obigen Beispiel für $k = 2$ und $n = 4$ erhalten wir also $4!/(4-2)! = 24/2 = 12$ Variationen ohne Wiederholung.

Sind Wiederholungen erlaubt, dann spricht man von *Variationen mit Wiederholung*. Davon gibt es n^k viele, denn für die erste Position können n Werte gewählt werden, ebenso für die zweite Position und für jede weitere Position. Für $k = 2$ und $n = 4$ erhalten wir:

$1,1$	$2,1$	$3,1$	$4,1$
$1,2$	$2,2$	$3,2$	$4,2$
$1,3$	$2,3$	$3,3$	$4,3$
$1,4$	$2,4$	$3,4$	$4,4$

Wenn die Reihenfolge der k Zahlen keine Rolle spielt, so wie bei Mengen oder beim Lotto, dann müssen wir den obigen Bruch für die Anzahl der Variationen ohne Wiederholung noch durch $k!$ teilen, denn k viele Zahlen können auf $k!$ viele Weisen hintereinander geschrieben werden. Es gibt also

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

viele *Kombinationen ohne Wiederholung*, oder anders gesagt, es gibt $\binom{n}{k}$ viele k-elementige Teilmengen einer n-elementigen Menge. Wir hatten uns ja bereits überlegt, dass die Aufzählung der Elemente einer Menge in beliebiger Reihenfolge erfolgen kann.

Beispiel: Betrachten wir die Menge $[4] = \{1, 2, 3, 4\}$, dann gibt es

- $\binom{4}{0} = 1$ null-elementige Teilmenge: $\emptyset$
- $\binom{4}{1} = 4$ ein-elementige Teilmengen: $\{1\}$, $\{2\}$, $\{3\}$, $\{4\}$
- $\binom{4}{2} = 6$ zwei-elementige Teilmengen: $\{1, 2\}$, $\{1, 3\}$, $\{1, 4\}$, $\{2, 3\}$, $\{2, 4\}$, $\{3, 4\}$
- $\binom{4}{3} = 4$ drei-elementige Teilmengen: $\{1, 2, 3\}$, $\{1, 2, 4\}$, $\{1, 3, 4\}$, $\{2, 3, 4\}$
- $\binom{4}{4} = 1$ vier-elementige Teilmenge: $\{1, 2, 3, 4\}$

Da der Wert $\binom{n}{k}$ in der Mathematik sehr wichtig ist, hat er einen eigenen Namen bekommen, er heißt *Binomialkoeffizient* und wird als „n über k“ ausgesprochen. Beim Lotto, also bei 6-aus-49, gibt es

$$\binom{49}{6} = \frac{49!}{(49-6)! \cdot 6!} = \frac{49 \cdot 48 \cdot 47 \cdot 46 \cdot 45 \cdot 44}{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2} = 13.983.816$$

viele mögliche Kombinationen ohne Wiederholung.

Entgegen dem üblichen Sprachgebrauch spricht man in der Mathematik von Kombinationen, wenn die Reihenfolge der Werte keine Rolle spielt. Bei einem Tresor oder einem Zahlenschloss für das Fahrrad spricht man umgangssprachlich von Kombination, obwohl es im mathematischen Sinn eine Variation ist.

Zahlen Beschäftigen wir uns nun etwas mit Zahlen. Gerade Zahlen lassen sich ohne Rest durch zwei teilen, ungerade nicht. Für jede gerade Zahl $n \in \mathbb{N}$ existiert daher eine Zahl $k \in \mathbb{N}$ mit $n = 2 \cdot k$. Eine ungerade Zahl n lässt sich als $n = 2 \cdot k + 1$ für ein $k \in \mathbb{N}_0$ darstellen.

Der Fundamentalsatz der Zahlentheorie besagt, dass jede natürliche Zahl, die größer als eins ist, eine eindeutige Primfaktorzerlegung[4] hat. Beispiele: $18 = 2 \cdot 3^2$, $24 = 2^3 \cdot 3$ und $90 = 2 \cdot 3^2 \cdot 5$. Die Primfaktorzerlegung lässt sich als Produkt von Primzahlpotenzen schreiben.

Für zwei natürliche Zahlen $n, m \in \mathbb{N}$ definieren wir den *größten gemeinsamen Teiler* von m und n als

$$\text{ggT}(m, n) = \max\{k \mid k \text{ teilt } m \text{ und } k \text{ teilt } n\}$$

und das *kleinste gemeinsame Vielfache* von m und n als

$$\text{kgV}(m, n) = \min\{k \mid m \text{ teilt } k \text{ und } n \text{ teilt } k\}.$$

Die Primfaktorzerlegung von m und n ist hilfreich, um den größten gemeinsamen Teiler sowie das kleinste gemeinsame Vielfache zu berechnen. Beispiel: $n = 180 = 2^2 \cdot 3^2 \cdot 5^1 \cdot 7^0$ und $m = 294 = 2^1 \cdot 3^1 \cdot 5^0 \cdot 7^2$. Dann gilt:

$$\begin{aligned} \text{ggT}(m, n) &= 2^{\min\{2,1\}} \cdot 3^{\min\{2,1\}} \cdot 5^{\min\{1,0\}} \cdot 7^{\min\{0,2\}} = 6 \\ \text{kgV}(m, n) &= 2^{\max\{2,1\}} \cdot 3^{\max\{2,1\}} \cdot 5^{\max\{1,0\}} \cdot 7^{\max\{0,2\}} = 8.820 \end{aligned}$$

Da eine Primfaktorzerlegung bisher nur unter sehr hohem Aufwand berechnet werden kann, ist diese Methode nicht effizient. In der Mathematik-Vorlesung lernen Sie mit dem Euklidschen Algorithmus[5] eine effizientere Methode zum Bestimmen des ggT kennen.

[4] `https://de.wikipedia.org/wiki/Primfaktorzerlegung`
[5] `https://de.wikipedia.org/wiki/Euklidischer_Algorithmus`

Eine Summe[6] bezeichnet das Ergebnis einer Addition. Das große griechische Sigma Σ wird oft verwendet, um Folgen von Zahlen zu addieren. Es wird dann „Summenzeichen“ genannt. Dabei sind mehrere Schreibweisen möglich. Für die Menge $M = \{1, 2, 3, \ldots, 10\}$ sind bspw. die folgenden Schreibweisen äquivalent:

$$1 + 2 + 3 + \ldots + 10 = \sum_{i=1}^{10} i = \sum_{1 \leq k \leq 10} k = \sum_{e \in M} e$$

Die leere Summe hat den Wert 0 (das neutrale Element der Addition). Auch für das Produkt[7], dem Ergebnis einer Multiplikation, wird ein griechischer Buchstabe, das große Pi Π verwendet. So kann bspw. die Fakultät $n!$ einer natürlichen Zahl n geschrieben werden als

$$n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n = \prod_{i=1}^{n} i = \prod_{k \in \{1,2,3,\ldots,n\}} k$$

Das leere Produkt hat den Wert 1 (das neutrale Element der Multiplikation). Auch hier sind verschiedene Schreibweisen möglich. Schauen wir uns noch einmal die Primfaktorzerlegung von oben an. Sind die m verschiedenen Primfaktoren $p_1, \ldots, p_m$ einer natürlichen Zahl n aufsteigend geordnet ($p_i < p_{i+1}$), dann spricht man auch von der kanonischen Primfaktorzerlegung:

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_m^{e_m} = \prod_{i=1}^{m} p_i^{e_i}$$

Dabei bezeichnet der Exponent e_i die *Vielfachheit* von p_i. Er gibt an, wie oft die Zahl n durch p_i teilbar ist.

Zu einer reellen Zahl $x \in \mathbb{R}$ definieren wir wie folgt ganze Zahlen, die „nah“ an x liegen.

- $\lfloor x \rfloor$ bezeichnet die größte, ganze Zahl k, die kleiner oder gleich x ist. Die Zeichen $\lfloor\ \rfloor$ werden untere Gauß-Klammern genannt.

  Beispiele: $\lfloor 8,2 \rfloor = 8$, $\lfloor 6,99 \rfloor = 6$, $\lfloor -7,3 \rfloor = -8$

- $\lceil x \rceil$ bezeichnet die kleinste, ganze Zahl k, die größer oder gleich x ist. Die Zeichen $\lceil\ \rceil$ werden entsprechend als obere Gauß-Klammern bezeichnet.

  Beispiele: $\lceil 8,2 \rceil = 9$, $\lceil 6,01 \rceil = 7$, $\lceil -9,6 \rceil = -9$

Die Gauß-Klammern werden oft benötigt, wenn eine Position in einem Array berechnet werden soll, da der Index beim Array-Zugriff immer ganzzahlig sein muss. Anwendung bspw. bei der binären Suche oder der Interpolationssuche.

Schauen wir uns nun die Division zweier Zahlen an, speziell die Modulo-Operation:

- Für positive Werte n und m entspricht der Wert der Modulo-Operation dem Rest bei der ganzzahligen Division $n \div m$.
  - $n \bmod m = b$, sodass $0 \leq b < |m|$ und $m \cdot a + b = n$ gilt für ein $a \in \mathbb{Z}$.
  - Beispiel: $14 \bmod 3 = 2$, denn $14 \div 3 = 4$ Rest 2, oder entsprechend $3 \cdot 4 + 2 = 14$.

[6] `https://de.wikipedia.org/wiki/Summe`

[7] `https://de.wikipedia.org/wiki/Produkt_(Mathematik)`

- Für negative Werte n und m unterscheidet sich der „Rest der ganzzahligen Division“ von der Modulo-Operation. Wir betrachten hier nur negative Werte für n, der Wert m ist bei unseren Anwendungen eigentlich immer positiv.
  - $n \bmod m := n - m\lfloor \frac{n}{m} \rfloor$, für eine positive Zahl m ist der Rest also auch positiv.
  - Beispiel: $(-7) \bmod 4 = (-7) - 4 \cdot \lfloor \frac{-7}{4} \rfloor = (-7) - 4 \cdot (-2) = (-7) + 8 = 1$, oder anders ausgedrückt: $4 \cdot (-2) + 1 = (-7)$

Die Modulo-Operation wird oft benötigt, wenn eine Position in einem Array berechnet werden soll, da der Index beim Array-Zugriff nicht negativ sein darf. Anwendung bspw. bei Hash-Tabellen und Interpolationssuche.

Die Modulo-Operation steht in C/C++ nicht direkt zur Verfügung, wir können sie aber relativ einfach als Funktion implementieren:

```
1  #include <stdio.h>
2
3  int mod(int n, int m) {
4      int r = n % m;
5      return (r + m) % m;
6  }
7
8  int main(void) {
9      printf(" 9 %% 4= %3d,  9 mod 4= %3d\n", 9 % 4, mod(9, 4));
10     printf("-9 %% 4= %3d, -9 mod 4= %3d\n", -9 % 4, mod(-9, 4));
11     return 0;
12 }
```

Ausgabe:

```
 9 % 4=   1,  9 mod 4=   1
-9 % 4=  -1, -9 mod 4=   3
```

Eine andere Implementierung stellt der folgende Code-Ausschnitt dar.

```
1  int mod(int n, int m) {
2      int r = n % m;
3      if (r < 0)
4          r += m;
5      return r;
6  }
```

Mathematische Beweise Oft müssen irgendwelche Aussagen bewiesen werden, in ALD sind es meist Aussagen zur Laufzeit oder Korrektheit von Algorithmen. Schauen wir uns daher einige Beweismethoden[8] an, die in der Vorlesung ALD benötigt werden.

- **direkter Beweis:** Man nimmt einen bereits als richtig bewiesenen Satz A (Prämisse) und leitet, durch logische Schlussfolgerungen, daraus den zu beweisenden Satz B (Konklusion) ab: $A \Rightarrow X_1 \Rightarrow X_2 \Rightarrow \ldots \Rightarrow X_k \Rightarrow B$, wobei alle Folgerungen bzw. Implikationen wahr sein müssen.

[8] https://de.wikipedia.org/wiki/Beweis_(Mathematik).

Beispiel: Wir wollen zeigen, dass das Quadrat einer ungeraden natürlichen Zahl auch ungerade ist. Sei also n eine ungerade Zahl. Dann lässt sich n darstellen als $n = 2k + 1$, wobei $k \in \mathbb{N}_0$ eine natürliche Zahl ist. Aufgrund der ersten binomischen Formel

$$(a + b)^2 = a^2 + 2ab + b^2$$

gilt daher $n^2 = (2k + 1)^2 = (2k)^2 + 2 \cdot (2k) \cdot 1 + 1^2 = 4k^2 + 4k + 1 = 2 \cdot \underbrace{(2k^2 + 2k)}_{=k'} + 1$.

Also ist auch n^2 eine ungerade Zahl. Oder kürzer:

$$\begin{aligned} n \text{ ist ungerade} &\Rightarrow n = 2k + 1 \text{ für ein } k \in \mathbb{N}_0 \\ &\Rightarrow n^2 = (2k + 1)^2 = 2 \cdot (2k^2 + 2k) + 1 = 2k' + 1 \\ &\Rightarrow n^2 \text{ ist ungerade} \end{aligned}$$

Beispiel: Für die Binomialkoeffizienten gilt

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

Direkter Beweis für die erste Aussage über Binomialkoeffizienten:

$$\binom{n}{k} \overset{Def.}{=} \frac{n!}{(n-k)! \cdot k!} \overset{komm.}{=} \frac{n!}{k! \cdot (n-k)!} = \frac{n!}{\underbrace{(n-(n-k))}_{=k}! \cdot (n-k)!} \overset{Def.}{=} \binom{n}{n-k}$$

Direkter Beweis für die zweite Aussage über Binomialkoeffizienten:

$$\begin{aligned} &\binom{n}{k-1} + \binom{n}{k} \overset{Def.}{=} \frac{n!}{(n-(k-1))! \cdot (k-1)!} + \frac{n!}{(n-k)! \cdot k!} \\ &= \frac{n! \cdot k}{(n-k+1)! \cdot \underbrace{(k-1)! \cdot k}_{=k!}} + \frac{n! \cdot (n-k+1)}{\underbrace{(n-k)! \cdot (n-k+1)}_{=(n-k+1)!} \cdot k!} \qquad \text{(Hauptnenner)} \\ &= \frac{n! \cdot k + n! \cdot (n-k+1)}{(n-k+1)! \cdot k!} = \frac{n! \cdot [k + (n-k+1)]}{(n-k+1)! \cdot k!} = \frac{n! \cdot (n+1)}{(n-k+1)! \cdot k!} \\ &= \frac{(n+1)!}{(n+1-k)! \cdot k!} \overset{Def.}{=} \binom{n+1}{k} \end{aligned}$$

- **indirekter Beweis:** Aus der Aussagenlogik wissen wir, dass die Implikation $A \Rightarrow B$ äquivalent zu $\neg B \Rightarrow \neg A$ ist, wie man sich auch anhand der folgenden Wertetafeln klar machen kann.

A	B	$A \Rightarrow B$
0	0	1
0	1	1
1	0	0
1	1	1

$\neg B$	$\neg A$	$\neg B \Rightarrow \neg A$
1	1	1
0	1	1
1	0	0
0	0	1

Anstatt $A \Rightarrow B$ zu zeigen, können wir also genauso gut die Kontraposition $\neg B \Rightarrow \neg A$ zeigen. (Man nennt indirekte Beweise daher oft auch Beweis durch Kontraposition.)

Beispiel: Wir wollen zeigen, dass für alle natürlichen Zahlen $n \in \mathbb{N}$ gilt, dass n gerade ist, wenn n^2 gerade ist. Sei also $A :=$ (n^2 ist gerade) und $B :=$ (n ist gerade). Dann ist also $A \Rightarrow B$ zu zeigen. Stattdessen zeigen wir

$$\neg B = (n \text{ ist ungerade}) \;\Rightarrow\; \neg A = (n^2 \text{ ist ungerade}),$$

was wir oben bereits getan haben.

- **Beweis durch Widerspruch:** Wir wollen wieder etwas in der Art $A \Rightarrow B$ zeigen. In der klassischen zweiwertigen Logik wissen wir, dass nicht gleichzeitig B und $\neg B$ gelten kann. Wir nehmen daher an, dass A gilt, aber B nicht, oder als Formel $A \wedge \neg B$. Dies müssen wir durch logische Schlüsse zu einem Widerspruch führen, da genau dieser Fall laut obiger Wertetafel für die Implikation $A \Rightarrow B$ nicht gelten darf. Wir zeigen also:

  $$(A \wedge \neg B) \Rightarrow C_1 \Rightarrow C_2 \Rightarrow \ldots \Rightarrow C_k \Rightarrow \lightning$$

  Bevor wir uns ein Beispiel aus der Mathematik anschauen, machen wir uns klar, das in vielen Krimiserien genau dieses Prinzip angewendet wird. Nehmen wir an, jemand wird verdächtigt, eine Straftat zu einer bestimmten Zeit an einem bestimmten Ort begangen zu haben. Wenn nun der Verdächtige Zeugen nennen kann, die nachweisen, dass der Verdächtigte zu der Zeit an einem anderen Ort mit den Zeugen zusammen war, dann kann der Verdacht nicht stimmen. Das Alibi hat den Verdächtigten entlastet und gezeigt, dass der Verdächtige nicht als Täter in Frage kommt. Niemand kann zur gleichen Zeit an zwei verschiedenen Orten sein, Widerspruch!

  Beispiel: Für jede Primzahl p ist $\sqrt{p}$ keine rationale Zahl. Sei $A :=$ (n ist prim) und $B :=$ ($\sqrt{n}$ ist keine rationale Zahl), dann wollen wir $A \Rightarrow B$ zeigen. Allerdings tun wir das nicht direkt, sondern wir führen $A \wedge \neg B$ zu einem Widerspruch.

  Angenommen, die Zahl $\sqrt{p}$ ist rational. Dann können wir $\sqrt{p} = {}^{a}\!/_{b}$ als Bruch darstellen. Dabei seien $a, b \in \mathbb{N}$ teilerfremd, der Bruch kann also nicht mehr gekürzt werden. Dann gilt $\sqrt{p}^2 = p = ({}^{a}\!/_{b})^2 = {}^{a^2}\!/_{b^2}$, also $p \cdot b^2 = a^2$.

  Der Fundamentalsatz der Zahlentheorie besagt, dass jede natürliche Zahl eine eindeutige Primfaktorzerlegung hat. Bei der Primfaktorzerlegung von a^2 sind alle Exponenten gerade, wohingegen auf der linken Seite der Gleichung der Primfaktor p einen ungeraden Exponenten hat. $\lightning$

- **Vollständige Induktion:** Wird oft angewendet, wenn man Aussagen der Form „Für jede natürliche Zahl n gilt ...“ zeigen will. Man zeigt zunächst, dass die Aussage für einen Anfangswert $n_0 \in \mathbb{N}$ gilt, und danach, dass sie immer auch für $n+1$ gilt, wenn sie für ein $n \geq n_0$ gilt. Wir müssen also zeigen: Wenn $A(n)$ für ein beliebiges n gilt, dann gilt auch $A(n+1)$. Damit erhalten wir folgende „Kette“ von Implikationen:

  $$A(n_0) \Rightarrow A(n_0+1) \Rightarrow A(n_0+2) \Rightarrow A(n_0+3) \Rightarrow \ldots$$

  Die vollständige Induktion lässt sich mit einem Domino-Effekt veranschaulichen. Man stellt die Domino-Steine so auf, dass, wenn einer umfällt, auch immer der nächste umfällt ($n \to n+1$), und stößt den ersten Stein um ($n = n_0$).

  Beispiel: Die Summe der ersten n natürlichen Zahlen $\sum_{i=1}^{n} i$ ist gleich ${}^{n(n+1)}\!/_{2}$.

  - Induktionsanfang für $n = 1$: $\sum_{i=1}^{1} i = 1 = {}^{1 \cdot 2}\!/_{2}$ ist eine wahre Aussage. ✓
  - Induktionsvoraussetzung: Wir setzen voraus, dass die Behauptung für ein beliebiges, aber fest gewähltes $n \geq n_0$ gültig ist, es gilt also $\sum_{i=1}^{n} i = {}^{n(n+1)}\!/_{2}$ für ein n.
  - Induktionsschluss: Da die Behauptung für n korrekt ist, gilt

    $$\begin{aligned}\sum_{i=1}^{n+1} i &= \sum_{i=1}^{n} i + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \\ &= \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2} = \frac{(n+1) \cdot ((n+1)+1)}{2}\end{aligned}$$

    und daher gilt die Aussage auch für $n+1$.

Der Vollständigkeit halber wollen wir darauf hinweisen, dass im Allgemeinen ein Beispiel kein Beweis ist. Die Aussage „Alle ungeraden Zahlen sind Primzahlen“ kann also nicht mit den Beispielen 3, 5 und 7 bewiesen werden, denn für 9 gilt die Aussage nicht. Manchmal, nämlich bei Existenzaussagen, kann eine Aussage durch ein Beispiel gezeigt werden: Es gibt eine gerade Primzahl, nämlich die Zahl 2.

Aufgabe 0-1: Zeigen Sie durch einen direkten Beweis:

(a) Die Summe zweier ungerader Zahlen ist stets gerade.

(b) Jede ganze Zahl, deren letzte Dezimalstelle eine 5 ist, ist durch 5 teilbar.

(c) Ist a ein Teiler von b und b ein Teiler von c, dann ist auch a ein Teiler von c.

(d) Für je zwei rationale Zahlen $a, b \in \mathbb{Q}$ mit $a < b$ gibt es eine rationale Zahl $c \in \mathbb{Q}$, sodass $a < c < b$ gilt.

(e) Für jede natürliche Zahl $n \in \mathbb{N}$ gilt: $n + (n+1) + (n+2)$ ist durch drei teilbar.

Aufgabe 0-2: Zeigen Sie durch einen indirekten Beweis:

(a) Seien $a, b, c \in \mathbb{Z}$ und $a \neq b$. Dann gilt $a + c \neq b + c$.

(b) Wenn eine Zahl $n \in \mathbb{Z}$ nicht durch 2 oder 5 teilbar ist, dann ist sie auch nicht durch 10 teilbar.

Aufgabe 0-3: Zeigen Sie durch einen Widerspruchsbeweis:

(a) Wenn n^3 eine gerade Zahl ist, dann ist auch n eine gerade Zahl.

(b) Es gibt unendlich viele Primzahlen.

Aufgabe 0-4: Zeigen Sie mittels vollständiger Induktion, dass für jede natürliche Zahl n gilt:

(a) $\sum_{i=0}^{n} 2i + 1 = (n+1)^2$
Beispiel: $\sum_{i=0}^{3} 2i + 1 = 1 + 3 + 5 + 7 = 16 = 4^2$

(b) $\sum_{i=0}^{n} i^2 = 1/6 \cdot n \cdot (n+1) \cdot (2n+1)$
Beispiel: $\sum_{i=0}^{3} i^2 = 0^2 + 1^2 + 2^2 + 3^2 = 0 + 1 + 4 + 9 = 14 = 1/6 \cdot 3 \cdot 4 \cdot 7 = 84/6$

(c) $n! > 2^n$ für $n \in \mathbb{N}$ und $n \geq 4$.

(d) Für $n \in \mathbb{N}$ und $x \in \mathbb{R}$, $x > -1$ gilt $(1+x)^n \geq 1 + nx$. (Bernoulli-Ungleichung)

(e) Jede natürliche Zahl $n = 5^k + 7$ mit $k \in \mathbb{N}_0$ ist durch 4 teilbar.

(f) Zeigen Sie, dass die binomische Formel $(a+b)^2 = a^2 + 2ab + b^2$ verallgemeinert werden kann zu

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

Wie könnte ein direkter Beweis aussehen?

Aufgabe 0-5: Zeigen Sie, dass für zwei natürliche Zahlen $m, n \in \mathbb{N}$ gilt:

$$m \cdot n = \mathrm{ggT}(m, n) \cdot \mathrm{kgV}(m, n)$$

Beispiel: Für $m = 180$ und $n = 294$ hatten wir oben festgestellt, dass $\mathrm{ggT}(m, n) = 6$ und $\mathrm{kgV}(m, n) = 8.820$ gilt. Daher erhalten wir $m \cdot n = 180 \cdot 294 = 52.920 = 6 \cdot 8.820$.