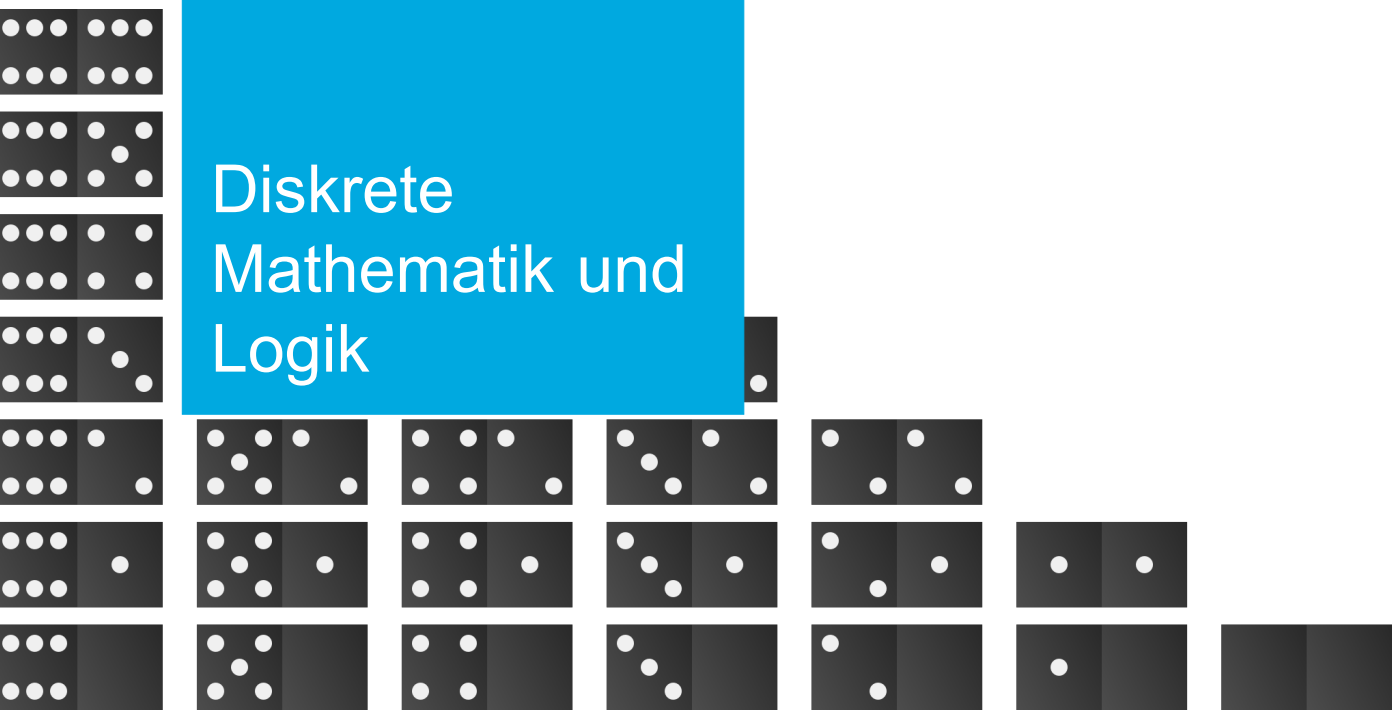
Universität Konstanz

09.02.2023

Diskrete Mathematik und Logik



Sven Kosub

Vorlesungsskriptum für das Wintersemester 2022/23 – Version: 5.21

Inhaltsverzeichnis

1 Mathematische Konstruktionen

1.1 Zuweisung

Die Zuweisung ist die Standardform der Nominaldefinition in der Mathematik. Dabei wird die linke Seite durch die rechte Seite definiert, schematisch:

$$x =_{\text{def}} y$$

Die linke Seite x wird als Name oder Abkürzung für die üblicherweise komplizierte, rechte Seite y eingeführt. Beide Seiten x und y dürfen in Beweisen, Rechnungen oder Umformungen beliebig gegeneinander ausgetauscht werden.

Beispiele: Folgende Definitionen sind Beispiele für Zuweisungen:

- $x =_{\text{def}} 2$
- $x =_{\text{def}} 2n + 1$
- $f(x) =_{\text{def}} x^2$
- $p \mid q \iff_{\text{def}}$ es gibt eine ganze Zahl k mit $q = k \cdot p$

Im Gegensatz zur Definition „$x =_{\text{def}} y$“ behauptet der Ausdruck „$x = y$“ eine Gleichheit, wofür eine Begründung nötig ist.

1.2 Iteration

Die iterative Definitionsform dient zum Ausdrücken von Wiederholungen in variablen, aber bestimmten Grenzen. Typische Anwendungen finden sich in Summen- oder Produktdefinitionen:

$$\sum_{k=1}^{n} a_k \quad =_{\text{def}} \quad a_1 + a_2 + \cdots + a_n$$
$$\prod_{k=1}^{n} a_k \quad =_{\text{def}} \quad a_1 \cdot a_2 \cdot \cdots \cdot a_n$$

Iterationen entsprechen `for`-Schleifen in Programmiersprachen.

Beispiel: Die Fakultätsfunktion ist für alle natürlichen Zahlen n definiert als

$$n! =_{\text{def}} \prod_{k=1}^{n} k \quad \text{für } n > 0, \qquad 0! =_{\text{def}} 1.$$

Ein Code-Fragment in Java sieht wie folgt aus:

```
int h=1;
for (int k=1; k<=n; k++) h=h*k;
```

Der Index k in der Produktdefinition übernimmt die Rolle der Laufvariable.

Ein typisches Problem bei iterativen Definitionen ist das Finden wertgleicher Ausdrücke ohne Verwendung der Laufvariable k (explizite Darstellung).

Beispiel: $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ für alle natürlichen Zahlen n.

1.3 Rekursion

Bei der rekursiven Definitionsform darf die definierte Seite (linke Seite) auf der definierenden Seite (rechte Seite) vorkommen (auch mehrmals):

$$x =_{\text{def}} \ldots x \ldots$$

Da x wieder auf der rechten Seite eingesetzt werden kann, ergeben sich Schachtelungen:

$$x, \quad \ldots x \ldots, \quad \ldots (\ldots x \ldots) \ldots, \quad \ldots (\ldots (\ldots x \ldots) \ldots) \ldots, \quad \text{usw. usf.}$$

Für den Auschluss unendlicher Schachtelungen müssen Abbruchbedingungen festgelegt werden.

Beispiele: Einige Beispiele für rekursive Definitionen sind folgende:

- Die Fakultätsfunktion kann ebenfalls rekursiv definiert werden:

  $$n! =_{\text{def}} n \cdot (n-1)!, \quad 0! =_{\text{def}} 1$$

  Die rekursive Form wird bestimmt durch die Verwendung des Symbols !, das auf beiden Seiten der Definition vorkommt. Man könnte abweichend von der üblichen mathematischen Notation auch $\mathsf{fak}(n) =_{\text{def}} n \cdot \mathsf{fak}(n-1)$ und $\mathsf{fak}(0) =_{\text{def}} 1$ definieren.
  Durch wiederholtes Einsetzen der Definition erhalten wir beispielsweise

  $$4! = 4 \cdot 3! = 12 \cdot 2! = 24 \cdot 1! = 24 \cdot 0! = 24.$$

- Die Folge der Fibonacci-Zahlen ist wie folgt rekursiv definiert:

  $$F_n =_{\text{def}} F_{n-1} + F_{n-2} \quad \text{fr } n \geq 2, \quad F_1 =_{\text{def}} 1, \quad F_0 =_{\text{def}} 0$$

  Beispielsweise ergibt sich:

  $$\begin{aligned} F_5 &= F_4 + F_3 \\ &= F_3 + F_2 + F_2 + F_1 \\ &= F_2 + F_1 + F_1 + F_0 + F_1 + F_0 + F_1 \\ &= F_1 + F_0 + F_1 + F_1 + F_0 + F_1 + F_0 + F_1 \\ &= 5 \cdot F_1 + 3 \cdot F_0 \\ &= 5 \end{aligned}$$

- Eine in der Berechenbarkeitstheorie prominente Funktion ist die Ackermann-Funktion $A(x, y)$, die für natürliche Zahlen x und y durch folgende kompliziertere rekursive Definition gegeben ist:

  $$\begin{array}{lll} A(0,y) =_{\text{def}} & y+1 & \\ A(x,0) =_{\text{def}} & x & \text{falls } x \geq 1 \\ A(x,y) =_{\text{def}} & A(x-1, A(x, y-1)) & \text{falls } x \geq 1, y \geq 1 \end{array}$$

  Beispielsweise ergibt sich:

  $$A(1,y) = A(0, A(1, y-1)) = A(1, y-1) + 1 = \cdots = A(1,0) + y = y + 1$$

Typische Probleme bei rekursiven Definitionen sind zum einen der Nachweis der Terminierung, die nicht immer offensichtlich sein muss, und zum anderen die Auflösung oder Abschätzung der rekursiven Definition, d.h. das Finden einer äquivalenten oder näherungsweise äquivalenten Definition, bei der die linke Seite nicht mehr auf der rechten Seite vorkommt.

Beispiel: Für die oben rekursiv definierten Funktionen ergeben sich beispielsweise folgende Ungleichungen und Gleichungen:

- $\left(\frac{n}{2}\right)^{\frac{n}{2}} \leq n! \leq n^n$ für alle natürlichen Zahlen n.
- $F_n = \frac{1}{\sqrt{5}} \cdot \left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$ für alle natürlichen Zahlen n.
- $A(5,y) \geq \underbrace{2^{2^{2^{\cdot^{\cdot^{\cdot^2}}}}}}_{y-\text{mal}}$ für alle natürlichen Zahlen y.

1.4 Strukturelle Induktion

Während es bei der rekursiven Definition um das Zerlegen einer Größe geht, steht bei der induktiven Definition das Zusammensetzen von Größen aus kleineren im Vordergrund. Typische Anwendungen sind Konstruktionen von Mengen und Begriffsinstanzen. Die allgemeine Form der induktiven Definition einer Menge A ist durch folgendes Schema beschrieben:

1. Induktionsanfang: Lege die Basiselemente der Menge fest.
2. Induktionsschritt: Lege Operationen zur Konstruktion neuer Elemente der Menge aus bereits bestehenden Elementen fest.
3. Nichts sonst ist ein Element dieser Menge.

Beispiele: Folgende Mengendefinition sollen das Schema der induktiven Definition verdeutlichen:

- Die Menge der natürlichen Zahlen ist wie folgt induktiv definiert:
  1. Induktionsanfang: 0 ist eine natürliche Zahl.
  2. Induktionsschritt: Ist n eine natürliche Zahl, so ist auch $n+1$ (Inkrementierung von n) eine natürliche Zahl.
  3. Nichts sonst ist eine natürliche Zahl.
- Die Menge der korrekten Klammerausdrücke, d.h. der endlichen Folgen von Symbolen (oder), ist wie folgt induktiv definiert:
  1. Induktionsanfang: () ist ein korrekter Klammerausdruck.
  2. Induktionsschritt: Sind H_1 und H_2 korrekte Klammerausdrücke, so sind auch (H_1) (Einklammerung von H_1) und H_1H_2 (Konkatenation von H_1 und H_2) korrekte Klammerausdrücke.
  3. Nichts sonst ist ein korrekter Klammerausdruck.

Suchbäume

Wir wollen an einem größeren Fallbeispiel das Zusammenwirken von induktivem Definieren und induktivem Beweisen, wie es bereits aus Beweisen mittels vollständiger Induktion von $n-1$ nach n bekannt ist, studieren. Eine für die Informatik sehr wichtige Datenstruktur sind Suchbäume. Suchbäume dienen der Suche nach Elementen (Schlüssel) in einer geordneten, variablen Menge (Wörterbuch) mittels binärer Suche.

Die zugrunde liegenden kombinatorischen Strukturen sind volle, gewurzelte Binarbäume, die eine Verallgemeinerung von Listen darstellen. In einer Liste hat jedes Element bis auf das letzte genau einen Nachfolger und jedes Element bis auf das erste genau einen Vorgänger. Verlangt man nur die Eigenschaft, dass jedes Element bis auf eines genau einen Vorgänger besitzt (und Kreise ausgeschlossen werden), gelangt man zu Bäumen. Eine Sonderklasse von Bäumen sind volle, gewurzelte Binärbäume. Ein voller, gewurzelter Binärbaum besteht aus Knoten und Kanten, die Knoten mittels eines Pfeils $\rightarrow$ geordnet verknüpfen, sowie einem ausgezeichneten Knoten r als der Wurzel des Baumes.

Formal ist ein voller, gewurzelter Binärbaum T zunächst einmal ein Tripel (V, E, r), wobei V die Menge der Knoten (die durch natürliche Zahlen beschrieben werden) und E die Menge der Kanten (d.h., Paare (u, v) von Knoten aus V mit $u \rightarrow v$) bezeichnen sowie $r \in V$ gilt. Die interne Struktur der Kantenmenge ist damit noch nicht festgelegt. Dies geschieht induktiv durch das Einhängen zweier Bäume unter eine gemeinsame neue Wurzel:

1. Induktionsanfang: Für jede natürliche Zahl r ist der Knoten r ein voller, gewurzelter Binärbaum.

   Formal: $(\{r\}, \emptyset, r)$ ist ein voller, gewurzelter Binärbaum.

2. Induktionsschritt: Sind T_1 und T_2 volle gewurzelte Binärbäume mit den Wurzeln r_1 und r_2 (alle Knoten seien paarweise verschieden), so ist die Kollektion der Knoten und Kanten von T_1 und T_2 sowie den neuen Kanten $r \rightarrow r_1$ und $r \rightarrow r_2$ mit der neuen Wurzel $r \neq r_1, r_2$ ein voller, gewurzelter Binärbaum.

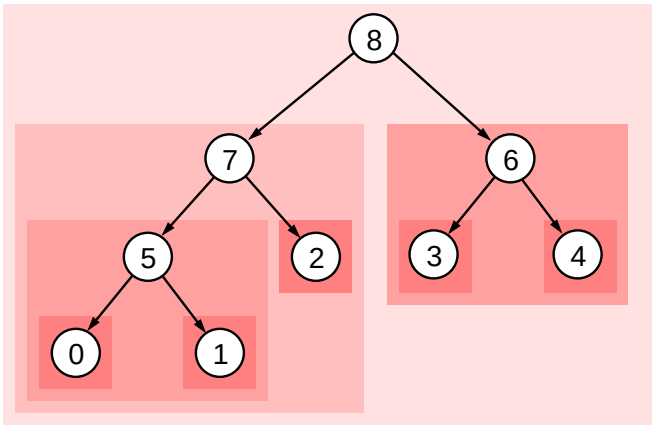
   Formal: Sind $T_1 = (V_1, E_1, r_1)$ und $T_2 = (V_2, E_2, r_2)$ volle, gewurzelte Binärbäume mit $V_1 \cap V_2 = \emptyset$ und ist $r \notin V_1 \cup V_2$, so ist

   $$f(T_1, T_2, r) =_{\text{def}} (\{V_1 \cup V_2 \cup \{r\}, E_1 \cup E_2 \cup \{(r, r_1), (r, r_2)\}, r)$$

   ein voller, gewurzelter Binärbaum.

3. Nichts sonst ist ein voller, gewurzelter Binärbaum.

Beispielsweise lässt sich folgender Baum mit der angegebenen Operation (formal beschrieben durch die Funktion f) konstruieren:



Entlang der induktiven Definition können nun Eigenschaften, die für alle vollen, gewurzelten Binärbäum gelten, bewiesen werden. Für eine beispielhafte Eigenschaft führen wir noch zwei Begriffe ein. Es sei $T = (V, E, r)$ ein voller, gewurzelter Binärbaum. Ein Knoten $v \in V$ heißt Blatt (bzw. Blattknoten), falls es kein $u \in V$ mit $(v, u) \in E$ gibt; sonst heißt v innerer Knoten. Blätter sind also

Knoten ohne ausgehende Kanten; alle anderen Knoten sind innere Knoten.

Proposition 1.1

Für einen vollen, gewurzelten Binärbaum T seien n_T die Anzahl innerer Knoten und m_T die Anzahl der Blätter. Dann gilt stets $n_T = m_T - 1$.

Beweis: (Induktion über den Aufbau der Bäume) Es sei T ein beliebiger voller, gewurzelter Binärbaum.

- Induktionsanfang: Besteht T aus nur einem Knoten r, d.h. $T = (\{r\}, \emptyset, r)$, so gilt $n_T = 0$ und $m_T = 1$.
- Induktionsschritt: Besteht T aus mehr als einem Knoten, so ist T aus zwei geeigneten Bäumen T_1 und T_2 mit den Wurzeln r_1 und r_2 zusammengesetzt, d.h. $T = f(T_1, T_2, r)$ für geeignete Bäume $T_1 = (V_1, E_1, r_1)$ und $T_2 = (V_2, E_2, r_2)$ mit $V_1 \cap V_2 = \emptyset$ und $r \notin V_1 \cup V_2$. Insbesondere gilt, dass die Blätter bzw. inneren Knoten von T_1 und T_2 auch Blätter bzw. innere Knoten von T sind, da in T nur die Paare (r, r_1) und (r, r_2) hinzukommen. Mithin folgt:

$$\begin{aligned} n_T &= n_{T_1} + n_{T_2} + 1 && (r \text{ ist ein innerer Knoten von } T) \\ &= (m_{T_1} - 1) + (m_{T_2} - 1) + 1 && (\text{nach Induktionsvoraussetzung}) \\ &= (m_{T_1} + m_{T_2}) - 1 \\ &= m_T - 1 \end{aligned}$$

Damit ist die Proposition bewiesen. ■

Vollständige Induktion

Ein Spezialfall des induktiven Beweisens ist der Beweis entlang der Struktur der natürlichen Zahlen: der Beweis mittels vollständiger Induktion von $n-1$ nach n gemäß obiger induktiver Definition der natürlichen Zahlen. Da die Menge der natürlichen Zahlen auf unterschiedliche Art und Weise induktiv definiert werden kann, ergeben sich mit anderen induktiven Definitionen auch jeweils andere Formen der Induktion. Wir werden in einem späteren Abschnitt noch einmal darauf zurückkommen.

Wir wollen beispielhaft eine vollständige Induktion von $n-1$ nach n durchführen.

Tipp!

Gewöhnen Sie sich an, **Beweise mit vollständiger Induktion immer nach** n (nicht nach $n+1$) zu führen. Damit vermeiden Sie eine häufige Fehlerquelle bei komplexeren Induktionsbeweisen.

Proposition 1.2

Für alle natürlichen Zahlen n gilt

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

Beweis: (Induktion) Wir führen einen Beweis mittels vollständiger Induktion von $n-1$ nach n.

- Induktionsanfang $n = 0$: $\sum_{k=0}^{0}(-1)^k \cdot k^2 = (-1)^0 \cdot 0^2 = 0 = (-1)^0 \cdot \frac{0(0+1)}{2}$.
- Induktionsschritt $n > 0$: Es gilt also $n = (n-1)+1$. Wir nehmen an, die Aussage gilt bereits für $n-1$ (Induktionsvoraussetzung). Somit gilt

$$\begin{aligned}
\sum_{k=0}^{n}(-1)^k \cdot k^2 &= (-1)^n \cdot n^2 + \sum_{k=0}^{n-1}(-1)^k \cdot k^2 \\
&= (-1)^n \cdot n^2 + (-1)^{n-1} \cdot \frac{(n-1)n}{2} \quad \text{(nach Induktionsvoraussetzung)} \\
&= (-1)^n \cdot \left(n^2 - \frac{(n-1)n}{2}\right) \\
&= (-1)^n \cdot \frac{n(n+1)}{2}
\end{aligned}$$

Damit ist die Proposition bewiesen. ■

2 Elementare Logik

2.1 Aussagen

Definition 2.1

Eine (mathematische) Aussage ist ein sprachlicher Ausdruck (Satz), dem eindeutig einer der Wahrheitswerte „wahr“ oder „falsch“ zugeordnet werden kann.

Wir werden Aussagen mit großen Buchstaben bezeichnen und wie folgt beschreiben:

$$X =_{\text{def}} \text{ Beschreibung}$$

Beispiele: Die folgenden Beispiele verdeutlichen die obige Begriffsbildung:

- $A =_{\text{def}}$ „Zu jeder natürlichen Zahl gibt es eine Primzahl, die größer ist“ ist eine wahre Aussage.
- $B =_{\text{def}}$ „Zu jeder natürlichen Zahl gibt es eine Primzahl, die kleiner ist“ ist eine falsche Aussage, da die Zahl 2 ein Gegenbeispiel ist.
- $C =_{\text{def}}$ „Jede gerade Zahl, die größer als 2 ist, ist die Summe zweier Primzahlen“ ist eine Aussage, da der Satz entweder gültig oder nicht gültig ist. Der Wahrheitswert ist noch offen; bei der Aussage handelt es sich um die bekannte Goldbachsche Vermutung.
- $D =_{\text{def}}$ „Diese Aussage ist falsch“ ist keine Aussage, da kein Wahrheitswert zugeordnet werden kann: Ist D wahr, dann ist D falsch; ist D falsch, dann ist D wahr.

2.2 Logische Verknüpfungen

Aussagen können mittels logischer Operationen verknüpft werden. Dadurch entstehen wiederum Aussagen. Unverknüpfte Aussagen heißen Elementaraussagen oder auch, wenn der operationale bzw. funktionale Aspekt hervorgehoben werden soll, aussagenlogische Variablen; verknüpfte Aussagen heißen zusammengesetzte Aussagen oder auch, wenn der operationale bzw. funktionale Aspekt hervorgehoben werden soll, aussagenlogische Formeln.

Im Folgenden wollen wir die Menge der aussagenlogischen Formeln mit Hilfe der gängigsten logischen Verknüpfungen induktiv definieren.

Definition 2.2 (Syntax aussagenlogischer Formeln)

Es seien $X_1, X_2, \ldots$ aussagenlogische Variablen.

1. Induktionsanfang (Elementaraussagen): $X_i, \mathsf{f}, \mathsf{w}$ sind aussagenlogische Formeln.
2. Induktionsschritt (zusammengesetzte Aussagen): Sind A, B aussagenlogische Formeln, so sind auch

$(\neg A)$	(gelesen: „nicht A“)	Negation
$(A \wedge B)$	(gelesen: „A und B“)	Konjunktion
$(A \vee B)$	(gelesen: „A oder B“)	Disjunktion
$(A \rightarrow B)$	(gelesen: „wenn A, dann B“)	Implikation
$(A \leftrightarrow B)$	(gelesen: „genau dann A, wenn B“)	Äquivalenz
$(A \oplus B)$	(gelesen: „entweder A oder B“)	Antivalenz

   aussagenlogische Formeln.
3. Nichts sonst ist eine aussagenlogische Formel.

Einige Anmerkungen zur Definition sind hilfreich:

1. Außer $\rightarrow, \leftrightarrow$ werden auch oft $\Rightarrow, \Leftrightarrow$ für die Implikation und Äquivalenz verwendet. Es empfiehlt sich jedoch, zur Definition von Formeln diese Symbole nicht zu verwenden. Insbesondere wenn wir Aussagen über aussagenlogische Formeln treffen oder beweisen wollen, ist es wichtig, die logischen Ebenen getrennt zu halten.
2. Äußere Klammern werden üblicherweise weggelassen, d.h., wir schreiben beispielsweise $X_1 \vee X_2$ statt $(X_1 \vee X_2)$.
3. Ähnlich der Addition und Multiplikation („Punktrechnung geht vor Strichrechnung“) gibt es Bindungsregeln bei der Verwendung der logischen Verknüpfungen, um die Klammerungen in zusammengesetzten Ausdrücken wegzulassen. Für die gebräuchlichsten Verknüpfungen $\neg, \wedge$ und $\vee$ vereinbaren wir: „$\neg$ geht vor $\wedge$“ und „$\wedge$ geht vor $\vee$“. Zum Beispiel ist die Aussage $\neg X_1 \wedge X_2 \vee X_3$ die gleiche Aussage wie $((\neg X_1) \wedge X_2) \vee X_3$. Um Missverständnissen in komplizierteren Zusammenhängen vorzubeugen, werden wir jedoch auch weiterhin Klammern setzen, wo sie eigentlich nach den Bindungsregeln nicht notwendig wären.

Im Folgenden definieren wir die Wahrheitswerte bzw. die Bedeutung oder Semantik von aussagenlogischen Formeln. Eine Interpretation I ist eine Belegung aller Variablen X_i mit genau einem Wert 0 oder 1. Wir erweitern Interpretationen auf aussagenlogische Formeln induktiv über deren Aufbau.

Definition 2.3 (Semantik aussagenlogischer Formel)

Es sei I eine Interpretation. Für eine aussagenlogische Formel H ist $I(H)$ wie folgt definiert:

1. Induktionsanfang (Elementaraussagen):

   Ist $H = X_i$, so ist $I(H) =_{\text{def}} I(X_i)$.
   Ist $H = \mathsf{f}$, so ist $I(H) =_{\text{def}} 0$.
   Ist $H = \mathsf{w}$, so ist $I(H) =_{\text{def}} 1$.

2. Induktionsschritt (zusammengesetzte Aussagen):

   Ist $H = (\neg A)$, so ist $I(H) =_{\text{def}} 1 - I(A)$
   Ist $H = (A \wedge B)$, so ist $I(H) =_{\text{def}} \min\{I(A), I(B)\}$
   Ist $H = (A \vee B)$, so ist $I(H) =_{\text{def}} \max\{I(A), I(B)\}$
   Ist $H = (A \rightarrow B)$, so ist $I(H) =_{\text{def}} \begin{cases} 1 & \text{falls } I(A) \leq I(B) \\ 0 & \text{sonst} \end{cases}$
   Ist $H = (A \leftrightarrow B)$, so ist $I(H) =_{\text{def}} \begin{cases} 1 & \text{falls } I(A) = I(B) \\ 0 & \text{sonst} \end{cases}$
   Ist $H = (A \oplus B)$, so ist $I(H) =_{\text{def}} \begin{cases} 1 & \text{falls } I(A) \neq I(B) \\ 0 & \text{sonst} \end{cases}$

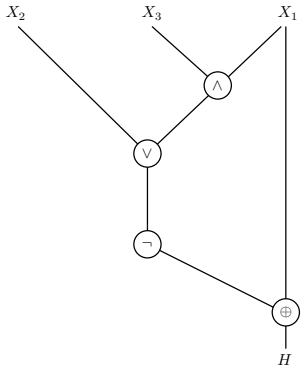
Eine Aussage H heißt genau dann wahr, wenn $I(H) = 1$ gilt.

Die Wahrheitswerte der durch logische Verknüpfungen entstandenen zusammengesetzten Aussagen können auch durch Wertetabellen definiert werden. Die in Definition 2.3 angegebenen Formeln können leicht aus den folgenden Wertetabellen abgelesen werden:

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \rightarrow B$	$A \leftrightarrow B$	$A \oplus B$	–
0	0	1	0	0	1	1	0	1
0	1	1	0	1	1	0	1	1
1	0	0	0	1	0	0	1	1
1	1	0	1	1	1	1	0	0
Funktionsname		NOT	AND	OR	–	–	XOR	NAND

Bei digitalen Schaltungen entsprechen diese Wertetabellen den booleschen Funktionen. Die Namen der den Verknüpfungen zugehörigen booleschen Funktionen sind in der untersten Zeile angegeben.

Beispiel: Der Ausdruck $H =_{\text{def}} X_1 \oplus \neg(X_2 \vee (X_3 \wedge X_1))$ ist eine aussagenlogische Formel (mit den aussagenlogischen Variablen X_1, X_2 und X_3) im Sinne von Definition 2.2. In der Tat ergibt sich der Aufbau von H über die folgenden aussagenlogischen (Teil)Formeln:



$$\begin{aligned} H_1 &=_{\text{def}} X_3 \wedge X_1 \\ H_2 &=_{\text{def}} X_2 \vee H_1 \\ H_3 &=_{\text{def}} \neg H_2 \\ H &=_{\text{def}} X_1 \oplus H_3 \end{aligned}$$

Die Abbildung auf der rechten Seite zeigt eine Darstellung von H als Schaltkreis (mit den Eingängen X_1, X_2 und X_3 und dem Ausgang H). Der Wahrheitswert von H hängt von einer gegebenen Belegung I für die in H vorkommenden aussagenlogischen Variablen ab. Es sei beispielsweise I wie folgt gegeben:

$$I(X_1) =_{\text{def}} 0, \qquad I(X_2) =_{\text{def}} 1, \qquad I(X_3) =_{\text{def}} 1$$

Dann ergibt sich für die Teilformeln H_1, H_2 und H_3

$$\begin{aligned} I(H_1) &= \min\{I(X_3), I(X_1)\} = \min\{1, 0\} = 0 \\ I(H_2) &= \max\{I(X_2), I(H_1)\} = \max\{1, 0\} = 1 \\ I(H_3) &= 1 - I(H_2) = 1 - 1 = 0 \end{aligned}$$

und somit $I(H) = 0$ wegen $I(X_1) = I(H_3) = 0$. Die folgende Wertetabelle fasst die Interpretation von H für alle Belegungen von X_1, X_2 und X_3 zusammen:

X_1	X_2	X_3	H_1	H_2	H_3	H
0	0	0	0	0	1	1
0	0	1	0	0	1	1
0	1	0	0	1	0	0
0	1	1	0	1	0	0
1	0	0	0	0	1	0
1	0	1	1	1	0	1
1	1	0	0	1	0	1
1	1	1	1	1	0	1

Eine Aussage H heißt genau dann wahr, wenn $I(H) = 1$. Die Wahrheit einer Aussage hängt stets Interpretationen ab. Je nachdem, wie viele erfüllende Interpretationen existieren, können einer

Aussage folgende Begriffe zugeordnet werden.

Definition 2.4

Es sei H eine aussagenlogische Formel.

1. H heißt genau dann erfüllbar, wenn $I(H) = 1$ für mindestens eine Belegung I gilt.
2. H heißt genau dann allgemeingültig (oder Tautologie), wenn $I(H) = 1$ für alle Belegungen I gilt.
3. H heißt genau dann widerlegbar, wenn $I(H) = 0$ für mindestens eine Belegung I gilt.
4. H heißt genau dann unerfüllbar (oder Kontradiktion), wenn $I(H) = 0$ für alle Belegungen I gilt.

Zwischen den einzelnen Erfüllbarkeitskonzepten bestehen offensichtliche Beziehungen.

Proposition 2.5

Es sei H eine Aussage.

1. Ist H allgemeingültig, so ist H erfüllbar.
2. H ist genau dann erfüllbar, wenn $\neg H$ widerlegbar ist.
3. H ist genau dann allgemeingültig, wenn $\neg H$ unerfüllbar ist.

Beispiele: Einige Beispiele sollen die Begriffsbildungen verdeutlichen (Begründungen mittels Wertetabelle):

- Die Elementaraussage w ist allgemeingültig; f ist unerfüllbar.
- $A \vee B$ ist erfüllbar und widerlegbar.
- $((A \to B) \to A) \wedge (\neg A)$ ist unerfüllbar.
- $(A \wedge (A \to B)) \to B$ ist allgemeingültig.

2.3 Rechnen mit logischen Verknüpfungen

Definition 2.6

Zwei Aussagen A und B heißen genau dann (logisch) äquivalent, symbolisch $A \equiv B$, wenn für alle Interpretationen I gilt $I(A) = I(B)$.

Mit anderen Worten: $A \equiv B \iff_{\text{def}} A \leftrightarrow B$ ist stets wahr.

Beispiel: Wir wollen uns davon überzeugen, dass die Aussagen $A \leftrightarrow (B \leftrightarrow C)$ und $(A \oplus B) \oplus C$ logisch äquivalent sind. Dazu betrachten wir die zusammengesetzten Aussagen:

$$H_1 =_{\text{def}} B \leftrightarrow C, \quad H_2 =_{\text{def}} A \leftrightarrow H_1, \qquad H_3 =_{\text{def}} A \oplus B, \quad H_4 =_{\text{def}} H_3 \oplus C$$

Letztlich muss also gezeigt werden, dass $H_2 \leftrightarrow H_4$ stets eine wahre Aussage ist. Wir bestimmen die zugehörige Wahrheitswerttabelle:

A	B	C	H_1	H_2	H_3	H_4	$H_2 \leftrightarrow H_4$
0	0	0	1	0	0	0	1
0	0	1	0	1	0	1	1
0	1	0	0	1	1	1	1
0	1	1	1	0	1	0	1
1	0	0	1	1	1	1	1
1	0	1	0	0	1	0	1
1	1	0	0	0	0	0	1
1	1	1	1	1	0	1	1

Mithin gilt also $A \leftrightarrow (B \leftrightarrow C) \equiv (A \oplus B) \oplus C$.

Logisch äquivalente Aussagen können in zusammengesetzten Aussagen beliebig gegeneinander ausgetauscht werden. Die wichtigsten logischen Äquivalenzen sind in folgendem Theorem zusammen-

gefasst.

Theorem 2.7

Es seien A, B und C aussagenlogische Formeln. Dann gilt:

1. $(A \wedge B) \wedge C \equiv A \wedge (B \wedge C)$ — Assoziativgesetze
   $(A \vee B) \vee C \equiv A \vee (B \vee C)$
2. $A \wedge B \equiv B \wedge A$ — Kommutativgesetze
   $A \vee B \equiv B \vee A$
3. $(A \wedge B) \vee C \equiv (A \vee C) \wedge (B \vee C)$ — Distributivgesetze
   $(A \vee B) \wedge C \equiv (A \wedge C) \vee (B \wedge C)$
4. $\neg(A \wedge B) \equiv (\neg A) \vee (\neg B)$ — De Morgansche Regeln
   $\neg(A \vee B) \equiv (\neg A) \wedge (\neg B)$
5. $A \vee (\neg A) \equiv \mathsf{w}$ — *tertium non datur*
   $A \wedge (\neg A) \equiv \mathsf{f}$ (Regeln vom ausgeschlossenen Dritten)
6. $A \vee \mathsf{w} \equiv \mathsf{w}$ — Dominanzgesetze
   $A \vee \mathsf{f} \equiv A$
   $A \wedge \mathsf{w} \equiv A$
   $A \wedge \mathsf{f} \equiv \mathsf{f}$
7. $A \to B \equiv (\neg A) \vee B$ — Auflösung der Implikation
   $A \to B \equiv (\neg B) \to (\neg A)$ — Kontraposition
8. $A \leftrightarrow B \equiv (A \to B) \wedge (B \to A)$ — Auflösung der Äquivalenz
9. $\neg(\neg A) \equiv A$ — Dopppelte Negation

Beweis: Wir beweisen nur die erste De Morgansche Regel $\neg(A \wedge B) \equiv (\neg A) \vee (\neg B)$. Dazu definieren wir zunächst die Hilfsaussagen $H_1 =_{\text{def}} \neg(A \wedge B)$ und $H_2 =_{\text{def}} (\neg A) \vee (\neg B)$. Die Überprüfung der Aussage $H_1 \leftrightarrow H_2$ erfolgt mittels einer Wertetabelle:

A	B	$A \wedge B$	H_1	$\neg A$	$\neg B$	H_2	$H_1 \leftrightarrow H_2$
0	0	0	1	1	1	1	1
0	1	0	1	1	0	1	1
1	0	0	1	0	1	1	1
1	1	1	0	0	0	0	1

Somit ist $H_1 \leftrightarrow H_2$ eine wahre Aussage. Also sind H_1 und H_2 logisch äquivalent. Alle anderen logischen Äquivalenzen können ebenfalls mittels Berechnung der Wertetabellen gezeigt werden. Damit ist das Theorem bewiesen. ■

Mit Hilfe von Theorem 2.7 können Aussagen umgeformt werden, genauso wie es von der algebraischen Umformung von Gleichungen her bekannt ist.

Beispiel: Zur Demonstration der Anwendung von Theorem 2.7 wollen wir die Aussage

$$C =_{\text{def}} (A \wedge (A \to B)) \to B$$

vereinfachen. Wir formen die Aussage wie folgt logisch äquivalent um:

$$\begin{aligned}
C &\equiv (A \wedge (\neg A \vee B)) \to B && \text{(Auflösung der Implikation)} \\
&\equiv ((A \wedge \neg A) \vee (A \wedge B)) \to B && \text{(Distributivgesetz)} \\
&\equiv (\mathsf{f} \vee (A \wedge B)) \to B && \text{(tertium non datur)} \\
&\equiv (A \wedge B) \to B && \text{(Dominanzgesetz)} \\
&\equiv \neg(A \wedge B) \vee B && \text{(Auflösung der Implikation)} \\
&\equiv (\neg A \vee \neg B) \vee B && \text{(De Morgansche Regel)} \\
&\equiv \neg A \vee (\neg B \vee B) && \text{(Assoziativgesetz)} \\
&\equiv \neg A \vee \mathsf{w} && \text{(tertium non datur)} \\
&\equiv \mathsf{w} && \text{(Dominanzgesetz)}
\end{aligned}$$

Die Aussage C ist also stets wahr unabhängig von den Wahrheitswerten der Aussagen A und B.

2.4 Aussageformen

Definition 2.8

Eine Aussageform über den Universen $U_1, \ldots, U_n$ ist ein Satz $A(x_1, \ldots, x_n)$ mit den freien Variablen $x_1, \ldots, x_n$, der zu einer Aussage wird, wenn jedes x_i durch ein Objekt aus dem Universum U_i ersetzt wird.

Beispiel: Die Begriffsbildung verdeutlichen wir durch folgende Aussageformen:

- $A(x) =_{\text{def}}$ „x ist eine gerade Zahl“ ist eine Aussageform über den natürlichen Zahlen: $A(2) =$ „2 ist eine gerade Zahl“ ist eine wahre Aussage; $A(3) =$ „3 ist eine gerade Zahl“ ist eine falsche Aussage.
- $B(x, y) =_{\text{def}}$ „Das Wort x ist y Buchstaben lang“ ist eine Aussageform über den Universen U_1 aller Wörter (über einem Alphabet) und U_2 aller natürlichen Zahlen. So ist $B($ Konstanz$, 8) =$ „Das Wort Konstanz ist 8 Buchstaben lang“ eine wahre Aussage.
- $C(x) =_{\text{def}}$ „$x < x + 1$“ ist als Aussageform über den natürlichen Zahlen stets wahr unabhängig davon, welche natürliche Zahl n für x eingesetzt wird. Als Aussageform über der Java-Klasse `Integer` gilt dies nicht: $C($`Integer.MAX_VALUE`$)$ ist eine falsche Aussage.

Wenn wir es mit einer Aussageform $A(x_1, \ldots, x_n)$ mit mehreren freien Variablen $x_1, \ldots, x_n$ zu tun haben, die wir alle über dem gleichen Universum $U_1 = U_2 = \ldots = U_n = U$ betrachten, so sprechen wir von einer Aussageform über dem Universum U.

2.5 Aussagen mit Quantoren

Das Einsetzen konkreter Objekte aus einem Universum macht aus einer Aussageform eine Aussage. Eine weitere Möglichkeit dafür ist die Quantifizierung von Aussagen mittels Quantoren. Im Unterschied zum konkreten Einsetzen müssen wir dabei die Objekte nicht kennen, deren Einsetzen den Wahrheitswert bestimmt. Wir brauchen nur sagen, dass es solche Objekte gibt oder nicht gibt. Die beiden wichtigsten Quantoren sind:

- Existenzquantor (oder existenzieller Quantor) $\exists$ (manchmal auch $\bigvee$ geschrieben)
- Allquantor (oder universeller Quantor) $\forall$ (manchmal auch $\bigwedge$ geschrieben)

Die Quantoren werden gemäß folgender Definition verwendet, um aus Aussageformen mit einer freien Variablen Aussagen zu machen.

Definition 2.9

Es sei $A(x)$ eine Aussageform mit einer freien Variablen über dem Universum U.

1. Die Aussage $(\exists x)[A(x)]$ (gelesen: „es gibt ein x, für das $A(x)$ gilt“) ist genau dann wahr, wenn es ein u aus U gibt, für das $A(u)$ eine wahre Aussage ist.
2. Die Aussage $(\forall x)[A(x)]$ (gelesen: „für alle x gilt $A(x)$“) ist genau dann wahr, wenn $A(u)$ für alle u aus U eine wahre Aussage ist.

Beispiele: Folgende quantifizierte Aussagen verdeutlichen die Begriffsbildung.

- Für die Aussageform $A(x) =_{\text{def}}$ „x ist eine ungerade Zahl“ über dem Universum der natürlichen Zahlen ist $(\exists x)[A(x)]$ eine wahre Aussage, da $A(3) =$ „3 ist eine ungerade Zahl“ wahr ist, und ist $(\forall x)[A(x)]$ eine falsche Aussage, da $A(2) =$ „2 ist eine ungerade Zahl“ falsch ist.
- Für die Aussageform $C(x) =_{\text{def}}$ „$x < x + 1$“ über dem Universum der natürlichen Zahlen ist $(\forall x)[C(x)] = (\forall x)[x < x + 1]$ eine wahre Aussage.
- Es sei U ein endliches Universum mit den Objekten $u_1, \ldots, u_n$. Dann gilt:

$$(\exists x)[A(x)] \text{ ist wahr} \iff A(u_1) \vee A(u_2) \vee \ldots \vee A(u_n) \underset{\text{def}}{=} \bigvee_{i=1}^{n} A(u_i) \text{ ist wahr}$$

$$(\forall x)[A(x)] \text{ ist wahr} \iff A(u_1) \wedge A(u_2) \wedge \ldots \wedge A(u_n) \underset{\text{def}}{=} \bigwedge_{i=1}^{n} A(u_i) \text{ ist wahr}$$

Der Existenzquantor stellt somit eine endliche oder unendliche Disjunktion und der Allquantor eine endliche oder unendliche Konjunktion dar.

Wir erweitern nunmehr die Anwendung von Quantoren auf Aussageformen mit mehr als einer Variablen. Dabei entstehen nicht sofort wieder Aussagen, vielmehr wird pro Anwendung eines Quantors die Anzahl freier Variablen um eine Variable reduziert. Erst wenn alle Variablen durch Quantoren oder Einsetzen konkreter Objekte gebunden sind, können wir der nun entstandenen Aussage einen

Wahrheitswert zuordnen.

Definition 2.10

Es sei $A(x_1, \ldots, x_n)$ eine Aussageform mit n Variablen über den Universen $U_1, \ldots, U_n$.

1. $(\exists x_i)[A(x_1, \ldots, x_n)]$ und $(\forall x_i)[A(x_1, \ldots, x_n)]$ sind Aussageformen mit den $n-1$ Variablen $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$.
2. In $(\exists x_i)[A(x_1, \ldots, x_n)]$ bzw. $(\forall x_i)[A(x_1, \ldots, x_n)]$ heißt $A(x_1, \ldots, x_n)$ der Wirkungsbereich des Quantors $\exists x_i$ bzw. $\forall x_i$.

Beispiele: Wir setzen unsere Beispiele für quantifizierte Aussagen fort.

- Es seien $A(x) =_{\text{def}}$ „x ist eine ungerade Zahl“ und $B(x, y) =_{\text{def}}$ „$x \cdot y$ ist eine ungerade Zahl“ Aussageformen über dem Universum der natürlichen Zahlen. Dann sind
  - $C_x(y) =_{\text{def}} (\exists x)[A(x) \to B(x, y)]$ eine Aussageform mit der freien Variable y und
  - $C_y(x) =_{\text{def}} (\forall y)[A(x) \to B(x, y)]$ eine Aussageform mit der freien Variable x,

  und es gilt beispielsweise:
  - $C_x(3) =_{\text{def}} (\exists x)[A(x) \to B(x, 3)]$ ist eine wahre Aussage
  - $C_y(3) =_{\text{def}} (\forall y)[A(3) \to B(3, y)]$ ist eine falsche Aussage, da $A(3)$ zwar wahr aber $B(3, 2)$ falsch ist.

  Für vollständig quantifizierte Aussagen erhalten wir:
  - $(\exists y)(\forall x)[A(x) \to B(x, y)]$ ist eine wahre Aussage
  - $(\exists x)(\forall y)[A(x) \to B(x, y)]$ ist eine wahre Aussage
  - $(\forall y)(\forall x)[A(x) \to B(x, y)]$ ist eine falsche Aussage
  - $(\forall x)(\forall y)[A(x) \to B(x, y)]$ ist eine falsche Aussage

  In der Aussage $(\exists y)(\forall x)[A(x) \to B(x, y)]$ ist $A(x) \to B(x, y)$ der Wirkungsbereich von $\forall x$ und $(\forall x)[A(x) \to B(x, y)]$ der Wirkungsbereich von $\exists y$.
- Für die Aussageform „$x < y$“ über dem Universum der natürlichen Zahlen ist $(\forall x)(\exists y)[x < y]$ (lies: „für alle x gibt es ein y mit $x < y$“) eine wahre Aussage, da $A(x, x+1)$ stets wahr ist, und $(\exists y)(\forall x)[x < y]$ (lies: „es gibt ein y mit $x < y$ für alle x“) eine falsche Aussage, da $A(y, y)$ stets falsch ist. Das letzte Beispiel macht deutlich, dass es bei geschachtelten quantifizierten Aussagen ganz entscheidend auf die Stellung der Existenz- und Allquantoren zueinander ankommt.

Die Namen von Variablen, die zur Quantifizierung verwendet werden, sind nur innerhalb der Wirkungsbereiche der Quantoren relevant: Zum Beispiel ist $(\exists x)(\forall x)[x < x]$ keine korrekte Quantifizierung, da bei der Einsetzung von Objekten nicht klar ist, welches für welches x die Einsetzung erfolgt; $(\exists x)[x < y] \wedge (\forall x)[x < y]$ ist dagegen unmissverständlich, da $\exists x$ und $\forall x$ überschneidungsfreie Wirkungsbereiche besitzen.

Auch für quantifizierte Aussagen können Rechenregeln (d.h. logische Äquivalenzen) angegeben

werden. Dazu erweitern wir zunächst die logische Äquivalenz $\equiv$ auf Aussageformen.

Definition 2.11

Es seien $A(x_1, \ldots, x_n)$ und $B(x_1, \ldots, x_n)$ Aussageformen über den Universen $U_1, \ldots, U_n$. Dann gilt:

$A(x_1, \ldots, x_n) \equiv B(x_1, \ldots, x_n)$

$\iff_{\text{def}}$ $A(u_1, \ldots, u_n) \leftrightarrow B(u_1, \ldots, u_n)$ ist wahr für alle $u_1, \ldots, u_n$ aus den jeweiligen Universen

$\iff$ $(\forall x_1)(\forall x_2)\cdots(\forall x_n)[A(x_1, \ldots, x_n) \leftrightarrow B(x_1, \ldots, x_n)]$ ist wahr (über den Universen $U_1, \ldots, U_n$)

Im Falle endlicher Universen können wir die Frage nach der logischen Äquivalenz von Aussageformen im Prinzip mit Wertetabellen beantworten. Abgesehen von praktischen Erwägungen funktioniert dies im Falle unendlicher Universen auch prinzipiell nicht mehr und wir müssen andere Verfahren heranziehen (siehe auch den nächsten Abschnitt über Beweise). Wie in der Aussagenlogik können einige logische Äquivalenzen zur Umformung von quantifizierten Aussagen verwendet werden.

Wir erwähnen die folgenden Regeln hier nur auszugsweise (und ohne Beweise). Zur besseren Lesbarkeit verwenden wir die Notation $\vec{x}$ für die freien Variablen $x_1, \ldots, x_n$, d.h., wir schreiben $A(\vec{x})$ für $A(x_1, \ldots, x_n)$.

Theorem 2.12

Es seien $A(\vec{x})$ und $B(\vec{x})$ Aussageformen mit den freien Variablen $x_1, \ldots, x_n$ über den Universen $U_1, \ldots, U_n$ sowie $i \neq j$ zwei Indizes.

1. $(\exists x_i)[A(\vec{x})] \vee (\exists x_i)[B(\vec{x})] \equiv (\exists x_i)[A(\vec{x}) \vee B(\vec{x})]$
   $(\forall x_i)[A(\vec{x})] \wedge (\forall x_i)[B(\vec{x})] \equiv (\forall x_i)[A(\vec{x}) \wedge B(\vec{x})]$
2. $(\exists x_i)(\exists x_j)[A(\vec{x})] \equiv (\exists x_j)(\exists x_i)[A(\vec{x})]$
   $(\forall x_i)(\forall x_j)[A(\vec{x})] \equiv (\forall x_j)(\forall x_i)[A(\vec{x})]$
3. $\neg(\exists x_i)[A(\vec{x})] \equiv (\forall x_i)[\neg A(\vec{x})]$ — De Morgansche Regeln
   $\neg(\forall x_i)[A(\vec{x})] \equiv (\exists x_i)[\neg A(\vec{x})]$

Die Stichhaltigkeit und Namensgebung der Rechenregeln ist leicht einzusehen, wenn wir endliche Universen für die Aussage zu Grunde legen und endliche Konjunktionen und Disjunktionen betrachten.

Beispiel: Es sei $P(x) =_{\text{def}}$ „x ist eine Primzahl“ eine Aussageform über dem Universum der natürlichen Zahlen. Wir formulieren die Aussage, dass es unendlich viele Primzahlen gibt, wie folgt:

$$A =_{\text{def}} (\forall x)(\exists y)[P(y) \wedge x < y]$$

Die Negation der Aussage ist: „Es gibt endlich viele Primzahlen“. Wir negieren die Aussage A dazu formal:

$$\neg A \equiv \neg(\forall x)(\exists y)[P(y) \wedge x < y]$$

$$
\begin{aligned}
&\equiv (\exists x)\Big[\neg(\exists y)[P(y) \wedge x < y]\Big] \\
&\equiv (\exists x)(\forall y)[\neg(P(y) \wedge x < y)] \\
&\equiv (\exists x)(\forall y)[\neg P(y) \vee x \geq y] \\
&\equiv (\exists x)(\forall y)[P(y) \rightarrow x \geq y]
\end{aligned}
$$

Intuitiv ausgedrückt bedeutet dies Aussage: „Es gibt eine größte Primzahl“.

Quantifizierte Aussagen in komplexeren Domänen werden in der Regel schnell unübersichtlich. Deshalb finden sich oft Abkürzungen für häufig benutzte Redewendungen. Wir wollen diesen Abschnitt mit einigen davon beschließen.

1. „Es gibt $x_1, \ldots, x_n$, sodass $A(x_1, \ldots, x_n)$ gilt“: Die zugehörige Abkürzung für die exakte logische Definition ist:

$$(\exists x_1, \ldots, x_n)[A(x_1, \ldots, x_n)] =_{\text{def}} (\exists x_1)(\exists x_2) \cdots (\exists x_n)[A(x_1, \ldots, x_n)]$$

2. „Für alle $x_1, \ldots, x_n$ gilt $A(x_1, \ldots, x_n)$“: Die zugehörige Abkürzung für die exakte logische Definition ist:

$$(\forall x_1, \ldots, x_n)[A(x_1, \ldots, x_n)] =_{\text{def}} (\forall x_1)(\forall x_2) \cdots (\forall x_n)[A(x_1, \ldots, x_n)]$$

3. „Für alle x mit $A(x)$ gilt $B(x)$“: Die zugehörige Abkürzung für die exakte logische Definition ist:

$$(\forall x; A(x))[B(x)] =_{\text{def}} (\forall x)[A(x) \rightarrow B(x)]$$

4. „Es gibt ein x mit $A(x)$, sodass $B(x)$ gilt“: Die zugehörige Abkürzung für die exakte logische Definition ist:

$$(\exists x; A(x))[B(x)] =_{\text{def}} (\exists x)[A(x) \wedge B(x)]$$

Die beiden letzten Regeln sind verträglich mit den De Morganschen Regeln:

$$
\begin{aligned}
\neg(\exists x; A(x))[B(x)] &\equiv \neg(\exists x)[A(x) \wedge B(x)] \\
&\equiv (\forall x)[\neg(A(x) \wedge B(x))] \\
&\equiv (\forall x)[(\neg A(x)) \vee (\neg B(x))] \\
&\equiv (\forall x)[A(x) \rightarrow (\neg B(x))] \\
&\equiv (\forall x; A(x))[\neg B(x)]
\end{aligned}
$$

Beispiel: Das Pumping-Lemma für reguläre Sprachen ist ein wichtiges Hilfsmittel im Bereich der Automatentheorie und Formaler Sprachen. Eine übliche Formulierung als Theorem ist die folgende:

> „Für jede reguläre Sprache L gibt es ein $n_0 > 0$ mit folgender Eigenschaft: Für jedes z aus L mit $|z| \geq n_0$ gibt es eine Zerlegung $z = uvw$ mit $|uv| \leq n_0$ und $|v| > 0$, sodass $uv^k w$ zu L gehört für alle $k \geq 0$.“

Mit Hilfe unserer Quantorennotationen ist das Theorem wie folgt ausdrückbar:

$$
\begin{aligned}
&(\forall L; L \text{ ist regulär})\ (\exists n_0; n_0 > 0)\ (\forall z; z \text{ gehört zu } L \wedge |z| \geq n_0) \\
&\quad (\exists u, v, w; z = uvw \wedge |uv| \leq n_0 \wedge |v| > 0)\ (\forall k; k \geq 0)\ [uv^k w \text{ gehört zu } L]
\end{aligned}
$$

Die Handhabung des Theorems (abgesehen vom Wissen um die verwendeten Begriffe und Notationen) bedarf einiger Übung, da die Quantorenstruktur $\forall\exists\forall\exists$ der Aussage vier Wechsel zwischen All- und Existenzquantoren aufweist.

2.6 Beweise

Unter einem Beweis wollen wir eine Folge von allgemeingültigen Implikationen (Regeln) verstehen, die auf wahren Anfangsaussagen (Prämissen) basieren und zu der Zielaussage (Folgerung) führen, deren Wahrheit damit nachgewiesen wird.

Universelle Beweisregeln

Wichtige Beweisregeln (Implikationen) für den mathematischen Alltagsgebrauch sind:

- Abtrennungsregel (modus ponens): Sind A und $A \to B$ wahr, so ist B wahr.
  Korrektheit folgt aus der Allgemeingültigkeit von $(A \wedge (A \to B)) \to B$.
- Fallunterscheidung: Sind $A \to B$ und $\neg A \to B$ wahr, so ist B wahr.
  Korrektheit folgt aus der Allgemeingültigkeit von $((A \to B) \wedge ((\neg A) \to B)) \to B$.
- Kettenschluss: Sind $A \to B$ und $B \to C$ wahr, so ist $A \to C$ wahr.
  Korrektheit folgt aus der Allgemeingültigkeit von $((A \to B) \wedge (B \to C)) \to (A \to C)$.
- Kontraposition: Ist $A \to B$ wahr, so ist $(\neg B) \to (\neg A)$ wahr.
  Korrektheit folgt aus der Allgemeingültigkeit von $(A \to B) \to ((\neg B) \to (\neg A))$.
- Indirekter Beweis (oder Beweis mittels Widerspruch): Sind $A \to B$ und $A \to \neg B$ wahr, so ist $\neg A$ wahr.
  Korrektheit folgt aus der Allgemeingültigkeit von $((A \to B) \wedge (A \to (\neg B))) \to (\neg A)$.

Beweisanalyse*

Im Folgenden wollen an dem Beweis der Irrationalität von $\sqrt{2}$ die logische Struktur und das Zusammenspiel der verschiedenen Beweisregeln offenlegen.

Lemma 2.13

Ist n eine ungerade Zahl, so ist n^2 eine ungerade Zahl.

Beweis: (direkt) Es sei n eine ungerade Zahl, d.h.

$$n = 2\lfloor n/2 \rfloor + 1. \qquad =_{\text{def}} \mathsf{A}$$

Wir müssen zeigen:

$$n^2 = 2\lfloor n^2/2 \rfloor + 1. \qquad =_{\text{def}} \mathsf{Z}$$

Mit $n = 2\lfloor n/2 \rfloor + 1$ gilt:

$$\begin{aligned} n^2 &= (2\lfloor n/2 \rfloor + 1)^2 && =_{\text{def}} \mathsf{B} \\ &= 4\lfloor n/2 \rfloor^2 + 4\lfloor n/2 \rfloor + 1 && =_{\text{def}} \mathsf{C} \\ &= 2\left(2\lfloor n/2 \rfloor^2 + 2\lfloor n/2 \rfloor\right) + 1 && =_{\text{def}} \mathsf{D} \end{aligned}$$

Wir zeigen zunächst die Hilfsaussage:

$$\lfloor n^2/2 \rfloor = 2\lfloor n/2 \rfloor^2 + 2\lfloor n/2 \rfloor \qquad =_{\text{def}} \mathsf{H}$$

Wegen $n = 2\lfloor n/2 \rfloor + 1$ gilt:

$$\begin{aligned} \lfloor n^2/2 \rfloor &= \left\lfloor (2\lfloor n/2 \rfloor + 1)^2 /2 \right\rfloor && =_{\text{def}} \mathsf{E} \\ &= \left\lfloor \left(4\lfloor n/2 \rfloor^2 + 4\lfloor n/2 \rfloor + 1\right) /2 \right\rfloor && =_{\text{def}} \mathsf{F} \\ &= \left\lfloor 2\lfloor n/2 \rfloor^2 + 2\lfloor n/2 \rfloor + 1/2 \right\rfloor && =_{\text{def}} \mathsf{G} \\ &= 2\lfloor n/2 \rfloor^2 + 2\lfloor n/2 \rfloor && = \mathsf{H} \end{aligned}$$

Einsetzen der Hilfsaussage in D ergibt:

$$n^2 = 2\lfloor n^2/2 \rfloor + 1. \qquad = \mathsf{Z}$$

d.h. n^2 ist ungerade. ■

A (für eine konkrete Zahl) ist eine wahre Prämisse

Z ist die Zielaussage

$\mathsf{A} \to \mathsf{B}$ ist wahr

$\mathsf{B} \to \mathsf{C}$ ist wahr

$\mathsf{C} \to \mathsf{D}$ ist wahr

$\mathsf{A} \to \mathsf{E}$ ist wahr

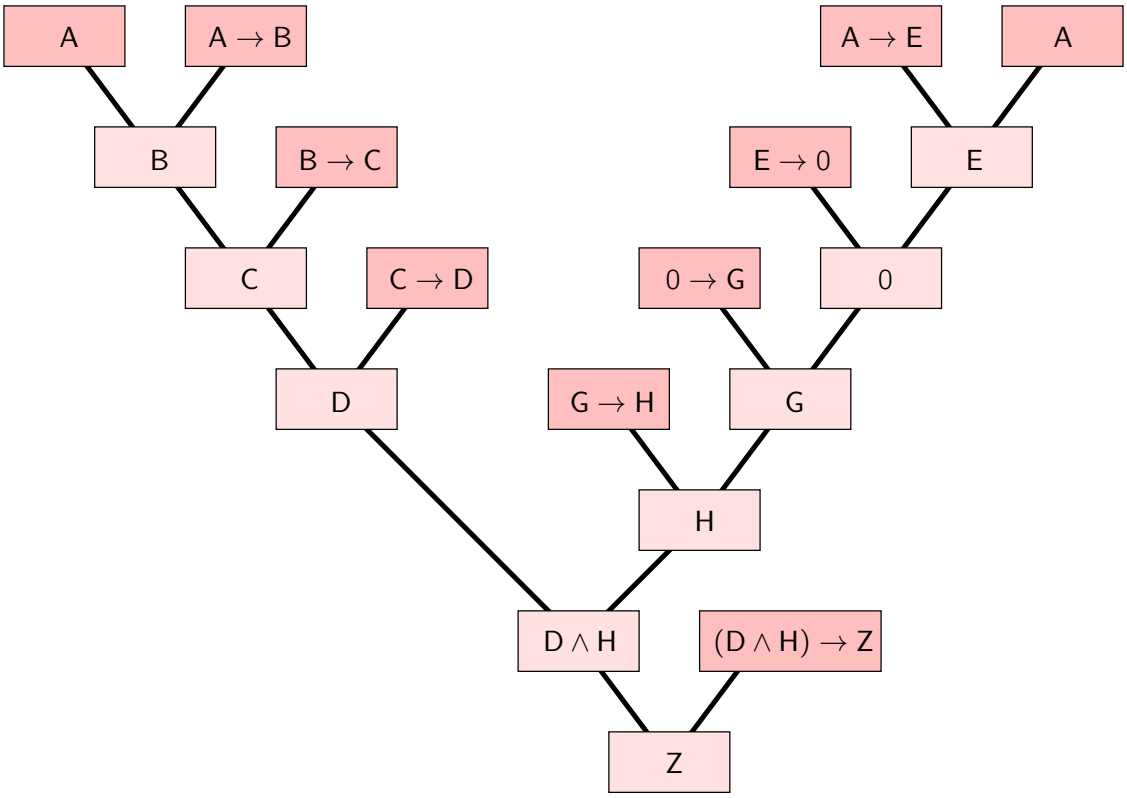
$\mathsf{E} \to \mathsf{F}$ ist wahr

$\mathsf{F} \to \mathsf{G}$ ist wahr

$\mathsf{G} \to \mathsf{H}$ ist wahr

$(\mathsf{D} \wedge \mathsf{H}) \to \mathsf{Z}$ ist wahr

Die logische Struktur des Beweises kann schematisch in Form eines Ableitungsbaumes dargestellt werden:



Hierbei sind die heller unterlegten Aussagen (bis auf $D \wedge H$) durch Anwendung der Abtrennungsregel aus den beiden darüber liegenden Aussagen abgeleitet worden. Die dunkler unterlegten Aussagen sind per Voraussetzung wahr (Aussage A) oder durch Anwendung algebraischer Umformungsregeln wahr.

Durch Kontraposition von Lemma 2.13 lässt sich nun direkt Korollar 2.14 folgern.

Korollar 2.14

Ist n^2 eine gerade Zahl, so ist n eine gerade Zahl.

Beweis: (Kontraposition)

Ist n eine ungerade Zahl,	$=_{\text{def}}$ A
so ist n^2 eine ungerade Zahl	$=_{\text{def}}$ B
(nach Lemma A).	
Damit gilt nach Kontraposition:	
Ist n^2 eine gerade Zahl,	$\equiv \neg$B
so ist n eine gerade Zahl.	$\equiv \neg$A

Damit ist das Korollar bewiesen. ■

$A \rightarrow B$ ist wahr

$\neg B \rightarrow \neg A$ ist wahr

Mit Hilfe von Korollar B kann die Irrationalität von $\sqrt{2}$ mittels Widerspruchbeweis gezeigt werden.

Theorem 2.15

$\sqrt{2}$ ist irrational.

Beweis: (indirekt) Wir nehmen an: $\sqrt{2}$ ist eine rationale Zahl, d.h.

$$(\exists p)(\exists q)\Big[\underbrace{\mathrm{ggT}(p,q)=1}_{=_{\text{def}}\ \mathsf{Z}} \wedge \sqrt{2}=p/q\Big] \quad =_{\text{def}}\ \mathsf{A}$$

A → Z ist wahr

Dann gilt

$$2q^2 = p^2, \quad =_{\text{def}}\ \mathsf{B}$$

A → B ist wahr

d.h. p^2 ist gerade.

Nach Korollar B ist p gerade, d.h.

$$p = 2\lfloor p/2\rfloor. \quad =_{\text{def}}\ \mathsf{C}$$

B → C ist wahr

Wollen zeigen, dass auch q^2 gerade ist, d.h.

$$q^2 = 2\lfloor q^2/2\rfloor. \quad =_{\text{def}}\ \mathsf{D}$$

Mit $2q^2 = p^2$ und $p = 2\lfloor p/2\rfloor$ folgt

$$\begin{aligned} q^2 &= p^2/2 && =_{\text{def}}\ \mathsf{E} \\ &= (2\lfloor p/2\rfloor)^2/2 && =_{\text{def}}\ 0 \\ &= 2\lfloor p/2\rfloor^2 && =_{\text{def}}\ \mathsf{G} \end{aligned}$$

B → E ist wahr

(C ∧ E) → 0 ist wahr

0 → G ist wahr

und somit

$$\begin{aligned} 2\lfloor q^2/2\rfloor &= 2\lfloor 2\lfloor p/2\rfloor^2/2\rfloor && =_{\text{def}}\ \mathsf{H} \\ &= 2\lfloor \lfloor p/2\rfloor^2\rfloor && =_{\text{def}}\ \mathsf{I} \\ &= 2\lfloor p/2\rfloor^2 && =_{\text{def}}\ \mathsf{J} \\ &= q^2 && \equiv\ \mathsf{D} \end{aligned}$$

G → H ist wahr

H → I ist wahr

I → J ist wahr

J → D ist wahr

Nach Korollar B ist q gerade. $=_{\text{def}}\ \mathsf{K}$

D → K ist wahr

Damit gilt $\mathrm{ggT}(p,q) \geq 2$. $\equiv \neg\mathsf{Z}$

K → ¬Z ist wahr

A → ¬Z ist wahr

Dies ist ein Widerspruch, d.h. die Annahme ist falsch und $\sqrt{2}$ ist irrational. $\equiv \neg\mathsf{A}$

¬A ist wahr

Damit ist das Theorem bewiesen. ■

Spezielle Beweisregeln

Neben den Beweisregeln, die ganz allgemein für beliebige Aussagen anwendbar sind, gibt es noch eine ganze Menge spezieller Beweisregeln für Aussagen mit bestimmter Quantorenstruktur und bestimmter Universen. Zwei wichtige unter diesen sind die folgenden:

- Spezialisierung (Substitution): Ist $(\forall x)[A(x)]$ wahr, so ist $A(y)$ wahr, falls y nicht in einem Wirkungsbereich eines Quantors in $A(x)$ vorkommt.

  Korrektheit folgt aus Allgemeingültigkeit von $(\forall y)\,[(\forall x)[A(x)] \to A(y)]$ (mit obiger Einschränkung).

- Vollständige Induktion: Es sei $A(n)$ eine Aussageform über dem Universum der natürlichen Zahlen. Sind $A(0)$ und $A(n-1) \to A(n)$ für alle $n > 0$ wahr, so ist $A(n)$ für alle n wahr.

Wir wollen die Korrektheit der vollständigen Induktion überprüfen.

Theorem 2.16

Es sei $A(n)$ eine Aussageform mit der freien Variable n über dem Universum der natürlichen Zahlen. Dann ist die Aussage

$$\Big(A(0) \wedge (\forall n; n > 0)[A(n-1) \to A(n)]\Big) \to (\forall n)[A(n)]$$

allgemeingültig.

Beweis: (indirekt) Es gelte $A(0)$ und $A(n-1) \to A(n)$ für alle $n > 0$. Zum Widerspruch nehmen wir an, dass es ein n gibt, sodass $A(n)$ nicht gilt. Dann gibt es auch eine kleinste natürliche Zahl n_0, für die $A(n_0)$ nicht wahr ist, d.h. es gilt $\neg A(n_0) \wedge (\forall n; n < n_0)[A(n)]$. Wir unterscheiden zwei Fälle für n_0:

- 1. Fall: Ist $n_0 = 0$, so ist $\neg A(0)$ wahr. Dies steht jedoch im Widerspruch zur Voraussetzung, dass $A(0)$ gilt.
- 2. Fall: Ist $n_0 > 0$, so ist $\neg A(n_0) \wedge A(n_0 - 1) \equiv \neg(A(n_0 - 1) \to A(n_0))$ wahr. Dies steht jedoch im Widerspruch zur Voraussetzung, dass $A(n-1) \to A(n)$ für alle $n > 0$ gilt, also insbesondere auch $A(n_0 - 1) \to A(n_0)$.

Also ist die Annahme falsch und es gilt $A(n)$ für alle n. Damit ist das Theorem bewiesen. ■

Die logische Struktur des Beweises für Theorem 2.16 ist typisch für einen Widerspruchsbeweis einer Implikation. Wenn wir die Aussage $A \to B$ als wahr beweisen wollen, so nehmen wir an, dass A aber nicht B gilt. Damit folgt sofort, dass die Aussage $(A \wedge (\neg B)) \to A$ wahr ist. Anschließend müssen wir noch beweisen, dass auch $(A \wedge (\neg B)) \to (\neg A)$ allgemeingültig ist, d.h. wir konstruieren einen Widerspruch zur eigentlichen Prämisse A unserer zu beweisenden Implikation. Nach der Regel vom indirekten Beweis folgt nun, dass $\neg(A \wedge (\neg B)) \equiv A \to B$ wahr ist.

2.7 Exkurs: Aussagen in Normalform*

Im Folgenden betrachten wir Aussagen besonderer Struktur mit den Konnektoren $\neg, \wedge, \vee$. Wir führen zunächst zwei Abkürzungen ein. Für Aussagen $H_1, \ldots, H_n$ definieren wir:

$$\bigwedge_{i=1}^{n} H_i \quad =_{\text{def}} \quad H_1 \wedge H_2 \wedge \ldots \wedge H_n$$
$$\bigvee_{i=1}^{n} H_i \quad =_{\text{def}} \quad H_1 \vee H_2 \vee \ldots \vee H_n$$

Ein Literal ist eine Aussage der Form X oder $\neg X$, wobei X eine aussagenlogische Variable ist.

Definition 2.17

Eine Aussage A mit den aussagenlogischen Variablen $X_1, \ldots, X_n$ heißt

1. konjunktive Normalform (KNF, CNF), falls für geeignete Zahlen k und ℓ_i sowie Literale L_{ij} gilt:
$$A = \bigwedge_{i=1}^{k} \bigvee_{j=1}^{\ell_i} L_{ij}$$
2. disjunktive Normalform (DNF), falls für geeignete Zahlen k und ℓ_i sowie Literale L_{ij} gilt:
$$A = \bigvee_{i=1}^{k} \bigwedge_{j=1}^{\ell_i} L_{ij}$$

Beispiele: Wir wollen die Definitionen an einigen Aussagen nachvollziehen.

- Die Aussage $(X_1 \wedge X_2) \vee (\neg X_1 \wedge \neg X_3 \wedge X_4) \vee (X_2 \wedge X_4) \vee X_3$ ist eine disjunktive Normalform mit $k = 4, \ell_1 = 2, \ell_2 = 3, \ell_3 = 2, \ell_4 = 1$ und
$$\begin{array}{lll} L_{11} = X_1, & L_{12} = X_2, & \\ L_{21} = \neg X_1, & L_{22} = \neg X_3, & L_{23} = X_4 \\ L_{31} = X_2, & L_{32} = X_4, & \\ L_{41} = X_3, & & \end{array}$$
- $X_1 \wedge (X_2 \vee X_3)$ ist eine konjunktive Normalform, aber keine disjunktive Normalform.
- $X_1 \vee (X_2 \wedge X_3)$ ist eine disjunktive Normalform, aber keine konjunktive Normalform.
- $X_1 \wedge X_2$ ist eine disjunktive Normalform (mit $k = 1$) und eine konjunktive Normalform (mit $k = 2$).
- $X_1 \wedge (X_2 \vee (X_3 \wedge X_4))$ ist weder eine disjunktive noch eine konjunktive Normalform. Aber es gilt
$$X_1 \wedge (X_2 \vee (X_3 \wedge X_4)) \equiv (X_1 \wedge X_2) \vee (X_1 \wedge X_3 \wedge X_4)),$$
d.h., die Aussage ist äquivalent zu einer disjunktiven Normalform.

Wir wollen die Einsicht aus dem letzten Beispiel ausdehnen und zeigen, dass jede Aussage äquivalent zu einer konjunktiven und zu einer disjunktiven Normalform ist. Dazu führen wir für eine Aussage X folgende Schreibweise ein:

$$X^1 =_{\text{def}} X, \qquad X^0 =_{\text{def}} \neg X$$

Proposition 2.18

Für eine beliebige Aussage X und eine Interpretation I gilt

$$I(X^\sigma) = 1 \iff I(X) = \sigma$$

Beweis: Wir führen eine Fallunterscheidung durch. Ist $\sigma = 1$, so gilt $X^\sigma = X$, d.h., X ist genau dann wahr, wenn $I(X) = 1$ gilt. Ist $\sigma = 0$, so gilt $X^\sigma = \neg X$, d.h., $\neg X$ ist genau dann wahr, wenn $I(X) = 0$ gilt. Damit ist die Proposition bewiesen. ■

Proposition 2.19

Es seien $H_1, \ldots H_n$ Aussagen und I eine Intepretation. Dann gilt:

1. $I(\bigwedge_{i=1}^n H_i) = 1$ gilt genau dann, wenn für alle Aussagen $I(H_i) = 1$ gilt.
2. $I(\bigvee_{i=1}^n H_i) = 1$ gilt genau dann, wenn für eine Aussage $I(H_i) = 0$ gilt.

Beweis: Der Induktionsbeweis bleibt zur selbständigen Übung überlassen. ■

Ohne Beweis führen wir den folgenden Satz an, der die Existenz der kanonischen disjunktiven Normalform für jede erfüllbare Aussage sichert.

Theorem 2.20

Für jede erfüllbare Aussage H mit den aussagenlogischen Variablen $X_1, \ldots, X_n$ gilt

$$H \equiv \bigvee_{\substack{\text{Belegung } I \\ \text{erfüllt } H}} \bigwedge_{i=1}^{n} X_i^{I(X_i)}$$

Beispiele: Für $H =_{\text{def}} X_1 \oplus \neg(X_2 \vee (X_3 \wedge X_1))$ betrachten wir die Wertetabelle. Dabei setzen wir

$$\begin{aligned} H_1 &=_{\text{def}} X_3 \wedge X_1 \\ H_2 &=_{\text{def}} X_2 \vee H_1 \\ H_3 &=_{\text{def}} \neg H_2 \end{aligned}$$

Somit ist $H = X_1 \oplus H_3$. Wir erhalten folgende Wertetabelle:

X_1	X_2	X_3	H_1	H_2	H_3	H
0	0	0	0	0	1	1
0	0	1	0	0	1	1
0	1	0	0	1	0	0
0	1	1	0	1	0	0
1	0	0	0	0	1	0
1	0	1	1	1	0	1
1	1	0	0	1	0	1
1	1	1	1	1	0	1

Nach Theorem 2.20 gilt somit

$$H \equiv (\neg X_1 \wedge \neg X_2 \wedge \neg X_3) \vee (\neg X_1 \wedge \neg X_2 \wedge X_3) \vee (X_1 \wedge \neg X_2 \wedge X_3) \vee (X_1 \wedge X_2 \wedge \neg X_3) \vee (X_1 \wedge X_2 \wedge X_3)$$

Das analoge Theorem gilt auch für die kanonische konjunktive Normalform (wiederum ohne Beweis).

Theorem 2.21

Für jede widerlegbare Aussage H mit den aussagenlogischen Variablen $X_1, \ldots, X_n$ gilt

$$H \equiv \bigwedge_{\substack{\text{Belegung } I \\ \text{widerlegt } H}} \bigvee_{i=1}^{n} X_i^{1-I(X_i)}$$

Beispiel: Mit Hilfe obiger Wertetabelle erhalten wir die logische Äquivalenz:

$$X_1 \oplus \neg(X_2 \vee (X_3 \wedge X_1)) \equiv (X_1 \vee \neg X_2 \vee X_3) \wedge (X_1 \vee \neg X_2 \vee \neg X_3) \wedge (\neg X_1 \vee X_2 \vee X_3)$$

3 Mengen

In diesem Kapitel beschäftigen wir uns mit den grundlegenden Begriffen der Mengenlehre. Hierbei folgen wir im Wesentlichen der naiven Mengenlehre, wie sie im mathematischen Alltagsgeschäft der Informatik ausreichend ist. Unter einer streng mathematischen Sichtweise ist die naive Mengenlehre nicht widerspruchsfrei (Russellsches Paradoxon); jedoch können Widersprüche mit einer gewissen Umsicht vermieden werden.

3.1 Aussagen über Mengen

Eine Menge A besteht aus paarweise verschiedenen Objekten. Damit wird ein mehrfaches Vorkommen von Objekten ignoriert – im Gegensatz z.B. zu Listen als Datenstruktur. Mengen können auf unterschiedliche Art und Weise beschrieben werden:

- extensionale Darstellung (Darstellung nach dem Umfang der Menge): Die in der Menge A enthaltenen Objekte werden aufgezählt (soweit dies möglich ist), wobei die Reihenfolge keine Rolle spielt – auch hier im Gegensatz zu Listen; symbolisch:

  $$A = \{a_1, a_2, \ldots\}$$

- intensionale Darstellung (Darstellung nach dem Inhalt der Menge): Es werden alle Objekte a selektiert, die aus dem zu einer Aussageform $E(x)$ gehörenden Universum stammen, sodass $E(a)$ eine wahre Aussage ist; symbolisch:

  $$A = \{\ a \mid E(a)\ \}$$

  Mit anderen Worten enthält die Menge A alle Objekte a, die eine gewisse Eigenschaft E erfüllen.

Extensionale Darstellungen sind für die Fälle endlicher Mengen häufig einsichtiger als intensionale Darstellungen, da die Selektion der Objekte bereits ausgeführt vorliegt. Für unendliche Mengen sind extensionale Darstellungen im Allgemeinen nicht mehr möglich.

Beispiele: Die folgenden Darstellungen derselben (endlichen) Menge verdeutlichen die unterschiedlichen Beschreibungsaspekte:

- $\{3, 5, 7, 11\} = \{11, 5, 7, 3\}$
- $\{3, 5, 7, 11\} = \{3, 3, 3, 5, 5, 7, 11, 11\}$
- $\{3, 5, 7, 11\} = \{\ a \mid 2 < a < 12 \wedge a \text{ ist eine Primzahl}\ \}$

Im Folgenden vereinbaren wir Schreib- und Sprechweisen für mengenbezogene Aussagen. Positive Aussagen sind die folgenden:

$a \in A$	steht für:	a ist Element von A
$A \subseteq B$	steht für:	A ist Teilmenge von B
$B \supseteq A$	steht für:	B ist Obermenge von A
$A = B$	steht für:	A und B sind gleich
$A \subset B$	steht für:	A ist echte Teilmenge von B
$B \supset A$	steht für:	B ist echte Obermenge von A

Die zugehörigen negativen Aussagen sind:

$a \notin A$	steht für:	a ist kein Element von A
$A \not\subseteq B$	steht für:	A ist keine Teilmenge von B
$B \not\supseteq A$	steht für:	B ist keine Obermenge von A
$A \neq B$	steht für:	A und B sind verschieden
$A \not\subset B$	steht für:	A ist keine echte Teilmenge von B
$B \not\supset A$	steht für:	B ist keine echte Obermenge von A

Die exakten Bedeutungen der Bezeichnungen werden aussagenlogisch festgelegt. Dazu setzen wir im Folgenden für die verwendeten Aussageformen stets ein Universum voraus.

$a \in A$	$=_{\text{def}}$	a gehört zur Menge A	$a \notin A$	$=_{\text{def}}$	$\neg(a \in A)$
$A \subseteq B$	$=_{\text{def}}$	$(\forall a)[a \in A \to a \in B]$	$A \not\subseteq B$	$=_{\text{def}}$	$\neg(A \subseteq B)$
$B \supseteq A$	$=_{\text{def}}$	$A \subseteq B$	$B \not\supseteq A$	$=_{\text{def}}$	$\neg(B \supseteq A)$
$A = B$	$=_{\text{def}}$	$A \subseteq B \wedge B \subseteq A$	$A \neq B$	$=_{\text{def}}$	$\neg(A = B)$
$A \subset B$	$=_{\text{def}}$	$A \subseteq B \wedge A \neq B$	$A \not\subset B$	$=_{\text{def}}$	$\neg(A \subset B)$
$B \supset A$	$=_{\text{def}}$	$A \subset B$	$B \not\supset A$	$=_{\text{def}}$	$\neg(B \supset A)$

Aussagen über Mengen werden also als Abkürzungen für quantifizierte Aussagen über ihren Elementen eingeführt.

Beispiele: Wir verdeutlichen den Zusammenhang zwischen Aussagen über Mengen und den definierenden quantifizierten Aussagen über den Elementen an Hand zweier Mengenaussagen:

$$\begin{aligned}
A \not\subseteq B &\equiv \neg(A \subseteq B) \\
&\equiv \neg(\forall a)[a \in A \to a \in B] \\
&\equiv (\exists a)[\neg(a \in A \to a \in B)] \\
&\equiv (\exists a)[\neg(a \notin A \vee a \in B)] \\
&\equiv (\exists a)[a \in A \wedge a \notin B]
\end{aligned}$$

$$\begin{aligned}
A = B &\equiv A \subseteq B \wedge A \supseteq B \\
&\equiv A \subseteq B \wedge B \subseteq A \\
&\equiv (\forall a)[a \in A \to a \in B] \wedge (\forall a)[a \in B \to a \in A] \\
&\equiv (\forall a)[(a \in A \to a \in B) \wedge (a \in B \to a \in A)] \\
&\equiv (\forall a)[(a \in A \leftrightarrow a \in B)]
\end{aligned}$$

Häufig muss die Gleichheit zweier Mengen A und B, die in intensionaler Darstellung gegeben sind, gezeigt werden. Nach Definition des Wahrheitswertes der Aussage $A = B$ müssen dafür stets zwei Richtungen gezeigt werden. Ein einfaches Beispiel soll dies verdeutlichen.

Beispiel: Es seien die beiden Mengen $A =_{\text{def}} \{ n \mid n \text{ ist gerade} \}$ und $B =_{\text{def}} \{ n \mid n^2 \text{ ist gerade} \}$ als Teilmengen natürlicher Zahlen gegeben. Wir wollen zeigen, dass $A = B$ gilt. Dazu zeigen wir zwei Inklusionen:

$\subseteq$: Es sei $n \in A$. Dann ist n gerade, d.h., es gibt ein $k \in \mathbb{N}$ mit $n = 2k$. Es gilt $n^2 = (2k)^2 = 2(2k^2)$. Somit ist n^2 gerade. Folglich gilt $n \in B$. Damit gilt $A \subseteq B$.

$\supseteq$: Es sei $n \in B$. Dann ist n^2 gerade. Nach Korollar B (Abschnitt 1.6) ist n gerade. Also gilt $n \in A$. Somit gilt $B \subseteq A$.

Damit ist die Gleichheit der Mengen bewiesen.

Eine ausgezeichnete Menge (in jedem Universum) ist die leere Menge: Eine Menge A heißt leer, falls A kein Element enthält. Logisch ausgedrückt bedeutet die Bedingung: $(\forall a)[a \notin A]$.

Proposition 3.1

Es gibt nur eine leere Menge (in jedem Universum).

Beweis: (Kontraposition) Wir wollen zeigen: Sind A und B leere Mengen, so gilt $A = B$. Dafür zeigen wir: Gilt $A \neq B$, so ist A nicht leer oder B nicht leer. Es gilt:

$$\begin{aligned} A \neq B &\equiv A \not\subseteq B \vee B \not\subseteq A \\ &\equiv (\exists a)[a \in A \wedge a \notin B] \vee (\exists a)[a \in B \wedge a \notin A] \\ &\equiv (\exists a) \underbrace{[(a \in A \wedge a \notin B) \vee (a \in B \wedge a \notin A)]}_{=_{\text{def}}\, D(a)} \end{aligned}$$

Es sei x ein Objekt im Universum, so dass $D(x)$ eine wahre Aussage ist. Dann gilt $x \in A$ oder $x \in B$. Also ist A oder B nicht leer. ■

Damit ist gerechtfertigt, dass ein eigenes Symbol $\emptyset$ für die Bezeichnung der leeren Menge eingeführt wird. $|A|$ (oder auch: $\|A\|, \#A$) ist die Anzahl der Elemente von A bzw. die Kardinalität von A. Die Kardinalität der leeren Menge ist also stets 0. Ist $|A| < \infty$, so heißt A endliche Menge, sonst unendliche Menge. Mengen mit nur einem Element werden Einermengen genannt. Die natürlichen Zahlen sind also genau die Kardinalitäten endlicher Mengen.

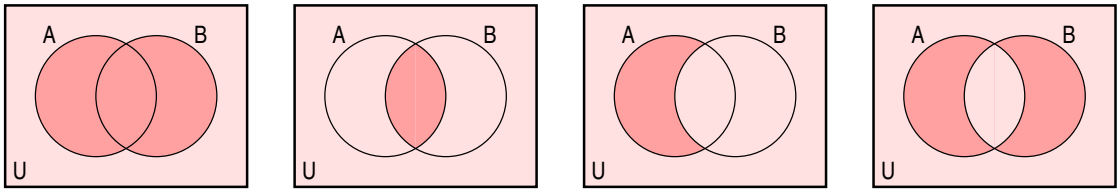
3.2 Rechnen mit Mengen

Wir definieren die folgenden Operationen, die aus zwei Mengen A und B eines Universums U wieder eine Menge desselben Universums U formen (zur Verdeutlichung geben wir U mit an):

Vereinigung:	$A \cup B =_{\text{def}} \{ x \in U \mid x \in A \vee x \in B \}$
Durchschnitt:	$A \cap B =_{\text{def}} \{ x \in U \mid x \in A \wedge x \in B \}$
Differenz:	$A \setminus B =_{\text{def}} \{ x \in U \mid x \in A \wedge x \notin B \}$
symmetrische Differenz:	$A \triangle B =_{\text{def}} (A \setminus B) \cup (B \setminus A)$

Eine besondere Differenzoperation ist die Komplementierung einer Menge A:

Komplement:	$\overline{A} =_{\text{def}} U \setminus A$



$A \cup B$ $A \cap B$ $A \setminus B$ $A \triangle B$

Üblicherweise werden Mengenoperationen zur Veranschaulichung durch die aus der Schule bekannten Venn-Diagramme dargestellt. Die vier obigen Operationen auf zwei Mengen lassen sich wie folgt visualisieren:

Dabei sind die dunkler dargestellten Punktmengen immer das Ergebnis der jeweiligen Mengenoperationen auf den durch die Kreis A und B eingefassten Punktmengen. Diese Darstellungsformen sind zwar illustrativ; sie sind jedoch keinesfalls ausreichend für Beweise.

Beispiele: Es seien $A = \{2, 3, 5, 7, 11\}$ und $B = \{2, 3, 4, 5, 6\}$. Dann gilt:

- $A \cup B = \{2, 3, 4, 5, 6, 7, 11\}$
- $A \cap B = \{2, 3, 5\}$
- $A \setminus B = \{7, 11\}$
- $B \setminus A = \{4, 6\}$
- $A \triangle B = \{4, 6, 7, 11\}$
- $(A \setminus B) \cap B = \{7, 11\} \cap \{2, 3, 4, 5, 6\} = \emptyset$

Zwei Mengen A und B heißen disjunkt genau dann, wenn $A \cap B = \emptyset$ gilt.

Die logische Formulierung der Zugehörigkeit von Elementen zu einer Menge ermöglicht eine einfache Gewinnung von Rechenregeln durch Übertragung der logischen Äquivalenzen. Eine Auswahl sinnvoller Rechenregeln wird in folgendem Theorem gegeben.

Theorem 3.2

Es seien A, B und C Mengen (über dem Universum U). Dann gilt:

1. $(A \cap B) \cap C = A \cap (B \cap C)$ — Assoziativgesetze
   $(A \cup B) \cup C = A \cup (B \cup C)$
2. $A \cap B = B \cap A$ — Kommutativgesetze
   $A \cup B = B \cup A$
3. $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ — Distributivgesetze
   $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$
4. $\overline{A \cap B} = \overline{A} \cup \overline{B}$ — De Morgansche Regeln
   $\overline{A \cup B} = \overline{A} \cap \overline{B}$
5. Wenn $A \subseteq B$, dann $\overline{B} \subseteq \overline{A}$ — Kontraposition
6. $\overline{\overline{A}} = A$ — Doppeltes Komplement

Beweis: Wir zeigen exemplarisch die erste De Morgansche Regel, um den Zusammenhang zur logischen Äquivalenz zu verdeutlichen.

$$\begin{aligned}
\overline{A \cup B} &= \{\, x \in U \mid x \notin A \cup B \,\} \\
&= \{\, x \in U \mid \neg(x \in A \cup B) \,\} \\
&= \{\, x \in U \mid \neg(x \in A \vee x \in B) \,\} \\
&= \{\, x \in U \mid \neg(x \in A) \wedge \neg(x \in B) \,\} \qquad \text{(De Morgansche Regel der Aussagenlogik)} \\
&= \{\, x \in U \mid x \notin A \wedge x \notin B \,\} \\
&= \{\, x \in U \mid x \in \overline{A} \wedge x \in \overline{B} \,\} \\
&= \overline{A} \cap \overline{B}
\end{aligned}$$

Damit ist das Theorem bewiesen. ■

Beispiel: Die Regeln aus Theorem 3.2 lassen sich verwenden, um aus Venn-Diagrammen leicht abzulesende Mengengleichheiten formal zu beweisen. Zum Beispiel ist die Identität $A \setminus B = A \setminus (A \cap B)$ einfach auszurechnen:

$$A \setminus (A \cap B) = A \cap \overline{A \cap B} = A \cap (\overline{A} \cup \overline{B}) = (A \cap \overline{A}) \cup (A \cap \overline{B}) = \emptyset \cup (A \cap \overline{B}) = A \cap \overline{B} = A \setminus B$$

3.3 Rechnen mit unendlich vielen Mengen

In einigen Fällen werden auch Verallgemeinerungen von Vereinigung und Durchschnitt auf eine beliebige, auch unendliche, Anzahl von Mengen betrachtet. Dazu betrachten wir Teilmengen eines Universums U. Weiterhin sei I eine beliebige Menge (Indexmenge). Für jedes $i \in I$ sei eine Menge $A_i \subseteq U$ gegeben. Dann sind Vereinigung und Durchschnitt aller A_i definiert als:

$$\bigcup_{i \in I} A_i =_{\text{def}} \{\, a \mid (\exists i \in I)[a \in A_i] \,\}$$

$$\bigcap_{i \in I} A_i =_{\text{def}} \{\, a \mid (\forall i \in I)[a \in A_i] \,\}$$

Für $I = \mathbb{N}$ schreiben wir auch $\bigcup_{i=0}^{\infty} A_i$ bzw. $\bigcap_{i=0}^{\infty} A_i$.

Beispiele: Folgende Beispiele und Spezialfälle sollen die Wirkungsweise von allgemeiner Vereinigung und Durchschnitt demonstrieren:

- Es seien $U = \mathbb{R}$, $I = \mathbb{N}_+$ und

  $$A_k =_{\text{def}} \left\{ x \;\middle|\; |x^2 - 1| \leq \frac{1}{k} \right\}$$

  Dann gilt:

  $$\begin{aligned}
  \bigcup_{k \in I} A_k = \bigcup_{k=1}^{\infty} A_k &= \left\{ x \;\middle|\; |x^2 - 1| \leq 1 \right\} \\
  &= \left\{ x \;\middle|\; -\sqrt{2} \leq x \leq \sqrt{2} \right\} \overset{\text{def}}{=} \left[-\sqrt{2}, \sqrt{2}\right]
  \end{aligned}$$

  $$\bigcap_{k \in I} A_k = \bigcap_{k=1}^{\infty} A_k = \{-1, 1\}$$

- Es gilt stets $\bigcup_{i \in \emptyset} A_i = \emptyset$. Dies ist verträglich mit folgender Rechenregel für Indexmengen I_1 und I_2:

$$\left(\bigcup_{i \in I_1} A_i \right) \cup \left(\bigcup_{i \in I_2} A_i \right) = \bigcup_{i \in I_1 \cup I_2} A_i$$

- Es gilt stets $\bigcap_{i \in \emptyset} A_i = U$. Dies ist verträglich mit folgender Rechenregel für Indexmengen I_1 und I_2:

$$\left(\bigcap_{i \in I_1} A_i \right) \cap \left(\bigcap_{i \in I_2} A_i \right) = \bigcap_{i \in I_1 \cup I_2} A_i$$

Wir merken abschließend an, dass auch die logischen Äquivalenzen für quantifizierte Aussagen ihre Entsprechung auf Mengenebene besitzen:

$$\bigcup_{i \in I} A_i \ \cup \bigcup_{i \in I} B_i = \bigcup_{i \in I} (A_i \cup B_i) \qquad \text{bzw.} \qquad \bigcap_{i \in I} A_i \ \cap \bigcap_{i \in I} B_i = \bigcap_{i \in I} (A_i \cap B_i)$$

und insbesondere

$$\overline{\bigcup_{i \in I} A_i} = \bigcap_{i \in I} \overline{A_i} \qquad \text{bzw.} \qquad \overline{\bigcap_{i \in I} A_i} = \bigcup_{i \in I} \overline{A_i}$$

3.4 Potenzmengen

Mengen von Mengen heißen (Mengen)Familien. Um dies widerspruchsfrei einzuführen, benötigen wir die Operation der Potenzmengenbildung, die von einem anderen Typ als Vereinigung, Durchschnitt und Differenzen ist. Die Potenzmenge einer Menge A ist definiert als

$$\mathcal{P}(A) =_{\text{def}} \{ X \mid X \subseteq A \}$$

Für die Potenzmenge von A gelten folgenden Aussagen:

Proposition 3.3

Es sei A eine beliebige Menge.

1. $X \in \mathcal{P}(A) \Longleftrightarrow X \subseteq A$
2. $\emptyset, A \in \mathcal{P}(A)$
3. Ist A endlich, so gilt $|\mathcal{P}(A)| = 2^{|A|}$.

Beweis: Die ersten beiden Aussagen folgen direkt aus der Definition. Die dritte Aussage werden wir im Kapitel über Kombinatorik beweisen. ■

Die Elemente der Potenzmenge sind also Mengen aus dem Universum $\mathcal{P}(A)$. Der letzte Sachverhalt lässt die mitunter auch verwendete Bezeichnung 2^A für die Potenzmenge von A plausibel erscheinen.

Beispiele: Folgende Mengen verdeutlichen die Potenzmengenkonstruktion.

- $\mathcal{P}(\{1\}) = \{\emptyset, \{1\}\}$

- $\mathcal{P}(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$
- $\mathcal{P}(\{1,2,3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$
- $\mathcal{P}(\emptyset) = \{\emptyset\}$
- $\mathcal{P}(\mathcal{P}(\emptyset)) = \mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$
- $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset))) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$

Die Teilmengen der Potenzmenge heißen Mengenfamilien.

Beispiel: Für eine Menge A und $k \in \mathbb{N}$ ist $\mathcal{P}_k(A)$ definiert als

$$\mathcal{P}_k(A) =_{\text{def}} \{\ X \mid X \subseteq A, |X| = k\ \}.$$

Insbesondere ist also $\mathcal{P}_1(A)$ die Familie der Einermengen von A, $\mathcal{P}_2(A)$ ist die Familien der Zweiermengen von A usw. usf. Für $|A| = n < \infty$ gilt

$$\mathcal{P}(A) = \bigcup_{k=0}^{n} \mathcal{P}_k(A).$$

Eine wichtige Mengenfamilie ist die Partition oder Zerlegung eines Universums.

Definition 3.4

Eine Mengenfamilie $\mathcal{F} \subseteq \mathcal{P}(A)$ heißt (ungeordnete) Partition von A, falls folgende Bedingungen erfüllt sind:

1. $B \cap C = \emptyset$ für alle Mengen $B, C \in \mathcal{F}$ mit $B \neq C$
2. $\bigcup_{B \in \mathcal{F}} B = A$

Die Mengen $B \in \mathcal{F}$ heißen Komponenten der Partition.

Leere Mengen werden als Komponenten einer Partition weggelassen.

Beispiele: Folgende Familien verdeutlichen das Konzept von Partitionen.

- $\{\mathbb{R}_{<0}, \{0\}, \mathbb{R}_{>0}\}$ ist eine Partition von $\mathbb{R}$ mit drei Komponenten.
- $\{\ \{x\} \mid x \in \mathbb{R}\ \}$ ist eine Partition von $\mathbb{R}$ mit unendlich vielen Komponenten. (Genauer gesagt besteht die Partition aus überabzählbar vielen Komponenten.)
- Für jede Menge $A \subseteq U$ ist $\{A, \overline{A}\}$ eine Partition von U mit zwei Komponenten. Tatsächlich ist für jede Menge $U \neq \emptyset$ die Partition $\{A, \overline{A}\}$ die einzige Partition von U, die die Menge A als Komponente besitzt. Dazu muss nur gezeigt werden, dass für zwei Partitionen $\{A, B\}$ und $\{A, \overline{A}\}$ stets $B = \overline{A}$ gilt. Dies ist leicht einzusehen, da einerseits $A \cap B = \emptyset$ äquivalent zu $A \subseteq \overline{B}$ und andererseits $A \cup B = U$ einmal äquivalent zu $\overline{A} \cap \overline{B} = \emptyset$ und somit auch zu $\overline{B} \subseteq A$ ist. Damit folgt $B = \overline{A}$.

Im letzten Beispiel haben wir die Gleichheit zweier Partitionen dadurch gezeigt, dass wir die Gleichheit aller einzelnen Komponenten nachgeweisen haben ($A = A$ und $B = \overline{A}$). Damit haben wir

uns zuviel Arbeit gemacht. Es hätte genügt Inklusionen der Komponenten zu zeigen ($A \subseteq A$ und $B \subseteq \overline{A}$). Die Gleichheiten der Komponenten folgen mittels des Hauberschen Theorems.

Theorem 3.5 (Hauber)

Es seien $\{ A_i \mid i \in I \}$ und $\{ B_i \mid i \in I \}$ zwei Partitionen von U mit einer beligen Indexmenge I. Gilt $A_i \subseteq B_i$ für alle $i \in I$, so gilt $B_i \subseteq A_i$ (und mithin $A_i = B_i$) für alle $i \in I$.

Beweis: Es sei A_i eine beliebige Komponente mit $i \in I$. Dann gilt

$$\emptyset = \overline{U} = \overline{A_i \cup \bigcup_{j \in I \setminus \{i\}} A_j} = \overline{A_i} \cap \overline{\bigcup_{j \in I \setminus \{i\}} A_j}$$

und somit

$$\overline{A_i} \subseteq \bigcup_{j \in I \setminus \{i\}} A_j \subseteq \bigcup_{j \in I \setminus \{i\}} B_j \subseteq \overline{B_i}$$

Daraus folgt $B_i \subseteq A_i$. Damit ist der Satz bewiesen. ■

4 Relationen

Relationen beschreiben die Beziehungen zwischen Mengen und sind somit der eigentliche Gegenstand der Mathematik.

4.1 Kreuzprodukt

Es seien $A_1, \ldots, A_n$ beliebige Mengen. Das Kreuzprodukt (oder kartesisches Produkt) von $A_1, \ldots, A_n$ ist definiert als:

$$A_1 \times \cdots \times A_n =_{\text{def}} \{ (a_1, \ldots, a_n) \mid \text{für alle } i \in \{1, \ldots, n\} \text{ gilt } a_i \in A_i \}$$

Die Elemente von $A_1 \times \cdots \times A_n$ heißen n-Tupel (mit speziellen Benennungen für feste n: Paare für $n = 2$, Tripel für $n = 3$, Quadrupel für $n = 4$).

Im Gegensatz zu Mengen sind Tupel geordnet (und damit eine Formalisierung von Listen): Für zwei n-Tupel $(a_1, \ldots, a_n)$ und $(a'_1, \ldots, a'_n)$ gilt

$$(a_1, \ldots, a_n) = (a'_1, \ldots, a'_n) \iff \text{für alle } i \in \{1, \ldots, n\} \text{ gilt } a_i = a'_i$$

Sind alle Mengen gleich, so schreibt man:

$$A^n =_{\text{def}} \underbrace{A \times \cdots \times A}_{n\text{-mal}}$$

Beispiele: Folgende Mengen verdeutlichen die Kreuzproduktkonstruktion.

- Mit $A = \{1, 2, 3\}$ und $B = \{a, b\}$ gilt $A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$
- Mit $A = \{5, 7\}$ und $n = 3$ gilt

$$\begin{aligned} A^3 &= \{5, 7\} \times \{5, 7\} \times \{5, 7\} \\ &= \{(5, 5, 5), (5, 5, 7), (5, 7, 5), (5, 7, 7), (7, 5, 5), (7, 5, 7), (7, 7, 5), (7, 7, 7)\} \end{aligned}$$

- $\emptyset \times A = \emptyset$ (Beachte: Die rechte leere Menge ist die Menge in der kein Paar enthalten ist)
- $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ beschreibt den dreidimensionalen Raum

Es seien $A_1, \ldots, A_n$ beliebige Mengen. Eine Menge $R \subseteq A_1 \times \cdots \times A_n$ heißt n-stellige Relation.

Beispiel: Eine relationale Datenbank ist eine Sammlung von Tabellen mit einer gewissen Struktur. Eine Tabelle wiederum ist eine (extensionale Darstellung einer) Relation. Beispielsweise sei folgender Auszug einer Tabelle gegeben:

Vorname	Name	Geburtsdatum
Max	Mustermann	07.07.1987
Erika	Mustermann	12.09.1955
John	Smith	05.05.1965
Lyudmila	Dyakovska	02.04.1976
Karsten	Brill	27.10.1980
Timnit	Gebru	13.05.1983
Robert	Palfrader	11.11.1968
Ruth Maria	Renner	27.09.1980
Leslie	Valiant	28.03.1949
Harvey	Elliott	04.04.2003
⋮	⋮	⋮

Wir fassen die Tabelle als Teilmenge eines Kreuzproduktes auf. Dazu seien:

$$\begin{aligned} A_1 &=_{\text{def}} \text{Menge aller Vornamen in der Tabelle} \\ A_2 &=_{\text{def}} \text{Menge aller Namen in der Tabelle} \\ A_3 &=_{\text{def}} \text{Menge aller Geburtsdaten in der Tabelle} \end{aligned}$$

Dann ist $(\texttt{Max}, \texttt{Mustermann}, 07.07.1987) \in A_1 \times A_2 \times A_3$ und die Menge aller Zeilen der Tabelle ist eine Relation $R \subseteq A_1 \times A_2 \times A_3$.

Eine Relation $R \subseteq A_1 \times A_2$ heißt binäre Relation. Gilt $A_1 = A_2 = A$, so sprechen wir von einer binären Relation auf A. Binäre Relationen R werde auch in Infix-Notation geschrieben:

$$xRy \iff_{\text{def}} (x, y) \in R$$

Der Ausdruck „xRy“ steht dabei für die Leseweise: „x steht in Relation R zu y.“

Beispiele: Wir betrachten binäre Relationen über der Menge $A = \mathbb{N}$.

- $R_1 =_{\text{def}} \mathbb{N} \times \mathbb{N}$
- $R_2 =_{\text{def}} \{(0,0), (2,3), (5,1), (5,3)\}$
- $R_3 =_{\text{def}} \{\ (n_1, n_2) \mid n_1 \leq n_2\ \} = \{(0,0), (0,1), (1,1), (0,2), \ldots\}$
- $R_4 =_{\text{def}} \{\ (n_1, n_2) \mid n_1 \text{ teilt } n_2\ \} = \{(1,2), (2,4), (2,6), (7,0), \ldots\}$
- $R_5 =_{\text{def}} \{\ (n_1, n_2) \mid 2 \text{ teilt } |n_1 - n_2|\ \} = \{(0,2), (2,2), (1,1), (3,1), \ldots\}$
- $R_6 =_{\text{def}} \{\ (n_1, n_2) \mid 2n_1 = n_2\ \} = \{(0,0), (1,2), (2,4), (3,6), \ldots\}$

Die Relationen R_3 und R_4 sind Ordnungsrelationen. Relation R_5 ist eine Äquivalenzrelation. Relation R_6 ist eine Funktion.

In den folgenden Abschnitten wenden wir uns den im Beispiel erwähnten Relationentypen systematisch zu.

4.2 Äquivalenzrelationen

Äquivalenzrelationen extrahieren den mathematischen Gehalt von Objekten, die wir als im Wesentlichen gleich ansehen können. Dafür werden die folgenden Begriffe benötigt.

Definition 4.1

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

1. reflexiv $\iff_{\text{def}}$ $(\forall a \in A)[(a,a) \in R]$
2. transitiv $\iff_{\text{def}}$ $(\forall a,b,c \in A)[((a,b) \in R \wedge (b,c) \in R) \to (a,c) \in R]$
3. symmetrisch $\iff_{\text{def}}$ $(\forall a,b \in A)[(a,b) \in R \to (b,a) \in R]$
4. Äquivalenzrelation $\iff_{\text{def}}$ R ist reflexiv, transitiv und symmetrisch

Bei einer Äquivalenzrelation R verwenden wir statt $(a,b) \in R$ die Infix-Schreibweise $a \sim_R b$ (oder $a \approx_R b$, $a \equiv_R b$).

Beispiele: Wir überprüfen die Eigenschaften für folgende endliche Relationen über der Menge $A = \{0,1,2\}$:

Relation	reflexiv	transitiv	symmetrisch	Äquivalenzrelation
$\{ (0,1),(1,0),(0,2),(2,0) \}$			X	
$\{ (0,0),(0,1),(1,0),(1,1),(0,2),(2,0),(2,2) \}$	X		X	
$\{ (0,0),(0,1),(1,0),(1,1),(2,2) \}$	X	X	X	X
$\{ (0,0),(0,1),(1,0),(1,1) \}$		X	X	
$\{ (0,0),(0,1),(1,1),(2,2) \}$	X	X		

Wir wollen die Intuitivität des Äquivalenzrelationenbegriff an komplexeren Relationen verdeutlichen.

Beispiele: Folgende Beispiele sind typisch für die Bildung von Äquivalenzrelationen.

- Es seien $A =_{\text{def}}$ Menge aller (logischen) Aussagen und

  $$R =_{\text{def}} \{ (H,H') \mid H \leftrightarrow H' \text{ ist eine Tautologie } \} \subseteq A \times A.$$

  Dann ist R eine Äquivalenzrelation, denn es gelten folgende Aussagen (z.B. mittels Überprüfung durch Wertetabellen):

  - R ist reflexiv: $H \leftrightarrow H$ ist eine Tautologie für alle Aussagen H
  - R ist transitiv: Sind $H \leftrightarrow H'$ und $H' \leftrightarrow H''$ Tautologien, so ist auch $H \leftrightarrow H''$ eine Tautologie (wegen doppelter Anwendung der Kettenschlussregel)

- R ist symmetrisch: Ist $H \leftrightarrow H'$ eine Tautologie, so ist auch $H' \leftrightarrow H$ eine Tautologie.

- Es sei f beliebige Funktion mit Argumenten aus einer Menge A. Dann ist die Relation

$$R_f =_{\text{def}} \{ (x, y) \mid f(x) = f(y) \} \subseteq A \times A$$

ganz offensichtlich eine Äquivalenzrelation. Zum Beispiel ergeben sich für spezielle Funktionen folgende Äquivalenzrelationen:

  - Auf der Menge $A =_{\text{def}} \mathbb{Z}$ sei die Funktion $f_n(x) = \text{mod}(x, n)$ mit Funktionswerten in der Menge $\{0, 1, \ldots, n-1\}$ definiert. Dann schreiben wir auch $x \equiv y \bmod n$ für $(x, y) \in R_{f_n}$ und sagen „x ist kongruent y modulo n“.
  - Auf der Menge A aller Wörter eines Wörterbuches (wobei alle Wörter nur aus Kleinbuchstaben bestehen und keine Umlaute enthalten) sei f als Funktion definiert, die jedes Wort auf den ersten Buchstaben abbildet. Zwei Wörter sind damit also äquivalent, wenn sie mit dem gleichen Buchstaben beginnen.

Definition 4.2

Es seien $R \subseteq A \times A$ eine Äquivalenzrelation und $x \in A$ ein beliebiges Element. Dann heißt die Menge

$$[x]_R =_{\text{def}} \{ y \mid (x, y) \in R \} \subseteq A$$

Äquivalenzklasse von x. Wir nennen x Repräsentant der Äquivalenzklasse.

Beispiel: Wir betrachten die Kongruenz „ $\equiv \bmod 8$ “ auf den ganzen Zahlen. Dann gilt:

$$\begin{aligned} [13]_{\equiv} &= \{ y \mid y \equiv 13 \bmod 8 \} \\ &= \{ y \mid \text{mod}(y - 13, 8) = 0 \} \\ &= \{\ldots, -11, -3, 5, 13, 21 \ldots\} \\ &= [5]_{\equiv} \end{aligned}$$

Proposition 4.3

Es seien $R \subseteq A \times A$ eine Äquivalenzrelation und $x, y \in A$. Dann gilt:

1. Ist $(x, y) \in R$, so gilt $[x]_R = [y]_R$.
2. Ist $(x, y) \notin R$, so sind $[x]_R$ und $[y]_R$ disjunkt.

Beweis: Wir beweisen die Aussagen einzeln.

1. Es gelte $(x, y) \in R$, d.h. $y \in [x]_R$. Wegen der Transitivität von R gilt $(x, z) \in R$ für alle $z \in [y]_R$ (d.h. $(y, z) \in R$). Somit gilt $[y]_R \subseteq [x]_R$. Wegen der Symmetrie von R gilt $(y, x) \in R$. Somit können wir analog auch $[x]_R \subseteq [y]_R$ zeigen. Mithin gilt $[x]_R = [y]_R$.
2. Wir zeigen die Kontraposition der Aussage. Dazu gelte $[x]_R \cap [y]_R \neq \emptyset$. Dann gibt es ein $z \in A$ mit $z \in [x]_R$ und $z \in [y]_R$ bzw. $(x, z) \in R$ und $(y, z) \in R$. Wegen der Symmetrie von R gilt $(z, y) \in R$. Wegen der Transitivität gilt somit $(x, y) \in R$.

Damit ist die Proposition bewiesen. ■

Definition 4.4

Es sei $R \subseteq A \times A$ eine Äquivalenzrelation. Eine Menge $K \subseteq A$ heißt Repräsentantensystem von R, falls folgende Bedingungen erfüllt sind:

1. Für alle $k_1, k_2 \in K$ mit $k_1 \neq k_2$ gilt $(k_1, k_2) \notin R$
2. $A = \bigcup_{k \in K} [k]_R$

Beispiel: Wir betrachten die Kongruenz „ $\equiv \mod 8$ “ auf den ganzen Zahlen.

- $\{0, 1, 2, 3, 4, 5, 6, 7\}$ ist ein Repräsentantensystem
- $\{8, 1, 2, 19, -4, 13, 6, 7\}$ ist ebenfalls ein Repräsentantensystem

Die zu einem Repräsentantensystem gehörenden Äquivalenzklassen bilden eine Partition der Grundmenge.

Korollar 4.5

Es seien $R \subseteq A \times A$ eine Äquivalenzrelation und $K \subseteq A$ ein Repräsentantensystem von R. Dann bilden die Äquivalenzklassen (der Elemente) von K eine Partition von A.

Beweis: Wegen $(k_1, k_2) \notin R$ für $k_1, k_2 \in K$ mit $k_1 \neq k_2$ (die erste Eigenschaft eines Repäsentantensystems) folgt aus Proposition 4.3:

$$[k_1]_R \cap [k_2]_R = \emptyset$$

Aus der zweiten Eigenschaft eines Repräsentantensystem folgt für K weiterhin

$$\bigcup_{k \in K} [k]_R = A.$$

Somit ist die Mengenfamilie $\{\, [k]_R \mid k \in K \,\}$ eine Partition von A. Damit ist das Korollar bewiesen. ■

Proposition 4.6

Es sei $\mathcal{F} \subseteq \mathcal{P}(A)$ eine Partition von A. Dann ist die Relation $R \subseteq A \times A$ mit

$$(x, y) \in R \quad \Longleftrightarrow_{\text{def}} \quad (\exists X \in \mathcal{F})[x \in X \wedge y \in X]$$

eine Äquivalenzrelation.

Beweis: Wir überprüfen die Eigenschaften von Äquivalenzrelationen:

- R ist reflexiv: Für jedes $x \in A$ gibt es ein $X \in \mathcal{F}$ mit $x \in X$, da $\mathcal{F}$ eine Partition ist. Somit gilt $(x, x) \in R$.
- R ist transitiv: Es seien $(x, y) \in R$ und $(y, z) \in R$. Dann gibt es $X_1, X_2 \in \mathcal{F}$ mit $x, y \in X_1$ sowie $y, z \in X_2$. Mithin gilt $y \in X_1 \cap X_2$. Also sind X_1 und X_2 nicht disjunkt. Da $\mathcal{F}$ eine Partition ist, gilt folglich $X_1 = X_2$. Somit gilt $x, z \in X_1$. Es folgt $(x, z) \in R$.
- R ist symmetrisch: Ist $(x, y) \in R$, so gilt $x, y \in X$ für ein geeignetes $X \in \mathcal{F}$. Also gilt auch $(y, x) \in R$.

Damit ist die Proposition bewiesen ■

4.3 Ordnungsrelationen

Ordnungsrelationen extrahieren den mathematischen Gehalt von natürlichen Ordnungen, wie sie beispielsweise beim Sortieren benötigt werden. Formal unterscheiden sie sich von Äquivalenzrelationen nur durch den Begriff der Antisymmetrie.

Definition 4.7

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

1. reflexiv $\iff_{\text{def}} (\forall a \in A)[(a, a) \in R]$
2. transitiv $\iff_{\text{def}} (\forall a, b, c \in A)[((a, b) \in R \wedge (b, c) \in R) \rightarrow (a, c) \in R]$
3. antisymmetrisch $\iff_{\text{def}} (\forall a, b \in A)[((a, b) \in R \wedge (b, a) \in R) \rightarrow a = b]$
4. linear $\iff_{\text{def}} (\forall a, b \in A)[a \neq b \rightarrow ((a, b) \in R \vee (b, a) \in R)]$

Die Eigenschaft der Antisymmetrie wird anschaulicher, wenn für alle $a, b \in A$ die Kontraposition

$$a \neq b \rightarrow ((a, b) \notin R \vee (b, a) \notin R)$$

betrachtet wird. Mit anderen Worten darf für verschiedene Elemente a und b höchstens eines der Paare (a, b) oder (b, a) zu R gehören. Zu beachten ist weiterhin, dass die Eigenschaft der Antisymmetrie nicht die Negation der Symmetrie ist, wie sie im Abnschnitt über Äquivalenzrelationen eingeführt wird.

Beispiele: Wir überprüfen die Eigenschaften für folgende endliche Relationen über der Menge $A = \{0, 1, 2\}$:

Relation	reflexiv	transitiv	antisymmetrisch	linear
$\{ (0,0), (0,1), (0,2), (1,1), (1,2), (2,2) \}$	X	X	X	X
$\{ (0,0), (0,1), (2,0), (1,1), (1,2), (2,2) \}$	X		X	X
$\{ (0,0), (0,1), (2,0), (0,2), (1,1), (1,2), (2,2) \}$	X			X
$\{ (0,0), (0,1), (2,0), (0,2), (1,1), (2,2) \}$	X			
$\{ (0,1), (2,0), (0,2), (1,1), (2,2) \}$				
$\{ (0,1), (1,2), (0,2) \}$		X	X	X
$\{ (0,0), (0,1), (1,0), (1,1), (2,2) \}$	X	X		
$\{ (0,0), (0,1), (0,2), (1,1), (2,2) \}$	X	X	X	
$\{ (0,1), (1,2), (2,1), (2,0) \}$				X

Durch die Analyse der obigen Beispiele bekommt man ein technisches Gefühl für die Definitionen. Im Folgenden wollen wir auch die Intuitivität von Definition 4.7 durch weitere Beispiele verdeutlichen.

Beispiele: Die folgenden Beispiele repräsentieren im Allgemeinen unendliche Relationen.

- $R_1 =_{\text{def}} \{ (m,n) \mid m \leq n \} \subseteq \mathbb{N}^2$, wobei $m \leq n \Leftrightarrow_{\text{def}} (\exists c \in \mathbb{N})[n = m + c]$. Dann gilt:
  - R_1 ist reflexiv, denn für alle $n \in \mathbb{N}$ gilt $n = n + 0$ bzw. $n \leq n$.
  - R_1 ist transitiv, denn gilt $k \leq m$ und $m \leq n$, so gibt es $c_1, c_2 \in \mathbb{N}$ mit $m = k + c_1$ sowie $n = m + c_2$ und es gilt $n = k + (c_2 + c_1)$ bzw. $k \leq n$.
  - R_1 ist antisymmetrisch, denn gilt $m \leq n$ und $n \leq m$, so gibt es $c_1, c_2 \in \mathbb{N}$ mit $n = m + c_1$ sowie $m = n + c_2$ und mit $n = n + c_1 + c_2$ folgt $c_1 = c_2 = 0$ und mithin $n = m$.
  - R_1 ist linear, denn $n - m \in \mathbb{N}$ oder $m - n \in \mathbb{N}$.

  R_1 besitzt mithin alle Eigenschaften von Definition 4.7.
- $R_2 =_{\text{def}} \{ (m,n) \mid m \text{ teilt } n \}$, wobei $m|n \Leftrightarrow_{\text{def}} (\exists c \in \mathbb{N})[n = c \cdot m]$. Dann gilt:
  - R_2 ist reflexiv, denn für alle $n \in \mathbb{N}$ gilt $n = 1 \cdot n$ bzw. n teilt n.
  - R_2 ist transitiv, denn teilt k die Zahl m und teilt m die Zahl n, so gibt es $c_1, c_2 \in \mathbb{N}$ mit $m = c_1 \cdot k$ sowie $n = c_2 \cdot m$ und es gilt $n = (c_2 \cdot c_1) \cdot k$ bzw. k teilt n.
  - R_2 ist antisymmetrisch, denn teilt m die Zahl n und teilt n die Zahl m, so gibt es $c_1, c_2 \in \mathbb{N}$ mit $n = c_1 \cdot m$ sowie $m = c_2 \cdot n$ und mit $n = c_1 \cdot c_2 \cdot n$ folgt $c_1 = c_2 = 1$ und mithin $m = n$.
  - R_2 ist nicht linear, denn weder teilt 2 die Zahl 3 noch teilt 3 die Zahl 2.

  R_2 besitzt mithin alle Eigenschaften von Definition 4.7 außer der Linearität.
- $R_3 =_{\text{def}} \{ (A,B) \mid A \subseteq B \} \subseteq \mathcal{P}(X)^2$ für eine Grundmenge X. Dann gilt:
  - R_3 ist reflexiv, denn es gilt $A \subseteq A$ für alle $A \subseteq X$.
  - R_3 ist transitiv, denn gilt $A \subseteq B$, d.h. $(\forall a \in A)[a \in B]$, und gilt $B \subseteq C$, d.h. $(\forall a \in B)[a \in C]$, so gilt nach dem Kettenschluss auch $(\forall a \in A)[a \in C]$, d.h. $A \subseteq C$.
  - R_3 ist antisymmetrisch, denn mit $A \subseteq B$ und $B \subseteq A$ gilt $A = B$.

- R_3 ist nicht linear, falls $|X| \geq 2$: Es seien $a, b \in X$ mit $a \neq b$, dann gilt $\{a\} \cap \{b\} = \emptyset$.

R_3 besitzt mithin alle Eigenschaften von Definition 4.7 außer der Linearität.

Definition 4.8

Es sei $R \subseteq A \times A$ eine binäre Relation über A.

1. R heißt Halbordnung (oder partielle Ordnung), falls R reflexiv, transitiv und antisymmetrisch ist.
2. R heißt Ordnung (oder totale bzw. lineare Ordnung), falls R eine Halbordnung und zusätzlich linear ist.
3. Ist R eine Halbordnung, so heißt das Paar (A, R) halbgeordnete Menge (oder partiell geordnete Menge).
4. Ist R eine Ordnung, so heißt das Paar (A, R) geordnete Menge (oder total bzw. linear geordnete Menge).

Beispiele (Fortsetzung): Für die drei Relationen aus obigem Beispiel gilt:

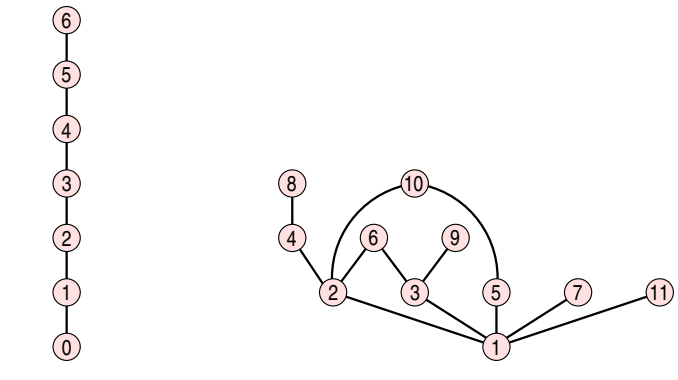
- R_1 ist eine Ordnung; wir schreiben die geordnete Menge als $(\mathbb{N}, \leq)$.
- R_2 ist eine Halbordnung; wir schreiben die halbgeordnete Menge als $(\mathbb{N}, |)$.
- R_3 ist eine Halbordnung für jede Menge X; wir schreiben die halbgeordnete Menge als $(\mathcal{P}(X), \subseteq)$.

Endliche Halbordnungen lassen sich durch Hasse-Diagramme graphisch darstellen. Diese Diagramme sind wie folgt für eine halbgeordnete Menge (A, R) definiert:

- Elemente der Grundmenge A werden durch Punkte (Knoten) in der Ebene dargestellt.
- Ist $(x, y) \in R$ für $x \neq y$, so wird der Knoten y oberhalb von Knoten x gezeichnet.
- Genau dann, wenn $(x, y) \in R$ für $x \neq y$ gilt und es kein $z \notin \{x, y\}$ mit $(x, z) \in R$ und $(z, y) \in R$ gibt, werden x und y durch eine Linie (Kante) verbunden.

Bei dieser Darstellungsform werden jene Paare einer Halbordnung nicht dargestellt, deren Zugehörigkeit zur Relation sich wegen der Transitivität sowieso aus den anderen Paaren ergeben würde. Eine derart vollständig reduzierte Relation heißt auch transitive Reduktion einer Halbordnung.

Beispiele: Die folgende Abbildung zeigt Hasse-Diagramme für die beiden endlichen, halbgeordneten Mengen $(\{0, 1, \ldots, 6\}, \leq)$ und $(\{1, \ldots, 11\}, |)$:



$(\{0, 1, \ldots, 6\}, \leq)$ $(\{1, \ldots, 11\}, |)$

Im Folgenden verwenden wir $x \leq_R y$ für $(x, y) \in R$, falls R eine Halbordnung ist.

Definition 4.9

Es seien $R \subseteq A \times A$ eine Halbordnung und $K \subseteq A$.

1. Ein Element $a \in K$ heißt Minimum (bzw. Maximum) von K, falls $a \leq_R b$ (bzw. $b \leq_R a$) für alle $b \in K$ gilt.
2. Ein Element $a \in A$ heißt untere Schranke (bzw. obere Schranke) von K, falls $a \leq_R b$ (bzw. $b \leq_R a$) für alle $b \in K$ gilt.
3. Ein Element $a \in A$ heißt Infimum (bzw. Supremum) von K, falls a eine untere Schranke (bzw. obere Schranke) von K ist und $b \leq_R a$ (bzw. $a \leq_R b$) für alle unteren Schranken (bzw. oberen Schranken) b von K gilt.

Der Unterschied zwischen einer unteren Schranke von K und einem Minimum von K liegt darin, dass die untere Schranke nicht zur Menge K gehören muss, was für das Minimum verlangt ist. Gleiches gilt natürlich auch für obere Schranken von K und einem Maximum von K. Darüber hinaus sind Minima, Maxima, Infima und Suprema stets eindeutig, falls sie überhaupt existieren.

Proposition 4.10

Es seien $R \subseteq A \times A$ eine Halbordnung und $K \subseteq A$. Existiert das Minimum (Maximum, Infimum, Supremum) von K, so ist es eindeutig.

Beweis: (nur für das Minimum) Es seien $a, a' \in K$ Minima von K. Dann gilt $a \leq_R a'$, da a ein Minimum von K ist, und es gilt $a' \leq_R a$, da a' ein Minimum von K ist. Wegen der Antisymmetrie von $\leq_R$ gilt $a = a'$. Damit ist die Proposition bewiesen. ■

Die Eindeutigkeit dieser Elemente ermöglicht uns spezielle Notationen einzuführen:

$$\begin{aligned} \min(K) &\quad \text{steht für das Minimum von } K \\ \max(K) &\quad \text{steht für das Maximum von } K \\ \inf(K) &\quad \text{steht für das Infimum von } K \\ \sup(K) &\quad \text{steht für das Supremum von } K \end{aligned}$$

Anschaulich ist das Infimum die größte untere Schranke und das Supremum die kleinste obere Schranke. Im Allgemeinen müssen Minimum, Maximum, Infimum und Supremum nicht existieren.

Beispiele: Folgende Beispiele verdeutlichen die Begriffsbildungen.

- $\min(\emptyset)$ und $\max(\emptyset)$ existieren für keine Halbordnung.
- Es sei $A =_{\text{def}} \mathbb{Q}$ und $R =_{\text{def}} \{ (m, n) \mid m \leq n \}$. Für die Mengen

$$\begin{aligned} K_+ &=_{\text{def}} \{ x \mid 0 < x \} \subseteq A \\ K_- &=_{\text{def}} \{ x \mid x < 0 \} \subseteq A \end{aligned}$$

  gelten die folgenden Aussagen:

- $\min(K_+)$ und $\min(K_-)$ existieren nicht
- $\max(K_+)$ und $\max(K_-)$ existieren nicht
- Die Menge der unteren Schranken von K_+ ist $K_- \cup \{0\}$
- Die Menge der unteren Schranken von K_- ist $\emptyset$
- Die Menge der oberen Schranken von K_+ ist $\emptyset$
- Die Menge der oberen Schranken von K_- ist $K_+ \cup \{0\}$
- $\inf(K_+) = \max(K_- \cup \{0\}) = 0$
- $\inf(K_-)$ existiert nicht
- $\sup(K_+)$ existiert nicht
- $\sup(K_-) = \min(K_+ \cup \{0\}) = 0$

- Wir setzen das vorangehende Beispiel fort. Bei veränderter Grundmenge $A =_{\text{def}} \mathbb{Q} \setminus \{0\}$ sowie unverändertem R, K_+ und K_- gelten die folgenden Aussagen:
  - Die Menge der unteren Schranken von K_+ ist K_-
  - $\inf(K_+)$ existiert nicht, da K_- kein Maximum besitzt
- Für $A =_{\text{def}} \{0, 1, \ldots, 10\}$ und $R =_{\text{def}} \{ (m, n) \mid m \leq n \} \subseteq A \times A$ gelten folgende Aussagen:
  - $\inf(\emptyset) = 10$
  - $\sup(\emptyset) = 0$

Definition 4.11

Es seien $R \subseteq A \times A$ eine Halbordnung und $K \subseteq A$. Ein Element $a \in K$ heißt minimal (bzw. maximal) in K, falls für alle $b \in K$ gilt: Ist $b \leq_R a$ (bzw. $b \geq_R a$), so ist $a = b$.

Beispiel: Es seien $A =_{\text{def}} \mathbb{N}$ und $R =_{\text{def}} \{ (m, n) \mid m \text{ teilt } n \} \subseteq A \times A$. Für

$$K_1 =_{\text{def}} \mathbb{N} \quad \text{und} \quad K_2 =_{\text{def}} \mathbb{N} \setminus \{1\}$$

gelten die Aussagen:

- Die Menge der minimalen Elemente von K_1 ist $\{1\}$
- Die Menge der minimalen Elemente von K_2 ist die Menge der Primzahlen

Proposition 4.12

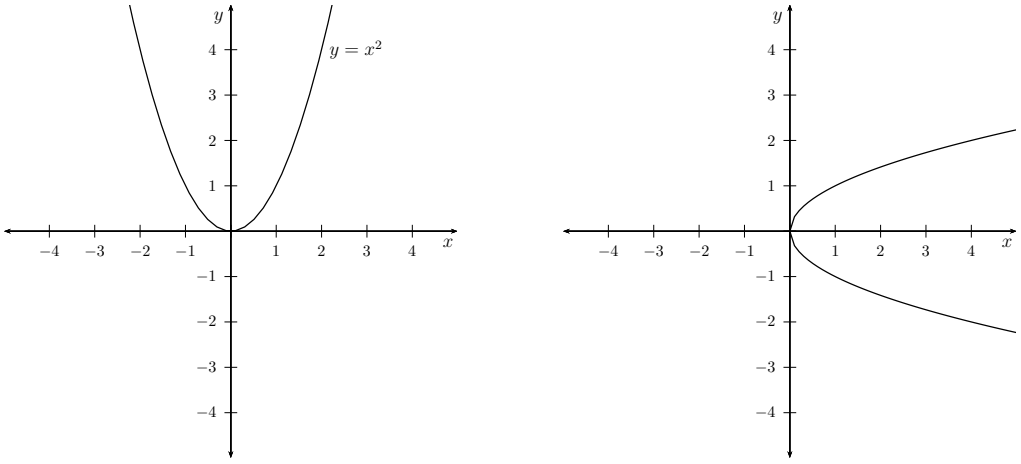
Es seien $R \subseteq A \times A$ eine Ordnung und $K \subseteq A$. Ist $a \in K$ minimal (bzw. maximal) in K, so ist a ein Minimum (bzw. Maximum) von K.

Beweis: (nur für die Minimalität) Es sei $a \in K$ ein minimales Element. Für $b \in K$ gilt $a \leq_R b$ oder $b \leq_R a$ wegen der Totalität von R. Gilt $b \leq_R a$, so folgt $a = b$ (bzw. $a \leq_R b$) wegen der Minimalität von a. Somit gilt in jedem Fall $a \leq_R b$ für alle $b \in K$. Somit ist a das Minimum von K. Damit ist die Proposition bewiesen. ■

4.4 Funktionen und Abbildungen

In diesem Abschnitt führen wir Begriffe ein, die Funktionen, oder synonym Abbildungen, als spezielle Relationen zwischen Mengen von Argumenten und Mengen von Werten charakterisieren.

Beispiel: Das folgende Beispiel soll den relationalen Zugang zur Beschreibung von Funktionen verdeutlichen. Die linke Seite der folgende Abbildung zeigt den Verlauf der Funktion $f(x) =_{\text{def}} x^2$:



Die Funktion $f(x)$ ist dabei extensional über die Menge der Punkte (x, y), die auf der Kurve liegen, festgelegt. Die intensionale Darstellung der Menge der Kurvenpunkte ist also

$$\{\ (x, y) \mid y = x^2\ \} \subseteq \mathbb{R} \times \mathbb{R}$$

Wird die Reihenfolge in den Paaren (bzw. die Achsen des Koordinatensystems) vertauscht, so erhalten wir die auf der rechten Seite dargestellte Kurve und als Menge der Kurvenpunkte:

$$\{\ (y, x) \mid y = x^2\} = \{\ (x, y) \mid y = \sqrt{x} \text{ oder } y = -\sqrt{x}\ \}$$

Diese Menge beschreibt keine Funktion, da für alle $x > 0$ zwei Zuordnungen von Werten existieren.

Folgende Eigenschaften extrahieren den relationalen Gehalt des anschaulichen Funktionsbegriffs.

Definition 4.13

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

1. linkstotal $\iff_{\text{def}} (\forall x \in A)(\exists y \in B)[(x, y) \in R]$
2. rechtseindeutig $\iff_{\text{def}}$
   $(\forall x \in A)(\forall y, z \in B)[((x, y) \in R \wedge (x, z) \in R) \to y = z]$
3. rechtstotal $\iff_{\text{def}} (\forall y \in B)(\exists x \in A)[(x, y) \in R]$
4. linkseindeutig $\iff_{\text{def}}$
   $(\forall x, y \in A)(\forall z \in B)[((x, z) \in R \wedge (y, z) \in R) \to x = y]$

Beispiele: Wir überprüfen die Eigenschaften für folgende Relationen über $A = \{1, 2, 3\}$ und $B = \{1, 2, 3, 4\}$:

Relation		linkstotal	rechtseindeutig	rechtstotal	linkseindeutig
$\{ (1,1), (1,2), (2,2) \}$					
$\{ (1,1), (1,2), (2,2), (3,3) \}$		X			
$\{ (1,1), (2,1) \}$			X		
$\{ (1,1), (1,2), (1,3), (1,4), (2,4) \}$				X	
$\{ (1,1), (1,2) \}$					X
$\{ (1,1), (2,2), (3,2) \}$		X	X		
$\{ (1,1), (1,2), (1,3), (1,4) \}$				X	X
$\{ (1,1), (2,2), (3,3) \}$		X	X		X

Definition 4.14

Es sei $R \subseteq A \times B$ eine binäre Relation.

1. R heißt (totale) Funktion, falls R linkstotal und rechtseindeutig ist.
2. R heißt partielle Funktion, falls R rechtseindeutig ist.

Beispiele: Wir diskutieren an folgenden Relationen die Funktionenbegriffe.

- Die Relation $R =_{\text{def}} \{ (1,1), (2,2), (3,2) \} \subseteq \{1,2,3\} \times \{1,2,3,4\}$ ist eine Funktion.
- Die Relation $R =_{\text{def}} \{ (1,1), (2,1) \} \subseteq \{1,2,3\} \times \{1,2,3,4\}$ ist eine partielle Funktion. Fassen wir R jedoch als Teilmenge von $\{1,2\} \times \{1,2,3,4\}$ auf, so ist R eine Funktion.
- Die Relation $R =_{\text{def}} \{ (x,y) \mid y = |x| \} \subseteq \mathbb{Z} \times \mathbb{N}$ ist eine Funktion.
- Die Relation $R =_{\text{def}} \{ (y,x) \mid y = |x| \} \subseteq \mathbb{N} \times \mathbb{Z}$ ist keine Funktion.
- Die folgende Methode einer in Java implementierten Klasse

```
int gcd(int x, int y) {
    if (y==0) return x;
    if (y>x) return gcd(y,x);
    return gcd(y,x%y);
}
```

ist eine partielle Funktion als Teilmenge von $\texttt{int}^2 \times \texttt{int}$, wobei wir `gcd` als Relation $\{ (x,y,z) \mid z = \texttt{gcd}(x,y) \}$ auffassen.

In Java gilt $\mathrm{mod}(-1,-2) = -1$, d.h. (-1) % (-2) wird zu -1 ausgewertet. Damit wird beim Methodenaufruf $\texttt{gcd}(-1,-2)$ erst rekursiv $\texttt{gcd}(-2,-1)$ und dann wieder $\texttt{gcd}(-1,-2)$ aufgerufen. Somit terminiert $\texttt{gcd}(-1,-2)$ nicht, und es gibt folglich kein $z \in \texttt{int}$ mit $(-1,-2,z) \in \texttt{gcd}$. Die Methode ist also nicht linkstotal. Die Rechtseindeutigkeit ist gegeben (wenn der verwendete Java-Compiler und die verwendete *Java Virtual Machine* korrekt sind).

Bisher haben wir Funktionen als binäre Relationen $R \subseteq A \times B$ eingeführt und damit streng genommen lediglich einstellige Funktionen definiert. Dies ist jedoch keine inhaltliche Einschränkung, da die Mengen A und B hinreichend kompliziert werden können. Dennoch vereinbaren wir Folgendes: Es sei $R \subseteq A_1 \times \cdots \times A_n$ eine n-stellige Relation. Dann heißt R eine k-stellige Funktion, falls die binäre Relation $R \subseteq B \times C$ mit $B = A_1 \times \cdots \times A_k$ und $C = A_{k+1} \times \cdots \times A_n$ eine Funktion ist. Die Begriffsbildung für partielle Funktionen überträgt sich entsprechend.

Für Funktionen werden üblicherweise eigene Schreibweisen verwendet (wie im letzten der obigen Beispiele):

- Funktionen werden häufig klein geschrieben: $f \subseteq A \times B$.
- Statt $f \subseteq A \times B$ schreiben wir auch $f : A \to B$; statt $(a,b) \in f$ schreiben wir auch $f(a) = b$.
- Kompakt notieren wir eine Funktion als $f : A \to B : a \mapsto f(a)$; für den dritten Fall in den obigen Beispielen schreiben wir also z.B. $f : \mathbb{Z} \to \mathbb{N} : x \mapsto |x|$.

Bild- und Urbildmengen

Wichtige Begriffe zur Beschreibung der Eigenschaften von Funktionen sind die Bild- und Urbildmengen.

Definition 4.15

Es seien $f : A \to B$ eine Funktion, $A_0 \subseteq A$ und $B_0 \subseteq B$.

1. Die Menge $f(A_0) \subseteq B$ ist definiert als

$$f(A_0) =_{\text{def}} \{\ b \mid (\exists a \in A_0)[f(a) = b]\ \} \qquad _{\text{def}} = \ \{\ f(a) \mid a \in A_0\ \}$$

   und heißt Bild(menge) von A_0 unter f. Die Elemente von $f(A_0)$ heißen Bilder von A_0 unter f.

2. Die Menge $f^{-1}(B_0) \subseteq A$ ist definiert als

$$f^{-1}(B_0) =_{\text{def}} \{\ a \mid (\exists b \in B_0)[f(a) = b]\ \} \quad _{\text{def}} = \ \{\ a \mid f(a) \in B_0\ \}$$

   und heißt Urbild(menge) von B_0 unter f. Die Elemente von $f^{-1}(B_0)$ heißen Urbilder von B_0 unter f.

Beispiele: Wir verdeutlichen Bilder und Urbilder exemplarisch.

- Es sei die Funktion $f =_{\text{def}} \{\ (1,1),(2,2),(3,2)\ \} \subseteq \{1,2,3\} \times \{1,2,3,4\}$ gegeben. Unter anderem können folgende Bildmengen gebildet werden:

$$\begin{aligned} f(\{1\}) &= \{1\} \\ f(\{1,2\}) &= \{1,2\} \\ f(\{1,2,3\}) &= \{1,2\} \end{aligned}$$

Beispiele für Urbildmengen sind unter anderem:

$$\begin{aligned} f^{-1}(\{1\}) &= \{1\} \\ f^{-1}(\{1,2\}) &= \{1,2,3\} \\ f^{-1}(\{3\}) &= \emptyset \end{aligned}$$

- Es sei die Funktion $f : \mathbb{Z} \to \mathbb{N} : x \mapsto |x|$ gegeben. Die Bildmenge das ganzzahligen Intervalls $[-1, 1]$ unter f ist:
$$f([-1,1]) = f(\{-1,0,1\}) = \{0,1\}$$
Die Urbildmengen zu $\{2\}$ und $[2, 4]$ unter f sind wie folgt:
$$\begin{aligned} f^{-1}(\{2\}) &= \{-2,2\} \\ f^{-1}([2,4]) &= \{-4,-,3,-2,2,3,4\} \end{aligned}$$

Proposition 4.16

Es seien A und B endliche Mengen und $f : A \to B$ eine Funktion. Dann gilt:

$$|A| = \sum_{b \in B} \left| f^{-1}(\{b\}) \right|$$

Beweis: Da f eine Funktion ist, bildet die Mengenfamilie $\{\ f^{-1}(\{b\}) \mid b \in B\ \}$ eine Partition von A. Damit folgt

$$|A| = \sum_{b \in B} |f^{-1}(\{b\})|$$

und die Proposition ist bewiesen. ■

Injektivität, Surjektivität und Bijektivität

Funktionen werden danach klassifiziert, welche Eigenschaften sie zusätzlich zur Linkstotalität und Rechtseindeutigkeit erfüllen.

Definition 4.17

Eine Funktion $f : A \to B$ heißt

1. surjektiv $\iff_{\text{def}}$ f ist rechtstotal
2. injektiv $\iff_{\text{def}}$ f ist linkseindeutig
3. bijektiv $\iff_{\text{def}}$ f ist rechtstotal und linkseindeutig

Beispiele: Folgende Funktionen verdeutlichen die Begriffsbildung.

- Die Funktion $f : \mathbb{Z} \to \mathbb{N} : x \mapsto |x|$ ist surjektiv, aber nicht injektiv.
- Die Funktion $f : \mathbb{N} \to \mathbb{Z} : x \mapsto x^3$ ist injektiv, aber nicht surjektiv.

- Die Funktion $f : \mathbb{Z} \to \mathbb{Z} : x \mapsto -x$ ist bijektiv.

Das folgende Lemma ergibt sich unmittelbar aus den Definition der Funktioneneigenschaften. Der Beweis bleibt dem Leser zur Übung überlassen.

Lemma 4.18

Es sei $f : A \to B$ eine Funktion. Dann gilt:

1. f ist surjektiv $\iff (\forall b \in B) \left[\left| f^{-1}(\{b\}) \right| \geq 1 \right]$
2. f ist injektiv $\iff (\forall b \in B) \left[\left| f^{-1}(\{b\}) \right| \leq 1 \right]$
3. f ist bijektiv $\iff (\forall b \in B) \left[\left| f^{-1}(\{b\}) \right| = 1 \right]$

Während das vorangegangene Lemma eine Charakterisierung der Eigenschaften für eine konkrete Funktion angibt, stellt Theorem 4.19 eine Beziehung zwischen Mengen mit Hilfe von Funktioneneigenschaften her. Das durch das Theorem beschriebene Abzählprinzip ist eine fundamentale Technik beim Lösen kombinatorischer Fragestellungen.

Theorem 4.19

Es seien A und B nicht-leere, endliche Mengen. Dann gilt:

1. Es gibt eine surjektive Funktion $f : A \to B \iff |A| \geq |B|$
2. Es gibt eine injektive Funktion $f : A \to B \iff |A| \leq |B|$
3. Es gibt eine bijektive Funktion $f : A \to B \iff |A| = |B|$

Beweis: Wir beweisen die Äquivalenzen im Block.

$\Leftarrow$: Es seien $A = \{a_1, \ldots, a_n\}$ und $B = \{b_1, \ldots, b_m\}$ endliche Mengen. Wir definieren eine Funktion $f : A \to B$ wie folgt für $a_i \in A$:

$$f(a_i) =_{\text{def}} \begin{cases} b_i & \text{falls } i \leq m \\ b_1 & \text{falls } i > m \end{cases}$$

Dann gelten folgende Aussage in Abhängigkeit von A und B:

1. Ist $|A| \geq |B|$, d.h. $n \geq m$, so ist f surjektiv
2. Ist $|A| \leq |B|$, d.h. $n \leq m$, so ist f injektiv
3. Ist $|A| = |B|$, d.h. $n = m$, so ist f bijektiv

$\Rightarrow$: Es sei $f : A \to B$ eine Funktion. Dann gelten folgende Aussagen:

1. Ist f surjektiv, so gilt nach Proposition 4.16 und Lemma 4.18.1:

$$|A| = \sum_{b \in B} \left| f^{-1}(\{b\}) \right| \geq \sum_{b \in B} 1 = |B|$$

2. Ist f injektiv, so gilt nach Proposition 4.16 und Lemma 4.18.2:

$$|A| = \sum_{b \in B} |f^{-1}(\{b\})| \leq \sum_{b \in B} 1 = |B|$$

3. Ist f bijektiv, so gilt nach Proposition 4.16 und Lemma 4.18.3:

$$|A| = \sum_{b \in B} |f^{-1}(\{b\})| = \sum_{b \in B} 1 = |B|$$

Damit ist das Theorem bewiesen ■

Theorem 4.20

Es seien A und B endliche Mengen mit $|A| = |B| > 0$ und $f : A \to B$ eine Funktion. Dann sind folgende Aussagen äquivalent:

1. f ist surjektiv
2. f ist injektiv
3. f ist bijektiv

Die logische Struktur des Theorems besagt, dass entweder alle Aussagen gelten oder keine.

Beweis: Wir zeigen die paarweise Äquivalenz aller Aussagen über einzelne Implikationen.

- 3. $\Rightarrow$ 1.: Ist f bijektiv, so ist f surjektiv (nach Definition).
- 3. $\Rightarrow$ 2.: Ist f bijektiv, so ist f injektiv (nach Definition).
- 1. $\Rightarrow$ 3.: Es sei f surjektiv, d.h. für alle $b \in B$ gilt $|f^{-1}(\{b\})| \geq 1$ (nach Lemma 4.18.1). Dann gilt nach Proposition 4.16 und der Voraussetzung:

  $$|A| = \sum_{b \in B} |f^{-1}(\{b\})| \geq |B| = |A|$$

  Somit gilt $|f^{-1}(\{b\})| = 1$ für alle $b \in B$. Folglich ist f bijektiv (nach Lemma 4.18.3).
- 2. $\Rightarrow$ 3.: Es sei f injektiv, d.h. für alle $b \in B$ gilt $|f^{-1}(\{b\})| \leq 1$ (nach Lemma 4.18.2). Dann gilt nach Proposition 4.16 und der Voraussetzung:

  $$|A| = \sum_{b \in B} |f^{-1}(\{b\})| \leq |B| = |A|$$

  Somit gilt $|f^{-1}(\{b\})| = 1$ für alle $b \in B$. Folglich ist f bijektiv (nach Lemma 4.18.3).

Damit ist das Theorem bewiesen. ■

Invertierbarkeit

Für eine Relation $R \subseteq A \times B$ definieren wir die Umkehrrelation $R^{-1} \subseteq B \times A$ wie folgt:

$$R^{-1} =_{\text{def}} \{ (y, x) \mid (x, y) \in R \}$$

Die folgende Proposition ist einfach an Hand der Definitionen einzusehen.

Proposition 4.21

Es sei R eine binäre Relation. Dann gelten die folgenden Aussagen:

1. R ist linkstotal $\iff$ R^{-1} ist rechtstotal
2. R ist rechtseindeutig $\iff$ R^{-1} ist linkseindeutig
3. R ist rechtstotal $\iff$ R^{-1} ist linkstotal
4. R ist linkseindeutig $\iff$ R^{-1} ist rechtseindeutig

Korollar 4.22

Ist f eine bijektive Funktion, so ist die Umkehrrelation f^{-1} eine bijektive Funktion.

Definition 4.23

Eine Funktion f heißt invertierbar (umkehrbar), falls die Umkehrrelation f^{-1} eine Funktion ist.

Korollar 4.24

Eine Funktion f ist genau dann invertierbar, wenn f bijektiv ist.

Hintereinanderausführung

Eine wichtige Operation auf Funktionen ist die Hintereinanderausführung (oder auch Verkettung, Superposition oder Komposition in anderen Zusammenhängen): Für Funktionen $f : A \to B$ und $g : B \to C$ definieren wir die Funktion $g \circ f : A \to C$ wie folgt für alle $x \in A$:

$$(g \circ f)(x) =_{\text{def}} g(f(x))$$

Beispiele: Wir beleuchten im Folgenden Aspekte der Hintereinanderausführung exemplarisch.

- Für die beiden Funktionen $f : \mathbb{N} \times \mathbb{N} : x \mapsto x^2$ und $g : \mathbb{N} \times \mathbb{N} : x \mapsto 2^x$ gilt

$$\begin{aligned}(g \circ f)(x) &= g(f(x)) = g(x^2) = 2^{(x^2)} = 2^{x^2}\\ (f \circ g)(x) &= f(g(x)) = f(2^x) = (2^x)^2 = 2^{2x}\end{aligned}$$

  Mithin gilt $g \circ f \neq f \circ g$, denn wir erhalten $(g \circ f)(3) = 2^9 = 512$ und $(f \circ g)(3) = 2^6 = 64$.

- Wodurch unterscheiden sich Klassen- und Instanzenmethoden in Java (ohne Nebeneffekte) mathematisch? Zur Veranschaulichung sei dazu eine Methode `method` einerseits als Klassenmethode

```
public static int method (int x, int y)
```

  und andererseits als Instanzenmethode

```
public int method (int x, int y)
```

  deklariert. Im ersten Fall beschreibt die Methode eine Funktion

$$\texttt{method} : \texttt{int} \times \texttt{int} \to \texttt{int}.$$

  Im zweiten Fall dagegen wird eine Funktion

$$\texttt{method} : S \times \texttt{int} \times \texttt{int} \to \texttt{int}$$

  beschrieben, wobei S für die Menge der verfügbaren Speicheradressen steht. Bei der Instanziierung eines Objektes `obj` aus der entsprechenden Klasse ordnet die *Java Virtual Machine* eine Adresse $s(\texttt{obj}) \in S$ zu, d.h. die Instanzenmethode wird dann zu einer Funktion

$$\texttt{obj.method} : \texttt{int} \times \texttt{int} \to \texttt{int} : (x, y) \mapsto \texttt{method}(s(\texttt{obj}), x, y)$$

  als Hintereinanderausführung der Funktionen s und `method`.

Proposition 4.25

Es seien $f : A \to B$ und $g : B \to C$ beliebige Funktionen.

1. Sind f und g injektiv, so ist $g \circ f$ injektiv.
2. Sind f und g surjektiv, so ist $g \circ f$ surjektiv.
3. Sind f und g bijektiv, so ist $g \circ f$ bijektiv.

Beweis: Wir zeigen die Aussagen einzeln.

1. Es seien f und g injektive Funktionen. Wir müssen zeigen, dass $g \circ f$ linkseindeutig ist. Dazu seien $x, y \in A$ beliebig mit $(g \circ f)(x) = (g \circ f)(y) \in C$. Da g injektiv ist, folgt aus $g(f(x)) = g(f(y))$ die Gleichheit $f(x) = f(y)$. Da auch f injektiv ist, folgt aus $f(x) = f(y)$ wiederum die Gleichheit $x = y$. Mithin ist $g \circ f$ linkseindeutig und also injektiv.
2. Es seien f und g surjektive Funktionen. Wir müssen zeigen, dass $g \circ f$ rechtstotal ist. Es sei $x \in C$ beliebig. Da g surjektiv ist, gibt es ein $y \in B$ mit $y \in g^{-1}(\{x\}) \subseteq B$, d.h. $g(y) = x$. Da auch f surjektiv ist, gibt es ein $z \in A$ mit $z \in f^{-1}(\{y\}) \subseteq A$, d.h. $f(z) = y$. Insgesamt erhalten wir also
$$(g \circ f)(z) = g(f(z)) = g(y) = x.$$
   Somit gilt $|(g \circ f)^{-1}(\{x\})| \geq 1$ für alle $x \in C$. Mithin ist $g \circ f$ surjektiv (nach Lemma 4.18.1).
3. Direkte Folgerung aus der ersten und der zweiten Aussage dieser Proposition.

Damit ist die Proposition bewiesen. ■

Für eine Menge A heißt die Funktion $\mathrm{id}_A : A \to A : x \mapsto x$ Identitätsfunktion von A.

Proposition 4.26

Es sei $f : A \to B$ eine bijektive Funktion. Dann gilt $f^{-1} \circ f = \mathrm{id}_A$ und $f \circ f^{-1} = \mathrm{id}_B$.

Beweis: Es genügt $f^{-1} \circ f = \mathrm{id}_A$ zu zeigen (da wir f und f^{-1} vertauschen können). Es gilt $f^{-1} \circ f : A \to A$ wegen $f : A \to B$ und $f^{-1} : B \to A$. Außerdem gilt $f^{-1}(\{f(x)\}) = \{x\}$, da f bijektiv ist. Somit gilt $f^{-1}(f(x)) = x$ für alle $x \in A$, d.h. $f^{-1} \circ f = \mathrm{id}_A$. Damit ist die Proposition bewiesen. ■

5 Kombinatorik

Der Schwerpunkt in diesem einführenden Kapitel über Kombinatorik liegt auf dem Abzählen endlicher Mengen.

Beispiel: Wie viele verschiedene logische Gatter mit 2 Eingängen (Fan-in) und 1 Ausgang (Fan-out) gibt es? Die folgende Übersicht gibt alle 16 möglichen booleschen Funktionen an, die sich durch logische Gatter berechnen lassen (siehe auch Kapitel 2):

Nr.	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$	Name(n)	Formel (mit Literalen)
f_0^2	0	0	0	0	Kontradiktion, 0	$x_1 \wedge \neg x_1$
f_1^2	0	0	0	1	Konjunktion, AND	$x_1 \wedge x_2$
f_2^2	0	0	1	0	Inhibition von x_1	$x_1 \wedge \neg x_2$
f_3^2	0	0	1	1	Identität von x_1	x_1
f_4^2	0	1	0	0	Inhibition von x_2	$\neg x_1 \wedge x_2$
f_5^2	0	1	0	1	Identität von x_2	x_2
f_6^2	0	1	1	0	Antivalenz, XOR	$(x_1 \wedge \neg x_2) \vee (\neg x_1 \wedge x_2)$
f_7^2	0	1	1	1	Disjunktion, OR	$x_1 \vee x_2$
f_8^2	1	0	0	0	Peirce-Funktion, NOR	$\neg x_1 \wedge \neg x_2$
f_9^2	1	0	0	1	Äquivalenz	$(x_1 \wedge x_2) \vee (\neg x_1 \wedge \neg x_2)$
f_{10}^2	1	0	1	0	Negation von x_2	$\neg x_2$
f_{11}^2	1	0	1	1	Replikation	$x_1 \vee \neg x_2$
f_{12}^2	1	1	0	0	Negation von x_1	$\neg x_1$
f_{13}^2	1	1	0	1	Implikation	$\neg x_1 \vee x_2$
f_{14}^2	1	1	1	0	Sheffer-Funktion, NAND	$\neg x_1 \vee \neg x_2$
f_{15}^2	1	1	1	1	Tautologie, 1	$x_1 \vee \neg x_1$

Mit Hilfe einfacher Grundregeln des Abzählens lassen sich die Anzahlen für logische Gatter mit n Eingängen bestimmen.

5.1 Grundregeln des Abzählens

Lemma 5.1 (Gleichheitsregel; Theorem 4.19.3)

Es seien A und B endliche Mengen. Es gibt genau dann eine Bijektion $f : A \to B$, wenn $|A| = |B|$ gilt.

Lemma 5.2 (Summenregel)

Es seien $A_1, \ldots, A_n$ endliche, paarweise disjunkte Mengen. Dann gilt:

$$|A_1 \cup \cdots \cup A_n| = \sum_{j=1}^{n} |A_j|$$

Beweis: Wegen der paarweisen Disjunktheit der Mengen kommt jedes Element aus $A_1 \cup \cdots \cup A_n$ in genau einer Menge A_j vor. ■

Lemma 5.3 (Produktregel)

Es seien $A_1, \ldots, A_n$ endliche Mengen. Dann gilt:

$$|A_1 \times \cdots \times A_n| = \prod_{j=1}^{n} |A_j|$$

Beweis: Wir beweisen die Aussage mittels Induktion über die Anzahl n der Mengen.

- Induktionsanfang $n = 1$: Offensichtlich.
- Induktionsschritt $n > 1$: Es sei seien $A_1, \ldots, A_n$ endliche Mengen. Wir setzen

$$\begin{aligned} A^* &=_{\text{def}} A_1 \times \cdots \times A_{n-1} \\ B_y &=_{\text{def}} \{\, (x_1, \ldots, x_{n-1}, y) \mid (x_1, \ldots, x_{n-1}) \in A^* \,\} \qquad \text{für } y \in A_n \end{aligned}$$

  Für die so definierten Mengen gelten folgende Eigenschaften:

  (i) Die Mengenfamilie $\{\, B_y \mid y \in A_n \,\}$ ist eine Partition von $A_1 \times \cdots \times A_n$.

  (ii) Für jedes $y \in A_n$ ist die Funktion

$$f_y : B_y \to A^* : (x_1, \ldots, x_{n-1}, y) \mapsto (x_1, \ldots, x_{n-1})$$

  eine Bijektion, d.h. $|B_y| = |A^*|$ für alle $y \in A_n$ (nach Lemma 5.1).

Damit erhalten wir:

$$\begin{aligned}
|A_1 \times \cdots \times A_n| &= \left| \bigcup_{y \in A_n} B_y \right| && \text{(nach Eigenschaft (i))} \\
&= \sum_{y \in A_n} |B_y| && \text{(nach Lemma 5.2 und Eigenschaft (i))} \\
&= \sum_{y \in A_n} |A^*| && \text{(nach Lemma 5.1 und Eigenschaft (ii))} \\
&= |A^*| \cdot |A_n| \\
&= \left(\prod_{j=1}^{n-1} |A_j| \right) \cdot |A_n| && \text{(nach Induktionsvoraussetzung)} \\
&= \prod_{j=1}^{n} |A_j|
\end{aligned}$$

Damit ist das Lemma bewiesen. ■

Lemma 5.4 (Potenzregel)

Es seien A und B endliche Mengen mit $|A| = m$ und $|B| = n$. Dann existieren genau n^m Funktionen $f : A \to B$.

Beweis: Nach Lemma 5.1 dürfen wir $A = \{1, \ldots, m\}$ ohne Beeinträchtigung der Allgemeinheit annehmen. Jeder Funktion $f : A \to B$ kann nun eineindeutig (injektiv) ein Tupel $(f(1), \ldots, f(m)) \in B^m$ zugeordnet werden. Außerdem entspricht jedes Tupel (die Wertetabelle) $(y_1, \ldots, y_m) \in B^m$ einer Funktion $f : A \to B : j \mapsto y_j$. Damit ist die Zuordnung sowohl injektiv als auch surjektiv, also eine Bijektion. Aus Lemma 5.1 und Produktregel (Lemma 5.3) folgt somit

$$|\{ f \mid f : A \to B \}| = |B^m| = |B|^m = n^m.$$

Damit ist das Lemma bewiesen. ■

Beispiel: Wie viele logische Gatter mit n Eingängen bzw. boolesche Funktionen mit n Variablen gibt es? Die Antwort lautet $|\{ f \mid f : \{0,1\}^n \to \{0,1\} \}| = 2^{2^n}$. (Für $n = 2$ ergeben sich gerade die am Anfang des Kapitels gelisteten 16 Funktionen.)

Korollar 5.5

Für endliche Mengen A mit $|A| = n$ gilt $|\mathcal{P}(A)| = 2^n$.

Beweis: Wir konstruieren eine Bijektion zwischen $\mathcal{P}(A)$ und der Menge der Funktionen $f : A \to \{0, 1\}$. Dazu definieren wir für eine Menge $B \in \mathcal{P}(A)$ die Funktion:

$$c_B : A \to \{0, 1\} : x \mapsto \begin{cases} 1 & \text{falls } x \in B \\ 0 & \text{falls } x \notin B \end{cases}$$

Diese Zuordnung ist offensichtlich eine Bijektion zwischen $\mathcal{P}(A)$ und der Menge der Funktionen $f : A \to \{0, 1\}$. Nach der Potenzregel (Lemma 5.4) und Lemma 5.1 gilt folglich

$$|\mathcal{P}(A)| = |\{\ f \mid f : A \to \{0, 1\}\ \}| = 2^n.$$

Damit ist das Korollar bewiesen. ■

Die im Beweis von Korollar 5.5 angegebenen Funktionen haben einen Namen: Für eine Menge $B \subseteq A$ heißt c_B die charakteristische Funktion von B.

5.2 Urnenmodelle

Urnenmodelle stellen ein exemplarisches Szenario für kombinatorische Problemstellungen dar. Die einfachste Situation ist die folgende: In *einer* Urne (daher: einfache Urnenmodelle) liegen n *unterscheidbare* Kugeln, von den k Kugel gezogen werden dürfen. Die zu beantwortende Frage ist dann: Wie viele Möglichkeiten gibt es, diese k Kugeln zu ziehen? Zur Präzisierung des Szenarios werden Unterschiede danach gemacht, ob

- die Reihenfolge, in der die Kugeln gezogen werden, eine Rolle spielt,
- gezogene Kugeln wieder zurückgelegt werden.

Damit ergeben sich vier verschiedene Szenarios.

Beispiele: Wir geben für vier Beispiele die Szenarien an:

- Die Anzahl der Ziehungen der Lotto-Zahlen „6 aus 49“ entspricht der Anzahl der Ziehungen von 6 Kugeln aus einer Urne mit 49 Kugeln ohne Zurücklegen und ohne Reihenfolge.
- Die Anzahl der vierstelligen PIN-Codes entspricht der Anzahl der Ziehungen von 4 Kugeln aus einer Urne mit 10 Kugeln (Ziffern) mit Zurücklegen und mit Reihenfolge.
- Die Anzahl der Siegerehrungen mit Gold-, Silber- und Bronzemedaillen bei einem Wettkampf mit 8 Startern entspricht dem Ziehen von 3 Kugeln aus einer Urne mit 8 Kugeln ohne Zurücklegen und mit Reihenfolge.
- Die Anzahl verschiedener Stimmenverteilungen auf 3 zur Wahl stehenden Kandidaten mit 100 Wählern entspricht dem Ziehen von 100 Kugeln aus einer Urne mit 3 Kugeln mit Zurücklegen und ohne Reihenfolge.

Theorem 5.6

Die Anzahl der Möglichkeiten, aus einer Urne mit n Kugeln k Kugeln auszuwählen, ist durch folgende Tabelle gegeben:

	mit Zurücklegen	ohne Zurücklegen
mit Reihenfolge	n^k	$(n)_k =_{\text{def}} \frac{n!}{(n-k)!}$
ohne Reihenfolge	$\binom{n+k-1}{k}$	$\binom{n}{k} =_{\text{def}} \frac{n!}{k!(n-k)!}$

Die im Theorem mitdefinierten Größen $(n)_k$ und $\binom{n}{k}$ heißen fallende Faktorielle von n der Länge k sowie Binomialkoeffizient („n über k“).

Beweis: Wir beweisen alle Fälle einzeln, aber aufeinander aufbauend:

1. Ziehen mit Zurücklegen, mit Reihenfolge: Für die erste gezogene Kugel gibt es n Möglichkeiten, für die zweite gezogene Kugel gibt es ebenfalls n Möglichkeiten unabhängig davon, welche Kugel vorher gezogen wurde. Für die k-te gezogene Kugel gibt es weiterhin n Möglichkeiten unabhängig davon, welche Kugeln vorher gezogen wurden. Insgesamt gibt es damit

$$\underbrace{n \cdot n \cdot \ \cdots \ \cdot n}_{k-\text{mal}} = n^k$$

   Möglichkeiten. (Alternativ: Eine Ziehung entspricht einer Funktion $f : \{1, \ldots, k\} \to \{1, \ldots, n\}$, wobei $f(i)$ die Nummer der im i-ten Versuch gezogenen Kugel angibt. Nach Potenzregel gibt es n^k Funktionen, nach Gleichheitsregel mithin n^k Ziehungen.)

2. Ziehen ohne Zurücklegen, mit Reihenfolge: Für die erste gezogene Kugel gibt es n Möglichkeiten, für die zweite gezogene Kugel gibt es $n-1$ Möglichkeiten. Für die k-te gezogene Kugel ($k \leq n$) gibt es mithin noch $n-k+1$ Möglichkeiten. Insgesamt gibt es damit

$$n \cdot (n-1) \cdot \ \cdots \ \cdot (n-k+1) = \frac{n!}{(n-k)!} = (n)_k$$

   Möglichkeiten.

3. Ziehen ohne Zurücklegen, ohne Reihenfolge: Mit Berücksichtigung der Reihenfolge gibt es $\frac{n!}{(n-k)!}$ Auswahlmöglichkeiten. Wenn die Reihenfolge keine Rolle mehr spielt, zählen alle Auswahlfolgen, bei denen die gleichen k Kugeln gezogen wurden, nur noch als eine Auswahlmöglichkeit. Dies sind gerade $k!$ viele. Damit gibt es insgesamt

$$\frac{n!}{(n-k)!} \cdot \frac{1}{k!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}$$

   Möglichkeiten.

4. Ziehen mit Zurücklegen, ohne Reihenfolge: Da jede Kugel mehrmals gezogen werden kann, die Reihenfolge jedoch keine Rolle spielt, ist nur wichtig, wie oft eine Kugel gezogen wird. Es sei also $(a_1, \ldots, a_n)$ ein Tupel mit den entsprechenden Anzahlen, wobei a_j gerade angibt, wie oft die Kugel j gezogen wird. Für ein Anzahltupel $(a_1, \ldots, a_n)$ muss nun gelten:

   (i) $a_j \in \{0, \ldots, k\}$ für alle $j \in \{1, \ldots, n\}$

(ii) $a_1 + \cdots + a_n = k$

Wir müssen nun zählen, wie viele derartige Tupel es geben kann. Dazu repäsentieren wir die Tupel in einer anderen Weise, die es uns ermöglicht, das Szenario zu wechseln. Wir verwenden k-mal das Symbol $*$ und $(n-1)$-mal das Symbol $|$. Ein Anzahltupel $(a_1, \ldots, a_n)$ kann nun als Symbolfolge

$$\underbrace{**\ldots*}_{a_1}|\underbrace{**\ldots*}_{a_2}|\ldots|\underbrace{**\ldots*}_{a_n}$$

aufgeschrieben werden. Umgekehrt entspricht auch jede Symbolfolge, die k-mal das Symbol $*$ und $(n-1)$-mal das Symbol $|$ enthält, einem Anzahltupel mit obigen Eigenschaften.Die Zuordnung ist also bijektiv. Statt Anzahltupel zu zählen, können wir nach der Gleichheitsregel also auch Symbolfolgen zählen. Die Anzahl möglicher Symbolfolgen zu bestimmen, entspricht aber gerade dem Ziehen von k Positionen für das Symbol $*$ aus $n+k-1$ möglichen Positionen ohne Zurücklegen und ohne Reihenfolge. Mithin gibt es insgesamt

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

Möglichkeiten.

Damit ist das Theorem bewiesen. ■

Beispiele: Wir geben für die obigen vier Beispiele die Anzahlen an:

- Die Anzahl der Ziehungen der Lotto-Zahlen „6 aus 49“ entspricht der Anzahl der Ziehungen von 6 Kugeln aus einer Urne mit 49 Kugeln ohne Zurücklegen und ohne Reihenfolge. Somit gibt es $\binom{49}{6} = 13.983.816$ verschiedene Ziehungen (bzw. Lottoscheine).
- Die Anzahl der vierstelligen PIN-Codes entspricht der Anzahl der Ziehungen von 4 Kugeln aus einer Urne mit 10 Kugeln (Ziffern) mit Zurücklegen und mit Reihenfolge. Somit gibt es $10^4 = 10.000$ verschiedene PIN-Codes.
- Die Anzahl der Siegerehrungen mit Gold-, Silber- und Bronzemedaillen bei einem Wettkampf mit 8 Startern entspricht dem Ziehen von 3 Kugeln aus einer Urne mit 8 Kugeln ohne Zurücklegen und mit Reihenfolge. Somit gibt es $(8)_3 = 336$ verschiedene Siegerehrungen.
- Die Anzahl verschiedener Stimmenverteilungen auf 3 zur Wahl stehenden Kandidaten mit 100 Wählern entspricht dem Ziehen von 100 Kugeln aus einer Urne mit 3 Kugeln mit Zurücklegen und ohne Reihenfolge. Somit gibt es $\binom{102}{100} = 5.151$ verschiedene Wahlausgänge.

Urnenmodelle treten oft gemischt auf.

Beispiele: Folgende Beispiele sollen das Zusammenspiel der kombinatorischen Szenarien verdeutlichen:

- Wir wollen Wörter der Länge n über dem Alphabet $\{a, b, c\}$ mit verschiedenen Eigenschaften zählen:
  1. Es gibt 3^n Wörter der Länge n ohne weitere Einschränkungen.
  2. Es gibt $3^n - 3$ Wörter der Länge n, die mindestens 2 verschiedene Buchstaben enthalten. (Es gibt 3 Wörter mit nur einem einzigen Buchstaben.)
  3. Es gibt $\binom{3k}{k}\binom{2k}{k}$ Wörter der Länge $n = 3k$, in denen jeder Buchstabe genau gleich oft vorkommt. (Zuerst werden unter den $3k$ verfügbaren Positionen k Positionen für den Buchstaben a gewählt, dann unter übrigen $2k$ Positionen k Positionen für b; somit müssen die restlichen k Positionen mit c besetzt werden.)
- Wir wollen die Anzahl unterschiedlicher Beflaggungen für die Siegerehrung (Gold-Silber-Bronze) für einen 100m-Lauf mit 8 Teilnehmern in einem internationalen Wettkampf bestimmen, wobei jeweils zwei Teilnehmer aus einem Land kommen sollen:

$$\underbrace{\binom{4}{3}\cdot 3!}_{\text{alle Flaggen verschieden}} + \underbrace{\binom{4}{2}\cdot\binom{3}{2}\cdot 2}_{\text{zwei Flaggen gleich}} + \underbrace{0}_{\text{alle Flaggen gleich}} = 24 + 36 + 0 = 60$$

Alternativ kann die Anzahl so bestimmt werden, dass von allen Beflaggungen mit 4 Fahnen genau 4 ausscheiden, da keine Fahne dreimal vorkommen kann. Mithin ergibt sich wiederum $4^3 - 4 = 60$.

- Die Studierenden Alice und Bob wollen versuchen, die folgende kombinatorische Aufgabe zu lösen: Über einem k-elementigen Alphabet werden Wörter der Länge n mit $n \geq k$ gebildet. Wie viele Wörter gibt es, in denen jeder Buchstaben mindestens einmal vorkommt?

  Bob argumentiert wie folgt. Da jeder Buchstabe mindestens einmal vorkommen muss, gibt es $\binom{n}{k}$ Möglichkeiten, k Buchstaben auf n Positionen zu verteilen. Die restlichen $n - k$ freien Positionen können beliebig mit Buchstaben belegt werden, was k^{n-k} Möglichkeiten sind. Damit ergeben sich insgesamt $\binom{n}{k}k^{n-k}$ Möglichkeiten. Alice erhebt Einspruch und besteht darauf, diese mit $k!$ zu multiplizieren, da jeder der $\binom{n}{k}$ Möglichkeiten von oben genau $k!$ Buchstabenkombinationen entsprechen. Alice und Bob sind froh, die Aufgabe gelöst zu haben, und bestimmen die Lösung zu $k!\binom{n}{k}k^{n-k}$.

  Haben sie recht?

5.3 Binomialkoeffizienten

Aus dem vorangegangenen Abschnitt (Theorem 5.6) wissen wir, dass die Anzahl der Kombinationen von k Elementen aus n Elementen (d.h. die Anzahl der Möglichkeiten aus n Kugeln k Kugeln ungeordnet ohne Zurücklegen zu ziehen) gerade dem Binomialkoeffizienten $\binom{n}{k}$ entspricht. Da Binomialkoeffizienten auch über die reine Kombinatorik hinaus wichtig sind, wollen in diesem Abschnitt die wichtigsten Eigenschaften von Binomialkoeffizienten festhalten. Dazu definieren wir den Binomialkoeffzienten noch einmal explizit: Für $n, k \in \mathbb{N}$ definieren wir

$$\binom{n}{k} =_{\text{def}} \frac{n!}{k!(n-k)!}, \qquad \text{mit } \binom{n}{k} = 0 \qquad \text{für } k > n.$$

Eine einfache, sofort einsichtige Beobachtung ist:

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

Damit lässt sich der Binomialkoeffizient konsistent auch für negative Werte für k definieren:

$$\binom{n}{k} =_{\text{def}} 0 \qquad \text{für } k \in \mathbb{Z} \setminus \mathbb{N}$$

Theorem 5.7 (Pascalsches Dreieck)

Für $n \in \mathbb{N}_+$ und $k \in \mathbb{N}$ gilt

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

Wir geben zwei Beweise für das Theorem an.

Beweis: (rechnerisch) Wir führen eine Fallunterscheidung bezüglich der Werte von k durch:

- Für $k = 0$ und $n > 1$ gilt $\binom{n}{0} = 1 = \binom{n-1}{-1} + \binom{n-1}{0}$.

- Für $0 < k < n$ rechnen wir aus:

$$\begin{aligned}
\binom{n-1}{k-1} + \binom{n-1}{k} &= \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-1-k)!} \\
&= \frac{(n-1)!}{(k-1)!(n-k)!} \cdot \frac{k}{k} + \frac{(n-1)!}{k!(n-1-k)!} \cdot \frac{n-k}{n-k} \\
&= \frac{(n-1)! \cdot k}{k!(n-k)!} + \frac{(n-1)!(n-k)}{k!(n-k)!} \\
&= \frac{(n-1)!(k+n-k)}{k!(n-k)!} \\
&= \frac{(n-1)! \cdot n}{k!(n-k)!} \\
&= \binom{n}{k}
\end{aligned}$$

- Für $k = n$ und $n > 1$ gilt $\binom{n}{n} = 1 = \binom{n-1}{n-1} + \binom{n-1}{n}$.
- Für $k > n > 1$ gilt $\binom{n}{k} = 0 = \binom{n-1}{k-1} + \binom{n-1}{k}$.

Damit ist das Theorem durch Nachrechnen bewiesen. ■

Beweis: (kombinatorisch) Wir interpretieren die Gleichung als Bestimmung der Kardinalität von Mengen auf zwei verschiedene Weisen. Es seien $n \in \mathbb{N}_+$ und $k \in \mathbb{N}$. Wir definieren folgende Mengenfamilien:

$$\begin{aligned}
\mathcal{F} &=_{\text{def}} \{ \{a_1, \ldots, a_k\} \mid a_i \in \{1, \ldots, n\} \text{ und } a_i \neq a_j \text{ für } i \neq j\} \\
\mathcal{F}_+ &=_{\text{def}} \{ A \mid A \in \mathcal{F} \text{ und } 1 \in A\} \\
\mathcal{F}_- &=_{\text{def}} \{ A \mid A \in \mathcal{F} \text{ und } 1 \notin A\}
\end{aligned}$$

Die einzelnen Mengenfamilien stehen für folgende Urnenmodelle:

- $\mathcal{F}$ entspricht dem ungeordneten Ziehen von k Kugeln aus n Kugeln ohne Zurücklegen.
- $\mathcal{F}_+$ entspricht dem ungeordneten Ziehen von k Kugeln aus n Kugeln ohne Zurücklegen, wobei Kugel 1 *immer* gezogen wird.
- $\mathcal{F}_-$ entspricht dem ungeordneten Ziehen von k Kugeln aus n Kugeln ohne Zurücklegen, wobei Kugel 1 *nie* gezogen wird.

Nun gilt offensichtlich $\mathcal{F} = \mathcal{F}_+ \cup \mathcal{F}_-$ sowie $\mathcal{F}_+ \cap \mathcal{F}_- = \emptyset$, also $|\mathcal{F}| = |\mathcal{F}_+| + |\mathcal{F}_-|$ nach der Summenregel (Lemma 5.2). Nach Theorem 5.6 gilt:

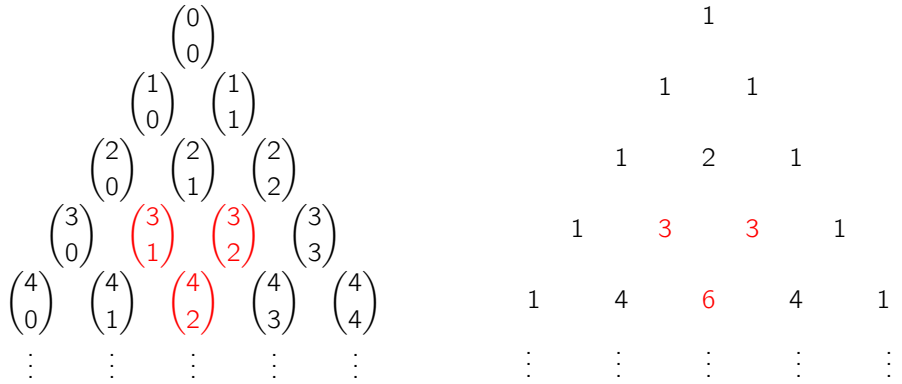
$$|\mathcal{F}| = \binom{n}{k}, \qquad |\mathcal{F}_+| = \binom{n-1}{k-1}, \qquad |\mathcal{F}_-| = \binom{n-1}{k}$$

Mithin erhalten wir:

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

Damit ist das Theorem kombinatorisch bewiesen. ■

Beispiel: Der Dreiecksaufbau des rekursiven Zusammenhangs in Theorem 5.7 lässt sich leicht veranschaulichen und ist schon aus der Schule bekannt:



Ein weiteres Beispiel für die Anwendung von Theorem 5.6 ist das Binomialtheorem. Das Binomialtheorem kann durch vollständige Induktion über n bewiesen werden. Dies ist eine gute Übung zu Anwendung des Pascalschen Dreiecks. Wir geben einen kombinatorischen Beweis.

Theorem 5.8 (Binomialtheorem)

Für alle $a, b \in \mathbb{R}$ und $n \in \mathbb{N}$ gilt

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

Beweis: Es seien $a, b \in \mathbb{R}$ und $n \in \mathbb{N}$ beliebig. Ausmultiplizieren von $(a+b)^n$ ergibt:

$$\begin{aligned}(a+b)^n \quad = \quad & \overbrace{a \cdot \cdots \cdot a \cdot a}^{n \text{ Faktoren}} + \\ & + a \cdot \cdots \cdot a \cdot b + \\ & + a \cdot \cdots \cdot b \cdot a + \\ & + a \cdot \cdots \cdot b \cdot b + \\ & \vdots \\ & + \underbrace{b \cdot \cdots \cdot b \cdot b}_{n \text{ Faktoren}}\end{aligned}$$

Die Summanden können zusammengefasst werden zu Produkten von jeweils n Faktoren, von denen k Faktoren gerade b und $n-k$ Faktoren gerade a sind. Die Summanden sind also von der Form $a^{n-k}b^k$, da die Reihenfolge bei der Multiplikation keine Rolle spielt. Die Anzahl der Produkte $a^{n-k}b^k$ entspricht somit gerade dem Ziehen von k Kugeln (die Positionen für b im Produkt) aus n Kugeln (die Gesamtheit aller Positionen für Faktoren), d.h. $\binom{n}{k}$. Folglich gilt insgesamt:

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

Damit ist das Theorem bewiesen. ■

Korollar 5.9

Für alle $n \in \mathbb{N}_+$ gilt

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0.$$

Beweis: Nach dem Binomialtheorem gilt

$$0 = (1-1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} (-1)^k = \sum_{k=0}^{n} (-1)^k \binom{n}{k}.$$

Damit ist das Korollar bewiesen. ■

Korollar 5.10

Für alle $n \in \mathbb{N}$ gilt

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

Beweis: Nach dem Binomialtheorem gilt

$$2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} 1^k = \sum_{k=0}^{n} \binom{n}{k}.$$

Damit ist das Korollar bewiesen. ■

Theorem 5.11 (Vandermondesche Identität)

Für $k, m, n \in \mathbb{N}$ gilt

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

Beweis: Es seien A und B disjunkte Mengen mit $|A| = n$ und $|B| = m$. Für jedes $j \in \{0, \ldots, k\}$ definieren wir die Mengenfamilie

$$\mathcal{X}_j =_{\text{def}} \{\ X \mid X \subseteq A \cup B, |X \cap A| = j \text{ und } |X \cap B| = k - j\ \}$$

Es gibt $\binom{n}{j}$ viele j-elementige Teilmengen von A und $\binom{m}{k-j}$ viele $(k-j)$-elementige Teilmengen von B. Damit gilt

$$|\mathcal{X}_j| = \binom{n}{j} \binom{m}{k-j}.$$

Wegen $\mathcal{X}_i \cap \mathcal{X}_j = \emptyset$ für $i \neq j$ folgt nun

$$\binom{n+m}{k} = \sum_{j=0}^{k} |\mathcal{X}_j| = \sum_{j=0}^{k} \binom{n}{j}\binom{m}{k-j}.$$

Damit ist das Theorem bewiesen. ■

Beispiel: Wenn zum Beispiel in einer Vorlesung $n+m$ Studenten sitzen, n weibliche und m männliche, wie viele verschiedene Gruppen mit genau k Studenten gibt es dann? Dies lässt sich auf zwei Arten bestimmen:

- Ohne Berücksichtigung des Geschlechts erhalten wir $\binom{n+m}{k}$ Gruppen.
- Mit Berücksichtigung des Geschlechts zählen wir für jedes $j \in \{0, 1, \ldots, k\}$ alle Gruppen mit jeweils genau j weiblichen und genau $k-j$ männlichen Studenten, damit also insgesamt $\sum_{j=0}^{k} \binom{n}{j}\binom{m}{k-j}$ Gruppen.

Da wir über dieselbe Menge von Studenten argumentieren, sind beide Anzahlen gleich.

5.4 Stirling-Zahlen

Stirling-Zahlen erster Art und Permutationen

Es sei A eine endliche Menge mit $|A| = n$. Eine Permutation von A ist eine bijektive Funktion $\pi : A \to A$. Ohne Beeinträchtigung der Allgemeinheit setzen wir stets $A = \{1, \ldots, n\}$ voraus. Die Menge $\{1, \ldots, n\}$ notieren wir auch als $[n]$. Weiterhin definieren wir die Menge

$$\mathcal{S}_n =_{\text{def}} \{\ \pi \mid \pi : [n] \to [n] \ \text{ ist eine Permutation }\},$$

die sogenannte symmetrische Gruppe von n Elementen zur Namensgebung siehe das Kapitel über Algebraische Strukturen).

Theorem 5.12

Für alle $n \in \mathbb{N}_+$ gilt $|\mathcal{S}_n| = n!$.

Beweis: $|\mathcal{S}_n|$ entspricht dem Ziehen von n Kugeln aus einer Urne mit n Kugeln ohne Zurücklegen mit Berücksichtigung der Reihenfolge. Nach Theorem 5.6 gilt

$$|\mathcal{S}_n| = \frac{n!}{(n-n)!} = n!.$$

Damit ist das Theorem bewiesen. ■

Ohne Beweis geben wir folgendes Resultat über das Verhalten der Fakultätsfunktion an:

Theorem 5.13 (Stirlingsche Formel)

Für alle $n \in \mathbb{N}_+$ gilt

$$\sqrt{2\pi n}\left(\frac{n}{e}\right)^n < n! < \sqrt{2\pi n}\left(\frac{n}{e}\right)^n e^{\frac{1}{12n}},$$

wobei $e = e^1 = 2,718281828459\ldots$ die Eulersche Zahl ist.

Permutationen können auf verschiedene Arten geschrieben werden. Im Folgenden behandeln wir drei Schreibweisen:

Matrixschreibweise: Dazu schreiben wir die Permutation $\pi : [n] \to [n]$ als $2 \times n$-Matrix der Form

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \pi(1) & \pi(2) & \pi(3) & \dots & \pi(n) \end{pmatrix}$$

Da π bijektiv ist, kommen alle Werte $1, \dots, n$ in der zweiten Zeile vor.

Beispiel: Folgende Permutation ist in Matrixschreibweise gegeben:

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

Tupelschreibweise: Im Prinzip genügt es, von der Matrixschreibweise lediglich die zweite Zeile zu übernehmen, d.h. Permutationen können angegeben werden in der Form

$$\pi = (\pi(1), \pi(2), \pi(3), \dots, \pi(n)).$$

Beispiel: $\pi = (4, 1, 6, 2, 5, 3)$ ist obige Permutation in Tupelschreibweise.

Zyklenschreibweise: Die Zyklenschreibweise entsteht, wenn wir für $x \in [n]$ die iterierte Hintereinanderausführung von π auf x betrachten. Dadurch entsteht eine Folge:

$$\begin{aligned} \pi^0(x) &=_{\text{def}} x, \\ \pi^1(x) &=_{\text{def}} \pi(x), \\ \pi^2(x) &=_{\text{def}} \pi(\pi(x)), \\ &\vdots \\ \pi^k(x) &=_{\text{def}} \pi(\pi^{k-1}(x)), \\ &\vdots \end{aligned}$$

Für jedes $x \in [n]$ gibt es dann ein minimales $0 < k \leq n$ mit $\pi^k(x) = x$.

Beispiel: Für die Permutation $\pi = (4, 1, 6, 2, 5, 3)$ gilt

$$\begin{array}{llll} \pi^0(1) = 1, & \pi^1(1) = 4, & \pi^2(1) = 2, & \pi^3(1) = 1; \\ \pi^0(2) = 2, & \pi^1(2) = 1, & \pi^2(2) = 4, & \pi^3(2) = 2; \\ \pi^0(3) = 3, & \pi^1(3) = 6, & \pi^2(3) = 3; & \\ \pi^0(4) = 4, & \pi^1(4) = 2, & \pi^2(4) = 1, & \pi^3(4) = 4; \\ \pi^0(5) = 5, & \pi^1(5) = 5; & & \\ \pi^0(6) = 6, & \pi^1(6) = 3, & \pi^2(6) = 6. & \end{array}$$

Eine Folge $x, \pi(x), \pi^2(x), \dots, \pi^{k-1}(x)$ mit minimalem $k > 0$, so dass $\pi^k(x) = x$, heißt *Zyklus* der Länge k und wird als $(x\ \pi(x)\ \pi^2(x)\ \dots\ \pi^{k-1}(x))$ geschrieben.

Beispiel: $\pi = (4, 1, 6, 2, 5, 3)$ enthält die Zyklen (1 4 2), (3 6) und (5).

Jede Permutation kann als Produkt von Zyklen geschrieben werden, indem die Zyklen einfach hintereinander gesetzt werden. Die Schreibweise ist jedoch nicht eindeutig. Insbesondere kann jeder Zyklus der Länge k auf genau k Arten geschrieben werden.

Beispiel: Die Permutation $\pi = (4, 1, 6, 2, 5, 3)$ können wir als Produkt von Zyklen wie folgt schreiben:

$$\begin{aligned}(4, 1, 6, 2, 5, 3) &= (1\ 4\ 2)(3\ 6)(5)\\ &= (4\ 2\ 1)(6\ 3)(5)\\ &= (5)(2\ 1\ 4)(6\ 3)\end{aligned}$$

Insbesondere gilt $(1\ 4\ 2) = (4\ 2\ 1) = (2\ 1\ 4)$.
Die Anzahl der Zyklen, aus der eine Permutation bestehen kann, liegt zwischen 1, wie in $(1\,2\,3\ \ldots\ n)$, und n, wie in $(1)(2)(3)\ldots(n)$. Im Folgende wollen wir die Anzahl der Permutationen mit genau k Zyklen genauer bestimmen.

Für $n, k \in \mathbb{N}$ sei $\left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right]$ (manchmal auch $s_{n,k}$) geschrieben) die Anzahl der Permutationen von n Elementen mit genau k Zyklen. Dann gilt also

$$\sum_{k=1}^{n} \left[\begin{matrix} n \\ k \end{matrix}\right] = n!.$$

Die Zahlen $\left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right]$ heißen Stirling-Zahlen erster Art. Folgende Sonderfälle sind zu beachten:

- Für $k > n$ gilt $\left[\begin{matrix} n \\ k \end{matrix}\right] = 0$, da eine Permutation von n Elementen höchstens n Zyklen enthalten kann.
- Für $n > 0$ gilt $\left[\begin{matrix} n \\ 0 \end{matrix}\right] = 0$, da jede Permutation mindestens einen Zyklus enthält.
- Wir definieren $\left[\begin{matrix} 0 \\ 0 \end{matrix}\right] =_{\text{def}} 1$.

Mit diesen Sonderfällen können wir wiederum eine Rekursionsvorschrift für die Berechnung der Stirling-Zahlen erster Art angeben.

Theorem 5.14 (Stirling-Dreieck erster Art)

Für alle $k, n \in \mathbb{N}$ mit $n \geq k$ gilt

$$\left[\begin{matrix} n \\ k \end{matrix}\right] = \left[\begin{matrix} n-1 \\ k-1 \end{matrix}\right] + (n-1) \cdot \left[\begin{matrix} n-1 \\ k \end{matrix}\right].$$

Beweis: (kombinatorisch) Es sei $\pi \in \mathcal{S}_n$ eine Permutation mit k Zyklen. Dann kann π auf zwei Arten aus einer Permutation aus $\mathcal{S}_{n-1}$ entstanden sein:

(i) Einfügen eines Zyklus (n) in Permutationen aus $\mathcal{S}_{n-1}$ mit $k-1$ Zyklen
(ii) Einfügen des Elementes n in einen der Zyklen einer Permutation aus $\mathcal{S}_{n-1}$ mit k Zyklen

Beide Fälle sind disjunkt. Für die Anzahl der Möglichkeiten, Permutationen mit k Zyklen auf diese zwei Arten zu erzeugen, ergibt sich jeweils:

(i) $\left[\begin{matrix} n-1 \\ k-1 \end{matrix}\right]$

(ii) $(n-1) \cdot \left[\begin{matrix} n-1 \\ k \end{matrix}\right]$ (denn für das Einfügen eines Elementes in einen Zyklus der Länge t gibt es t Möglichkeiten; Einfügen als erstes und Einfügen als letztes Element erzeugen den gleichen Zyklus)

Insgesamt erhalten wir also:

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

Damit ist das Theorem bewiesen. ■

Beispiel: Um die Konstruktion aus dem Beweis von Theorem 5.14 zu verdeutlichen, betrachten wir die 6 Permutationen von 4 Elementen mit 3 Zyklen:

(1)(2 3)(**4**)	(1 **4**)(2)(3)
(1 2)(3)(**4**)	(1)(2 **4**)(3)
(1 3)(2)(**4**)	(1)(2)(3 **4**)

Die linken Permutationen entstehen aus den Permutationen (1)(2 3), (1 2)(3) und (1 3)(2) durch Einfügen des Einerzyklus (4). Die rechten Permutationen entstehen aus der Permutation (1)(2)(3) durch Einfügen von 4 in jeden Einerzyklus.

Um einen Eindruck von Wachstum der Stirling-Zahlen erster Art zu erhalten, können die Werte analog dem Pascalschen Dreieck angeordnet werden.

Beispiel: Der Dreiecksaufbau des rekursiven Zusammenhangs in Theorem 5.14 lässt sich wie folgt veranschaulichen:

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 0 & & 1 & & & & \\
 & & & 0 & & 1 & & 1 & & & \\
 & & 0 & & 2 & & 3 & & 1 & & \\
 & 0 & & 6 & & 11 & & 6 & & 1 & \\
0 & & 24 & & 50 & & 35 & & 10 & & 1 \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots
\end{array}$$

Mit Permutationen, insbesondere mit der symmetrischen Gruppe, werden wir uns im Kapitel über algebraische Strukturen noch einmal ausführlich beschäftigen.

Stirling-Zahlen zweiter Art und Mengenpartitionen

In diesem Abschnitt wollen wir bestimmen, wie viele Möglichkeiten es gibt n-elementige Grundmengen in k nichtleere, disjunkte Komponenten zu zerlegen.

Es sei A eine endliche Menge mit $|A| = n$. Eine k-Partition $\mathcal{F} = \{A_1, A_2, \ldots, A_k\}$ ist eine k-elementige Familie von nichtleeren Teilmengen von A mit $A_1 \cup A_2 \cdots \cup A_k = A$ und $A_i \cap A_j = \emptyset$, falls $i \neq j$.

Es sei $\left\{ {n \atop k} \right\}$ (manchmal auch: $S_{n,k}$) die Anzahl der k-Partitionen einer n-elementigen Grundmenge. Die Zahlen $\left\{ {n \atop k} \right\}$ heißen Stirling-Zahlen zweiter Art.

Beispiel: Die Studierenden Alice und Bob liegen falsch, wenn sie die Anzahl der Wörter der Länge n über einem k-elementigen Alphabet, in denen jeder Buchstabe mindestens einmal vorkommt, mit $k!\binom{n}{k}k^{n-k}$ angeben. Dabei werden diejenigen Wörter, in denen Buchstaben mehr als einmal vorkommen, mehrfach gezählt. Die korrekte Anzahl ist:

$$\left\{ {n \atop k} \right\} \cdot k!$$

Folgende Spezialfälle sind für die Stirling-Zahlen zweiter Art zu beachten:

- Für $k > n$ gilt $\left\{ {n \atop k} \right\} = 0$, da die n Elemente höchstens in n Komponenten liegen können.
- Für $k = 0$ gilt $\left\{ {n \atop 0} \right\} = 0$, da die n Elemente in wenigstens einer Komponenten liegen müssen.
- Wir definieren $\left\{ {0 \atop 0} \right\} =_{\text{def}} 1$.

Wir können nun eine ähnliche rekursive Darstellung wie in Theorem 5.14 für die Stirling-Zahlen erster Art auch für die Stirling-Zahlen zweiter Art beweisen.

Theorem 5.15 (Stirling-Dreieck zweiter Art)

Für alle $k, n \in \mathbb{N}$ mit $n \geq k$ gilt

$$\left\{ {n \atop k} \right\} = \left\{ {n-1 \atop k-1} \right\} + k \cdot \left\{ {n-1 \atop k} \right\}.$$

Beweis: (kombinatorisch) Es sei $\mathcal{F}$ eine k-Partition einer n-elementigen Menge. Dann kann $\mathcal{F}$ auf zwei Arten aus einer Partition einer $(n-1)$-elementigen Menge entstehen:

(i) Hinzufügen der Menge $\{n\}$ zu einer $(k-1)$-Partition von $n-1$ Elementen
(ii) Einfügen von n in einer der Mengen einer k-Partition von $n-1$ Elementen

Die Anzahl der Möglichkeiten k-Partitionen von n Elementen zu bilden, ist wie folgt:

(i) $\left\{ {n-1 \atop k-1} \right\}$

(ii) $k \cdot \left\{ {n-1 \atop k} \right\}$

Mithin gilt also:

$$\left\{ {n \atop k} \right\} = \left\{ {n-1 \atop k-1} \right\} + k \cdot \left\{ {n-1 \atop k} \right\}$$

Damit ist das Theorem bewiesen. ■

Wir geben wieder einen Eindruck für das Wachstum der Zahlen $\left\{ {n \atop k} \right\}$ gemäß Theorem 5.15.

Beispiel: Der Dreiecksaufbau des rekursiven Zusammenhangs in Theorem 5.15 lässt sich wie folgt veranschaulichen:

$$\begin{array}{ccccccc} & & & 1 & & & \\ & & 0 & & 1 & & \\ & 0 & & 1 & & 1 & \\ 0 & & 1 & & 3 & & 1 \end{array}$$

$$\begin{array}{ccccccccccccc}
 & & & 0 & & 1 & & 7 & & 6 & & 1 & \\
 & & 0 & & 1 & & 15 & & 25 & & 10 & & 1 \\
 & 0 & & 1 & & 31 & & 90 & & 65 & & 15 & & 1 \\
 \vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots
\end{array}$$

Interessieren wir uns nur für die Anzahl aller möglichen Partitionen einer Grundmenge A mit $|A| = n$, so kann man die Bell-Zahlen bestimmen:

$$B_n =_{\text{def}} \sum_{k=0}^{n} \left\{ {n \atop k} \right\}$$

Insbesondere gibt B_n also die Anzahl aller Äquivalenzrelationen auf n Elementen an.

5.5 Weitere Abzählprinzipien

In diesem Abschnitt fassen wir drei weitere kombinatorische Prinzipien zusammen.

Doppeltes Abzählen

Wir haben bereits mehrfach kombinatorische Indentitäten durch Abzählen einer Menge auf unterschiedliche Weise gewonnen. Insbesondere wurden so das Pascalsche Dreieck und die Stirlingschen Dreiecke hergeleitet. Im Folgenden wollen wir dieses Beweisprinzip beim Bestimmen der Kardinalität von binären Relationen anwenden.

Lemma 5.16 (Doppeltes Abzählen)

Es sei $R \subseteq A \times B$ eine endliche Relation. Dann gilt

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

Beweis: Jedes Paar $(a,b) \in R$ wird in beiden Summen genau einmal gezählt. ■

Beispiel: Wir wollen die Anzahl der Einsen in einer Matrix $A \in \{0,1\}^{n \times m}$ zählen. Man beachte, dass jede binäre Relation $R \subseteq \{1,\ldots,n\} \times \{1,\ldots,m\}$ durch eine Matrix A beschrieben werden kann mittels $(i,j) \in R \iff a_{i,j} = 1$. Konkret sei die folgende Matrix gegeben:

$$A = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix} \begin{array}{l} \to 8 \\ \to 4 \\ \to 2 \\ \to 2 \\ \to 1 \\ \to 1 \\ \to 1 \\ \to 1 \end{array}$$

$$\begin{array}{cccccccccc} \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & & \downarrow \\ 1 & 2 & 2 & 3 & 2 & 4 & 2 & 4 & \rightarrow & 20 \end{array}$$

Im allgemeinen Fall einer Matrix $A \in \{0,1\}^{n \times m}$ mit den Einträgen $a_{i,j}$ stehen in der letzten Spalte in der i-ten Zeile die Zeilensumme $\sum_{j=1}^{m} a_{i,j}$ und in der letzten Zeile in der j-ten Spalte die Spaltensumme $\sum_{i=1}^{n} a_{i,j}$. Klarerweise muss die Summe über alle Zeilensummen stets gleich der Summe über alle Spaltensummen sein:

$$\sum_{j=1}^{m} \sum_{i=1}^{n} a_{i,j} = \sum_{i=1}^{n} \sum_{j=1}^{m} a_{i,j}$$

Das Inklusion-Exklusions-Prinzip

Das Inklusion-Exklusions-Prinzip ist eine Verallgemeinerung der Summenregel (Lemma 5.2) auf beliebige, nicht notwendig paarweise disjunkte Mengen.

Theorem 5.17 (Inklusions-Exkusions-Prinzip)

Es seien $A_1, \ldots, A_n$ endliche Mengen. Dann gilt:

$$\left| \bigcup_{j=1}^{n} A_j \right| = \sum_{\emptyset \neq K \subseteq \{1,\ldots,n\}} (-1)^{1+|K|} \left| \bigcap_{k \in K} A_k \right|$$

Beispiel: Wir wollen die Formel für kleine Anzahlen n entwickeln. Für $n = 2$ reduzieren sich die Ausdrücke in Theorem 5.17 zu folgender Identität:

$$|A_1 \cup A_2| \;=\; |A_1| + |A_2| - |A_1 \cap A_2|$$

Für $n = 3$ reduzieren sich die Ausdrücke in Theorem 5.17 zu folgender Identität:

$$|A_1 \cup A_2 \cup A_3| \;=\; |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$$

Beweis: Wir bestimmen, wie oft jedes Element auf beiden Seiten der Gleichung gezählt wird. Es sei $x \in \bigcup_{j=1}^{n} A_j$.

- Linke Seite: Das Element x wird genau einmal gezählt.
- Rechte Seite: Wir müssen zeigen, dass x auch hier genau einmal gezählt wird. Dazu sei $\ell =_{\text{def}} |\{\, j \mid x \in A_j \,\}|$ die Anzahl der Mengen, in denen x vorkommt. Ohne Beeinträchtigung der Allgemeinheit komme x genau in den Mengen $A_1, \ldots, A_\ell$ vor. Dann gilt:
  - Für $\emptyset \neq K \subseteq \{1, \ldots, \ell\}$ wird x genau $(-1)^{1+|K|}$-mal gezählt.
  - Für alle anderen Menge K wird x gar nicht gezählt.

  Somit folgt für den Beitrag von x zur rechten Seite der Gleichung insgesamt:

$$\begin{aligned} \sum_{\emptyset \neq K \subseteq \{1,\ldots,\ell\}} (-1)^{1+|K|} &= \sum_{k=1}^{\ell} \binom{\ell}{k} (-1)^{1+k} = -\sum_{k=1}^{\ell} \binom{\ell}{k} (-1)^{k} \\ &= 1 - \sum_{k=0}^{\ell} \binom{\ell}{k} (-1)^{k} \\ &= 1 \qquad \text{(nach Korollar 5.10)} \end{aligned}$$

Damit ist das Theorem bewiesen. ■

Wir wollen an einem Beispiel verdeutlichen, wie der doch recht kompliziert wirkende Ausdruck auf der rechten Seite gewinnbringend angewendet werden kann.

Beispiel: Wie viele Primzahlen gibt es zwischen 2 und 100? Um diese Frage zu beantworten, bestimmen wir die zusammengesetzten Zahlen zwischen 2 und 100 mit Hilfe des Inklusions-Exklusions-Prinzip. Es sei $A =_{\text{def}} \{2, \ldots, 100\}$. Eine Zahl $x \in A$ ist zusammengesetzt, falls $x = p \cdot n$ für geeignete Zahlen $p, n \in A$ gilt, wobei p eine Primzahl mit $p \leq \sqrt{100} = 10$ ist. Damit kommen als Primzahlen nur $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ und $p_4 = 7$ in Frage. Für $i \in \{1, 2, 3, 4\}$ betrachten wir die Menge der Vielfachen von p_i, d.h. die Menge

$$A_i =_{\text{def}} \{\ x \in A \mid (\exists n \in A)[x = p_i \cdot n]\ \}.$$

Damit gilt:

- $A_1 \cup A_2 \cup A_3 \cup A_4$ ist die Menge der zusammengesetzten Zahlen aus A
- Die Kardinalitäten der möglichen Schnittmengen sind

$$\begin{aligned} |A_i| &= \left\lfloor \frac{100}{p_i} \right\rfloor - 1 \quad (\text{da } p_i \notin A_i) \\ \left| \bigcap_{j=1}^{k} A_{i_j} \right| &= \left\lfloor \frac{100}{\prod_{j=1}^{k} p_{i_j}} \right\rfloor \quad \text{für } k \in \{2, 3, 4\} \text{ und } 1 \leq i_1 < \ldots < i_k \leq 4 \end{aligned}$$

Nach Theorem 5.17 erhalten wir:

$$\begin{aligned} |A_1 \cup A_2 \cup A_3 \cup A_4| &= \left(\left\lfloor \frac{100}{2} \right\rfloor - 1 + \left\lfloor \frac{100}{3} \right\rfloor - 1 + \left\lfloor \frac{100}{5} \right\rfloor - 1 + \left\lfloor \frac{100}{7} \right\rfloor - 1 \right) \\ &\quad - \left(\left\lfloor \frac{100}{6} \right\rfloor + \left\lfloor \frac{100}{10} \right\rfloor + \left\lfloor \frac{100}{14} \right\rfloor + \left\lfloor \frac{100}{15} \right\rfloor + \left\lfloor \frac{100}{21} \right\rfloor + \left\lfloor \frac{100}{35} \right\rfloor \right) \\ &\quad + \left(\left\lfloor \frac{100}{30} \right\rfloor + \left\lfloor \frac{100}{42} \right\rfloor + \left\lfloor \frac{100}{70} \right\rfloor + \left\lfloor \frac{100}{105} \right\rfloor \right) \\ &\quad - \left\lfloor \frac{100}{210} \right\rfloor \\ &= 49 + 32 + 19 + 13 - 16 - 10 - 7 - 6 - 4 - 2 + 3 + 2 + 1 + 0 - 0 \\ &= 74 \end{aligned}$$

Damit gibt es $99 - 74 = 25$ Primzahlen zwischen 2 und 100.

Der Schubfachschluss

Ein weiteres wichtiges Abzählprinzip, um die Existenz von Objekten zu beweisen, ist der Schubfachschluss (engl. *pigeonhole principle*).

Theorem 5.18 (Schubfachschluss)

Es seien A und B endliche Mengen mit $|A| > |B| > 0$ und $f : A \to B$ eine Funktion. Dann gibt es ein $y \in B$ mit $|f^{-1}(y)| > 1$.

Beweis: (Widerspruch) Angenommen es gilt $|f^{-1}(y)| \leq 1$ für alle $y \in B$. Dann wissen wir aus dem letzten Semester, dass f eine injektive Funktion ist. Daraus folgt $|A| \leq |B|$. Dies ist ein Widerspruch zu $|A| > |B|$. Mithin war die Annahme falsch, und das Theorem ist beweisen. ■

Mit anderen Worten: Um $|A|$ Objekte in $|B|$ Schubfächer zu stecken, müssen sich in mindestens einem Schubfach 2 Objekte befinden (falls $|A| > |B|$ ist).

Beispiele: An folgenden Fällen wollen wir die Anwendung des Schubfachschlusses demonstrieren:

- Von 13 Personen feiern mindestens zwei Personen im gleichen Monat ihren Geburtstag.
- In jeder Menge P von mindestens zwei Personen gibt es immer mindestens zwei Personen, die die gleiche Anzahl von Personen in P kennen. (Hierbei sei angenommen, dass „kennen“ eine symmetrische Relation ist.)

  Zur Begründung: Es seien $P = \{p_1, \ldots, p_n\}$ die Personenmenge mit $n \geq 2$ Personen sowie $f : P \to \{0, \ldots, n-1\}$ eine Funktion, die der Person p_i die Anzahl ihrer Bekannten in P zuordnet. Wegen $|P| = |\{0, \ldots, n-1\}| = n$ kann Theorem 5.18 nicht direkt angewendet werden. Eine genauere Analyse ermöglicht jedoch die folgende Fallunterscheidung:

  (i) Es gibt ein $p \in P$ mit $f(p) = 0$. Wegen der Symmetrie der Bekanntschaftsrelation gibt es auch keine Person, die alle Personen in P kennt. Also gilt $f(q) \neq n-1$ für alle $q \in P$ und folglich $f(P) \subseteq \{0, \ldots, n-2\}$.

  (ii) Für alle $p \in P$ gilt $f(p) \neq 0$. Damit gilt $f(P) \subseteq \{1, \ldots, n-1\}$.

  In beiden Fällen gilt also $|f(P)| < |P|$. Nach Theorem 5.18 folgt die Aussage.

Theorem 5.19 (Verallgemeinerter Schubfachschluss)

Es seien A und B endliche, nichtleere Mengen und $f : A \to B$ eine Funktion. Dann existiert ein $y \in B$ mit $|f^{-1}(y)| \geq \left\lceil \frac{|A|}{|B|} \right\rceil$.

Beweis: (Widerspruch) Wir nehmen wiederum an, dass $|f^{-1}(y)| \leq \left\lceil \frac{|A|}{|B|} \right\rceil - 1$ für alle $y \in B$ gilt. Dann folgt:

$$\begin{aligned}
|A| &= \sum_{y \in B} |f^{-1}(y)| \\
&\leq |B| \cdot \left(\left\lceil \frac{|A|}{|B|} \right\rceil - 1 \right) \\
&\leq |B| \cdot \left(\frac{|A| + |B| - 1}{|B|} - 1 \right) \\
&= |B| \cdot \frac{|A| - 1}{|B|} \\
&= |A| - 1
\end{aligned}$$

Dies ist jedoch ein Widerspruch. Mithin war die Annahme falsch, und das Theorem ist bewiesen. ■

Beispiel: Wir wollen wieder an zwei Beispielen den verallgemeinerten Schubfachschluss verdeutlichen.

- Von 100 Personen feiern mindestens 9 Personen im gleichen Monat ihren Geburtstag.

- In jeder Menge von 6 Personen gibt es 3 Personen, die sich alle untereinander kennen, oder 3, die sich alle nicht kennen. (Hierbei nehmen wir wiederum an, dass „kennen“ eine symmetrische Relation ist.)

  Zur Begründung: Es sei $P = \{p_1, \ldots, p_6\}$ eine beliebige Personenmenge. Wir betrachten für die Person p_1 die Funktion

  $$f : \{p_2, \ldots, p_5\} \to \{\text{„bekannt“}, \text{„nicht bekannt“}\},$$

  die jeder Person $p_2, \ldots, p_5$ zuordnet, ob p_1 diese Person kennt. Nach Theorem 5.19 sind $\lceil \frac{5}{2} \rceil = 3$ Personen mit p_1 „bekannt“ oder 3 Personen mit p_1 „nicht bekannt“. Ohne Beeinträchtigung der Allgemeinheit seien 3 Personen mit p_1 bekannt (sonst vertauschen wir in nachfolgender Argumentation einfach „kennen“ und „nicht kennen“) und zwar p_2, p_3 und p_4. Nun gibt es zwei Möglichkeiten für die Personen p_2, p_3 und p_4:

  (i) Es gibt zwei Personen in $\{p_2, p_3, p_4\}$, die sich kennen. Diese beiden Personen kennen aber auch p_1. Somit gibt es also 3 Personen, die sich alle untereinander kennen.

  (ii) Die Personen p_2, p_3 und p_4 kennen sich nicht. Also gibt es 3 Personen, die sich untereinander nicht kennen.

6 Graphentheorie

Graphen sind kombinatorische Strukturen zur Beschreibung binärer Relationen. Binäre Relationen sind entweder symmetrisch oder nicht symmetrisch. Entsprechend gibt es unterschiedliche Typen von Graphen.

6.1 Gerichtete und ungerichtete Graphen

Wir beginnen zunächst mit dem Studium ungerichteter Graphen, da sich viele Sachverhalte für diese einfacher beschreiben lassen. Eine Erweiterung auf den Fall gerichteter Graphen ist meist leicht möglich und nur fallweise erklärungsbedürftig.

Definition 6.1

Ein (ungerichteter) Graph G ist ein Paar (V, E), wobei V eine endliche, nichtleere Mengen von Knoten (oder Ecken) ist und E eine Teilmenge aller zweielementigen Teilmengen von V ist:

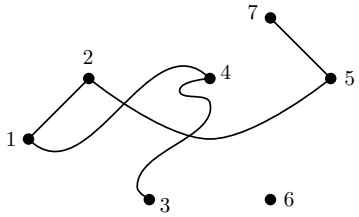
$$E \subseteq \mathcal{P}_2(V) =_{\text{def}} \{\ \{x, y\} \mid x, y \in V \wedge x \neq y\ \}$$

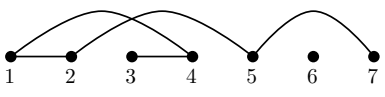
Die Elemente von E heißen Kanten.

Ein Graph $G = (V, E)$ kann wie folgt visualisiert werden:

- Die Knotenmenge $V = \{v_1, \ldots, v_n\}$ wird durch eine Menge von Punkten in der Ebene dargestellt.
- Für eine Kante $e = \{v_i, v_k\} \in E$ verbinden wir v_i und v_k mit einer Linie.

Beispiel: Der Graph $G = (V, E)$ mit der Knotenmenge $V = \{1, 2, 3, 4, 5, 6, 7\}$ und der Kantemenge $E = \{\ \{1, 2\}, \{1, 4\}, \{2, 5\}, \{3, 4\}, \{5, 7\}\ \}$ kann auf die beiden folgenden Arten dargestellt werden:





Wir unterscheiden zwischen markierten und unmarkierten Graphen. Bei einem markierten Graphen spielen die Namen der Knoten eine Rolle, wobei wir in Darstellungen den jeweiligen Namen direkt

neben den Knoten schreiben. Bei unmarkierten Graphen lassen wir die Knotennamen weg.

Definition 6.2

Es seien $G = (V, E)$ und $G' = (V', E')$ Graphen. G heißt isomorph zu G', symbolisch: $G \simeq G'$, wenn es eine bijektive Funktion $\varphi : V \to V'$ gibt mit

$$\{u, v\} \in E \iff \{\varphi(u), \varphi(v)\} \in E'$$

für alle $u, v \in V$. Die Funktion φ heißt (Graph-)Isomorphismus.

Anschaulich sind zwei Graphen genau dann isomorph sind, wenn sie mit dem gleichen Bild (ohne Knotennamen) gezeichnet werden können. Mit unmarkierten Graphen sind also gleichzeitig alle isomorphen Graphen mitgemeint.

Beispiel: Wir betrachten die beiden Graphen $G = ([4], E)$ und $G' = ([4], E')$ mit derselben Knotenmenge $[4] = \{1, 2, 3, 4\}$ und den Kantenmengen

$$E =_{\text{def}} \{\ \{1,2\}, \{1,3\}, \{2,3\}, \{2,4\}\ \}, \quad E' =_{\text{def}} \{\ \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}\ \}.$$

Bei gleicher Positionierung der Knoten ergeben sich die folgenden Abbildungen:

Wie nun leicht einzusehen ist, definiert die bijektive Funktion $\varphi : [4] \to [4]$ mit

$$\varphi :\ 1 \mapsto 2,\ 2 \mapsto 4,\ 3 \mapsto 3,\ 4 \mapsto 1$$

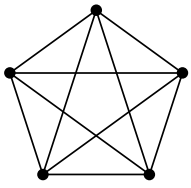
einen Isomorphismus von G nach G'. Für die 6 möglichen Kanten von G gilt:

$$\begin{array}{ll}
\{1,2\} \in E & \{\varphi(1), \varphi(2)\} = \{2,4\} \in E' \\
\{1,3\} \in E & \{\varphi(1), \varphi(3)\} = \{2,3\} \in E' \\
\{1,4\} \notin E & \{\varphi(1), \varphi(4)\} = \{1,2\} \notin E' \\
\{2,3\} \in E & \{\varphi(2), \varphi(3)\} = \{3,4\} \in E' \\
\{2,4\} \in E & \{\varphi(2), \varphi(4)\} = \{1,4\} \in E' \\
\{3,4\} \notin E & \{\varphi(3), \varphi(4)\} = \{1,3\} \notin E'
\end{array}$$

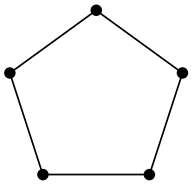
Mithin gilt $\{u, v\} \in E \Leftrightarrow \{\varphi(u), \varphi(v)\} \in E'$, also $G \simeq G'$ (via φ). Wenn in G' jedoch eine Kante entfernt wird, dann sind die beiden Graphen klarerweise nicht mehr isomorph.

Wir erwähnen einige wichtige Typen unmarkierter Graphen.

1. K^n bezeichnet einen vollständigen Graphen mit n Knoten, d.h., alle Knoten sind miteinander verbunden. Der K^5 kann beispielsweise wie folgt dargestellt werden:



2. C_n bezeichnet einen Kreis mit n Knoten, die jeweils zyklisch verbunden sind. Der C_5 kann beispielsweise wie folgt dargestellt werden:



Knoten- und die Kantenmenge des C_n können wie folgt definiert werden:

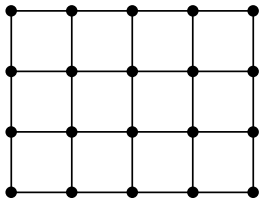
$$V =_{\text{def}} \{0, 1, \ldots, n-1\}, \quad E =_{\text{def}} \{\, \{i, j\} \mid \text{mod}(i+1, n) = j \,\}$$

3. P_n bezeichnet einen Pfad mit $n+1$ Knoten und n Kanten, die aufeinander folgende Knoten verbinden. Der P_4 kann beispielsweise wie folgt dargestellt werden:

Knoten- und die Kantenmenge des P_n können wie folgt definiert werden:

$$V =_{\text{def}} \{0, 1, \ldots, n\}, \quad E =_{\text{def}} \{\, \{i, j\} \mid |i - j| = 1 \,\}$$

4. $M_{n,m}$ bezeichnet einen Gittergraph mit n Zeilen und m Spalten, bei dem die Knoten jeweils zeilen- und spaltenweise verbunden sind. Der $M_{4,5}$ kann beispielsweise wie folgt dargestellt werden:



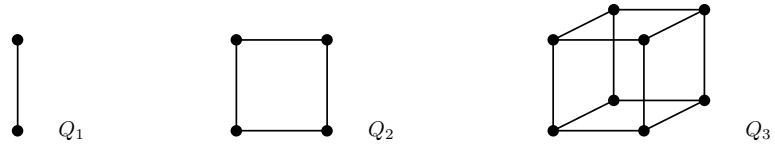
Knoten- und die Kantenmenge des $M_{n,m}$ können wie folgt definiert werden:

$$V =_{\text{def}} \{1, \ldots, n\} \times \{1, \ldots, m\}, \quad E =_{\text{def}} \{\, \{(i, j), (i', j')\} \mid |i - i'| + |j - j'| = 1 \,\}$$

5. Q_d bezeichnet den d-dimensionalen Hyperwürfel mit der Knotenmenge $\{0, 1\}^d$ und Kanten zwischen Knoten, die sich in genau einer Komponente unterscheiden, d.h.,

$$V =_{\text{def}} \{0, 1\}^d, \quad E =_{\text{def}} \{\, \{(i_1, \ldots, i_d), (j_1, \ldots, j_d)\} \mid \textstyle\sum_{r=1}^{d} |i_r - j_r| = 1 \,\}$$

Q_1, Q_2 und Q_3 können beispielsweise wie folgt dargestellt werden:



Bemerkung: In verschiedenen Anwendungen werden manchmal noch zuätzliche Kanten betrachtet:

- Schleifen: Kanten, die Knoten v mit sich selbst verbinden.
- Mehrfachkanten: Knoten u und v können durch mehr als eine Kante verbunden sein.

Wir betrachten ausschließlich schlichte, einfache Graphen, d.h. Graphen ohne Schleifen und Mehrfachkanten.

Ein wichtiges Unterscheidungskriterium für Knoten in einem Graphen ist ihre Nachbarschaft. Es seien $G = (V, E)$ ein Graph, $u, v \in V$ Knoten und $e, f \in E$ Kanten.

- Die Knoten u und v heißen adjazent (oder benachbart), falls $\{u, v\} \in E$ gilt.
- Der Knoten u und die Kante e heißen inzident, falls $u \in e$ gilt.
- Die Kanten e und f heißen inzident, falls $e \cap f \neq \emptyset$ gilt.

Definition 6.3

Es seien $G = (V, E)$ ein Graph und $v \in V$ ein Knoten.

1. Die Nachbarschaft $N_G(v)$ von v in G ist definiert als
$$N_G(v) =_{\text{def}} \{\ u \in V \mid \{v, u\} \in E\ \}.$$
2. Der Grad $\deg_G(v)$ von v in G ist definiert als
$$\deg_G(v) =_{\text{def}} |N_G(v)|.$$

Der Grad eines Knoten v entspricht ebenso der Anzahl der mit v inzidenten Kanten. Wenn der Graph G im Kontext klar ist, so lassen wir den Index G sowohl bei der Nachbarschaft als auch beim Grad weg.

Beispiele:

1. Für alle Knoten v im K^n gilt $\deg(v) = n - 1$.
2. Für alle Knoten v im C_n gilt $\deg(v) = 2$.
3. Für alle Knoten v im Q_d gilt $\deg(v) = d$.

Ein Graph $G = (V, E)$ heißt k-regulär, falls $\deg(v) = k$ für alle $v \in V$ gilt; G heißt regulär, falls G k-regulär für irgendein $k \in \mathbb{N}$ ist. K^n, C_n und Q_d sind jeweils reguläre Graphen.

Proposition 6.4

Für jeden Graphen $G = (V, E)$ gilt
$$\sum_{v \in V} \deg_G(v) = 2 \cdot |E|.$$

Beweis: (Doppeltes Abzählen) Es sei $e = \{u, v\} \in E$ eine Kante. Wie oft trägt e zu beiden Seiten der Gleichung bei?

- Linke Seite: Für beide Knoten u und v trägt e jeweils 1 zum Grad bei, d.h., e wird zweimal gezählt.

- Rechte Seite: e wird zweimal gezählt.

Somit wird e auf beiden Seite gleich oft gezählt und die Proposition ist bewiesen. ■

Korollar 6.5

Für jeden Graphen $G = (V, E)$ ist die Anzahl der Knoten mit ungeradem Grad gerade.

Beweis: Es sei $V_i =_{\text{def}} \{ v \in V \mid \text{mod}(\deg(v), 2) = i \}$, d.h., V_0 enthält die Knoten mit geradem Grad, V_1 die mit ungeradem Grad. Es gilt $V = V_0 \cup V_1$ und $V_0 \cap V_1 = \emptyset$. Somit gilt mit Proposition 6.4:

$$2 \cdot |E| = \sum_{v \in V} \deg(v) = \sum_{v \in V_0} \deg(v) \quad + \sum_{v \in V_1} \deg(v)$$

Damit die rechte Summe gerade wird, muss also $|V_1|$ gerade sein und das Korollar ist bewiesen. ■

Der Knotengrad ist eine lokale Eigenschaft für einen Knoten. Die zugehörigen globalen Graphenparameter sind in folgender Definition zusammengefasst.

Definition 6.6

Es sei $G = (V, E)$ ein ungerichteter Graph, $|V| = n$.

1. $\Delta(G) =_{\text{def}} \max \{ \deg_G(v) \mid v \in V \}$ heißt Maximalgrad von G.
2. $\delta(G) =_{\text{def}} \min \{ \deg_G(v) \mid v \in V \}$ heißt Minimalgrad von G.
3. $\bar{d}(G) =_{\text{def}} \frac{1}{n} \cdot \sum_{v \in V} \deg_G(v)$ heißt Durchschnittgrad von G.

Nach Proposition 6.4 gilt $\bar{d}(G) = 2|E|/|V|$. Außerdem ist offensichtlich:

$$0 \leq \delta(G) \leq \bar{d}(G) \leq \Delta(G) \leq n - 1.$$

Häufig werden Eigenschaften von Graphen über Teilstrukturen ausgedrückt.

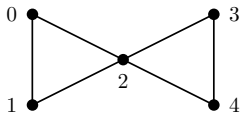
Definition 6.7

Es sei $G = (V_G, E_G)$ ein Graph.

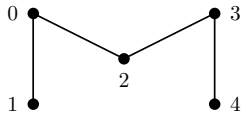
1. Ein Graph $H = (V_H, E_H)$ heißt Teilgraph von G, symbolisch: $H \subseteq G$, falls $V_H \subseteq V_G$ und $E_H \subseteq E_G$ gilt.
2. Ein Graph $H = (V_H, E_H)$ heißt induzierter Teilgraph von G, symbolisch: $H = G[V_H]$, falls $V_H \subseteq V_G$ und $E_H = E_G \cap \mathcal{P}_2(V_H)$.

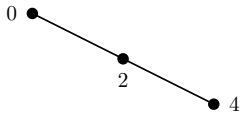
Ein induzierter Teilgraph $G[V_H]$ von G ist ein kantenmaximaler Teilgraph von G mit dieser Knotenmenge, d.h., alle Kanten aus G, für die beide Endknoten in V_H liegen, gehören zu $G[V_H]$.

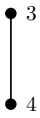
Beispiel: Für den Graphen $G = (V, E)$ mit Knotenmenge $V = \{0, 1, 2, 3, 4\}$



zeigt (a) einen Teilgraphen von G, (b) einen induzierten Teilgraphen von G und (c) den durch die Knotenmenge $\{0, 1, 3, 4\}$ induzierten Teilgraph $G[\{0, 1, 3, 4\}]$:







Abschließend für diesen Abschnitt nehmen wir noch einige begriffliche Anpassungen für gerichtete Graphen vor.

Definition 6.8

Ein gerichteter Graph G ist ein Paar $G = (V, E)$ mit endlicher, nichtleerer Knotenmenge V und Kantenmenge

$$E \subseteq V \times V = \{ (u, v) \mid u, v \in V \}.$$

Für eine Kante $e = (u, v) \in E$ heißt u der Startknoten und v der Endknoten.

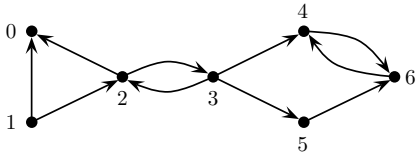
In der graphischen Repräsentierung einer gerichteten Kante (u, v) wird die Orientierung von u nach v durch $u \to v$ wiedergegeben.

Knotengrade fallen in einem gerichteten Graph $G = (V, E)$ auseinander nach eingehenden oder ausgehenden Kanten:

- $\deg^+_G(v) =_{\text{def}} |\{ u \in V \mid (v, u) \in E \}|$ ist der Ausgangsgrad von v in G
- $\deg^-_G(v) =_{\text{def}} |\{ u \in V \mid (u, v) \in E \}|$ ist der Eingangsgrad von v in G
- $\deg_G(v) =_{\text{def}} \deg^+_G(v) + \deg^-_G(v)$ ist der Grad von v in G

Ein Knoten v mit $\deg^+_G(v) = 0$ heißt Senke. Ein Knoten v mit $\deg^-_G(v) = 0$ heißt Quelle.

Beispiel: In folgendem gerichteten Graphen



sind der Knoten 0 eine Senke und der Knoten 1 eine Quelle. Somit sind der minimale Ausgangsgrad $\delta^+(G) = 0$ und der minimale Eingangsgrad $\delta^-(G) = 0$. Der maximale Ausgangsgrad $\Delta^+(G)$ beträgt 3. Ebenso gilt für den maximalen Eingangsgrad $\Delta^-(G) = 2$. Der maximale Grad $\Delta(G)$ ist 4 und der minimale Grad $\delta(G) = 2$.

6.2 Wege in Graphen

Definition 6.9

Es sei $G = (V, E)$ ein Graph.

1. Ein Weg (oder Kantenzug) der Länge k in G ist eine Folge

$$W =_{\text{def}} (v_0, e_1, v_1, e_2, v_2, \ldots, v_{k-1}, e_k, v_k)$$

   mit $v_0, \ldots, v_k \in V$, $e_1, \ldots, e_k \in E$ sowie $e_i = \{v_{i-1}, v_i\}$ für alle $i \in \{1, \ldots, k\}$. Der Knoten v_0 heißt Anfangsknoten von W; der Knoten v_k heißt Endknoten von W; die anderen Knoten heißen innere Knoten. Ein Weg mit u als Anfangsknoten und v als Endknoten heißt (u, v)-Weg.

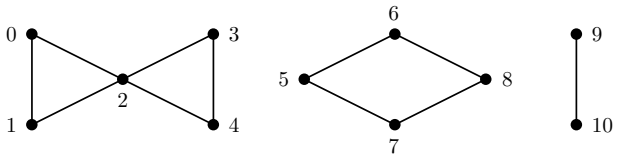
2. Ein Pfad in G ist ein knotendisjunkter Weg in G, d.h., alle Knoten auf dem Weg sind paarweise verschieden.

3. Ein Kreis in G ist ein Weg mit gleichem Anfangs- und Endknoten.

4. Ein einfacher Kreis in G ist ein Kreis der Länge $k \geq 3$, bei dem alle inneren Knoten paarweise verschieden und verschieden zum Anfangs- und Endknoten sind.

Wenn uns die Kanten nicht interessieren, dann können wir in der Beschreibung eines Weges $(v_0, e_1, v_1, e_2, v_2, \ldots, v_{k-1}, e_k, v_k)$ die Kanten $e_1, \ldots, e_k$ auch weglassen und sprechen stattdessen vom Weg $(v_0, v_1, \ldots, v_k)$. Dabei gilt jedoch nach wie vor $\{v_{i-1}, v_i\} \in E$ für alle $i \in \{1, \ldots, k\}$.

Beispiel: In folgendem Graphen $G = (V, E)$ mit $V = \{0, 1, \ldots, 10\}$



sind $(0, 1, 2)$, $(0, 2, 3, 4, 2, 1)$, $(5, 6, 5, 7)$ Wege der Längen 2, 5 und 3; nur $(0, 1, 2)$ ist ein Pfad. Die Folge $(2, 3, 4, 5, 6)$ ist kein Weg. Die Folge (0) ist ein Weg der Länge 0. Weiterhin sind $(0, 1, 2, 0)$ und $(6, 8, 7, 5, 6)$ einfache Kreise der Längen 3 und 4; der $(0, 0)$-Weg $(0, 2, 3, 4, 2, 1, 0)$ ist ein Kreis, aber kein einfacher Kreis.

Proposition 6.10

Es seien $G = (V, E)$ ein Graph und $u, v \in V$ Knoten.

1. Gibt es einen (u, v)-Weg in G, so gibt es einen (u, v)-Pfad in G.

2. Liegt die Kante $\{u, v\}$ auf einem kantendisjunkten Kreis in G, so liegt $\{u, v\}$ auf einem einfachen Kreis in G.

Beweis: Übungsaufgabe. ■

Anzahl der Wege in Graphen*

Es sei $G = (V, E)$ ein ungerichteter Graph, $u, v \in V$ seien Knoten.

- $W_k(G)_{u,v}$ bezeichne die Anzahl der (u, v)-Wege der Länge k in G,
- $W_k(G)_u$ bezeichne die Anzahl der Wege der Länge k in G, mit u als Anfangsknoten,
- $W_k(G)$ bezeichne die Anzahl der Wege der Länge k in G.

Es gelten folgende Zusammenhänge:

$$W_k(G)_u = \sum_{v \in V} W_k(G)_{u,v}, \qquad W_k(G) = \sum_{u \in V} W_k(G)_u = \sum_{u \in V} \sum_{v \in V} W_k(G)_{u,v}$$

Beispiele: Folgende Beispiele verdeutlichen die Definitionen:

1. Für einen beliebigen ungerichteten Graph $G = (V, E =$ gilt:

$$\begin{aligned} W_0(G) &= |V| = \sum_{v \in V} \deg_G(v)^0 \\ W_1(G) &= 2|E| = \sum_{v \in V} \deg_G(v)^1 \\ W_2(G) &= \sum_{v \in V} W_1(G)_v \cdot W_1(G)_v = \sum_{v \in V} \deg_G(v)^2 \end{aligned}$$

   Für $k = 3$ gilt die entsprechende Formel $W_3(G) = \sum_{v \in V} \deg_G(v)^3$ im Allgemeinen nicht mehr.

2. In einem r-regulären Graphen $G = (V, E)$ mit $|V| = n$ gilt

$$W_k(G)_u = r^k, \qquad W_k(G) = n \cdot r^k.$$

   Eine einfache Formel für $W_k(G)_{u,v}$ ist hingegen nicht immer möglich.

Proposition 6.11

Für jeden Graphen $G = (V, E)$ mit $|V| = n$ gilt

$$\delta(G)^k \leq W_k(G)_u \leq \Delta(G)^k, \qquad n \cdot \delta(G)^k \leq W_k(G) \leq n \cdot \Delta(G)^k$$

für $u \in V$, $k \in \mathbb{N}$. Für reguläre Graphen gilt Gleichheit.

Es sei $G = (V, E)$ ein Graph mit $V = [n]$ (ohne Beeinträchtigung der Allgemeinheit). Wir definieren die Adjazenzmatrix $A(G) \in \{0, 1\}^{n \times n}$ mit den Einträgen $a_{ij} = (A(G))_{ij}$ für $i, j \in \{1, \ldots, n\}$ wie folgt:

$$a_{ij} =_{\text{def}} \begin{cases} 1 & \text{falls } \{i, j\} \in E \\ 0 & \text{sonst} \end{cases}$$

Für ungerichtete Graphen G ist die Adjazenzmatrix symmetrisch, d.h. $a_{ij} = a_{ji}$, und auf der Diagonale stehen nur Nullen, d.h. $a_{ii} = 0$.

Wir verwenden Matrizenmultiplikation: Für Matrizen $A, B \in \mathbb{R}^{n \times n}$ definieren wir wie üblich

$$(A \cdot B)_{ij} =_{\text{def}} \sum_{k=1}^{n} a_{ik} b_{kj}$$

für $i, j \in \{1, \ldots, n\}$. Für Matrizen $A, B, C \in \mathbb{R}^{n \times n}$ gilt:

- $(A \cdot B) \cdot C = A \cdot (B \cdot C)$ (d.h., Matrizenmultiplikation ist assoziativ)
- $A \cdot I = I \cdot A = A$ für die Einheitsmatrix I (d.h., $I_{ii} =_{\text{def}} 1$ und $I_{ij} =_{\text{def}} 0$ für $i \neq j$)
- $A \cdot B \neq B \cdot A$ (im Allgemeinen)

Für $k \in \mathbb{N}$ definieren wir die k-te Potenz von A induktiv wie folgt:

$$A^0 =_{\text{def}} I, \qquad A^k =_{\text{def}} A \cdot A^{k-1} \text{ für } k > 0$$

Lemma 6.12

Es sei $G = (V, E)$ ein Graph, $V = [n]$. Es sei $A = A(G) \in \{0,1\}^{n \times n}$ die Adjazenzmatrix von G. Für alle $k \in \mathbb{N}$ und für alle $i, j \in V$ gilt

$$W_k(G)_{ij} = (A^k)_{ij}.$$

Beweis: (Induktion) Wir führen den Beweis mittels vollständiger Induktion über k:

- Induktionsanfang $k = 0$: Für $i \neq j$ gilt $W_0(G)_{ij} = 0 = I_{ij} = (A^0)_{ij}$. Weiterhin gilt $W_0(G)_{ii} = 1 = I_{ii} = (A^0)_{ii}$.
- Induktionsschritt $k > 0$: Es sei $B =_{\text{def}} A^{k-1}$. Dann gilt $A^k = A \cdot B$. Außerdem gilt nach Induktionsvoraussetzung $b_{ij} = W_{k-1}(G)_{ij}$ für alle $i, j \in \{1, \ldots, n\}$. Somit erhalten wir:

$$W_k(G)_{ij} = \sum_{\ell \in N_G(i)} W_{k-1}(G)_{\ell j} = \sum_{\ell \in N_G(i)} b_{\ell j} = \sum_{\ell=1}^{n} a_{i\ell} b_{\ell j} = (A \cdot B)_{ij} = (A^k)_{ij}$$

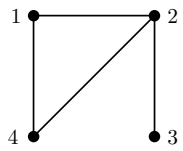
Damit ist das Lemma bewiesen. ■

Korollar 6.13

Es sei $A = A(G)$ die Adjzenzmatrix von $G = (V, E)$, $V = [n]$. Dann gilt:

1. $(A^2)_{ii} = \deg_G(i)$ für alle $i \in \{1, \ldots, n\}$
2. $(A^3)_{ii} = 2 \cdot \text{triad}_G(i)$ für alle $i \in \{1, \ldots, n\}$, wobei $\text{triad}_G(i)$ die Anzahl der Dreiecke K^3 ist, die i enthalten.

Beispiel: Für den Graphen $G = ([4], E)$ und die Adjazenmatrix $A(G)$



erhalten wir als Adjazenzmatrix

$$A(G) = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

Für $k = 2$ ergibt sich:

$$A^2 = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 1 & 1 \\ 1 & 3 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 2 \end{pmatrix}$$

Damit erhalten wir die Knotengrade $2, 3, 1, 2$ für die Knoten $1, 2, 3, 4$. Für $k = 3$ ergibt sich nun:

$$A^3 = \begin{pmatrix} 2 & 1 & 1 & 1 \\ 1 & 3 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 4 & 1 & 3 \\ 4 & 2 & 3 & 4 \\ 1 & 3 & 0 & 1 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

Das einzige Dreieck im Graphen bilden die Knoten $1, 2, 4$. Dies entspricht gemäß obiger Formel genau den Einträgen $2, 2, 0, 2$ auf der Diagonale.

Distanzen in Graphen

Definition 6.14

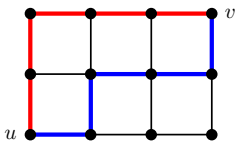
Es sei $G = (V, E)$ ein Graph. Für Knoten $u, v \in V$ ist der Abstand (oder die Distanz) $\text{dist}_G(u, v)$ definiert als die kürzeste Länge eines (u, v)-Weges, d.h.

$$\text{dist}_G(u, v) =_{\text{def}} \min \{ k \in \mathbb{N} \mid \text{es gibt einen } (u, v)\text{-Weg der Länge } k \},$$

wobei $\text{dist}_G(u, v) =_{\text{def}} \infty$, falls kein (u, v)-Weg in G existiert.

Klarerweise ist ein kürzester (u, v)-Weg stets ein Pfad. Im Allgemeinen muss ein kürzester (u, v)-Weg nicht eindeutig sein.

Beispiel: Für die Knoten u und v im $M_{3,4}$ gilt $\text{dist}_G(u, v) = 5$.



Angegeben sind mindestens zwei der kürzesten Wege.

Proposition 6.15

Es sei $G = (V, E)$ ein ungerichteter Graph. Für die $u, v, w \in V$ gilt:

1. $\text{dist}_G(v, v) \geq 0$ und $\text{dist}_G(u, v) = 0 \Leftrightarrow u = v$ — positive Definitheit
2. $\text{dist}_G(u, v) = \text{dist}_G(v, u)$ — Symmetrie
3. $\text{dist}_G(u, v) \leq \text{dist}_G(u, w) + \text{dist}_G(w, v)$ — Dreiecksungleichung
4. $\text{dist}_G(u, v) = \text{dist}_G(u, w) + \text{dist}_G(w, v)$, falls w auf einem kürzesten (u, v)-Weg liegt

Mit anderen Worten: dist_G ist eine Metrik auf der Knotenmenge V von $G = (V, E)$.

Beweis: Wir bewiesen die Aussagen einzeln für beliebige Knoten $u, v, w \in V$ eines ungerichteten Graphen $G = (V, E)$:

1. Klar.
2. Klar (G ist ungerichtet).
3. Es seien $W_u = (u, \ldots, w)$ und $W_v = (w, \ldots, v)$ kürzeste (u, w)- bzw. (w, v)-Wege. Dann gibt es auch den (u, v)-Weg $W = (u, \ldots, w, \ldots, v)$ in G. Die Länge von W ist gerade $\text{dist}_G(u, w) + \text{dist}_G(w, v)$. Folglich gilt
$$\text{dist}_G(u, w) + \text{dist}_G(w, v) \geq \text{dist}_G(u, v).$$
4. Der Knoten w liege auf einem kürzesten (u, v)-Weg W der Länge $k = \text{dist}_G(u, v)$ in G, $W = (v_0, \ldots, v_\ell, \ldots, v_k)$ mit $v_0 = u$, $v_\ell = w$ und $v_k = v$. Dann gilt sowohl $\text{dist}_G(u, w) \leq \ell$ als auch $\text{dist}_G(w, v) \leq k - \ell$. Mithin erhalten wir
$$\text{dist}_G(u, w) + \text{dist}_G(w, v) \leq \ell + k - \ell = k = \text{dist}_G(u, v) \leq \text{dist}_G(u, w) + \text{dist}_G(w, v);$$
letzteres mit der Dreiecksungleichung. Somit gilt
$$\text{dist}_G(u, w) + \text{dist}_G(w, v) = \text{dist}_G(u, v).$$

Damit ist die Proposition bewiesen. ■

Definition 6.16

Es sei $G = (V, E)$ ein Graph.

1. Der Durchmesser $\operatorname{diam}(G)$ von G ist der längste kürzeste Weg zwischen zwei Knoten $u, v \in V$, d.h.

$$\operatorname{diam}(G) =_{\text{def}} \max \{ \operatorname{dist}_G(u, v) \mid u, v \in V \}$$

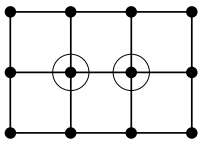
2. Ein Knoten $u \in V$ heißt Mittelpunkt in G, falls für alle Knoten $v \in V$ gilt:

$$\max \{ \operatorname{dist}_G(u, w) \mid w \in V \} \leq \max \{ \operatorname{dist}_G(v, w) \mid w \in V \}$$

   Der Radius $\operatorname{rad}(G)$ ist der maximale Abstand eines Mittelpunktes zu einem anderen Knoten, also gerade die linke Seite der Ungleichung.

Wie zu erwarten, gilt stets $\operatorname{rad}(G) \leq \operatorname{diam}(G) \leq 2 \cdot \operatorname{rad}(G)$.

Beispiel: Es gilt $\operatorname{diam}(C_{2n}) = n$ und $\operatorname{diam}(C_{2n+1}) = n$ sowie $\operatorname{rad}(M_{3,4}) = 3$ mit den Mittelpunkten:



Proposition 6.17

Enthält $G = (V, E)$ einen einfachen Kreis, so gilt

$$g(G) \leq 2 \cdot \operatorname{diam}(G) + 1,$$

wobei $g(G)$ die Taillenweite von G ist, d.h., $g(G)$ ist die minimale Länge eines einfachen Kreises in G.

Beweis: Übungsaufgabe. ■

Zusammenhang in Graphen

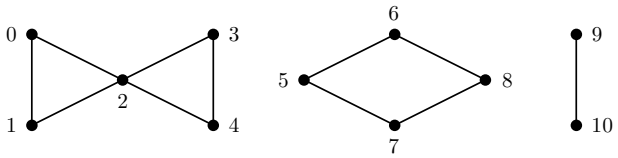
Definition 6.18

Es seien $G = (V, E)$ ein Graph und $C \subseteq G$ ein induzierter Teilgraph.

1. G heißt zusammenhängend, falls für jedes Paar von Knoten $u, v \in V$ ein (u, v)-Pfad in G existiert.
2. C heißt Zusammenhangskomponente von G, falls C zusammenhängend und ein knotenmaximaler induzierter Teilgraph mit dieser Eigenschaft ist.

Jeder Knoten v eines Graphen $G = (V, E)$ liegt in einer Zusammenhangskomponente, denn der induzierte Teilgraph $G[\{v\}]$ ist zusammenhängend (wenn auch nicht unbedingt knotenmaximal). Außerdem sind zwei Zusammenhangskomponenten entweder identisch oder knotendisjunkt. Somit lässt sich die Knotenmenge als disjunkte Vereinigung von Komponenten $V_1, \ldots, V_\ell$ schreiben. Es ist üblich, sowohl V_j als auch den induzierten Teilgraph $G[V_j]$ als Zusammenhangskomponente zu bezeichnen.

Beispiel: Der schon bekannte Graph $G = (V, E)$



besteht aus den Zusammenhangskomponenten $G[\{0, 1, 2, 3, 4\}]$, $G[\{5, 6, 7, 8\}]$ und $G[\{9, A\}]$.

Theorem 6.19

Jeder Graph $G = (V, E)$ enthält mindestens $|V| - |E|$ Zusammenhangskomponenten.

Beweis: (Vollständige Induktion) Wir beweisen den Satz mittels Induktion über $m = |E|$.

- Induktionsanfang: Es sei $m = 0$. Somit bildet jeder Knoten eine eigene Zusammenhangskomponente. Mithin enthält G genau $|V| = |V| - 0 = |V| - |E|$ Komponenten.
- Induktionsschritt: Es sei $m > 0$. Somit gibt es eine Kante $e \in E$. Wir wählen eine feste Kante $e \in E$ und betrachten den Graph $G' = (V, E')$ mit $E' =_{\text{def}} E \setminus \{e\}$. Es gilt $|E'| = m - 1$ und wir können die Induktionsvoraussetzung anwenden. Damit enthält G' mindestens

$$|V| - |E'| = |V| - (m - 1) = |V| - m + 1$$

Komponenten. Beim Einfügen von e in G' können zwei Fälle auftreten:

1. Beide Endknoten von e liegen in einer Zusammenhangskomponente von G'. Dann sind die Anzahlen der Komponenten in G und G'gleich.
2. Die Endknoten von e liegen in verschiedenen Zusammenhangskomponenten von G'. Damit ist die Anzahl der Komponenten von G um genau 1 kleiner als die Anzahl der Komponenten von G'.

Insgesamt enthält G somit mindestens

$$\begin{aligned}&(\text{Anzahl der Komponenten von } G') - 1\\ &\qquad \geq (|V| - m + 1) - 1 = |V| - m = |V| - |E|\end{aligned}$$

Komponenten.

Damit ist das Theorem bewiesen. ■

Korollar 6.20

Für jeden zusammenhängenden Graph $G = (V, E)$ gilt $|E| \geq |V| - 1$.

Beweis: Ein zusammenhängender Graph besteht aus genau einer Zusammenhangskomponente. Nach Theorem 6.19 gilt somit $1 \geq |V| - |E|$. Durch Umstellung der Ungleichung nach $|E|$ ergibt sich das Korollar. ■

6.3 Kreisfreie Graphen

Eine wichtige Klasse von Graphen sowohl im ungerichteten als auch im gericheteten Fall sind kreisfreie Graphen. Ein ungerichteter Graph ist kreisfrei, falls er keinen einfachen Kreis enthält. Für den gerichteten Fall werden wir später die Begriffsbildung anpassen.

Ungerichtete, kreisfreie Graphen: Bäume und Wälder

Definition 6.21

Es sei $G = (V, E)$ ein ungerichteter Graph.

1. G heißt Baum, falls G zusammenhängend und kreisfrei ist.
2. G heißt Wald, falls dessen Zusammenhangskomponenten Bäume sind.
3. Ein Knoten $v \in V$ heißt Blatt, falls $\deg_G(v) = 1$ gilt.

Lemma 6.22

Jeder Baum $T = (V, E)$ mit $|V| \geq 2$ Knoten enthält mindestens zwei Blätter.

Beweis: Es sei e eine beliebige Kante. Wir laufen von den Endknoten durch den Baum, bis es keine Kante mehr gibt, über die der aktuelle Knoten wieder verlassen werden kann (ohne Zurückgehen). Da T ein Baum ist, wird kein Knoten doppelt besucht. Somit müssen Läufe enden und die gefundenen Knoten sind Blätter. Da e zwei Endknoten besitzt, gibt es mindestens zwei Blätter und das Lemma ist bewiesen. ■

Lemma 6.23

Es sei $T = (V, E)$ ein Baum mit $|V| \geq 2$ und $v \in V$ ein Blatt. Dann ist der Graph $T' =_{\text{def}} T[V \setminus \{v\}]$ ein Baum.

Beweis: Durch Wegnahme von Knoten und Kanten können keine neuen Kreise entstehen; somit ist T' kreisfrei, da T kreisfrei ist. Es sei $x, y \in V \setminus \{v\}$. Da T zusammenhängend ist, gibt es einen (x, y)-Pfad P in T. Für jeden Knoten $u \notin \{x, y\}$ auf dem Pfad P gilt mithin $\deg(u) \geq 2$. Somit liegt v nicht auf P. Der Pfad P existiert also auch in T'. Damit ist T' zusammenhängend und das Lemma ist bewiesen. ■

Theorem 6.24

Für jeden Baum $T = (V, E)$ gilt $|E| = |V| - 1$.

Beweis: (Induktion) Wir führen einen Beweis mittels vollständiger Induktion über die Anzahl n der Knoten von V, d.h., wir beweisen die Aussage: Für alle $n \in \mathbb{N}_+$ und alle Bäume $T = (V, E)$ mit $|V| = n$ gilt $|E| = |V| - 1$.

- Induktionsanfang: Es sei $n = 1$. Dann gilt für jeden Baum T mit einem Knoten $|E| = 0$ und folglich $|E| = |V| - 1$.
- Induktionsschritt: Es sei $n > 1$. Es sei $T = (V, E)$ ein Baum mit $|V| = n \geq 2$ Knoten. Dann gibt es nach Lemma 6.22 ein Blatt $v \in V$ mit der zugehörigen Kante $e = \{u, v\} \in E$. Wir definieren $T' =_{\text{def}} T[V \setminus \{v\}]$. Nach Lemma 6.23 ist T' ein Baum. Außerdem besteht T' aus $n - 1$ Knoten und besitzt somit nach Induktionsvoraussetzung $n - 2$ Kanten. Wir erhalten:

$$\begin{aligned} |V| &= |V \setminus \{v\} \cup \{v\}| = |V \setminus \{v\}| + |\{v\}| = (n-1) + 1 = n \\ |E| &= |E \setminus \{e\} \cup \{e\}| = |E \setminus \{e\}| + |\{e\}| = (n-2) + 1 = n - 1 \end{aligned}$$

  Mithin gilt $|E| = |V| - 1$.

Damit ist das Theorem bewiesen. ■

Lemma 6.25

Es seien $T = (V, E)$ ein Baum, $v \in V$ ein Knoten und $T_1, \ldots, T_k$ die Komponenten von $T[V \setminus \{v\}]$. Dann gilt $k = \deg_T(v)$ und $T_1, \ldots, T_k$ sind Bäume.

Beweis: Da T zusammenhängend und kreisfrei, sind $T_1, \ldots, T_k$ zusammenhängend und kreisfrei, d.h., $T_1, \ldots, T_k$ sind Bäume. Es sei $T_i = (V_i, E_i)$ die i-te Komponente von $T[V \setminus \{v\}]$. Dann gilt:

1. Jeder Knoten aus $V \setminus \{v\}$ gehört zu einem T_i, d.h., es gilt

$$|V| = 1 + \sum_{i=1}^{k} |V_i|$$

2. Jede Kante $e \in E$ mit $v \notin e$ gehört zu einem T_i, d.h., es gilt

$$|E| = \deg_T(v) + \sum_{i=1}^{k} |E_i|$$

Mit Hilfe von Theorem 6.24 erhalten wir somit:

$$\begin{aligned} |V| - 1 &= \deg_T(v) + \sum_{i=1}^{k} (|V_i| - 1) \\ &= \deg_T(v) + \sum_{i=1}^{k} |V_i| \quad - k \\ &= \deg_T(v) + |V| - 1 - k \end{aligned}$$

Umstellung nach $\deg_T(v)$ ergibt $\deg_T(v) = k$ und das Lemma ist bewiesen. ■

Lemma 6.26

Es seien $G = (V, E)$ ein zusammenhängender Graph und C ein einfacher kreis in G. Dann gilt für alle auf C liegenden Kanten e, dass der Graph $(V, E \setminus \{e\})$ zusammenhängend ist.

Beweis: (Widerspruch) Angenommen es gibt eine Kante $e = \{u, v\} \in C$, sodass der Graph $G - e =_{\text{def}} (V, E \setminus \{e\})$ nicht zusammenhängend ist. Dann liegen die Endknoten u und v in verschiedenen Komponenten von $G - e$. Da aber e auf einem einfachen Kreis C liegt gibt es einen (u, v)-Pfad, der e nicht enthält (wir laufen in C einfach „außen“ herum). Somit existiert der (u, v)-Pfad auch in $G - e$. Folglich liegen u und v in der gleichen Komponenten. Dies ist ein Widerspruch und somit muss $G - e$ zusammenhängend sein, egal welche Kante aus dem Kreis aus G entfernt wird. Damit ist das Lemma bewiesen. ■

Ein Graph $T = (V_T, E_T)$ heißt Spannbaum (oder aufspannender Baum) eines Graphen $G = (V_G, E_G)$, falls T ein Baum mit $V_T = V_G$ und $E_T \subseteq E_G$ ist.

Theorem 6.27

Jeder zusammenhängende Graph $G = (V, E)$ enthält einen Spannbaum.

Beweis: Für $|V| = 1$ gilt die Aussage trivialerweise. Es sei also $G = (V, E)$ ein Graph mit $|V| \geq 2$ und $|E| = m$. Wir betrachten eine beliebige Folge $E_0, E_1, \ldots, E_m$ von Kantenmengen in G, die folgende Bedingungen erfüllt:

$$E_0 = E$$
$$E_i = \begin{cases} E_{i-1} \setminus \{e_i\}, & \text{wobei } e_i \in E_{i-1} \text{ eine beliebige auf einem einfachen Kreis in } (V, E_{i-1}) \\ & \text{liegende Kante ist} \\ E_{i-1}, & \text{falls kein einfacher Kreis in } (V, E_{i-1}) \text{ existiert} \end{cases}$$

Klarerweise gilt $E_0 \supseteq E_1 \supseteq E_2 \supseteq \cdots \supseteq E_m$. Nach Lemma 6.26 ist (V, E_m) zusammenhängend und kreisfrei, da höchstens m Kanten aus G entfernt werden können. Somit ist (V, E_m) ein Spannbaum und das Theorem ist bewiesen. ■

Theorem 6.28 (Cayley)

Für $n \geq 2$ gibt es genau n^{n-2} markierte Bäume mit n Knoten.

Beweis: Wir konstruieren eine Bijektion zwischen der Menge aller markierten Bäume mit n Knoten und der Menge $\{1, \ldots, n\}^{n-2}$. Dabei fassen wir die Elemente von $\{1, \ldots, n\}^{n-2}$ als Wörter der Länge $n-2$ über dem Alphabet $\{1, \ldots, n\}$ auf. Wir betrachten folgende Abbildung φ für einen Baum $T = (V, E)$ mit $V \subseteq [n]$:

$$\begin{array}{lll} \varphi(T) & =_{\text{def}} \quad \varepsilon, & \text{falls } |V| = 2 \\ \varphi(T) & =_{\text{def}} \quad v \cdot \varphi(T[V \setminus \{u\}]), & \text{wobei } u \text{ das kleinste Blatt in } T \text{ ist und} \\ & & v \text{ der zu } u \text{ adjazente Knoten ist} \end{array}$$

Nach Lemma 6.23 sind die induzierten Teilgraphen stets Bäume. Außerdem gilt: Jeder Knoten v von T kommt $(\deg_T(v) - 1)$-mal im Wort $\varphi(T)$ vor. Somit erhalten wir für die Länge:

$$\begin{aligned} |\varphi(T)| &= \sum_{v \in V} (\deg_T(v) - 1) \\ &= \sum_{v \in V} \deg_T(v) \quad - |V| \\ &= 2 \cdot |E| - |V| \\ &= 2 \cdot (|V| - 1) - |V| \\ &= |V| - 2 \end{aligned}$$

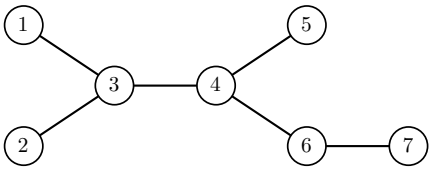
Die Injektivität der Abbildung ist leicht zu sehen. Zum Nachweis der Bijektivität der Abbildung φ geben wir an, wie wir zu einem gegebenen Wort $t = t_1 \ldots t_{n-2}$ einen Baum T finden mit $\varphi(T) = t$:

```
[1]   S := ∅
[2]   E := ∅
[3]   for i := 1 to n − 2 do
[4]       s_i := min [n] \ (S ∪ {t_i, ..., t_{n−2}})
[5]       E := E ∪ {{s_i, t_i}}
[6]       S := S ∪ {s_i}
[7]   E := E ∪ {[n] \ S}
```

Damit ist φ surjektiv und somit bijektiv. Es gibt also genauso viele Bäume, wie es Wörter in $\{1, \ldots, n\}^{n-2}$ gibt. Dies sind nach der Produktregel der Kombinatorik n^{n-2} viele. Damit ist das Theorem bewiesen. ■

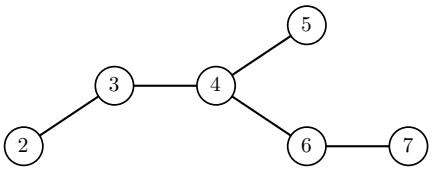
Theorem 6.27 kann auf verschiedene Arten bewiesen werden. Die in unserem Beweis angegebene Kodierung eines markierten Baumes als Wort heißt Prüfer-Code nach dem Erfinder der Kodierung.

Beispiel: Wir bestimmen den Prüfer-Code für den folgenden Baum $T = T_0$: Im Baum T_0 ist das Blatt mit der kleinsten Nummer der Knoten 1.



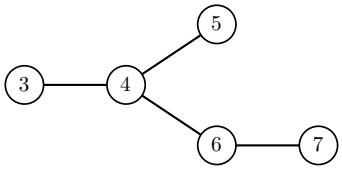
$\varphi(T_0) = 3\varphi(T_1)$

Im Baum T_1 ist das Blatt mit der kleinsten Nummer der Knoten 2.



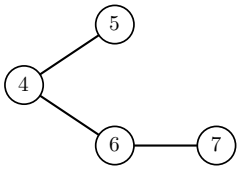
$\varphi(T_0) = 33\varphi(T_2)$

Im Baum T_2 ist das Blatt mit der kleinsten Nummer der Knoten 3.



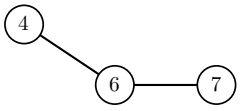
$\varphi(T_0) = 334\varphi(T_3)$

Im Baum T_3 ist das Blatt mit der kleinsten Nummer der Knoten 5.



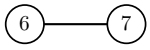
$\varphi(T_0) = 3344\varphi(T_4)$

Im Baum T_4 ist das Blatt mit der kleinsten Nummer der Knoten 4.



$\varphi(T_0) = 33446\varphi(T_5)$

Der Baum T_5 enthält nur noch zwei Knoten.



$\varphi(T_0) = 33446$

Somit ergibt sich der Prüfer-Code $\varphi(T) = 33446$.

Wenn nun umgekehrt das Wort 33446 gegeben ist, so bestimmen wieder den zugehörigen Baum T wie folgt:

i	s_i	S	$t_i \dots t_{n-2}$	E
0	–	$\emptyset$	33446	$\emptyset$
1	1	$\{1\}$	3446	$\{\{1,3\}\}$
2	2	$\{1,2\}$	446	$\{\{1,3\},\{2,3\}\}$
3	3	$\{1,2,3\}$	46	$\{\{1,3\},\{2,3\},\{3,4\}\}$
4	5	$\{1,2,3,5\}$	6	$\{\{1,3\},\{2,3\},\{3,4\},\{4,5\}\}$
5	4	$\{1,2,3,4,5\}$	ε	$\{\{1,3\},\{2,3\},\{3,4\},\{4,5\},\{4,6\}\}$
–	–	–	–	$\{\{1,3\},\{2,3\},\{3,4\},\{4,5\},\{4,6\},\{6,7\}\}$

Gerichtete, kreisfreie Graphen*

Im Falle eines gerichteten Graphen macht es einen Unterschied, ob für eine Kante (u, v) auch die umgekehrte Kante (v, u) im Graphen vorkommt oder nicht. Daher benötigen wir eine eigenen Begriff für einen Kreises, um die Kreisfreiheit zu definieren.

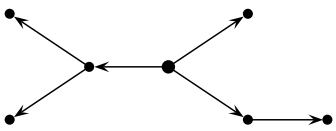
Definition 6.29

Es sei $G = (V, E)$ ein gerichteter Graph.

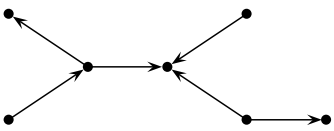
1. Ein Weg $(v_0, e_0, v_1, \dots, v_{n-1}, e_n, v_n)$ mit $v_0 = v_n$ und $n > 0$ heißt (gerichteter) Kreis in G.
2. Enthält G keinen gerichteten Kreis, so heißt G gerichteter, azyklischer (oder kreisfreier) Graph (englisch: *directed acyclic graph* oder kurz *dag*).

Es ist auch im Deutschen üblich, einen gerichteten, kreisfreien Graph nach dem englischen Ausdruck Dag zu nennen.

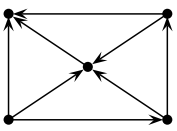
Beispiel: Folgende gerichtete Graphen sind Beispiele für kreisfreie Graphen:



Wurzelbaum



Polytree



Dag

Theorem 6.30

Für einen gerichteten Graphen $G = (V, E)$ sind folgende Aussagen äquivalent:

1. G ist kreisfrei.
2. Jeder (induzierte) Teilgraph von G enthält eine Senke.
3. Jeder (induzierte) Teilgraph von G enthält eine Quelle.

Beweis: Wir beweisen nur, dass die Aussage 1 zu Aussage 2 äquivalent ist. Durch die Vertauschung von ausgehenden und eingehenden Kanten (und aller zugehörigen Begriffe) ergibt sich dann auch die Äquivalenz von 1 und 3. Wir zeigen beide Richtungen einzeln:

- 1. $\Rightarrow$ 2.: Wir zeigen die Kontraposition. Es gibt $U \subseteq V$, sodass $G[U]$ keine Senke enthält, d.h. $\deg^+_{G[U]}(v) > 0$ für alle Knoten $v \in U$. Somit gibt es für jeden Knoten eine ausgehende Kante in $G[U]$. Wir wählen einen beliebigen Knoten $v_0 \in U$. Wegen $\deg^+_{G[U]}(v_0) > 0$ gibt es eine Kante $e_1 = (v_0, v_1)$ in $G[U]$. Wiederum wegen $\deg^+_{G[U]}(v_1) > 0$ gibt es eine Kante $e_2 = (v_1, v_2)$ in $G[U]$ usw. usf. Auf diese Weise erhalten wir eine unendlich lange Knotenfolge $(v_0, v_1, v_2, \ldots)$. Da es nur endlich viele Knoten gibt, muss ein Knoten doppelt vorkommen. Somit gibt es einen Kreis in G.
- 2. $\Rightarrow$ 1.: Wir zeigen die Kontraposition. G enthalte einen Kreis $W = (v_0, v_1, \ldots, v_k)$, d.h. $v_k = v_0$ und $k \geq 2$. Dann besitzen alle Knoten v_i in $G' =_{\text{def}} G[\{v_0, v_1, \ldots, v_{k-1}\}]$ einen Ausgangsgrad $\deg^+_{G'}(v_i) > 0$. Mithin enthält G' keine Senke.

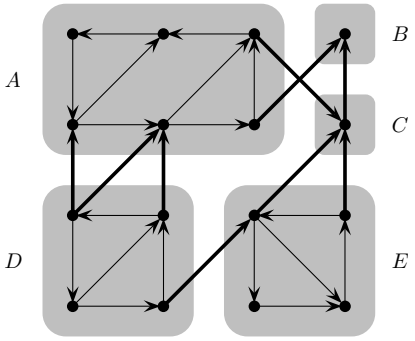
Damit ist das Theorem bewiesen. ■

Betrachten wir die Erreichbarkeitsrelation $\rightarrow^*$ auf gerichteten Graphen, d.h. die für den Graphen $G = (V, E)$ und die Knoten $u, v \in V$ wie folgt definierte Relation

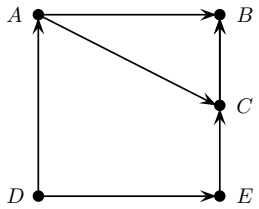
$$u \rightarrow^* v \iff_{\text{def}} \text{ es gibt einen } (u, v)\text{-Weg in } G,$$

so bedeutet das Vorhandensein eines Kreises, dass alle Knoten auf dem Kreis in derselben starken Zusammenhangskomponente liegen. Gilt dagegen $u \rightarrow^* v$ und $v \not\rightarrow^* u$, so liegen u und v in jedem Fall in verschiedenen Komponenten und auf keinem Kreis. Wir können somit jeden gerichteten Graphen eindeutig in seine starken Zusammenhangskomponenten sowie einen gerichteten, kreisfreien Graphen zerlegen.

Beispiel: Wir betrachten exemplarisch für die Zerlegung den Graphen G:



Die grau unterlegten Teilgraphen sind jeweils starke Zusammenhangskomponenten. Es ist ersichtlich, dass alle Kanten, die zwischen zwei unterschiedlichen Komponenten verlaufen, in dieselbe Richtung zeigen. Führen wir die Superknoten A, B, C, D, E ein, um die Komponenten zu repräsentieren, so können wir den Graphen in naheliegender Weise auf den folgenden Graphen reduzieren:



Der reduzierte Graph ist der gesuchte gerichtete, kreisfreie Graph.

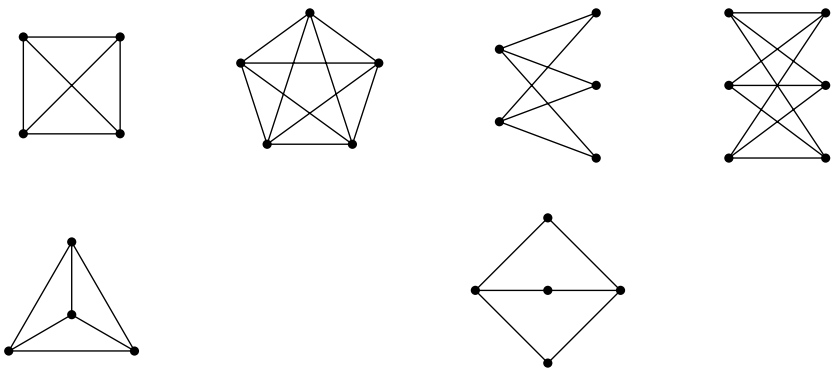
6.4 Planare Graphen

Definition 6.31

Es sei $G = (V, E)$ ein (ungerichteter) Graph.

1. G heißt planar (oder plättbar), falls G so gezeichnet werden kann, dass sich keine Kanten kreuzen.
2. G heißt eben, falls G planar und in einer kreuzungsfreien Darstellung (Einbettung in der Ebene) gegeben ist.

Beispiele: Im Folgenden sind der oberen Reihe die vier Graphen K^4, K^5, $K_{2,3}$ und $K_{3,3}$ angegeben. Die Reihe darunter enthalten Darstellungen der ebenen Graphen im Falle, dass die darüber liegenden Graphen planar sind.



K^4 und $K_{2,3}$ sind planar, K^5 und $K_{3,3}$ sind nicht planar.

Es sei $G = (V, E)$ ein ebener Graph. Ein Gebiet (Facette) ist ein Teil der Ebene, der entsteht, wenn die Ebene entlang der Kanten zerschnitten wird.

Beispiele: Wir zählen leicht nach, dass der K^4 vier Gebiete und der $K_{2,3}$ drei Gebiete besitzt. Dabei heißen die endlichen Gebiete im Inneren von Kreisen innere Gebiete und das unendliche Gebiet äußeres Gebiet.

Theorem 6.32 (Eulersche Polyederformel)

Es sei $G = (V, E)$ ein zusammenhängender, ebener Graph. Es sei F die Menge der Gebiete von G. Dann gilt:

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

Beweis: (Induktion) Wir führen ein Beweis mittels vollständiger Induktion über den Exzess von Graphen. Der Exzess von $G = (V, E)$ ist definiert als

$$\text{ex}(G) =_{\text{def}} |E| - |V| + k,$$

wobei k die Anzahl der Zusammenhangskomponenten von G ist. Für zusammenhängende Graphen $G = (V, E)$ gilt somit $\text{ex}(G) = |E| - |V| + 1 \geq 0$.

- Induktionsanfang: Es sei $G = (V, E)$ ein zusammenhängender, ebener Graph mit $\text{ex}(G) = 0$, d.h. $|E| = |V| - 1$. Somit ist G ein Baum. Da G keine Kreise enthält, gibt es genau *ein* Gebiet und es gilt $1 = |E| - |V| + 2$.
- Induktionsschritt: Es sei $G = (V, E)$ ein zusammenhängender, ebener Graph mit $\text{ex}(G) > 0$. Somit ist G kein Baum. Es gibt also einen einfachen Kreis C in G. Es sei e eine beliebige Kante auf C. Die Kante e trennt das Gebiet f_1 innerhalb des Kreises C von dem Gebiet f_2 außerhalb von C. Es sei $G' =_{\text{def}} (V, E \setminus \{e\})$ der ebene Graph, der aus G entsteht, wenn e entfernt wird. Dadurch verschmelzen die Gebiet f_1 und f_2 zu einem Gebiet in G'. Außerdem ist G' nach ... wieder zusammenhängend, also gilt $\text{ex}(G') = \text{ex}(G) - 1$. Nach Induktionsvoraussetzung gilt somit:

$$|F| = \underbrace{|F| - 1}_{\text{Gebiete von } G'} + 1 = \underbrace{|E| - 1}_{\text{Kanten von } G'} - |V| + 2 + 1 = |E| - |V| + 2$$

Damit ist das Theorem bewiesen. ■

Theorem 6.33

Für jeden planaren Graphen $G = (V, E)$ mit $|V| \geq 3$ gilt

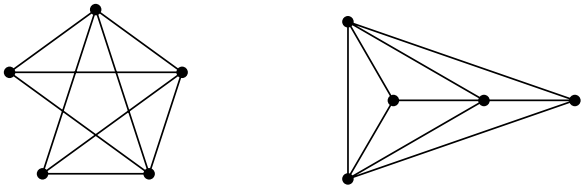
$$|E| \leq 3|V| - 6.$$

Beweis: Es genügt die Aussage für kantenmaximale planare Graphen zu zeigen. Es sei $G = (V, E)$ ein kantenmaximaler planarer Graph. Das Einfügen einer weiteren Kante in G würde also die Planarität zerstören. Somit ist G zusammenhängend. G sei als ebener Graph gegeben. Jede Kante begrenzt höchstens zwei Gebiete von G. Somit gilt $|F| \leq 2|E|$. Weiterhin wird jedes Gebiet von mindestens drei Kanten begrenzt. Somit folgt $|F| \leq \frac{2}{3} \cdot |E|$. Mit Theorem 6.32 erhalten wir:

$$\frac{2}{3} \cdot |E| \geq |F| = |E| - |V| + 2$$

Umstellung der Ungleichung nach $|E|$ ergibt das Theorem. ■

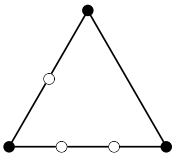
Beispiele: K^5 ist nicht planar, denn es gilt $10 \not\leq 3 \cdot 5 - 6 = 9$. Der K^5 hat also eine Kante zuviel. Entfernen wir eine beliebige Kante aus dem K^5, so erhalten wir den fast vollständigen Graphen K^{5*}. Dieser erfüllt die Kantenbilanz und ist auch planar:



Der $K_{3,3}$ erfüllt auch die Kantenbilanz, ist jedoch nicht planar (siehe Übungsaufgabe).

Eine Unterteilung eines Graphen $G = (V, E)$ entsteht dadurch, dass Kanten $e \in E$ durch neue Pfade p_e ersetzt werden.

Beispiel: Eine Untereilung des K^3 könnte zum Beispiel wie folgt aussehen:



K^5 und $K_{3,3}$ sind gewissermaßen die kleinsten, nicht planaren Graphen. Ohne Beweis geben wir den Satz von Kuratowski an, der planare Graphen durch den Ausschluss von K^5 und $K_{3,3}$ charakterisiert.

Theorem 6.34 (Kuratowski)

Ein Graph G ist genau dann planar, wenn G keine Unterteilung des K^5 oder $K_{3,3}$ als Teilgraph enthält.

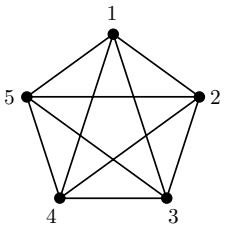
6.5 Färbungen

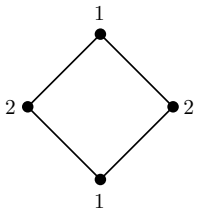
Definition 6.35

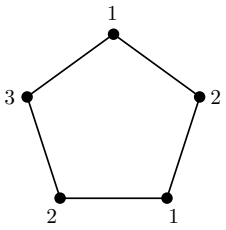
Es sei $G = (V, E)$ ein Graph.

1. Eine Knotenfärbung von G mit k Farben ist eine Abbildung $c : V \to \{1, \ldots, k\}$ mit $c(u) \neq c(v)$ für alle Kanten $\{u, v\} \in E$.
2. Die chromatische Zahl $\chi(G)$ von G ist die minimale Anzahl k von Farben, sodass eine Knotenfärbung von G mit k Farben existiert.

Beispiele: In den folgenden Abbildung sind Graphfärbungen mit der minimalen Anzahl von Farben gezeigt:







Dazu korrespondieren die allgemeinen Fälle:

1. K^n benötigt n Farben.
2. C_{2n} benötigt 2 Farben.
3. C_{2n+1} benötigt 3 Farben.

Die Graphen mit chromatischer Zahl 2 sind genau die bipartiten Graphen:

Definition 6.36

Ein ungerichteter Graph $G = (V, E)$ heißt bipartit, falls es disjunkte, nichtleere Knotenmengen A und B mit $A \cup B = V$ gibt, sodass die induzierten Teilgraphen $G[A]$ und $G[B]$ keine Kante enthalten.

In bipartiten Graphen verlaufen Kanten also nur zwischen den Knotenmengen A und B, aber nicht innerhalb der Mengen. Wenn wir uns auf die Bipartitheit beziehen, schreiben wir auch $G = (A \uplus B, E)$. (Hierbei bedeutet $A \uplus B$, dass wir die Vereinigung von zwei disjunkten Mengen A und B bilden.)

Theorem 6.37

Ein Graph $G = (V, E)$ ist genau dann bipartit, wenn er keinen einfachen Kreis ungerader Länge als Teilgraph enthält.

Beweis: Wir zeigen beide Richtungen einzeln. Ohne Beeinträchtigung der Allgemeinheit kann der Graph als zusammenhängend angenommen werden. Anderenfalls argumentieren wir für jede Komponente.

$\Rightarrow$: Wir beweisen die Kontraposition. Ein einfacher Kreis C_{2n+1} ungerader Länge ist nicht bipartit. Somit ist ein Graph, der einen solchen Kreis enthält, nicht bipartit.

$\Leftarrow$: Es sei $G = (V, E)$ ein Graph, der nur einfache Kreise gerader Länge enthält. Wir wählen einen beliebigen Knoten v und betrachten die zugehörigen Knotenmengen:

$$\begin{aligned} A &=_{\text{def}} \{\, u \mid \text{kürzester } (u, v)\text{-Weg hat gerade Länge} \,\} \\ B &=_{\text{def}} \{\, u \mid \text{kürzester } (u, v)\text{-Weg hat ungerade Länge} \,\} \end{aligned}$$

Dann gilt sicherlich $A \cap B = \emptyset$ sowie $A \cup B = V$. Wir müssen noch zeigen, dass die induzierten Teilgraphen $G[A]$ und $G[B]$ keine Kanten enthalten. Es seien $x, y \in V$ zwei verschiedene

Knoten, die entweder beide in A oder beide in B liegen. Es seien $P_x = (u_0, u_1, \ldots, u_k)$ mit $x = u_0$ und $u_k = v$ ein kürzester (x, v)-Pfad und $P_y = (u'_0, u'_1, \ldots, u'_{k'})$ mit $y = u'_0$ und $u'_{k'} = v$ ein kürzester (y, v)-Weg. Dann ist $k + k'$ gerade. Es sei u_j der erste Knoten auf P_x, der auch auf P_y vorkommt, d.h., $u_j = u'_{j'}$ für ein geeignetes j'. Betrachten wir die Pfade $P'_x = (u_0, \ldots, u_j, u'_{j'+1}, \ldots, u'_{k'})$ und $P'_y = (u'_0, \ldots, u'_{j'}, u_{j+1}, \ldots, u_k)$, dann sind P'_x wieder ein kürzester (x, v)-Pfad und P'_y ein kürzester (y, v)-Pfad. Mithin gilt $j + k' - j' = k$. Also gilt $j + j' = k + k' + 2(j' - k')$, und $j + j'$ ist gerade. Wenn nun $\{x, y\} \in E$ gelten würde, so würde G den einfachen Kreis $(x, \ldots, u_j, u'_{j'-1}, \ldots, y, x)$ der Länge $j + j' + 1$ enthalten. Da einfache Kreise ungerader Länge ausgeschlossen sind, gilt $\{x, y\} \notin E$. Somit verlaufen keine Kanten zwischen Knoten in A und keine Kanten zwischen den Knoten in B. Damit ist G bipartit.

Damit ist das Theorem bewiesen. ■

Korollar 6.38

Jeder Baum ist bipartit.

Beweis: Bäume enthalten keine Kreise, also auch keine Kreise ungerader Länge. ■

Ohne Beweis geben wir das folgende berühmte Theorem an, das erstmals 1976 von Appel und Haken unter Einsatz eines Computerprogramms zur Überprüfung von mehr als 1.500 Einzelfällen bewiesen wurde. Insbesondere folgt aus dem Theorem, dass auf politisch-geographischen Landkarten vier Farben genügen, um alle Länder so zu färben, dass Grenzen nur zwischen Ländern unterschiedlicher Farben verlaufen.

Theorem 6.39 (Vierfarbensatz)

Für jeden planaren Graphen ist $\chi(G) \leq 4$.

Definition 6.40

Es sei $G = (V, E)$ ein Graph.

1. Eine Kantenfärbung von G mit k Farben ist eine Abbildung $c : E \to \{1, \ldots, k\}$ mit $c(e) \neq c(f)$ für alle Kanten $e, f \in E$ mit $e \cap f \neq \emptyset$.
2. Der chromatische Index $\chi'(G)$ von G ist die minimale Anzahl k von Farben, sodass eine Kantenfärbung von G mit k Farben existiert.

Wiederum ohne Beweis geben wir folgendes Theorem an, das zeigt, dass der chromatische Index eines Graphen nur einen von zwei Werten annehmen kann.

Theorem 6.41 (Vizing)

Für jeden Graphen $G = (V, E)$ gilt $\Delta(G) \leq \chi'(G) \leq \Delta(G) + 1$, wobei $\Delta(G)$ der maximale Grad eines Knoten von G ist.

6.6 Paarungen*

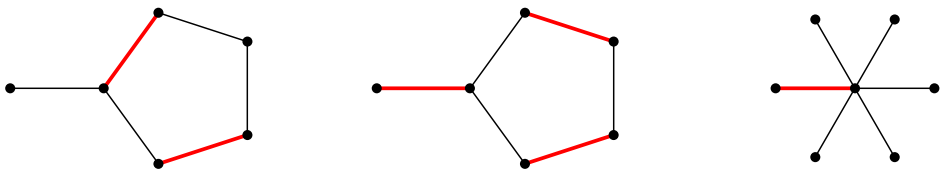
Definition 6.42

Es sei $G = (V, E)$ ein Graph.

1. Eine Kantenmenge $M \subseteq E$ heißt Matching (oder Paarung) in G, falls $e \cap f = \emptyset$ für alle Kanten $e, f \in M$ mit $e \neq f$ gilt.
2. Ein Matching $M \subseteq E$ heißt perfekt, falls $|M| = \frac{1}{2}|V|$ gilt.

Mit anderen Worten: Ist M ein Matching in einem Graphen G, so ist jeder Knoten v von G zu höchstens einer Kante $e \in M$ inzident. Gilt $v \in e$ für eine Kante $e \in M$, so wird der Knoten v von M überdeckt. Ein perfektes Matching überdeckt somit jeden Knoten des Graphen G.

Beispiele: In folgenden Graphen bilden die roten Kanten jeweils Matchings:



Das Matching in der Mitte ist perfekt, während links nur ein weiteres Matching gezeigt ist. Der Sterngraph rechts besitzt kein perfektes Matching.

Für bipartite Graphen können wir die existierenden Matchings genau charakterisieren. Dafür erweitern für einen Graphen $G = (V, E)$ die Schreibweise $N_G(v)$ für die Nachbarschaft eines Knotens v auf die Nachbarschaft $N_G(X)$ einer Knotenmenge $X \subseteq V$:

$$N_G(X) =_{\text{def}} \bigcup_{v \in X} N_G(v)$$

Wenn der Graph G aus dem Kontext heraus klar ist, lassen wir wieder den Index G weg.

Theorem 6.43 (Hall; Heiratssatz)

Für einen bipartiten Graphen $G = (A \uplus B, E)$ gibt es genau dann ein Matching M der Kardinalität $|M| = |A|$, wenn $|N(X)| \geq |X|$ für alle $X \subseteq A$ gilt.

Beweis: Wir beweisen beide Richtung einzeln.

$\Rightarrow$: Es sei M ein Matching der Kardinalität $|M| = |A|$. Jede Teilmenge $X \subseteq A$ hat somit genau $|X|$ Nachbarn in B. Folglich gilt $|N(X)| \geq |X|$.

$\Leftarrow$: Wir führen den Beweis mittels Induktion über die Kardinalität der Menge $|A|$.

- Induktionsanfang: Für $m = 1$ ist die Aussage offensichtlich.
- Induktionsschritt: Es sei $m > 1$. Es sei $G = (A \uplus B, E)$ ein beliebiger bipartiter Graph mit $|A| = m$. Wir unterscheiden zwei Fälle:

  1. Fall: Für alle $S \subseteq A$ mit $0 < |S| < m$ gilt $|N(S)| \geq |S| + 1$. Wir konstruieren ein Matching M wie folgt: Es sei $e = \{u, v\} \in E$ eine beliebige Kante mit $u \in A$ und $v \in B$. Für den Graphen $G' =_{\text{def}} G[A \uplus B \setminus \{u, v\}]$ gilt $N_{G'}(X) = N_G(X) \setminus \{v\}$ und mithin $|N_{G'}(X)| \geq |X|$ für alle $X \subseteq A \setminus \{u\}$. Nach Induktionsvoraussetzung enthält der Graph G' ein Matching M' der Kardinalität $|M'| = |A \setminus \{u\}| = m - 1$. Somit ist $M =_{\text{def}} M' \cup \{e\}$ ein Matching in G der Kardinalität $|M| = |A| = m$.

  2. Fall: Es gibt ein $S \subseteq A$ mit $0 < |S| < m$ und $|N(S)| = |S|$. Wir halten ein S fest und konstruieren ein Matching M wie folgt: Es seien

  $$\begin{aligned} G' &=_{\text{def}} G[S \cup N_G(S)] \\ G'' &=_{\text{def}} G[(A \setminus S) \cup (N_G(A) \setminus N_G(S))] \end{aligned}$$

  Für alle $X \subseteq S$ gilt $N_{G'}(X) = N_G(X)$ und somit $|N_{G'}(X)| \geq |X|$. Nach Induktionsvoraussetzung (beachte: $|S| \leq m - 1$) gibt es ein Matching M' der Kardinalität $|M'| = |S|$ in G'. Für alle $X \subseteq A \setminus S$ gilt $N_{G''}(X) \cap N_G(S) = \emptyset$. Wir erhalten:

  $$\begin{aligned} |N_{G''}(X)| &= |N_{G''}(X) \cup N_G(S)| - |N_G(S)| \\ &= |N_G(X) \cup N_G(S)| - |N_G(S)| \\ &= |N_G(X \cup S)| - |N_G(S)| \\ &\geq |X \cup S| - |N_G(S)| \\ &= |X| + |S| - |N_G(S)| \\ &= |X| \end{aligned}$$

  Nach Induktionsvoraussetzung (beachte: $|S| \geq 1$ bzw. $|A \setminus S| \leq m - 1$) gibt es ein Matching M'' der Kardinalität $|M''| = |A \setminus S|$ in G''. Da die Menge der durch M' und die Menge der durch M'' überdeckten Knoten disjunkt sind, ist $M =_{\text{def}} M' \cup M''$ ein Matching in G der Kardinalität $|M| = |S| + |A \setminus S| = |A| = m$.

Damit ist das Theorem bewiesen. ■

Korollar 6.44

Jeder k-reguläre, bipartite Graph G enthält ein perfektes Matching und hat den chromatischen Index $\chi'(G) = k$.

Beweis: Wir beweisen beide Aussagen einzeln.

1. Es sei $G = (A \uplus B, E)$ ein k-regulärer, bipartiter Graph. Dann gibt es $k \cdot |A| = |E|$ Kanten, die von A nach B verlaufen. Andererseits verlaufen auch $|E| = k \cdot |B|$ Kanten von B nach A. Mithin gilt $|A| = |B|$. Jedes Matching M der Kardinalität $|M| = |A|$ ist somit ein perfektes Matching. Es sei $X \subseteq A$. Dann gibt es $k \cdot |X|$ Kanten, die in die Nachbarschaft $N(X)$ führen. Jeder Knoten $v \in N(X)$ ist adjazent zu höchstens k Knoten in X. Somit gilt $k \cdot |X| \leq k \cdot |N(X)|$ bzw. $|X| \leq |N(X)|$. Nach Theorem 6.43 gibt es somit ein perfektes Matching in G.

2. Der Nachweis erfolgt über Induktion über k und ist eine Übungsaufgabe.

Damit ist das Korollar bewiesen. ■

7 Algebraische Strukturen*

7.1 Universelle Algebren

Definition 7.1

Eine (universelle) Algebra $\langle S, f_1, \ldots, f_t \rangle$ besteht aus einer nichtleeren Trägermenge S und Operatoren $f_1, \ldots, f_t$ der Stelligkeiten $m_1, \ldots, m_t \in \mathbb{N}$, d.h. der Operator f_i ist eine Abbildung $f_i : S^{m_i} \to S$. Das Tupel $(m_1, \ldots, m_t)$ heißt Signatur der Algebra.

Beispiele: Im Folgenden werden Beispiele zum Begriff der Algebra diskutiert.

1. Die boolesche Algebra $\langle \{\mathsf{w}, \mathsf{f}\}, \vee, \wedge, \neg \rangle$ besteht aus der Menge der Wahrheitswerte w und f mit den wie folgt beschriebenen Operatoren:

$\vee$	f	w
f	f	w
w	w	w

$\wedge$	f	w
f	f	f
w	f	w

   $\neg \mathsf{f} =_{\text{def}} \mathsf{w}$
   $\neg \mathsf{w} =_{\text{def}} \mathsf{f}$

   Die Signatur der Algebra ist somit $(2, 2, 1)$.

2. $\langle \mathbb{N}, + \rangle$, $\langle \mathbb{Z}, + \rangle$ und $\langle \mathbb{N}, +, \cdot \rangle$ sind Algebren.

3. Für die Menge $S =_{\text{def}} \{\ n \in \mathbb{N} \mid n \text{ ist eine Quadratzahl } \} \subseteq \mathbb{N}$ ist $\langle S, \cdot \rangle$ eine Algebra; $\langle S, + \rangle$ ist dagegen keine Algebra.

4. Es seien Σ ein endliches Alphabet und Σ^* die Menge aller endlichen Wörter über Σ. Der zweistellige Operator $\circ : \Sigma^* \times \Sigma^* \to \Sigma^*$ ist die Konkatenation zweier Wörter x und y, d.h. $x \circ y = xy$, wobei y an x angehängt wird. Dann ist $\langle \Sigma^*, \circ \rangle$ eine Algebra.

5. Es seien U eine beliebige, nichtleere Menge, $F(U) =_{\text{def}} \{\ f \mid f : U \to U\ \}$ und $\circ$ die Hintereinanderausführung von Funktionen, d.h. $f \circ g : U \to U$ ist definiert durch $(f \circ g)(x) =_{\text{def}} f(g(x))$ für alle $x \in U$. Dann ist $\langle F(U), \circ \rangle$ eine Algebra.

Für die Stelligkeiten von Operatoren haben sich gewisse Namen eingebürgert:

- Nullstellige Operatoren sind Konstanten, z.B. $0, 42$ und $\bot$.
- Einstellige Operatoren heißen unär, z.B. $x \mapsto 2^x$, $x \mapsto \neg x$ und $A \mapsto \mathcal{P}(A)$.
- Zweistellige Operatoren heißen binär oder Verknüpfungen, z.B. $(x, y) \mapsto \max\{x, y\}$, $(x, y) \mapsto \mathrm{ggT}(x, y)$ oder $(f, g) \mapsto f \circ g$. Verknüpfungen werden häufig durch die Infix-Notation statt der Funktionsschreibweise angegeben, z.B. $x + y$ statt $+(x, y)$.
- Dreistellige Operatoren heißen ternär, z.B. $(x, y, z) \mapsto$ `if` x `then` y `else` z und $(x, y, z) \mapsto 2 \cdot (xy + xz + yz)$.

Universelle Algebren erfüllen als einzige, aber wesentliche Bedingung die Eigenschaft der Abgeschlossenheit unter der Anwendung der Operatoren. Algebren können weiter differenziert werden, welche Eigenschaften noch erfüllt sind. Wesentlich sind hierfür vor allem binäre Operatoren oder eben Verknüfpungen, auf die wir uns im Folgenden beziehen werden.

Definition 7.2

Es sei $\langle S, \circ \rangle$ eine Algebra mit Verknüpfung $\circ$. Ein Element $e \in S$ heißt

1. linksneutral $\quad \Longleftrightarrow_{\text{def}} \quad (\forall a \in S)[e \circ a = a]$
2. rechtsneutral $\quad \Longleftrightarrow_{\text{def}} \quad (\forall a \in S)[a \circ e = a]$
3. neutral $\quad \Longleftrightarrow_{\text{def}} \quad e$ ist linksneutral und rechtsneutral

Beispiele: Einige Beispiele sollen die Begriffsbildung verdeutlichen.

1. $\langle \mathbb{N}, \cdot \rangle$ besitzt 1 als neutrales Element, denn es gilt sowohl $1 \cdot n = n$ als auch $n \cdot 1 = n$.
2. $\langle \mathbb{N}_+, + \rangle$ besitzt kein neutrales Element.
3. Wir betrachten die Algebra $\langle \{a, b\}, \circ \rangle$ mit der wie folgt definierten Verknüpfung $\circ$:

$\circ$	a	b
a	a	b
b	a	b

   Dann gilt sowohl $a \circ a = a$ und $a \circ b = b$ als auch $b \circ a = a$ und $b \circ b = b$. Somit sind a und b linksneutrale Elemente. Andererseits sind weder a noch b rechtsneutral, denn es gilt $a \circ b = b$ und $b \circ a = a$.

Proposition 7.3

Es sei $\langle S, \circ \rangle$ eine Algebra mit Verknüpfung $\circ$. Sind $c \in S$ linksneutral und $d \in S$ rechtsneutral, so gilt $c = d$.

Beweis: Da c linksneutral ist, gilt insbesondere $c \circ d = d$. Da d rechtsneutral ist, gilt insbesondere $c = c \circ d$. Somit gilt $c = c \circ d = d$. Damit ist die Proposition bewiesen. ■

Eine einfache Folgerung aus dieser Proposition ist das folgende Korollar.

Korollar 7.4

Jede Algebra $\langle S, \circ \rangle$ mit einer Verknüpfung $\circ$ besitzt höchstens ein neutrales Element.

Beweis: Sind c und d zwei neutrale Elemente von $\langle S, \circ \rangle$, so ist insbesondere c linksneutral und d rechtsneutral. Mithin gilt $c = d$. Damit ist das Korollar bewiesen. ■

Beispiele: Wir geben die neutralen Elemente weiterer Algebren an.

1. In $\langle \Sigma^*, \circ \rangle$ ist das leere Wort ε das neutrale Element.
2. In $\langle F(U), \circ \rangle$ ist die Identitätsfunktion $\mathrm{id}_U : U \to U : x \mapsto x$ neutrales Element.

Definition 7.5

Es sei $\langle S, \circ \rangle$ eine Algebra mit binärer Verknüpfung $\circ$ und neutralem Element $e \in S$. Weiterhin seien $a, x \in S$ beliebig. Dann heißt x

1. linksinvers zu a $\quad \Longleftrightarrow_{\text{def}} \quad x \circ a = e$
2. rechtsinvers zu a $\quad \Longleftrightarrow_{\text{def}} \quad a \circ x = e$
3. invers zu a $\quad \Longleftrightarrow_{\text{def}} \quad x$ ist linksinvers und rechtsinvers zu a

Beispiele: Folgende Beispiele verdeutlichen die Begriffsbildung.

1. In $\langle \mathbb{Z}, + \rangle$ ist $-x$ invers zu $x \in \mathbb{Z}$.
2. In $\langle \mathbb{Q}, \cdot \rangle$ ist $1/x$ invers zu $x \neq 0$.
3. In $\langle \mathbb{Z} \setminus \{0\}, \cdot \rangle$ besitzen nur -1 und 1 inverse Elemente.
4. Wir betrachten die Algebra $\langle \{e, a, b\}, \circ \rangle$ mit den paarweise verschiedenen Elementen e, a, b und der wie folgt gegebenen Verknüpfung $\circ$:

$\circ$	e	a	b
e	e	a	b
a	a	e	e
b	b	e	e

   Aus der Tabelle kann man ablesen, dass e das neutrale Element ist. Weiterhin ist zu sehen, dass $a \circ a = a \circ b = b \circ a = b \circ b = e$ gilt. Mithin sind a und b invers zu a und auch invers zu b.

Das letzte Beispiel macht deutlich, dass im Allgemeinen in einer Algebra die Elemente mehrere inverse Elemente besitzen können. In Algebren mit assoziativer Verknüpfung ist dies nicht möglich. Es sei $\langle S, \circ \rangle$ eine Algebra mit binärer Verknüpfung $\circ$. Dann heißt $\circ$ assoziativ, falls für alle $x, y, z \in S$ gilt:

$$(x \circ y) \circ z = x \circ (y \circ z)$$

Proposition 7.6

Es sei $\langle S, \circ \rangle$ eine Algebra mit assoziativer Verknüpfung $\circ$ und neutralem Element e. Weiterhin seien $a, x, y \in S$ beliebig. Sind x linksinvers zu a und y rechtsinvers zu a, so gilt $x = y$.

Beweis: Da e ein neutrales Element ist, gilt insbesondere $x = x \circ e$ und $y = e \circ y$. Somit ergibt sich mit Hilfe der Assoziativität:

$$x = x \circ e = x \circ (a \circ y) = (x \circ a) \circ y = e \circ y = y$$

Damit ist die Proposition bewiesen. ■

Korollar 7.7

Jedes Element $a \in S$ einer Algebra $\langle S, \circ \rangle$ mit assoziativer Verknüpfung $\circ$ und neutralem Element e besitzt höchstens ein inverses Element.

Beispiele: Wir geben die inversen Elemente für weitere Algebren an, soweit sie existieren.

1. In $\langle \Sigma^*, \circ \rangle$ besitzt nur ε ein inverses Element.
2. In $\langle F(U), \circ \rangle$ besitzen genau die bijektiven Funktionen f inverse Elemente.

Um Algebren vergleichen zu können, führen wir im Folgenden Morphismen ein. Morphismen sind Abbildungen zwischen Algebren, die in einem gewissen Sinne verträglich mit den Operatoren sind.

Beispiele: Auf der Menge $\mathbb{Z}_k =_{\text{def}} \{0, 1, \ldots, k-1\}$ definieren wir die Multiplikation $\cdot_k$ modulo k:

$$x \cdot_k y =_{\text{def}} \text{mod}(x \cdot y, k)$$

Dann ist $\langle \mathbb{Z}_k, \cdot_k \rangle$ für alle $k \in \mathbb{N}_+$ eine Algebra. Wenn wir nun die beiden Algebren $\langle \mathbb{Z}_2, \cdot_2 \rangle$ und $\langle \{\mathsf{f}, \mathsf{w}\}, \wedge \rangle$ und insbesondere die Verknüpfungen

$\cdot_2$	0	1
0	0	0
1	0	1

$\wedge$	f	w
f	f	f
w	f	w

vergleichen, so sind die beiden Algebren sehr ähnlich. Der Unterschied liegt lediglich in der Benennung der Elemente und Operatoren. Später werden wir solche Algebren isomorph nennen.

Definition 7.8

Es seien $A = \langle S, f_1, \ldots, f_t \rangle$ und $\tilde{A} = \langle \tilde{S}, \tilde{f}_1, \ldots, \tilde{f}_t \rangle$ zwei Algebren mit gleicher Signatur $(m_1, \ldots, m_t)$. Eine Abbildung $h : S \to \tilde{S}$ heißt Homomorphismus von A nach $\tilde{A}$, falls für alle $i \in \{1, \ldots, t\}$ und alle $a_1, \ldots, a_{m_i} \in S$ gilt:

$$\tilde{f}_i(h(a_1), \ldots, h(a_{m_i})) = h(f_i(a_1, \ldots, a_{m_i})),$$

d.h., f_i und $\tilde{f}_i$ sind mit h vertauschbar.

Beispiele: Wir demonstrieren das Konzept von Homomorphismen für einige Algebren.

1. Für die Algebren $A =_{\text{def}} \langle \mathbb{N}, + \rangle$ und $\tilde{A} =_{\text{def}} \langle \mathbb{Z}, + \rangle$ ist die Abbildung $h : \mathbb{N} \to \mathbb{Z} : n \mapsto n$ ein Homomorphismus von A nach $\tilde{A}$, denn für alle $n, m \in \mathbb{N}$ gilt

$$h(n) + h(m) = n + m = h(n + m).$$

2. Für $A =_{\text{def}} \langle \mathbb{N}, + \rangle$ und $\tilde{A} =_{\text{def}} \langle \mathbb{Z}_k, +_k \rangle$ mit $+_k : (x, y) \mapsto \text{mod}(x + y, k)$ ist die Abbildung $h : \mathbb{N} \to \mathbb{Z}_k : n \mapsto \text{mod}(n, k)$ ein Homorphismus von A nach $\tilde{A}$, denn wegen der Rechenregeln der Modularen Arithmetik gilt für alle $n, m \in \mathbb{N}$:

$$\begin{aligned} h(n) +_k h(m) &= \text{mod}(h(n) + h(m), k) \\ &= \text{mod}(\text{mod}(n, k) + \text{mod}(m, k), k) \\ &= \text{mod}(n + m, k) \\ &= h(n + m) \end{aligned}$$

3. Für die Algebren $A =_{\text{def}} \langle \Sigma^*, \circ \rangle$ mit der Konkatenation $\circ$ als Verknüpfung und $\tilde{A} =_{\text{def}} \langle \mathbb{N}, + \rangle$ ist die Abbildung $h : \Sigma^* \to \mathbb{N} : x \mapsto |x|$ (wobei $|x|$ die Länge von x bezeichnet) ein Homomorphismus, denn es gilt für alle Wörter $x, y \in \Sigma^*$

$$h(x) + h(y) = |x| + |y| = |x \circ y| = h(x \circ y).$$

Definition 7.9

Es sei $\langle S, f_1, \ldots, f_t \rangle$ eine Algebra mit Signatur $(m_1, \ldots, m_t)$. Eine nichtleere Teilmenge $S' \subseteq S$ erzeugt die Unteralgebra $\langle S', f_1, \ldots, f_t \rangle$, falls S' abgeschlossen ist unter $f_1, \ldots, f_t$, d.h., für alle $i \in \{1, \ldots, t\}$ und alle $a_1, \ldots, a_{m_i} \in S'$ gilt $f_i(a_1, \ldots, a_{m_i}) \in S'$.

Beispiele: Wir verdeutlichen die Begriffsbildung an einfachen Beispielen.

1. $\langle \mathbb{N}, + \rangle$ ist eine Unteralgebra von $\langle \mathbb{Z}, + \rangle$.
2. Es seien $S =_{\text{def}} \{ n \in \mathbb{N} \mid n \text{ istgerade} \}$ und $S' =_{\text{def}} \mathbb{N} \setminus S$. Dann sind $\langle S, + \rangle$ und $\langle S, \cdot \rangle$ Unteralgebren von $\langle \mathbb{N}, + \rangle$ bzw. $\langle \mathbb{N}, \cdot \rangle$. Außerdem ist auch $\langle S', \cdot \rangle$ eine Unteralgebra von $\langle \mathbb{N}, \cdot \rangle$; $\langle S', + \rangle$ ist dagegen keine Unteralgebra von $\langle \mathbb{N}, + \rangle$.

Proposition 7.10

Es sei $h : S \to \tilde{S}$ ein Homomorphismus von $A = \langle S, f_1, \ldots, f_t \rangle$ nach $\tilde{A} = \langle \tilde{S}, \tilde{f}_1, \ldots, \tilde{f}_t \rangle$. Dann ist $\langle h(S), \tilde{f}_1, \ldots, \tilde{f}_t \rangle$ eine Unteralgebra von $\tilde{A}$.

Beweis: Wir müssen die Abgeschlossenheit der Menge $h(S)$ unter $\tilde{f}_1, \ldots, \tilde{f}_t$ zeigen, d.h., für jeden Operator $\tilde{f}_i$ (der Stelligkeit m_i) muss für alle $\tilde{a}_1, \ldots, \tilde{a}_{m_i} \in h(S)$ wiederum $\tilde{f}_i(\tilde{a}_1, \ldots, \tilde{a}_{m_i}) \in h(S)$ gelten. Es sei $\tilde{a}_j \in h(S)$, d.h., es gibt ein $a_j \in S$ mit $h(a_j) = \tilde{a}_j$. Somit gilt:

$$\tilde{f}_i(\tilde{a}_1, \ldots, \tilde{a}_{m_i}) = \tilde{f}_i(h(a_1), \ldots, h(a_{m_i})) = h(f_i(a_1, \ldots, a_{m_i})) \in h(S)$$

Damit ist die Proposition bewiesen. ■

Definition 7.11

Es seien $A = \langle S, f_1, \ldots, f_t \rangle$ und $\tilde{A} = \langle \tilde{S}, \tilde{f}_1, \ldots, \tilde{f}_t \rangle$ zwei Algebren mit gleicher Signatur.

1. Eine Abbildung $h : S \to \tilde{S}$ heißt (Algebra-)Isomorphismus von A nach $\tilde{A}$, falls h bijektiv und ein Homomorphismus von A nach $\tilde{A}$ ist.
2. A und $\tilde{A}$ heißen isomorph (symbolisch: $A \simeq \tilde{A}$), falls ein Isomorphismus von A nach $\tilde{A}$ existiert.
3. Gilt $A = \tilde{A}$, so heißt ein Isomorphismus von A nach A Automorphismus auf A.

Beispiele: Folgende Beispiele verdeutlichen die Begriffsbildung.

1. Für $A =_{\text{def}} \langle \mathbb{N}, + \rangle$ und $\tilde{A} =_{\text{def}} \langle \{\, 2n \mid n \in \mathbb{N} \,\}, + \rangle$ ist $h : n \mapsto 2n$ ein Isomorphismus von A nach $\tilde{A}$.
2. Für $A =_{\text{def}} \langle \mathbb{R}_{>0}, \cdot \rangle$ und $\tilde{A} =_{\text{def}} \langle \mathbb{R}, + \rangle$ ist $h : \mathbb{R}_{>0} \to \mathbb{R} : x \mapsto \ln x$ (wegen $\ln(x \cdot y) = \ln x + \ln y$) ein Isomorphismus von A nach $\tilde{A}$.
3. Auf $A =_{\text{def}} \langle \mathbb{Z}_3, +_3 \rangle$ ist durch die Abbildung
$$h : \mathbb{Z}_3 \to \mathbb{Z}_3 : n \mapsto \begin{cases} 0, & \text{falls } n = 0 \\ 2, & \text{falls } n = 1 \\ 1, & \text{falls } n = 2 \end{cases}$$
ein Automorphismus gegeben.
4. Auf $A =_{\text{def}} \langle \mathbb{Z}_5^*, \cdot_5 \rangle$ mit $\mathbb{Z}_5^* =_{\text{def}} \{1, 2, 3, 4\}$ ist durch die Abbildung
$$h : \mathbb{Z}_5^* \to \mathbb{Z}_5^* : n \mapsto \begin{cases} 1, & \text{falls } n = 1 \\ 3, & \text{falls } n = 2 \\ 2, & \text{falls } n = 3 \\ 4, & \text{falls } n = 4 \end{cases}$$
ein Automorphismus gegeben.

Proposition 7.12

Ein Isomorphismus h von $A = \langle S, \circ \rangle$ nach $\tilde{A} = \langle \tilde{S}, \tilde{\circ} \rangle$ bildet neutrale Elemente auf neutrale Elemente und inverse Elemente auf inverse Elemente ab.

Beweis: (nur für Rechtsneutralität) Es sei $e \in S$ rechtsneutral für $\circ$. Dann gilt für $b \in \tilde{S}$
$$b \,\tilde{\circ}\, h(e) = h(h^{-1}(b)) \,\tilde{\circ}\, h(e) = h(h^{-1}(b) \circ e) = h(h^{-1}(b)) = b.$$
Somit ist $h(e)$ ein rechtsneutrales Element von $\tilde{A}$. Damit ist die Proposition bewiesen. ■

Proposition 7.13

Gibt es einen Isomorphismus h von $A = \langle S, \circ \rangle$ nach $\tilde{A} = \langle \tilde{S}, \tilde{\circ} \rangle$, so gibt es einen Isomorphismus $\tilde{h}$ von $\tilde{A} = \langle \tilde{S}, \tilde{\circ} \rangle$ nach $A = \langle S, \circ \rangle$.

Beweis: Wir definieren $\tilde{h} =_{\text{def}} h^{-1}$. Da $h : S \to \tilde{S}$ bijektiv ist, gibt es $\tilde{h} : \tilde{S} \to S$ stets und $\tilde{h}$ ist ebenfalls bijektiv. Weiterhin gilt für $a, b \in \tilde{S}$:

$$\begin{aligned}
\tilde{h}(a \mathbin{\tilde{\circ}} b) &= \tilde{h}(h(h^{-1}(a)) \mathbin{\tilde{\circ}} h(h^{-1}(b))) \\
&= \tilde{h}(h(h^{-1}(a) \circ h^{-1}(b))) \\
&= h^{-1}(h(h^{-1}(a) \circ h^{-1}(b))) \\
&= h^{-1}(a) \circ h^{-1}(b) \\
&= \tilde{h}(a) \circ \tilde{h}(b)
\end{aligned}$$

Somit ist $\tilde{h}$ ein Homomorphismus und mithin ein Isomorphismus. Damit ist die Proposition bewiesen. ■

7.2 Algebrentypen

Wir betrachten die folgenden drei Eigenschaften für eine Algebra $A = \langle S, \circ \rangle$:

- (E1) : Die Verknüpfung $\circ$ ist assoziativ.
- (E2) : Es gibt ein neutrales Element $e \in S$.
- (E3) : Jedes Element $a \in S$ besitzt ein eindeutiges inverses Element.

Natürlich kann für eine Algebra die Eigenschaft (E3) nur gelten, wenn auch (E2) gilt.

Definition 7.14

Es sei $A = \langle S, \circ \rangle$ eine Algebra mit der Verknüpfung $\circ$. Dann wird A einer der folgenden Namen zugewiesen, je nachdem welche der Eigenschaften (E1), (E2) oder (E3) gelten:

Name	(E1)	(E2)	(E3)
Gruppoid (oder Magma)			
Halbgruppe	X		
Monoid	X	X	
Gruppe	X	X	X
Loop		X	X
Gruppoid mit 1		X	

Definition 7.15

Ein Gruppoid $\langle S, \circ \rangle$ heißt abelsch, falls $a \circ b = b \circ a$ für alle $a, b \in S$ gilt, d.h., $\circ$ ist kommutativ.

Beispiele: Wir klassifizieren exemplarisch Algebren gemäß obiger Definition.

1. Die Algebra $A =_{\text{def}} \langle \{a, b\}, \circ \rangle$ mit dem durch die Verknüpfungstabelle

$\circ$	a	b
a	b	a
b	b	b

   gegebenen Operator $\circ$ ist lediglich ein nicht-abelscher Gruppoid, denn $\circ$ ist nicht assoziativ (wegen $(a \circ b) \circ a = a \circ a = b$ und $a \circ (b \circ a) = a \circ b = a$) und A besitzt kein neutrales Element (b ist zwar rechtsneutral aber nicht linksneutral; a ist weder rechts- noch linksneutral). Die Kommutativität gilt ebenfalls nicht für $\circ$ (wegen $a \circ b \neq b \circ a$).

2. $\langle \mathbb{N}_+, + \rangle$ ist eine abelsche Halbgruppe, aber kein Monoid.

3. $\langle \mathbb{N}, + \rangle$ ist ein abelscher Monoid, aber keine Gruppe.

4. $\langle \mathbb{Z}, + \rangle$ ist eine abelsche Gruppe.

5. $\langle \mathbb{Z}, - \rangle$ ist ein nicht-abelscher Gruppoid.

6. $\langle \Sigma^*, \circ \rangle$ ist ein nicht-abelscher Monoid.

7. Die Algebra $A =_{\text{def}} \langle \{e, a, b\}, \circ \rangle$ mit dem durch die Verknüpfungstabelle

$\circ$	e	a	b
e	e	a	b
a	a	e	b
b	b	b	e

   gegebenen Operator $\circ$ ist ein abelscher Loop, denn $\circ$ ist nicht assoziativ (wegen $a \circ (b \circ b) = a \circ e = a$ und $(a \circ b) \circ b = b \circ b = e$), e ist das neutrale Element und jedes Element ist zu sich selbstinvers. Die Kommutativität von $\circ$ folgt aus der Symmetrie der Verknüpfungstabelle entlang der Diagonale von links oben nach rechts unten.

Definition 7.16

Eine Algebra $A = \langle S, +, \cdot \rangle$ der Signatur $(2, 2)$ heißt Ring, falls folgende Bedingungen gelten:

1. $\langle S, + \rangle$ ist eine abelsche Gruppe mit neutralem Element $0 \in S$.

2. $\langle S, \cdot \rangle$ ist ein Monoid mit neutralem Element $1 \in S$.

3. Für alle $a, b, c \in S$ gilt:

$$\begin{aligned} a \cdot (b + c) &= (a \cdot b) + (a \cdot c) \\ (b + c) \cdot a &= (b \cdot a) + (c \cdot a) \end{aligned}$$

   D.h., $+$ und $\cdot$ sind distributiv.

Beispiele: Wir führen einige Beispiele zur die Definition von Ringen an.

1. $\langle \mathbb{Z}, +, \cdot \rangle$ ist ein Ring.

2. $\langle \{\mathsf{f}, \mathsf{w}\}, \oplus, \wedge \rangle$ ist ein Ring.

3. $\langle \{\mathsf{f}, \mathsf{w}\}, \oplus, \vee \rangle$ ist kein Ring, denn die Distributivität gilt nicht.

4. Die univariaten ganzzahligen Polynome bilden einen Ring.

Definition 7.17

Eine Algebra $A = \langle S, +, \cdot \rangle$ der Signatur $(2, 2)$ heißt Körper, falls folgende Bedingungen gelten:

1. $\langle S, + \rangle$ ist eine abelsche Gruppe mit neutralem Element $0 \in S$.
2. $\langle S \setminus \{0\}, \cdot \rangle$ ist eine abelsche Gruppe mit neutralem Element $1 \in S$.
3. Für alle $a, b, c \in S$ gilt

$$\begin{aligned} a \cdot (b + c) &= (a \cdot b) + (a \cdot c) \\ (b + c) \cdot a &= (b \cdot a) + (c \cdot a) \end{aligned}$$

   D.h., $+$ und $\cdot$ sind distributiv.

Beispiele: Wir führen wiederum einige Beispiele zur Definition von Körpern an.

1. $\langle \mathbb{Z}, +, \cdot \rangle$ ist kein Körper.
2. $\langle \{\mathsf{f}, \mathsf{w}\}, \oplus, \wedge \rangle$ ist ein Körper.
3. Die univariaten ganzzahligen Polynome bilden keinen Körper, denn es gibt kein ganzzahliges Polynom $p(x)$ mit $x \cdot p(x) = 1$.
4. $\langle \mathbb{Q}, +, \cdot \rangle$, $\langle \mathbb{R}, +, \cdot \rangle$ und $\langle \mathbb{C}, +, \cdot \rangle$ sind Körper.

Definition 7.18

Eine Algebra $A = \langle S, +, \cdot, \overline{} \rangle$ der Signatur $(2, 2, 1)$ heißt boolesche Algebra, falls folgende Bedingungen gelten:

1. $\langle S, + \rangle$ ist ein abelscher Monoid mit neutralem Element $0 \in S$.
2. $\langle S, \cdot \rangle$ ist ein abelscher Monoid mit neutralem Element $1 \in S$.
3. Für alle $a \in S$ gilt $a + \overline{a} = 1$ und $a \cdot \overline{a} = 0$.
4. Für alle $a, b, c \in S$ gilt:

$$\begin{aligned} a \cdot (b + c) &= (a \cdot b) + (a \cdot c) \\ a + (b \cdot c) &= (a + b) \cdot (a + c) \end{aligned}$$

Beispiele: Wir geben die beiden wichtigsten Beispiele für boolesche Algebren an.

1. $\langle \{\mathsf{f}, \mathsf{w}\}, \vee, \wedge, \neg \rangle$ ist eine boolesche Algebra.
2. $\langle \mathcal{P}(A), \cup, \cap, \overline{} \rangle$ ist eine boolesche Algebra (für beliebiges A).

7.3 Gruppen

Zur Erinnerung: Eine Gruppe $\langle G, \circ \rangle$ ist ein Gruppoid mit den folgenden Eigenschaften:

- (G1) : Die Verknüpfung $\circ$ ist assoziativ auf G.
- (G2) : Es gibt ein neutrales Element $e \in G$.
- (G3) : Für jedes Element $a \in G$ gibt es ein Inverses $a^{-1} \in G$.

Im Folgenden werden wir eine Gruppe $\langle G, \circ \rangle$ mit der Trägermenge G identifizieren.

Theorem 7.19

Es seien G eine Gruppe, $a, b, c \in G$ und $x, y \in G$. Dann gilt:

1. $a = (a^{-1})^{-1}$ — Involutionsregel
2. $a \circ b = c \circ b \iff a = c$ — Kürzungsregeln
   $b \circ a = b \circ c \iff a = c$
3. $a \circ x = b \iff x = a^{-1} \circ b$ — Eindeutige Lösbarkeit linearer Gleichungen
   $x \circ a = b \iff x = b \circ a^{-1}$

Beweis: (Involutionsregel) Wir definieren $b =_{\text{def}} (a^{-1})^{-1}$, d.h., b ist das inverse Element von a^{-1} in G. Dann gilt

$$b = b \circ e = b \circ (a^{-1} \circ a) = (b \circ a^{-1}) \circ a = e \circ a = a$$

Die anderen Regeln sind ähnlich zu beweisen. Damit ist der Satz bewiesen. ■

Wir führen einige Schreib- und Sprechweisen ein für eine Gruppe G, $a \in G$ und $n \in \mathbb{N}$:

$$\begin{aligned} a^0 &=_{\text{def}} e \\ a^n &=_{\text{def}} a \circ a^{n-1} \qquad \text{fr } n \geq 1 \\ a^{-n} &=_{\text{def}} \left(a^{-1}\right)^n \end{aligned}$$

Hierbei heißt a^n die n-te Potenz von a. Zu beachten ist, dass a^{-n} wohldefiniert ist:

$$\left(a^{-1}\right)^n = \left(a^{-1}\right)^n \circ \left(a^n \circ (a^n)^{-1}\right) = \left(\left(a^{-1}\right)^n \circ a^n\right) \circ (a^n)^{-1} = e \circ (a^n)^{-1} = (a^n)^{-1}$$

Im Allgemeinen gelten folgende Rechenregeln für alle $m, n \in \mathbb{Z}$ und $a \in G$:

$$\begin{aligned} a^m \circ a^n &= a^{m+n} \\ (a^n)^m &= a^{m \cdot n} \\ a^m = a^n &\iff a^{m-n} = e \end{aligned}$$

Definition 7.20

Es seien G eine Gruppe und $a \in G$. Die Ordnung $\text{ord}(a)$ von a ist die kleinste Zahl $r \in \mathbb{N}_+$ mit $a^r = e$. Falls kein solches r existiert, dann definieren wir $\text{ord}(a) =_{\text{def}} \infty$.

Beispiele: Für einige Gruppen sollen exemplarisch die Ordnungen angegeben werden.

1. In $\langle \mathbb{Z}, + \rangle$ gilt $\text{ord}(0) = 1$ und $\text{ord}(n) = \infty$ für alle $n \in \mathbb{Z} \setminus \{0\}$.
2. In $\langle \mathbb{Z}_{12}, +_{12} \rangle$ sind die Ordnungen für die Elemente der folgenden Tabelle zu entnehmen:

a	0	1	2	3	4	5	6	7	8	9	10	11
$\text{ord}(a)$	1	12	6	4	3	12	2	12	3	4	6	12

Proposition 7.21

Es sei G eine endliche Gruppe. Dann hat jedes Element in G eine endliche Ordnung.

Beweis: Es sei $a \in G$. Dann sind alle Elemente $a^0, a^1, \ldots, a^{|G|}$ ebenfalls Elemente von G. Da G nur $|G|$ Elemente enthält, sind unter diesen $|G| + 1$ Elementen mindestens zwei gleiche Elemente a^k und a^j mit $k \neq j$. Wir wählen k minimal mit $a^k = a^j$ für $0 \leq j \leq k - 1$. Es gilt $a^{k-j} = e$. Da k minimal ist, muss $j = 0$ gelten. Mithin gilt $a^k = e$ und somit $\text{ord}(a) = k$. Damit ist die Proposition bewiesen. ■

Lemma 7.22

Es seien G eine Gruppe und $a \in G$ mit $\text{ord}(a) < \infty$. Dann gilt:

$$a^k = e \iff \text{ord}(a) | k$$

Beweis: Wir zeigen beide Richtungen einzeln.

$\Rightarrow$: Mit $k = s \cdot \text{ord}(a) + r$ für $r, s \in \mathbb{N}$ mit $0 \leq r < \text{ord}(a)$ folgt:

$$e = a^k = a^{s \cdot \text{ord}(a) + r} = \left(a^{\text{ord}(a)}\right)^s \circ a^r = e^s \circ a^r = e \circ a^r = a^r$$

Wegen $r < \text{ord}(a)$ gilt $r = 0$. Somit gilt $k = s \cdot \text{ord}(a)$ bzw. $\text{ord}(a) | k$.

$\Leftarrow$: Mit $k = s \cdot \text{ord}(a)$ gilt $a^k = (a^{\text{ord}(a)})^s = e^s = e$.

Damit ist das Lemma bewiesen. ■

Lemma 7.23

Es sei G eine abelsche Gruppe. Es seien $a, b \in G$ Elemente endlicher, teilerfremder Ordnung, d.h., $\text{ord}(a), \text{ord}(b) < \infty$ und $\text{ggT}(\text{ord}(a), \text{ord}(b)) = 1$. Dann gilt:

$$\text{ord}(a \circ b) = \text{ord}(a) \cdot \text{ord}(b)$$

Beweis: Da G abelsch ist, gilt:

$$(a \circ b)^{\mathrm{ord}(a)\cdot\mathrm{ord}(b)} = \left(a^{\mathrm{ord}(a)}\right)^{\mathrm{ord}(b)} \circ \left(b^{\mathrm{ord}(b)}\right)^{\mathrm{ord}(a)} = e^{\mathrm{ord}(b)} \circ e^{\mathrm{ord}(a)} = e$$

Nach Lemma 7.22 gilt mithin $\mathrm{ord}(a \circ b) \mid \mathrm{ord}(a) \cdot \mathrm{ord}(b)$. Angenommen $\mathrm{ord}(a \circ b) < \mathrm{ord}(a) \cdot \mathrm{ord}(b)$. Dann gibt es eine Primzahl $p \geq 2$ mit

$$\mathrm{ord}(a \circ b) \;\Big|\; \frac{\mathrm{ord}(a) \cdot \mathrm{ord}(b)}{p}.$$

Da $\mathrm{ord}(a)$ und $\mathrm{ord}(b)$ teilerfremd sind, kann p nur eine der beiden Ordnungen teilen. Ohne Beeinträchtigung der Allgemeinheit gelte $p \mid \mathrm{ord}(a)$. Somit folgt

$$e = (a \circ b)^{\frac{\mathrm{ord}(a)\cdot\mathrm{ord}(b)}{p}} = a^{\frac{\mathrm{ord}(a)\cdot\mathrm{ord}(b)}{p}} \circ \left(b^{\mathrm{ord}(b)}\right)^{\frac{\mathrm{ord}(a)}{p}} = a^{\frac{\mathrm{ord}(a)\cdot\mathrm{ord}(b)}{p}}$$

und mithin gilt nach Lemma 7.22 auch

$$\mathrm{ord}(a) \;\Big|\; \frac{\mathrm{ord}(a) \cdot \mathrm{ord}(b)}{p}$$

Wegen $p \nmid \mathrm{ord}(b)$ folgt:

$$\mathrm{ord}(a) \;\Big|\; \frac{\mathrm{ord}(a)}{p}$$

Dies ist ein Widerspruch. Somit gilt $\mathrm{ord}(a \circ b) = \mathrm{ord}(a) \cdot \mathrm{ord}(b)$ und das Lemma ist bewiesen. ■

Lemma 7.24

Es seien G eine endliche, abelsche Gruppe und $a \in G$ ein Element maximaler Ordnung, d.h. $\mathrm{ord}(a) = \max\{\mathrm{ord}(b) | b \in G\}$. Dann gilt $\mathrm{ord}(b) | \mathrm{ord}(a)$ für alle $b \in G$.

Beweis: Zum Beweis mittels Widerspruch nehmen wir an, dass b ein Element in G mit $\mathrm{ord}(b) \nmid \mathrm{ord}(a)$ ist. Dann gibt es eine Primzahl $p \geq 2$ mit:

$$p^i \mid \mathrm{ord}(a), \qquad p^{i+1} \nmid \mathrm{ord}(a), \qquad p^{i+1} \mid \mathrm{ord}(b)$$

Wir definieren $a' =_{\mathrm{def}} a^{p^i}$ und $b' =_{\mathrm{def}} b^{\frac{\mathrm{ord}(b)}{p^{i+1}}}$ und bestimmen die Ordnungen von a' und b':

$$\mathrm{ord}(a') = \frac{\mathrm{ord}(a)}{p^i}, \qquad \text{denn} \quad (a')^{\frac{\mathrm{ord}(a)}{p^i}} = \left(a^{p^i}\right)^{\frac{\mathrm{ord}(a)}{p^i}} = a^{\mathrm{ord}(a)} = e$$

$$\mathrm{ord}(b') = p^{i+1}, \qquad \text{denn} \quad (b')^{p^{i+1}} = \left(b^{\frac{\mathrm{ord}(b)}{p^{i+1}}}\right)^{p^{i+1}} = b^{\mathrm{ord}(b)} = e$$

Da $p^{i+1} \nmid \mathrm{ord}(a)$ sind $\frac{\mathrm{ord}(a)}{p^i}$ und p^{i+1} teilerfremd. Somit folgt aus Lemma 7.23

$$\mathrm{ord}(a' \circ b') = \mathrm{ord}(a') \cdot \mathrm{ord}(b') = p \cdot \mathrm{ord}(a) > \mathrm{ord}(a).$$

Dies ist ein Widerspruch zur Maximalität der Ordnung von a und das Lemma ist bewiesen. ■

Definition 7.25

Eine Unteralgebra $\langle H, \circ \rangle$ einer Gruppe $\langle G, \circ \rangle$ heißt Untergruppe von G, falls $\langle H, \circ \rangle$ eine Gruppe ist.

Proposition 7.26

Es seien G eine Gruppe und H eine Untergruppe von G. Dann sind die neutralen Elemente von G und H identisch.

Beweis: Es seien e_H ein neutrales Element von H und e_G ein neutrales Element von G. Es gilt $e_H \circ e_H = e_H$ und $e_G \circ e_H = e_H$, d.h., $e_H \circ e_H = e_G \circ e_H$. Nach der Kürzungsregel für G gilt $e_H = e_G$. ■

Proposition 7.27

Jede Unteralgebra einer endlichen Gruppe ist eine Untergruppe.

Beweis: Es sei $\langle H, \circ \rangle$ ein Unteralgebra der endlichen Gruppe $\langle G, \circ \rangle$. Die Assoziativität überträgt sich von H auf G. Für die Existenz des neutralen Elementes und der inversen Elemente sei $b \in H$. Da H abgeschlossen ist unter $\circ$, gilt $b^n \in H$ für alle $n \in \mathbb{N}$. Nach Proposition 7.21 hat b eine endliche Ordnung in G. Definiere $m =_{\text{def}} \text{ord}(b)$. Dann gilt $e = b^m \in H$ und $e = b \circ b^{m-1}$. Somit gehört das neutrale Element e zu H und b^{m-1} ist das inverse Element zu b. ■

Korollar 7.28

Ist G eine endliche Gruppe und sind H und K Untergruppen von G, so ist $H \cap K$ eine Untergruppe von G.

Beweis: $H \cap K$ ist abgeschlossen unter den Gruppenoperationen. ■

Korollar 7.29

Es seien G eine endliche Gruppe und $a \in G$ ein beliebiges Element. Dann ist $S_a =_{\text{def}} \left\{ e, a, a^2, \ldots, a^{\text{ord}(a)-1} \right\}$ die kleinste Untergruppe von G, die a enthält.

Beweis: S_a ist abgeschlossen unter den Gruppenoperationen. Jede Unteralgebra, die a enthält, muss auch a^n für $n \in \mathbb{N}$ enthalten. ■

Definition 7.30

Eine Gruppe G heißt zyklisch, falls es ein $b \in G$ gibt mit $G = \{b^i | i \in \mathbb{Z}\}$. Das Element b heißt erzeugendes Element (bzw. Generator) von G.

Beispiele: Die wesentlichen zyklischen Gruppen sind die folgenden:

1. $\langle \mathbb{Z}, + \rangle$ ist zyklisch mit 1 als erzeugendem Element.
2. $\langle \mathbb{Z}_n, +_n \rangle$ ist zyklisch mit 1 als erzeugendem Element.

Korollar 7.31

Für eine endliche, zyklische Gruppe G mit dem Generator $b \in G$ gilt $|G| = \text{ord}(b)$.

Theorem 7.32

Es sei G eine zyklische Gruppe.

1. Ist $|G| = \infty$, so ist G isomorph zu $\langle \mathbb{Z}, + \rangle$.
2. Ist $|G| = m < \infty$, so ist G isomorph zu $\langle \mathbb{Z}_m, +_m \rangle$.

Beweis: (nur endliche Gruppen) Es sei G zyklisch mit erzeugendem Element b und endlich, d.h., $|G| = m$ für $m \in \mathbb{N}_+$. Somit ist $G = \{ b^i \mid i \in \{0, 1, \ldots, m-1\} \}$ mit $\text{ord}(b) = m$. Wir definieren die folgende Abbildung:

$$h : \mathbb{Z}_m \to G : i \mapsto b^i$$

Dann ist h bijektiv (wegen $|\mathbb{Z}_m| = |G|$) und es gilt:

$$\begin{aligned} h(i) \circ h(j) &= b^i \circ b^j \\ &= b^{i+j} \\ &= b^{s \cdot m + \text{mod}(i+j,m)} \\ &= e^s \circ b^{\text{mod}(i+j,m)} \\ &= b^{\text{mod}(i+j,m)} \\ &= b^{i +_m j} \\ &= h(i +_m j) \end{aligned}$$

Damit ist das Theorem bewiesen. ■

Beispiel: $\langle \mathbb{Z}_5^*, \cdot_5 \rangle$ ist eine zyklische Gruppe mit erzeugendem Element 2:

$$\{2^0, 2^1, 2^2, 2^3\} = \{1, 2, 4, 3\}$$

Somit gilt $\langle \mathbb{Z}_5^*, \cdot_5 \rangle \cong \langle \mathbb{Z}_4, +_4 \rangle$ mittels der Abbildung:

$$0 \mapsto 1, \qquad 1 \mapsto 2, \qquad 2 \mapsto 4, \qquad 3 \mapsto 3$$

Die eulersche Phi-Funktion $\varphi : \mathbb{N}_+ \to \mathbb{N}_+$ ist definiert als:

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

Mit anderen Worten: $\varphi(n)$ ist die Anzahl der zu n teilerfremden Zahlen.

Lemma 7.33 (Lagrange)

Es sei G eine endliche Gruppe mit $|G| = n$. Dann gilt $\text{ord}(a)|n$ für alle Elemente $a \in G$.

Beweis: Für $a \in G$ betrachten wir die Untergruppe $S_a =_{\text{def}} \{e, a, a^2, \ldots, a^{\text{ord}(a)-1}\}$. Es gilt $|S_a| = \text{ord}(a)$. Weiter definieren für $x \in G$ die Menge (eine sogenannte Linksnebenklasse)

$$xS_a =_{\text{def}} \{ x \circ z \mid z \in S_a \}.$$

Nach den Kürzungsregeln in Gruppen gilt $|xS_a| = |S_a|$ (denn: $x \circ z = x \circ z' \Leftrightarrow z = z'$). Es gelte nun $xS_a \cap yS_a \neq \emptyset$, d.h., es gibt $z \in xS_a \cap yS_a$. Dann gibt es $z', z'' \in S_a$ mit $x \circ z' = z = y \circ z''$. Da S_a eine Gruppe ist, gilt $x = y \circ z'' \circ z'^{-1} \in yS_a$, d.h., $xS_a \subseteq yS_a$. Analog ergibt sich $yS_a \subseteq xS_a$, also $xS_a = yS_a$. Mithin sind zwei Mengen xS_a und yS_a entweder disjunkt oder identisch. Somit gibt es $x_1, \ldots, x_k \in G$ mit $x_iS_a \cap x_jS_a = \emptyset$ für $i \neq j$ und

$$G = \bigcup_{j=1}^{k} x_jS_a;$$

folglich gilt:

$$n = |G| = \sum_{j=1}^{k} |x_jS_a| = \sum_{j=1}^{k} |S_a| = k \cdot |S_a| = k \cdot \text{ord}(a),$$

d.h. $\text{ord}(a) \mid n$. Damit ist das Lemma bewiesen. ■

Theorem 7.34 (Euler)

Für alle $n \in \mathbb{N}$ mit $n \geq 2$ und für alle $a \in \mathbb{Z}_n^*$ gilt

$$\text{mod}(a^{\varphi(n)}, n) = 1.$$

Beweis: Es sei $a \in \mathbb{Z}_n^*$ mit $k =_{\text{def}} \text{ord}(a)$. Nach Lemma 7.33 gilt $k|\varphi(n)$ und wir erhalten

$$\text{mod}(a^{\varphi(n)}, n) = \text{mod}(a^{k \cdot \frac{\varphi(n)}{k}}, n) = \text{mod}(1^{\frac{\varphi(n)}{k}}, n) = 1.$$

Damit ist das Theorem bewiesen. ■

Theorem 7.35 (Fermat)

Für alle $n \in \mathbb{N}$ mit $n \geq 2$ gilt:

$$n \text{ ist eine Primzahl} \iff \text{mod}(a^{n-1}, n) = 1 \text{ für alle } a \in \mathbb{Z}_n \setminus \{0\}$$

Beweis: Wir zeigen beide Richtungen einzeln.

$\Rightarrow$: Es sei n eine Primzahl. Dann gilt $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{0\}$ und $\varphi(n) = n - 1$. Nach Theorem 7.34 gilt somit $\text{mod}(a^{n-1}, n) = 1$ für alle $a \in \mathbb{Z}_n \setminus \{0\}$.

$\Leftarrow$: Es sei $1 \leq p < n$ ein Teiler von n. Wir wollen zeigen, dass $p = 1$ gilt. Nach Voraussetzung gilt $\text{mod}(p^{n-1}, n) = 1$ und folglich $p^{n-1} - 1 = k \cdot n = k \cdot k' \cdot p$ für geeignete $k, k' \in \mathbb{Z}$. Damit p sowohl p^{n-1} als auch 1 teilt, muss $p = 1$ gelten. Somit besitzt n keine von 1 verschiedenen Teiler. Mithin ist n eine Primzahl.

Damit ist das Theorem bewiesen. ■

7.4 Endliche Körper

Zur Erinnerung: Ein Körper $K = \langle K, +, \cdot \rangle$ ist eine Algebra mit:

- (K1) : $\langle K, + \rangle$ ist eine abelsche Gruppe mit dem neutralen Element 0, wobei inverse Elemente mit $-a$ für $a \in S$ bezeichnet werden.
- (K2) : $\langle K \setminus \{0\}, \cdot \rangle$ ist eine abelsche Gruppe mit dem neutralen Element 1, wobei inverse Elemente mit a^{-1} für $a \in S \setminus \{0\}$ bezeichnet werden.
- (K3) : Es gelten die Distributivgesetze für alle $a, b, c \in K$:

$$\begin{aligned} a \cdot (b + c) &= (a \cdot b) + (a \cdot c) \\ (b + c) \cdot a &= (b \cdot a) + (c \cdot a) \end{aligned}$$

Wie im Falle von Gruppen identifizieren wir einen Körper mit seiner Trägermenge K.

Beispiele: Wir geben nochmals einige Beispiele für Körper an.

1. $\mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ (mit den üblichen Operationen) sind Körper.
2. $\langle \mathbb{Z}_2, +_2, \cdot_2 \rangle$ ist ein Körper.
3. $\langle \mathbb{Z}_4, +_4, \cdot_4 \rangle$ ist kein Körper, denn: $2 \cdot_4 2 = 0 \notin \mathbb{Z}_4 \setminus \{0\}$

Proposition 7.36

In jedem Körper K gilt für alle $a \in K$:

$$a \cdot 0 = 0 \cdot a = 0$$

Beweis: Es sei $a \in K$. Aus den Distributivgesetzen erhalten wir:

$$0 + (a \cdot 0) = a \cdot 0 = a \cdot (0 + 0) = (a \cdot 0) + (a \cdot 0)$$
$$0 + (0 \cdot a) = 0 \cdot a = (0 + 0) \cdot a = (0 \cdot a) + (0 \cdot a)$$

Mit Hilfe der Kürzungsregeln für Gruppen folgt $0 = a \cdot 0 = 0 \cdot a$. Damit ist die Proposition bwiesen. ■

Proposition 7.37

In jedem Körper K gilt für alle $a, b \in K$:

$$a \cdot b = 0 \quad \Longrightarrow \quad a = 0 \text{ oder } b = 0$$

(Wir sagen auch: Körper sind nullteilerfrei.)

Beweis: Es gelte $a \cdot b = 0$. Wir unterscheiden zwei Fälle:

- 1. Fall: Es sei $a = 0$. Dann gilt die Aussage.
- 2. Fall: Es sei $a \neq 0$. Dann gibt es ein multiplikatives Inverse $a^{-1} \in K \setminus \{0\}$. Somit gilt nach Voraussetzung und Proposition 7.36:

$$b = 1 \cdot b = a^{-1} \cdot a \cdot b = a^{-1} \cdot 0 = 0$$

Damit ist die Proposition bewiesen. ■

Theorem 7.38

Für alle $n \in \mathbb{N}$ mit $n \geq 2$ gilt:

$$\langle \mathbb{Z}_n, +_n, \cdot_n \rangle \text{ ist ein Körper} \quad \Longleftrightarrow \quad n \text{ ist eine Primzahl}$$

Beweis: $\langle \mathbb{Z}_n, +_n \rangle$ ist für alle $n \geq 2$ eine abelsche Gruppe; die Distributivgesetze gelten offensichtlich. Wir müssen noch zeigen, wann $\langle \mathbb{Z}_n \setminus \{0\}, \cdot_n \rangle$ eine (abelsche) Gruppe ist.

$\Leftarrow$: Ist n eine Primzahl, so gilt $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{0\}$. Somit ist $\langle \mathbb{Z} \setminus \{0\}, \cdot_n \rangle$ eine Gruppe.

$\Rightarrow$: Wir zeigen die Kontraposition. Es sei n also keine Primzahl. Somit gibt es ein $a \in \mathbb{Z} \setminus \{0\}$ mit $\mathrm{ggT}(a, n) > 1$, d.h., $a \notin \mathbb{Z}_n^*$. Es sei $a \in \mathbb{Z} \setminus \{0\}$ minimal mit $\mathrm{ggT}(a, n) > 1$. Dann gilt $a|n$. Es gibt somit $b \in \mathbb{Z} \setminus \{0\}$ mit $a \cdot b = n$ bzw. $a \cdot_n b = 0$. Somit ist $\langle \mathbb{Z}_n \setminus \{0\}, \cdot_n \rangle$ kein Gruppoid, also auch keine Gruppe.

Damit ist das Theorem bewiesen. ■

Für einen Körper K bezeichnen wir mit $K^* =_{\text{def}} K \setminus \{0\}$ die multiplikative Gruppe.

Theorem 7.39

In jedem endlichen Körper K ist die multiplikative Gruppe K^* zyklisch.

Beweis: Mit K ist auch K^* endlich. Somit besitzt jedes Element von K^* eine endliche Ordnung in der Gruppe K^*. Es sei $a \in K^*$ ein Element maximaler Ordnung. Wir müssen zeigen, dass $\mathrm{ord}(a) = |K^*|$ gilt. Dazu betrachten wir das Polynom

$$p(x) =_{\text{def}} x^{\mathrm{ord}(a)} - 1.$$

Wir können nun wie folgt argumentieren:

1. Der Grad von p ist $\mathrm{ord}(a)$.
2. Für alle $b \in K^*$ gilt $\mathrm{ord}(b)|\mathrm{ord}(a)$.
3. Für alle $b \in K^*$ gilt $b^{\mathrm{ord}(a)} = 1$, d.h., alle $b \in K^*$ sind Nullstellen von p.
4. Ein Polynom vom Grad $\mathrm{ord}(a)$ hat höchstens $\mathrm{ord}(a)$ Nullstellen, d.h., $\mathrm{ord}(a) \geq |K^*|$.

Damit folgt $\mathrm{ord}(a) = |K^*|$ und das Theorem ist bewiesen. ■

Theorem 7.40

Für $n \in \mathbb{N}$ mit $n \geq 2$ gibt es genau dann einen Körper mit $|K| = n$ Elementen, wenn $n = p^k$ für eine geeignete Primzahl p sowie ein geeignetes $k \in \mathbb{N}$ gilt. Sind K_1 und K_2 endliche Körper mit $|K_1| = |K_2|$, so gilt $K_1 \cong K_2$.

Der nach diesem Theorem (bis auf Isomorphie) eindeutige endliche Körper mit p^k Elementen heißt Galoiskörper und wird mit $\mathrm{GF}(p^k)$ bezeichnet.

Beispiel: Wir wollen den $\mathrm{GF}(4)$ konstruieren. Wie wir bereits wissen, ist $\langle \mathbb{Z}_4, +_4, \cdot_4 \rangle$ kein Körper. Wir definieren also $K =_{\text{def}} \{0, 1, a, b\}$, wobei 0 das additive neutrale Element und 1 das multiplikative neutrale Element sind.

Zunächst legen wir die Multiplikation fest. Die zugehörige Verknüpfungstabelle erhalten wir durch Wahl von a als erzeugendes Element (mit $a^2 = b$ und $a^3 = 1$):

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Durch die Multiplikation ergibt sich eine Verknüpfungstabelle für die Addition:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

Die Einträge lassen sich wie folgt begründen:

- Die Einträge für das Nullelement 0 sind eindeutig festgelegt.
- Die Einträge für a ermitteln wir wie folgt:
  - $a+1 \neq 1$, denn aus $a+1=1$ folgt $a=0$.
  - $a+1 \neq a$, denn aus $a+1=a$ folgt $1=0$.
  - $a+1 \neq 0$, denn aus $a+1=0$ folgt $0=a+a^3=a\cdot(1+a^2)=a\cdot(1+b)$ (wegen der Distributivgesetze), d.h., $1+b=0$ (wegen der Nullteilerfreiheit) und folglich $1+a=1+b$ bzw. $a=b$.

  Somit gilt $a+1=b$ und folglich $a+b=a+a^2=a\cdot(1+a)=a\cdot b=1$.
- Die inversen Elemente werden eindeutig aufgeteilt.

Literaturverzeichnis

Ch. Meinel, M. Mundhenk: *Mathematische Grundlagen der Informatik. Mathematisches Denken und Beweisen. Eine Einführung*. 3., überarbeitete und erweiterte Auflage. B. G. Teubner Verlag, Wiesbaden, 2006.

A. Steger: *Diskrete Strukturen. Band 1: Kombinatorik-Graphentheorie-Algebra*. 2. Auflage. Springer-Verlag, Berlin, 2007.
`https://doi.org/10.1007/978-3-540-46664-2`

R. L. Graham, D. E. Knuth, O. Patashnik: *Concrete Mathematics: A Foundation for Computer Science.* 2. Auflage, Addison-Wesley, Reading, MA, 1994.

D. E. Knuth: *The Art of Computer Programming*, Band 1: *Fundamental Algorithms*. 3. Auflage, Addison-Wesley, Reading, MA, 1997.

D. Makinson: *Sets, Logic and Maths for Computing*. Undergraduate Topics in Computer Science. 2. Auflage. Springer-Verlag, London, 2012.
`https://doi.org/10.1007/978-1-4471-2500-6`