Mitschrieb der Vorlesung

Mathematik 1 für Informatiker und Bioinformatiker

Prof. Dr. Peter Hauck

Wintersemester 2006/2007*

Mitschrieb in LaTeXvon
Rouven Walter

*Letzte Änderung: 10. Oktober 2010

Lizenz

Vorwort

Dieser Mitschrieb entstand während meiner Nachbearbeitung zur Vorlesung „Mathematik 1 für Informatiker und Bioinformatiker“ im Wintersemester 2006/2007 bei Prof. Dr. Peter Hauck an der Eberhard-Karls-Universität Tübingen. Der Mitschrieb wurde im Laufe der Zeit um kleinere und größere Bemerkungen von mir abgeändert, um die Verständlichkeit des Inhaltes zu fördern. Die ursprüngliche Nummerierung der Abschnitte wurde jedoch beibehalten.

Ich erhebe keinen Anspruch auf Vollständigkeit oder Richtigkeit. Bei Verständnisschwierigkeiten zum Inhalt empfehle ich daher ausdrücklich, sich an die jeweiligen Dozenten/Tutoren zu wenden.

Wer Fehler findet, Verbesserungsvorschläge hat oder mir sonstige Anregungen mitteilen möchte, kann mir gerne eine E-Mail an folgende Adresse schicken:
rouvenwalter@web.de oder kontakt@rouvenwalter.de

Inhaltsverzeichnis

1 Mathematisches Argumentieren

In diesem einführenden Kapitel werden wir zunächst eine Einführung in die Aussagenlogik und Quantorenlogik geben. Mit diesen Mitteln können wir mathematische Aussagen formalisieren. Weiter zeigen wir grundlegende Techniken, um diese mathematischen Aussagen zu beweisen.

Beispiel:

Man betrachte einen Chip mit 200 Millionen Transistoren (Schaltern). Dabei kann jeder Schalter zwei Zustände annehmen: „offen“ oder „geschlossen“. Das sind $2^{200000000}$ mögliche Zustände des Chips.
Zur Überprüfung der Funktionsweise des Chips ist man an Aussagen vom folgenden Typ interessiert: Wenn T_1 oder T_2 offen sind, dann ist T_3 offen und T_4 geschlossen.

Durch sogenannte *logische Junktoren* werden aus einfachen Aussagen neue (kompliziertere) Aussagen gebildet.

Aussagen werden durch *Wahrheitswerte* bestimmt:

„wahr“	„falsch“
w	f
1	0

(Eine präzise Beschreibung der Junktoren gibt es in der *Junktorenlogik*)

Definition 1.1. *(Negation) Verneinung einer Aussage A: „nicht A“*

$$\underbrace{\neg A}_{\text{Neue Aussage}} \qquad \text{oder} \qquad \overline{A}$$

A	$\neg A$
1	0
0	1

Hat die Aussage A den W-Wert (Wahrheitswert) x, so hat $\neg A$ den Wahrheitswert $1 - x$.

Definition 1.2. *(Konjunktion) Seien A und B Aussagen. Die neue Aussage $A \wedge B$ bzw. „A und B“ heißt* Konjunktion *von A und B.*

A	B	$A \wedge B$
1	1	1
1	0	0
0	1	0
0	0	0

Hat die Aussage A den Wahrheitswert x und B den Wahrheitswert y, so hat die Konjunktion $A \wedge B$ den Wahrheitswert $x \cdot y$ bzw. $min(x, y)$.

Definition 1.3. *Seien A und B Aussagen. Die neue Aussage $A \vee B$ bzw. „A oder B“ heißt* Disjunktion *von A und B.*
Bei der Aussage $A \vee B$ handelt es sich um das einschließende Oder*. Sie ist wahr, wenn mindestens eine der beiden Aussagen oder* beide *Aussagen wahr sind.*

A	B	$A \vee B$
1	1	1
1	0	1
0	1	1
0	0	0

Hat die Aussage A den Wahrheitswert x und B den Wahrheitswert y, so hat die Aussage $A \vee B$ den Wahrheitswert $max(x, y)$ bzw. $x + y - x \cdot y$.

Definition 1.4. *(Exklusives Oder) Seien A und B Aussagen. Die neue Aussage A XOR B bzw. „entweder A oder B“ ist das* exklusive Oder*, bezeichnet mit* XOR *(exclusive or).*
Bei der Aussage A XOR B handelt es sich um das ausschließende Oder*. Sie wahr, wenn eine der beiden Aussagen wahr ist. Sie ist aber falsch, wenn beide Aussagen A und B gleichzeitig wahr oder falsch sind.*

A	B	A XOR B
1	1	0
1	0	1
0	1	1
0	0	0

Hat die Aussage A den Wahrheitswert x und B den Wahrheitswert y, so hat A XOR B den Wahrheitswert $max(x, y) - x \cdot y$ bzw. $x + y - 2 \cdot x \cdot y$.

Beispiel 1.5. *a) Seien A und B Aussagen. Die zusammengesetzte Aussage $(A \vee B) \wedge (\neg(A \wedge B))$ in der Wahrheitswertetabelle:*

A	B	$A \vee B$	$A \wedge B$	$\neg(A \wedge B)$	$(A \vee B) \wedge (\neg(A \wedge B))$
1	1	1	1	0	0
1	0	1	0	1	1
0	1	1	0	1	1
0	0	0	0	1	0

Es stellt sich heraus, dass A XOR B *und* $(A \vee B) \wedge (\neg(A \wedge B))$ logisch äquivalent *sind.*

b) *Die Aussagen* $A \vee B$ *und* $B \vee A$ *sind logisch äquivalent.*
Die Aussagen $A \wedge B$ *und* $B \wedge A$ *sind logisch äquivalent.*
Die Aussagen A XOR B *und* B XOR A *sind logisch äquivalent.*

c) *Die Aussage* $(A \wedge (\neg B)) \vee (B \text{ XOR } C)$ *in der Wahrheitswertetabelle:*

A	B	C	$\neg B$	$(A \wedge (\neg B))$	$(B$ XOR $C)$	$(A \wedge (\neg B)) \vee (B$ XOR $C)$
1	1	1	0	0	0	0
1	1	0	0	0	1	1
1	0	1	1	1	1	1
1	0	0	1	1	0	1
0	1	1	0	0	0	0
0	1	0	0	0	1	1
0	0	1	1	0	1	1
0	0	0	1	0	0	0

Die Aussagen A, B *und* C *könnten beispielsweise für folgendes stehen:*

$$\begin{aligned} A &= \textit{Schalter } T_1 \textit{ ist offen} \\ B &= \textit{Schalter } T_2 \textit{ ist offen} \\ C &= \textit{Schalter } T_3 \textit{ ist offen} \end{aligned}$$

Angenommen man weiß, dass obige Aussage wahr ist und außerdem, dass genau 2 Schalter offen sind. Dann ist T_1 *offen.*

d) *Die Aussage* $(A \wedge B) \wedge C$ *ist logisch äquivalent zu* $A \wedge (B \wedge C)$.
Die Aussage $(A \vee B) \vee C$ *ist logisch äquivalent zu* $A \vee (B \vee C)$.

Man schreibt daher: $A \wedge B \wedge C$ *bzw.* $A \vee B \vee C$.

$A \wedge B \wedge C$ *ist wahr, genau dann wenn alle Aussagen* A, B, C *wahr sind.*
$A \vee B \vee C$ *ist wahr, genau dann wenn mindestens eine Aussage von* A, B, C *wahr ist.*

e) *Wieviele Zeilen hat die Wahrheitstabelle für eine Aussage mit 2 Elementaussagen?*
$2^2 = 4$ *Zeilen.*
3 Elementaussagen: $2^3 = 8$ *Zeilen.*
100 Elementaussagen: $2^{100} \approx 2 \cdot 10^{30}$ *Zeilen.*

Angenommen, man benötigt 1 Sekunde zum Schreiben einer Zeile, dann benötigt man bei 100 Elementaussagen $2 \cdot 10^{30} \approx 6 \cdot 10^{22}$ *Jahre für die gesamte Tabelle.*

Definition 1.6. *Seien A und B Aussagen. Wir definieren die neue Aussage „wenn, dann“, $A \Rightarrow B$, „Wenn A gilt, dann gilt B“, „A impliziert B“ bzw. „aus A folgt B“.*

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

e.f.q. *(*ex falso quodlibet*) (lateinisch: aus Falschem folgt Beliebiges)*

Für $A \Rightarrow B$ sagt man auch „A ist hinreichend für B“ oder „B ist notwendig für A“.

Beispiel:

a) *Wenn eine natürliche Zahl n durch 4 teilbar ist, dann ist sie auch durch 2 teilbar (wahr).*
Teilbarkeit durch 4 ist hinreichend für Teilbarkeit durch 2 (wahr).
Teilbarkeit durch 2 ist notwendig für Teilbarkeit durch 4 (wahr).
Teilbarkeit durch 4 ist notwendig für Teilbarkeit durch 2 (falsch).

Man beachte aber, dass die Aussage $A \Rightarrow B$ nicht logisch äquivalent zu $B \Rightarrow A$ ist:

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

b) *Sei $A_i =$ „T_i ist offen“ für $i = 1, 2, 3, 4$. Wann ist die Aussage $(A_1 \vee A_2) \Rightarrow (A_3 \wedge \neg A_4)$ falsch? Wenn $(A_1 \vee A_2)$ wahr ist und $(A_3 \wedge \neg A_4)$ falsch ist. Das bedeutet, mindestens einer von T_1 und T_2 ist offen und T_3 ist geschlossen oder T_4 ist offen.*

Definition 1.7. *Seien A und B Aussagen. Wir definieren die neue Aussage $A \Leftrightarrow B$, „genau dann, wenn“, „dann und nur dann“, „if and only if (iff)“, „A gilt genau dann, wenn B gilt“, „A ist äquivalent zu B“.*

A	B	$A \Leftrightarrow B$
1	1	1
1	0	0
0	1	0
0	0	1

Satz 1.8. *(Wichtige logische Äquivalenzen)*

a) $\neg(\neg A)$ *ist logisch äquivalent zu* A *(doppelte Negation).*
Man schreibt: $\neg\neg A$ *statt* $\neg(\neg A)$*.*

b) $\neg(A \wedge B)$ *ist logisch äquivalent zu* $(\neg A) \vee (\neg B)$ *(Verneinung der Konjunktion).*

c) $\neg(A \vee B)$ *ist logisch äquivalent zu* $(\neg A) \wedge (\neg B)$ *(Verneinung der Disjunktion).*

d) $A \Rightarrow B$ *ist logisch äquivalent zu* $(\neg B) \Rightarrow (\neg A)$
$A \Rightarrow B$ *ist logisch äquivalent zu* $(\neg A \vee B)$

e) $A \Leftrightarrow B$ *ist logisch äquivalent zu* $(A \Rightarrow B) \wedge (B \Rightarrow A)$

Beweis. Beweis erfolgt jeweils mit Hilfe der Wahrheitstabelle.

a)

A	$\neg A$	$\neg(\neg A)$
1	0	1
0	1	0

b)

A	B	$\neg A$	$\neg B$	$A \wedge B$	$\neg(A \wedge B)$	$(\neg A) \vee (\neg B)$
1	1	0	0	1	0	0
1	0	0	1	0	1	1
0	1	1	0	0	1	1
0	0	1	1	0	1	1

c)

A	B	$\neg A$	$\neg B$	$A \vee B$	$\neg(A \vee B)$	$(\neg A) \wedge (\neg B)$
1	1	0	0	1	0	0
1	0	0	1	1	0	0
0	1	1	0	1	0	0
0	0	1	1	0	1	1

d)

A	B	$\neg A$	$\neg B$	$A \Rightarrow B$	$(\neg B) \Rightarrow (\neg A)$	$\neg A \vee B$
1	1	0	0	1	1	1
1	0	0	1	0	0	0
0	1	1	0	1	1	1
0	0	1	1	1	1	1

e)

A	B	$A \Rightarrow B$	$B \Rightarrow A$	$A \Leftrightarrow B$	$(A \Rightarrow B) \wedge (B \Rightarrow A)$
1	1	1	1	1	1
1	0	0	1	0	0
0	1	1	0	0	0
0	0	1	1	1	1

□

Bemerkung 1.9. *Die Aussagen in 1.8 b) c) sind die* De Morgan'schen Regeln.

In der Aussagenlogik ist nur der Wahrheitswert von Aussagen interessant. Der nächste Schritt ist eine etwas genauere Betrachtung gewisser Typen von Aussagen.

All- und Existenzaussagen (Prädikatenlogik):

Beispiel:

Sprachliche Beschreibung:

a) Für alle natürlichen Zahlen n gilt: n ist gerade oder n ist ungerade.
(Allaussage, wahre Aussage)

b) Es gibt (mindestens) eine natürliche Zahl, die durch 3 und 7 teilbar ist.
(Existenzaussage, wahre Aussage)

c) Es gibt eine natürliche Zahl, die durch 9, aber nicht durch 3 teilbar ist.
(Existenzaussage, falsche Aussage)

Formale Beschreibung:

a) $\forall n \in \mathbb{N} : (n \text{ ist gerade}) \vee (n \text{ ist ungerade})$

b) $\exists n \in \mathbb{N} : (n \text{ ist durch 3 teilbar}) \wedge (n \text{ ist durch 7 teilbar})$

c) $\exists n \in \mathbb{N} : (n \text{ ist durch 9 teilbar}) \wedge \neg(n \text{ ist durch 3 teilbar})$

Allgemein:

$\forall x \in E : P(x)$ Aussage, Allaussage
„Für alle x aus der Menge E gilt die Eigenschaft $P(x)$."

$\exists x \in E : Q(x)$ Aussage, Existensaussage
„Es gibt (mindestens) ein x aus der Menge E, das die Eigenschaft $Q(x)$ hat."

$\in$: „Element von"
E : Menge
$P(x)$, $Q(x)$: Eigenschaft, die x haben kann oder nicht (*Prädikat*)

Die Aussage $\forall x \in E : P(x)$ ist wahr genau dann, wenn alle $P(x)$ (für sämtliche $x \in E$) wahr sind.
Die Aussage $\exists x \in E : Q(x)$ ist wahr genau dann, wenn $Q(x)$ für mindestens ein $x \in E$ wahr ist.

Beispiel:

a) Sei $E = \{2, 4, 6\}$. $\forall x \in E : x$ ist gerade (wahre Aussage).
Die Aussage ist logisch äquivalent mit (2 ist gerade)$\wedge$(4 ist gerade)$\wedge$(6 ist gerade).

b) Ist $E = \{x_1, \ldots, x_n\}$ eine endliche Menge, dann ist die Aussage $\forall x \in E : P(x)$ logisch äquivalent zu $P(x_1) \wedge P(x_2) \wedge P(x_3) \wedge \ldots \wedge P(x_n)$.

Da E auch unendlich sein kann, nennt man Allaussagen auch *verallgemeinerte Konjunktionen*.

c) Sei $E = \{2, 4, 6\}$. $\exists x \in E : x > 7$ (falsche Aussage).
Die Aussage ist logisch äquivalent mit $(2 > 7) \vee (4 > 7) \vee (6 > 7)$.

d) Ist $E = \{x_1, \ldots, x_n\}$ eine endliche Menge, dann ist die Aussage $\exists x \in E : Q(x)$ logisch äquivalent zu $Q(x_1) \vee Q(x_2) \vee \ldots \vee Q(x_n)$.

Existenzaussagen sind *verallgemeinerte Disjunktionen*.

All- und Existenzquantor:

$\forall$	*Allquantor*	$\bigwedge_{x \in E}$	$(\forall x \in E, \forall_{x \in E})$
$\exists$	*Existenzquantor*	$\bigvee_{x \in E}$	$(\exists x \in E, \exists_{x \in E})$

Bemerkung 1.10. *(Negation von Existenz- und Allaussagen)*

a) $\neg(\exists x \in E : Q(x))$ *ist logisch äquivalent mit* $\forall x \in E : \neg Q(x)$

b) $\neg(\forall x \in E : P(x))$ *ist logisch äquivalent mit* $\exists x \in E : \neg P(x)$

Bemerkung 1.11. *(Reihenfolge der Quantoren)*

Beispiel:

$\exists n \in \mathbb{N}\ \forall m \in \mathbb{N} : n > m$ *(falsch)*
$\forall m \in \mathbb{N}\ \exists n \in \mathbb{N} : n > m$ *(wahr)*
(denn zu $m \in \mathbb{N}$ *kann man beispielsweise* $n = m + 1$ *wählen)*

Bedeutung:

All- und Existenzquantoren dürfen in der Reihenfolge nicht vertauscht werden.

Beispiel:

$\exists n \in \mathbb{N}\ \exists m \in \mathbb{N} : n + m = 17$ *(wahr)*
gleichbedeutend mit
$\exists m \in \mathbb{N}\ \exists n \in \mathbb{N} : n + m = 17$ *(wahr)*

Bedeutung:

Existenzquantoren und Allquantoren können jeweils untereinander getauscht werden, nicht jedoch übergreifend.

Man unterscheidet in der Mathematik folgende Typen von Aussagen:

- *Axiome* (Grundaussagen, die nicht bewiesen werden)
- *Sätze* (wahre Aussagen, die aus Axiomen oder bereits bewiesenen Sätzen gefolgert werden)
  - *Lemma* (Hilfssatz)
  - *Theorem* (wichtiger Satz)
- *Definitionen*

Mathematische Sätze sind häufig von der Form: „Wenn V gilt, dann gilt B“.
Wobei V und B mathematische Aussagen sind. V ist Voraussetzung und B ist Behauptung des Satzes. Das bedeutet: Die Implikation $V \Rightarrow B$ ist wahr.

Um eine Implikation zu beweisen, nimmt man an, dass V wahr ist und zeigt dann, dass B wahr ist. Unterschiedliche Vorgehensweisen für Beweise, zeigen wir im Folgenden auf:

Bemerkung 1.12. *(Direkte Beweise) Die Implikation $V \Rightarrow B$ wird gezeigt, indem man $V \Rightarrow B_1, B_1 \Rightarrow B_2, \ldots, B_n \Rightarrow B$ als wahr nachweist. Die Gültigkeit der einzelnen Implikationen folgt aus schon bewiesenen Sätzen oder Axiomen.*
Man beachte: Sind $A_1 \Rightarrow A_2$ und $A_2 \Rightarrow A_3$ wahr, so ist $A_1 \Rightarrow A_3$ wahr.

Beispiel:

Behauptung: Ist n eine ungerade natürliche Zahl, so ist n^2 ungerade.
Voraussetzung: n ist ungerade natürliche Zahl.

Beweis:

Sei $n \in \mathbb{N}$ ungerade. Dann ist $n+1$ gerade. Also existiert natürliche Zahl k, so dass $n+1 = 2 \cdot k$. Folglich ist $n = 2 \cdot k - 1$. Dann gilt:

$$\begin{aligned} n^2 &= (2 \cdot k - 1)^2 \\ &= 4 \cdot k^2 - 4 \cdot k + 1 \\ &= 2 \cdot (2 \cdot k^2 - 2 \cdot k) + 1 \end{aligned}$$

Daher ist n^2 ungerade.

Formaler:

Es gilt: $\forall n \in \mathbb{N} : (n \text{ ungerade} \Rightarrow n^2 \text{ ungerade})$

Beweis:

$$\begin{aligned} n \text{ ungerade} &\Rightarrow n+1 \text{ gerade} \\ &\Rightarrow \exists k \in \mathbb{N} : n+1 = 2 \cdot k \\ &\Rightarrow n = 2 \cdot k - 1 \\ &\Rightarrow n^2 = 2 \cdot (2 \cdot k^2 - 2 \cdot k) + 1 \\ &\Rightarrow n^2 \text{ ungerade} \end{aligned}$$

Bemerkung 1.13. *(Indirekter Beweis) Statt $V \Rightarrow B$ beweist man die nach 1.8 c) dazu logisch äquivalente Aussage $\neg B \Rightarrow \neg V$.*

Beispiel:

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

Beweis:

Indirekter Beweis: Die zur Behauptung logisch äquivalente Aussage lautet: Ist n gerade, so ist n^2 gerade.
Sei n gerade, so existiert eine natürliche Zahl k mit $n = 2 \cdot k$ und es gilt:

$$\begin{aligned} n^2 &= (2 \cdot k)^2 \\ &= 4 \cdot k^2 \\ &= 2 \cdot (2 \cdot k^2) \end{aligned}$$

Somit ist n^2 gerade.

Bemerkung 1.14. *(Äquivalenzbweise) Einige Sätze sind von der Form*

„genau dann gilt A, wenn B gilt“

Es sind also A und B äquivalent bzw. gleichwertig. Das bedeutet: $A \Leftrightarrow B$ ist wahr.
Um einen Satz dieser Form zu beweisen, muss man zeigen, dass $A \Rightarrow B$ wahr ist und dass $B \Rightarrow A$ wahr ist.

Beispiel:

Sei n eine natürliche Zahl, dann gilt: n ist ungerade genau dann, wenn n^2 ungerade ist.

Beweis:

Folgt aus 1.12 und 1.13.

Paarweise Äquivalenz

Manchmal will man zeigen, dass die Aussagen $A_1, A_2, \ldots, A_n$ paarweise äquivalent sind. Dazu muss man zeigen: $A_1 \Leftrightarrow A_2$ ist wahr, $A_1 \Leftrightarrow A_3$ ist wahr, ... , $A_1 \Leftrightarrow A_n$ ist wahr, $A_2 \Leftrightarrow A_3, \ldots, A_2 \Leftrightarrow A_n, \ldots, A_{n-1} \Leftrightarrow A_n$ sind wahr.

Verkürzt: Man beweist, dass $A_1 \Rightarrow A_2$, $A_2 \Rightarrow A_3$, ..., $A_{n-1} \Rightarrow A_n$, $A_n \Rightarrow A_1$ wahr sind. Dieses Verfahren nennt man Ringschluss *oder* zyklisches Beweisverfahren*. Bei n Aussagen, müssen n Implikationen nachgewiesen werden.*

Bemerkung 1.15. *(Widerspruchsbeweis) Man will zeigen, dass $V \Rightarrow B$ gilt. Dazu nimmt man an, dass V wahr ist, aber B falsch. Man beweist dann, dass eine Aussage C wahr sein muss, von der man aber weiss, dass sie falsch ist. Dann ist die Annahme, dass B falsch ist, nicht aufrecht zu erhalten. Also ist B wahr.*

Beispiel:

Voraussetzung: $(\neg G \vee H) \wedge (D \Rightarrow C) \wedge ((D \Rightarrow G) \Rightarrow \neg C) \wedge D$
Behauptung: Die Aussage G ist falsch.

Beweis:

Angenommen es gilt die Voraussetzung und die Behauptung nicht, d.h. G ist wahr.
Die Aussage aus der Voraussetzung ist eine Konjunktion mit 4 Einzelaussagen. Daher muss jede Einzelaussage wahr sein.
(1) D ist wahr.
Da $D \Rightarrow C$ wahr ist, folgt mit (1):
(2) C ist wahr.
Es ist $(D \Rightarrow G) \Rightarrow \neg C$ wahr. Da nach (2) $\neg C$ falsch ist, folgt, dass $D \Rightarrow G$ falsch ist. Da G wahr ist (nach Annahme) folgt, dass D falsch ist. Das ist ein Widerspruch zu (1). Folglich ist G falsch.

2 Mengen

Nach Georg Cantor[1]:

> „Menge ist eine Zusammenfassung von bestimmten, wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen."

Diese Definiton ist problematisch.

Die Objekte heißen *Elemente* der Menge. Eine Menge wird beschrieben mit { und }. Aufzählende Schreibweise: $\{1, 2, a, 7\}$, $\{1, 2, 3, 4, \ldots\}$. Angabe durch Beschreibung: $\{x : x$ hat Eigenschaft E$\}$.

Beispiele:

$$\begin{aligned} & \{x : x \text{ ist natürliche Zahl und } x \text{ ist größer als } 7\} \\ = \; & \{8, 9, 10, \ldots\} \\ = \; & \{x : x \in \mathbb{N} \wedge x > 7\} \\ = \; & \{x \in \mathbb{N} : x > 7\} \end{aligned}$$

Schreibweise:

Ist x ein Element von Menge M, so schreibt man: $x \in M$
Ist x kein Element von Menge M, so schreibt man: $x \notin M$

Wichtige Mengen:

$\mathbb{N} =$ Menge der natürlichen Zahlen $= \{1, 2, 3, \ldots\}$
$\mathbb{N}_0 = \{0, 1, 2, \ldots\}$
$\mathbb{Z} =$ Menge der ganzen Zahlen
$\mathbb{Q} =$ Menge der rationalen Zahlen

[1] Georg Cantor (1845 - 1918) war ein deutscher Mathematiker.

$\mathbb{R} =$ Menge der reellen Zahlen
$\mathbb{C} =$ Menge der komplexen Zahlen

Die leere Menge enthält kein Elment: $\emptyset$
Die Anzahl der Elemente einer Menge kennzeichnet man mit: $|M|$

Beispiele:

$$\begin{aligned} |\{1,2,a,4\}| &= 4 \\ |\mathbb{N}| &= \infty \\ |\{\mathbb{N}\}| &= 1 \end{aligned}$$

Definition 2.1. *Seien M, N Mengen. M heißt* Teilmenge *(*Untermenge*) von N, falls gilt: Jedes Element von M ist auch Element von N.*
Wir schreiben dafür: $M \subseteq N$. Ist M keine Teilmenge von N, so schreiben wir: $M \not\subseteq N$.

Beispiel:

a) Es gilt $\{1,2,3\} \subseteq \{1,2,a,4,3\}$, aber $\{1,2,b\} \not\subseteq \{1,2,a,4,3\}$.

b) $1 \in \mathbb{N}, \quad 1 \notin \{\mathbb{N}\}, \quad \mathbb{N} \not\subseteq \{\mathbb{N}\}, \quad \mathbb{N} \in \{\mathbb{N}\}$.

c) $2 \in \{1,2,3,7,205\} = \{7,3,205,2,1\} = \{1,1,2,3,7,7,7,205\}$.

d) Sei $A = \{\mathbb{N}, \mathbb{Z}\}$. Dann ist $\mathbb{N} \in A$, $\mathbb{Z} \in A$, $\mathbb{Q} \notin A$, $1 \notin A$, $\{\mathbb{N}\} \subseteq A$, $A \supseteq \{\mathbb{N}\}$.

Beachte:

Es gilt $\emptyset \subseteq M$ für jede Menge M.
Die Gleichheit $M = N$ zweier Mengen M und N gilt genau dann, wenn $M \subseteq N$ und $N \subseteq M$.

Definition 2.2. *a) $M \cap N = \{x : x \in M \wedge x \in N\}$,* Durchschnitt *von M und N.*

b) $M \cup N = \{x : x \in M \vee x \in N\}$, Vereinigung *von M und N.*

c) $M \setminus N = \{x : x \in M \wedge x \notin N\}$, Differenz *von M und N*
Ist $N \subseteq M$, so heißt $M \setminus N$ Komplement *von N in M, geschrieben N^C.*

d) $M \triangle N = (M \setminus N) \cup (N \setminus M)$, Symmetrische Differenz.

Mengen können veranschaulicht werden durch Venn-Diagramme. *Abbildung 2.1 zeigt Beispiele von Venn-Diagrammen. Man beachte: Venn-Diagramme sind kein Beweis, son-*

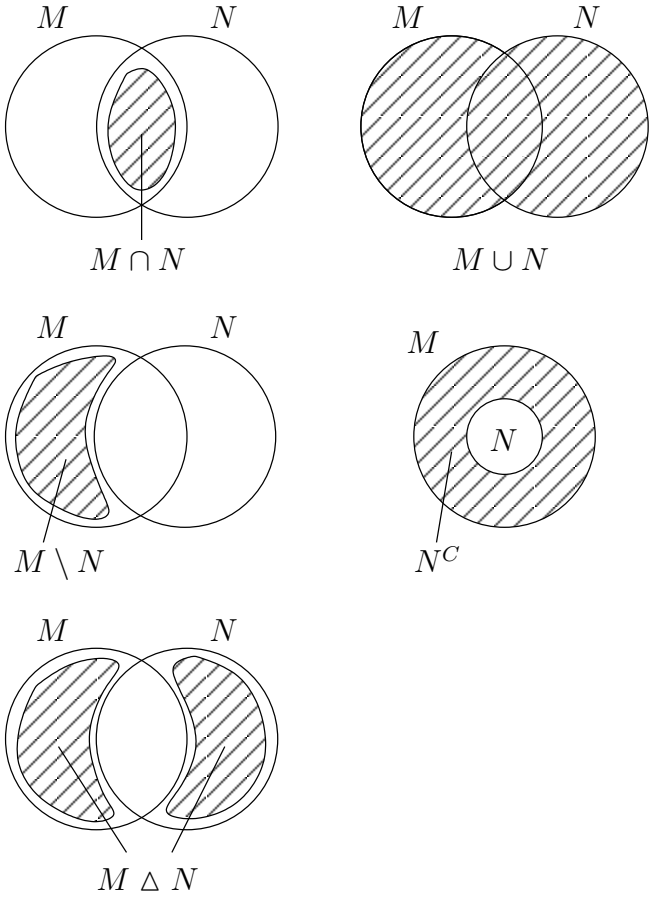


Abbildung 2.1: Venn-Diagramme von Mengen zur Definition 2.2

dern dienen nur der Veranschaulichung.

Kommutativgesetz und Assoziativgesetz:

Für den Durchschnitt und die Vereinigung von Mengen gilt das Kommutativgesetz:

$$\begin{aligned} M \cup N &= N \cup M \\ M \cap N &= N \cap M \end{aligned}$$

Für den Durchschnitt und die Vereinigung von Mengen gilt das Assoziativgesetz:

$$\begin{aligned} (M \cup N) \cup L &= M \cup (N \cup L) \\ (M \cap N) \cap L &= M \cap (N \cap L) \end{aligned}$$

Frage:

Gilt auch $(M \setminus N) \setminus L = M \setminus (N \setminus L)$?
Zur Beantwortung entweder Beweis oder Gegenbeispiel. Ein Venn-Diagramm kann Hinweise auf die Antwort liefern. Abbildung 2.2 und Abbildung 2.3 liefern solche Hinweise. Nachdem die Hinweise auf eine Ungleichheit hindeuten, stellen wir ein Gegenbeispiel

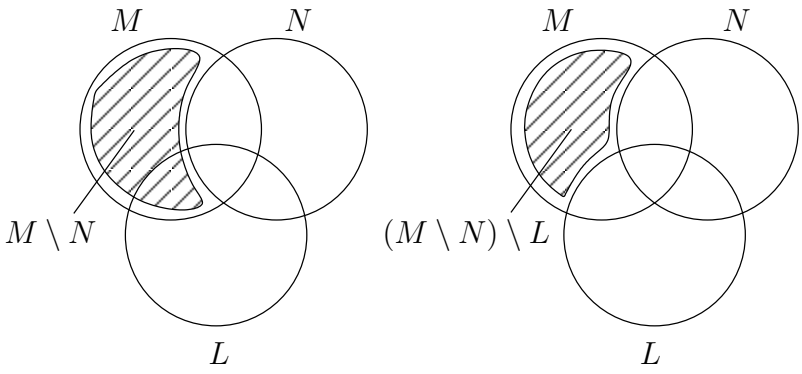


Abbildung 2.2: Veranschaulichung von $(M \setminus N) \setminus L$

auf. Sei $M = L = \{1\}$ und $N = \emptyset$. Dann gilt:

$$\begin{aligned} & (M \setminus N) \setminus L = M \setminus L = \emptyset \\ \neq \quad & M \setminus (N \setminus L) = M \setminus \emptyset = M = \{1\} \end{aligned}$$

Somit gilt das Assoziativgesetz nicht für die Differenz.

Satz 2.3. *Seien L, M und N Mengen. Dann gilt:*

a) $M \triangle N = (M \cup N) \setminus (M \cap N)$

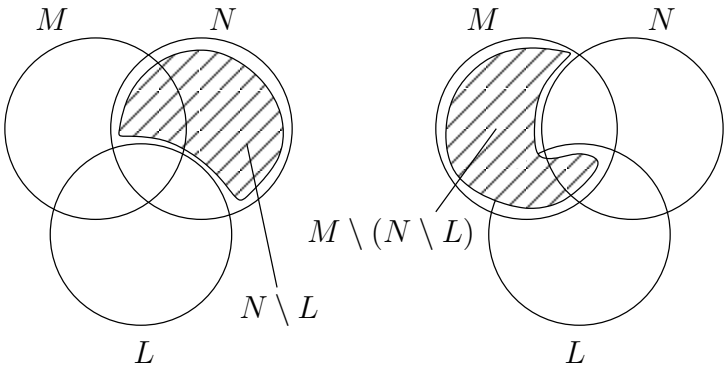


Abbildung 2.3: Veranschaulichung von $M \setminus (N \setminus L)$

b) Gilt $L, M \subseteq N$, so gilt:

$$(L \cup M)^C = L^C \cap M^C$$
$$(L \cap M)^C = L^C \cup M^C$$

Wobei die Komplemente in N gebildet sind. Dies sind die De Morgan'sche Regeln für Mengen.

c) $M \cap N = M$ genau dann, wenn $M \subseteq N$.

d) $M \cup N = M$ genau dann, wenn $N \subseteq M$.

Beweis. a) (1) $M \triangle N \subseteq (M \cup N) \setminus (M \cap N)$:

Sei $x \in M \triangle N = (M \setminus N) \cup (N \setminus M)$. Dann gilt $x \in M \setminus N$ oder $x \in N \setminus M$.

1.Fall: $x \in M \setminus N$. Dann $x \in M$, also auch $x \in M \cup N$. Außerdem $x \notin N$, dann auch $x \notin M \cap N$. Also $x \in (M \cup N) \setminus (M \cap N)$.

2.Fall: $x \in N \setminus M$. Dann $x \in N$, also auch $x \in M \cup N$. Außerdem $x \notin M$, dann auch $x \notin M \cap N$. Also $x \in (M \cup N) \setminus (M \cap N)$.

(2) $(M \cup N) \setminus (M \cap N) \subseteq M \triangle N$:

Sei $x \in (M \cup N) \setminus (M \cap N)$. Dann gilt $x \in M \cup N$. Dann $x \in M$ oder $x \in N$.

1.Fall: $x \in M$. Dann $x \notin N$, denn sonst $x \in M \cap N$ im Widerspruch zu $x \in (M \cup N) \setminus (M \cap N)$, d.h. $x \in M \setminus N$, also auch $x \in (M \setminus N) \cup (N \setminus M) = M \triangle N$.

2.Fall: $x \in N$. Dann $x \notin M$, denn sonst $x \in M \cap N$ im Widerspruch zu $x \in (M \cup N) \setminus (M \cap N)$, d.h. $x \in N \setminus M$, also auch $x \in (M \setminus N) \cup (N \setminus M) = M \triangle N$.

b)

$$\begin{aligned}
(L \cap M)^c &= \{x \in N : x \notin L \cap M\} \\
&= \{x \in N : \neg((x \in L) \wedge (x \in M))\} \\
&\underset{\text{1.8 b)}}{=} \{x \in N : \neg(x \in L) \vee \neg(x \in M)\} \\
&= \{x \in N : x \notin L \vee x \notin M\} \\
&= L^c \cup M^c
\end{aligned}$$

$$\begin{aligned}
(L \cup M)^c &= \{x \in N : x \notin L \cup M\} \\
&= \{x \in N : \neg((x \in L) \vee (x \in M))\}
\end{aligned}$$

$$\begin{aligned} &\underset{\text{1.8 c)}}{=} && \{x \in N : \neg(x \in L) \wedge \neg(x \in M)\} \\ &= && \{x \in N : x \notin L \wedge x \notin M\} \\ &= && L^c \cap M^c \end{aligned}$$

c) Übungsaufgabe.

d) Übungsaufgabe.

□

Definition 2.4. *Sei M eine Menge. Dann ist die* Potenzmenge *von M definiert als*

$$\mathcal{P}(M) \quad := \quad \{A : A \subseteq M\}$$

Man beachte: Für jede Menge M gilt $M \in \mathcal{P}(M)$ und $\emptyset \in \mathcal{P}(M)$.

Beispiel:

a) Sei $M = \{1\}$, so $\mathcal{P}(M) = \{\emptyset, \{1\}\}$.

b) Sei $M = \{1, 2\}$, so $\mathcal{P}(M) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.

c) Sei $M = \{1, 2, 3\}$, so $\mathcal{P}(M) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

d) Sei $M = \emptyset$, so $\mathcal{P}(M) = \{\emptyset\}$ und $|\mathcal{P}(M)| = 1$.

Definition 2.5. *Sei $\mathcal{A}$ eine Menge von Mengen. Die Vereinigung beliebig vieler Mengen ist definiert durch:*

$$\bigcup_{A \in \mathcal{A}} A \quad := \quad \{x : \exists A \in \mathcal{A} : x \in A\}$$

Der Durchschnitt beliebig vieler Mengen ist definiert durch:

$$\bigcap_{A \in \mathcal{A}} A \quad := \quad \{x : \forall A \in \mathcal{A} : x \in A\}$$

Beispiele:

a) Sei $\mathcal{A} = \{A_1, A_2\}$. Dann gilt $\bigcup_{A \in \mathcal{A}} = A_1 \cup A_2$.

b) Seien $A_1 \supseteq A_2 \supseteq \ldots \supseteq A_n$ Mengen.

$$\begin{aligned} A_1 \cap A_2 \cap \ldots \cap A_n &= \bigcap_{i=1}^{n} A_i \\ &= A_n \end{aligned}$$

Die Abbildung 2.4 veranschaulicht das Beispiel mit Hilfe eines Venn-Diagramms.

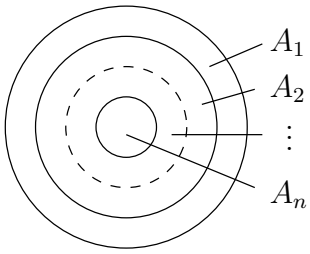


Abbildung 2.4: Verschachtelte Mengen

c) Für $n \in \mathbb{N}$ definieren wir $B_n := \left\{x \in \mathbb{R} : 0 \leq x \leq \frac{1}{n}\right\}$.
Es gilt $B_1 \supseteq B_2 \supseteq B_3 \supseteq \ldots \supseteq B_n$. Alle B_i sind unendliche Mengen.

$$\begin{aligned} \{0\} &= \bigcap_{i \in \mathbb{N}} B_i \\ &= \bigcap_{B \in \mathcal{B}} B \end{aligned}$$

wobei $\mathcal{B} = \{B_1, B_2, \ldots\} = \{B_i : i \in \mathbb{N}\}$.

Bemerkung:

Die Reihenfolge der Elemente in einer Menge ist irrelevant.
Bei relevanter Reihenfolge spricht man von einem geordneten Tupel. *Für dieses gilt: $(x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n)$ genau dann, wenn $x_1 = y_1$, $x_2 = y_2$,$\ldots$,$x_n = y_n$.*

Beispiel:

Es ist $(1, 2) \neq (2, 1)$, aber $\{1, 2\} = \{2, 1\}$.
Ist $n = 2$, so hat man Paare, 2-er Tupel. Ist $n = 3$: Tripel.
Es ist $(1, 1, 2) \neq (1, 2)$ und $(1, 1, 2) \neq (1, 2, 1)$.
Paare von reellen Zahlen beschreiben Punkte in der Ebene.

Definition 2.6. *Sei $n \in \mathbb{N}$, $n \geq 2$. Seien $M_1, \ldots, M_n$ Mengen. Dann heißt*

$$M_1 \times \ldots \times M_n := \{(x_1, \ldots, x_n) : x_i \in M_i \; \forall i \in \{1, \ldots, n\}\}$$

kartesisches Produkt *von* $M_1, \ldots, M_n$.
Ist $M_1 = \ldots = M_n = M$*, so schreiben wir* M^n *für* $M_1 \times \ldots \times M_n = M \times \underset{\leftarrow n \rightarrow}{\ldots} \times M$.

Beispiel: $\mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\} = \mathbb{R} \times \mathbb{R}$.

3 Abbildungen

Abbildungen spielen in der Mathematik eine wichtige Rolle. Darüber hinaus gibt es wichtige Speziallfälle von Abbildungen, wie beispielsweise die inkektive, surjektive oder bijektive Abbildung.

Definition 3.1. *Seien M und N nicht leere Mengen (nicht notwendig verschieden).*

a) Eine Abbildung *f von M nach N, $f : M \to N$, ist eine Zuordnung, die jedem Element aus M genau ein Element aus N zuordnet, bezeichnet mit $x \mapsto f(x)$.*
Ein Element $x \in M$ heißt Argument *oder* Urbild *von f. Das Element $f(x) \in N$ heißt* Bild *von x unter f.*
Die Menge M heißt Definitionsbereich *von f. Die Menge $f(M) := \{f(x) : x \in M\}$ heißt* Bild *oder* Bildbereich *von f. Dabei gilt $f(M) \subseteq N$.*
Eine Funktion ist dasselbe wie eine Abbildung.

b) Die Menge $G_f = \{(x, f(x)) : x \in M\} \subseteq M \times N$ heißt Graph *von f.*

Die Abbildung 3.1 zeigt eine korrekte Abbildung, die Abbildung 3.2 dagegen zeigt zwei Beispiele für Abbildungen, die nicht korrekt sind.

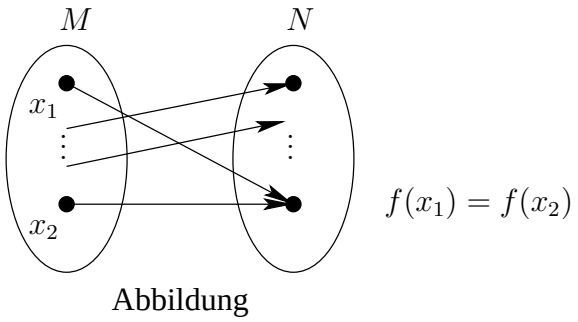


Abbildung 3.1: Beispiel einer korrekten Abbildung

Beispiel:

a) Sei M eine nicht leere Menge. Die Abbildung $\mathrm{id}_M : M \to M$ *mit* $\mathrm{id}_M(x) = x$ *heißt* identische Abbildung *auf M.*

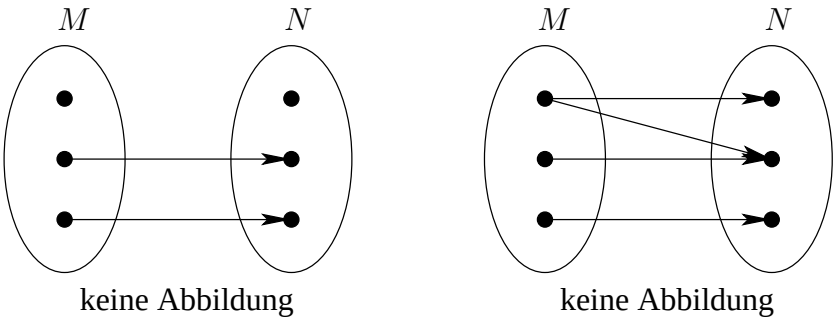


Abbildung 3.2: Beispiele für keine Abbildungen

b)

$$f : \begin{cases} \mathbb{R} \setminus \{0\} \to \mathbb{R} \\ x \mapsto \frac{1}{x} \end{cases}$$

Die Abbildung f ist eine korrekte Abbildung, aber keine Abbildung von $\mathbb{R}$ nach $\mathbb{R}$.

$$g : \begin{cases} \mathbb{R} \to \mathbb{R} \\ x \mapsto \begin{cases} \frac{1}{x} & \textit{wenn } x \neq 0 \\ 0 & \textit{wenn } x = 0 \end{cases} \end{cases}$$

Die Abbildung g ist eine Abbildung von $\mathbb{R}$ nach $\mathbb{R}$. Die Abbildung 3.3 veranschaulicht dies anhand des Graphen von g.

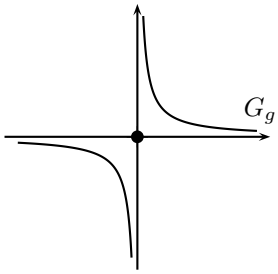


Abbildung 3.3: Graph der Abbildung g

c) Die Abbildung $|\,.\,|$ *heißt* Betragsfunktion *und ist wie folgt definiert:*

$$|\,.\,| : \begin{cases} \mathbb{R} \to \mathbb{R} \\ x \mapsto \begin{cases} x & \textit{falls } x \geq 0 \\ -x & \textit{falls } x < 0 \end{cases} \end{cases}$$

Die Abbildung 3.4 zeigt den Graph der Betragsfunktion.

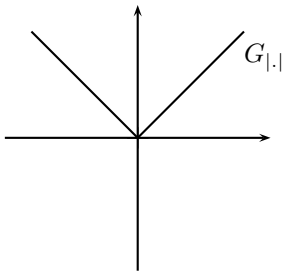


Abbildung 3.4: Graph der Betragsfunktion

d) Eine Abbildung von $\{0,1\}^n \to \{0,1\}^m$ *heißt* Schaltfunktion.
Beispiel: $\wedge : \{0,1\}^2 \to \{0,1\}$ *definiert durch:*

$$\begin{aligned} \wedge((1,1)) &= 1 \\ \wedge((1,0)) &= 0 \\ \wedge((0,1)) &= 0 \\ \wedge((0,0)) &= 0 \end{aligned}$$

(vgl. 1.2 Konjunktion)

e) Sei $A \subseteq M$*. Die Abbildung* 1_A *mit*

$$1_A : \begin{cases} M \to \{0,1\} \\ x \mapsto \begin{cases} 1 & \text{wenn } x \in A \\ 0 & \text{wenn } x \notin A \end{cases} \end{cases}$$

heißt Indikatorfunktion *von* A *in* M*.*

f)

$$f : \begin{cases} \{0,1\} \to \{0,1\} \\ x \mapsto x \end{cases}$$

$$g : \begin{cases} \{0,1\} \to \{0,1\} \\ x \mapsto x^2 \end{cases}$$

Die Abbildungen f*,* g *beschreiben die gleiche Abbildung:*

$$\begin{aligned} f(0) &= 0 \\ &= 0^2 \\ &= g(0) \\ f(1) &= 1 \\ &= 1^2 \\ &= g(1) \end{aligned}$$

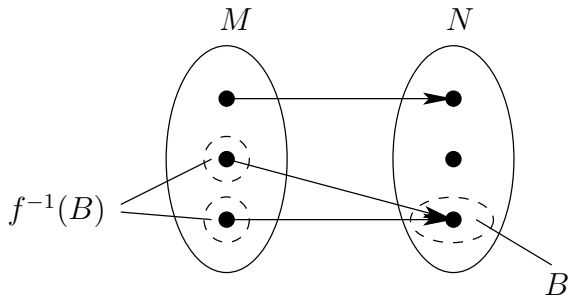


Abbildung 3.5: Veranschauung von Bildmenge und Urbild

Definition 3.2. *Zwei Abbildungen $f_1 : M_1 \to N_1$ und $f_2 : M_2 \to N_2$ heißen* gleich, *wenn $M_1 = M_2$, $N_1 = N_2$ und $f_1(x) = f_2(x)$ für alle $x \in M_1 = M_2$.*
Äquivalent: $f = g$ genau dann, wenn $N_1 = N_2$ und $G_f = G_g$.

Beispiel: Siehe 3.1 Beispiel f).

Schreibweise:

Sei $f : M \to N$ eine Abbildung. Für $A \subseteq M$ heißt $f(A) := \{f(x) : x \in A\}$ das Bild *(oder die* Bildmenge*) von A unter f. Für $B \subseteq N$ heißt $f^{-1}(B) := \{x \in M : f(x) \in B\}$ das* (volle) Urbild *von B bzgl. f. Die Abbildung 3.5 veranschaulicht diese Begriffe.*

Beispiel:

Wir betrachten folgende Abbildung f:

$$f : \begin{cases} \mathbb{Z} \to \mathbb{N}_0 \\ x \mapsto x^2 \end{cases}$$

Es gilt $f(\mathbb{Z}) = \{0, 1, 4, 9, \ldots\} = f(\mathbb{N}_0)$. Folgerung: Aus der Gleichheit von $f(A_1) = f(A_2)$ folgt im Allgemeinen nicht *$A_1 = A_2$.*

Sei $B_1 = \{1, 2, 3, 4\}$ und $B_2 = \{1, 4, 5\}$. Es gilt:

$$\begin{aligned} f^{-1}(B_1) &= \{1, -1, 2, -2\} \\ &= f^{-1}(B_2) \end{aligned}$$

Folgerung: Aus der Gleichheit von $f^{-1}(B_1) = f^{-1}(B_2)$ folgt im Allgemeinen nicht *$B_1 = B_2$.*

Definition 3.3. *Sei $f : M \to N$ eine Abbildung.*

a) *Die Abbildung f heißt* surjektiv, *falls $f(M) = N$.*
Äquivalente Aussage: $\forall n \in N\ \exists m \in M : f(m) = n$.

b) *Die Abbildung f heißt* injektiv, *falls für alle $m_1, m_2 \in M$ gilt:*
Ist $m_1 \neq m_2$, so ist $f(m_1) \neq f(m_2)$.
Äquivalente Aussage: $\forall m_1, m_2 \in M : f(m_1) = f(m_2) \Rightarrow m_1 = m_2$.

c) *Die Abbildung f heißt* bijektiv, *falls f surjektiv und injektiv ist.*
Eine bijektive Abbildung wird auch Bijektion *gennant.*

Die Abbildungen 3.6 und 3.7 zeigen beispielhafte Veranschauungen.

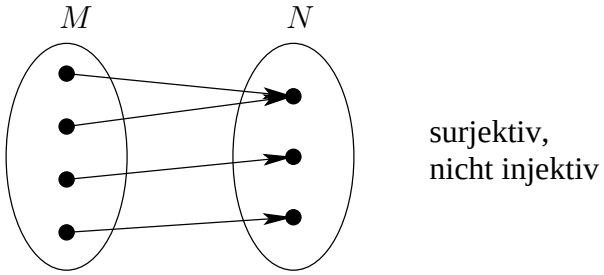


Abbildung 3.6: Beispiel für eine surjektive, aber nicht injektive Abbildung

Beispiel:

a)

$$f : \begin{cases} \mathbb{Z} \to \mathbb{N}_0 \\ x \mapsto x^2 \end{cases}$$

Die Abbildung f ist nicht surjektiv, z.B. gilt $2 \notin f(\mathbb{Z})$, da 2 keine ganzzahlige Quadratwurzel hat. Die Abbildung f ist nicht injektiv, z.B. gilt $f(2) = 4 = f(-2)$.

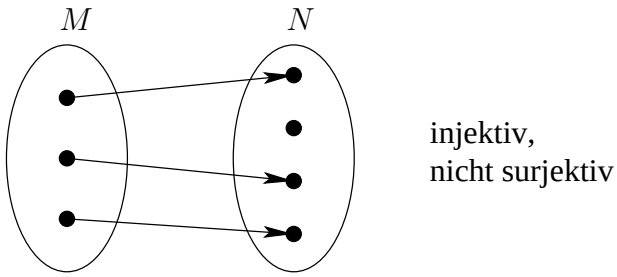


Abbildung 3.7: Beispiel für eine injektive, aber nicht surjektive Abbildung

b)

$$f : \begin{cases} \mathbb{R} \to \mathbb{R} \\ x \mapsto 3 \cdot x + 2 \end{cases}$$

Die Abbildung f ist surjektiv: Sei $y \in \mathbb{R}$. Suche x mit $3 \cdot x + 2 = y$. Es ist $x = \frac{y-2}{3}$. Es gilt $\frac{y-2}{3} \in \mathbb{R}$ für alle $y \in \mathbb{R}$. $f(x) = 3 \cdot (\frac{y-2}{3}) + 2 = y$.
Die Abbildung f ist injektiv: Seien $x_1, x_2 \in \mathbb{R}$ mit $f(x_1) = f(x_2)$. So gilt:

$$\begin{aligned} f(x_1) = f(x_2) &\Rightarrow 3 \cdot x_1 + 2 = 3 \cdot x_2 + 2 \\ &\Rightarrow 3 \cdot x_1 = 3 \cdot x_2 \\ &\Rightarrow x_1 = x_2 \end{aligned}$$

Die Abbildung f ist bijektiv, da sie surjektiv und injektiv ist.

c) Sei $\wedge : \{0,1\}^2 \to \{0,1\}$ die Abbildung der Konjunktion. $\wedge$ ist surjektiv, nicht injektiv:

$$\begin{aligned} (0,1) &\mapsto 0 \\ (1,0) &\mapsto 0 \\ (0,1) &\mapsto 0 \\ (1,1) &\mapsto 1 \end{aligned}$$

d)

$$f : \begin{cases} \mathbb{N} \to \mathbb{N} \\ x \mapsto x + 2 \end{cases}$$

Die Abbildung f ist nicht surjektiv: 1, 2 haben keine Urbilder.
Die Abbildung f ist injektiv: Seien $x_1, x_2 \in \mathbb{N}$, so gilt:

$$\begin{aligned} f(x_1) = f(x_2) &\Rightarrow x_1 + 2 = x_2 + 2 \\ &\Rightarrow x_1 = x_2 \end{aligned}$$

e) Sei $g : \{1,2,3,4,5\} \to \{a,b,c,d,e\}$ eine Abbildung mit:

$$\begin{aligned} g(1) &= a \\ g(2) &= b \\ g(3) &= c \\ g(4) &= d \\ g(5) &= e \end{aligned}$$

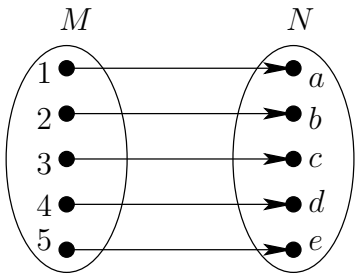


Abbildung 3.8: Beispiel einer Bijektion

Die Abbildung g ist bijektiv, die Abbildung 3.8 veranschaulicht dies.

Allgemein gilt: Sind M und N endlich und existiert Bijektion zwischen M und N, so ist $|M| = |N|$.

f)

$$g : \begin{cases} \mathbb{N} \to \mathbb{N}_0 \\ x \mapsto x - 1 \end{cases}$$

Die Abbildung g ist eine bijektive Abbildung.

Bemerkung 3.4. *Der Begriff der Bijektion wird zur exakten Definition der Anzahl der Elemente einer endlichen Menge benötigt:*

$$|M| = n \quad \Leftrightarrow \quad \text{Es existiert Bijektion } f : \{1, \ldots, n\} \to M$$

Eine unendliche Menge M heißt abzählbar*, wenn es eine Bijektion $f : \mathbb{N} \to M$ gibt.*

Beispiel:

Die Mengen $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$ sind abzählbar.
Die Mengen $\mathcal{P}(\mathbb{N})$, $\mathbb{R}$ sind nicht abzählbar (siehe dazu [WHK04], 2.11 - 2.13).

Satz 3.5. *Seien M und N endliche Mengen, $|M| = |N|$ und $f : M \to N$ eine Abbildung. Dann sind folgende Aussagen äquivalent:*

a) f ist injetkiv

b) f ist surjektiv

c) f ist bijektiv

Beweis. Beweis erfolgt durch das Ringschlussverfahren.

„a) ⇒ b)“: Sei f injektiv. Sind $m_1, m_2 \in M$ mit $m_1 \neq m_2$, so ist $f(m_1) \neq f(m_2)$, da f injektiv ist. Daher: $|M| = |f(M)|$. Da $|M| = |N|$, folgt $|f(M)| = |N|$. Da $f(M) \subseteq N$, ist $f(M) = N$. Also ist f surjektiv.

„b) ⇒ c)“: Sei f surjektiv. Da N endlich ist, gilt $|N| = k$ für ein $k \in \mathbb{N}$ und $N = \{n_1, \ldots, n_k\}$. Da f surjektiv ist, gilt: Zu jedem n_i, für $i \in \{1, \ldots, k\}$, existiert (mindestens) ein $m_i \in M$ mit $f(m_i) = n_i$. Da f eine Abbildung ist, ist $m_i \neq m_j$ für $i \neq j$. Also $|\{m_1, \ldots, m_k\}| = k$. Da $|M| = |N| = k$, gilt $M = \{m_1, \ldots, m_k\}$. Ist also $i \neq j$, dann $m_j \neq m_i$ und $f(m_i) = n_i \neq n_j = f(m_j)$. Somit ist f injektiv. Da f surjektiv und injektiv ist, ist f bijektiv.

„c) ⇒ a)“: Folgt direkt aus der Definition von Bijektivität. □

Definition 3.6. *Seien M, N nicht leere Mengen. Wir definieren:*

$$N^M \quad := \quad \{f : f \text{ ist Abbildung von } M \text{ nach } N\}$$

Spezialfall:

Sei $M = \{1, \ldots, n\}$ und eine N beliebige nicht leere Menge.

$$g : \begin{cases} N^M \to N \underbrace{\times \ldots \times}_{\leftarrow n \rightarrow} N = N^n \\ f \mapsto (f(1), \ldots, f(n)) \in N^n \end{cases}$$

Die Abbildung g ist bijektiv. Surjektivität:
Sei $(x_1, \ldots, x_n) \in N^n$ beliebig. Definiere $f \in N^M$ durch $f(1) = x_1, \ldots, f(n) = x_n$. Dann ist $f \in N^M$ und $g(f) = (x_1, \ldots, x_n)$.
Injektivität:
Seien $f_1, f_2 \in N^M$ mit $f_1 \neq f_2$. Da $f_1 : M \to N$ und $f_2 : M \to N$, existiert $x \in M$ mit $f_1(x) \neq f_2(x)$. Also ist
$g(f_1) = (f_1(1), \ldots, f_1(x), \ldots, f_1(n)) \neq (f_2(1), \ldots, f_2(x), \ldots, f_2(n)) = g(f_2)$.

Mit der bijektiven Abbildung g kann man $N^M = N^{\{1,\ldots,n\}}$ mit N^n „identifizieren“.

Satz 3.7. *a) Seien $f : M \to N$, $g : N \to P$ Abbildungen, wobei N, M, P nicht leere Mengen sind. Sei $x \in M$, dann definiert die Zuordnung $x \mapsto g(f(x))$ eine Abbildung von M nach P, die* Hintereinanderausführung *$g \circ f$ der Abbildungen g und f (gesprochen: „g nach f“). Genauer:*

$$(g \circ f)(x) \quad : \quad \begin{cases} M \to P \\ x \mapsto g(f(x)) \end{cases}$$

Die Abbildung 3.9 veranschaulicht die Hintereinanderausführung.

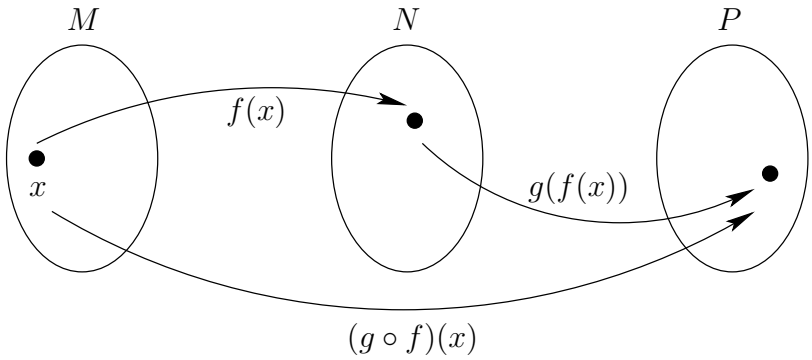


Abbildung 3.9: Veranschauung der Hintereinanderausführung zweier Abbildungen

b) Sei $h : P \to R$ eine weitere Abbildung, wobei R eine nicht leere Mengen ist. Dann gilt: $(h \circ g) \circ f = h \circ (g \circ f)$. Es gilt also das Assoziativgesetz *für die Hintereinanderausfürhung.*

Beweis. a) Klar.

b) Für alle $x \in M$ gilt:

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

□

Beispiele:

a)

$$f : \begin{cases} \mathbb{R} \to \mathbb{R} \\ x \mapsto x^2 \end{cases}$$

$$g : \begin{cases} \mathbb{R} \to \mathbb{R} \\ x \mapsto \sin(x) \end{cases}$$

Für alle $x \in \mathbb{R}$ gilt:

$$(g \circ f)(x) = g(f(x))$$

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

Folgerung: Selbst, wenn man $f \circ g$ und $g \circ f$ bilden kann ($f : M \to N$, $g : N \to M$), ist im Allgemeinen $f \circ g \neq g \circ f$.

b) Sei $M = \{1, 2, 3\}$ und seien $g : M \to M$, $f : M \to M$ Abbildungen mit:

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

Dann gilt:

$$\begin{aligned} (g \circ f)(1) &= g(f(1)) \\ &= g(2) \\ &= 3 \\ &\neq 1 \\ &= f(2) \\ &= f(g(1)) \\ &= (f \circ g)(1) \end{aligned}$$

Somit ist $g \circ f \neq f \circ g$.

Satz 3.8. *Die Hintereinanderausführung von surjektiven/injektiven/bijektiven Abbildungen ergibt wieder eine surjektive/injektive/bijektive Abbildung.*

Beweis. Übungsaufgabe. □

Satz 3.9. *Sei $f : M \to N$ eine Abbildung, dann sind äquivalent:*

(1) f ist bijektiv

(2) Es existiert eine Abbildung $g : N \to M$ mit $g \circ f = \mathrm{id}_M$ und $f \circ g = \mathrm{id}_N$

Diese Abbildung g ist eindeutig bestimmt und heißt Umkehrabbildung *oder* inverse Abbildug *f^{-1} zu f. Die Abbildung f^{-1} ist bijektiv und es gilt $(f^{-1})^{-1} = f$.*

Beweis. „(1) ⇒ (2)“: Sei f bijektiv. Wir geben einen Konstruktionsbeweis an: Sei $y \in N$ beliebig. Da f bijektiv ist, existiert genau ein $x \in M$ mit $f(x) = y$. Setze $g(y) = x$. Dann $(f \circ g)(y) = f(g(y)) = f(x) = y$, d.h. $f \circ g = \mathrm{id}_N$. Sei $z \in M$. Da f bijektiv ist, ist z das eindeutig bestimmte Urbild von $f(z)$ für f. Daher gilt nach Definition von g: $g(f(z)) = z$. Somit gilt $g \circ f = \mathrm{id}_M$.

„(2) ⇒ (1)“: Angenommen es existiere eine solche Abbildung g. Sei $y \in N$. Dann ist $g(y) \in M$. Es ist:

$$\begin{aligned} f(g(y)) &= (f \circ g)(y) \\ &\underset{\text{Voraussetzung}}{=} \mathrm{id}_N(y) \\ &= y \end{aligned}$$

Somit ist f surjektiv. Seien $x_1, x_2 \in M$ mit $f(x_1) = f(x_2)$. Dann gilt:

$$\begin{aligned} x_1 &= \mathrm{id}_M(x_1) \\ &\underset{\text{Voraussetzung}}{=} (g \circ f)(x_1) \\ &= g(f(x_1)) \\ &= g(f(x_2)) \\ &\underset{\text{Voraussetzung}}{=} (g \circ f)(x_2) \\ &= \mathrm{id}_M(x_2) \\ &= x_2 \end{aligned}$$

Somit ist f injektiv. Da f surjektiv und injektiv ist, ist f bijektiv.

Umkehrabbildung g ist eindeutig bestimmt:

Angenommen f ist bijektiv und es existieren zwei Abbildungen $g_1 : N \to M$, $g_2 : N \to M$ mit $(g_i \circ f) = \mathrm{id}_M$, $(f \circ g_i) = \mathrm{id}_N$ für $i = 1, 2$.
Wir zeigen: $g_1 = g_2$. Sei $y \in N$. Da f bijektiv ist, existiert genau ein $x \in M$ mit $f(x) = y$. Es gilt:

$$\begin{aligned} g_1(y) &= g_1(f(x)) \\ &= (g_1 \circ f)(x) \\ &= \mathrm{id}_M(x) \\ &= (g_2 \circ f)(x) \\ &= g_2(f(x)) \\ &= g_2(y) \end{aligned}$$

□

Beispiel:

a) Sei $f : \{1, 2, 3\} \to \{1, 2, 3\}$ *eine Abbildung mit:*

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

Die Abbildung f *ist bijektiv und für die zugehörige inverse Abbildung* f^{-1} *gilt:*

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

b) Sei $g : \{1, 2, 3\} \to \{1, 2, 3\}$ *eine Abbildung mit:*

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

Die Abbildung g *ist bijektiv und für die zugehörige inverse Abbildung* g^{-1} *gilt:*

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

Somit gilt $g^{-1} = g$.

c)

$$f : \begin{cases} \mathbb{R} \to \mathbb{R} \\ x \mapsto x^3 \end{cases}$$

Die Abbildung f *ist bijektiv. Für die zugehörige inverse Abbildung* f^{-1} *gilt:*

$$f^{-1} : \begin{cases} \mathbb{R} \to \mathbb{R} \\ x \mapsto \sqrt[3]{x} \end{cases}$$

d)

$$f : \begin{cases} \mathbb{R} \setminus \{0\} \to \mathbb{R} \setminus \{0\} \\ x \mapsto \frac{1}{x} \end{cases}$$

Die Abbildung f *ist bijektiv und es gilt* $f^{-1} = f$.

4 Relationen

Sei $f : M \to N$ eine Abbildung. Jedem Element aus M wird genau ein Element aus N zugeordnet. Das Weglassen dieser Bedingung führt zum Begriff Relation. Die Abbildung 4.1 zeigt beispielhaft eine Relation, welche entsprechend der Beschreibung von Abbildungen durch G_f gerade $\{(2, a), (2, b), (3, d), (4, d)\}$ entspricht.

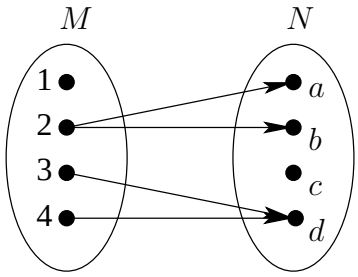


Abbildung 4.1: Keine Abbildung, aber eine Relation

Definition 4.1. *Seien $M_1, \ldots, M_n$ nicht leere Mengen mit $n \in \mathbb{N}$. Eine n-stellige* Relation *R über $M_1, \ldots, M_n$ ist eine Teilmenge von $M_1 \times \ldots \times M_n$.*
Gilt $M_1 = \ldots = M_n = M$, so spricht man von n-stelliger Relation auf M.

Ein besonders wichtiger Fall ist $n = 2$, also eine 2-stellige Relation. Für 2-stellige Relation wird häufig ein spezielles Symbol wie $\sim$ oder $\preceq$ verwendet. Statt $(x, y) \in R$ schreibt man oft $x \sim y$ (oder $x \preceq y$). Das Symbol der 2-stelligen Relation wird häufig im Index der Relation gekennzeichnet: $R_\sim$, $R_\preceq$.

Beispiele:

a) *Der Graph G_f einer Abbildung $f : M \to N$ ist eine Relation über $M \times N$:*

$$G_f \quad = \quad \{(x, f(x)) : x \in M\} \subseteq M \times N$$

In diesem Sinne sind Relationen Verallgemeinerung von Abbildungen.

b) *Sei M eine nicht leere Menge. Die Gleichheitsrelation $=$ auf M entspricht $R_= = \{(x, x) : x \in M\}$.*

c) Die übliche $<$-Relation auf $\mathbb{N}$ entspricht $R_< = \{(x, y) : x, y \in \mathbb{N}, x < y\}$. Der Ausdruck $3 < 4$ ist gleichwertig mit $(3, 4) \in R_<$.

d) Die Teilbarkeit $|$ auf $\mathbb{N}$ als Relation: $x|y$ (gesprochen „x teilt y“), d.h. $\exists k \in \mathbb{N} : y = k \cdot x$. $R_| = \{(1, 1), (1, 2), \ldots, (2, 2), (2, 4), (2, 6), \ldots, (3, 3), (3, 6), (3, 9), \ldots\}$.

e) Die übliche $\leq$-Relation auf $\mathbb{N}$ entspricht $R_\leq = \{(x, y) : x, y \in \mathbb{N}, x = y$ oder $x < y\}$.

f) Die normale $\leq$-Relation auf $\{1, 2, 3, 4\}$:

$$\begin{aligned} R_\leq &= \{(1,1),(1,2),(1,3),(1,4),(2,2),(2,3),(2,4),(3,3),(3,4),(4,4)\} \\ &\subset \{1,2,3,4\}^2 \end{aligned}$$

Man beachte: Das $\leq$-Symbol muss nicht immer die normale $\leq$-Relation auf Zahlen sein.

Wichtige Typen 2-stelliger Relationen:

- *Ordnungsrelationen*
- *Äquivalenzrelationen*

Beispiel d), e) sind Beispiele für Ordnungsrelationen. Wir werden diese beiden Begriffe im Folgenden definieren.

Definition 4.2. *Eine 2-stellige Relation R auf M heißt* Ordnungsrelation *(*Ordnung, partielle Ordnung*), wenn folgendes gilt:*

(1) $\forall x \in M : (x, x) \in R$
*(*Reflexivität *von R)*

(2) $\forall x, y \in M : (x, y) \in R \quad \wedge \quad (y, x) \in R \quad \Rightarrow \quad x = y$
*(*Antisymmetrie *von R)*

(3) $\forall x, y, z \in M : (x, y) \in R \quad \wedge \quad (y, z) \in R \quad \Rightarrow \quad (x, z) \in R$
*(*Transitivität *von R)*

Gilt zusätzlich die folgende Bedingung:

(4) $\forall x, y \in M : (x, y) \in R \quad \vee \quad (y, x) \in R$

Dann heißt die Ordnung linear *oder* total.

Schreibweise:

Man schreibt oft $x \leq y$ *statt* $(x, y) \in R$*:*

(1) $\forall x \in M : (x \leq x)$

(2) $\forall x, y \in M : (x \leq y) \quad \wedge \quad (y \leq x) \quad \Rightarrow \quad (x = y)$

(3) $\forall x, y, z \in M : (x \leq y) \quad \wedge \quad (y \leq z) \quad \Rightarrow \quad (x \leq z)$

(4) $\forall x, y \in M : (x \leq y) \quad \vee \quad (y \leq x)$

Üblicherweise wird $\leq$ *statt* $\preceq$ *verwendet, auch wenn* $\leq$ *nicht die normale kleiner-gleich-Ordnung auf* $\mathbb{N}$ *bedeutet. Der Ausdruck* $x < y$ *bedeutet:* $x \leq y$ *und* $x \neq y$*.*

Beispiele:

a) Die normale $\leq$*-Relation auf* $\mathbb{N}$ *ist eine totale Ordnung.*

b) Sei M *eine nicht leere Menge, so ist die Gleichheitsrelation auf* M *eine Ordnungsrelation, aber keine totale Ordnung.*

c) Die Teilerrelation auf $\mathbb{N}$ *ist eine Ordnung, aber nicht total.*

d) Sei X *eine Menge und* $M = \mathcal{P}(X)$*. Die Teilmengen-Relation* $R = \{(A, B) \in M^2 : A \subseteq B\}$ *auf* M *ist eine Ordnungsrelation. Keine totale Ordnung, wenn* $|X| > 1$*, denn: Seien* $a, b \in X$ *mit* $a \neq b$*, dann gilt weder* $\{a\} \subseteq \{b\}$ *noch* $\{b\} \subseteq \{a\}$*.*

e) Sei $M = \{a, b, c\}$ *und* $R = \{(a, a), (a, b), (b, b), (b, c), (c, c)\}$*.* R *ist eine Relation über* M*.* R *ist reflexiv, antisymmetrisch, aber nicht transitiv, also keine Ordnung. Denn:* $(a, b) \in R$*,* $(b, c) \in R$*, aber* $(a, c) \notin R$*.*

f) Sei $\leq$ *totale Ordnung auf* M*. Definiere eine Relation* $\preceq$ *auf* M^n *durch:*

$$\begin{aligned} & u = (u_1, \ldots, u_n) \preceq v = (v_1, \ldots, v_n) \\ \Leftrightarrow: \quad & u = v \text{ oder } u_1 < v_1 \text{ oder } \exists k < n : u_1 = v_1, \ldots, u_k = v_k, u_{k+1} < v_{k+1} \end{aligned}$$

Dann $\preceq$ *ist totale Ordnung auf* M^n*, genannt* Lexikographische Ordnung*.*

Die lexikographische Ordnung wird in der Informatik oft auf binäre Strings der Länge n *über dem Alphabet* $\{0, 1\}$ *mit Relation* $0 < 1$ *angewendet.*

g) Sei $\leq$ *eine partielle Ordnung auf* M*. Definiere* $\leq$ *auf* M^n *durch:*

$$u = (u_1, \ldots, u_n) \leq v = (v_1, \ldots, v_n)$$

$$\Leftrightarrow: \quad u_1 \leq v_1, \ldots, u_n \leq v_n$$

Die Relation $\leq$ auf M^n ist eine partielle Ordnung, aber keine totale Ordnung. Dies gilt auch, wenn die Ordnung auf M total ist.

Beispiel: $M = \mathbb{N}$ mit normaler $\leq$-Relation. Die Relation $\leq$ auf M ist eine totale Ordnung. Die Relation $\leq$ auf M^2, also $n = 2$, ist keine totale Ordnung: Es ist gilt $(1,5) \not\leq (2,4)$ und $(2,4) \not\leq (1,5)$.

Definition 4.3. *Eine binäre Relation $\sim$ auf einer nicht leeren Menge M heißt* Äquivalenzrelation *auf M, falls folgendes gilt:*

(1) $\forall x \in M : (x \sim x)$
(Reflexivität)

(2) $\forall x, y \in M : (x \sim y) \quad \Rightarrow \quad (y \sim x)$
*(*Symmetrie*)*

(3) $\forall x, y, z \in M : (x \sim y) \quad \wedge \quad (y \sim z) \quad \Rightarrow \quad (x \sim z)$
(Transitivität)

Beispiel:

a) Gleichheitsrelation auf M.

b) Sei $M = \mathbb{Z}$. Wir definieren folgende Relation $\sim$ über M: $x \sim y \Leftrightarrow x - y$ ist eine gerade Zahl (also durch zwei teilbar).
Die Relation $\sim$ ist reflexiv: Für $x \in M$ gilt $x - x = 0 = 2 \cdot k$ für ein $k \in \mathbb{Z}$.
Die Relation $\sim$ ist symmetrisch: Gilt $x \sim y$, so existiert $k \in \mathbb{Z}$ mit:

$$\begin{aligned} x - y = 2 \cdot k &\Leftrightarrow 0 = 2 \cdot k + y - x \\ &\Leftrightarrow -2 \cdot k = y - x \\ &\Leftrightarrow 2 \cdot \underbrace{(-k)}_{=:k' \in \mathbb{Z}} = y - x \\ &\Leftrightarrow 2 \cdot k' = y - x \\ &\Leftrightarrow y \sim x \end{aligned}$$

Die Relation $\sim$ ist transitiv: Sind $x - y$ und $y - z$ gerade, so gilt:

$$x - z = \underbrace{(x - y) + (y - z)}_{gerade}$$

Somit ist $\sim$ eine Äquivalenzrelation.

c) Das vorherige Beispiel lässt sich wie folgt verallgemeinern: Sei $M = \mathbb{Z}$, $r \in \mathbb{N}$ fest. Wir definieren die Relation auf M durch:

$$x \sim y \quad \Leftrightarrow \quad x - y \text{ ist durch } r \text{ teilbar}$$

Die Relation ist eine Äquivalenzrelation. Der zugehörige Beweis lässt sich analog zum vorherigen Beispiel führen.

d) Sei $f : M \to N$ eine Abbildung. Definiere eine Relation $\sim$ auf M wie folgt:

$$x \sim y \quad \Leftrightarrow \quad f(x) = f(y)$$

Die Relation ist eine Äquivalenzrelation. Der zugehörige Beweis soll eine Übungsaufgabe sein.

Definition 4.4. *Sei M eine nicht leere Menge, R eine Äquivalenzrelation auf M. Sei $x \in M$. Dann heißt $[x] := \{y : y \in M,\ y \sim x\}$* Äquivalenzklasse *von x bzgl. R auf M.*

Satz 4.5. *Sei R eine Äquivalenzrelation auf einer nicht leeren Menge M.*

a) Dann sind folgende Aussagen äquivalent:

(i) $[x] = [y]$

(ii) $x \in [y]$

(iii) $x \sim y$

b) Ist $[x] \neq [y]$, so ist $[x] \cap [y] = \emptyset$.

Beweis. a) „(i) ⇒ (ii)“: Es gelte $[x] = [y]$. Wegen der Reflexivität von $\sim$ ist $x \in [x] = [y]$.

„(ii) ⇒ (iii)“: Es gelte $x \in [y]$. Nach Definition von $[y]$ ist dann $x \sim y$.

„(iii) ⇒ (i)“: Es gelte $x \sim y$. Um $[x] = [y]$ zu zeigen, müssen wir $[x] \subseteq [y]$ und $[y] \subseteq [x]$ zeigen.
„$[x] \subseteq [y]$“: Sei $z \in [x]$. Nach Definition ist $z \sim x$. Nach Voraussetzung ist $x \sim y$. Wegen der Transitivität von $\sim$ ist dann auch $z \sim y$, d.h. $z \in [y]$.
„$[y] \subseteq [x]$“: Mit der Symmetrie von $\sim$ gilt für $x \sim y$ auch $y \sim x$. Dann folgt wie oben: $[y] \subseteq [x]$.

b) Indirekter Beweis, d.h. wir zeigen: $[x] \cap [y] \neq \emptyset \ \Rightarrow\ [x] = [y]$.
Da $[x] \cap [y] \neq \emptyset$, existiert $z \in [x] \cap [y]$ mit $z \sim x$ und $z \sim y$. Da $z \sim x$, ist auch

$x \sim z$ (Symmetrie). Aus $x \sim z$ und $z \sim y$ folgt, dass $x \sim y$ (Transitivität). Nach 4.5 a) folgt damit $[x] = [y]$.

□

Beispiel:

a) Gleichheitsrelation auf M. Für ein $x \in M$ gilt $[x] = \{x\}$.

b) Sei $M = \mathbb{Z}$ und $\sim$ eine Relation auf M definiert durch: $x \sim y$ genau dann, wenn $x - y$ gerade Zahl ist (Äquivalenzrelation). Es gibt genau 2 Äquivalenzklassen:

$$\begin{aligned}
[0] &= [2] \\
&= [-14668] \\
&= \textit{Menge der geraden ganzen Zahlen} \\
[1] &= [3] \\
&= [-1] \\
&= \{1, 3, 5, 7, \ldots, -1, -3, -5, \ldots\} \\
&= \textit{Menge der ungeraden ganzen Zahlen}
\end{aligned}$$

c) Sei $f : M \to N$ eine Abbildung. Definiere eine Relation $\sim$ auf M: $x \sim y \Leftrightarrow f(x) = f(y)$ (Äquivalenzrelation). Sei $x \in M$. Dann gilt

$$\begin{aligned}
[x] &= \{y \in M : y \sim x\} \\
&= \{y \in M : f(y) = f(x)\} \\
&= f^{-1}(\{f(x)\}) \qquad \textit{volles Urbild von } \{f(x)\} \textit{ bzgl. } f
\end{aligned}$$

Definition 4.6. *a) Zwei Mengen A und B heißen* disjunkt, *falls gilt $A \cap B = \emptyset$.*

b) Sei M eine Menge und sei $\mathcal{Z}$ eine nicht leere Menge von Teilmengen von M, d.h. $\emptyset \neq \mathcal{Z} \subseteq \mathcal{P}(M)$. Wir sagen, dass die Elemente von $\mathcal{Z}$ paarweise disjunkt *sind, falls gilt: Sind $A, B \in \mathcal{Z}$ und ist $A \neq B$, dann ist $A \cap B = \emptyset$.*

c) Sei $\mathcal{Z}$ eine Menge von paarweise disjunkten nicht leeren Teilmengen von M. Dann schreibt man für $\bigcup\limits_{A \in \mathcal{Z}} A$ auch $\biguplus\limits_{A \in \mathcal{Z}} A$ (oder $\dot{\bigcup\limits_{A \in \mathcal{Z}}} A$) und nennt dies die disjunkte Vereinigung *der Elemente von $\mathcal{Z}$.*
Ist außerdem $\biguplus\limits_{A \in \mathcal{Z}} A = M$, so heißt $\mathcal{Z}$ eine Zerlegung *(oder* Partition*) von M.*

Beispiel:

Sei $M = \{1, 2, 3, 4, 5\}$. Die folgende Mengen sind jeweils Zerleungen von M:

$$\begin{aligned} \mathcal{Z}_1 &= \{\{1, 3\}, \{2, 4\}, \{5\}\} \\ \mathcal{Z}_2 &= \{\{1, 2, 3\}, \{4\}, \{5\}\} \\ \mathcal{Z}_3 &= \{\{1, 2, 3, 4, 5\}\} \end{aligned}$$

Satz 4.7. *Sei M eine nicht leere Menge.*

a) Ist $\sim$ eine Äquivalenzrelation auf M und $\mathcal{Z}_\sim$ die Menge der verschiedenen Äquivalenzklassen zu $\sim$, so ist $\mathcal{Z}_\sim$ eine Zerlegung von M.

b) Sei umgekehrt $\mathcal{Z}$ eine Zerlegung von M. Definiere für $x, y \in M : x \sim y \Leftrightarrow x$ und y liegen in derselben Menge $A \in \mathcal{Z}$. Dann ist $\sim$ eine Äquivalenzrelation auf M. Die verschiedenen Äquivalenzklassen sind gerade die $A \in \mathcal{Z}$.

Beweis. a) Nach 4.5 b) sind verschiedene Äquivalenzklassen disjunkt. Also ist $\bigcup_{A \in \mathcal{Z}_\sim} A$ disjunkte Vereinigung. Mit der Reflexivität gilt $x \in [x] \in \mathcal{Z}_\sim$ für alle $x \in M$. Daher $\bigcup_{A \in \mathcal{Z}_\sim} A = M$. Also ist $\mathcal{Z}_\sim$ eine Zerlegung von M.

b) Wir zeigen: $\sim$ ist Äquivalenzrelation.
Sei $x \in M$, dann gilt $x \in A$ für ein $A \in \mathcal{Z}$. D.h. $x \sim x$ (Reflexivität).
Ist $x \sim y$, so liegen x und y in der gleichen Menge $A \in \mathcal{Z}$. Da x und y in der gleichen Menge $A \in \mathcal{Z}$ liegen, gilt auch $y \sim x$ (Symmetrie).
Sei $x \sim y$ und $y \sim z$. Es gibt $A \in \mathcal{Z}$ mit $x, y \in A$ und es gibt $B \in \mathcal{Z}$ mit $y, z \in B$. Dann gilt $y \in A \cap B$, d.h. $A = B$ und damit $x, z \in A$, d.h. $x \sim z$ (Transitivität).

□

Definition 4.8. *Sei $\sim$ eine Äquivalenzrelation auf M, $\mathcal{Z}_\sim$ die Menge der Äquivalenzklassen zu $\sim$. Sei weiter ρ eine Abbildung von $\mathcal{Z}_\sim$ nach M, die aus jeder Äquivalenzklasse genau ein Element auswählt, d.h. $\rho([x]) \in [x]$. (Nach 4.5 b) ist ρ injektiv). Das Bild $\rho(\mathcal{Z}_\sim)$ heißt* Repräsentantensystem *der Äquivalenzklassen zu $\sim$.*

Beispiel:

a) Sei $\mathcal{Z}$ Menge der Äquivalenzklassen zur folgenden Relation über $\mathbb{Z}$: $x \sim y \Leftrightarrow x - y$ gerade. Es gibt genau 2 Äquivalenzklassen:

$$\begin{aligned} [0] &= \{\textit{gerade Zahlen}\} \\ [1] &= \{\textit{ungerade Zahlen}\} \end{aligned}$$

Repräsentantensysteme: $\{0, 1\}$ *oder* $\{646, -17\}$

b) Sei $M = \{$*Spieler vom VFB, Bayern, Werder*$\}$*. Sei* $\sim$ *eine Relation über* M *definiert durch:* $x \sim y \Leftrightarrow x$ *und* y *sind im gleichen Verein. Es gibt 3 Äquivalenzklassen: Vereine. Repräsentantensysteme:* $\{$*Hildebrandt, Kahn, Frings*$\}$ *oder* $\{$*Cacau, Schweinsteiger, Kese*$\}$

5 Natürliche Zahlen und vollständige Induktion

Die Natürliche Zahlen $\mathbb{N}$ lassen sich durch die sogenannten Peano[1]-Axiome beschreiben. Das entscheidende Axiom dabei ist das Induktionsaxiom. Mit Hilfe dessen kann das Induktionsprinzip aufgestellt werden, welches eine der wichtigsten Beweismethoden darstellt.

Bemerkung 5.1. *(Induktionsaxiom) Jede nicht leere Teilmenge A der natürlichen Zahlen besitzt ein kleinstes Element, $min(A)$, das Minimum von A.*

Dies Gilt unter anderem nicht für die Mengen $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\{x \in \mathbb{R} : x > 0\}$.

Satz 5.2. *(Beweisprinzip der vollständigen Induktion) Sei $n_0 \in \mathbb{N}$ fest (z.B. $n_0 = 1$). Für jedes $n \geq n_0$ sei $A(n)$ eine Aussage. Es gelte:*

*(1) $A(n_0)$ ist wahr. (*Induktionsanfang*)*

*(2) Für jedes $n \geq n_0$ ist $A(n) \Rightarrow A(n+1)$ wahr (*Induktionsschritt/-schluss*)*

Dann Aussage $A(n)$ wahr für alle $n \geq n_0$.

Beweis. Setze $X = \{n \in \mathbb{N} : n \geq n_0\}$ und $Y = \{n \in \mathbb{N} : n \geq n_0$ und $A(n)$ wahr$\}$. Wir müssen die Gleichheit von $Y = X$ nachweisen:
„$Y \subseteq X$“: Klar.
„$X \subseteq Y$“: Angenommen es gilt $X \not\subseteq Y$, so gilt $\mathcal{Z} := X \setminus Y \neq \emptyset$. Nach 5.1 enthält $\mathcal{Z}$ ein kleinstes Element n_1. Nach (1) ist $n_0 \in Y$, also $n_1 > n_0$. Dann gilt $n_1 - 1 \geq n_0$, d.h. $n_1 - 1 \in X$. Da $n_1 - 1 < n_1$, ist $n_1 - 1 \notin \mathcal{Z}$. Also: $A(n_1 - 1)$ ist wahr. Mit (2) folgt: (A_{n_1}) ist wahr. Somit gilt $n_1 \in Y$. Dies ist ein Widerspruch zu $n_1 \in X \setminus Y$. □

Beweis per vollständiger Induktion:

Möchte man eine Aussage $\forall n \geq n_0 : A(n)$ per vollständiger Induktion beweisen, so hat man zweierlei zu zeigen:

[1] Guiseppe Peano (1858 - 1932) war ein italienischer Mathematiker.

(1) (Induktionsanfang) $A(n_0)$ ist wahr.

(2) (Induktionsschritt) Sei $n \geq n_0$ und sei $A(n)$ wahr (Induktionsvoraussetzung), so muss man zeigen, dass $A(n+1)$ wahr ist (Induktionsbehauptung).

Man beachte, dass die obigen eingeführten Begriffe „Induktionsanfang“, „Induktionsschritt“, „Induktionsvoraussetzung“ und „Induktionsbehauptung“ zur Orientierung in einem Induktionsbeweis dienen. Sie haben für den eigentlichen Beweis keine relevante Bedeutung.

Beispiel 5.3. *Für jede natürliche Zahl $n \in \mathbb{N}$ gilt die Aussage $A(n) : 1+\ldots+n = \frac{n\cdot(n+1)}{2}$. Dabei stellt $1+\ldots+n$ die Summe der ersten n natürlichen Zahlen dar, also $\sum_{i=0}^{n} i$. Die Darstellung einer Summe als Summenformel werden wir später noch kennenlernen.*

Beweis. Induktionsanfang: $n_0 = 1$.
Linke Seite: 1.
Rechte Seite: $\frac{1\cdot(1+1)}{2} = 1$.
Da $1 = 1$ gilt, ist $A(1)$ wahr.

Induktionsschluss: Sei $n \geq 1$.
Induktionsvoraussetzung: $A(n)$ gilt, d.h. es gilt die Gleichung $1 + \ldots + n = \frac{n\cdot(n+1)}{2}$.
Wir zeigen die Induktionsbehauptung $A(n+1)$, d.h. die Gleichung $1+\ldots+n+(n+1) = \frac{(n+1)\cdot((n+1)+1)}{2}$:

$$\begin{aligned}
1 + \ldots + n + (n+1) &\underset{\text{Ind.-Vor.}}{=} \frac{n\cdot(n+1)}{2} + (n+1) \\
&= \frac{n\cdot(n+1) + 2\cdot(n+1)}{2} \\
&= \frac{n^2 + n + 2\cdot n + 2}{2} \\
&= \frac{n^2 + 3\cdot n + 2}{2} \\
&= \frac{(n+1)\cdot(n+2)}{2} \\
&= \frac{(n+1)\cdot((n+1)+1)}{2}
\end{aligned}$$

□

Ein Beweis durch vollständige Induktion gilt auch für Aussagen über $\mathbb{N}_0$ (d.h. $n_0 = 0$ ist auch möglich). Allgemein können Induktionsbeweise auf rekusriv (bzw. induktiv) definierten Strukturen angewandt werden. Wobei der Induktionsschritt je nach Aufbau der Struktur variiert. Die natürlichen Zahlen $\mathbb{N}$ haben eine rekursive Definition. Die Menge aller aussagenlogischen Formeln ist beispielsweise ebenfalls rekursiv definiert.

Satz 5.4. *(Verschärftes Induktionsprinzip) Seien $A(n)$ und n_0 wie in 5.2. Es gelte:*

(1) (Induktionsanfang) $A(n_0)$ ist wahr.

(2) (Induktionsschritt) Für jedes $n \geq n_0$ ist die folgende Implikation wahr:

$$\underbrace{A(n_0) \wedge \ldots \wedge A(n)}_{Induktionsvoraussetzung} \Rightarrow \underbrace{A(n+1)}_{Induktionsbehauptung}$$

Dann gilt $A(n)$ für alle $n \geq n_0$.

Beweis. Beweis: Angenommen es gelten die Voraussetzungen (1) und (2). Zu zeigen ist: Für alle $n \geq n_0$ gilt $A(n)$. Wir teilen den Beweis zur besseren Übersicht in (I) und (II).

(I) Wir zeigen zunächst per einfacher Induktion: Für alle $n \geq n_0$ gilt die Aussage $B(n)$, wobei $B(n) := \forall k : n_0 \leq k \leq n \Rightarrow A(k)$.
IA: Die Aussage $B(n_0)$ gilt: Für $k = n_0$ gilt $A(n_0)$ nach Voraussetzung (1). Alle anderen k erfüllen die Voraussetzung der Implikation in $B(n_0)$ nicht.
IS: Sei $n \geq n_0$. Angenommen es gelte $B(n) := \forall k : n_0 \leq k \leq n \Rightarrow A(k)$. Da mit $B(n)$ die Aussage $A(n_0) \wedge \ldots \wedge A(n)$ gilt, folgt mit der Voraussetzung (2) die Gültigkeit von $A(n+1)$. Somit gilt $B(n+1)$.

(II) Sei nun $n \geq n_0$, dann gilt die Aussage $B(n)$ (in (I) bewiesen). Aus der Gültigkeit von $B(n)$ folgt mit der Wahl von $k = n$ die Gültigkeit von $A(n)$. Da $n \geq n_0$ beliebig war, gilt $A(n)$ für alle $n \geq n_0$.

□

Beispiel 5.5. *Jede natürliche Zahl $n \geq 2$ gilt: n ist Primzahl oder Produkt von Primzahlen.*

Dabei ist eine Primzahl p definiert durch: $p \in \mathbb{N}$ mit $p > 1$ und p besitzt als natürliche Teiler nur die 1 und sich selbst.

Beweis. Wir beweisen die Behauptung per vollständiger Induktion nach 5.4.
Induktionsanfang: $n_0 = 2$.
Es gilt $2 > 1$ und 2 ist nur durch 1 und sich selbst teilbar. Somit ist 2 eine Primzahl.

Induktionsschluss: Sei $n \geq 2$.
Induktionsvoraussetzung: Behauptung sei richtig für alle $i \in \mathbb{N}$ mit $2 \leq i \leq n$.
Induktionsbehauptung: Behauptung sei richtig für $n+1$.
Ist $n+1$ Primzahl, dann gilt die Behauptung für $n+1$.

Ist $n+1$ keine Primzahl, dann existieren $k, l \in \mathbb{N}$ mit $1 < k < n+1$, $1 < l < n+1$ und $n+1 = k \cdot l$. Nach Induktionsvoraussetzung gilt die Behauptung für k und l, d.h. k und l sind Primzahlen oder Produkte von Primzahlen. Also ist $n+1 = k \cdot l$ ein Produkt von Primzahlen. □

Beispiel 5.6. *Die* Fakultätsfunktion $n!$ *(gesprochen „n Fakultät“) ist rekursiv definiert durch:*

$$n! : \begin{cases} \mathbb{N}_0 \to \mathbb{N} \\ n \mapsto \begin{cases} 1 & n = 0 \\ n \cdot (n-1)! & n > 0 \end{cases} \end{cases}$$

Konkrete Beispiele: $0! = 0$, $1! = 1$, $4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$.
Die Fakultätsfunktion ist die Aufmultiplizierung der ersten n Elemente: $n! = 1 \cdot \ldots \cdot n$.

Bemerkung 5.7. *(Prinzip der rekursiven Definition) Sei* $n_0 \in \mathbb{N}_0$, $A = \{n \in \mathbb{N}_0 : n \geq n_0\}$. *Sei* $M \neq \emptyset$ *Menge,* $f : A \times M \to M$ *Abbildung,* $s \in M$. *Dann liefert die folgende Vorschrift eine eindeutige Abbildung* $g : A \to M$*:*

(1) (Startwert) $g(n_0) := s$

(2) (Rekursionsschritt) $g(n+1) := f(n, g(n))$ *für alle* $n \geq n_0$

Beispiel:

Wir betrachten die Fakultätsfunktion $n!$ *aus 5.6. Setze* $n_0 = 0$, $M = \mathbb{N}$, $g(n) := n!$ *und* $f(n, y) := (n+1) \cdot y$, *so gilt:*

$$\begin{aligned} 0! &:= 1 \\ (n+1)! &:= f(n, n!) \\ &= (n+1) \cdot n! \end{aligned}$$

Beispiel 5.8. *a) Sei* $x \in \mathbb{R}$. Potenzen *von x sind definiert durch folgende Rekursion:*

$$\begin{aligned} x^0 &:= 1 \\ x^{n+1} &:= x^n \cdot x \qquad \text{für alle } n \in \mathbb{N}, n \geq 0 \end{aligned}$$

b) Wir wollen eine Summen *über eine Folge von reellen Zahlen definieren. Sei diese Folge von reellen Zahlen die folgende:*

$$a : \begin{cases} \mathbb{N}_0 \to \mathbb{R} \\ n \mapsto a_n \end{cases} \qquad \textit{Folge von reellen Zahlen}$$

Für jedes $n \in \mathbb{N}_0$ definiere die Summe $\sum_{k=0}^{n} a_k$ durch:

$$\begin{aligned}\sum_{k=0}^{0} a_k &:= a_0 \\ \sum_{k=0}^{n+1} a_k &:= \left(\sum_{k=0}^{n} a_k\right) + a_{n+1} \qquad \text{für alle } n \geq 0\end{aligned}$$

Das Resultat dieser Definition ist:

$$\sum_{k=0}^{n} a_k = a_0 + \ldots + a_n$$

c) *Das* Produkt $\prod_{k=0}^{n} a_k$ *definieren wir analog zur Summe über eine Folge von reellen Zahlen rekursiv:*

$$\begin{aligned}\prod_{k=0}^{0} a_k &:= a_0 \\ \prod_{k=0}^{n+1} a_k &:= \left(\prod_{k=0}^{n} a_k\right) \cdot a_{n+1} \qquad \text{für alle } n \in \mathbb{N}_0, n \geq 0\end{aligned}$$

Das Resultat dieser Definition ist:

$$\prod_{k=0}^{n} a_k = a_0 \cdot \ldots \cdot a_n$$

d) *Sei $g : \mathbb{N} \to \mathbb{N}$ wie folgt rekursiv definiert:*

$$\begin{aligned}g(1) &:= 2 \\ g(n+1) &:= 3 \cdot g(n) + 4 \qquad \text{für } n \geq 1\end{aligned}$$

Konkrete Beispiele für g:

$$\begin{aligned}g(1) &= 2 \\ g(2) &= 3 \cdot g(1) + 4 \\ &= 10 \\ g(3) &= 3 \cdot g(2) + 4 \\ &= 34\end{aligned}$$

Wir können für die Abbildung g eine geschlossene Form angeben. Es gilt $g(n) = 4 \cdot 3^{n-1} - 2$ für alle $n \in \mathbb{N}$.

Beweis. Wir beweisen die geschlossene Form von g durch vollständige Induktion.
Induktionsanfang: $n = 1$

$$\begin{aligned} g(1) &\underset{\text{Def.}}{=} 2 \\ 4 \cdot 3^{1-1} - 2 &= 4 \cdot 3^0 - 2 \\ &= 2 \end{aligned}$$

Induktionsschritt: $n \to (n+1)$.
Induktionsvoraussetzung: $g(n) = 4 \cdot 3^{n-1} - 2$.
Induktionsbehauptung: $g(n+1) = 4 \cdot 3^{(n+1)-1} - 3$.

$$\begin{aligned} g(n+1) &\underset{\text{Def.}}{=} 3 \cdot g(n) + 4 \\ &\underset{\text{Ind.-Vor.}}{=} 3 \cdot (4 \cdot 3^{n-1} - 2) + 4 \\ &= 4 \cdot 3^n - 6 + 4 \\ &= 4 \cdot 3^{(n+1)-1} - 2 \end{aligned}$$

□

Beispiel 5.9. *Sei $h : \mathbb{N} \to \mathbb{N}$ wie folgt rekursiv definiert:*

$$\begin{aligned} h(1) &:= 1 \\ h(2) &:= 3 \\ h(n+1) &:= 2 \cdot h(n) - h(n-1) \qquad \text{für alle } n \geq 2 \end{aligned}$$

Konkrekte Beispiele für h:

$$\begin{aligned} h(3) &= 2 \cdot h(2) - h(1) \\ &= 5 \\ h(4) &= 2 \cdot h(3) - h(2) \\ &= 7 \end{aligned}$$

Wir vermuten für h die folgende geschlossene Form: $h(n) = 2 \cdot n - 1$ für alle $n \geq 1$.

Beweis. Da wir $h(n+1)$ für den Induktionsschluss verwenden wollen, muss man den Induktionsanfang für $n = 1$ und $n = 2$ zeigen.

Induktionsanfang: $n = 1$, $n = 2$

$$\begin{aligned} h(1) &= 1 \\ &= 1 \cdot 1 - 1 \\ h(2) &= 3 \\ &= 2 \cdot 2 - 1 \end{aligned}$$

Induktionsschluss: Sei $n \geq 2$.

$$\begin{aligned} h(n+1) &= 2 \cdot h(n) - h(n-1) \\ &\underset{\text{IV}}{=} 2 \cdot (2 \cdot n - 1) - (2 \cdot (n-1) - 1) \\ &= 4 \cdot n - 2 - 2 \cdot n + 3 \\ &= 2 \cdot n + 1 \\ &= 2 \cdot (n+1) - 1 \end{aligned}$$

□

Bemerkung 5.10. *Für Summen $\sum_{k=0}^{n} a_k$ und Produkte $\prod_{k=0}^{n} a_k$ gelten folgende Regeln:*

a) Änderung der Summationsgrenzen:

$$\sum_{k=0}^{n} a_k = \sum_{k=1}^{n+1} a_{k-1} \qquad \textit{(entsprechend für Produkte)}$$

Folgende Schreibweisen haben die gleiche Bedeutung:

$$\sum_{k=0}^{n} a_k = \sum_{0 \leq k \leq n} a_k = \sum_{k \in \{0,\ldots,n\}} a_k$$

Sei $A = \{1, \ldots, n\}$, so gilt:

$$\sum_{k=0}^{n} a_k = \sum_{a \in A} a \qquad \textit{(entsprechend für Produkte)}$$

Man schreibt auch $\sum_k a_k$, wenn die untere und die obere Summationsgrenzen aus dem Kontext hervorgehen.

b) Die Summe $\sum_{k=n_0}^{n_1}$ wird definiert wie in 5.8 b) für $n_0 \leq n_1$. Es gilt:

$$\sum_{k=n_0}^{n_1} a_k = \sum_{k=0}^{n_1-n_0} a_{k+n_0} \qquad \textit{(entsprechend für Produkte)}$$

Ist $n_1 < n_0$, so heißt $\sum_{k=n_0}^{n_1} a_k := 0$ die leere Summe *und $\prod_{k=n_0}^{n_1} a_k := 1$ heißt das* leere Produkt.

c) Doppeltsumme*: Sei $f : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{R}$ eine Abbildung mit $(i,j) \in \mathbb{N}_0 \times \mathbb{N}_0 \mapsto f(i,j)$. Es gilt:*

$$\sum_{i=0}^{n} \sum_{j=0}^{m} f(i,j) = \sum_{i=0}^{n} \left(\sum_{j=0}^{m} f(i,j) \right)$$

$$\begin{aligned} &= \sum_{i=0}^{n}(f(i,0)+\ldots+f(i,m)) \\ &= f(0,0)+\ldots+f(0,m)+ \\ &\quad f(1,0)+\ldots+f(1,m)+ \\ &\quad f(n,0)+\ldots+f(n,m) \\ &= \sum_{j=0}^{m}\left(\sum_{i=0}^{n} f(i,j)\right) \end{aligned}$$

Die Vertauschung der Summen ist erlaubt und führt zum gleichen Resultat:

$$\sum_{i=0}^{n}\sum_{j=0}^{m} f(i,j) \;=\; \sum_{j=0}^{m}\sum_{i=0}^{n} f(i,j)$$

Ist $n = m$, so schreibt man auch: $\sum_{i=0}^{n}\sum_{j=0}^{m} f(i,j) = \sum_{i,j=0}^{n} f(i,j)$.

Beispiel:

$$\begin{aligned} \sum_{i=2}^{5}\sum_{j=0}^{3}(i+j+2) &= \sum_{i=2}^{5}(i+2+i+3+i+4+i+5) \\ &= 2+2+2+3+2+4+2+5+ \\ &\quad 3+2+3+3+3+4+3+5+ \\ &\quad 4+2+4+3+4+4+4+5+ \\ &\quad 5+2+5+3+5+4+5+5 \\ &= 112 \end{aligned}$$

d) Es gilt das Distributivgesetz *bei Summen:*

$$a \cdot \sum_{k=0}^{n} b_k \;=\; \sum_{k=0}^{n} a \cdot b_k$$

Beispielsweise gilt auch:

$$\begin{aligned} (a_0+a_1)\sum_{k=0}^{n} b_k &\underset{Distributivgesetz}{=} a_0 \cdot \sum_{k=0}^{n} b_k + a_1 \cdot \sum_{k=0}^{n} b_k \\ &= \sum_{k=0}^{n} a_0 \cdot b_k + \sum_{k=0}^{n} a_1 \cdot b_k \\ &= \sum_{i=0}^{1}\sum_{k=0}^{n} a_i \cdot b_k \end{aligned}$$

Es gilt das verallgemeinerte Distributivgesetz:

$$\left(\sum_{i=0}^{m} a_i\right) \cdot \left(\sum_{k=0}^{n} b_k\right) = \sum_{i=0}^{m}\sum_{k=0}^{n} a_i \cdot b_k$$

Beispiel:

$$\begin{aligned}
\sum_{i=0}^{2}(i+1)\cdot\sum_{k=0}^{2}2\cdot k &= (1+2+3)\cdot(0+2+6)\\
&= 36\\
\sum_{i=0}^{2}\sum_{k=0}^{2}(i+1)\cdot 2\cdot k &= 1\cdot 2+1\cdot 4+2\cdot 2+2\cdot 4+3\cdot 2+3\cdot 4\\
&= 36
\end{aligned}$$

6 Elementare Zahlentheorie

Die Zahlentheorie beschäftigt sich im Allgemeinen um Eigenschaften von Zahlen. In der Elementaren Zahlentheorie, ein Teilgebiet der Zahlentheorie, werden mit Hilfe der ganzen Zahlen, Teilbarkeit von Zahlen und das Rechnen mit Kongruenzen Fragestellungen bearbeitet.
Für die Informatik wichtig ist außerdem die Darstellung von Zahlen im Binärsystem. Dazu werden wir allgemein Stellenwertsysteme betrachten und wie Zahlen zwischen verschiedenen Stellenwertsystemen übersetzt werden können.

Definition 6.1. *Seien $a, b \in \mathbb{Z}$ und $b \neq 0$. Die Zahl b heißt* Teiler *von a, falls ein $q \in \mathbb{Z}$ existiert mit $a = b \cdot q$. Die Zahl a heißt* Vielfaches *von b. Wir schreiben dafür auch $b \mid a$. Ist b kein Teiler von a, so schreiben wir $b \nmid a$.*

Man beachte: 0 ist nie ein Teiler.

Beispiele: Es gilt $2 \mid 4$, $-3 \mid 9$, $17 \mid 0$ und $10 \nmid 15$.

Satz 6.2. *Seien $a, b, c, d \in \mathbb{Z}$, so gilt:*

a) Ist $b \mid c$ und $b \mid d$, so gilt $b \mid (k \cdot c + l \cdot d)$ für alle $k, l \in \mathbb{Z}$.

b) Ist $b \mid a$ und $a \neq 0$, so gilt $|b| \leq |a|$.

Dabei ist $|.|$ die Betragsfunktion*, die definiert ist durch:*

$$|x| \quad : \quad \begin{cases} \mathbb{R} \to \mathbb{R}_{\geq 0} \\ x \mapsto \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases} \end{cases}$$

c) Ist $b \mid a$ und $a \mid b$, so gilt $a = \pm b$.

Beweis. a) Übungsaufgabe.

b) Wenn $b \mid a$, so ist $|b| \mid |a|$. Denn es gilt jeweils:
$a > 0$, $b > 0$: $|a| = a = q \cdot b = q \cdot |b|$

$a > 0, b < 0$: $|a| = a = q \cdot b = (-q) \cdot (-b) = (-q) \cdot |b|$
$a < 0, b > 0$: $a = q \cdot b = q \cdot |b| \quad \Leftrightarrow \quad (-a) = |a| = (-q) \cdot |b|$
$a < 0, b < 0$: $a = q \cdot b \quad \Leftrightarrow |a| = (-a) = q \cdot (-b) = q \cdot |b|$
Es existiert also ein $q \in \mathbb{N}$ mit $|a| = q \cdot |b|$, d.h. es gilt $|a| = \underbrace{|b| + \ldots + |b|}_{q\text{-mal}} \geq |b|$.

c) Ist $b \mid a$, d.h. $a = q \cdot b$, und $a \mid b$, d.h. $b = r \cdot a$ für geeignete $q, r \in \mathbb{Z}$, so gilt:

$$\begin{aligned} a \;=\; q \cdot b \;=\; q \cdot r \cdot a \quad &\Leftrightarrow \quad q \cdot r \cdot a - a \;=\; 0 \\ &\Leftrightarrow \quad a \cdot (q \cdot r - 1) \;=\; 0 \end{aligned}$$

Da $a \mid b$ gilt, ist $a \neq 0$. Daraus folgt $q \cdot r = 1$. Somit gilt $q \mid 1$ und $r \mid 1$. Nach b) gilt $|q| \leq 1$ und $|r| \leq 1$. Es gilt weiter $q, r \neq 0$, denn sonst würde gelten $q \cdot r = 0 \neq 1$. Da $q \cdot r = 1$ gilt, folgt $q = \pm 1$ und $r = \pm 1$. Es gibt zwei Möglichkeiten, die diese Bedingung erfüllen: $q = r = 1$ oder $q = r = -1$.
Ist $q = r = 1$ der Fall, so gilt $a = 1 \cdot b = b$.
Ist $q = r = -1$ der Fall, so gilt $a = (-1) \cdot b = -b$.

□

Satz 6.3. *(Division mit Rest) Seien $a, b \in \mathbb{Z}$ und $b \neq 0$. Dann existieren eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit:*

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

(2) $0 \leq r < |b|$

Die Zahl q heißt Quotient*, die Zahl r heißt* Rest*.*

Beweis. Wir betrachten zunächst den Fall $b > 0$. Sei q die größte ganze Zahl mit $q \leq \frac{a}{b}$. Da $b > 0$ ist, gilt $b \cdot q \leq a$. Setze $r = a - q \cdot b \geq 0$. Es gilt (1): $a = q \cdot b + r$.
(2): Gezeigt ist bereits $r \geq 0$. Es bleibt zu zeigen: $r < b$. Angenommen es gilt $r \geq b$, d.h. $r = b + s$ für ein $s \geq 0$, so gilt:

$$\begin{aligned} b + s \;=\; r \;=\; a - q \cdot b \quad &\Leftrightarrow \quad s \;=\; a - q \cdot b - b \;=\; a - (q+1) \cdot b \\ &\Leftrightarrow \quad (q+1) \cdot b \;=\; a - s \;\leq\; a \\ &\Leftrightarrow \quad q + 1 \;\leq\; \frac{a}{b} \end{aligned}$$

Dies ist ein Widerspruch zur Wahl von q. Somit gilt $r < b$.

Sei $b < 0$. Es gilt $a = q \cdot |b| + r$ und $0 \leq r < |b|$ nach dem schon bewiesenen Teil. Es gilt somit weiter $a = q \cdot (-b) + r = (-q) \cdot b + r$.

Wir haben (1) und (2) in Bezug auf die Existenz von q und r nachgewiesen. Als nächstes beweisen wir die Eindeutigkeit von q und r. Angenommen es gilt $a = q_1 \cdot b + r_1 = q_2 \cdot b + r_2$, wobei $0 \leq r_1, r_2 < |b|$. Wir müssen zeigen, dass gilt $q_1 = q_2$ und $r_1 = r_2$. O.B.d.A.[1] sei $r_1 \geq r_2$. Aus obiger Gleichung folgt $(q_1 - q_2) \cdot b + (r_1 - r_2) \underset{(*)}{=} 0$. Es gilt $b \mid 0$ und $b \mid (q_1 - q_2) \cdot b$. Mit 6.2 a) folgt $b \mid (q_1 - q_2) \cdot b + (r_1 - r_2) - (q_1 - q_2) \cdot b = r_1 - r_2$. Angenommen $r_1 \neq r_2$, so gilt $0 < r_1 - r_2 < |b|$. Mit 6.2 b) gilt $|b| \leq |r_1 - r_2| = r_1 - r_2$. Es gilt weiter $r_1 - r_2 < |b| \leq r_1 - r_2$, dies ist ein Widerspruch. Somit gilt $r_1 = r_2$. Dann folgt aus $(*)$: $(q_1 - q_2) \cdot b = 0$. Da $b \neq 0$, ist $q_1 - q_2 = 0$, also $q_1 = q_2$. □

Beispiel:

a	b	q	r
5	2	2	1
5	−2	−2	1
−5	2	−3	1
−5	−2	3	1

Definition 6.4. *Seien $a, b \in \mathbb{Z}$ und $b \neq 0$. Sei $a = q \cdot b + r$ mit $0 \leq r < |b|$ für $q, r \in \mathbb{Z}$ wie in 6.3. Dann heißt a* div *$b := q$ und a* mod *$b := r$, wobei q und r durch a und b eindeutig bestimmt sind, d.h.* div *und* mod *sind Abbildungen wie folgt:*

$$\text{div} \quad : \quad \begin{cases} \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \to \mathbb{Z} \\ (a, b) \mapsto a \text{ div } b \end{cases}$$

$$\text{mod} \quad : \quad \begin{cases} \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \to \mathbb{N}_0 \\ (a, b) \mapsto a \text{ mod } b \end{cases}$$

Beispiele: $16 \text{ mod } 7 = 2$, $16 \text{ div } 7 = 2$, $-5 \text{ mod } 2 = 1$, $-5 \text{ div } 2 = -3$.

Definition 6.5. *Sei $x \in \mathbb{R}$. Wir definieren die* Ceiling-Funktion *wie folgt*

$$\lceil x \rceil \quad := \quad \textit{Kleinste ganze Zahl, die größer oder gleich } x \textit{ ist}$$

und die Floor-Funktion *wie folgt*

$$\lfloor x \rfloor \quad := \quad \textit{Größte ganze Zahl, die kleiner oder gleich } x \textit{ ist}$$

Beispiele: $\lceil 7,23 \rceil = 8$, $\lceil -5,3 \rceil = -5$, $\lceil -17 \rceil = -17$, $\lfloor 7,23 \rfloor = 7$, $\lfloor -5,3 \rfloor = -6$, $\lfloor -17 \rfloor = -17$.

Bemerkung 6.6. *Es gilt* $a \text{ div } b = \begin{cases} \lfloor \frac{a}{b} \rfloor & b > 0 \\ \lceil \frac{a}{b} \rceil & b < 0 \end{cases}$ *und* $a \text{ mod } b = a - b \cdot (a \text{ div } b)$.

[1] O.B.d.A steht für „Ohne Beschränkung der Allgemeinheit“. Damit wird zum Ausdruck gebracht, dass die gemachte Einschränkung nur zur Vereinfachung der Beweisführung dient, nicht jedoch die Gültigkeit der Aussage einschränkt.

Beweis. Übungsaufgabe. □

Beispiele: $16 \text{ div } 7 = \left\lfloor \frac{16}{7} \right\rfloor = 2$, $-5 \text{ div } 2 = \left\lfloor \frac{-5}{2} \right\rfloor = -3$, $5 \text{ div } -2 = \left\lceil \frac{5}{-2} \right\rceil = -2$.

Anwendung für Division mit Rest: Stellenwertsysteme zur Basis b, wobei $b \in \mathbb{N}$ und $b > 1$.

$b = 2$	Binärsystem
$b = 8$	Oktalsystem
$b = 10$	Dezimalsystem
$b = 16$	Hexadezimalsystem

Satz 6.7. *Sei $b \in \mathbb{N}$ und $b > 1$. Jede Zahl $n \in \mathbb{N}_0$ lässt sich darstellen in der Form $n = \sum_{i=0}^{k} x_i \cdot b^i$, wobei gilt:*

(1) $b^k \leq n < b^{k+1}$ für $n > 0$ und $k = 0$ für $n = 0$.

(2) $x_i \in \mathbb{N}_0$ mit $0 \leq x_i \leq b - 1$ und $x_k \neq 0$ für $n \neq 0$

Diese Darstellung ist eindeutig.

Die x_i heißen die Ziffern *der Darstellung von n zur* Basis *b.*

Beweis. Existenz und Eindeutigkeit durch Induktion nach n.
IA: $n = 0$
Setze $x_0 = 0$ und $k = 0$, so gilt

$$0 = \sum_{i=0}^{0} 0 \cdot b^i$$

Andere Möglichkeit gibt es nicht, also eindeutig.

IS: Sei $n > 0$.
IV: Die Aussage gelte für alle $n' \in \mathbb{N}_0$ mit $n' < n$.
Setze $x_0 = n \bmod b$, so gilt $0 \leq x_0 \leq b - 1$ und $n - x_0 = b \cdot n'$. Dabei ist $0 \leq n' < n$, da $b > 1$. Wir wenden die Induktionsvoraussetzung auf n' an: $n' = \sum_{i=0}^{k} x'_i \cdot b^i$, wobei k und x'_i wie in (1) und (2) sind. Setze $x_{i+1} = x'_i$ für $i = 0, \ldots, k$. Dann gilt:

$$\begin{aligned} n &= b \cdot n' + x_0 \\ &= \sum_{i=0}^{k} x'_i \cdot b^{i+1} + x_0 \\ &= \sum_{i=1}^{k+1} x_i \cdot b^{i+1} + x_0 \cdot b^0 \end{aligned}$$

$$= \sum_{i=0}^{k+1} x_i \cdot b^{i+1}$$

Dabei gilt $0 \leq x_i \leq b-1$ für alle $i = 1, \ldots, k+1$.

Zeige: $b^{k+1} \leq n < b^{k+2}$ und $x_{k+1} \neq 0$.
Fall 1: Sei $n' > 0$, so gilt nach IV: $b^k \leq n' < b^{k+1}$, also $b^{k+1} \leq n' \cdot b = n - x_0 \leq n$. Da $n' \leq b^{k+1} - 1$, gilt $b \cdot n' \leq b^{k+2} - b$. Somit gilt $n = b \cdot n' + x_0 \leq b^{k+2} - b + x_0 < b^{k+2} - b + b = b^{k+2}$ und $x_0 < b$, $x_{k+1} = x'_k \neq 0$.
Fall 2: Sei $n' = 0$, so gilt $n = x_0$ und $b^0 = 1 \leq n < b^1$.

Eindeutigkeit: Es gelte $n = \sum_{i=0}^{l} x_i \cdot b^i = \sum_{i=0}^{m} y_i \cdot b^i$ und x_i, y_i, l, m erfüllen (1) und (2). Dann $x_0 = n \bmod b = y_0$ und es gilt:

$$\begin{aligned}
\frac{n - x_0}{b} &= \frac{n - y_0}{b} \\
&= \sum_{i=1}^{l} x_i \cdot b^{i-1} \\
&= \sum_{i=1}^{m} y_i \cdot b^{i-1} \\
&= \sum_{i=0}^{l-1} x_{i+1} \cdot b^i \\
&= \sum_{i=0}^{m-1} y_{i+1} \cdot b^i
\end{aligned}$$

IV: $l - 1 = m - 1$, d.h. $l = m$ und $x_1 = y_1, \ldots, x_m = y_m$. □

Beispiel:

Darstellung der Zahl $(161)_{10}$ *im Binärsystem:*

$161 \bmod 2 = 1$		1
$\frac{161-1}{2} = 80$	$80 \bmod 2 = 0$	0
$\frac{80}{2} = 40$	$40 \bmod 2 = 0$	0
$\frac{40}{2} = 20$	$20 \bmod 2 = 0$	0
$\frac{20}{2} = 10$	$10 \bmod 2 = 0$	0
$\frac{10}{2} = 5$	$5 \bmod 2 = 1$	1
$\frac{5-1}{2} = 2$	$2 \bmod 2 = 0$	0
$\frac{2}{2} = 1$	$1 \bmod 2 = 1$	1

Somit gilt $(10100001)_2 = (161)_{10}$.

Alternativ:

Suche größtes k mit $2^k \leq n$.

Es gilt $2^8 = 256 > 161$ *und* $2^7 = 127 \leq 161$. *Also* $161 - 128 = 33$.
Es gilt $2^5 = 32 \leq 33$. *Also* $33 - 32 = 1$.
Es gilt $2^0 = 1 \leq 1$.

Somit gilt $(161)_{10} = 2^7 + 2^5 + 2^0 = (10100001)_2$.

Hexadezimalsystem:

Basis $b = 16$. *Die Ziffern sind* $(0, 1, \ldots, 9, A, B, C, D, E, F)$, *wobei* $A \hat{=} 10$, $B \hat{=} 11$, $C \hat{=} 12$, $D \hat{=} 13$, $E \hat{=} 14$ *und* $F \hat{=} 15$.

Beispiel:

$$\begin{array}{ll|l} 161 \bmod 16 = 1 & & 1 \\ \frac{161-1}{16} = 10 \hat{=} A & 10 \bmod 16 = 10 & A \end{array}$$

Somit gilt $(A1)_{16} = (161)_{10}$.

Satz 6.8. *(Schnelles Potenzieren) Sei $a \in \mathbb{R}$ und $m \in \mathbb{N}$. Wir wollen a^m berechnen.*

Die übliche Art ist: Bilde a^2, $a^2 \cdot a$, $a^3 \cdot a$, $\ldots$, $a^{m-1} \cdot a$. Bei einem großen m ist dieses Verfahren langsam.

Spezialfall: $m = 2^l$. Bilde a^2, $(a^2)^2 = a^4$, $(a^4)^2$,$\ldots$, $(a^{2^{l-1}})^2$. Das sind l viele Quadrierungen.

Allgemein: Schreibe m in Binärdarstellung: $m = x_k \cdot 2^k + \ldots + x_1 \cdot 2 + x_0$, wobei $x_i \in \{0, 1\}$ und $x_k = 1$. Es gilt:

$$\begin{aligned} a^m &= a^{2^k} \cdot a^{x_{k-1} \cdot 2^{k-1}} \cdot \ldots \cdot a^{x_1 \cdot 2} \cdot a^{x_0} \\ &= \left(a^{2^{k-1}} \cdot a^{x_{k-1} \cdot 2^{k-2}} \cdot \ldots \cdot a^{x_1}\right)^2 \cdot a^{x_0} \\ &= \ldots \\ &= \left(\ldots \left(\left(a^2 \cdot a^{x_{k-1}}\right)^2 \cdot a^{x_{k-2}}\right)^2 \cdot \ldots \cdot a^{x_1}\right)^2 \cdot a^{x_0} \end{aligned}$$

Folgender Algorithmus führt obiges Schema aus:

```
1: Input(a, m)
2: b ← a
3: for j = k − 1 down to 0 do
4:     b ← b^2
5:     if x_j = 1 then
6:         b ← b · a
```

7: ***end if***
8: ***end for***
9: *Output(b)*

Maximal $2 \cdot k$ *viele Multiplikationen, wobei* k *maximal mit* $2^k \leq m$.

Beispiel:

Sei $m = 10^6$, *d.h.* $a^{1000000}$. *Es ist* $(10^6)_{10} = (11110100001001000000)_2$. *Es gilt* $2^{19} = 524288$, *somit sind es* $19 + 7 = 26$ *Multiplikationen.*

Definition 6.9. *Sei* $m \in \mathbb{N}$. *Für* $x, y \in \mathbb{Z}$ *definieren wir die folgende Relation:*

$$x \equiv y \pmod{m} \quad \Leftrightarrow \quad m \mid (x - y)$$

Diese Relation heißt Kongruenzrelation modulo m. *Den Ausdruck* $x \equiv y \pmod{m}$ *liest man als „x Kongruent y modulo m“.*

Satz 6.10. *a) Die Kongruenzrelation modulo m ist eine Äquivalenzrelation.*

b) Wenn $a \equiv b \pmod{m}$, $k \in \mathbb{Z}$, *so ist* $k \cdot a \equiv k \cdot b \pmod{m}$.

Man beachte: Die Umkehrung gilt im Allgemeinen nicht.

c) Es gilt: $a \equiv 0 \pmod{m} \Leftrightarrow m \mid a$.

d) Es gilt: $a \equiv b \pmod{m} \Leftrightarrow a \bmod m = b \bmod m$.
D.h. a und b haben bei Division durch m den gleichen Rest.

e) Es gilt: $a \bmod m \equiv a \pmod{m}$.

Beweis. a) Reflexivität: Es gilt $a \equiv a \pmod{m}$, denn $m \mid (a - a) = 0$ für alle $a \in \mathbb{Z}$.

Symmetrie: Gilt $a \equiv b \pmod{m}$, dann $m \mid (a - b)$, also $m \mid (-1) \cdot (a - b) = b - a$ und damit $b \equiv a \pmod{m}$.

Transitivität: Gilt $a \equiv b \pmod{m}$ und $b \equiv c \pmod{m}$, dann $m \mid (a - b)$ und $m \mid (b - c)$, nach 6.2 a) gilt damit $m \mid (a - b) + (b - c) = a - c$, d.h. $a \equiv c \pmod{m}$.

b)

$$\begin{aligned} & a \equiv b \pmod{m} \\ \Rightarrow \quad & m \mid (a - b) \end{aligned}$$

$$\begin{aligned} &\underset{\text{6.2 a)}}{\Rightarrow} && m \mid k \cdot (a-b) = k \cdot a - k \cdot b \\ &\Rightarrow && k \cdot a \equiv k \cdot b \pmod{m} \end{aligned}$$

Gegenbeispiel für die Umkehrung: Es gilt $3 \cdot 3 \equiv 3 \cdot 1 \pmod 6$, aber $3 \not\equiv 1 \pmod 6$.

c) $a \equiv 0 \pmod m$ gilt nach Definition genau dann, wenn gilt $m \mid (a - 0) = a$.

d) „$\Leftarrow$“: Gilt $a \bmod m = b \bmod m$, d.h. $a = q_1 \cdot m + r$ und $b = q_2 \cdot m + r$, $0 \leq r < m$, so gilt:

$$\begin{aligned} (a-b) &= q_1 \cdot m + r - q_2 \cdot m - r \\ &= q_1 \cdot m - q_2 \cdot m \\ &= (q_1 - q_2) \cdot m \end{aligned}$$

d.h. $m \mid (a - b)$, also $a \equiv b \pmod m$.

„$\Rightarrow$“: Sei $a = q_1 \cdot m + r_1$, $b = q_2 \cdot m + r_2$, wobei $0 \leq r_1, r_2 < m$. Sei O.B.d.A. $r_1 \geq r_2$. Nach Voraussetzung gilt $m \mid (a - b) = (q_1 - q_2) \cdot m + (r_1 - r_2)$. Da $m \mid (q_1 - q_2) \cdot m$, folgt nach 6.2 a), dass gilt $m \mid (r_1 - r_2)$. Wäre $r_1 - r_2 \neq 0$, so gilt nach 6.2 b), dass $m \leq r_1 - r_2$, was einen Widerspruch darstellt zu $0 \leq r_1 - r_2 < m$. Somit gilt $r_1 - r_2 = 0$, d.h. $r_1 = r_2$ und damit gilt $a \bmod m = b \bmod m$.

e) Es gilt $(a \bmod m) \bmod m = a \bmod m$. Nach d) gilt $a \bmod m \equiv a \pmod m$.

□

Wichtig:

Man beachte den Unterschied zwischen $\underbrace{a \bmod m}_{\textit{Zahl}}$ *und* $\underbrace{a \equiv b \pmod m}_{\textit{Relation}}$.

Bei festem m *ist* $\begin{cases} \mathbb{Z} \to \{0, \ldots, m-1\} \\ a \mapsto a \bmod m \end{cases}$ *eine Abbildung.*

Beispiele:

$$\begin{aligned} 17 \bmod 7 &= 10 \bmod 7 \\ &= -4 \bmod 7 \\ &= 3 \end{aligned}$$

$$\begin{aligned} 17 &\equiv 3 \pmod 7 \\ 17 &\equiv 10 \pmod 7 \\ 17 &\equiv -4 \pmod 7 \end{aligned}$$

Satz 6.11. *Die Äquivalenzklassen der Kongruenzrelation modulo m (Äquivalenzklassen* mod m*) sind genau die Mengen $\{r + k \cdot m : \ k \in \mathbb{Z}\}$ für $r = 0, \ldots, m-1$. Ein Repräsentantensystem dieser Äquivalenzklassen ist $\mathbb{Z}_m := \{0, 1, \ldots, m-1\}$.*

Beweis. Folgt aus 6.10 d). □

Beispiel:

Sei $m = 2$. Äquivalenzklassen zu mod 2*:*

$$\begin{aligned} \{2 \cdot k : \ k \in \mathbb{Z}\} &= \textit{Menge der geraden Zahlen} \\ \{1 + 2 \cdot k : \ k \in \mathbb{Z}\} &= \textit{Menge der ungeraden Zahlen} \end{aligned}$$

Ein Repräsentantensystem ist $\mathbb{Z}_2 = \{0, 1\}$.

Satz 6.12. *Seien $a_1 \equiv a_2 \pmod m$ und $b_1 \equiv b_2 \pmod m$. Dann gilt:*

$$\begin{aligned} a_1 + b_1 &\equiv a_2 + b_2 \pmod m \\ a_1 - b_1 &\equiv a_2 - b_2 \pmod m \\ a_1 \cdot b_1 &\equiv a_2 \cdot b_2 \pmod m \end{aligned}$$

Beweis. Nach Voraussetzung gilt $m \mid (a_1 - a_2)$ und $m \mid (b_1 - b_2)$.
Nach 6.2 a) gilt $m \mid (a_1 - a_2) + (b_1 - b_2) = (a_1 + b_1) - (a_2 + b_2)$ und damit folgt $a_1 + b_1 \equiv a_2 + b_2 \pmod m$.
Nach 6.2 a) gilt $m \mid (a_1 - a_2) + (-1) \cdot (b_1 - b_2) = (a_1 - b_1) - (a_2 - b_2)$ und damit folgt $a_1 - b_1 \equiv a_2 - b_2 \pmod m$.
$m \mid (a_1 - a_2) \underset{\text{6.2 a)}}{\Rightarrow} m \mid (a_1 - a_2) \cdot b_1 = a_1 \cdot b_1 - a_2 \cdot b_1$.
$m \mid (b_1 - b_2) \underset{\text{6.2 a)}}{\Rightarrow} m \mid a_2 \cdot (b_1 - b_2) \cdot b_1 = a_2 \cdot b_1 - a_2 \cdot b_2$.
Daraus folgt nach 6.2 a): $m \mid (a_1 \cdot b_1 - a_2 \cdot b_1) + (a_2 \cdot b_1 - a_2 \cdot b_2) = a_1 \cdot b_1 - a_2 \cdot b_2$ und damit $a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod m$. □

Korollar 6.13. *Seien $a, b \in \mathbb{Z}$, so gilt:*

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

Beweis. Nach 6.10 e) gilt $a \bmod m \equiv a \pmod m$ und $b \bmod m \equiv b \pmod m$. Nach 6.12 gilt:

$$\begin{aligned}(a \bmod m) + (b \bmod m) &\equiv a + b \pmod m \\ (a \bmod m) \cdot (b \bmod m) &\equiv a \cdot b \pmod m\end{aligned}$$

Weiter folgt mit 6.10 d):

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

□

Beispiele:

a) Was ist $11 \cdot 12 \cdot 13 \bmod 7$ *? Es gilt:*

$$\begin{aligned}11 \cdot 12 \cdot 13 &= 1761 \\ 1761 &\equiv 1 \pmod 7 \\ 11 \cdot 12 \cdot 13 \bmod 7 &= 1\end{aligned}$$

oder

$$\begin{aligned}11 \cdot 12 \cdot 13 &= 132 \cdot 13 \underset{6.12}{\equiv} (-1) \cdot (-1) = 1 \pmod 7 \\ 11 \cdot 12 \cdot 13 &\underset{6.13}{=} 4 \cdot 5 \cdot 6 = 120 \equiv 1 \pmod 7 \\ 11 \cdot 12 \cdot 13 &\underset{6.12}{\equiv} (-3) \cdot (-2) \cdot (-1) = -6 \equiv 1 \pmod 7\end{aligned}$$

b) Welchen Rest lässt $214934^{1517433}$ *bei Division durch 7?*

$$\begin{aligned}214934^{1517433} \bmod 7 &\underset{6.13}{=} (214934 \bmod 7)^{1517433} \bmod 7 \\ &= ((210000 + 4900 + 35 - 1) \bmod 7)^{1517433} \bmod 7 \\ &\underset{6.13}{=} ((-1) \bmod 7)^{1517433} \bmod 7 \\ &\underset{6.13}{=} (-1)^{1517433} \bmod 7 \\ &= (-1) \bmod 7 \\ &= 6\end{aligned}$$

Definition 6.14. *Seien* $a_1, \ldots, a_r \in \mathbb{Z}$.

a) Ist mindestens ein $a_i \neq 0$*, so ist der* größte gemeinsame Teiler $\mathrm{ggT}(a_1, \ldots, a_r)$ *die größte natürliche Zahl, die alle* $a_1, \ldots, a_r$ *teilt.*
Ist $\mathrm{ggT}(a_1, \ldots, a_r) = 1$*, so heißen* $a_1, \ldots, a_r$ teilerfremd.
Ist $\mathrm{ggT}(a_i, a_j) = 1$ *für alle* i, j *mit* $i \neq j$*, so heißen* $a_1, \ldots, a_r$ paarweise teilerfremd.

b) Sind alle $a_1, \ldots, a_r \neq 0$*, so ist das* kleinste gemeinsame Vielfache $\mathrm{kgV}(a_1, \ldots, a_r)$ *die kleinste natürliche Zahl, die von allen* $a_1, \ldots, a_r$ *geteilt wird.*

Beispiel: Die Zahlen 2, 3, 4 sind teilerfremd, aber nicht paarweise, da $\mathrm{ggT}(2, 4) = 2$.

Bemerkung

Seien $a_1, \ldots, a_r \in \mathbb{Z}$ *und* $a_i \neq 0$ *für alle* $i \in \{1, \ldots, r\}$*, so gilt:*

a) Der $\mathrm{ggT}(a_1, \ldots, a_r)$ *existiert und ist eindeutig bestimmt.*

b) Der $\mathrm{kgV}(a_1, \ldots, a_r)$ *existiert und ist eindeutig bestimmt.*

Beweis. a) Sei $A = \{t \in \mathbb{N} : t \mid a_1 \wedge \ldots \wedge t \mid a_r\}$. Es gilt $1 \in A$. Da $a_i \neq 0$ gilt, folgt nach 6.2 b) $t \in A \Rightarrow t \leq |a_i|$. In der endlichen Menge A existiert eine eindeutig bestimmte größte Zahl, $\mathrm{ggT}(a_1, \ldots, a_r)$.

b) Sei $B = \{t \in \mathbb{N} : a_1 \mid t \wedge \ldots \wedge a_r \mid t\}$. Es gilt $|a_1 \cdot a_2 \cdot \ldots \cdot a_r| \in B$, also $B \neq \emptyset$. Nach Induktionsaxiom 5.1 enthält B ein eindeutig bestimmtes kleinstes Element, $\mathrm{kgV}(a_1, \ldots, a_r)$.

□

Satz 6.15. *(Euklidische Algorithmus[2]) Der folgende Algorithmus berechnet den größten gemeinsamen Teiler zweier ganzer Zahlen a und b, beide nicht gleich 0.*

```
1:  Input(a, b)
2:  if b = 0 then
3:     y ← |a|
4:  end if
5:  if b | a then
6:     y ← |b|
7:  end if
8:  if b ≠ 0 ∧ b ∤ a then
9:     x ← a, y ← b
10:    while x mod y ≠ 0 do
11:       r ← x mod y
12:       x ← y, y ← r
13:    end while
14: end if
15: Output(y)
```

[2]Euklid von Alexandria (365 v.Chr. - 300 v.Chr.) war ein griechischer Mathematiker.

Beispiel:

Seien $a = 48$, $b = -30$.

x	y	$x \bmod y = r$
48	-30	18
-30	18	6
18	6	0

Somit gilt $\mathrm{ggT}(48, -30) = 6$.

Lemma 6.16. *Seien* $q, u, v, w \in \mathbb{Z}$ *und* $u = q \cdot v + w$, *dann gilt* $\mathrm{ggT}(u, v) = \mathrm{ggT}(v, w)$.

Beweis. Es gilt: $(t \mid u \ \wedge \ t \mid v) \underset{\text{6.2 a)}}{\Leftrightarrow} (t \mid u - q \cdot v \ \wedge \ t \mid v) \Leftrightarrow (t \mid w \ \wedge \ t \mid v)$.
Daraus folgt $\mathrm{ggT}(u, v) = \mathrm{ggT}(v, w)$. □

Beweis von 6.15:

Wir brauchen nur den Fall $b \neq 0$ und $b \nmid a$ zu betrachten.
Der Algorithmus bewirkt: $a_0 = a$, $a_1 = b$. $a_0 = q_1 \cdot a_1 + a_2$, $a_1 = q_2 \cdot a_2 + a_3$, …, $a_{n-2} = q_{n-1} \cdot a_{n-1} + a_n$, $a_{n-1} = q_n \cdot a_n + 0$. Für alle a_i mit $i \geq 2$ gilt $a_i \geq 0$ und $a_{i+1} < a_i$. Also terminiert der Algorithmus mit Ausgabe $a_n > 0$. Da $a_1 \nmid a_0$ ist $n \geq 2$. Daher $a_n > 0$. Mit 6.16 gilt:

$$\begin{aligned}
\mathrm{ggT}(a, b) &= \mathrm{ggT}(a_0, a_1) \\
&\underset{6.16}{=} \mathrm{ggT}(a_1, a_2) \\
&\underset{6.16}{=} \mathrm{ggT}(a_2, a_3) \\
&= \dots \\
&\underset{6.16}{=} \mathrm{ggT}(a_{n-1}, a_n) \\
&\underset{6.16}{=} \mathrm{ggT}(a_n, 0) \\
&= a_n
\end{aligned}$$

Satz 6.17. *(Bachet de Méziriac)*[3] *Seien* $a, b \in \mathbb{Z}$, *nicht beide gleich 0, dann existieren* $s, t \in \mathbb{Z}$ *mit* $\mathrm{ggT}(a, b) = s \cdot a + t \cdot b$.

Beweis. Ist $b = 0$, so $\mathrm{ggT}(a, b) = |a| = s \cdot a + t \cdot b$ mit $s = \begin{cases} 1 & a > 0 \\ -1 & a < 0 \end{cases}$.
Ist $b \neq 0$ und $b \mid a$, so $\mathrm{ggT}(a, b) = |b| = 0 \cdot a + t \cdot b$ mit $t = \begin{cases} 1 & b > 0 \\ -1 & b < 0 \end{cases}$.

[3] Claude Gaspard Bachet de Méziriac (1581 - 1638) war ein französischer Mathematiker.

Sei also $b \neq 0$ und $b \nmid a$. Setze $a_0 = a$, $a_1 = b$. Der Euklidischer Algorithmus liefert:

$$\begin{aligned} a_0 &= q_1 \cdot a_1 + a_2 \\ a_1 &= q_2 \cdot a_2 + a_3 \\ &\vdots \\ a_{n-1} &= q_n \cdot a_n + 0 \end{aligned}$$

Dabei ist $a_n = \mathrm{ggT}(a, b)$. Wir zeigen durch Induktion nach j die Existenz von $u_j, v_j \in \mathbb{Z}$ mit $a_j = u_j \cdot a_0 + v_j \cdot a_1$, $j = 0, 1, \ldots, n$.

IA: Sei $j = 0$, so $u_0 = 1$, $v_0 = 0$.
Sei $j = 1$, so $u_1 = 0$, $v_1 = 1$.

IS: Sei $j \geq 2$ für $j \leq n$ und es gelte die Behauptung für alle $0 \leq i < j$. Es gilt:

$$\begin{aligned} a_{j-2} &= u_{j-2} \cdot a_0 + v_{j-2} \cdot a_1 \\ a_{j-1} &= u_{j-1} \cdot a_0 + v_{j-1} \cdot a_1 \\ a_j &= a_{j-2} - q_{j-1} \cdot a_{j-1} \\ &\underset{\text{IV}}{=} u_{j-2} \cdot a_0 + v_{j-2} \cdot a_1 - q_{j-1} \cdot u_{j-1} \cdot a_0 - q_{j-1} \cdot v_{j-1} \cdot a_1 \\ &= (u_{j-2} - q_{j-1} \cdot u_{j-1}) \cdot a_0 + (v_{j-2} - q_{j-1} \cdot v_{j-1}) \cdot a_1 \end{aligned}$$

Setze $u_j = u_{j-2} - q_{j-1} \cdot u_{j-1}$ und $v_j = v_{j-2} - q_{j-1} \cdot v_{j-1}$. Dann gilt $\mathrm{ggT}(a, b) = a_n = u_n \cdot a_0 + v_n \cdot a_1$. □

Satz 6.18. *(Erweiterter Euklidischer Algorithmus) Seien $a, b \in \mathbb{Z}$, nicht beide gleich 0. Der Erweiterte Euklidische Algorithmus (EEA) bestimmt den $\mathrm{ggT}(a, b)$ und $s, t \in \mathbb{Z}$ mit $\mathrm{ggT}(a, b) = s \cdot a + t \cdot b$.*

```
1:  Input(a, b)
2:  if b = 0 then
3:     d ← |a|, t ← 0
4:     if a > 0 then
5:        s ← 1
6:     else
7:        s ← −1
8:     end if
9:  end if
10:
11: if b | a then
12:    d ← |b|, s ← 0
13:    if b > 0 then
14:       t ← 1
15:    else
16:       t ← −1
```

```
17:    end if
18: end if
19:
20: if b ≠ 0    ∧    b ∤ a then
21:    x ← a, y ← b
22:    s_1 ← 1, s_2 ← 0
23:    t_1 ← 0, t_2 ← 1
24:    while x mod y ≠ 0 do
25:       q ← x div y, r ← x mod y
26:       s ← s_1 − q · s_2, t ← t_1 − q · t_2
27:       s_1 ← s_2, s_2 ← s, t_1 ← t_2, t_2 ← t
28:       x ← y, y ← r
29:    end while
30:    d ← y
31: end if
32: Output(d, s, t)
```

Dabei gilt $d = \mathrm{ggT}(a, b) = a \cdot s + t \cdot b$.

Beispiel:

Seien $a = 48$, $b = -30$.

x	mod y	x	y	s_1	s_2	s	t_1	t_2	t	q	r
		48	−30	1	0		0	1			
	18	−30	18	0	1	1	1	1	1	−1	18
	6	18	6	1	2	2	1	3	3	−2	6
	0										

Es ist $\mathrm{ggT}(48, -30) = 6$, $s = 2$ *und* $t = 3$. *Also gilt* $6 = 2 \cdot 48 + 3 \cdot (-30)$.

Korollar 6.19. *Seien* $a, b \in \mathbb{Z}$, *nicht beide gleich 0. So gilt:*

a) $\mathrm{ggT}(a, b) = 1 \quad \Leftrightarrow \quad \exists s, t \in \mathbb{Z} : s \cdot a + t \cdot b = 1$.

b) Ist $c \in \mathbb{Z}$ *mit* $c \mid a$ *und* $c \mid b$, *so gilt* $c \mid \mathrm{ggT}(a, b)$.

Beweis. a) „⇒“: Folgt aus 6.17.

„⇐“: Sei $d = \mathrm{ggT}(a, b)$, so gilt $d \mid a$ und $d \mid b$. Es gilt $d \mid s \cdot a + t \cdot b = 1$ nach 6.2 a) und Voraussetzung. Somit $d = 1$.

b) Nach 6.17 gilt $\mathrm{ggT}(a, b) = s \cdot a + t \cdot b$ für geeignete $s, t \in \mathbb{Z}$. Gilt $c \mid a$ und $c \mid b$, so gilt nach 6.2 a) auch $c \mid s \cdot a + t \cdot b$, also $c \mid \mathrm{ggT}(a, b)$.

□

Satz 6.20. *a) Seien $a_1, \ldots, a_k, b_1, \ldots, b_l \in \mathbb{Z}$. Ist $\mathrm{ggT}(a_i, b_j) = 1$ für alle i, j, dann ist auch $\mathrm{ggT}(a, b) = 1$, wobei $a = a_1 \cdot \ldots \cdot a_k$ und $b = b_1 \cdot \ldots \cdot b_j$.*

b) Ist $a, b, c \in \mathbb{Z}$ und $a \mid b \cdot c$ und $\mathrm{ggT}(a, b) = 1$, so gilt $a \mid c$.

c) Seien $a_1, \ldots, a_k$ paarweise teilerfremde ganze Zahlen und $c \in \mathbb{Z}$, so gilt:

$$a_i \mid c \text{ für alle } i \quad \Rightarrow \quad a_1 \cdot \ldots \cdot a_k \mid c$$

Beweis. a) Induktion nach $k + l$.
IA: Sei $k + l = 2$. Dann $a = a_1$ und $b = b_1$ und somit $\mathrm{ggT}(a_1, b_1) = 1 = \mathrm{ggT}(a, b)$.

IS: Sei $k + l = m + 1$ mit $m \geq 2$.
IV: Behauptung sei richtig für alle $k + l = i$ mit $2 \leq i \leq m$.
Sei O.B.d.A. $k \geq l$. Setze $a' = a_1 \cdot \ldots \cdot a_{k-1}$, so gilt nach Induktionsvoraussetzung $\mathrm{ggT}(a', b) = 1$ und $\mathrm{ggT}(a_k, b) = 1$. Mit 6.17 folgt: $\exists s, s', t, t' \in \mathbb{Z}$ mit:

$$\begin{aligned} s \cdot a_k + t \cdot b &= 1 \\ &= s' \cdot a' + t' \cdot b \end{aligned}$$

Multipliziere diese beiden Gleichungen:

$$\begin{aligned} 1 &= s \cdot s' \cdot a' \cdot a_k + t \cdot s' \cdot b \cdot a' + s \cdot t' \cdot a_k \cdot b + t \cdot t' \cdot b^2 \\ &= s \cdot s' \cdot a + (t \cdot s' \cdot a' + s \cdot t' \cdot a_k + t \cdot t' \cdot b) \cdot b \end{aligned}$$

Mit 6.19 folgt $\mathrm{ggT}(a, b) = 1$.

b) Sei $\mathrm{ggT}(a, b) = 1$. Nach 6.17 gilt $1 = s \cdot a + t \cdot b$ für geeignete $s, t \in \mathbb{Z}$. Multiplizieren der Gleichung mit c ergibt $c = s \cdot a \cdot c + t \cdot b \cdot c$. Es gilt $a \mid s \cdot a \cdot c$ und $a \mid t \cdot b \cdot c$, da $a \mid b \cdot c$. Nach 6.2 a) gilt $a \mid s \cdot a \cdot c + t \cdot b \cdot c = c$.

c) Induktion nach k.
IA: Sei $k = 1$. Klar.

IS: $k \to k + 1$.
Induktionsvoraussetzung: $\underbrace{a_1 \cdot \ldots \cdot a_k}_{=:a'} \mid c$ und $a_{k+1} \mid c$. Also $\exists u, v \in \mathbb{Z}$ mit $c = u \cdot a' = v \cdot a_{k+1}$. Nach a) gilt $\mathrm{ggT}(a', a_{k+1}) = 1$. Mit 6.17 folgt: $\exists s, t \in \mathbb{Z}$: $1 = s \cdot a' + t \cdot a_{k+1}$. Multiplikation dieser Gleichung mit c ergibt:

$$\begin{aligned} c &= c \cdot s \cdot a' + c \cdot t \cdot a_{k+1} \\ &= v \cdot a_{k+1} \cdot s \cdot a' + u \cdot a' \cdot t \cdot a_{k+1} \end{aligned}$$

$$= \quad (v \cdot s + u \cdot t) \cdot a' \cdot a_{k+1}$$

Somit gilt $a_1 \cdot \ldots \cdot a_{k+1} = a' \cdot a_{k+1} \mid c$.

□

Satz 6.21. *Sei $m \in \mathbb{N}$ und $c \in \mathbb{Z}$. Die folgenden Aussagen sind äquivalent:*

(1) $\mathrm{ggT}(c, m) = 1$

(2) $\exists d \in \mathbb{Z}$*:* $c \cdot d \equiv 1 \pmod{m}$

(3) $\forall x, y \in \mathbb{Z}$*:* $c \cdot x \equiv c \cdot y \pmod{m} \Rightarrow x \equiv y \pmod{m}$

Beweis. „(1) ⇒ (2)“: Da $\mathrm{ggT}(c, m) = 1$, folgt mit 6.17: $\exists d, t \in \mathbb{Z}$ mit:

$$\begin{aligned} 1 &= d \cdot c + t \cdot m \\ c \cdot d - 1 &= (-t) \cdot m \end{aligned}$$

d.h. $m \mid (c \cdot d - 1)$, also $c \cdot d \equiv 1 \pmod{m}$.

„(2) ⇒ (3)“: Es existiere ein $d \in \mathbb{Z}$ mit $c \cdot d \equiv 1 \pmod{m}$. Seien $x, y \in \mathbb{Z}$ mit $c \cdot x \equiv c \cdot y \pmod{m}$. Mit 6.12 gilt $c \cdot d \cdot x \equiv x \pmod{m}$, $c \cdot d \cdot x \equiv c \cdot d \cdot y \pmod{m}$ und $c \cdot d \cdot y \equiv y \pmod{m}$. Da es sicht bei $\equiv$ um eine Äquivalenzrelation handelt, folgt $x \equiv y \pmod{m}$.

„(3) ⇒ (1)“: Setze $z := \mathrm{ggT}(c, m)$. Es gilt $c = q_1 \cdot z$ und $m = q_2 \cdot z$ für geeignete $q_1, q_2 \in \mathbb{Z}$, d.h. es gilt $c \cdot q_2 = q_1 \cdot z \cdot q_2 = m \cdot q_1$. Also $m \mid m \cdot q_1 = c \cdot q_2$ und damit:

$$\begin{aligned} c \cdot q_2 &\equiv 0 \pmod{m} \\ c \cdot q_2 &\equiv c \cdot 0 \pmod{m} \end{aligned}$$

Nach (3) gilt $q_2 \equiv 0 \pmod{m}$. Also $m \mid q_2$ und $q_2 \mid m$, wobei $m, q_2 > 0$. Somit $m = q_2$. Dann $z = 1$ und $\mathrm{ggT}(c, m) = 1$. □

Wichtig sind hierbei die Implikationen „(1) ⇒ (2)“ und „(1) ⇒ (3)“.

Bemerkung 6.22. *Die Folgerung „(1) ⇒ (2)“ in 6.21 lautet:*
Seien $c \in \mathbb{Z}$ und $m \in \mathbb{N}$ mit $\mathrm{ggT}(c, m) = 1$, so existiert $d \in \mathbb{Z}$ mit $c \cdot d \equiv 1 \pmod{m}$.

Ist $m \geq 2$, so kann man d so wählen, dass gilt $0 < d < m$. Ersetze dafür d durch $d \bmod m$. Dann ist d eindeutig. Die Zahl d wird mit dem erweiterten Euklidischen Algorithmus bestimmt.

Beispiel:

Bestimme $0 < d < 85$ *mit* $23 \cdot d \equiv 1 \pmod{58}$. *Es ist* $\mathrm{ggT}(23, 58) = 1$. *Also existiert* d *nach 6.21 bzw. 6.22. Wende den erweiterten Euklidischen Algorithmus auf 23 und 58 an:*

$x \bmod y$	x	y	s_1	s_2	s	t_1	t_2	t	q	r
	58	23	1	0		0	1			
12	23	12	0	1	1	1	−2	−2	2	12
11	12	11	1	−1	−1	−2	3	3	1	11
1	11	1	−1	2	2	3	−5	−5	1	1
0										

Es gilt:

$$\begin{aligned} 1 &= 2 \cdot 58 + (-5) \cdot 23 \\ (-5) \cdot 23 &\equiv 1 \pmod{58} \\ (-5) \mod 58 &= \underbrace{53}_{=:d} \end{aligned}$$

Für $d = 53$ *gilt* $53 \cdot 23 \equiv 1 \pmod{58}$.

Bemerkung 6.23. *Satz 6.17 und 6.19 gelten auch für den* ggT *beliebig vieler Zahlen* $a_1, \ldots, a_k \in \mathbb{Z}$, $k \geq 2$, *nicht alle gleich 0. Dann gilt:*

a) $\exists s_1, \ldots, s_k \in \mathbb{Z}$: $s_1 \cdot a_1 + \ldots + s_l \cdot a_k = \mathrm{ggT}(a_1, \ldots, a_k)$.

b) $\mathrm{ggT}(a_1, \ldots, a_k) = \mathrm{ggT}(\mathrm{ggT}(a_1, \ldots, a_{k-1}), a_k)$

Für $k = 2$ *ist dabei* $\mathrm{ggT}(a_1) = |a_1|$ *zu setzen.*

c) Ist $c \mid a_1, \ldots, c \mid a_k$, *so ist* $c \mid \mathrm{ggT}(a_1, \ldots, a_k)$.

Beweis. Siehe 3.14, 3.15 in [WHK04]. □

Definition 6.24. *Eine natürliche Zahl* $p \geq 2$ *heißt* Primzahl, *falls 1 und* p *die einzigen natürlichen Zahlen sind, die* p *teilen. D.h.* $\mathrm{ggT}(k, p) = 1$ *für alle* $1 \leq k \leq p - 1$.

Satz 6.25. *Ist* p *eine Primzahl und gilt* $p \mid a_1 \cdot \ldots \cdot a_n$ *für* $a_i \in \mathbb{Z}$, *so existiert* j *mit* $p \mid a_j$.

Beweis. Falls $p \mid a_n$, so fertig. Also angenommen $p \nmid a_n$. D.h. $\mathrm{ggT}(p, a_n) = 1$. Also gilt nach 6.20 b) $p \mid a_1 \cdot \ldots \cdot a_{n-1}$. Fertig per Induktion. □

Theorem 6.26. *(Fundamentalsatz der elementaren Zahlentheorie) Zu jeder natürlichen Zahl $a \geq 2$ gibt es eindeutig bestimmte paarweise verschiedene Primzahlen $p_1, \ldots, p_n$ und natürliche Zahlen $e_1, \ldots, e_n$ mit*

$$a \quad = \quad p_1^{e-1} \cdot \ldots \cdot p_n^{e_n}$$

Die p_j heißen Primfaktoren *von a. Die Darstellung von a als Produkt von Primzahlen ist bis auf die Reihenfolge eindeutig bestimmt.*

Beweis. Die Existenz der Darstellung gilt nach 5.5.

Eindeutigkeit: Es gelte $a = p_1^{e_1} \cdot \ldots \cdot p_n^{e_n} = q_1^{f_1} \cdot \ldots \cdot q_m^{f_m}$, wobei $e_i, f_j \in \mathbb{N}$ und p_i, f_j Primzahlen, p_i paarweise verschieden, f_j paarweise verschieden.
Zu zeigen: $n = m$ und bei geeigneter Nummerierung gilt $p_i = q_i$, $e_i = f_i$ für $i = 1, \ldots, n$.
Nach 6.25 gilt: Jedes p_i teilt ein q_j, jedes q_k teil ein p_l. D.h. $p_i = q_j$, d.h. $q_k = p_l$. D.h. $n = m$ und bei geeigneter Nummerierung $p_1 = q_1, \ldots, p_n = q_n$.

Angenommen es existiert k mit $e_k \neq f_k$. Sei $e_k < f_k$. Teile beide Seiten durch $p_k^{e_k}$:

$$p_1^{e_1} \cdot \ldots \cdot p_{k-1}^{e_{k-1}} \cdot p_{k+1}^{e_{k+1}} \cdot \ldots \cdot p_n^{e_n} \quad = \quad p_1^{f_1} \cdot \ldots \cdot p_{k-1}^{f_{k-1}} \cdot p_k^{f_k - e_k} \cdot p_{k+1}^{f_{k+1}} \cdot \ldots \cdot p_n^{f_n}$$

Es gilt $f_k - e_k > 0$. Die rechte Seite ist also durch p_k teilbar. D.h. p_k teilt beide Seiten. Mit 6.25 gilt: p_k teilt ein p_j, $j \neq k$. D.h. $p_k = p_j$ für $j \neq k$, dies ist ein Widerspruch. Somit gilt für alle $k = 1, \ldots, n$ gerade $e_k = f_k$. □

Satz 6.27. *(Euklid) Es gibt unendlich viele Primzahlen.*

Beweis. Angenommen es gibt nur endlich viele Primzahlen $p_1, \ldots, p_n$. Bilde $a = p_1 \cdot \ldots \cdot p_n + 1$. Nach 6.26 existiert Primzahl q mit $q \mid a$. Da $p_1, \ldots, p_n$ sämtliche Primzahlen sind, ist $q = p_i$ für ein $i \in \{1, \ldots, n\}$. Dann $q = p_i \mid a - p_1 \cdot \ldots \cdot p_n = 1$, d.h. $q \mid 1$, also $q = 1$, Widerspruch. □

Korollar 6.28. *Seien $a, b \in \mathbb{N}$ mit $a, b \geq 2$. Seien $P(a)$ und $P(b)$ die Menge der Primteiler von a bzw. b, so dass gilt: $a = \prod_{p \in P(a)} p^{n(p)}$ und $b = \prod_{p \in P(b)} p^{m(p)}$. Dabei sind $n(p), m(p) \in \mathbb{N}$ geeignet gewählt. Es gilt:*

$$\begin{aligned} \mathrm{ggT}(a,b) &= \prod_{p \in P(a) \cap P(b)} p^{\min(n(p), m(p))} \\ \mathrm{kgV}(a,b) &= \prod_{p \in P(a) \setminus P(b)} p^{n(p)} \cdot \prod_{p \in P(b) \setminus P(a)} p^{m(p)} \prod_{p \in P(a) \cap P(b)} p^{\max(n(p), m(p))} \end{aligned}$$

Insbesondere gilt $a \cdot b = \mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b)$.

Beweis. Übungsaufgabe. □

Beispiel: Seien $a = 1248$ *und* $b = 3780$. *Es gilt* $a = 2^5 \cdot 3 \cdot 13$ *und* $b = 2^2 \cdot 3^3 \cdot 5 \cdot 7$. *Weiter gilt:*

$$\begin{aligned} \mathrm{ggT}(a,b) &= 2^2 \cdot 3 \\ &= 12 \\ \mathrm{kgV}(a,b) &= 13 \cdot 5 \cdot 7 \cdot 2^5 \cdot 3^3 \\ &= 393120 \end{aligned}$$

Bemerkung 6.29. *Aus 6.28 folgt sofort: Ist* $a \mid c$ *und* $b \mid c$, *so ist* $\mathrm{kgV}(a,b) \mid c$.

Dies gilt auch für $\mathrm{kgV}(a_1, \ldots, a_n)$.

Satz 6.30. *(Chinesischer Restsatz) Seien* $n_1, \ldots, n_r$ *paarweise teilerfremde natürliche Zahlen und* $a_1, \ldots, a_r \in \mathbb{Z}$. *Dann existiert genau eine Zahl* $x \in \mathbb{Z}$ *mit* $0 \leq x \leq n_1 \cdot \ldots \cdot n_r - 1$, *die das folgende Kongruenzsystem löst:*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ &\vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

Beispiel:

$$\begin{aligned} x &\equiv -6 \pmod{13} \\ x &\equiv 5 \pmod{8} \\ x &\equiv 12 \pmod{23} \end{aligned}$$

Für x *muss also gelten:*

$$\begin{aligned} 13 &\mid x + 6 \\ 8 &\mid x - 5 \\ 23 &\mid x - 12 \end{aligned}$$

Beweis. Sei $i \in \{1, \ldots, n\}$ und $N_i := \prod_{j \neq i} n_j$. Nach 6.20 a) gilt $\mathrm{ggT}(n_i, N_i) = 1$. Nach 6.21 existiert $t_i \in \mathbb{Z}$ mit $t_i \cdot N_i \equiv 1 \pmod{n_i}$. Mit 6.12 gilt $a_i \cdot t_i \cdot N_i \equiv a_i \pmod{n_i}$. Außerdem gilt $a_i \cdot t_i \cdot N_i \equiv 0 \pmod{n_j}$ für alle $j \neq i$, da $n_j \mid N_i$. Wir setzen $y = \sum_{i=1}^{r} a_i \cdot t_i \cdot N_i$. Dann gilt $y \equiv a_i \pmod{n_i}$. Wir setzen $x = y \mod n_1 \cdot \ldots \cdot n_r$. Es gilt $0 \leq x \leq n_1 \cdot \ldots \cdot n_r - 1$ und $x \equiv y \pmod{n_1 \cdot \ldots \cdot n_r}$, also $n_1 \cdot \ldots \cdot n_r \mid x - y$ und damit $n_i \mid x - y$ für alle $i = 1, \ldots, r$. Daraus folgt sofort:

$$\begin{aligned} x &\equiv y \pmod{n_i} \qquad \text{für alle } i = 1, \ldots, r \\ x &\equiv a_i \pmod{n_i} \qquad \text{für alle } i = 1, \ldots, r \end{aligned}$$

Eindeutigkeit: Angenommen $0 \leq x_1, x_2 \leq n_1 \cdot \ldots \cdot n_r - 1$ erfüllen die Kongruenzgleichungen, wobei O.B.d.A. $x_1 \geq x_2$. Dann gilt:

$$\begin{aligned} x_1 - x_2 &\underset{6.12}{\equiv} 0 \pmod{n_i} \qquad \text{für alle } i = 1, \ldots, r \\ x_1 - x_2 &\underset{6.20\ \text{c)}}{\equiv} 0 \pmod{n_1 \cdot \ldots \cdot n_r} \end{aligned}$$

Es gilt also $0 \leq x_1 - x_2 \leq n_1 \cdot \ldots \cdot n_r - 1$ und $n_1 \cdot \ldots \cdot n_r \mid x_1 - x_2$. Mit 6.2 b) gilt somit $x_1 - x_2 = 0$, also $x_1 = x_2$. □

Bedeutung:

Das Rechnen mod n_i *ist gegebenfalls mit Maschinenzahlen möglch, während das Rechnen* mod $n_1 \cdot \ldots \cdot n_r$ *gegebenfalls Langzeitarithmetik erfordert.*

Beispiel:

Gibt es ein $x \in \mathbb{N}_0$ *mit* $x^2 + 3 \cdot x - 1 \equiv 0 \pmod{663}$ *? Wenn es eine Lösung gibt, dann auch eine, die zwischen 0 und 663 liegt.*

$$\begin{aligned} y^2 + 3 \cdot y - 1 &\equiv 0 \pmod{663} \\ x &:= y \mod 663 \\ x^2 + 3 \cdot x - 1 &\equiv 0 \pmod{663} \end{aligned}$$

Es gilt $663 = 3 \cdot 13 \cdot 17$. *Versuche Kongruenz* mod 3, mod 13 *und* mod 17 *zu lösen:*

$$\begin{aligned} a_1 &= 1 \\ 1 + 3 \cdot 1 - 1 &\equiv 0 \pmod{3} \\ a_2 &= 5 \\ 25 + 3 \cdot 5 - 1 &\equiv 0 \pmod{13} \\ a_3 &= 3 \\ 9 + 3 \cdot 3 - 1 &\equiv 0 \pmod{17} \end{aligned}$$

Chinesischer Restsatz: Liefert Lösung $0 \leq x \leq 663$ *für das folgende Kongruenzsystem:*

$$\begin{aligned} x &\equiv 1 \pmod{3} \\ x &\equiv 5 \pmod{13} \\ x &\equiv 3 \pmod{17} \end{aligned}$$

Ist dieses x gefunden, so gilt:

$$x^2 + 3 \cdot x - 1 \equiv 0 \pmod{3}$$

$$\begin{aligned} x^2 + 3 \cdot x - 1 &\equiv 0 \pmod{13} \\ x^2 + 3 \cdot x - 1 &\equiv 0 \pmod{17} \end{aligned}$$

Da 3, 13 *und* 17 *paarweise teilerfremd sind, folgt mit 6.20 c), dass gilt* $x^2 + 3 \cdot x - 1 \equiv 0 \pmod{663}$. *Bestimmung von* x *mit Hilfe des Konstruktionsbeweises des Chinesischen Restsatzes:*

n_1	n_2	n_3	N_1	N_2	N_3
3	13	17	$13 \cdot 17 = 221$	$3 \cdot 17 = 51$	$3 \cdot 13 = 39$

Bestimmen von t_1, t_2 *und* t_3 *mit:*

$$\begin{aligned} t_1 \cdot N_1 &\equiv 1 \pmod{3} \\ t_1 \cdot 221 &\equiv 1 \pmod{3} \\ t_1 &= 2 \\ t_2 \cdot N_2 &\equiv 1 \pmod{13} \\ t_2 \cdot 51 &\equiv 1 \pmod{13} \\ t_2 &= 12 \\ t_3 \cdot N_3 &\equiv 1 \pmod{17} \\ t_3 \cdot 39 &\equiv 1 \pmod{17} \\ t_3 &= 7 \end{aligned}$$

Bestimmung von y *und* x*:*

$$\begin{aligned} y &= \sum_{i=1}^{3} a_i \cdot t_i \cdot N_i \\ &= 1 \cdot 2 \cdot 221 + 5 \cdot 12 \cdot 51 + 3 \cdot 7 \cdot 39 \\ &= 4321 \\ x &= y \mod 663 \\ &= 4321 \mod 663 \\ &= 343 \end{aligned}$$

Dieses x *erfüllt Kongruenz* $x^2 + 3 \cdot x - 1 \equiv 0 \pmod{663}$, *denn es gilt:*

$$\begin{aligned} 343^2 + 3 \cdot 343 - 1 &= 118677 \\ &= 663 \cdot 179 \end{aligned}$$

7 Kombinatorik

In der Kombinatorik beschäftigen wir uns hauptsächlich mit Abzähltechniken, wie beispielsweise die Anzahlen von Auswahlen von k Elementen aus n Elementen mit/ohne Wiederholung und mit/ohne Berücksichtigung der Reihenfolge.

Satz 7.1. *Sei $n \in \mathbb{N}$ und seien $M_1, \ldots, M_n$ endliche Mengen, dann gilt $|M_1 \times \ldots \times M_n| = |M_1| \cdot \ldots \cdot |M_n|$.*

Speziell: $M_1 = \ldots = M_n$, so ist $|M^n| = |M|^n$.

Beweis. Wir führen eine Induktion nach n durch. Dabei beginnen wir jedoch mit $n = 2$, da wir die Argumentation in diesem Fall für den Induktionsschritt noch einmal benötigen werden. Der Fall $n = 1$ gilt offensichtlich.

IA: $n = 2$:

$$\begin{aligned} |M_1 \times M_2| &= \left| \bigcup_{y \in M_1} \{y\} \times M_2 \right| \\ &= \sum_{y \in M_1} \underbrace{|\{y\} \times M_2|}_{=|M_2|} \\ &= |M_1| \cdot |M_2| \end{aligned}$$

IS: Sei $n \geq 2$.

$$\begin{aligned} |M_1 \times \ldots \times M_{n+1}| &= |M_1 \times (M_2 \times \ldots \times M_{n+1})| \\ &\underset{\text{I.A.}}{=} |M_1| \cdot |M_2 \times \ldots \times M_{n+1}| \\ &\underset{\text{I.V.}}{=} |M_1| \cdot |M_2| \cdot \ldots \cdot |M_{n+1}| \end{aligned}$$

□

Beispiel: Wieviele Wörter der Länge $n \in \mathbb{N}$ gibt es über dem Alphabet $\{0, 1\}$? Mit obigen Satz sind es $|\{0, 1\}^n| = |\{0, 1\}|^n = 2^n$.

Als nächstes wollen wir uns mit den Anzahlen von bestimmten Auswahlmöglichkeiten beschäftigten. Dabei unterscheidet man vier unterschiedliche Auswahlmöglichkeiten von k Gegenständen aus einer Menge mit n Gegenständen:

- Die Anordnung ist relevant (z.B. Spiel 77) oder auch nicht (z.B. Lotto)
- Wiederholungen sind möglich (z.B. Spiel 77) oder auch nicht (z.B. Lotto)

Bemerkung 7.2. *(Geordnete Auswahl ohne Wiederholung) Sei A eine Menge („Urne“) und seien $g_1, \ldots, g_n \in A$ verschiedene Gegenstände. Wähle nacheinander k davon aus und lege sie der Reihenfolge nach aus (Berücksichtigung der Anrodnung): $g_{i_1}, \ldots, g_{i_k}$ wobei $g_{i_j} \neq g_{i_l}$ für $j \neq l$.*
Fragestellung: Wieviele unterschiedliche Auswahlen gibt es?

Alternative Interpretation: Wieviele verschiedene k-Tupel $(g_{i_1}, \ldots, g_{i_k})$ mit verschiedenen g_{i_j} sind möglich?

Alternative Interpretation: Wieviele Verteilungen von k verschiedenen Gegenständen aus einer Menge mit n Gegenständen auf die Plätze $1, \ldots, k$ gibt es?
Dies kann man beschreiben als injektive Abbildung $f : \{1, \ldots, k\} \to A$, $|A| = n$, mit

$$f = \begin{pmatrix} 1 & \ldots & k \\ g_{i_1} & \ldots & g_{i_k} \end{pmatrix}$$

Definition 7.3. *Wir setzen für $n, k \in \mathbb{N}$:*

$$(n)_k \quad = \quad \begin{cases} n & k = 1 \\ n \cdot (n-1) \cdot \ldots \cdot (n-k+1) & k \geq 2 \end{cases}$$

Man beachte: Es ist $(n)_k = 0$, falls $k > n$.
Für $k \leq n$ gilt: $(n)_k = \frac{n!}{(n-k)!}$. Insbesondere gilt: $(n)_n = n!$.

Satz 7.4. *Es gibt $(n)_k$ viele Auswahlen von k Objekten aus einer Menge mit n Objekten, wenn keine Wiederholungen möglich sind und unter Berücksichtigung der Anordnung.*

Beweis. Falls $k > n$, ist die Anzahl $0 = (n)_k$.

Falls $k \leq n$ (Induktions-Beweis). Betrachte die Zuordnung der gewählten Elemente auf die Plätze 1 bis k:

$$\begin{matrix} 1 & 2 & \ldots & k \\ g_{i_1} & g_{i_2} & \cdots & g_{i_k} \end{matrix}$$

Für das Element g_{i_1} gibt es n-Möglichkeiten.
Für das Element g_{i_2} gibt es $(n-1)$-Möglichkeiten (alles aus A außer g_{i_1}), usw.
Für das Element g_{i_k} gibt es $(n-k+1)$-Möglichkeiten.
Insgesamt $n \cdot (n-1) \cdot \ldots \cdot (n-k+1) = (n)_k$ viele Möglichkeiten. □

Beispiele:

a) Seien $n = 3$, $k = 2$ und $A = \{a, b, c\}$. Alle Auswahlmöglichkeiten ohne Wiederholung und unter Berücksichtigung der Reihenfolge sind (a, b), (a, c), (b, a), (b, c), (c, a), (c, b).
Bestimmung der Anzahl der Möglichkeiten mit Hilfe von 7.4: $(3)_2 = 3 \cdot 2 = 6$.

b) Wieviele Möglichkeiten gibt es für den Rang $1, 2, 3$ am Ende der Saison bei 18 Vereinen? Mit 7.4 gilt: $(18)_3 = 18 \cdot 17 \cdot 16 = 4896$.

Korollar 7.5. *Seien A, B nicht leere Mengen mit $|B| = k$, $|A| = n$. Dann gibt es genau $(n)_k$ injektive Abbildungen $B \to A$.*

Ist insbesondere $|A| = |B| = n$, so gibt es $n!$ verschiedene bijektive Abbildungen von B nach A.

Beweis. Folgt aus 7.4 und 3.5. □

Definition 7.6. *Sei M eine Menge. Eine bijektive Abbildung $M \to M$ heißt* Permutation.

Ist M endlich, $|M| = n$, so gibt es $n!$ Permutationen von M. Die Menge der Permutationen von M wird bezeichnet mit S_n. Eine Permutation $\pi \in S_n$ wird oft beschrieben durch:

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

Beispiele:

a) Sei $M = \{1, 2, 3\}$.

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

b) Es gilt:

n	1	2	3	4	5
$\lvert S_n \rvert$	1	2	6	24	120

Bemerkung 7.7. *(Geordnete Auswahl mit Wiederholungen) Aus einer Urne A mit n Elemente werden k Elemente ausgewählt (mit Wiederholungen). Sei $B = \{1, \dots, k\}$, dann lässt sich eine solche Auswahl durch eine Abbildung* $\begin{pmatrix} 1 & \dots & k \\ a_1 & \dots & a_k \end{pmatrix}$ *beschreiben,*

wobei die $a_i \in A$ nicht notwendig verschieden sind.
Frage: Wieviel solcher Auswahlen bzw. Abbildungen $B \to A$ gibt es?

Alternative Interpretation: Wieviele Möglichkeiten gibt es k Gegenstände mit n Farben zu Färben (Farben dürfen mehrfach vorkommen)?

Satz 7.8. *Es gibt genau n^k geordnete Auswahlen mit möglichen Wiederholungen von k Elementen aus einer Menge A mit n Elementen.*

Beweis. Die gesuchte Anzahl ist $|A^k| \underset{7.1}{=} |A|^k = n^k$. □

Korollar 7.9. *Es gibt genau n^k viele Abbildungen $B \to A$, falls $|B| = k$ und $|A| = n$.*

Bemerkung 7.10. *(Ungeordnete Auswahl ohne Wiederholungen) Fragestellung: Urne mit n vielen verschiedenen Objekten. Wähle k viele aus (ohne Zurücklegen) und lege sie in einen Korb.*
Frage: Wieviele verschiedene Korbfüllungen gibt es?

Andere Interpretation: Wieviele k-elementige Teilmengen hat eine Menge mit n Elementen?

Definition 7.11. *Seien $n, k \in \mathbb{N}_0$. Wir definieren den* Binomialkoeffizient*, gesprochen „n über k“, wie folgt:*

$$\binom{n}{k} := \begin{cases} 0 & k > n \\ \frac{n!}{k! \cdot (n-k)!} & k \leq n \end{cases}$$

Man beachte, dass gilt: $\binom{n}{0} = 1 = \binom{n}{n}$.

Bemerkung 7.12. *a) Für alle $k, n \in \mathbb{N}_0$ mit $k \leq n$ gilt* $\binom{n}{k} = \binom{n}{n-k}$.

b) Für alle $n, k \in \mathbb{N}_0$ mit $0 < k \leq n$ gilt:

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

Beispiel: Pascal'sches Dreieck[1]*:*

$$\begin{array}{ccccccc} & & & \binom{0}{0}=1 & & & \\ & & \binom{1}{0}=1 & & \binom{1}{1}=1 & & \\ & \binom{2}{0}=1 & & \binom{2}{1}=2 & & \binom{2}{2}=1 & \\ \binom{3}{0}=1 & & \binom{3}{1}=3 & & \binom{3}{2}=3 & & \binom{3}{3}=1 \end{array}$$

Satz 7.13. *Die Anzahl der ungeordneten Auswahlen ohne Wiederholungen von k Elementen aus einer Menge mit n Elementen ist genau $\binom{n}{k}$. Dies ist ebenfalls die Anzahl der k-elementigen Teilmengen einer Menge mit n Elementen.*

Beweis. Offensichtlich gilt die Behauptung für $k > n$ und $k = 0$. Sei also $1 \leq k \leq n$. Die Anzahl der geordneten Auswahl ohne Wiederholungen ist nach 7.4 genau $(n)_k$. Je $k!$ dieser geordneten Auswahlen führen zur selben ungeordneten Auswahl. Die Division von $(n)_k$ liefert $\binom{n}{k}$. □

Beispiele:

a) *Seien $A = \{1, 2, 3, 4\}$ und $k = 3$, dann gibt es $(4)_3 = 4 \cdot 3 \cdot 2 = 24$ Möglichkeiten an Auswahlen für die Elemente $1, 2, 4$ mit Anordnung und ohne Wiederholung. Die Auswahlen $(2, 4, 1)$, $(2, 1, 4)$, $(4, 1, 2)$, $(4, 2, 1)$, $(1, 2, 4)$, $(1, 4, 2)$ entsprechen einer geordneten Auswahl aus $\{1, 2, 4\}$ mit 3 Elementen, also $(3)_3 = 3! = 6$. Also gibt es $\frac{(n)_k}{k!} = \frac{n!}{(n-k)!\cdot k!} = \binom{n}{k}$ ungeordnete Auswahlen ohne Wiederholung.*

b) *Lotto: 6 aus 49 (ungeordnete Auswahl, ohne Wiederholungen). Die Anzahl der möglichen Tipps ist:*

$$\begin{aligned} \binom{49}{6} &= \frac{49 \cdot 48 \cdot 47 \cdot 46 \cdot 45 \cdot 44}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6} \\ &= 13983816 \end{aligned}$$

Die Warscheinlichkeit für 6 richtige im Lotto ist $\frac{1}{13983816}$. Die Warscheinlichkeit für 6 richtige mit Zusatzzahl ist $\frac{1}{13983816 \cdot 10}$.

[1] Blaise Pascal (1623 - 1662) war ein französischer Mathematiker.

Die Anzahlmöglichkeiten für Auswahlaufgaben lässt sich zusammenfassen:

k aus n	ohne Wiederholungen	mit Wiederholungen
Anordnung relevant	$(n)_k$	n^k
Anordnung nicht relevant	$\binom{n}{k}$	$\binom{n+k-1}{k}$

Korollar 7.14. *Sei $M = \{0,1\}^n$. Die Anzahl aller 0-1-Folgen in M, die genau an k Stellen eine 1 haben, ist $\binom{n}{k}$.*

Satz 7.15. *(Binomialsatz) Wir setzen $0^0 = 1$. Für alle $a, b \in \mathbb{R}$ und $n \in \mathbb{N}_0$ gilt:*

$$\begin{aligned}(a+b)^n &= \sum_{k=0}^{n} \binom{n}{k} \cdot a^{n-k} \cdot b^k \\ &= a^n \\ &\quad + \binom{n}{1} \cdot a^{n-1} \cdot b^1 \\ &\quad + \binom{n}{2} \cdot a^{n-2} \cdot b^2 \\ &\quad + \dots \\ &\quad + \binom{n}{n-1} \cdot a^1 \cdot b^{n-1} \\ &\quad + b^n\end{aligned}$$

Beweis. Induktion nach n:

IA: $n = 0$

$$\begin{aligned}(a+b)^0 &= 1 \\ &= 1 \cdot a^0 \cdot b^0 \\ &= \sum_{k=0}^{0} \binom{0}{k} \cdot a^{0-k} \cdot b^k\end{aligned}$$

IS: $n \to n+1$

$$\begin{aligned}(a+b)^{n+1} &= (a+b) \cdot (a+b)^n \\ &\underset{\text{I.V.}}{=} (a+b) \cdot \sum_{k=0}^{n} \binom{n}{k} a^{n-k} \cdot b^k \\ &= a \cdot \sum_{k=0}^{n} \binom{n}{k} a^{n-k} \cdot b^k + b \cdot \sum_{k=0}^{n} \binom{n}{k} a^{n-k} \cdot b^k\end{aligned}$$

$$
\begin{aligned}
&= \sum_{k=0}^{n} \binom{n}{k} a^{n-k+1} \cdot b^k + \sum_{k=0}^{n} \binom{n}{k} a^{n-k} \cdot b^{k+1} \\
&= a^{n+1} + \sum_{k=1}^{n} \binom{n}{k} a^{n-k+1} \cdot b^k + \sum_{k=0}^{n-1} \binom{n}{k} a^{n-k} \cdot b^{k+1} + b^{n+1} \\
&= a^{n+1} + \sum_{k=1}^{n} \binom{n}{k} a^{n-k+1} \cdot b^k + \sum_{k=1}^{n} \binom{n}{k-1} a^{n-k+1} \cdot b^k + b^{n+1} \\
&= a^{n+1} + \sum_{k=1}^{n} \left(\binom{n}{k} + \binom{n}{k-1} \right) \cdot a^{n-k+1} \cdot b^k + b^{n+1} \\
&\underset{7.12\ b)}{=} a^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} \cdot a^{n-k+1} \cdot b^k + b^{n+1} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} \cdot a^{(n+1)-k} \cdot b^k
\end{aligned}
$$

□

Korollar 7.16. *Sei M eine endliche Menge mit $|M| = n \in \mathbb{N}_0$, dann gilt $|\mathcal{P}(M)| = 2^n$.*

Beweis. Entweder per Induktion nach n oder:

$$
\begin{aligned}
|\mathcal{P}(M)| &\underset{7.10}{=} \sum_{k=0}^{n} \binom{n}{k} \\
&= \sum_{k=0}^{n} \binom{n}{k} \cdot 1^{n-k} \cdot 1^k \\
&\underset{7.15}{=} (1+1)^n \\
&= 2^n
\end{aligned}
$$

□

Bemerkung 7.17. *(Ungeordnete Auswahl mit Wiederholungen) Fragestellung: Wieviele Möglichkeiten gibt es k Objekte aus n Objekten auszuwählen ohne Berücksichtigung der Anordnung und möglichen Wiederholungen?*

Interpretation als Färbungsproblem: n Farben und k gleiche Kugeln. Wieviele Möglichkeiten gibt es, diese k Kugeln mit jeweils einer dieser n Farben zu färben?

Satz 7.18. *Seien $|A| = n$, $k \in \mathbb{N}_0$. Die folgenden drei Größen sind gleich:*

(1) Die Anzahl der Möglichkeiten, k Elemente aus A ohne Berücksichtigung der Anordnung und mit möglichen Wiederholungen auszuwählen.

(2) Die Anzahl der geordneten n-Tupel $(x_1, \ldots, x_n)$, wobei $x_i \in \mathbb{N}_0$ und $\sum_{i=1}^{n} x_i = k$.

(3) Die Anzahl der $0,1$-Folgen der Länge $n+k-1$, die genau k Einsen haben.

Diese gemeinsame Zahl ist $\binom{n+k-1}{k}$, *wobei $k > n$ möglich ist.*

Beweis. „(1) = (2)“: Sei $A = \{a_1, \ldots, a_n\}$. Jede Auswahl von k Elementen von A ohne Berücksichtigung der Anordnung mit Wiederholungen ordnen wir eindeutig zu $(x_1, \ldots, x_n)$, $x_i \in \mathbb{N}_0$, wobei x_i = Anzahl, wie oft a_i ausgewählt worden ist. Dann gilt $\sum_{i=1}^{n} x_i = k$.

„(2) = (3)“:

$$(x_1, \ldots, x_n) \quad \to \quad (\underbrace{1 \ldots 1}_{\leftarrow x_1 \rightarrow} 0 \underbrace{1 \ldots 1}_{\leftarrow x_2 \rightarrow} 0 \ldots 0 \underbrace{1 \ldots 1}_{\leftarrow x_n \rightarrow}) \in \{0,1\}^{n+k-1}$$

Nach 7.14 ist die Anzahl in (3) gerade $\binom{n+k-1}{k}$. □

Beispiel:

a) Wieviele Möglichkeiten gibt es, 8 gleiche Kugeln mit 3 Farben zu färben? Nach 7.18 sind es: $\binom{10}{8} = \binom{10}{2} = \frac{10 \cdot 9}{2} = 45$.

b) Wieviele Möglichkeiten gibt es, 3 gleiche Kugeln mit 8 Farben zu färben? Nach 7.18 sind es: $\binom{10}{3} = \frac{10 \cdot 9 \cdot 8}{1 \cdot 2 \cdot 3} = 120$.

Satz 7.19. *(Vereinigung von Mengen) Seien A_1, A_2 und A_3 endliche Mengen. Für die Vereingung zweier Mengen A_1 und A_2 gilt:*

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

Für die Vereinigung dreier Mengen A_1, A_2 und A_3 gilt:

$$\begin{aligned} |A_1 \cup A_2 \cup A_3| &= |A_1| + |A_2 \cup A_3| - |A_1 \cap (A_2 \cup A_3)| \\ &= |A_1| + |A_2| + |A_3| - |A_2 \cap A_3| - |(A_1 \cap A_2) \cup (A_1 \cap A_3)| \\ &= |A_1| + |A_2| + |A_3| - |A_2 \cap A_3| \\ &\quad -|A_1 \cap A_2| - |A_1 \cap A_3| + |A_1 \cap A_2 \cap A_3| \end{aligned}$$

Die Abbildung 7.1 visualisiert die Situation für zwei Mengen und die Abbildung 7.2 visualisiert die Situation für drei Mengen.

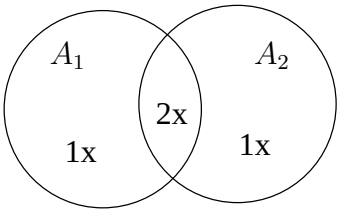


Abbildung 7.1: Vereinigung zweier Mengen

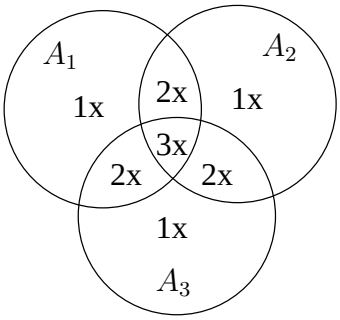


Abbildung 7.2: Vereinigung dreier Mengen

Die Verallgemeinerung dieser Vorgehensweise führt uns zum nächsten Satz:

Satz 7.20. *(Einschließungs-Ausschließungs-Prinzip) Seien $A_1, \ldots, A_n$ endliche Mengen, so gilt:*

$$|A_1 \cup \ldots \cup A_n| \quad = \quad \sum_{j=1}^{n} (-1)^{j+1} \cdot \left(\sum_{1 \leq i_1 < i_2 < \ldots < i_j \leq n} \left| \bigcap_{k=1}^{j} A_{i_k} \right| \right)$$

Beweis. Beweis durch Induktion nach n, siehe Satz 2.32 in [WHK04]. □

Satz 7.21. *Seien A, B nicht leere endliche Mengen mit $|B| = k$, $|A| = n$. Die Anzahl der surjektiven Abbildungen $B \to A$ ist:*

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

Beweis. Sei $Sur(B, A) := \{f : f : B \to A \text{ surjektiv}\}$, $A = \{a_1, \ldots, a_n\}$ und $S_l = \{\varrho : \varrho : B \to A \text{ Abbildung mit } a_l \notin \varrho(B)\}$ für $l = 1, \ldots, n$. Dann gilt:

$$Sur(B, A) \quad = \quad A^B \setminus \bigcup_{l=1}^{n} S_l$$

Dabei ist A^B die Menge aller Abbildungen $B \to A$. Weiter gilt:

$$\begin{aligned} |Sur(B,A)| &= \left|A^B\right| - \left|\bigcup_{l=1}^{n} S_l\right| \\ \left|A^B\right| &\underset{7.8}{=} n^k \end{aligned}$$

Wir bestimmen $|\bigcup_{l=1}^{n} S_l|$ mit Hilfe von 7.20 in mehreren Schritten:

(1) Es gilt:

$$\begin{aligned} |S_l| &= \left|(A \setminus \{a_l\})^B\right| \\ &= (n-1)^k \end{aligned}$$

und es gibt $\binom{n}{1} = n$ viele verschiedene S_l.

(2) Für $i_1 < i_2$ gilt:

$$\begin{aligned} |S_{i_1} \cap S_{i_2}| &= \left|(A \setminus \{a_{i_1}, a_{i_2}\})^B\right| \\ &= (n-2)^k \end{aligned}$$

und es gibt $\binom{n}{2}$ viele solche Schnitte $S_{i_1} \cap S_{i_2}$.

(3) Analog erhält man $\binom{n}{j}$ viele Möglichkeiten für Indizes $1 \leq i_1 < \ldots < i_j \leq n$ und

$$|S_{i_1} \cap \ldots \cap S_{i_j}| = (n-j)^k$$

Nach 7.20 gilt:

$$\begin{aligned} \left|\bigcup_{l=1}^{n} S_l\right| &= \sum_{j=1}^{n} (-1)^{j+1} \cdot \binom{n}{j} \cdot (n-j)^k \\ |Sur(B,A)| &= \left|A^B\right| - \left|\bigcup_{l=1}^{n} S_l\right| \\ &= n^k - \sum_{j=1}^{n} (-1)^{j+1} \cdot \binom{n}{j} \cdot (n-j)^k \\ &= n^k + \sum_{j=1}^{n} (-1)^{j} \cdot \binom{n}{j} \cdot (n-j)^k \end{aligned}$$

$$
\begin{aligned}
&= n^k + \sum_{j=1}^{n-1} (-1)^j \cdot \binom{n}{j} \cdot (n-j)^k \\
&= \sum_{j=0}^{n-1} (-1)^j \cdot \binom{n}{j} \cdot (n-j)^k
\end{aligned}
$$

□

Bemerkung:

Sei $k = n$, *so gilt* $\sum_{j=0}^{n-1} (-1)^j \cdot \binom{n}{j} \cdot (n-j)^n = n!$.

Sei $k < n$, *so gilt* $\sum_{j=0}^{n-1} (-1)^j \cdot \binom{n}{j} \cdot (n-j)^k = 0$.

Beispiele:

a) Seien $k = 5$ *und* $n = 3$, *so gilt:*

$$
\begin{aligned}
\sum_{j=0}^{2} (-1)^j \cdot \binom{3}{j} \cdot (3-j)^5 &= 3^5 - 3 \cdot 2^5 + 3 \\
&= 150
\end{aligned}
$$

b) Seien $k = 3$ *und* $n = 5$, *so gilt:*

$$
\begin{aligned}
\sum_{j=0}^{4} (-1)^j \cdot \binom{5}{j} \cdot (5-j)^3 &= 5^3 - 5 \cdot 4^3 + 10 \cdot 3^3 - 10 \cdot 2^3 + 5 \\
&= 125 - 320 + 270 - 80 + 5 \\
&= 0
\end{aligned}
$$

c) Seien $k = 3$ *und* $n = 3$, *so gilt:*

$$
\begin{aligned}
\sum_{j=0}^{2} (-1)^j \cdot \binom{3}{j} \cdot (3-j)^3 &= 3^3 - 3 \cdot 2^3 + 3 \\
&= 27 - 24 + 3 \\
&= 6 \\
&= 3!
\end{aligned}
$$

Seien A, B Mengen mit $|B| = k$ und $|A| = n$. Die Anzahlen für injektive, surjektive, bijektive Abbildungen lassen sich wie folgt zusammenfassen:

Abbildung $B \to A$	alle	injektive	surjektive	bijektive
Anzahl	n^k	$(n)_k$	$\sum_{j=0}^{n-1}(-1)^j \cdot \binom{n}{j} \cdot (n-j)^k$	$\begin{cases} 0 & k! = n \\ n! & k = n \end{cases}$
Satz	7.9	7.5	7.21	7.9

8 Graphen

Graphen spielen in der Informatk eine wichtige Rolle, insbesondere Baumstrukturen. In diesem Kapitel werden wir verschiedene Graphen betrachten und einige grundlegende Eigenschaften dieser Graphen nachweisen.

Definition 8.1. *Ein* Graph $G = (E, K, \tau)$ *besteht aus den folgenden Komponenten:*

- $E \neq \emptyset$*, Menge der* Ecken *bzw.* Knoten *(engl. vertex, vertices).*
- K*, Menge der* Kanten *(engl. edge).*
- *Es gilt:* $E \cap K = \emptyset$*.*
- τ *Abbildung, die jeder Kante eine nicht leere, aber höchstens 2-elementige Menge* $\{u, v\}$ *von Ecken zuordnet. Die Ecken* u, v *heißen Ecken oder* Endknoten *der betreffenden Kante.*

Man schreibt oft auch nur $G = (E, K)$*, falls* τ *aus der Beschreibung von* G *oder aus dem Kontext hervorgeht.*

Beispiele:

a) Seien $E = \{1, 2, 3, 4, 5, 6\}$ *und* $K = \{k_1, \ldots, k_8\}$ *mit folgender Abbildung* τ*:*

$$\begin{aligned}
\tau(k_1) &= \{1, 2\} \\
&= \tau(k_2) \\
\tau(k_3) &= \{2, 4\} \\
\tau(k_4) &= \{2, 3\} \\
\tau(k_5) &= \{4\} \\
\tau(k_6) &= \{3, 4\} \\
\tau(k_7) &= \{3, 5\} \\
\tau(k_8) &= \{4, 5\}
\end{aligned}$$

Abbildung 8.1 zeigt den Graph visualisiert.

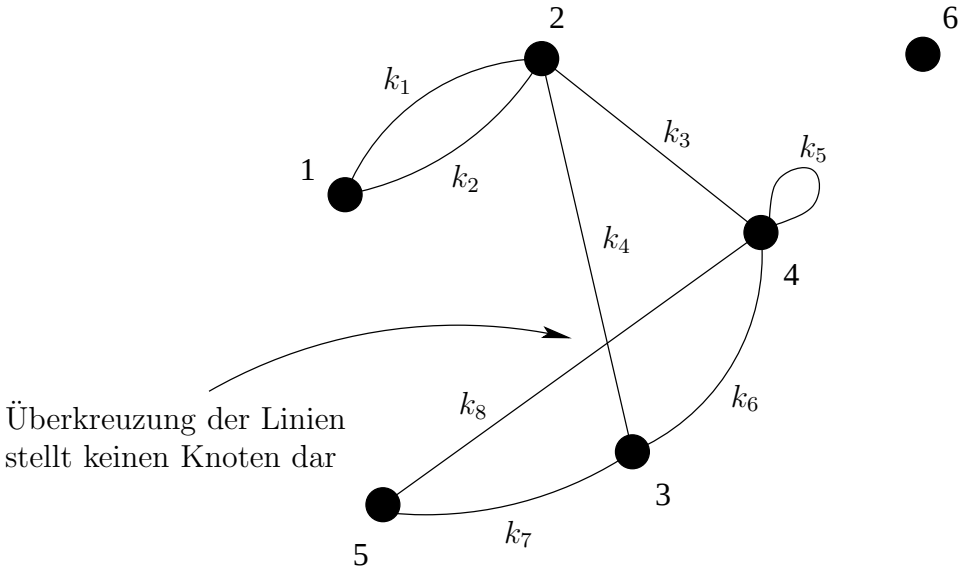


Abbildung 8.1: Visualisierung des Beispielgraphen

b) Landkarte: E = Menge der Städte und K = Menge der Straßen, die benachbarte Städte verbinden.

c) Arbeitszuweisungen: Sei $E = \{P_1, \ldots, P_4, A_1, \ldots, A_5\}$. Abbildung 8.2 zeigt den Beispielgraphen.

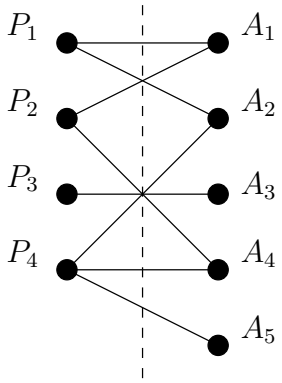


Abbildung 8.2: Ein bipartiter Graph

Ein Graph heißt bipartit*, falls sich die Menge der Knoten in zwei disjunkte Mengen A, B zerlegen lässt. Innerhalb der Menge A bzw. B dürfen keine zwei Knoten durch eine Kante verbunden sein. Kanten zwischen zwei Knoten $a \in A$ und $b \in B$ sind erlaubt.*

d) Ein vollständiger Graph $G = (E, K, \tau)$ *ist definiert durch* $K = \{\{u, v\} : u, v \in E,\ u \neq v\}$ *und* $\tau(A) = A$ *für alle* $A \in K$. *Abbildung 8.3 zeigt einen vollständigen Graphen mit 5 Ecken.*

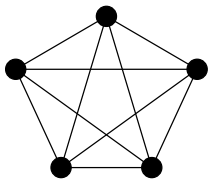


Abbildung 8.3: Ein vollständiger Graph mit 5 Ecken

Anzahl der Kanten: Hat ein vollständiger Graph n Ecken, so gibt es

$$\binom{n}{2} = \frac{n \cdot (n-1)}{2}$$

viele Kanten (Anzahl der 2-elementigen Teilmengen aus n-elementiger Menge).

Definition 8.2. *a) Sei* $G = (E, K, \tau)$ *ein Graph. Eine Kante* $k \in K$ *mit* $|\tau(k)| = 1$ *heißt* Schleife *(engl. loop).*

Beispiel: In Beispiel a) aus 8.1 ist Kante k_5 *eine Schleife.*

b) Ist τ *injektiv (d.h. G hat keine „Mehrfachkanten“) und hat G keine Schleife, so heißt G* schlicht *oder* einfach.

Ist G ein schlichter Graph, so hat jede Kante zwei verschiedene Eckpunkte und durch die Knoten ist die Kante eindeutig bestimmt. K lässt sich identifizieren mit Teilmenge von $\mathcal{P}(E) = \{A \subseteq E : |A| = 2\}$.

Beispiele: Beispiel a) aus 8.1 ist kein schlichter Graph. Beispiel c), d) aus 8.1 sind schlichte Graphen.

Verallgemeinerungen:

Obige Definitionen lassen sich wie folgt verallgemeinern:

- Gerichtete Graphen, *d.h. es gibt Endknoten und Anfangsknoten einer Kante. Abbildung 8.4 zeigt einen gerichteten Graphen.*
- Gewichtete Graphen, *d.h. Kanten haben ein „Gewicht“.*
- *Gerichtet und gewichteter Graph:* Netzwerk

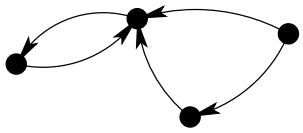


Abbildung 8.4: Ein gerichteter Graph

Im Folgenden geht es nur um endliche Graphen, d.h. E und K sind endlich.

Definition 8.3. *Sei $G = (E, K)$ ein Graph. Der* Grad *(bzw. die* Valenz*) einer Ecke u ist die Anzahl der Kanten, die u als Endknoten besitzen und wird mit $d(u)$ bezeichnet. Eine Schleife mit Ecke u erhöht die Valenz von u um 2.*

Beispiele:

a) Für einen vollständigen Graph mit n Ecken gilt $d(u) = n - 1$ für alle Ecken u.

b) Im Graph aus Beispiel 8.1 a) haben die Ecken folgende Valenzen:

$$\begin{aligned} d(1) &= 2 \\ d(2) &= 4 \\ d(3) &= 3 \\ d(4) &= 5 \\ d(5) &= 2 \\ d(6) &= 0 \end{aligned}$$

Lemma 8.4. *(Handshaking-Lemma) Sei $G = (E, K)$ ein Graph, dann gilt:*

$$\sum_{u \in E} d(u) \quad = \quad 2 \cdot |K|$$

Beweis. (I) Angenommen der Graph G besitzt keine Schleifen. Wir wenden das „Prinzip des doppelten Abzählens“ an:

$$A \quad := \quad \{(u, k) : u \in E,\ k \in K,\ u \text{ ist Endknoten von } k\}$$

Da jede Ecke u Endknoten von genau $d(u)$ vielen Kanten ist, gilt $|A| = \sum_{u \in E} d(u)$. Weiter gilt $|A| = 2 \cdot |K|$, da jede Kante genau 2 Endknoten hat.

(II) Allgemeiner Fall: Jede Schleife führt zu Summand 2 auf beiden Seiten.

□

Korollar 8.5. *In jedem Graph ist die Anzahl der Ecken mit ungerader Valenz gerade.*

Beweis. Mit 8.4 gilt für einen beliebigen Graph $G = (E, K)$:

$$\sum_{u \in E} d(u) = \sum_{u \in \{v \in E : d(v) \text{ gerade}\}} d(u) + \sum_{u \in \{v \in E : d(v) \text{ ungerade}\}} d(u) = 2 \cdot |K|$$

$$\Leftrightarrow \sum_{u \in \{v \in E : d(v) \text{ ungerade}\}} d(u) = \underbrace{2 \cdot |K| - \sum_{u \in \{v \in E : d(v) \text{ gerade}\}} d(u)}_{\text{gerade}}$$

Damit die Summe $\sum_{u \in \{v \in E : d(v) \text{ ungerade}\}} d(u)$ gerade wird, muss die Anzahl der Ecken u mit ungerader Valenz gerade sein. □

Definition 8.6. *Sei $G = (E, K)$ ein Graph.*

a) Eine Folge $(u_0, k_1, u_1, k_2, u_2, \ldots, u_{n-1}, k_n, u_n)$, $u_i \in E$, $k_i \in K$, heißt Kantenzug, *falls u_{i-1} und u_i die Endknoten von k_i sind.*

Ein Kantenzug verbindet *u_0 mit u_n. Dabei ist n die Länge des Kantenzugs. Ein Kantenzug heißt* geschlossen, *wenn $u_0 = u_n$.*

Man beachte: Ist $n = 0$, so Kantenzug (u_0). Ist $n = 1$, so Kantenzug mit einer Kante und deren Eckpunkte.

Beispiel: Abbildung 8.5 enthält beispielsweise den Kantenzug $1a2a1f3$ *und den geschlossenen Kantenzug* $1a2a1f3b2a1$.

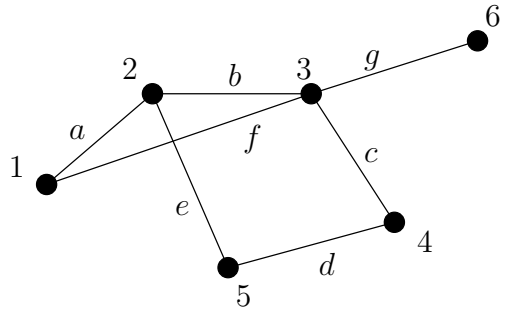


Abbildung 8.5: Beispiel Graph

b) Ein Kantenzug heißt einfach, *falls alle auftretenden Kanten verschieden sind. Auftretende Ecken dürfen jedoch mehrfach vorkommen.*

Beispiel: Die Beispielkantenzüge aus a) sind keine einfachen Kantenzüge. Der Kantenzug $2b3c4d5e2a1$ *ist ein einfacher Kantenzug.*

c) *Ein einfacher Kantenzug* $(u_0, k_1, u_1, k_2, u_2, \ldots, u_{n-1}, k_n, u_n)$ *heißt* Weg*, falls alle* u_i *paarweise verschieden sind (außer eventuell* $u_0 = u_n$*). Ein geschlossener Weg, d.h.* $u_0 = u_n$*, heißt* Kreis*, falls* $n \geq 1$*.*

Beispiel: Der Kantenzug 2*b*3*c*4*d*5*e*2*a*1 *ist einfacher Kantenzug,* 2*b*3*c*4*d*5 *ist ein Weg,* 2*b*3*c*4*d*5*e*2 *ist ein Kreis.*

d) *Ein Graph* G *heißt* zusammenhängend*, falls je zwei Ecken von* G *durch Kantenzug verbunden werden können.*

Bemerkung 8.7. *a) In schlichten Graphen haben alle Kreise Länge* ≥ 3*.*

b) Ein Graph G *ist zusammenhängend genau dann, wenn je zwei Ecken von* G *durch einen Weg verbindbar sind.*

Beweis. a) Kreis der Länge 1: Schleife. Schleife ist im schlichten Graph nicht erlaubt. Kreis der Länge 2: Mehrfachkante. Mehrfachkante ist im schlichten Graph nicht erlaubt.

b) Klar.

□

Definition 8.8. *Ein Graph* G *heißt* Euler'scher Graph[1]*, falls es einen geschlossenen einfachen Kantenzug gibt, der jede Kante enthält. Ein solcher Kantenzug heißt* Euler'scher Kantenzug*.*

Satz 8.9. *Sei Graph* G *ein zusammenhängender Graph, so gilt:*
Ein Graph G *ist ein Euler'scher Graph genau dann, wenn jede Ecke in* G *einen geraden Grad hat.*

Beweis. „⇒“: Sei G ein Euler'scher Graph, dann gibt es einen Euler'schen Kantenzug. In diesem Kantenzug wird jede Ecke von einer Kante angefahren und von einer anderen verlassen. Somit ist der Grad jeder Ecke gerade.

„⇐“: Nach Voraussetzung ist $d(u)$ gerade für alle $u \in E$. Die folgende Vorgehensweise ist in Abbildung 8.6 veranschaulicht.
Beginne bei beliebiger Ecke und durchlaufe so lange verschiedene Kanten wie möglich. Danach ist man wieder beim Anfangspunkt. Angenommen nicht, dann endet man bei einer Ecke, die nicht die Startecke war. Diese Ecke wurde eine gewisse Anzahl angelaufen und wieder verlassen und am Schluss einmal angelaufen: Ungerade Anzahl von Kanten benutzt. Es gibt noch mindestens eine unbenutzte Kante. Dies ist ein Widerspruch.

[1] Leonhard Euler (1707 - 1783) war ein schweizer Mathematiker.

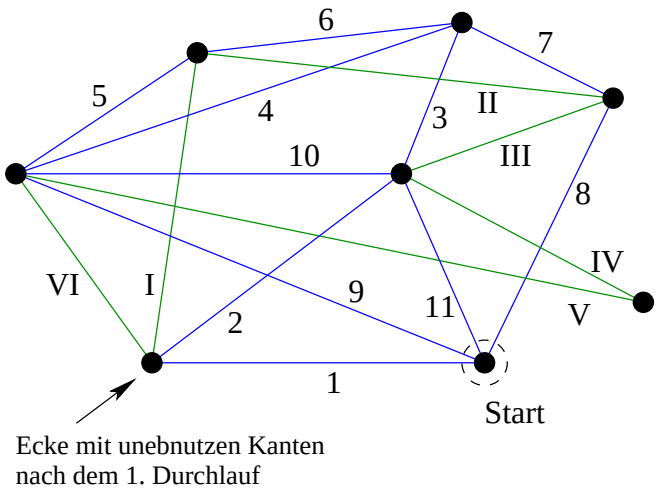


Abbildung 8.6: Bestimmung eines Euler'schen Kantenzugs

Wenn der obige Kantenzug alle Kanten enthält, so fertig. Ansonsten gibt es Ecken in dem Kantenzug, bei dem nicht benutzte Kanten enden (da G zusammenhängend ist). Gehe zu Ecke u im Kantenzug, wo nicht benutzte Kanten enden. An jeder Ecke gerade Anzahl nicht benutzter Kanten. Laufe entlang nicht benutzter Kanten. Endet bei u. Füge neuen Kantenzug ein.

Im Beispiel 8.6: Alter Kantenzug $(1, 2, 3, 4, 5, 6, 7, 8)$ wird zu folgendem Kantenzug $(1, I, II, III, IV, V, VI, 2, 3, 4, 5, 6, 7, 8)$) □

Bemerkung: Härteres Problem

Neben der Frage, ob es einen Euler'schen Kantenzug gibt, kann man auch das schwierigere Problem stellen: Gibt es einen geschlossenen Weg, der alle Ecken enthält? Dies ist ein sogenannter Hamilton Kreis.

Beispiel:

Das Königsberger Brückenproblem *(Euler) stellt die Frage, ob es einen Rundweg gibt, der jede Brücke genau einmal enthält? Graphentheoretische Formulierung: Ecken sind Sandstücke und Kanten sind Brücken. Abbildung 8.7 zeigt den Graph.*
Nach 8.9 handelt es sich hierbei nicht um einen Euler'schen Graphen, da es Ecken gibt, die eine ungeraden Grad besitzen. Somit ist das Problem nicht lösbar.

Definition 8.10. *Ein Graph heißt* Wald*, wenn er keine Kreise enthält. Ein zusammenhängender Wald heißt* Baum.

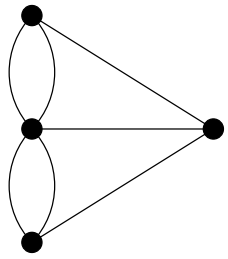


Abbildung 8.7: Graph zum Königsberger Brückenproblem

Man beachte: Wälder sind schlicht, denn eine Schleife oder eine mehrfache Kante wäre ein Kreis im Graphen.

Beispiel: Abbildung 8.8 zeigt einen Wald.

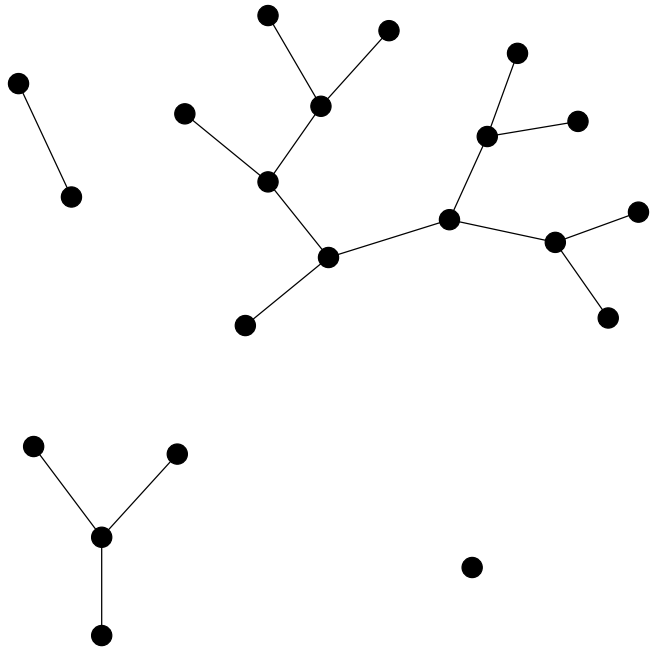


Abbildung 8.8: Ein Wald

Satz 8.11. *Sei $B = (E, K)$ ein Baum mit $|E| \geq 2$. Dann gibt es mindestens zwei Ecken mit Grad 1.*

Beweis. Sei $(u_0, k_1, u_1, \ldots, u_{n-1}, k_n, u_n)$ ein Weg maximaler Länge in B. Da B zusammenhängend ist und $|E| \geq 2$ gilt, gilt $n \geq 1$. Da B keine Kreise enthält, gilt $u_0 \neq u_n$. Wir zeigen: $d(u_0) = d(u_n) = 1$.
Angenommen $d(u_0) > 1$. Dann gibt es Kante $k \neq k_1$ mit Endknoten u_0. Der andere

Endknoten v von k kann nicht in $\{u_0, \ldots, u_n\}$ liegen. Denn sonst gäbe es in B einen Kreis. Somit gibt es mit $(v, k, u_0, k_1, u_1, \ldots, u_{n-1}, k_n, u_n)$ einen längeren Weg im Graph. Dies ist ein Widerspruch zur Maximalität von $u_0 k_1 \ldots k_n u_n$. Somit gilt $d(u_0) = 1$ und mit gleicher Argumentation gilt ebenfalls $d(u_n) = 1$. □

Definition 8.12. *Sei B ein Baum. Dann heißen die Ecken von Grad 1* Blätter. *Die anderen Knoten heißen* innere Knoten.

Lemma 8.13. *Sei $G = (E, K)$ ein zusammenhängender Graph und c ein Kreis in G. Entfernt man in G eine Kante k, die zu c gehört, so ist der Graph $G' = (E, K \setminus \{k\})$ auch zusammenhängend.*

Beweis. Klar. □

Satz 8.14. *Sei $G = (E, K)$ ein Graph. Dann sind folgende Aussagen äquivalent:*

a) Graph G ist Baum.

b) Graph G ist zusammenhängend und es gilt $|K| = |E| - 1$.

Beweis. „a) ⇒ b)“: Sei $G = (E, K)$ ein Baum. Induktion nach $|E|$:
IA: Sei $|E| = n = 1$.
Der Graph G hat keine Kanten, denn eine Kante wäre bei diesem Graphen eine Schleife, was wiederum ein Kreis wäre. Ein Baum enthält per Definition jedoch keine Kreise. Es gilt hier $0 = 1 - 1$ und der Graph ist zusammenhängend.

IS: Sei $|E| = n > 1$.
Nach 8.11 ein existiert $u \in E$ mit $d(u) = 1$. Sei k die eindeutige Kante mit Endknoten u. Setze $G' = (E \setminus \{u\}, K \setminus \{k\})$. G' ist zusammenhängend, da G zusammenhängend und $d(u) = 1$. G' enthält keine Kreise, da G keine Kreise enthält. Also G' ist ein Baum. Per Induktionvoraussetzung gilt:

$$\begin{aligned} |K| - 1 &= |E| - 1 - 1 \\ |K| &= |E| - 1 \end{aligned}$$

„b) ⇒ a)“: Sei Graph G zusammenhängend und es gelte $|K| = |E| - 1$. Wir zeigen: G enthält keine Kreise. Angenommen doch. Entfernt man die Kante k_1 aus dem Kreis, dann nach 8.13 Graph $G' = (E, K \setminus \{k_1\})$ zusammenhängend. Entferne solange Kanten bis kein Kreis mehr existiert. Der Graph $(E, K \setminus \{k_1, \ldots, k_m\})$, der übrig bleibt, ist zusammenhängend ohne Kreis, also ein Baum.
Aus der bereits bewiesenen Implikation „a) ⇒ b)“ folgt $|K| = |E| + m - 1$. Da in der Annahme mindestens ein Kreis vorhanden ist, also $m \geq 1$, führt dies zu einem Widerspruch: $|K| = |E| + m - 1 \neq |E| - 1$. Es muss also $m = 0$ gewesen sein und damit waren keine Kreis im ursprünglichen Graphen und dieser ist somit ein Baum. □

Bemerkung 8.15. *Beweisteil „b) ⇒ a)“ aus 8.14 zeigt: In jedem zusammenhängenden Graphen $G = (E, K)$ existiert eine Teilmenge $K' \subseteq K$, so dass Graph $B = (E, K')$ ein Baum ist. Ein sogenannter* aufspannender Baum.

Korollar 8.16. *Sei $B = (E, K)$ ein Baum. Dann gilt*

$$\sum_{u \in E} d(u) \quad = \quad 2 \cdot |E| - 2$$

Beweis. Folgt aus 8.4 und 8.14. □

Bemerkung 8.17. *Ein Baum, bei dem eine Ecke als Wurzel ausgezeichnet wird, heißt* Wurzelbaum.

Abbildung 8.9 zeigt einen Wurzelbaum, wobei die Wurzel bei solchen Visualisierungen meist oben liegen. Die Anzahl der Niveaus ist die Tiefe *des Baums. In dem beispielhaften*

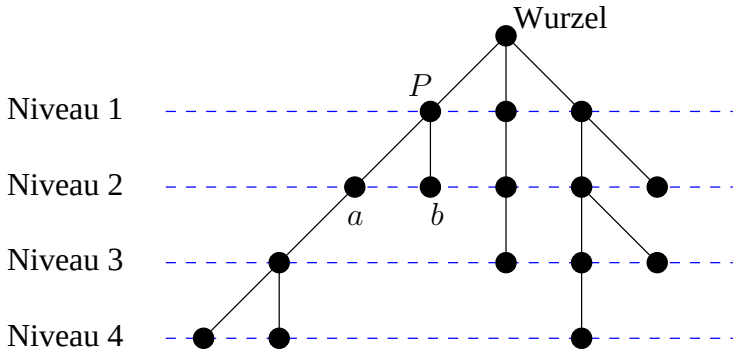


Abbildung 8.9: Ein Wurzelbaum

Wurzelbaum sind a und b „Kinder“ von P bzw. P ist „Elternknoten“ zu a und b.

Bei Wurzelbäumen wird die Wurzel, falls sie Grad 1 hat, nicht als Blatt bezeichnet. Wenn jeder Knoten höchstens zwei Kinder hat, so spricht man von einem Binären Wurzelbaum. *Wenn jeder Knoten (bis auf die Blätter) genau 2 Kinder hat und wenn der Wurzelbaum Tiefe n hat (und jedes Blatt Niveau n hat), so hat der Baum genau 2^n viele Blätter. In der Informatik spielen Bäume eine wichtige Rolle als Datenstruktur für Such- und Sortieralgorithmen.*

9 Formale Aussagenlogik

In der formalen Aussagenlogik werden wir den Formelbegriff aus Kapitel 1 präzise definieren. Dabei spielen die beiden Begriffe Syntax und Semantik eine bedeutende Rolle. Wir werden die konjunktive Normalform und die disjunktive Normalform kennenlernen und darüber hinaus das Resolutionskalkül vorstellen, welches hilft auf syntaktischer Ebene zu entscheiden, ob eine Formel erfüllbar ist.

Definition 9.1. *(Syntax der Aussagenlogik)*

a) Das Alphabet (die verwendeten Zeichen) bestehen aus:

- *V = Menge der Variablen (Aussagenvariablen)*
  Beispiel: $u, v, w, x, y, z, x_1, x_2, \ldots, y_1, y_2, \ldots$
- *Konstanten:* 0 *und* 1.
- *Logische Junktoren:*
  $\neg$: Negationsjunktor
  $\vee$: Disjunktionsjunktor
  $\wedge$: Konjunktionsjunktor
- *Klammern:* (*und*).

b) Ein Ausdruck ist eine Zeichenfolge, die nach gewissen Regeln gebildet werden muss. Induktive Definition:

1) 0, 1 *und alle Variablen sind Ausdrücke (*atomare Ausdrücke*).*

2) Sind A und B Ausdrücke, so auch $(\neg A)$, $(A \vee B)$ und $(A \wedge B)$.

3) Jede Zeichenkette, die durch (mehrfacher, endlich ofter) Anwendung mit Hilfe von 1) und 2) erzeugt werden kann, ist ein Ausdruck *(*aussagenlogische Formel*) und keine anderen.*

Wir bezeichnen mit $\mathcal{A}$ die Menge aller Ausdrücke.

Beispiele:

a) *Folgende Zeichenfolgen sind Ausdrücke:* $(x \vee y)$, $(x \wedge y)$, $(x \wedge 0)$, $((x \vee 1) \wedge (\neg y))$.

b) *Folgende Zeichenfolgen sind* keine *Ausdrücke:* $)x \wedge y$, $x \wedge y$, $x \vee \wedge$, $\neg)x$.

c) *Sind* A, B *Ausdrücke, so ist auch* $((A \vee B) \wedge (\neg(A \wedge B)))$ *ein Ausdruck. Dieser wird abgekürzt mit* $(A \oplus B)$ *oder* $(A \text{ XOR } B)$ *(vgl. 1.4 und Teil a) aus Beispiel 1.5).*

d) *Der Ausdruck* $((\neg A) \vee B)$ *wird abgekürzt mit* $(A \Rightarrow B)$. *Man beachte, dass* $\Rightarrow$ *kein Zeichen des Alphabets ist.*

e) $(((\neg A) \vee B) \wedge ((\neg B) \vee A))$ *wird abgekürzt mit* $(A \Leftrightarrow B)$. *Man beachte, dass* $\Leftrightarrow$ *kein Zeichen des Alphabets ist.*

Die Schreibweise wird häufig vereinfacht durch das Weglassen der äußersten Klammern.

Definition 9.2. *(Semantik der Aussagenlogik) In der Aussagenlogik kommt es* nur *auf die Wahrheitswerte von Aussagen an, nicht auf deren genauen Inhalt. Die Semantik (= Bedeutung) von Ausdrücken erfolgt durch Zuweisung eines Wahrheitswertes* 0 *oder* 1.

Schritt 1: Eine Abbildung $I : V \to \{0, 1\}$ *heißt* Belegung. *Sie legt den Wert der Variablen fest.*

Schritt 2: Man erweitert I *zur Abbildung* $I^* : \mathcal{A} \to \{0, 1\}$ *fort. Die Abbildung* I^* *heißt* Interpretation. *Die Definition von* I^* *ist rekursiv:*

1. $I^*(0) := 0$ *und* $I^*(1) := 1$.
2. *Sei* $x \in V$, *so* $I^*(x) := I(x)$.
3. *Sei* $B = (\neg A)$ *Ausdruck, so* $I^*(B) := 1 - I^*(A)$.
4. *Sei* $B = (A_1 \vee A_2)$ *Ausdruck, so* $I^*(B) = \max(I^*(A_1), I^*(A_2))$.
5. *Sei* $B = (A_1 \wedge A_2)$ *Ausdruck, so* $I^*(B) := \min(I^*(A_1), I^*(A_2))$.

Um alle möglichen Interpretationen von einer Aussage A zu bestimmen, muss man alle Belegungen der in A auftretenden Variablen betrachten, z.B. mit einer Wahrheitswertetabelle.

Beispiel:

Sei $A = (x \vee y) \wedge (\neg(x \wedge y))$ eine Aussage. Man schreibt für A auch $x \oplus y$. Was sind mögliche Wahrheitswerte von A?

$I^*(x)$	$I^*(y)$	$I^*(x \vee y)$	$I^*(x \wedge y)$	$I^*(\neg(x \wedge y))$	$I^*((x \vee y) \wedge (\neg(x \wedge y)))$
1	1	1	1	0	0
1	0	1	0	1	1
0	1	1	0	1	1
0	0	0	0	1	0

Definition 9.3. *a) Ein Ausdruck A heißt* erfüllbar*, wenn es eine Belegung I gibt mit $I^*(A) = 1$.*

b) Ein Ausdruck A heißt Tautologie*, wenn $I^*(A) = 1$ gilt für alle Belegungen I.*

c) Ein Ausdruck A heißt Kontradiktion*, wenn A nicht erfüllbar ist. D.h. es gilt $I^*(A) = 0$ für alle Belegungen von I.*

d) Eine endliche Menge $\mathcal{F} \subseteq \mathcal{A}$ heißt erfüllbar *oder* konsistent*, wenn es eine Belegung I gibt mit $I^*(A) = 1$ für alle $A \in \mathcal{F}$. Eine solche Abbildung I heißt dann* Modell *für $\mathcal{F}$. Gibt es keine solche Belegung, so heißt $\mathcal{F}$* unerfüllbar *oder* kontradiktorisch*.*

Beispiel:

a) Die Ausdrücke $x \vee y$ und $x \wedge y$ sind jeweils erfüllbar, aber keine Tautologie (vgl. 1.2 und 1.3).

b) Der Ausdruck 1 ist eine Tautologie, der Ausdruck 0 ist eine Kontradiktion.

c) Der Ausdruck $\neg A \vee A$ ist eine Tautologie für jeden Ausdruck A.
Der Ausdruck $\neg A \wedge A$ ist eine Kontradiktion für jeden Ausdruck A.

d) Sei $\mathcal{F} = \{(x \vee y) \wedge \neg z,\ z \vee y,\ x,\ \neg y \vee y\}$. $\mathcal{F}$ ist erfüllbar, z.B. mit $I(x) = 1$, $I(y) = 1$ und $I(z) = 0$.

e) Sei $\mathcal{F} = \{\neg x,\ y,\ \neg y \vee x\}$, dann ist $\mathcal{F}$ ist unerfüllbar.

Lemma 9.4. *Sei $\mathcal{F} = \{A_1, \ldots, A_n\}$ endliche Menge von Ausdrücken. Dann ist F erfüllbar genau dann, wenn der Ausdruck $(\ldots((A_1 \wedge A_2) \wedge A_3) \ldots A_n)$ erfüllbar ist.*

Definition 9.5. *Zwei Ausdrücke A und B heißen* logisch äquivalent*, $A \equiv B$, falls für jede Belegung I gilt $I^*(A) = I^*(B)$.*

Man beachte: Das Symbol $\equiv$ ist kein Zeichen der Sprache der Aussagenlogik. Das Symbol $\equiv$ ist ein Zeichen der Metasprache *der Aussagenlogik.*

Bemerkung 9.6. *a) Es gilt $A \equiv B$ genau dann, wenn $A \Leftrightarrow B$ eine Tautologie ist.*

b) $\equiv$ ist eine Äquivalenzrelation auf $\mathcal{A}$. In der Äquivalenzklasse von 1 liegen alle Tautologien, in der Äquivalenzklasse von 0 liegen alle Kontradiktionen.

Satz 9.7. *Seien $A, B, C \in \mathcal{A}$, so gilt:*

a) Doppelte Negation*: $\neg(\neg A) \equiv A$.*

b) Idempotenz*: $A \vee A \equiv A$ und $A \wedge A \equiv A$.*

c) Kommutativität*: $A \vee B \equiv B \vee A$ und $A \wedge B \equiv B \wedge A$.*

d) Assoziativität*: $(A \vee B) \vee C \equiv A \vee (B \vee C)$ und $(A \wedge B) \wedge C \equiv A \wedge (B \wedge C)$.*

e) Distributivität*: $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$ und $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$.*

f) Absorption*: $A \vee (A \wedge B) \equiv A$ und $A \wedge (A \vee B) \equiv A$.*

g) De Morgan'sche Regeln*: $\neg(A \vee B) \equiv \neg A \wedge \neg B$ und $\neg(A \wedge B) \equiv \neg A \vee \neg B$.*

h) $1 \vee A \equiv 1$
$1 \wedge A \equiv A$
$\neg A \vee A \equiv 1$, *d.h. $\neg A \vee A$ ist eine Tautologie.*

i) $0 \vee A \equiv A$
$0 \wedge A \equiv 0$
$\neg A \wedge A \equiv 0$, *d.h. $\neg A \wedge A$ ist eine Kontradiktion.*

Beweis. Wir beweisen nur die erste De Morgan'sche Regel. Sei I eine beliebige Belegung. Dann gilt:

$$\begin{aligned} I^*(\neg(A \vee B)) &= 1 - I^*(A \vee B) \\ &= 1 - \max(I^*(A), I^*(B)) \\ I^*(\neg A \wedge \neg B) &= \min(I^*(\neg A), I^*(\neg B)) \\ &= \min(1 - I^*(A), 1 - I^*(B)) \\ &= 1 - \max(I^*(A), I^*(B)) \end{aligned}$$

Alternativ lässt sich der Beweis auch mit Hilfe einer Wahrheitswertetabelle führen:

$I^*(A)$	$I^*(B)$	$I^*(A \vee B)$	$I^*(\neg(A \vee B))$	$I^*(\neg A)$	$I^*(\neg B)$	$I^*(\neg A \wedge \neg B)$
1	1	1	0	0	0	0
1	0	1	0	0	1	0
0	1	1	0	1	0	0
0	0	0	1	1	1	1

□

Vereinfachte Schreibweise:

Aufgrund der Assoziativität schreiben wir $A \vee B \vee C$ statt $(A \vee B) \vee C$ oder auch $A \wedge B \wedge C$ statt $(A \wedge B) \wedge C$. Desweiteren definieren wir:

$$\begin{aligned} \bigvee_{i=1}^{m} A_i &:= A_1 \vee A_2 \vee \ldots \vee A_m \\ \bigwedge_{i=1}^{m} A_i &:= A_1 \wedge A_2 \wedge \ldots \wedge A_m \end{aligned}$$

Sei I eine Belegung, so gilt:
$I^*\left(\bigvee_{i=1}^{m} A_i\right) = 1$ genau dann, wenn $I^*(A_i) = 1$ für ein $i \in \{1, \ldots, m\}$ gilt.
$I^*\left(\bigwedge_{i=1}^{m} A_i\right) = 1$ genau dann, wenn $I^*(A_i) = 1$ für alle $i \in \{1, \ldots, m\}$ gilt.

Lemma 9.8. *Sei A ein Ausdruck, A_0 ein Teilausdruck von A, d.h. eine zusammenhängende Zeichenfolge in A, die selbst ein Ausdruck ist. Angenommen es gelte $A_0 \equiv B$ für einen Ausdruck B. Ersetzt man in A den Teilausdruck A_0 durch B, so entsteht ein neuer Ausdruck A' mit $A' \equiv A$.*

Beweis. Für jede Belegung I steht bei der Berechnung von $I^*(A')$ an der Stelle, wo $I^*(B)$ auftritt, der gleiche Wert wie $I^*(A_0)$. Alle anderen Teile bleiben gleich. Somit gilt $I^*(A) = I^*(A')$. □

Beispiele:

a)

$$\begin{aligned} \neg(A_1 \wedge A_2 \wedge A_3) &\underset{9.7\ g)}{\equiv} \neg(A_1 \wedge A_2) \vee \neg A_3 \\ &\underset{\substack{9.8 \\ 9.7\ g)}}{\equiv} \neg A_1 \vee \neg A_2 \vee \neg A_3 \end{aligned}$$

b)

$$\begin{aligned} & (A_{11} \vee A_{12}) \wedge (A_{21} \vee A_{22} \vee A_{23}) \\ \underset{9.7\ e)\ c)}{\equiv} \; & ((A_{11} \vee A_{12}) \wedge (A_{21} \vee A_{22})) \vee ((A_{11} \vee A_{12}) \wedge A_{23}) \\ \underset{\substack{9.7\ e)\ c) \\ 9.8}}{\equiv} \; & (((A_{11} \vee A_{12}) \wedge A_{21}) \vee ((A_{11} \vee A_{12}) \wedge A_{22})) \vee \\ & ((A_{11} \wedge A_{23}) \vee (A_{12} \wedge A_{23})) \end{aligned}$$

$$\underset{\substack{9.7\ e)\ c)\\ 9.8}}{\equiv} \quad (A_{11} \wedge A_{21}) \vee (A_{12} \wedge A_{21}) \vee (A_{11} \wedge A_{22}) \vee$$
$$(A_{12} \wedge A_{22}) \vee (A_{11} \wedge A_{23}) \vee (A_{12} \wedge A_{23})$$

Die Beispiele a) und b) lassen sich verallgemeinern und per Induktion und De Morgan bzw. Distributivität beweisen.

Satz 9.9. *a) Verallgemeinerte De Morgan'sche Regeln:*

$$\neg \left(\bigwedge_{i=1}^{m} A_i \right) \equiv \bigvee_{i=1}^{m} \neg A_i$$
$$\neg \left(\bigvee_{i=1}^{m} A_i \right) \equiv \bigwedge_{i=1}^{m} \neg A_i$$

b)

$$(A_{1,1} \vee \ldots \vee A_{1,k_1}) \wedge (A_{2,1} \vee \ldots \vee A_{2,k_2}) \wedge (A_{m,1} \vee \ldots \vee A_{m,k_m})$$
$$\equiv \bigvee_{(i_1,\ldots,i_m) \in \bigtimes_{s=1}^{m} \{1,\ldots,k_s\}} (A_{1,i_1} \wedge A_{2,i_2} \wedge \ldots \wedge A_{m,i_m})$$

Disjunktion von $\prod_{j=1}^{m} k_j$ vielen Ausdrücken, die alle Konjunktionen sind.

Analog gilt die logische Äquivalenz für vertauschte $\wedge$ und $\vee$.

Definition 9.10. *a) Die Ausdrücke x und $\neg x$ für ein $x \in V$, heißen* Literale. *Die Menge der Literale wird bezeichnet mit $\mathcal{L}$.*

b) Im Folgenden seien $p_{i,j}$ Literale.

(i) Ein Ausdruck A ist eine konjunktive Normalform *(*KNF*), falls gilt $A = A_1 \wedge \ldots \wedge A_m$, wobei $A_i = p_{i,1} \vee \ldots \vee p_{i,k_i}$.*

(ii) Ein Ausdruck A ist eine disjunktive Normalform *(*DNF*), falls gilt $A = A_1 \vee \ldots \vee A_m$, wobei $A_i = p_{i,1} \wedge \ldots \wedge p_{i,k_i}$.*

Dabei ist $m = 1$ und $k_i = 1$ möglich.

Theorem 9.11. *Zu jedem Ausdruck $A \in \mathcal{A}$ gibt es eine logisch äquivalente KNF und eine logisch äquivalente DNF (nicht eindeutig bestimmt).*

Beweis. Wir beweisen nur die Existenz der KNF mit Hilfe einer Induktion nach der Anzahl r (r = Rang von A) der in A auftretendenen Junktoren.

IA: $r = 0$ Junktoren.

(1) $A = x$ mit $x \in V$, KNF.

(2) $A = 1$, so $A \equiv x \vee \neg x$, KNF mit $m = 1$, $k_1 = 2$.

(3) $A = 0$, so $A \equiv x \wedge \neg x$, KNF mit $m = 2$, $k_1 = k_2 = 1$.

IS: $r \geq 1$ Junktoren.
IV: Behauptung sei richtig für alle Ausdrücke mit weniger als r Junktoren.

(1) Sei $A = \neg D$. Per Induktion existiert eine KNF für D:

$$D \equiv \bigwedge_{i=1}^{m} \left(\bigvee_{j=1}^{k_i} p_{ij} \right)$$

Weiter gilt:

$$\begin{aligned} A &\underset{9.8}{\equiv} \neg \left(\bigwedge_{i=1}^{m} \left(\bigvee_{j=1}^{k_i} p_{ij} \right) \right) \\ &\underset{9.9\text{ a)}}{\equiv} \bigvee_{i=1}^{m} \left(\bigwedge_{j=1}^{k_i} \neg p_{ij} \right) \\ &\underset{9.9\text{ b)}}{\equiv} \text{KNF} \end{aligned}$$

Dabei muss noch $\neg(\neg x)$ durch x ersetzt werden.

(2) Sei $A = D_1 \wedge D_2$. Nach Induktionsvorausetzung gilt $D_i \equiv D_i'$ wobei D_i' KNF ist für $i = 1, 2$. Nach 9.8 gilt somit $A \equiv D_1' \wedge D_2'$, wobei $D_1' \wedge D_2'$ KNF ist.

(3) Sei $A = D_1 \vee D_2$. Nach Induktionsvorausetzung gilt $D_i \equiv D_i'$ wobei D_i' KNF ist für $i = 1, 2$. Weiter gilt:

$$\begin{aligned} A &\underset{9.8}{\equiv} D_1' \vee D_2' \\ &\equiv \bigwedge_{i=1}^{m_1} \left(\bigvee_{j=1}^{k_i} p_{ij}^{(1)} \right) \vee D_2' \\ &\underset{9.9\text{ b)}}{\equiv} \underbrace{\bigwedge_{i=1}^{m_1} \left(\bigvee_{j=1}^{k_i} p_{ij}^{(1)} \vee D_2' \right)}_{(*)} \end{aligned}$$

$$\bigvee_{j=1}^{k_i} p_{ij}^{(1)} \vee D_2' \equiv \bigvee_{j=1}^{k_i} p_{ij}^{(1)} \vee \left(\bigwedge_{i=1}^{m_2} \left(\bigvee_{j=1}^{l_i} p_{ij}^{(2)} \right) \right)$$

$$\underset{9.9\text{ b)}}{\equiv} \underbrace{\bigwedge_{i=1}^{m_2} \left(\bigvee_{j=1}^{k_i} p_{ij}^{(1)} \vee \bigvee_{j=1}^{l_i} p_{ij}^{(2)} \right)}_{(+)}$$

Audruck $(+)$ ersetzen für $(*)$ liefert eine KNF für A.

□

Beispiel:

$$\begin{aligned}
A &= \neg((x \Rightarrow y) \wedge (y \Rightarrow \neg z)) \\
&= \neg((\neg x \vee y) \wedge (\neg y \vee \neg z)) \\
&\underset{De\ Morgan}{\equiv} \neg(\neg x \vee y) \vee \neg(\neg y \vee \neg z) \\
&\underset{De\ Morgan}{\equiv} (x \wedge \neg y) \vee (y \wedge z) \qquad DNF \\
&\underset{Distributivität}{\equiv} (x \vee (y \wedge z)) \wedge (\neg y \vee (y \wedge z)) \\
&\underset{Distributivität}{\equiv} (x \vee y) \wedge (x \vee z) \wedge (\neg y \vee y) \wedge (\neg y \vee z) \qquad KNF \\
&\equiv (x \vee y) \wedge (x \vee z) \wedge 1 \wedge (\neg y \vee z) \\
&\equiv (x \vee y) \wedge (x \vee z) \wedge (\neg y \vee z) \qquad KNF
\end{aligned}$$

Wahrheitswertetabelle für A:

$I^*(x)$	$I^*(y)$	$I^*(z)$	$I^*(x \Rightarrow y)$	$I^*(y \Rightarrow \neg z)$	$I^*((x \Rightarrow y) \wedge (y \Rightarrow \neg z))$	$I^*(A)$
1	1	1	1	0	0	1
1	1	0	1	1	1	0
1	0	1	0	1	0	1
1	0	0	0	1	0	1
0	1	1	1	0	0	1
0	1	0	1	1	1	0
0	0	1	1	1	1	0
0	0	0	1	1	1	0

Die DNF $(x \wedge y \wedge z) \vee (x \wedge \neg y \wedge z) \vee (x \wedge \neg y \wedge \neg z) \vee (\neg x \wedge y \wedge z)$ für A hat die gleiche Wahrheitswertetabelle wie A, ist also logisch äquivalent zu A.
Die KNF $(\neg x \vee \neg y \vee z) \wedge (x \vee \neg y \vee z) \wedge (x \vee y \vee \neg z) \wedge (x \vee y \vee z)$ für A hat die gleiche Wahrheitswertetabelle wie A, ist also logisch äquivalent zu A.

Satz 9.12. *Sei $A \in \mathcal{A}$ ein Ausdruck.*

a) *Man bestimmt eine DNF für A folgendermaßen:*
Für jede Belegung I, für die $I^*(A) = 1$ ist, bildet man folgende Konjunktionen:
Ist $I(x_i) = 1$, so tritt x_i in der Konjunktion auf.
Ist $I(x_i) = 0$, so tritt $\neg x_i$ in der Konjunktion auf.
Dann wird Disjunktion über alle diese Konjunktionen gebildet.

b) *Man bestimmt KNF für A folgendermaßen:*
Für jede Belegung I, für die $I^*(A) = 0$ ist, bildet man folgende Disjunktionen:
Ist $I(x_i) = 1$, so tritt $\neg x_i$ in der Disjunktion auf.
Ist $I(x_i) = 0$, so tritt x_i in der Disjunktion auf.
Dann wird Konjunktion über alle diese Disjunktionen gebildet.

Beweis. a) Sei $D = K_1 \vee \ldots \vee K_l$ die angegebene DNF, wobei die K_i jeweils Konjunktionen von Literalen sind. Sei I eine Belegung mit $I^*(A) = 1$. Die Konjunktion enthält x_i, falls $I(x_i) = 1$ und $\neg x_i$, falls $I(x_i) = 0$. Also haben alle Literale in dieser Konjunktion unter I den Wert 1, d.h. ihre Konjunktion hat den Wert 1. Somit gilt $I^*(D) = 1$.
Ist umgekehrt J eine Belegung mit $J^*(D) = 1$. Dann muss eines der K_i den Wert 1 haben, d.h. $J^*(K_i) = 1$. Dann haben alle Literale in K_i den Wert 1. Nach Konstruktion der K_i ist also J Belegung mit $J^*(A) = 1$. Somit $A \equiv D$.

b) Sei K die konstruierte KNF. Es gilt $I^*(A) = 0 \Leftrightarrow I^*(\neg A) = 1$. Bilde DNF D nach a) für $\neg A$. Es gilt $D \equiv \neg A$ und damit $\neg D \equiv A$. Wende De Morgan auf $\neg D$ an. Das liefert gerade K und es gilt $K \equiv \neg D \equiv A$.

□

Bemerkung 9.13. *a) Bildet man für Ausdruck $A \in \mathcal{A}$ die DNF $K_1 \vee \ldots \vee K_m$ bzw. KNF $D_1 \wedge \ldots \wedge D_l$ entsprechend nach 9.12, so enthalten alle diese K_i bzw. D_j jede Variable bzw. dessen Negation genau einmal.*
Solche DNF bzw. KNF sind bis auf die Reihenfolge der Konjunktionen bzw. Disjunktionen eindeutig bestimmt. Man nennt sie kanonische DNF *bzw.* kanonische KNF*.*

b) *Jede Bool'sche Funktion, d.h. jede Abbildung $f : \{0,1\}^n \to \{0,1\}$, lässt sich mit $\wedge$, $\vee$ und $\neg$ ausdrücken.*
Insbesondere lässt sich jeder 2-stelliger logischer Junktor durch $\wedge$, $\vee$ und $\neg$ darstellen. Dabei entspricht ein 2-stelliger logischer Junktor einer Abbildung $f : \{0,1\}^2 \to \{0,1\}$.

Beweis. Teil b) folgt aus 9.12. □

Erfüllbarkeitsproblem:

Gegeben ist ein Ausdruck $A \in \mathcal{A}$. Frage: Ist A erfüllbar?

1.Möglichkeit: (semantisch)
Bildung der Warheitswertetabelle. Sind n Variablen in Ausdruck A, so hat die Tabelle 2^n Zeilen. Sehr zeitaufwendig.

2.Möglichkeit: (syntaktisch)
Verwendung eines Kalküls: *Resolutionskalkül.*
Idee: Sei $\mathcal{F} = \{(x \vee p_1 \vee \ldots \vee p_l), (\neg x \vee q_1 \vee \ldots \vee q_m)\}$. Unter jeder Belegung I hat x entweder den Wert 0 oder 1. Ist $\mathcal{F}$ erfüllbar und I Belegung, die $\mathcal{F}$ enthält, dann muss $I^*(p_1 \vee \ldots \vee p_l) = 1$ oder $I^*(q_1 \vee \ldots \vee q_m) = 1$ gelten.
$\mathcal{F}$ erfüllbar $\Leftrightarrow \mathcal{F} \cup \{p_1 \vee \ldots \vee p_l \vee q_1 \vee \ldots \vee q_m\}$ erfüllbar. Dies gilt auch, wenn $\mathcal{F}$ noch weitere Ausdrücke $A_1, \ldots, A_t$ enthält.
Im Resolutionskalkül werden Disjunktionen von Literalen beschrieben als Menge dieser Literale. Z.B. $x \vee \neg y \vee z \to \{x, \neg y, z\}$.

Definition 9.14. *a) Eine endliche Menge von Literalen heißt* Klausel.

b) Ist $A = (p_{1,1} \vee \ldots \vee p_{1,n_1}) \wedge \ldots \wedge (p_{m,1} \vee \ldots \vee p_{m,n_m}) \in \mathcal{A}$ eine KNF, $p_{i,j}$ Literale, so heißen die Mengen $\{p_{i,1}, \ldots, p_{i,n_i}\}$, für $i = 1, \ldots, m$, die Klauseln von A. Die Menge aller Klauseln heißt Klauselmenge von A, *bezeichnet mit $\mathcal{K}(A)$.*

Beispiel: Sei $A = (x \vee y \vee \neg z \vee y) \wedge (\neg x \vee w \vee y)$, so ist die Klauselmenge von A folgende: $\mathcal{K}(A) = \{\{x, y, \neg z\}, \{\neg x, w, y\}\}$.

c) Sei K eine Klausel.
Ist $K = \emptyset$, so setze $A(K) := 0$.
Ist $K \neq \emptyset$, so setze $A(K) := \bigvee_{q \in K} q$.

Beispiel: Ist $K = \{x, y, \neg z\}$, so $A(K) = x \vee y \vee \neg z$.

d) Ist $\mathcal{M}$ eine nicht leere Menge von Klauseln, so setze $A(\mathcal{M}) = \{A(K) : K \in \mathcal{M}\}$. Die Menge $\mathcal{M}$ heißt erfüllbar, *falls $A(\mathcal{M})$ erfüllbar. Sonst heißt $\mathcal{M}$* unerfüllbar.

Beispiel: Ist $\mathcal{M} = \{\{x, y, \neg z\}, \{u, w, \neg x\}\}$, so $A(\mathcal{M}) = \{x \vee y \vee \neg z, u \vee w \vee \neg x\}$.
$\mathcal{M}$ erfüllbar $\Leftrightarrow (x \vee y \vee \neg z) \wedge (u \vee w \vee \neg x)$ erfüllbar.

e) Zwei nicht leere Mengen M, N von Klauseln heißen (logisch) äquivalent, wenn $\bigwedge_{K \in M} A(K)$ (logisch) äquivalent $\bigwedge_{L \in N} A(L)$.

Bemerkung 9.15. *a) Die Menge $\mathcal{M} = \{\emptyset\}$ ist nicht erfüllbar.*

b) Sind $A, B \in \mathcal{A}$ Ausdrücke in KNF, so gilt:
$A \equiv B$ genau dann, wenn $\mathcal{K}(A)$, $\mathcal{K}(B)$ logisch äquivalent.

c) Ein Ausdruck $A \in \mathcal{A}$ in KNF ist erfüllbar genau dann, wenn $\mathcal{K}(A)$ erfüllbar ist.

Beispiel: Sei $A = (x \vee y) \wedge (\neg x \vee z) \wedge (x \vee y) \in \mathcal{A}$.
Es gilt $K(A) = \{\{x, y\}, \{\neg x, z\}\}$ und $A(K(A)) = \{x \vee y, \neg x \vee z\}$.

Schreibweise:

Sei p ein Literal, so definieren wir:

$$\overline{p} \quad := \quad \begin{cases} \neg x & p = x,\ x \in V \\ x & p = \neg x,\ x \in V \end{cases}$$

Bemerkung:

$$\begin{aligned} & \text{KNF } (x \vee p_1 \vee \ldots \vee p_m) \wedge (\neg x \vee q_1 \vee \ldots \vee q_t) \wedge A_1 \wedge \ldots \wedge A_n \text{ erfüllbar} \\ \Leftrightarrow\ & \{x \vee p_1 \vee \ldots \vee p_m,\ \neg x \vee q_1 \vee \ldots \vee q_t,\ A_1, \ldots, A_n\} = \mathcal{F} \text{ erüllbar} \\ \Leftrightarrow\ & \{x \vee p_1 \vee \ldots \vee p_m,\ \neg x \vee q_1 \vee \ldots \vee q_t,\ p_1 \vee \ldots \vee p_m \vee q_1 \vee \ldots \vee q_t,\ A_1,\ \ldots,\ A_n\} \\ & = \mathcal{F} \cup \{p_1 \vee \ldots \vee p_m \vee q_1 \vee \ldots \vee q_t\} \text{ erüllbar} \end{aligned}$$

Die Mengen $\mathcal{F}$ und $\mathcal{F} \cup \{p_1 \vee \ldots \vee p_m \vee q_1 \vee \ldots \vee q_t\}$ sind logisch äquivalent.

Definition 9.16. *Seien K, L Klauseln. Existiert ein Literal p mit $p \in K$ und $\overline{p} \in L$, so heißt die Klausel $R := (K \setminus \{p\}) \cup (L \setminus \{\overline{p}\})$* Resolvente *von K und L.*

Beispiele:

a) Seien $K = \{x, \neg y, z\}$, $L = \{\neg x, y\}$, dann ist
$\{\neg y, z, y\}$ eine Resolvente von K und L,
$\{x, z, \neg x\}$ eine Resolvente von K und L,
aber $\{z\}$ ist keine Resolvente von K und L.

b) Die Klauseln $K = \{x, y, \neg z\}$ und $L = \{x, w\}$ haben keine Resolvente.

c) Die Klauseln $\{x\}$ und $\{\neg x\}$ haben als Resolvente $\emptyset$.

Lemma 9.17. *Sei $\mathcal{K}$ eine endliche Menge von Klauseln und seien $K, L \in \mathcal{K}$. Ist R eine Resolvente von K und L, so sind $\mathcal{K}$ und $\mathcal{K} \cup R$ logisch äquivalent.*

Ist insbesondere $R = \emptyset$, so ist $\mathcal{K}$ unerfüllbar.

Definition 9.18. *Sei $\mathcal{K}$ eine nicht leere Menge von Klauseln. Definiere:*

$$Res(\mathcal{K}) \quad := \quad \mathcal{K} \cup \{R : R \text{ Resolvente zweier Klauseln aus } \mathcal{K}\}$$

Desweiteren führen wir folgende rekursive Definition ein:

$$\begin{aligned} Res^0(\mathcal{K}) &:= \mathcal{K} \\ Res^{n+1}(\mathcal{K}) &:= Res(Res^n(\mathcal{K})) \qquad \forall n \geq 0 \end{aligned}$$

Man beachte, dass gilt:

$$\begin{aligned} Res^1(\mathcal{K}) &= Res(Res^0(\mathcal{K})) \\ &= Res(\mathcal{K}) \\ Res^n(\mathcal{K}) &\subseteq Res^{n+1}(\mathcal{K}) \qquad \forall n \geq 0 \end{aligned}$$

Beispiel:

Wir betrachten den Ausdruck $(x \vee \neg y \vee z) \wedge (y \vee z) \wedge (\neg x \vee z) \wedge (\neg x \vee \neg y)$. Es gilt $\mathcal{K} = \{\{x, \neg y, z\}, \{y, z\}, \{\neg x, z\}, \{\neg x, \neg y\}\}$ und weiter gilt:

$$\begin{aligned} Res(\mathcal{K}) &= \mathcal{K} \cup \{\{\neg y, z\}, \{x, z\}\} \\ Res(\mathcal{K})^2 &= Res(\mathcal{K}) \cup \{\{z\}\} \\ Res(\mathcal{K})^3 &= Res(\mathcal{K})^2 \\ Res(\mathcal{K})^n &= Res(\mathcal{K})^2 \qquad \forall n \geq 2 \end{aligned}$$

Satz 9.19. *Sei $\mathcal{K}$ eine endliche Menge von Klauseln. In den Klauseln seien insgesamt k verschiedene Literale enthalten. Dann gilt für alle $n \in \mathbb{N}_0$:*

$$|Res^n(\mathcal{K})| \quad \leq \quad 2^k$$

Insbesondere existiert ein kleinstes $r \in \mathbb{N}_0$, so dass für alle $n \geq r$ gilt:

$$R^r(\mathcal{K}) \quad = \quad Res^n(\mathcal{K})$$

Wir bezeichnen $Res^r(\mathcal{K})$ mit $Res^*(\mathcal{K})$.

Beweis. Seien $p_1, \ldots, p_k$ alle Literale in $\mathcal{K}$, so ist $\mathcal{K} \subseteq \mathcal{P}(\{p_1, \ldots, p_k\})$. Bei der Resolventenbildung entstehen keine neuen Literale. D.h. $Res^n(\mathcal{K}) \subseteq \mathcal{P}(\{p_1, \ldots, p_k\})$ für alle $n \in \mathbb{N}_0$. Es gilt: $|Res^n(\mathcal{K})| \leq |\mathcal{P}(\{p_1, \ldots, p_k\})| \underset{7.16}{=} 2^k$. □

Theorem 9.20. *Sei $\mathcal{K}$ eine nicht leere endliche Menge von Klauseln. Dann gilt:*

$$\mathcal{K} \text{ erfüllbar} \quad \Leftrightarrow \quad \emptyset \notin Res^*(\mathcal{K})$$

Insbesondere: Ist A ein Ausdruck in KNF, so gilt:

$$A \text{ erfüllbar} \quad \Leftrightarrow \quad \emptyset \notin Res^*(\mathcal{K}(A))$$

Beweis. Siehe Theorem 2.62 in [WHK04]. □

Korollar 9.21. *Sei A ein Ausdruck. Durch Berechnung einer äquivalenten KNF und anschließender Durchführung des Resolutionskalküls ist in endlich vielen Schritten entscheidbar, ob A erfüllbar ist oder nicht.*

Beispiele:

a) *Sei $A = (x \vee \neg y \vee z) \wedge (y \vee z) \wedge (\neg x \vee z) \wedge (\neg x \vee \neg y)$, so ist $\mathcal{K}(A)$ genau die Menge der Klauseln aus dem Beispiel 9.18. Es gilt $\emptyset \notin Res^*(\mathcal{K})$, also ist A erfüllbar nach 9.20. Modelle: $I(z) = 1$, mindestens eines von $I(x)$ und $I(y)$ gleich 0.*

b) *Sei $A = (w \vee \neg x \vee y) \wedge (\neg w \vee z) \wedge (z \vee \neg y) \wedge (x \vee z) \wedge (\neg z \vee x) \wedge (\neg w \vee \neg z) \wedge (\neg y \vee \neg z)$, so gilt:*

$$\begin{aligned} Res(\mathcal{K}(A)) &\supseteq \mathcal{K}(A) \cup \{\{\neg x, y, z\}, \{\neg z, w\, y\}\} \\ Res^2(\mathcal{K}(A)) &\supseteq Res(\mathcal{K}(A)) \cup \{\{\neg x, z\}, \{\neg z, y\}\} \\ Res^3(\mathcal{K}(A)) &\supseteq Res(\mathcal{K}(A))^2 \cup \{\{z\}, \{\neg z\}\} \end{aligned}$$

Es gilt $\emptyset \in Res^4(\mathcal{K}(A))$. Der Ausdruck A ist somit nicht erfüllbar.

Bemerkung 9.22. *Mit dem Resolutionskalkül kann man auch nachprüfen, ob ein Ausdruck A eine Tautologie ist. Es gilt: A Tautologie $\Leftrightarrow \neg A$ nicht erfüllbar. Der Ausdruck $\neg A$ lässt sich mit Resolutionskalkül testen, nachdem $\neg A$ äquivalent auf KNF umgeformt wurde.*

Definition 9.23. *Sei $\mathcal{F}$ eine nicht leere endliche Menge von Ausdrücken. Ein Ausdruck $A \in \mathcal{A}$ heißt* logische Folgerung *aus $\mathcal{F}$, bezeichnet durch $\mathcal{F} \models A$, wenn für jedes Modell I von $\mathcal{F}$ gilt $I^*(A) = 1$.*

Bemerkung 9.24. *Sei $\mathcal{F} = \{B_1, \ldots, B_n\}$. Es gilt: $\mathcal{F} \models A \quad \Leftrightarrow \quad (B_1 \wedge \ldots \wedge B_n) \Rightarrow A$ ist Tautologie.*

Beispiele:

a) *Sei $\mathcal{F} = \{x, y\}$ und $A = x \wedge y$. Der Ausdruck A ist eine logische Folgerung aus $\mathcal{F}$.*

b) Sei $\mathcal{F} = \{B, B \Rightarrow A\}$, so gilt $\mathcal{F} \models A$.

Bemerkung 9.25. *Eine logische Folgerung $\mathcal{F} \models A$ kann man mit einer Wahrheitswertetabelle nachprüfen. Es geht auch mit dem Resolutionskalkül. Sei $\mathcal{F} = \{B_1, \ldots, B_n\}$, dann gilt:*

$$
\begin{array}{ll}
 & \mathcal{F} \models A \\
\underset{9.24}{\Leftrightarrow} & (B_1 \wedge \ldots \wedge B_n) \Rightarrow A \text{ ist Tautologie} \\
\Leftrightarrow & \neg(\neg(B_1 \wedge \ldots \wedge B_n) \vee A) \text{ ist unerfüllbar} \\
\underset{De\ Morgan}{\Leftrightarrow} & B_1 \wedge \ldots \wedge B_n \wedge \neg A \text{ ist unerfüllbar}
\end{array}
$$

10 Halbgruppen, Monoide, Gruppen

In der Algebra werden Mengen mit Verknüpfungen untersucht. Diese Verknüpfungen gehorchen gewissen Axiomen, man spricht daher auch von algebraischen Strukturen. In diesem Kapitel werden wir uns mit einigen grundlegenden Strukturen der Algebra vertraut machen.

Definition 10.1. *Sei $X \neq \emptyset$ eine Menge. Die folgende Abbildung ist eine* Verknüpfung *oder* (abstrakte) Multiplikation *auf X:*

$$\begin{cases} X \times X \to X \\ (a, b) \mapsto a \cdot b \end{cases}$$

Der Term $a \cdot b$ heißt auch Produkt *von a und b.*

Man beachte: Das Symbol $\cdot$ muss nichts mit der normalen Multiplikation von Zahlen zu tun haben. Es steht als Platzhalter für andere Verknüpfungssymbole in speziellen Beispielen.

Eine Verknüpfung $\cdot$ über einr endlichen Menge $X = \{x_1, \ldots, x_n\}$ lässt sich durch eine Verknüpfungstafel wie folgt beschreiben:

	x_1	$\ldots$	x_j	$\ldots$	x_n
x_1			$\vdots$		
$\vdots$			$\vdots$		
x_i	$\ldots$	$\ldots$	$x_i \cdot x_j$		
$\vdots$					
x_n					

Beispiele:

a) Sei $X = \{a, b\}$ und sei eine Verknüpfung auf X durch folgende Tabelle gegebenen:

	a	b
a	b	b
b	a	a

Diese Verknüpfung ist nicht assoziativ, denn es gilt beispielsweise $(a \cdot a) \cdot a = b \cdot a = a$ *und* $a \cdot (a \cdot a) = a \cdot b = b$*. Desweiteren ist die Verknüpfung auch nicht kommutativ, denn es gilt* $a \cdot b = b$ *und* $b \cdot a = a$*.*

b) Sei $X = \mathbb{Z} \setminus \mathbb{N}$*. Die normale Multiplikation ist keine Verknüpfung auf* X*, aber die normale Addition ist eine Verknüpfung auf* X*.*

Definition 10.2. *Sei* $H \neq \emptyset$ *eine Menge mit einer Verknüpfung* $\cdot$ *. Das Tupel* $(H, \cdot)$ *heißt* Halbgruppe*, wenn das Assoziativgesetz gilt:* $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in H$*.*

Man beachte, dass beim Assoziativgesetz die Elemente a*,* b *und* c *nicht notwendig verschieden sein müssen.*

Bemerkung 10.3. *Das Assoziativgesetz bedeutet, dass bei endlichen Produkten bei jeder sinnvollen Klammerung dasselbe Ergebnis entsteht. Wir betrachten dazu beispielhaft ein Produkt mit vier Elementen. Mit Hilfe des Assoziativgesetzes gilt die Gleichheit für alle sinnvollen Klammerungen:*

$$\begin{aligned}(a \cdot b) \cdot (c \cdot d) &= ((a \cdot b) \cdot c) \cdot d \\ &= (a \cdot (b \cdot c)) \cdot d \\ &= a \cdot ((b \cdot c) \cdot d) \\ &= a \cdot (b \cdot (c \cdot d))\end{aligned}$$

Man beachte: Die Reihenfolge der Faktoren darf dabei im Allgemeinen nicht *verändert werden.*

Beispiele:

a) Die Tupel $(\mathbb{N}, \cdot)$*,* $(\mathbb{Z}, \cdot)$*,* $(\mathbb{Q}, \cdot)$*,* $(\mathbb{R}, \cdot)$ *sind Halbgruppen, wobei* $\cdot$ *die normale Multiplikation ist. Für die normale Multiplikation gilt:* $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c.$

b) Die Tupel $(\mathbb{N}, +)$*,* $(\mathbb{Z}, +)$*,* $(\mathbb{Q}, +)$*,* $(\mathbb{R}, +)$ *sind Halbgruppen, wobei* $+$ *die normale Addition ist. Für die normale Addition gilt:* $a + (b + c) = (a + b) + c \quad \forall a, b, c.$

c) Das Tupel $(\mathbb{Q} \setminus \{0\}, :)$ *ist keine Halbgruppe, da* $:$ *nicht assoziativ ist. Es gilt beispielsweise* $(6 : 2) : 3 = 3 : 3 = 1$ *und* $6 : (2 : 3) = 6 : \frac{2}{3} = 9$*.*

d) Sei M *eine Menge. Das Tupel* $(\mathcal{P}(M), \cup)$ *ist eine Halbgruppe, denn es gilt:* $(A \cup B) \cup C = A \cup (B \cup C) \quad \forall A, B, C \in \mathcal{P}(M)$*.*

Das Tupel $(\mathcal{P}(M), \cap)$ *ist eine Halbgruppe, denn es gilt:* $(A \cap B) \cap C = A \cap (B \cap C) \quad \forall A, B, C \in \mathcal{P}(M)$*.*

e) Sei $A \neq \emptyset$ *ein Alphabet, sei* $A^+ := \bigcup_{n \in \mathbb{N}} A^n$*. In* A^+ *liegen alle Tupel* $(a_1, \ldots, a_n)$*, wobei* $a_i \in A$ *und* $n \in \mathbb{N}$*. Schreibweise: Statt* $(a_1, \ldots, a_n)$ *schreibe* $a_1 \ldots a_n$*.* A^+

besteht aus allen endlichen „Wörtern“ über A. A^+ wird zur Halbgruppe durch Verknüpfung $\cdot$ mit:

$$(a_1 \dots a_n) \cdot (a'_1 \dots a'_m) \quad = \quad a_1 \dots a_n a'_1 \dots a'_m$$

Diese Verknüpfung heißt Hintereinanderausführung *oder* Konkatenation.

Speziell: Sei $A = \{x\}$, so gilt:

$$\begin{aligned} x^n &:= \underbrace{x \dots x}_{n\text{-mal}} \\ A^+ &= \{x^n : n \in \mathbb{N}\} \\ x^n \cdot x^m &= x^{n+m} \end{aligned}$$

Die Elemente von $A^+ = \{x^n : n \in \mathbb{N}\}$ heißen Monome *in x.*

f) Sei $M \neq \emptyset$ eine Menge und M^M die Menge aller Abbildungen $f : M \to M$. Das Tupel $(M^M, \circ)$ ist eine Halbgruppe, wobei $\circ$ die Hintereinanderausführung von Abbildungen ist mit: $(f \circ g)(m) := f(g(m)) \quad \forall m \in M$. Für $\circ$ gilt mit 3.7 b) das Assoziativgesetz: $f \circ (g \circ h) = (f \circ g) \circ h \quad \forall f, g, h \in M^M$.

g) Sei $n \in \mathbb{N}$ und $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$. Wir definieren die Verknüpfung $\oplus$ wie folgt: $\forall a, b \in \mathbb{Z}_n : a \oplus b := (a + b) \bmod n \in \mathbb{Z}_n$. Wir definieren die Verknüpfung $\odot$ wie folgt: $\forall a, b \in \mathbb{Z}_n : a \odot b := (a \cdot b) \bmod n \in \mathbb{Z}_n$. Es gilt die Assoziativität von $\oplus$:

$$\begin{aligned} a \oplus (b \oplus c) &= (a + (b \oplus c)) \bmod n \\ &= (a + ((b + c) \bmod n)) \bmod n \\ &\underset{6.13}{=} (a + (b + c)) \bmod n \\ &= ((a + b) + c) \bmod n \\ &\underset{6.13}{=} (((a + b) \bmod n) + c) \bmod n \\ &= ((a \oplus b) + c) \bmod n \\ &= (a \oplus b) \oplus c \end{aligned}$$

Es gilt die Assoziativität von $\odot$:

$$\begin{aligned} a \odot (b \odot c) &= (a + (b \odot c)) \bmod n \\ &= (a + ((b + c) \bmod n)) \bmod n \\ &\underset{6.13}{=} (a + (b + c)) \bmod n \\ &= ((a + b) + c) \bmod n \\ &\underset{6.13}{=} (((a + b) \bmod n) + c) \bmod n \\ &= ((a \odot b) + c) \bmod n \\ &= (a \odot b) \odot c \end{aligned}$$

Somit sind $(\mathbb{Z}_n, \oplus)$ und $(\mathbb{Z}_n, \odot)$ jeweils Halbgruppen.

Bemerkung:

Bis auf e) und f) gilt in diesen Beispielen die Kommutativität: $a \cdot b = b \cdot a \forall a, b \in (H, \cdot)$.

Gegenbeispiel für f): Sei $M = \{1, 2, 3\}$, $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ *und* $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 1 \end{pmatrix}$, *dann gilt:*

$$\begin{aligned} f \circ g &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 2 \end{pmatrix} \\ g \circ f &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 1 \end{pmatrix} \\ g \circ f &\neq f \circ g \end{aligned}$$

Definition 10.4. *Eine Halbgruppe* $(H, \cdot)$ *heißt* kommutativ*, falls gilt* $a \cdot b = b \cdot a \ \forall a, b \in H$.

Beispiel: Das Tupel $(\mathbb{Z}, +)$ *ist eine kommutative Halbgruppe. Sei* $G \subseteq \mathbb{Z}$ *mit* $G = \{x \in \mathbb{Z} : 2 \mid x\}$, *so ist* $(G, +)$ *kommutative Halbgruppe.*

Definition 10.5. *Sei* $(H, \cdot)$ *eine Halbgruppe und* $\emptyset \neq U \subseteq H$. *Die Menge* U *heißt* Unterhalbgruppe *von* H*, falls gilt* $u \cdot v \in U \ \forall u, v \in U$.

Definition 10.6. *Seien* $(H, \cdot)$ *und* $(K, *)$ *Halbgruppen.*

a) *Eine Abbildung* $\varphi : H \to K$ *heißt* Homomorphismus*, falls gilt* $\varphi(a \cdot b) = \varphi(a) * \varphi(b) \ \forall a, b \in H$.

b) *Ein bijektiver Homomorphismus heißt* Isomorphismus.

c) *Existiert ein Isomorphismus zwischen* $(H, \cdot)$ *und* $(K, *)$*, so heißen* H *und* K isomorph*,* $H \cong K$.

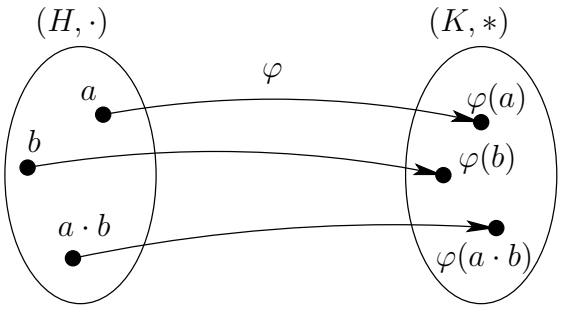
Bemerkung: Isomorphe Halbgruppen sind algebraisch nicht zu unterscheiden.

Ein Homomorphismus ist eine strukturerhaltende Abbildung. Die Abbildung 10.1 veranschaulicht die Situation.

Beispiele:

a) *Sei* $r > 0$ *reelle Zahl. Definiere* $\varphi_r : \begin{cases} (\mathbb{N}, +) \to (\mathbb{R}, \cdot) \\ n \mapsto r^n \end{cases}$ *. Die Abbildung* φ_r *ist ein Homomorphismus, denn für alle* $n, m \in \mathbb{N}$ *gilt:*

$$\varphi_r(n + m) = r^{n+m}$$



Bedingung: $\varphi(a) * \varphi(b) = \varphi(a \cdot b)$

Abbildung 10.1: Visualisierung eines Homomorphismus

$$\begin{aligned} &= r^n \cdot r^m \\ &= \varphi_r(n) \cdot \varphi_r(m) \end{aligned}$$

b) Sei $k \in \mathbb{N}$. *Wir definieren* $\psi_k : \begin{cases} (\mathbb{N}, +) \to (\mathbb{N}, +) \\ n \mapsto k \cdot n \end{cases}$. *Die Abbildung* ψ_k *ist ein injektiver Homomorphismus, aber nicht surjektiv, falls* $k \neq 1$*:*

$$\begin{aligned} \psi_k(n+m) &= k \cdot (n+m) \\ &= k \cdot n + k \cdot m \\ &= \psi_k(n) + \psi_k(m) \end{aligned}$$

c) Das Tupel $(H := \{0, 1, -1\}, \cdot)$ *ist eine Unterhalbgruppe von* $(\mathbb{Z}, \cdot)$. *Wir definieren* $\varphi : (\mathbb{Z}, \cdot) \to (H, \cdot)$ *wie folgt:*

$$\varphi(x) = \begin{cases} 0 & x = 0 \\ -1 & x < 0 \\ 1 & x > 0 \end{cases}$$

Dann ist φ *ein Homomorphismus, denn es gilt* $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)\ \forall x, y \in \mathbb{Z}$.

d) Die Abbildung $\tau_n : \begin{cases} (A^+, \cdot) \to (\mathbb{Z}_n, \oplus) \\ a_1 \dots a_m \mapsto m \bmod n \end{cases}$ *ist ein Homomorphismus, denn für alle* $a, b \in A^+$ *mit* $a = a_1 \dots a_m$, $b = b_1 \dots b_l$ *gilt:*

$$\begin{aligned} \tau_n(a \cdot b) &= \tau_n(a_1 \dots a_m \cdot b_1 \dots b_l) \\ &= (m + l) \bmod n \\ &\underset{6.13}{=} ((m \bmod n) + (l \bmod n)) \bmod n \end{aligned}$$

$$\begin{aligned} &= (\tau_n(a_1 \dots a_m) + \tau_n(b_1 \dots b_l)) \bmod n \\ &= (\tau_n(a) + \tau_n(b)) \bmod n \\ &= \tau_n(a) \oplus \tau_n(b) \end{aligned}$$

e) Die Abbildung $\varphi : \begin{cases} (\mathbb{R},+) \to (\mathbb{R},+) \\ x \mapsto x^2 \end{cases}$ *ist kein Homomorphismus, denn es gilt nicht für alle Zahlen* $x, y \in \mathbb{R}$ *die Gleichheit* $(x+y)^2 = x^2 + y^2$*, wobei:*

$$\begin{aligned} \varphi(x+y) &= (x+y)^2 \\ \varphi(x) + \varphi(y) &= x^2 + y^2 \end{aligned}$$

Satz 10.7. *Seien* $(H, \cdot)$*,* $(K, *)$ *Halbgruppen und sei* $\varphi : H \to K$ *ein Homomorphismus.*

a) $\varphi(H)$ *ist eine Unterhalbgruppe von* K*.*

b) Ist φ *injektiv, so ist* $H \cong \varphi(H)$*.*

c) Ist φ *ein Isomorphismus, so ist auch* $\varphi^{-1} : K \to H$ *ein Isomorphismus.*

Beweis. a) Für alle $\varphi(h_1), \varphi(h_2) \in \varphi(H)$ gilt $\varphi(h_1) * \varphi(h_2) = \varphi(\underbrace{h_1 \cdot h_2}_{\in H}) \in \varphi(H)$. Somit gilt für $\varphi(H)$ die Abgeschlossenheit bzgl. $*$. Die Assoziativität von $*$ folgt daher, dass $(K, *)$ eine Halbgruppe ist.

b) Da φ injektiv und surjektiv ist, ist φ bijektiv.

c) Ist φ bijektiv, so existiert eine Umkehrabbildung φ^{-1}, wobei φ^{-1} bijektiv ist. Seien $k_1, k_2 \in K$. Da φ surjektiv, existieren $h_1, h_2 \in H$ mit $\varphi(h_i) = k_i$ für $i = 1, 2$. Es gilt $\varphi^{-1}(k_i) = h_i$. Weiter gilt:

$$\begin{aligned} \varphi^{-1}(k_1 * k_2) &= \varphi^{-1}(\varphi(h_1) * \varphi(h_2)) \\ &\underset{\varphi \text{ Homomorphismus}}{=} \varphi^{-1}(\varphi(h_1 \cdot h_2)) \\ &= h_1 \cdot h_2 \\ &= \varphi^{-1}(k_1) \cdot \varphi^{-1}(k_2) \end{aligned}$$

□

Beispiele:

a) Sei $r \in \mathbb{R}$ *mit* $r > 1$*. Nach 10.7 b) gilt* $(\mathbb{N}, +) \cong (\{r^n : n \in \mathbb{N}\}, \cdot)$*, da der Homomorphismus* φ_r *aus Beispiel 10.6 a) injektiv ist.*

b) Sei $k \in \mathbb{N}$. Nach 10.7 b) gilt $(\mathbb{N}, +) \cong (\{k \cdot n : n \in \mathbb{N}\}, +)$, da der Homomorphismus ψ_k aus Beispiel 10.6 b) injektiv ist.

Lemma 10.8. *Sei $(H, \cdot)$ eine Halbgruppe. Existieren für alle $x \in H$ Elemente $e_1, e_2 \in H$ mit $e_1 \cdot x = x \cdot e_1 = x$ und $e_2 \cdot x = x \cdot e_2 = x$, so ist $e_1 = e_2$.*

Beweis. Es gilt $e_1 = e_1 \cdot e_2 = e_2$. □

Definition 10.9. *Eine Halbgruppe $(H, \cdot)$ heißt* Monoid*, falls ein $e \in H$ existiert mit:*

$$e \cdot x \;=\; x \cdot e \;=\; x \;\forall x \in H$$

Das Element e heißt neutrales Element *oder* Einselement/Eins*.*

Wir schreiben oft auch das Tupel $(H, \cdot, e)$, wobei e nach 10.8 eindeutig bestimmt ist.
Bei multiplikativer Schreibweise: Symbol 1 für das neutrale Element, Einselement*.*
Bei additiver Schreibweise: Symbol 0 für das neutrale Element, Nullelement*.*
Diese Schreibweisen werden auch dann angewendet, wenn H nicht aus Zahlen besteht.

Beispiele:

a) Sei A ein Alphabet, A^+ = Menge aller endlichen Wörter über A. Das Element ε heißt leeres Wort *für das gilt: $\varepsilon x = x\varepsilon = x \;\forall x \in A^+$. Sei $A^* := A^+ \cup \{\varepsilon\}$, dann ist $(A^*, \cdot, \varepsilon)$ ein Monoid bzgl. Konkatenation.*

b) Die Halbgruppe $(\mathbb{N}, \cdot)$ mit normaler Multiplikation ist ein Monoid, das neutrales Element ist 1. Die Halbgruppe $(\mathbb{N}, +)$ mit normaler Addition ist kein Monoid.

c) Die Halbgruppen $(\mathbb{N}_0, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ sind Monoide mit neutralem Element 0. Ebenso bzgl. Multiplikation mit neutralem Element 1.

d) Sei M eine Menge. Die Halbgruppe $(\mathcal{P}(M), \cup)$ ist ein Monoid mit neutralem Element $\emptyset$. Die Halbgruppe $(\mathcal{P}(M), \cap)$ ist ein Monoid mit neutralem Element M.

e) Sei M eine Menge. Die Halbgruppe $(M^M, \circ)$ ist ein Monoid mit neutralem Element id_M.

f) Die Halbgruppe $(\mathbb{Z}_n, \oplus)$ ist ein Monoid mit neutralem Element 0. Die Halbgruppe $(\mathbb{Z}_n, \odot)$ ist ein Monoid mit neutralem Element 1.

Definition 10.10. *Sei $(H, \cdot, e)$ ein Monoid. Ein* Untermonoid *U von H ist eine Unterhalbgruppe, die e enthält, d.h. $(U, \cdot, e)$ ist selbst ein Monoid.*

Man beachte: Die Mengen H, $\{e\}$ mit $\cdot$ sind immer Untermonoide.

Beispiele:

a) Das Tupel $(\mathbb{N}_0, +)$ *ist ein Untermonoid von* $(\mathbb{Z}, +)$.

b) Betrachte das Tupel $(H = \{e, a\}, \cdot)$ *mit* $\cdot$ *gegeben durch:*

$\cdot$	e	a
e	e	a
a	a	a

Das Tupel $(H = \{e, a\}, \cdot)$ *ist ein Monoid mit neutralem Element* e. *Das Tupel* $(\{a\}, \cdot)$ *ist eine Unterhalbgruppe und Monoid, aber* kein *Untermonoid von* H, *da* e *nicht enthalten ist.*

Lemma 10.11. *Sei* $(H, \cdot, e)$ *ein Monoid. Es gebe zu einem Element* $x \in H$ *Elemente* $y, z \in H$ *mit* $x \cdot y = e$ *und* $z \cdot x = e$, *dann gilt* $y = z$.

Beweis. Es gilt: $z = z \cdot e = z \cdot (x \cdot y) = (z \cdot x) \cdot y = e \cdot y = y$. □

Definition 10.12. *a) Sei* $(G, \cdot, e)$ *ein Monoid und* $x \in G$. *Existiert zu* x *ein* $y \in G$ *mit* $x \cdot y = y \cdot x = e$, *so heißt* x invertierbar *und* y *heißt das* Inverse *(oder das* inverse Element*) zu* x.

Bezeichnung für y *bei multiplikativer Verknüpfung:* x^{-1}. *Bezeichnung für* y *bei additiver Verknüpfung:* $-x$.

Nach 10.11 ist x^{-1} *eindeutig bestimmt.*

b) Ein Monoid $(G, \cdot, e)$ *heißt* Gruppe, *falls jedes Element invertierbar ist.*

c) Ist $(G, \cdot, e)$ *eine endliche Gruppe, so heißt die Anzahl der Elemente in* G *die* Ordnung *von* G, *bezeichnet mit* $|G|$.

d) Eine Gruppe, in der die Verknüpfung kommutativ ist, heißt kommutative Gruppe *oder* abelsche[1] Gruppe.

Satz 10.13. *Sei* $(H, \cdot, e)$ *ein Monoid. Dann ist die Menge der invertierbaren Elemente von* H *eine Gruppe. Genauer:*

- *Neutrales Element* e *ist invertierbar.*
- *Ist* x *invertierbar, so auch* x^{-1} *und* $(x^{-1})^{-1} = x$.

[1] Niels Henrik Abel (1802 - 1829) war ein norwegischer Mathematiker.

- *Sind x, y invertierbar, so ist auch $x \cdot y$ invertierbar und $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$.*

Beweis.
- $e^{-1} = e$, denn $e \cdot e = e$.
- $x^{-1} \cdot x = x \cdot x^{-1} = e$. x ist Inverses zu x^{-1}, $(x^{-1})^{-1} = x$.
- Es gilt:

$$\begin{aligned}
(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) &= x \cdot (y \cdot y^{-1}) \cdot x^{-1} \\
&= x \cdot e \cdot x^{-1} \\
&= x \cdot x^{-1} \\
&= e \\
(y^{-1} \cdot x^{-1}) \cdot (x \cdot y) &= y^{-1} \cdot (x^{-1} \cdot x) \cdot y \\
&= y^{-1} \cdot e \cdot y \\
&= y^{-1} \cdot y \\
&= e \\
(x \cdot y)^{-1} &= y^{-1} \cdot x^{-1}
\end{aligned}$$

□

Beispiele:

a) $(\mathbb{Z}, +, 0)$, $(\mathbb{Q}, +, 0)$, $(\mathbb{R}, +, 0)$ *sind Gruppen. Inverses zu x ist $-x$.*
Das Tupel $(\mathbb{N}_0, +, 0)$ ist keine Gruppe. Die Menge der invertierbaren Elemente in $(\mathbb{N}_0, +, 0)$ ist $\{0\}$.

b) Das Tupel $(\mathbb{Z}, \cdot, 1)$ ist keine Gruppe. Die Menge der invertierbaren Elemente ist $\{-1, 1\}$ und bildet Gruppe bzgl. $\cdot$.

c) $(\mathbb{Q}, \cdot, 1)$ *ist keine Gruppe, da 0 nicht invertierbar ist.* $(\mathbb{Q} \setminus \{0\}, \cdot, 1)$ *ist eine Gruppe. Ebenso ist* $(\mathbb{R} \setminus \{0\}, \cdot, 1)$ *eine Gruppe.*

d) Das Tupel $(A^*, \cdot)$ ist keine Gruppe. Nur ε ist invertierbar.

Satz 10.14. *Sei G eine Gruppe und seien $a, b \in G$. Es gibt genau ein $x \in G$ mit $a \cdot x = b$, nämlich $x = a^{-1} \cdot b$. Es gibt genau ein $y \in G$ mit $y \cdot a = b$, nämlich $y = b \cdot a^{-1}$.*

Beweis. $x = a^{-1} \cdot b$ ist eine Lösung: $a \cdot (a^{-1} \cdot b) = (a \cdot a^{-1}) \cdot b = e \cdot b = b$.
Eindeutigkeit der Lösung zu $a \cdot x = b$:

$$x = e \cdot x$$

$$\begin{aligned} &= (a^{-1} \cdot a) \cdot x \\ &= a^{-1} \cdot (a \cdot x) \\ &= a^{-1} \cdot b \end{aligned}$$

Die 2.Gleichung kann analog dazu bewiesen werden. □

Beispiel 10.15. *Die Menge $Bij(M)$ aller bijektiver Abbildungen $M \to M$ bildet bzgl. Hintereinanderausführung eine Gruppe. Für die Invertierbarkeit gilt:*

$$\begin{aligned} \varphi \in M^M \text{ invertierbar} &\Leftrightarrow \exists \psi \in M^M : \quad \varphi \circ \psi = \psi \circ \varphi = \mathrm{id}_M \\ &\underset{3.9}{\Leftrightarrow} \ \varphi \text{ bijektiv } : \psi = \varphi^{-1} \end{aligned}$$

$(Bij(M), \circ)$ Gruppe nach Beispiel e) aus 10.9.

Ist $M = \{1, \ldots, n\}$, so heißt $Bij(M)$ symmetrische Gruppe von Grad *n, bezeichnet mit S_n (Gruppe der Permutationen auf M). Mit 7.5 gilt $|S_n| = n!$.*

Beispiel:

Sei $n = 3$ und $\pi \in S_3$ mit $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, das Inverse zu π ist π^{-1} mit $\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$. Denn es gilt $\pi \circ \pi^{-1} = \pi^{-1} \circ \pi = \mathrm{id}_M$. Es ist $\pi = \pi^{-1}$, d.h. $\pi \circ \pi = \mathrm{id}_M$. Sei weiter $\varrho \in \S_3$ mit $\varrho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ und $\varrho^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$. S_3 ist nicht kommutativ. Für die Gleichung $\pi \circ x = \varrho$ gibt es die folgende eindeutige Lösung:

$$\begin{aligned} x &= \pi^{-1} \circ \varrho \\ &= \pi \circ \varrho \\ &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \end{aligned}$$

Für die Gleichung $y \circ \pi = \varrho$ gibt es die folgende eindeutige Lösung:

$$\begin{aligned} y &= \varrho \circ \pi^{-1} \\ &= \varrho \circ \pi \\ &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \end{aligned}$$

Beispiel 10.16. *a) Sei $n \in \mathbb{N}$, so ist $(\mathbb{Z}_n = \{0, \ldots, n-1\}, \oplus, 0)$ eine Gruppe: Monoid klar und das Inverse zu x ist $(-x) \bmod n$, d.h. $-x = \begin{cases} 0 & x = 0 \\ n - x & x \neq 0 \end{cases}$.*

b) Sei $n \in \mathbb{N}$ mit $n > 1$. Das Tupel $(\mathbb{Z}_n, \odot, 1)$ ist ein Monoid, aber keine Gruppe. Z.B. hat das Element 0 kein Inverses. Es gilt:

$$\begin{aligned} x \in \mathbb{Z}_n \text{ invertierbar bzgl. } \odot &\Leftrightarrow \exists y \in \mathbb{Z}_n : \; x \odot y = 1 \\ &\Leftrightarrow \exists y \in \mathbb{Z}_n : \; x \cdot y \bmod n = 1 \\ &\Leftrightarrow \exists \tilde{y} \in \mathbb{Z} : \; x \cdot \tilde{y} \equiv 1 \pmod{n} \end{aligned}$$

Dabei ist $y = \tilde{y} \bmod n$. Nach 6.21 gilt:

$$x \in \mathbb{Z}_n \text{ invertierbar bzgl. } \odot \;\Leftrightarrow\; \mathrm{ggT}(x, n) = 1$$

Die Menge $\mathbb{Z}_n^* = \{x \in \mathbb{Z} : \; \mathrm{ggT}(x, n) = 1\}$ bildet eine Gruppe bzgl. $\odot$ nach 10.13.

Wir definieren:

$$\begin{aligned} |\mathbb{Z}_n^*| &=: \varphi(n) \\ &= \text{Anzahl aller natürlichen Zahlen} < n, \text{ die teilerfremd sind zu } n \end{aligned}$$

Die Abbildung φ heißt Euler'sche φ-Funktion. *Sei p eine Primzahl, so gilt $\varphi(p) = p - 1$.*

Wie berechnet man x^{-1} ?

Erweiterter Euklidischer Algorithmus anwenden auf n und x. Liefert $s, t \in \mathbb{Z}$ mit $s \cdot n + t \cdot x \underset{(1)}{=} 1$. Es ist $x^{-1} = t \bmod n$, denn es gilt:

$$\begin{aligned} x \odot (t \bmod n) &= x \cdot (t \bmod n) \bmod n \\ &\underset{6.13}{=} x \cdot t \bmod n \\ &\underset{(1)}{=} (1 - s \cdot n) \bmod n \\ &\underset{6.13}{=} (1 \bmod n - s \cdot n \bmod n) \bmod n \\ &= (1 - 0) \bmod n \\ &= 1 \bmod n \\ &= 1 \end{aligned}$$

Beispiel:

Sei $n = 8$ und $x = 5$. Es ist $x \in (\mathbb{Z}_8, \cdot)$ und x ist invertierbar, da $\mathrm{ggT}(8, 5) = 1$. *Anwenden des EEA ergibt $1 = 2 \cdot 8 + (-3) \cdot 5$, dabei gilt $-3 \bmod 8 = 5$. Probe:*

$$\begin{aligned} 5 \odot 5 &= (5 \cdot 5) \bmod 8 \\ &= 25 \bmod 8 \\ &= 1 \end{aligned}$$

Definition 10.17. *Sei $(G, \cdot)$ eine Gruppe. Eine Teilmenge $U \neq \emptyset$ von G heißt Untergruppe von G, falls U bzgl. $\cdot$ selbst eine Gruppe ist. Bezeichnung: $U \leq G$*

Bemerkung: Jede Gruppe G besitzt $\{e\}$ und G als Untergruppe (triviale Untergruppen).

Bemerkung 10.18. *Sei $U \leq G$. Dann ist das neutrale Element von U gleich dem neutralen Element von G.*

Bemerkung: Daher gilt auch: Das Inverse zu $u \in U$ ist das Inverse von u in G.

Beweis. Sei e das neutrale Element in G und f das neutrale Element in U. Sei f^{-1} das Inverse zu f in G, d.h. $f \cdot f^{-1} = f^{-1} \cdot f = e$. Es gilt weilter:

$$\begin{aligned} f \cdot f = f &\Rightarrow f^{-1} \cdot (f \cdot f) = f^{-1} \cdot f \\ &\Rightarrow (f^{-1} \cdot f) \cdot f = e \\ &\Rightarrow e \cdot f = e \\ &\Rightarrow f = e \end{aligned}$$

□

Beispiele:

a) Es gilt $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +)$.

b) Es gilt $(\{1, -1\}, \cdot) \leq (\mathbb{Q} \setminus \{0\}, \cdot)$.

c) Sei $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in S_3$. Es gilt $\pi \circ \pi = \mathrm{id}$. Also $\{\mathrm{id}, \pi\} \leq S_3$.

d) Sei $n \in \mathbb{Z}$. Wir definieren:

$$\begin{aligned} n\mathbb{Z} &:= \{n \cdot k : \ k \in \mathbb{Z}\} \\ &= \textit{Menge aller ganzzahligen Vielfachen von } n \end{aligned}$$

Sei $n = 2$, so ist $2\mathbb{Z} =$ Menge aller geraden Zahlen. Es gilt $(n\mathbb{Z}, +) \leq (\mathbb{Z}, +)$. Denn Abgeschlossenheit gilt $n \cdot k_1 + n \cdot k_2 = n \cdot (k_1 + k_2)$ und Inverse existieren zu allen Elementen $-n \cdot k = n \cdot (-k)$.

Satz 10.19. *Sei G Gruppe, $\emptyset \neq U \subseteq G$. Dann sind äquivalent:*

(1) $U \leq G$

(2) $x^{-1} \cdot y \in U \ \forall x, y \in U$

(3) $x^{-1} \in U \; \forall x \in U \quad \wedge \quad x \cdot y \in U \; \forall x, y \in U$

Beweis. „(1) $\Rightarrow$ (2)“: Sei $U \leq G$. Es gilt $x \in U \Rightarrow x^{-1} \in U$. Sei $y \in U$, daraus folgt $x^{-1} \cdot y \in U$, da U eine Gruppe ist und somit bzgl $\cdot$ abgeschlossen ist.

„(2) $\Rightarrow$ (3)“:

$$\begin{aligned} U \neq \emptyset &\Rightarrow u \in U \\ &\underset{(2)}{\Rightarrow} e = u^{-1} \cdot u \in U \\ x \in U &\underset{(2)}{\Rightarrow} x^{-1} \cdot e = x^{-1} \in U \\ x, y \in U &\Rightarrow x^{-1} \in U \\ &\underset{(2)}{\Rightarrow} (x^{-1})^{-1} \cdot y = x \cdot y \in U \end{aligned}$$

„(3) $\Rightarrow$ (1)“:

$$\begin{aligned} U \neq \emptyset &\Rightarrow u \in U \\ &\underset{(3)}{\Rightarrow} u^{-1} \in U \\ &\underset{(3)}{\Rightarrow} e = u^{-1} \cdot u \in U \end{aligned}$$

Also gilt (1). □

Satz 10.20. *Sei G eine Gruppe und $U \leq G$. Wir definieren die Relation $\sim_U$ auf G wie folgt: Seien $x, y \in G$, so gilt:*

$$x \sim_U y \quad \Leftrightarrow \quad x^{-1} \cdot y \in U$$

Die Relation $\sim_U$ ist eine Äquivalenzrelation auf G. Ist $x \in G$, so ist $x \cdot U = \{x \cdot u : u \in U\}$ die Äquivalenzklasse von x bzgl. $\sim_U$. Die Äquivalenzklasse $x \cdot U$ heißt Linksnebenklasse *von U in G. Es gilt also:*

$$\begin{aligned} x \cdot U = y \cdot U &\Leftrightarrow x \sim_U y \\ &\Leftrightarrow x^{-1} \cdot y \in U \end{aligned}$$

Seien $x, y \in G$ so gilt entweder $x \cdot U = y \cdot U$ oder $x \cdot U \cap y \cdot U = \emptyset$. Ist $x \notin U$, so $x \cdot U \cap U = \emptyset$, $x \cdot U$ ist keine Untergruppe. Wenn die Verknüpfung in G additiv ist, $+$, so schreiben wir für die Linksnebenklasse $x + U = \{x + u : u \in U\}$.

Beweis. Sei $x \in G$, so $x^{-1} \cdot x = e \in U$, d.h. es gilt die Reflexivität $x \sim_U x$.

$$x \sim_U y \quad \Rightarrow \quad x^{-1} \cdot y \in U$$

$$\begin{aligned} &\Rightarrow\ y^{-1}\cdot x = (x^{-1}\cdot y)^{-1} \in U \\ &\Rightarrow\ y \sim_U x \qquad \text{Symmetrie} \end{aligned}$$

$$\begin{aligned} x \sim_U y \wedge y \sim_U z \ &\Rightarrow\ x^{-1}\cdot y \in U \wedge y^{-1}\cdot z \in U \\ &\Rightarrow\ x^{-1}\cdot z = (x^{-1}\cdot y)\cdot(y^{-1}\cdot z) \in U \\ &\Rightarrow\ x \sim_U z \qquad \text{Transitivität} \end{aligned}$$

Äquivalenzklasse von x ist $x \cdot U$: „$[x] \subseteq x \cdot U$“:

$$\begin{aligned} y \in [x] \ &\Rightarrow\ y \sim_U x \\ &\Rightarrow\ y^{-1}\cdot x \in U \\ &\Rightarrow\ y^{-1}\cdot x = u \in U \\ &\Rightarrow\ x = y\cdot u \\ &\Rightarrow\ y = x\cdot u^{-1} \in x\cdot U \end{aligned}$$

„$x \cdot U \subseteq [x]$“:

$$\begin{aligned} y \in x\cdot U \ &\Rightarrow\ y = x\cdot u \quad \text{für ein } u \in U \\ &\Rightarrow\ x^{-1}\cdot y = u \in U \\ &\Rightarrow\ x \sim_U y \\ &\Rightarrow\ y \in [x] \end{aligned}$$

□

Beispiel:

Wir betrachten $(\mathbb{Z}, +)$ und die Untergruppe $U = n\mathbb{Z}$ mit $n \in \mathbb{N}$, siehe Beispiel 10.18 d). Linksnebenklasse $k + n\mathbb{Z}$. Seien $x, y \in \mathbb{Z}$, dann gilt:

$$\begin{aligned} & x \sim_U y \\ \Leftrightarrow\ & -x + y \in n\mathbb{Z} \\ \Leftrightarrow\ & y - x = n\cdot k \textit{ für ein } k \in \mathbb{Z} \\ \Leftrightarrow\ & n \mid x - y \\ \Leftrightarrow\ & x \equiv y \pmod{n} \end{aligned}$$

Verschiedene Nebenklassen: $0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}$. Dabei gilt $n + n\mathbb{Z} = n\mathbb{Z}$. Diese Äquivalenzklassen nennt man auch Restklasse mod n.

Lemma 10.21. *Sei G eine Gruppe und U eine endliche Untergruppe von G. Ist $x \in G$, so ist $|x \cdot U| = |U|$.*

Beweis:

Wir betrachten die Abbildung $\varphi : \begin{cases} U \to x \cdot U \\ u \mapsto x \cdot u \end{cases}$ *. Die Abbildung* φ *ist surjektiv. Seien* $u_1, u_2 \in U$*, so gilt weiter:*

$$\begin{aligned} \varphi(u_1) = \varphi(u_2) &\Rightarrow x \cdot u_1 = x \cdot u_2 \\ &\Rightarrow x^{-1} \cdot (x \cdot u_1) = x^{-1} \cdot (x \cdot u_2) \\ &\Rightarrow u_1 = u_2 \end{aligned}$$

Somit ist φ *injektiv, also bijektiv. Damit gilt* $|U| = |x \cdot U|$*.*

Theorem 10.22. *(Satz von Lagrange[2]) Ist* G *eine endliche Gruppe und* $U \leq G$*, so ist* $|U|$ *ein Teiler von* $|G|$ *und* $q := \frac{|G|}{|U|}$ *ist genau die Anzahl der verschiedenen Linksnebenklassen von* U *in* G*.*

Die Zahl q *ist auch die Anzahl der verschiedenen Rechtsnebenklassen* $U \cdot x$*, wobei* $x \in G$ *und* $|U \cdot x| = |U|$*. Im Allgemeinen gilt jedoch* $U \cdot x \neq x \cdot U$*.*

Beweis. Seien $x_1 \cdot U, \ldots, x_q \cdot U$ die verschiedenen Nebenklassen von U in G (siehe 10.20), so gilt nach 4.7 $G = \biguplus_{i=1}^{q} x_i \cdot U$. Weiter gilt $|G| = \sum_{i=1}^{q} |x_i \cdot U| \underset{10.21}{=} q \cdot |U|$. □

Beispiel:

Sei G *die symmetrische Gruppe auf* $\{1, 2, 3, 4\}$*,* $G = S_4$*. Es gilt* $|S_4| = 4! = 24$*. Mögliche Ordnungen von Untergruppen von* S_4 *nach 10.22:* $1, 2, 3, 4, 6, 8, 12, 24$*. Die Gruppe* S_4 *enthält zu jedem dieser Teiler eine Untergruppe der entsprechenden Ordnung. Aber: Die Untergruppe der Ordnung 12 enthält keine Untergruppe der Ordnung 6. Man kann zeigen, das gilt:*

Ordnung	1	2	3	4	6	12	24
Anzahl der Untergruppe	1	9	4	7	4	1	1

Es gibt beispielsweise 9 Untergruppen der Ordnung 2: $U = \{\mathrm{id}, \pi\}$ *mit* $\pi = \pi^{-1}$*. Drei Untergruppen dieser Art können durch folgende Elemente gebildet werden:*

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

$$\pi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

[2] Joseph Louis Lagrange (1736 - 1813) war ein italienischer Mathematiker.

Die Menge $V = \{\mathrm{id}, \pi_1, \pi_2, \pi_3\}$ bildet eine Untergruppe der Ordnung 4. Es gilt $\pi_i \circ \pi_j = \pi_k$ für alle i, j, k, die paarweise verschieden sind. Die Untergruppe V ist abelsch.

Satz 10.23. *Seien $G_1, \ldots, G_n$ Gruppen (nicht notwendig verschieden). Dann wird das kartesische Produkt $G_1 \times \ldots \times G_n = \{(g_1, \ldots, g_n) : g_i \in G_i\}$ wieder zu einer Gruppe durch die folgende Verknüpfung:*

$$(g_1, \ldots, g_n) \cdot (g'_1, \ldots, g'_n) \quad := \quad (g_1 \cdot g'_1, \ldots, g_n \cdot g'_n)$$

Man nennt dies auch das Direkte Produkt der Gruppen $G_1, \ldots, G_n$. Weiter gilt:

$$|G_1 \times \ldots \times G_n| \quad = \quad |G_1| \cdot \ldots \cdot |G_n|$$

Sind alle G_i kommutativ, so auch $G_1 \times \ldots \times G_n$.

Beweis. Das Assoziativgesetz folgt aus dem Assoziativgesetz in G. Das neutrale Element ist $(e_{G_1}, \ldots, e_{G_n})$, wobei e_{G_i} das neutrale Element in G_i ist. Weiter gilt $(g_1, \ldots, g_n)^{-1} = (g_1^{-1}, \ldots, g_n^{-1})$. □

Beispiel:

Wir betrachten die Gruppe $(\mathbb{Z}_2, \oplus)$ und bilden $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (1,0), (0,1), (1,1)\}$. Die Verknüpfung wird additiv geschrieben: $(z_1, z_2) + (z'_1, z'_2) = (z_1 \oplus z'_1, z_2 \oplus z'_2)$.
Untergruppen der Ordnung 1: $\{(0,0)\}$.
Untergruppen der Ordnung 4: $\mathbb{Z}_2 \times \mathbb{Z}_2$.
Untergruppen der Ordnung 2: $\{(0,0),(1,0)\}$, $\{(0,0),(0,1)\}$, $\{(0,0),(1,1)\}$.

Die Gruppe $(\mathbb{Z}_4, \oplus)$ besitzt genau eine Untergruppe der Ordnung 2: $\{0, 2\}$.

Beispiel:

Wir betrachten die Gruppe $V = \{\mathrm{id}, \pi_1, \pi_2, \pi_3\}$ aus Beispiel 10.22. Wir zeigen, dass gilt $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Wir definieren:

$$\begin{aligned} x_1 &:= (1,0) \in \mathbb{Z}_2 \times \mathbb{Z}_2 \\ x_2 &:= (0,1) \in \mathbb{Z}_2 \times \mathbb{Z}_2 \\ x_3 &:= (1,1) \in \mathbb{Z}_2 \times \mathbb{Z}_2 \end{aligned}$$

Weiter definieren wir die Abbildung $\varphi : V \to \mathbb{Z}_2 \times \mathbb{Z}_2$ mit $\varphi(\mathrm{id}) = (0,0)$ und $\varphi(\pi_i) = x_i$ für $i = 1, 2, 3$. Dann gilt:

$$\begin{aligned} \varphi(\mathrm{id} \circ \mathrm{id}) &= \varphi(\mathrm{id}) \\ &= (0,0) \end{aligned}$$

$$
\begin{aligned}
& = (0,0) + (0,0) \\
& = \varphi(\mathrm{id}) + \varphi(\mathrm{id}) \\
\varphi(\mathrm{id} \circ \pi_i) & = \varphi(\pi_i) \\
& = x_i \\
& = (0,0) + x_i \\
& = \varphi(\mathrm{id}) + \varphi(\pi_i) \\
\varphi(\pi_i \circ \mathrm{id}) & = \varphi(\pi_i) \\
& = x_i \\
& = x_i + (0,0) \\
& = \varphi(\pi_i) + \varphi(\mathrm{id}) \\
\varphi(\pi_i \circ \pi_i) & = \varphi(\mathrm{id}) \\
& = (0,0) \\
& = x_i + x_i \\
& = \varphi(\pi_i) + \varphi(\pi_i)
\end{aligned}
$$

Für $i \neq j$ gilt:

$$
\begin{aligned}
\varphi(\pi_i \circ \pi_j) & = \varphi(\pi_k) \\
& = x_k \\
& = x_i + x_j \\
& = \varphi(\pi_i) + \varphi(\pi_j)
\end{aligned}
$$

Somit ist φ ein Homomorphismus. Da φ bijektiv ist, ist φ ein Isomorphismus.

Satz 10.24. *Seien G, H Gruppen mit neutralem Element e_G bzw. e_H und sei $\varphi : G \to H$ ein Homomorphismus. Dann gilt:*

a) $\varphi(e_G) = e_H$.

b) $\varphi(x^{-1}) = \varphi(x)^{-1}$ *für alle* $x \in G$.

c) Ist $U \leq G$, so ist $\varphi(U) = \{\varphi(u) : u \in U\} \leq H$.
Insbesondere: $\varphi(G) \leq H$.

d) Ist G kommutativ, so ist $\varphi(G)$ kommutativ.

e) Der Kern *von φ ist definiert durch* $\ker(\varphi) := \{x \in G : \varphi(x) = e_H\}$ *und bildet eine Untergruppe von G.*

f) Für alle $x, y \in G$ gilt:

$$\varphi(x) = \varphi(y) \quad \Leftrightarrow \quad y^{-1} \cdot x \in \ker(\varphi)$$

$$\Leftrightarrow \quad x \cdot \ker(\varphi) = y \cdot \ker(\varphi)$$

Insbesondere: φ ist injektiv $\Leftrightarrow \ker(\varphi) = \{e_G\}$.

Beweis. a) Es gilt $\varphi(e_G) \cdot \varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G)$. Multipliziere diese Gleichung mit $\varphi(e_G)^{-1}$: $\varphi(e_G) = e_H$.

b) Es gilt $\varphi(x^{-1}) \cdot \varphi(x) = \varphi(x \cdot x^{-1}) = \varphi(e_G) \underset{\text{a)}}{=} e_H$. Multipliziere diese Gleichung mit $\varphi(x)^{-1}$: $\varphi(x^{-1}) = \varphi(x)^{-1}$.

c) Übungsaufgabe.

d) Übungsaufgabe.

e) Es gilt $\varphi(e_G) \underset{\text{a)}}{=} e_H$, d.h. $e_G \in \ker(\varphi) \neq \emptyset$. Seien $x, y \in \ker(\varphi)$, dann gilt $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) = e_H \cdot e_H = e_H$. Somit gilt $x \cdot y \in \ker(\varphi)$. Weiter gilt $\varphi(x^{-1}) \underset{\text{b)}}{=} \varphi(x)^{-1} = e_H^{-1} = e_H$. Somit gilt $x^{-1} \in \ker(\varphi)$. Nach 10.19 gilt $\ker(\varphi) \leq G$.

f) Es gilt:

$$\begin{aligned}
\varphi(x) = \varphi(y) &\Leftrightarrow \varphi(y)^{-1} \cdot \varphi(x) = e_H \\
&\underset{\text{b)}}{\Leftrightarrow} \varphi(y^{-1}) \cdot \varphi(x) = e_H \\
&\Leftrightarrow \varphi(y^{-1} \cdot x) = e_H \\
&\Leftrightarrow y^{-1} \cdot x \in \ker(\varphi) \\
&\Leftrightarrow x \cdot \ker(\varphi) = y \cdot \ker(\varphi)
\end{aligned}$$

„$\Leftarrow$“: Es gelte $\ker(\varphi) = \{e_G\}$.

$$\begin{aligned}
\text{Seien } x, y \in G \text{ mit } \varphi(x) = \varphi(y) &\Rightarrow y^{-1} \cdot x \in \ker(\varphi) \\
&\Rightarrow y^{-1} \cdot x = e_G \\
&\Rightarrow x = y \\
&\Rightarrow \varphi \text{ injektiv}
\end{aligned}$$

„$\Rightarrow$“: Sei φ injektiv.

$$\begin{aligned}
x \in \ker(\varphi) &\Rightarrow \varphi(x) = e_H = \varphi(e_G) \\
&\underset{\varphi \text{ injektiv}}{\Rightarrow} x = e_G \\
&\Rightarrow \ker(\varphi) = \{e_G\}
\end{aligned}$$

□

Definition 10.25. *Sei $(G, \cdot, e)$ eine Gruppe und $a \in G$. Wir definieren:*

$$\begin{aligned} a^0 &:= e \\ a^m &:= (a^{m-1}) \cdot a \quad \forall m \in \mathbb{N} \end{aligned}$$

Ist $m \in \mathbb{Z} \setminus \mathbb{N}_0$, so definieren wir $a^m = (a^{-1})^{-m}$. Der Ausdruck a^m heißt Potenz *von a.*

Wird G additiv geschrieben, so schreibt man $m \cdot a$ statt a^m. Der Ausdruck $m \cdot a$ heißt dann Vielfaches *von a.*

Beispiel: $a^{-3} = (a^{-1})^{-(-3)} = (a^{-1})^3 = (a^{-1})^2 \cdot a^{-1} = a^{-1} \cdot a^{-1} \cdot a^{-1}$.

Satz 10.26. *Sei $(G, \cdot, e)$ Gruppe, $a \in G$*

a) Für alle $m \in \mathbb{Z}$ gilt $(a^{-1})^m = (a^m)^{-1} = a^{-m}$.

b) Für alle $m, n \in \mathbb{Z}$ gilt $a^m \cdot a^n = a^{m+n}$.

c) Für alle $m, n \in \mathbb{Z}$ gilt $(a^m)^n = a^{m \cdot n}$.

Beweis. a) Sei $m \in \mathbb{N}$, so gilt $(a^{-1})^m \cdot a^m = \underbrace{a^{-1} \cdot \ldots a^{-1}}_{m\text{-mal}} \cdot \underbrace{a \cdot \ldots \cdot a}_{m\text{-mal}} = e$. Genauer Beweis: Induktion nach m. D.h. es gilt:

$$\begin{aligned} (a^{-1})^m &= (a^m)^{-1} \\ a^{-m} &\underset{\text{Def.}}{=} (a^{-1})^{-(-m)} \\ &= (a^{-1})^m \end{aligned}$$

$m = 0$: Klar.
Sei $m \in \mathbb{Z} \setminus \mathbb{N}$, so gilt $a^m \underset{\text{Def.}}{=} (a^{-1})^{-m}$. Wende dies mit a^{-1} statt a an:

$$\begin{aligned} (a^{-1})^m &= ((a^{-1})^{-1})^{-m} \\ &= a^{-m} \\ (a^m)^{-1} &= ((a^{-1})^{-m})^{-1} \\ &= a^{-m} \end{aligned}$$

b) Beweist man zunächst für $m, n \geq 0$. Für die übrigen Fälle verwendet man a).

c) Beweist man zunächst für $m, n \geq 0$. Für die übrigen Fälle verwendet man a).

□

Satz 10.27. *Sei $(G, \cdot, e)$ eine Gruppe und $a \in G$. Dann ist $\langle a \rangle := \{a^i : i \in \mathbb{Z}\}$ eine Untergruppe von G, die von a erzeugte* zyklische Untergruppe. *Sie ist die kleinste Untergruppe von G, die a enthält. Wird G additiv geschrieben, so $\langle a \rangle = \{i \cdot a : i \in \mathbb{Z}\}$. $\langle a \rangle$ ist kommutativ.*

G heißt zyklisch, *falls ein $a \in G$ existiert mit $G = \langle a \rangle$.*

Beweis. Es gilt:

$$\begin{aligned} a &= a^1 \quad \in \langle a \rangle \\ (a^i)^{-1} &= a^{-i} \quad \in \langle a \rangle \\ a^i \cdot a^j &= a^{i+j} \quad \in \langle a \rangle \\ \langle a \rangle &\leq G \end{aligned}$$

Sei $U \leq G$, $a \in U$, $m \in \mathbb{N}$, dann gilt:

$$\begin{aligned} a^m &= \underbrace{a \cdot \ldots \cdot a}_{m\text{-mal}} \quad \in U \\ a^0 &= e \in U \\ a^{-1} &\in U \end{aligned}$$

Sei $m \in \mathbb{Z} \setminus \mathbb{N}$, so gilt $a^m = (a^{-1})^{-m} \in U$. Also: $\langle a \rangle \leq U$.

□

Beispiele:

a) Sei $G = S_3$ und $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, dann gilt:

$$\begin{aligned} a^2 &= \mathrm{id} \\ a &= a^{-1} \\ a^n &= \begin{cases} \mathrm{id} & \textit{falls } n \textit{ gerade} \\ a & \textit{falls } n \textit{ ungerade} \end{cases} \\ \langle a \rangle &= \{a^0 = \mathrm{id}, a^1 = a\} \end{aligned}$$

b) Es gilt $(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$. Die Gruppe $(\mathbb{Z}, +)$ ist zyklisch. Sei $n \in \mathbb{Z}$, so gilt $n\mathbb{Z} = \{n \cdot k : k \in \mathbb{Z}\} \leq \mathbb{Z}$ und $n\mathbb{Z} = \langle n \rangle = \langle -n \rangle$. Die Gruppe $(n\mathbb{Z}, +)$ ist zyklisch.

c) Sei $m \in \mathbb{N}$, $(\mathbb{Z}_m, \oplus)$, so gilt $(\mathbb{Z}_m, \oplus) = \langle 1 \rangle$ und weiter:

$$\underbrace{m \cdot 1}_{\textit{Vielfaches bzgl. } \oplus} = 0$$

$$\begin{aligned}(m-1)\cdot 1 &= -1\\ (m+1)\cdot 1 &= 1\\ (m+2)\cdot 1 &= 2\\ &\vdots\\ (2\cdot m)\cdot 1 &= 0\end{aligned}$$

Die gruppe $(\mathbb{Z}_m, \oplus)$ ist zyklisch und ist von der Ordnung m.

Definition 10.28. *Sei G eine Gruppe. $a \in G$. Ist $\langle a\rangle$ unendlich, so heißt a* unendliche Ordnung. *Ist $\langle a\rangle$ endlich, $|\langle a\rangle| = n$, so hat a* Ordnung n, *bezeichnet mit $o(a) = n$.*

Beispiele:

a) *In $(\mathbb{Z}, +)$ hat jedes Element $\neq 0$ unendliche Ordnung. Das Element 0 hat die Ordnung 1, denn $\langle 0\rangle = \{0\}$.*

b) *Wir betrachten die Gruppe S_3. Sei $a = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$. Es gilt $o(a) = 2$. Sei weiter $b = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$. Es gilt:*

$$\begin{aligned}b^2 &= \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}\\ b^3 &= \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}\\ &= \mathrm{id}\\ b^2 &= b^{-1}\\ \langle b\rangle &= \{b^0 = \mathrm{id}, b^1 = b, b^2\}\\ &= \langle b^2\rangle\\ o(b) &= 3\end{aligned}$$

S_3 enthält kein Element der Ordnung 6, denn sonst $S_3 = \langle c\rangle$, d.h. S_3 wäre kommutativ. Dies ist jedoch ein Widerspruch.

Satz 10.29. *Sei $(G, \cdot, e)$ eine Gruppe und $a \in G$.*

a) *Ist $o(a)$ unendlich, so $\langle a\rangle = \{a^k : k \in \mathbb{Z}\}$ und $a^i \neq a^j$ für alle $i \neq j$. Die Abbildung $\varphi : \begin{cases}(\mathbb{Z}, +) \to \langle a\rangle\\ k \mapsto a^k\end{cases}$ ist ein Isomorphismus, d.h. es gilt $\langle a\rangle \cong (\mathbb{Z}, +)$.*

b) Ist $o(a)$ endlich, so ist $o(a)$ die kleinste natürliche Zahl n mit $a^n = e$. Dann ist $\langle a\rangle = \{a^0 = e, a^1 = 1, \ldots, a^{n-1}\}$ und die Abbildung $\psi : \begin{cases}(\mathbb{Z}_n, \oplus) \to \langle a\rangle \\ k \mapsto a^k\end{cases}$ ist ein Isomorphismus, d.h. $\langle a\rangle \cong (\mathbb{Z}_n, \oplus)$.

c) Ist $o(a) = n \in \mathbb{N}$, so gilt: $a^k = e$ für $k \in \mathbb{Z}$ $\Leftrightarrow$ $o(a) \mid k$

d) Ist G endlich, so gilt $a^{|G|} = e$ für alle $a \in G$.

Beweis. a) b) Angenommen es existieren $i \neq j$ mit $a^i = a^j$. O.B.d.A. $i > j$, $i - j \in \mathbb{N}$.

$$\begin{aligned} a^{i-j} &\underset{10.26}{=} a^i \cdot a^{-j} \\ &\underset{10.26}{=} a^i \cdot (a^j)^{-1} \\ &= a^i \cdot (a^i)^{-1} \\ &= e \end{aligned}$$

Dann existiert kleinste natürliche Zahl mit $a^n = e$. Dann sind $a^0 = e$, $a^1 = a$, …, a^{n-1} paarweise verschieden (Argument wie oben). Außerdem gilt $\langle a\rangle = \{a^0, a^1, \ldots, a^{n-1}\}$. Sei $i \in \mathbb{Z}$, $a^i \in \langle a\rangle$. Division mit Rest: $i = k \cdot n + r$, $0 \leq r \leq n-1$.

$$\begin{aligned} a^i &= a^{k\cdot n+r} \\ &\underset{10.26}{=} (a^n)^k \cdot a^r \\ &= e \cdot a^r \\ &= a^r \in \{a^0, \ldots, a^{n-1}\} \\ a^i &= a^{i \bmod n} \qquad (*) \end{aligned}$$

Ist $o(a)$ unendlich, so $a^i \neq a^j$ für $i \neq j$. Die Abbildung φ aus a) ist ein Isomorphismus. Homomorphismus:

$$\begin{aligned} \varphi(k+l) &= a^{k+l} \\ &= a^k \cdot a^l \\ &= \varphi(k) \cdot \varphi(l) \end{aligned}$$

Ist $o(a) = n$, so $\langle a\rangle = \{a^0, \ldots, a^{n-1}\}$. Die Abbildung ψ aus b) ist ein Isomorphismus: Bijektivität klar.

$$\begin{aligned} \psi(k \oplus l) &= a^{k\oplus l} \\ &= a^{(k+l) \bmod n} \\ &\underset{(*)}{=} a^{k+l} \\ &= a^k \cdot a^l \\ &\underset{10.26}{=} \psi(k) \cdot \psi(l) \end{aligned}$$

c) „⇒“: Nach Voraussetzung gilt $o(a) = n$ und $a^k = e$. Nach $(*)$ gilt $a^k = a^{k \bmod n}$, $k \bmod n < n$. Somit $k \bmod n = 0$, $n \mid k$.

„⇐“: Ist $o(a) = n \mid k$, so gilt $k = n \cdot l$ und weiter $a^k = a^{n \cdot l} = (a^n)^l = e^l = e$.

d) Satz von Lagrange: $o(a) = |\langle a \rangle| \mid |G|$. Mit Teil c) folgt $a^{|G|} = e$.

□

Bemerkung 10.30. *Es gibt bis auf Isomorphie nur eine unendliche zyklische Gruppe, nämlich $(\mathbb{Z}, +)$. Es gibt bis auf Isomorphie zu jedem $n \in \mathbb{N}$ genau eine zyklische Gruppe der Ordnung n, nämlich $(\mathbb{Z}_n, \oplus)$.*

Korollar 10.31. *a) (Satz von Euler) Sei $n \in \mathbb{N}$, $a \in \mathbb{Z}$ und $\mathrm{ggT}(a, n) = 1$, dann ist $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

b) (Kleiner Satz von Fermat[3]) Ist p eine Primzahl, $a \in \mathbb{Z}$ und $p \nmid a$, so ist $a^{p-1} \equiv 1 \pmod{p}$.

Bemerkung: Mit Hilfe von 10.31 werden sogenannte Public-Key-Verfahren entwickelt, siehe dazu 4.4.4 in [WHK04].

Beweis. a) Wendet man auf $a \equiv (a \bmod n) \pmod{n}$ $\varphi(n)$-mal 6.12 an, so erhält man $a^{\varphi(n)} \equiv (a \bmod n)^{\varphi(n)} \pmod{n}$. Es bleibt zu zeigen, dass $(a \bmod n)^{\varphi(n)} \equiv 1 \pmod{n}$ gilt. Denn dann gilt mit der Transitivität von $\equiv$ die Behauptung. Sei also $1 \leq a < n$. Die Menge $(\mathbb{Z}_n^*, \odot, 1) = \{a \in \mathbb{N} : 1 \leq a \leq n, \mathrm{ggT}(a, n) = 1\}$ ist eine Gruppe bzgl. $\odot$ nach 10.16 b). Es ist $a \in \mathbb{Z}_n^*$ und es gilt:

$$\begin{aligned} a^{|\mathbb{Z}_n^*|} &\underset{\text{10.29 d)}}{=} 1 \\ |\mathbb{Z}_n^*| &= \varphi(n) \\ \underbrace{a \odot \ldots \odot a}_{\varphi(n)\text{-mal}} &= 1 \\ a^{\varphi(n)} \bmod n &= 1 \\ a^{\varphi(n)} \bmod n &\equiv 1 \pmod{n} \end{aligned}$$

b) Folgt aus a) mit $n = p$.

□

[3] Pierre de Fermat (1607/1608 - 1665) war ein französischer Mathematiker.

Literaturverzeichnis

[WHK04] Manfred Wolff, Peter Hauck, and Wolfgang Küchlin. *Mathematik für Informatik und BioInformatik*. Springer-Verlag, 2004.

Index