

# Logik und Algebra

---

Prof. Dr. Sebastian Ritterbusch

Studiengang  
Wirtschaftsinformatik

Studienakademie  
Mannheim



# Inhaltsverzeichnis

Kapitel 1. Aussagen, Logik und Beweise	5
1.1. Aussagen	5
1.2. Aussagenlogik	6
1.3. Logisches Schließen	10
1.4. Prädikatenlogik	16
1.5. Beweistechniken	19
1.6. Aufgaben	22
Kapitel 2. Mengen, Relationen und Abbildungen	25
2.1. Mengen	25
2.2. Relationen	31
2.3. Abbildungen	37
2.4. Aufgaben	41
Kapitel 3. Gruppen, Ringe und Körper	43
3.1. Gruppen	43
3.2. Ringe und Körper	46
3.3. Zyklische Codes	51
3.4. Kryptographie	55
3.5. Aufgaben	60
Kapitel 4. Boolesche Algebra und logische Schaltungen	63
4.1. Boolesche Funktionen und Normalformen	64
4.2. Logische Schaltungen	66
4.3. KV-Diagramme	69
4.4. Aufgaben	73
Literaturverzeichnis	75
Index	77



## KAPITEL 1

# Aussagen, Logik und Beweise

Die Mathematik befasst sich mit eindeutigen Eigenschaften von Objekten und deren Zusammenhängen. Damit ist sie eine universelle Wissenschaft, die sowohl auf natürliche Zusammenhänge als auch für rein theoretische Überlegungen angewendet werden kann.

Auch scheinbar ungenaue und uneindeutige Sachverhalte wie der Zufall können mit mathematischen Überlegungen behandelt werden: Hier werden Zusammenhänge und Regelmäßigkeiten untersucht, die im selbst in zufälligen Vorgängen enthalten sind. Für die Beschreibung der uns noch so unbekannten Natur werden vereinfachende Modelle erstellt, die Vorgänge und Untersuchungsobjekte auf die relevanten Einflussfaktoren reduzieren und eine gewisse verallgemeinernde Gültigkeit besitzen, und mit denen dann mathematisch gearbeitet werden kann.

### 1.1. Aussagen

Bei der menschlichen Beschreibung von Sachverhalten, ist die Möglichkeit Zusammenhänge zu beschreiben, ein grundlegender Bestandteil der Auseinandersetzung. Dabei ist es bei der Betrachtung wichtig den Begriff einer Aussage genau einzugrenzen.

**DEFINITION 1.1.** Eine **Aussage** ist ein feststellender Satz, mit der Eigenschaft, dass er eindeutig als **wahr** oder **falsch** bezeichnet werden kann, unabhängig davon, ob die Einstufung in dem Moment erfolgen kann.

Die Definition zeigt schon eine erste Herausforderung der menschlichen Sprache: Der Verb „können“ ist hier im ersten Teil mehrdeutig, da sowohl die Möglichkeit die Aussage zu bezeichnen, als auch das Vermögen dies jetzt zu tun gemeint sein könnte. In der Mathematik geht es sogar sehr oft um Aussagen, deren Wahrheitsgehalt wir noch nicht kennen, und die dann erst im Folgenden oder über viele Jahre viele Menschen beschäftigen.

Wird jedes Wort auf die Goldwaage gelegt, so werden viele Sätze nur schwer als „Aussagen“ bezeichnet werden können, da fast alle Worte mehrere Bedeutungen haben können oder unterschiedliche Implikationen beinhalten können. Genau daher besteht ein Großteil der Mathematik aus dem Ansatz mit **Definitionen** bestimmten Ausdruck oder Sachverhalt einen eindeutigen Sinn zu geben, der im Folgenden so verwendet wird. Darüber hinaus wird in der Mathematik eine eigene Sprache mit besonderen Symbolen eingeführt, die so Aussagen in der Form von Formeln noch eindeutiger formulieren.

Andererseits ist aber selbst die scheinbar so eindeutige Formel  $1 + 1 = 2$  nur dann als Aussage zu definieren, wenn klar ist, was hier die Symbole  $1$ ,  $+$ ,  $=$  und  $2$  bedeuten, und hier gibt es durchaus sinnvolle und oft verwendete Alternativen, die in der Betrachtung gewisser Zusammenhänge zum Einsatz kommen können. Normalerweise sollte bei Aussagen und Formeln aus dem Zusammenhang oder dem gesellschaftlichen Zusammenleben klar sein, was genau gemeint ist, und diese Interpretation gewählt werden. Gibt es jedoch einen berechtigten Einwand, so muss zuvor beispielsweise mit Axiomen, Definitionen und Beispielen eine gemeinsame Sprache und ein gemeinsames Verständnis gefunden werden, um überhaupt über Aussagen sprechen zu können.

BEISPIEL 1.2. Welche der folgenden Sätze sind Aussagen?

- (1) Die Hälfte von 1kg Mehl sind 450g Mehl.
- (2) Diese Aussage ist falsch.
- (3) Alle natürlichen Zahlen lassen sich eindeutig in Primzahlfaktoren zerlegen.
- (4) Die Hochschule ist schön.
- (5) Alle natürlichen geraden Zahlen größer 2 sind Summe zweier Primzahlen.
- (6) Er wollte den Kegel umfahren.
- (7) Baden-Württemberg und Mannheim sind Bundesländer.

Der erste Satz ist mit Alltagswissen verständlich und kann eindeutig als wahr oder falsch bezeichnet werden, stellt also eine Aussage dar, die viele als falsch bezeichnen würden. Der zweite Satz ist verständlich, jedoch kann dieser nicht eindeutig als wahr oder falsch bezeichnet werden, da diese Aussage den Sinn des Satzes verändert. Für den dritten Satz müssen zuvor einige Begriffe wie „natürliche Zahlen“, „eindeutig“ und „Primzahlfaktoren zerlegen“ erklärt werden, für die es aber einen weiten Konsens über die Bedeutung gibt. Daher ist auch der dritte Satz eine Aussage, die als richtig bewiesen wurde. Der vierte Satz ist eine persönliche und subjektive Einschätzung und kann daher nicht eindeutig als wahr oder falsch bezeichnet werden, da die Person und deren Einschätzung nicht eindeutig definiert ist. Der fünfte Satz ist analog zum dritten Satz eine Aussage, von der bisher aber niemand weiß, ob sie stimmt oder nicht. Es ist die Goldbach'sche Vermutung. Der sechste Satz ist so keine Aussage, da dieser Satz sowohl im Sinne des Herumfahrens aber auch im Sinne der Überfahrens verstanden werden kann und der Unterschied den Wahrheitsgehalt direkt beeinflusst. Der siebte Satz ist nach allgemeinem Verständnis eindeutig verständlich und kann auch als wahr oder falsch bezeichnet werden, ist also eine Aussage. Darüber hinaus ist der siebte Satz aber auch eine Komposition zweier Aussagen „Baden-Württemberg ist ein Bundesland“ und „Mannheim ist ein Bundesland“, die allgemein unterschiedlich eingestuft werden würden. Da hier die Komposition mit „und“ verlangt, dass beide Aussagen wahr sein müssen, damit die Gesamtaussage wahr sein kann, so wäre die siebte Aussage als falsch zu bezeichnen.

## 1.2. Aussagenlogik

Um Zusammenhänge zwischen Aussagen abstrakt darstellen zu können, werden Aussagen durch Platzhalter wie  $A$  oder  $B$  repräsentiert. Beispielsweise kann  $A$  die Aussage „5 ist eine gerade Zahl“ beschreiben. Die Aussage selbst kann dabei wahr oder falsch sein, eventuell wird der Wahrheitsgehalt erst durch die weitere Analyse bestimmt. Die Zusammenhänge zwischen Aussagen werden mit Junktoren beschrieben:

DEFINITION 1.3. Ein **Junktor** ist eine durch eine **Wahrheitstafel** eindeutig definierte Operation für eine Aussage oder für zwei Aussagen.

In Wahrheitstafeln werden alle möglichen Aussagemöglichkeiten der enthaltenen Variablen hier mit den Abkürzungen „w“ für wahr und „f“ für falsch aufgeführt und den daraus resultierenden Wahrheitswert aus dem zusammengesetzten Ausdruck. Mit dem Begriff des Junktors können nun elementare oder einfache Aussagen von zusammengesetzten Aussagen unterschieden werden.

DEFINITION 1.4. **Zusammengesetzte Aussagen** können äquivalent in zwei mit einem Junktor verbundene Aussagen zerlegt werden. **Elementare Aussagen** können nicht sinnvoll weiter zerlegt werden.

Das einfachste Beispiel für einen Junktor ist die logische Negation:

DEFINITION 1.5. Der Junktor  $\neg$  bezeichnet die **Negation**  $\neg A$  oder  $\overline{A}$  eines Ausdrucks  $A$  und besitzt die folgende Wahrheitstafel:

$A$	$\neg A$
f	w
w	f

Für elementare Aussagen ist eine Negation oft leicht durch Hinzufügen oder Weglassen des Wortes „nicht“ zu bestimmen. Liegt hingegen eine zusammengesetzte Aussage vor, so ist dies oft nicht mehr so einfach und benötigt weitere Überlegungen.

BEISPIEL 1.6. Die folgende Tabelle zeigt einige Aussagen mit ihrer Negation:

Aussage $A$	Negation $\neg A$
Die Zahl 5 ist gerade.	Die Zahl 5 ist nicht gerade.
Deutschland liegt nicht in Europa.	Deutschland liegt in Europa.
11 ist ungerade und eine Primzahl.	11 ist gerade oder keine Primzahl.
Alle Enten sind blau.	Es gibt eine Ente, die nicht blau ist.

Das dritte Beispiel ist eine durch „und“ zusammengesetzte Aussage aus der Aussage „11 ist ungerade“ und der Aussage „11 ist eine Primzahl“. Im letzten Beispiel bezieht sich die Aussage auf eine Menge von Objekten und ist dadurch wieder anders zu behandeln. Diese beiden Fälle werden in den Bemerkung 1.14 und in der Prädikatenlogik in Bemerkung 1.38 weiter erläutert.

DEFINITION 1.7. **Konjunktion, Disjunktion.** Der Junktor  $\wedge$  bezeichnet die **Konjunktion** oder das logische **Und**  $A \wedge B$  zwischen zwei Aussagen und der Junktor  $\vee$  bezeichnet die **Disjunktion** oder das logische **Oder**  $A \vee B$  zwischen zwei Aussagen  $A$  und  $B$ :

$A$	$B$	$A \wedge B$	$A \vee B$
f	f	f	f
f	w	f	w
w	f	f	w
w	w	w	w

Aus Aussagen, Junktoren und Klammerung zur Klarstellung der Bezüge können komplexere logische Ausdrücke wie  $A \vee (B \wedge A)$  neue, zusammengesetzte, Aussagen formuliert werden. Mit Hilfe der logischen Äquivalenz können so verschiedene Ausdrücke in ihrem Wahrheitsgehalt als Aussagen in direkte Beziehung gesetzt werden:

DEFINITION 1.8. Die **Logische Äquivalenz**  $A \leftrightarrow B$  oder auch  $A \Leftrightarrow B$  oder  $A = B$  zwischen zwei Aussagen  $A$  und  $B$  mit der folgenden Wahrheitstafel bezeichnet:

$A$	$B$	$A \leftrightarrow B$
f	f	w
f	w	f
w	f	f
w	w	w

Das Symbol für logische Äquivalenz unterscheidet sich je nach Anwendung: Der Doppelpfeil „ $\Leftrightarrow$ “ wird in Beweisen verwendet, wo größere Aussagenkomplexe in einen Zusammenhang gebracht werden. Das Gleichheitszeichen „ $=$ “ wird zwischen Umwandlungen zusammengesetzter logischer Ausdrücke verwendet. Der einfache Pfeil „ $\leftrightarrow$ “ findet Verwendung als gleichberechtigter Junktoren in logischen Aussagen. Im Gegensatz zu den bisherigen durchweg kommutativen Junktoren ist bei der Implikation die Reihenfolge der Aussagen wichtig:

DEFINITION 1.9. Der Junktoren  $\rightarrow$  wird als **Implikation**  $A \rightarrow B$  oder  $A \Rightarrow B$  zwischen zwei Aussagen  $A$  und  $B$  mit der folgenden Wahrheitstafel bezeichnet:

$A$	$B$	$A \rightarrow B$
f	f	w
f	w	w
w	f	f
w	w	w

Eine Äquivalenz zweier Aussagen kann beispielsweise durch zwei Implikationen gezeigt werden

$$(A \leftrightarrow B) = (A \rightarrow B) \wedge (B \rightarrow A).$$

BEISPIEL 1.10. Die Aussage  $(A \vee (B \wedge A)) \vee B$  kann auch einfacher als  $A \vee B$  geschrieben werden, es gilt also  $(A \vee (B \wedge A)) \vee B = A \vee B$  aufgrund der folgenden Wahrheitstafel:

$A$	$B$	$B \wedge A$	$A \vee (B \wedge A)$	$(A \vee (B \wedge A)) \vee B$	$A \vee B$
f	f	f	f	f	f
f	w	f	f	w	w
w	f	f	w	w	w
w	w	w	w	w	w

Aus den Wahrheitstafeln können einige direkte Eigenschaften der Disjunktion und Konjunktion abgelesen werden:



SATZ 1.11. Seien  $A$  und  $B$  beliebige Aussagen, dann gelten die folgenden logischen Äquivalenzen:

<b>Kommutativität</b>	$A \wedge B$	$=$	$B \wedge A$
	$A \vee B$	$=$	$B \vee A$
<b>Assoziativität</b>	$A \wedge (B \wedge C)$	$=$	$(A \wedge B) \wedge C$
	$A \vee (B \vee C)$	$=$	$(A \vee B) \vee C$
<b>Idempotenz</b>	$A \wedge A$	$=$	$A$
	$A \vee A$	$=$	$A$
<b>Neutralität</b>	$A \wedge w$	$=$	$A$
	$A \vee f$	$=$	$A$
<b>Adsorption</b>	$A \wedge (A \vee B)$	$=$	$A$
	$A \vee (A \wedge B)$	$=$	$A$

SATZ 1.12. Für beliebige Aussagen  $A$ ,  $B$  und  $C$  gelten die folgenden logischen Distributivgesetze:

<b>Distributivität</b>	$A \wedge (B \vee C)$	$=$	$(A \wedge B) \vee (A \wedge C)$
	$A \vee (B \wedge C)$	$=$	$(A \vee B) \wedge (A \vee C)$

Mit Hilfe der Negation ergeben sich weitere Äquivalenzen:

SATZ 1.13. Seien  $A$  und  $B$  beliebige Aussagen, dann gelten die folgenden logischen Äquivalenzen:

<b>Doppelte Negation</b>	$\neg\neg A$	$=$	$A$
<b>Tautologie</b>	$A \vee (\neg A)$	$=$	$w$
<b>Kontradiktion</b>	$A \wedge (\neg A)$	$=$	$f$
<b>De Morgansche Regeln</b>	$\neg(A \wedge B)$	$=$	$(\neg A) \vee (\neg B)$
	$\neg(A \vee B)$	$=$	$(\neg A) \wedge (\neg B)$

Die Begriffe Tautologie und Kontradiktion werden allgemein für logische Ausdrücke verwendet, die unabhängig von den Wahrheitswerten von eventuell verwendeten Teilaussagen immer den Wahrheitswert wahr oder falsch besitzen. Jede der aufgeführten Äquivalenzen sind als logische Ausdrücke gesehen Tautologien.

BEMERKUNG 1.14. Die dritte Negation im Beispiel 1.6 kann mit Hilfe der de Morganschen Regeln durchgeführt werden: Wenn die Aussage  $A$  „11 ist ungerade und eine Primzahl“ zerlegt wird in  $A = B \wedge C$  mit den Aussagen  $B$  für „11 ist ungerade“ und  $C$  für „11 ist eine Primzahl“, so ist  $\neg A = \neg(B \wedge C)$ , also lautet die Negation wie angegeben entsprechend „11 ist gerade oder keine Primzahl“.

Die Aussage aus Beispiel 1.10 kann nun mit Hilfe der Äquivalenzen umgeformt und vereinfacht werden:

$$\begin{aligned}
 (A \vee (B \wedge A)) \vee B &= (A \vee (A \wedge B)) \vee B && \text{(Kommutativität)} \\
 &= (A) \vee B && \text{(Adsorption)} \\
 &= A \vee B
 \end{aligned}$$

Mit Hilfe von Wahrheitstabellen und durch die Anwendung von logischen Äquivalenzen können Aussagen geprüft werden. Für das logische Schließen von Aussagen bieten sich aber deutlich mächtigere Verfahren an:

### 1.3. Logisches Schließen

Mit der Aussagenlogik können zusammengesetzte Ausdrücke formal beschrieben und umgeformt werden. Im Rahmen eines vollständigen Ausprobierens können Aussagen belegt werden. Durch logisches Schließen können weit effizienter viele weitere Aussagen belegt werden. Dabei wird zwischen dem **Kalkül**, **Präpositionen** und **Konklusionen** unterschieden: In einem Kalkül oder logischen System werden logische Axiome, das sind grundlegende und nicht bewiesene Aussagen, vorausgesetzt. Logische Schlüsse bestehen dann aus Präpositionen, das sind eine Menge von Aussagen, die Voraussetzungen, die zusammen mit den Aussagen des Kalküls nachvollziehbar verwendet werden können, um die gewünschte Konklusion zu belegen. Was Mengen genau sind, wird im folgenden Kapitel genauer definiert, hier reicht es zu wissen, dass es sich um eine nicht geordnete Anzahl von Voraussetzungen sind. Im Folgenden werden zwei Notationen zur Darstellung von Präpositionen und Konklusionen von logischen Schlüssen verwendet: Soll die Konklusion  $B$  aus den Voraussetzungen oder Präpositionen  $A$  und  $A \rightarrow B$  gezeigt werden, so ist die klassische Notation folgendermaßen:

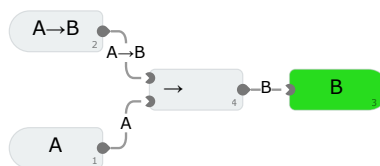
$$\frac{A \quad A \rightarrow B}{B}$$

Da die Präpositionen eine Menge von Aussagen sind, ist diese Darstellung dazu gleichbedeutend:

$$\frac{A \rightarrow B \quad A}{B}$$

Dieser Beweis von Präposition zu Konklusion kann nur geführt werden, wenn das zu Grunde liegende Kalkül eine entsprechende Auflösung von Implikation und Vorbedingung zur Verfügung stellt.

Innerhalb des visuellen Beweisumgebung der **Incredible Proof Machine** [4] <http://incredible.pm/> von Joachim Breitner, werden Beweise durch die Curry-Howard Korrespondenz visuell dargestellt:



Die visuelle Beweisumgebung soll helfen, das Grundprinzip des exakten logischen Beweisens zu verstehen, und gleichzeitig auch eine unmittelbare Überprüfung der eigenen Beweisführung zu ermöglichen. Wenn ein Beweis visuell erfolgreich, also korrekt, durchgeführt wird, kann damit der schriftliche Beweis leichter formuliert und damit erlernt werden. Die Entwicklung eines Beweises entspricht damit der Entwicklung eines Algorithmus, da die Präpositionen den Vorbedingungen entsprechen, die Axiomatik oder des Kalküls sind die erlaubten Operationen der Programmiersprache und die Konklusion entspricht dem erwarteten Ziel am Ende. Natürlich ist nicht jede Aussage beweisbar, genau wie ein Programm nur entwickelt werden kann, wenn die nötigen Voraussetzungen oder Präpositionen und die Mächtigkeit der Programmiersprache die Lösung ermöglicht.

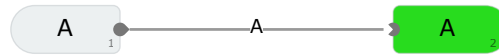
BEISPIEL 1.15. Die einfachsten Beweise können ohne Aussagen aus einem Kalkül geführt werden:

$$\frac{A}{A}$$

Hier ist die zu zeigende Konklusion direkt aus der gegebenen Prämisse belegbar und könnte lauten:

BEWEIS. Die Konklusion  $A$  ergibt sich aus der Prämisse  $A$ .  $\square$

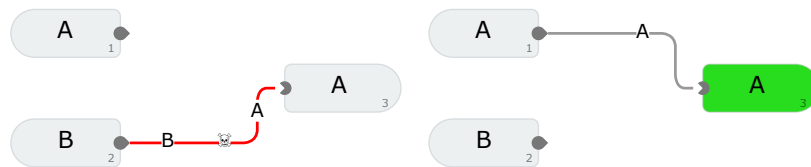
Das Symbol am Ende bedeutet „quod erat demonstrandum“, kurz „q.e.d.“, lateinisch für „was zu beweisen war“. Visuell wird der Beweis entsprechend durch Verbindung der Prämisse mit der Konklusion geführt:



Der schriftliche Beweis für den logischen Schluss

$$\frac{A \quad B}{A}$$

würde korrekt wie oben lauten, eine falsche Version hingegen, die beispielsweise versucht alleine aus  $B$  die Konklusion  $A$  zu schließen, muss der lesenden Person offensichtlich falsch erscheinen. Visuell wird so ein Fehler im Gegensatz zum korrekten Beweis unmittelbar markiert:

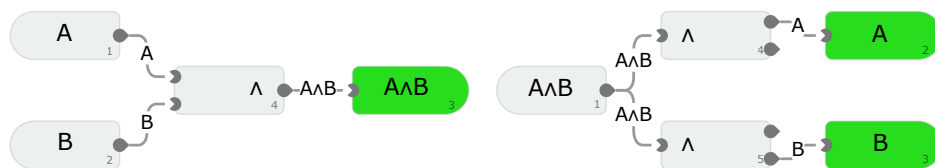


Im Folgenden werden die Regeln des Kalküls der klassischen Logik vorgestellt, und wie damit formal und visuell Beweise geführt werden können.

AXIOM 1.16. Die Regeln für die **Konjunktion** besagen, dass aus den Prämissen von zwei Einzelaussagen  $A$  und  $B$  die Konjunktion  $A \wedge B$  folgt, und dass aus der Konjunktion  $A \wedge B$  die Einzelaussagen  $A$  und  $B$  folgen, und hier als Regeln K, KL und KR beschrieben werden:

$$\text{K: } \frac{A \quad B}{A \wedge B} \quad \text{KL: } \frac{A \wedge B}{A} \quad \text{KR: } \frac{A \wedge B}{B}$$

In der visuellen Darstellung der drei Regeln K, KL und KR sind die Regeln KL und KR zu einem Block zusammengeführt, von dem wahlweise nur ein Ausgang zur Verwendung kommen kann:



Jetzt kann beispielsweise die Kommutativität der Konjunktion festgestellt werden:

SATZ 1.17. Die Konjunktion ist kommutativ, das heisst es gilt:

$$\frac{A \wedge B}{B \wedge A}$$

BEWEIS. Ist  $A \wedge B$  als Prämisse gegeben, so folgen aus den Regeln KL und KR die Aussagen  $A$  und  $B$ . Mengen von Aussagen haben keine Reihenfolge und somit können die Aussagen in der Reihenfolge vertauscht werden. Mit Regel K folgt dann aus den Aussagen  $B$  und  $A$  die Konklusion  $B \wedge A$ .  $\square$

Die Schritte des Beweises können auch wie in [7] durchnummeriert werden, und in jedem Schritt wird wie in einem Programmlisting genau eine Regel mit Angabe der durch den Schritt beschriebenen verwendeten Aussagen angewendet, damit der Beweis optimal nachvollziehbar wird:

Schritt	Aussage	Begründung
1	$A \wedge B$	Prämisse
2	$A$	KL 1
3	$B$	KR 1
4	$B \wedge A$	K 3 2

Es ist auch möglich, den Beweis als Baum darzustellen:

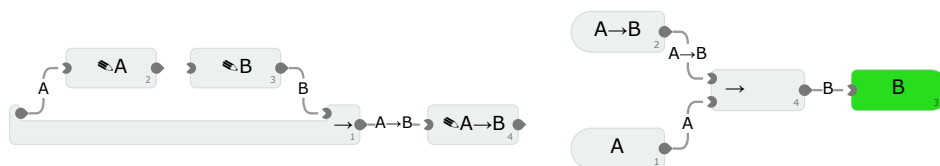
$$\text{K: } \frac{\text{KR: } \frac{A \wedge B}{B} \quad \text{KL: } \frac{A \wedge B}{A}}{B \wedge A}$$

Zur Übung und zur Selbstkontrolle sind die tabellarische oder die Baum-Darstellung am Anfang sehr hilfreich und sollten konsequent durchgeführt werden. Wenn beim Lesenden die genaue Kenntnis der verwendeten Axiomatik vorausgesetzt werden kann, werden in Texten bei eindeutigen Situationen die einzelnen Regeln nicht mehr aufgeführt.

AXIOM 1.18. Die Regeln für die **Implikation** besagen, dass wenn alleine aus einer Aussage  $A$  die Aussage  $B$  gefolgert werden kann, so eine Implikation  $A \rightarrow B$  induziert wird, und dass aus einer Implikation  $A \rightarrow B$  und der gegebenen Prämisse  $A$  die Aussage  $B$  gefolgert wird und die Implikation eliminiert wird:

$$\text{II: } \frac{\boxed{\frac{A}{B}}}{A \rightarrow B} \quad \text{IE: } \frac{A \rightarrow B \quad A}{B}$$

Der Kasten um die induzierte Implikation stellt dar, dass hier nur temporär  $A$  angenommen wird und eventuelle Auswirkungen nur durch die erzeugte Implikation entstehen können. Die Elimination der Implikation wird auch **Modus Ponens** genannt. Die visuelle Darstellung der Regeln II und IE sind:



Aus den Regeln ergibt sich direkt die Transitivität der Implikation:

SATZ 1.19. Die Implikation ist **transitiv**, das heisst es gilt:

$$\frac{A \rightarrow B \quad B \rightarrow C}{A \rightarrow C}$$

BEWEIS. Angenommen  $A$  gelte, so folgt nach der ersten Prämisse  $A \rightarrow B$ , dass  $B$  gilt. Nach der zweiten Prämisse  $B \rightarrow C$  gilt mit  $B$  dann auch  $C$ . Da aus der Annahme  $A$  so die Aussage  $C$  gezeigt haben, gilt die Konklusion  $A \rightarrow C$ .  $\square$

Der tabellarische Beweis ist entsprechend:

Schritt	Aussage	Begründung
1	$A \rightarrow B$	Prämisse
2	$B \rightarrow C$	Prämisse
3.1	$A$	Annahme
3.2	$B$	IE 1 3.1
3.3	$C$	IE 2 3.2
3	$A \rightarrow C$	II 3.1 3.3

Die lokale Untersuchung wird hier mit Unterschriften geführt, damit die dort entwickelten Aussagen auf Basis der lokalen Annahme oder lokalen Prämisse nicht fehlerhaft dann im eigentlichen Beweis genutzt werden.

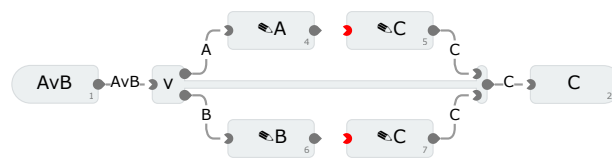
AXIOM 1.20. Die Regeln für die **Disjunktion** besagen, dass jeweils aus einer Aussage  $A$  oder  $B$  die Disjunktion  $A \vee B$  erzeugt werden kann, und dass aus einer Disjunktion und einer Folgerung einer Aussage  $C$  in beiden Fällen dann auch  $C$  gefolgert werden kann:

$$\text{DL: } \frac{A}{A \vee B} \quad \text{DR: } \frac{B}{A \vee B} \quad \text{D: } \frac{A \vee B \quad \boxed{\frac{A}{C}} \quad \boxed{\frac{B}{C}}}{C}$$

Visuell werden die Regeln DL und DR als einfache Bausteine dargestellt:



Für die Regel D muss die Aussage  $C$  in jedem der zwei Fälle nachgewiesen werden:



Auf Basis dieser Regeln können Assoziativität und Kommutativität der Disjunktion bewiesen werden, wie auch die Distributivität mit der Konjunktion:

SATZ 1.21. *Es gilt:*

$$\frac{A \wedge (B \vee C)}{(A \wedge B) \vee (A \wedge C)}$$

BEWEIS. Aus der Prämisse  $A \wedge (B \vee C)$  folgt nach KL und KR, dass  $A$  und  $B \vee C$  erfüllt sind. Aus den Aussagen  $A$  und  $B \vee C$  ist nun mit Regel D die Konklusion  $(A \wedge B) \vee (A \wedge C)$  zu zeigen:

- (1) Fall: Ist  $B$  erfüllt, so gilt nach K mit  $A$  und  $B$ , dass  $A \wedge B$  gilt.  
Wegen DL ist mit  $A \wedge B$  auch  $(A \wedge B) \vee (A \wedge C)$  erfüllt.

(2) Fall: Ist  $C$  erfüllt, so gilt nach K mit  $A$  und  $C$ , dass  $A \wedge C$  gilt.

Wegen DR ist mit  $A \wedge C$  auch  $(A \wedge B) \vee (A \wedge C)$  erfüllt.

Da mit der Aussage  $B \vee C$  und in beiden Fällen  $B$  und  $C$  die Aussage  $(A \wedge B) \vee (A \wedge C)$  erfüllt ist, gilt diese nach Regel D allgemein und die Konklusion ist bewiesen.  $\square$

Der entsprechende tabellarische Beweis zu Satz 1.21 könnte so geschrieben werden:

Schritt	Aussage	Begründung
1	$A \wedge (B \vee C)$	Prämisse
2	$A$	KL
3	$B \vee C$	KR
4.1	$B$	Annahme
4.1.1	$A \wedge B$	K 2 4.1
4.1.2	$(A \wedge B) \vee (A \wedge C)$	DL 4.1.1
4.2	$C$	Annahme
4.2.1	$A \wedge C$	K 2 4.2
4.2.2	$(A \wedge B) \vee (A \wedge C)$	DR 4.2.1
4	$(A \wedge B) \vee (A \wedge C)$	D 3 [4.1 4.1.2] [4.2 4.2.2]

Mit der Einführung des falschen Aussagewerts  $\perp$  können nun auch Negationen beschrieben werden:

AXIOM 1.22. Die Regel für die **Falsche Aussage**  $\perp$  besagt, dass **ex falso quodlibet** alles gefolgert werden kann:

$$F: \frac{\perp}{A}$$

Um die Aussage  $\neg A$  auszudrücken, kann durch dieses Axiom synonym die Notation  $A \rightarrow \perp$  verwendet werden. Es kann jetzt auch das wichtige Schlussprinzip Modus Tollens bewiesen werden:

SATZ 1.23. **Modus Tollens:** Gilt  $A \rightarrow B$  und  $\neg B$ , so gilt  $\neg A$ , es gilt also:

$$\frac{A \rightarrow B \quad B \rightarrow \perp}{A \rightarrow \perp}$$

BEWEIS. Es gelten die Prämissen  $A \rightarrow B$  und  $B \rightarrow \perp$ .

- (1) Angenommen es gilt  $A$ , dann ist zur Anwendung von II zu zeigen, dass dies auf  $\perp$  führt.
  - (a) Gilt  $A$  so ist mit  $A \rightarrow B$  nach Regel IE damit auch  $B$  gegeben.
  - (b) Gilt  $B$  und nach Prämisse  $B \rightarrow \perp$ , so ist nach Regel B die Aussage  $\perp$  hergeleitet.
- (2) Damit gilt nach Regel II die Konklusion  $A \rightarrow \perp$ .

$\square$

Beispielsweise kann für den indirekten Beweis eine Schlussrichtung bewiesen werden:

SATZ 1.24. Aus  $A \rightarrow B$  folgt  $\neg B \rightarrow \neg A$ , es gilt also:

$$\frac{A \rightarrow B}{(B \rightarrow \perp) \rightarrow (A \rightarrow \perp)}$$

BEWEIS. Es gelte die Prämisse  $A \rightarrow B$ .

- (1) Sei zusätzlich  $B \rightarrow \perp$ , dann ist zur Anwendung von Regel II daraus  $A \rightarrow \perp$  zu folgern.
  - (a) Sei zusätzlich  $A$  gegeben, dann ist zur Anwendung von II daraus  $\perp$  zu folgern.
    - (i) Mit  $A \rightarrow B$  und  $A$  gilt nach Regel IE, dass  $B$  gilt,
    - (ii) und zusammen mit  $B \rightarrow \perp$  ergibt  $B$  nach Regel IE  $\perp$ .
  - (b) Damit wurde nach II soeben  $A \rightarrow \perp$  gezeigt,
- (2) und wiederum nach Regel II die Konklusion  $(B \rightarrow \perp) \rightarrow (A \rightarrow \perp)$ .

□

Die umgekehrte Richtung, also dass aus  $\neg B \rightarrow \neg A$  dann  $A \rightarrow B$  folgt, ist jetzt aber noch nicht beweisbar, genauso wie zwar aus  $\neg\neg\neg A$  die Aussage  $\neg A$  gefolgert werden kann, noch nicht jedoch aus der doppelten Verneinung  $\neg\neg A$  dann die Aussage  $A$ . Dazu fehlt noch der Ausschluss des Dritten zur Vervollständigung des Kaküls der klassischen Logik:

AXIOM 1.25. Die Regel **Tertium Non Datur** besagt, dass eine Aussage  $A$  wahr oder  $\neg A$  beziehungsweise  $A \rightarrow \perp$  wahr ist.

$$\text{TND: } \frac{}{A \vee (A \rightarrow \perp)}$$

Diese Regel besitzt keine Prämissen und kann damit beliebige Aussagen „erzeugen“, damit verlässt diese Regel die konstruktive Logik, bei der Beweise immer konstruktiv sein müssen. Erst mit diesem Axiom wird der nicht-konstruktive indirekte Beweis benutzbar:

SATZ 1.26. **Indirekter Beweis:** Aus  $\neg B \rightarrow \neg A$  folgt  $A \rightarrow B$ , es gilt also:

$$\frac{(B \rightarrow \perp) \rightarrow (A \rightarrow \perp)}{A \rightarrow B}$$

BEWEIS. Gegeben sei die Prämisse  $(B \rightarrow \perp) \rightarrow (A \rightarrow \perp)$ .

- (1) Sei zusätzlich  $A$  gegeben, zur Anwendung von II ist daraus für die Konklusion  $B$  zu folgern.
  - (a) Nach TND gilt  $B \vee (B \rightarrow \perp)$ .
  - (b) Zur Anwendung der Regel D wird nun aus den Fällen  $B$  und  $B \rightarrow \perp$  jeweils  $B$  gefolgert:
    - (i) Fall: Gilt  $B$ , so ist das gewünschte Ergebnis schon gegeben.
    - (ii) Fall: Es gelte  $B \rightarrow \perp$ ,
      - (A) so gilt nach der Prämisse  $(B \rightarrow \perp) \rightarrow (A \rightarrow \perp)$  und Regel IE, dass  $A \rightarrow \perp$ .
      - (B) Da  $A$  gegeben, folgt aus  $A \rightarrow \perp$  mit Regel IE  $\perp$ .
      - (C) Ex falso quodlibet kann mit Regel F aus  $\perp$  die Aussage  $B$  hergeleitet werden.
  - (c) Nach Regel D folgt damit aus beiden Fällen und gegebener Disjunktion die Aussage  $B$ .
- (2) Damit ist nach Regel II die Konklusion  $A \rightarrow B$ .

□

### 1.4. Prädikatenlogik

Mit der klassischen Aussagenlogik können viele Zusammenhänge beschrieben und analysiert werden. Sie hat aber ihre Grenzen, wenn es um Aussagen über mehrere Objekte gleichzeitig geht. Beispielsweise kann in der Aussage „Nicht alle Vögel können fliegen.“ der Zusammenhang „nicht alle“ bisher nicht ausgedrückt werden. Dazu wird die Aussagenlogik um die Konzepte der **Prädikate** und **Quantoren** erweitert:

DEFINITION 1.27. Ein **Prädikat**  $P$  ist eine Funktion einer logischen Aussage  $P(x)$  oder  $P(x_1, \dots, x_n)$ , dessen Subjekt  $x$  oder Subjekte  $x_1, \dots, x_n$  variabel sind.

Der Begriff der Funktion wird später noch genauer erklärt. Hier zunächst nur vorausgesetzt, dass der logische Ausdruck für jeden Parameter  $x$  oder Parameterliste  $x_1, \dots, x_n$  eindeutig ausgewertet werden kann. Wenn im Folgenden nur von einstelligen Prädikaten  $P(x)$  geschrieben wird, so sind damit immer auch mehrstellige Prädikate wie  $P(x, y)$ ,  $P(x, y, z)$  oder  $P(x_1, \dots, x_n)$  gemeint.

BEISPIEL 1.28. Die Aussagen aus Beispiel 1.6 mit Hilfe von Prädikaten ausgedrückt:

Aussagen	Prädikat	Prädikataussage
Die Zahl 5 ist gerade.	$G(x)$ : Die Zahl $x$ ist gerade.	$G(5)$
Deutschland liegt nicht in Europa.	$E(x)$ : $x$ liegt in Europa.	$\neg E(\text{Deutschland})$
11 ist ungerade und eine Primzahl.	$G$ wie oben, $P(x)$ : $x$ ist eine Primzahl	$\neg G(x) \wedge P(x)$
Alle Enten sind blau.	$B(x)$ : $x$ ist Blau, $D(x)$ : ist eine Ente	$\forall D(x) : B(x)$

Das letzte Beispiel hat mit dem Symbol  $\forall$  schon das Konzept der Quantoren vorausgegriffen, die jetzt eingeführt werden.

**Quantoren** sind Operatoren für Prädikate:

DEFINITION 1.29. Der **Allquantor**  $\forall x : B(x)$ , oder oft  $\forall A(x) : B(x)$ , drückt aus, dass die folgende Aussagen  $B(x)$  für alle Parameter  $x$ , oder alle Parameter  $x$  mit  $A(x)$ , gilt.

Der **Existenzquantor**  $\exists x : B(x)$ , oder oft  $\exists A(x) : B(x)$ , drückt aus, dass es mindestens einen Parameter  $x$ , oder ein  $x$  mit  $A(x)$ , gibt, so dass  $B(x)$  gilt.

BEMERKUNG 1.30. Die vereinfachenden Schreibweisen der Ausdrücke  $\forall A(x) : B(x)$  und  $\exists A(x) : B(x)$ , die oft mit Hilfe von später eingeführten Mengen mit  $A(x) : x \in M$  als  $\forall x \in M : B(x)$  oder  $\exists x \in M : B(x)$  verwendet werden, können so in die elementare Form umgeschrieben werden:

$$\forall A(x) : B(x) \Leftrightarrow \forall x : \neg A(x) \vee B(x)$$

$$\exists A(x) : B(x) \Leftrightarrow \exists x : A(x) \wedge B(x)$$

Die Symbole des Allquantors und des Existenzquantors sind vertikal oder horizontal gespiegelte Buchstaben A und E, deren Schreibweise nach Gentzen 1934 und Peano 1897 den Begriffe „Alle“ und „Existenz“ entlehnt sind.

Bei einer begrenzten Anzahl von möglichen Parametern, hier beispielsweise die Zahlen 1, 2 und 3, können die Quantoren durch Konjunktion und Disjunktion beschrieben werden:

$$\forall x : A(x) \Leftrightarrow A(1) \wedge A(2) \wedge A(3)$$

$$\exists x : A(x) \Leftrightarrow A(1) \vee A(2) \vee A(3)$$



Da eine Aussage mit einem Quantor wieder eine Aussage ist, können Quantoren verkettet werden.

BEISPIEL 1.31. Wie wichtig die Reihenfolge von Quantoren in Fällen ist, wo sich die Quantoren unterscheiden, wird am Beispiel des Prädikats

$$L(x, y) : x \text{ liebt } y$$

anschaulich klar:

Prädikatenaussage	Direkte Übersetzung	Vereinfachung
$\forall x : \forall y : L(x, y)$	Für alle $x$ und alle $y$ wird $y$ von $x$ geliebt.	Jede(r) liebt jede(n).
$\forall x : \exists y : L(x, y)$	Für alle $x$ gibt es ein $y$ , das $x$ liebt.	Jede(r) liebt jemanden.
$\exists y : \forall x : L(x, y)$	Es gibt ein $y$ , das von allen $x$ geliebt wird.	Alle lieben eine(n).
$\exists x : \forall y : L(x, y)$	Es gibt ein $x$ , das alle $y$ liebt.	Eine(r) liebt alle.
$\forall y : \exists x : L(x, y)$	Für alle $y$ gibt es ein $x$ , das $y$ liebt.	Jede(r) wird geliebt.
$\exists x : \exists y : L(x, y)$	Es gibt ein $x$ , für das ein geliebtes $y$ existiert.	Jemand liebt jemanden.

Beispielsweise ist hier nachvollziehbar, dass aus der dritten Aussage „Alle lieben eine(n).“ die zweite Aussage „Jede(r) liebt jemanden.“ folgt, aber die Gegenrichtung wird nicht allgemein gelten. Zu beachten ist auch, dass die Existenzaussagen nicht bedeuten, dass es jeweils nur genau einen Fall gäbe: Ganz im Gegenteil können alle Allquantoren durch schwächere Existenzquantoren ersetzt werden, und die Aussagen bleiben wahr. Die Rückrichtung ist jedoch nicht allgemein gültig.

Die formalen Definitionen der Quantoren beziehen sich auf deren Elimination und Erzeugung:

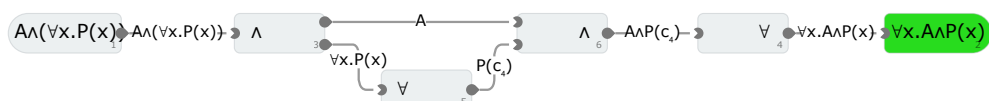
AXIOM 1.32. Der **Allquantor** zu einem Parameter zu einem Prädikat, ist gleichbedeutend dazu, dass eine Aussage für beliebige Parameter  $t$  gilt:

$$\text{AE: } \frac{\forall x : B(x)}{B(t)} \qquad \text{AI: } \frac{\boxed{\begin{array}{c} t : \\ t \\ \hline B(t) \end{array}}}{\forall x : B(x)}$$

Visuell sind die Elimination und Induktion des Allquantors einfache Blöcke, bei denen besonders die Vorbedingung der Allquantor-Induktion für einen beliebigen Parameter viel Sorgfalt in der Beweisführung erfordert:

$$\neg \forall x. P_3(x) \rightarrow \forall x. \neg P_3(x) \quad \neg P_1(c_1) \rightarrow \forall x. \neg P_1(x)$$

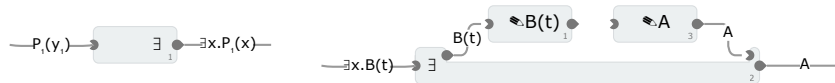
BEISPIEL 1.33. Im visuellen Beweis für die Aussage  $A \wedge (\forall x : P(x)) \Rightarrow \forall x : (A \wedge P(x))$  ist die Induktion für den Allquantor erfüllt, da die betreffende starke Aussage für den beliebigen Parameter aus einer Auflösung eines Allquantors gegeben ist:



AXIOM 1.34. Der **Existenzquantor** wird aus einer exemplarischen Aussage erzeugt, und mit einer Existenzaussage können andere Aussagen gezeigt werden, die für einen beliebigen Parameter gültig sind:

$$\text{EI: } \frac{B(y)}{\exists x : B(x)} \quad \text{EE: } \frac{\exists x : B(x) \quad \boxed{\begin{array}{c} t : \\ B(t) \\ \hline A \end{array}}}{A}$$

Visuell ist die Induktion ein einfacher Block, der aus einem Beispiel die Quantoraussage erzeugt, die Elimination wird über einen Einschub abgebildet:



SATZ 1.35. Für Prädikate  $P$  mit Parameter  $x$  und  $y$  ergeben sich folgende Äquivalenzen:

$$\begin{aligned} \forall x : \forall y : P(x, y) &\Leftrightarrow \forall y : \forall x : P(x, y) \\ \exists x : \exists y : P(x, y) &\Leftrightarrow \exists y : \exists x : P(x, y) \end{aligned}$$

BEWEIS. Wegen der Austauschbarkeit von  $x$  und  $y$  ist jeweils nur eine Richtung zu zeigen:

- (1)  $\forall x : \forall y : P(x, y) \Rightarrow \forall y : \forall x : P(x, y)$
- (2)  $\exists x : \exists y : P(x, y) \Rightarrow \exists y : \exists x : P(x, y)$

Diese Beweise werden in den Übungen geführt. □

Unterschiedliche Quantoren sind nur in eine Richtung vertauschbar, vergleichen Sie dazu Beispiel 1.31:

SATZ 1.36. Für Prädikate  $P$  mit Parameter  $x$  und  $y$  gilt:

$$\exists x : \forall y : P(x, y) \Rightarrow \forall y : \exists x : P(x, y)$$

BEWEIS. Als Übung. □

Negationen wandeln den Typ des Quantors:

SATZ 1.37. Für Prädikate  $P$  mit Parameter  $x$  ergeben sich folgende Äquivalenzen:

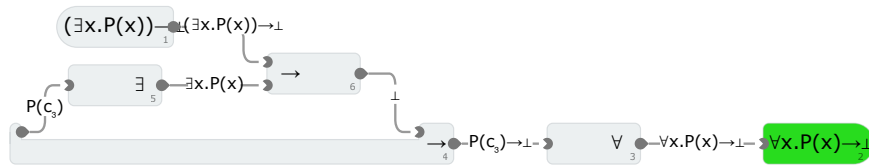
$$\begin{aligned} \neg \forall x : P(x) &\Leftrightarrow \exists x : \neg P(x) \\ \neg \exists x : P(x) &\Leftrightarrow \forall x : \neg P(x) \end{aligned}$$

BEWEIS. Es sind vier einzelne Aussagen zu beweisen:

- (1)  $\neg \forall x : P(x) \Rightarrow \exists x : \neg P(x)$
- (2)  $\exists x : \neg P(x) \Rightarrow \neg \forall x : P(x)$
- (3)  $\neg \exists x : P(x) \Rightarrow \forall x : \neg P(x)$
- (4)  $\forall x : \neg P(x) \Rightarrow \neg \exists x : P(x)$

Hier wird nur Fall (3) gezeigt, die restlichen Beweise erfolgen in den Übungen:

Gegeben ist, dass  $(\exists x : P(x)) \rightarrow \perp$  gilt, zu zeigen ist daraus  $\forall x : (P(x) \rightarrow \perp)$  :



Sei  $t$  beliebig und es gelte  $P(t)$ . Es wird gezeigt, dass daraus folgt, dass aus  $P(t)$  falsch folgt ist: Gilt  $P(t)$  so gilt nach EI, dass die Aussage  $\exists x : P(x)$  korrekt ist. Nach Prämisse folgt daraus falsch. Daher folgt aus  $P(t)$  falsch. Da dies für beliebige  $t$  mit  $P(t)$  gilt, folgt aus der Aussage  $P(t) \rightarrow \perp$  nach AI die Konklusion  $\forall x : (P(x) \rightarrow \perp)$ .  $\square$

BEMERKUNG 1.38. Nun kann die letzte Negation aus Beispiel 1.6 erklärt werden: Die Aussage „Alle Enten sind Blau“ wurde in Beispiel 1.28 schon in formale Schreibweise  $\forall D(x) : B(x)$  übersetzt. Für die Negation gilt nun:

$$\begin{aligned}
 & \neg \forall D(x) : B(x) \\
 \Leftrightarrow & \neg \forall x : \neg D(x) \vee B(x) && \text{Bemerkung 1.30} \\
 \Leftrightarrow & \exists x : \neg(\neg D(x) \vee B(x)) && \text{Satz 1.37} \\
 \Leftrightarrow & \exists x : D(x) \wedge \neg B(x) && \text{De Morgansche Regel Satz 1.13} \\
 \Leftrightarrow & \exists D(x) : \neg B(x) && \text{Bemerkung 1.30}
 \end{aligned}$$

Damit lautet die korrekte Negation „Es gibt eine Ente, die nicht blau ist“.

## 1.5. Beweistechniken

Grundsätzlich sollten Beweise immer damit beginnen, dass die Prämissen („Gegeben ist“) und die gewünschte Konklusion („Zu zeigen ist“) genau aufgeführt werden. Wenn in einem Beweis Hilfsaussagen benötigt werden, wie beispielsweise in Regeln D, AI oder EE, so sollten ebenso im Beweis der Teilaussage die lokalen Prämissen und die gewünschte Konklusion genau definiert werden. Selbstverständlich sollte auch genau gekennzeichnet werden, wann der Beweis vollständig ist, also die Konklusion erreicht wurde und alle benötigten Zwischenaussagen ebenso bewiesen wurden.

Zur Illustration befassen wir uns mit dem folgenden Satz:

SATZ 1.39. Sei  $n$  eine natürliche Zahl, also eine ganze positive Zahl. Dann ist  $n^2$  genau dann eine gerade Zahl, wenn  $n$  gerade ist.

Es ist möglich, eine Äquivalenz  $A \Leftrightarrow B$  direkt zu beweisen, wie in Beispiel 1.38 demonstriert, es ist aber immer sicherer und fast immer verständlicher, den Beweis in die zwei Teile  $A \Rightarrow B$  und  $B \Rightarrow A$  aufzuteilen, damit wirklich jeder Schritt in der natürlichen Beweisrichtung nachvollzogen und geprüft werden kann. Ein Beispiel für diese Beweistechnik ist in der Zerlegung der Aussagen im Beweis zu Satz 1.37 zu finden. Dieses Verfahren kann aber auch im Beweis zum Satz 1.39 angewendet werden:

BEWEIS. von Satz 1.39:

Gegeben ist:  $n$  ist eine ganze positive Zahl.

Zu zeigen ist: Genau dann, wenn  $n^2$  gerade ist, ist  $n$  gerade.

Dafür werden im Folgenden zwei Aussagen gezeigt:

$\Rightarrow$  Wenn  $n^2$  eine gerade Zahl ist, so ist  $n$  eine gerade Zahl.

$\Leftarrow$  Wenn  $n$  eine gerade Zahl ist, so ist  $n^2$  eine gerade Zahl.

Sind diese beiden Richtungen bewiesen, so ist die Äquivalenz bewiesen.  $\square$

Dieser Beweis ist natürlich nur vollständig, wenn beide Richtungen wirklich bewiesen werden.

Im Folgenden werden wir nutzen, dass eine Zahl  $n$  genau dann gerade ist, wenn sie als das Doppelte einer anderen ganzen positiven Zahl  $k$  geschrieben werden kann, also  $n = 2k$  gilt, und dass alle anderen positiven ganzen Zahlen, die also ungerade sind, immer als  $n = 2k - 1$  für eine ganze positive Zahl  $k$  geschrieben werden können.

Ein **direkter Beweis** einer Implikation  $A \Rightarrow B$  ist eine Abfolge von Implikationen zu Zwischenschritten

$$A \Rightarrow A_1 \Rightarrow A_2 \Rightarrow \dots \Rightarrow A_n \Rightarrow B,$$

die am Ende zur Konklusion  $B$  führen. Das Vorgehen ist genau durch Satz 1.19 begründet.

BEWEIS.  $\Leftarrow$  von Satz 1.39: Direkter Beweis von  $n$  ist gerade  $\Rightarrow n^2$  ist gerade.

Gegeben ist:  $n$  ist gerade.

Zu zeigen ist:  $n^2$  ist gerade.

- (1) Ist  $n$  gerade, so gibt es ein ganzes  $k$ , so dass  $n = 2k$  ist.
- (2) Damit ist  $n^2 = n \cdot n = 2k \cdot 2k = 2 \cdot 2k^2$ .
- (3) Damit ist  $m = 2k^2$  wieder eine ganze Zahl (was wir später noch erfahren werden).
- (4) Somit ist  $n^2 = 2 \cdot m$  eine gerade Zahl.

$\square$

Ein **Indirekter Beweis** macht sich die Äquivalenz  $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$  aus den Sätzen 1.26 und 1.24 zu Nutze. Um also  $A \Rightarrow B$  zu zeigen, wird die äquivalente Aussage  $\neg B \Rightarrow \neg A$  gezeigt.

BEWEIS.  $\Rightarrow$  von Satz 1.39: Indirekter Beweis von  $n^2$  ist gerade  $\Rightarrow n$  ist gerade.

Gegeben ist:  $n$  ist nicht gerade, also ungerade.

Zu zeigen ist:  $n^2$  ist nicht gerade, also ungerade.

- (1) Wenn  $n$  ungerade ist, so gibt es ein ganzes positives  $k$  mit  $n = 2k - 1$ .
- (2) Dann ist

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

- (3) Da  $k$  positive ganze Zahl, ist  $k^2 - k = k \cdot (k - 1)$  eine ganze Zahl, und größer oder gleich 0.
- (4) Damit ist  $m = 2(k^2 - k) + 1$  eine ganze positive Zahl.
- (5) Somit ist  $n^2 = 2m - 1$  eine ungerade Zahl.

$\square$

Ein **Beweis durch Widerspruch** nutzt die Äquivalenz  $(A \Rightarrow B) \Leftrightarrow \neg(A \wedge \neg B)$  und startet mit den Prämissen  $A$  und  $\neg B$ , um damit auf einen Widerspruch als auf Falsch zu schließen.

BEWEIS.  $\Leftarrow$  von Satz 1.39: Beweis durch Widerspruch von  $n$  ist gerade  $\Rightarrow n^2$  ist gerade.

Gegeben ist: Angenommen  $n$  ist gerade und  $n^2$  ist ungerade.

Zu zeigen ist: Dies führt auf einen Widerspruch.

- (1) Ist  $n$  gerade, so gibt es ein ganzes  $k$ , so dass  $n = 2k$  ist.
- (2) Damit ist  $n^2 = n \cdot n = 2k \cdot 2k = 2 \cdot 2k^2$ .
- (3) Damit ist  $m = 2k^2$  wieder eine ganze Zahl.
- (4) Da  $n^2$  ungerade, gibt es ein ganzes, positives  $p$  mit  $n^2 = 2 \cdot p - 1$ .
- (5) Also ist  $2 \cdot m = 2 \cdot p - 1$ , also  $p = m - \frac{1}{2}$ .
- (6) Das ist im Widerspruch dazu, dass sowohl  $p$  als auch  $m$  ganzzahlig sein sollen.

□

Der **Beweis durch Gegenbeispiel** kommt bei der Widerlegung von Aussagen mit Allquantor zum Einsatz: Um eine Aussage mit Allquantor zu widerlegen, reicht ein einziges Gegenbeispiel, welches nachvollziehbar der Aussage widerspricht.

BEISPIEL 1.40. Widerlegen Sie die Aussage „Für jede Primzahl  $p$  ist  $5(p^2 + p) + 1$  auch eine Primzahl“.

BEWEIS. Gegenbeispiel:  $5 \cdot (23^2 + 23) + 1 = 2761 = 11 \cdot 251$ .

□

Gegenbeispiele sind sehr kurze und gleichzeitig oft sehr starke Beweise. Um im Gegensatz eine Aussage mit einem Allquantor zu zeigen, gibt es die vollständige Induktion: Diese gibt es in verschiedenen Formen, die grundsätzliche Variante arbeitet auf den natürlichen Zahlen 1, 2, 3 und so weiter.

SATZ 1.41. **Vollständige Induktion** über den natürlichen Zahlen. Sei  $P$  ein Prädikat über den natürlichen Zahlen. Mit den folgenden zwei Schritten wird  $P(x)$  für alle natürlichen Zahlen  $x$  bewiesen:

Induktionsanfang  $n = 1$ :  $P(1)$  ist wahr.

Induktionsschritt  $n \rightarrow n + 1$ : Sei  $n$  eine natürliche Zahl und  $P(n)$  sei wahr. Dann folgt  $P(n + 1)$ .

Dann gilt  $P(x)$  für alle natürlichen Zahlen  $x$ .

Der Beweis basiert auf der Definition der natürlichen Zahlen und wird später erläutert.

SATZ 1.42. Die Summe aller natürlichen Zahlen bis  $n$  ist  $\sum_{k=1}^n k = \frac{n^2+n}{2}$ .

BEWEIS. Beweis mit vollständiger Induktion:

Induktionsanfang  $n = 1$ : Die Summe aller Zahlen bis 1 ist 1, und das gleicht  $\frac{1^2+1}{2} = 1$ .

Induktionsschritt:  $n \rightarrow n + 1$ :

Gegeben ist: Die Summe aller natürlichen Zahlen bis  $n$  ist  $\sum_{k=1}^n k = \frac{n^2+n}{2}$ .

Zu zeigen ist: Die Summe aller natürlichen Zahlen bis  $n + 1$  ist  $\frac{(n+1)^2+(n+1)}{2}$ .

- (1) Die Summe aller Zahlen bis  $n + 1$  ist die Summe aller Zahlen bis  $n$  plus  $n + 1$ .
- (2) Die Summe aller Zahlen bis  $n + 1$  ist demnach

$$\frac{n^2 + n}{2} + n + 1 = \frac{n^2 + 2n + 1 + n + 1}{2} = \frac{(n + 1)^2 + (n + 1)}{2}.$$

- (3) Damit ist die gesuchte Darstellung gezeigt.

Somit gilt die Formel für alle natürlichen Zahlen.

□

### 1.6. Aufgaben

**AUFGABE 1.** Sei die Aussage  $A$  das Ereignis, dass Sie im Pub-Quiz gewinnen, und  $B$  das Ereignis, dass Sie sich freuen. Formulieren Sie die folgenden zusammengesetzten Aussagen aus den beiden Aussagen:

- (1) Weder freue ich mich, noch gewinne ich im Pub-Quiz.
- (2) Ich gewinne im Pub-Quiz, wenn ich mich freue.
- (3) Wenn ich im Pub-Quiz gewinne, so bin ich nicht froh.
- (4) Keinesfalls werde ich im Pub-Quiz gewinnen.

**AUFGABE 2.** Sei  $A$  die Aussage, dass Sie für die Vorlesung üben, und  $B$  die Aussage, dass Sie in der Vorlesung aufpassen. Beschreiben Sie die folgenden Aussagen mit den Ereignissen:

- (1) Falls ich für die Vorlesung übe, so träume ich in der Vorlesung.
- (2) Niemals passe ich in der Vorlesung auf, ich übe aber dafür.
- (3) Ich übe viel, wenn ich in der Vorlesung nicht aufpasse.
- (4) Entweder übe ich, oder ich passe in der Vorlesung auf, aber nie beides.

**AUFGABE 3.** Modellieren Sie die folgenden Aussagen logisch und prüfen Sie, ob Felix am Raubzug beteiligt war: Nur Margot, Felix und Sascha können den Raub durchgeführt haben. Wenn Margot beteiligt war, jedoch Felix nicht, so war Sascha dabei. Sascha arbeitet nie alleine, aber Margot arbeitet nie mit Sascha.

**AUFGABE 4.** Formulieren Sie diese Aussagen mit Aussagenlogik und bewerten Sie den Schluss: Die Studierenden sind glücklich, wenn keine Klausur geschrieben wird. Der Dozent fühlt sich wohl, wenn die Studierenden glücklich sind. Wenn der Dozent sich wohl fühlt, so hat er keine Lust zu unterrichten. Wird aber keine Klausur geschrieben, so unterrichtet er gerne. Wird eine Klausur geschrieben?

**AUFGABE 5.** Formulieren Sie diese Aussagen mit Aussagenlogik und bestimmen Sie, ob Sarah eine gute Note bekommt:

- (1) Sarah bekommt genau dann in der Klausur eine gute Note, wenn sie lernt, alle Vorlesungen besucht und genug schläft.
- (2) Sarah kann nicht gut schlafen, wenn sie ständig Abends am Computer spielt.
- (3) Sarah besucht alle Vorlesungen, lernt, spielt ständig Abends am Computer und beteiligt sich sehr gut an der Vorlesungen.

**AUFGABE 6.** Der neue Diät-Tipp zur ausgewogenen Ernährung nur mit Kakao, Nachos und Erdnüssen in Boys Health lautet: Wenn es keinen Kakao zum Essen gibt, so muss es Nachos als Beilage geben. Wenn es Nachos als Beilage oder Kakao zum Trinken gibt, gibt es keine Erdnüsse. Genau dann wenn es Erdnüsse gibt oder keinen Kakao gibt, gibt es keine Nachos. Wie abwechslungsreich ist die Diät?

**AUFGABE 7.** Leiten Sie für einen logischen Ausdruck  $A$  die **Auslöschung**  $A \wedge f = f$  aus den Äquivalenzen der Aussagenlogik her.

**AUFGABE 8.** Leiten Sie für einen logischen Ausdruck  $A$  die **Auslöschung**  $A \vee w = w$  aus den Äquivalenzen der Aussagenlogik her.

**AUFGABE 9.** Vereinfachen Sie den logischen Ausdruck  $\neg(\neg A \wedge B) \wedge (A \vee B)$  mit Hilfe der Äquivalenzen der Aussagenlogik.

**AUFGABE 10.** Vereinfachen Sie den logischen Ausdruck  $(\neg A \wedge B) \vee \neg(A \vee B)$  mit Hilfe der Äquivalenzen der Aussagenlogik.

**AUFGABE 11.** Belegen Sie die logische Adsorption  $A \wedge (A \vee B) = A$  durch eine Wahrheitstabelle.

**AUFGABE 12.** Belegen Sie die logische Distributivität  $A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$  durch eine Wahrheitstabelle.

**AUFGABE 13.** Beweisen Sie die Kommutativität der Konjunktion visuell:

$$\frac{A \wedge B}{B \wedge A}$$

**AUFGABE 14.** Beweisen Sie die Assoziativität der Konjunktion visuell und als textuelle Beschreibung:

$$\frac{A \wedge (B \wedge C)}{(A \wedge B) \wedge C}$$

**AUFGABE 15.** Beweisen Sie, dass aus  $(A \rightarrow B) \wedge (A \rightarrow C)$  die Aussage  $A \rightarrow (B \wedge C)$  folgt, zeigen Sie also visuell und als tabellarische Beschreibung:

$$\frac{(A \rightarrow B) \wedge (A \rightarrow C)}{A \rightarrow (B \wedge C)}$$

**AUFGABE 16.** Beweisen Sie, dass aus der Äquivalenz  $A \leftrightarrow (A \rightarrow B)$  folgt, dass  $B$  gilt, zeigen Sie also visuell und als tabellarische Beschreibung:

$$\frac{A \rightarrow (A \rightarrow B) \quad (A \rightarrow B) \rightarrow A}{B}$$

**AUFGABE 17.** Beweisen Sie visuell diese Aussage und formulieren Sie einen schriftlichen Beweis:

$$\frac{(A \rightarrow \perp) \rightarrow \perp}{A}$$

**AUFGABE 18.** Beweisen Sie visuell diese Aussage ohne Verwendung von Tertium Non Datur und formulieren Sie einen schriftlichen Beweis:

$$\frac{((A \rightarrow \perp) \rightarrow \perp) \rightarrow \perp}{A \rightarrow \perp}$$

**AUFGABE 19.** Drücken Sie die beiden Aussagen mit Hilfe von Quantoren und dem Prädikat  $L(x, y)$  für  $x$  liebt  $y$  aus. Überlegen Sie nicht-formal, ob eine Aussage aus der anderen gefolgert werden kann und führen Sie dann den formalen Nachweis. Konstruieren Sie ein Gegenbeispiel, dass die Rückrichtung nicht stimmt.

- (1) Jede(r) liebt jemanden nicht.
- (2) Da ist eine Person, die von nicht eine(m/r) geliebt wird.

**AUFGABE 20.** Drücken Sie die beiden Aussagen mit Hilfe von Quantoren und dem Prädikat  $L(x, y)$  für  $x$  liebt  $y$  aus. Überlegen Sie nicht-formal, ob eine Aussage aus der anderen gefolgert werden kann und führen Sie dann den formalen Nachweis. Konstruieren Sie ein Gegenbeispiel, dass die Rückrichtung nicht stimmt.

- (1) Die Aussage, dass es für alle jemanden gibt, den sie oder er liebt, ist falsch.
- (2) Jede(r) wird von jemandem(m/r) nicht geliebt.

**AUFGABE 21.** Zeigen Sie die Folgerung  $\exists x : \neg P(x) \Rightarrow \neg \forall x : P(x)$ , zunächst visuell, einzugeben als

$$\frac{?x.(P(x) \rightarrow \text{False})}{(!x.P(x)) \rightarrow \text{False}},$$

und anschließend tabellarisch unter Angabe der verwendeten Axiome.

**AUFGABE 22.** Zeigen Sie die Folgerung  $\forall x : (P(x) \rightarrow A) \Rightarrow (\forall x : P(x)) \rightarrow A$  zunächst visuell, einzugeben als

$$\frac{!x.(P(x) \rightarrow A)}{(!x.P(x)) \rightarrow A},$$

und anschließend tabellarisch unter Angabe der verwendeten Axiome.

**AUFGABE 23.** Zeigen Sie, dass  $2^n \geq n^2$  für alle ganzen Zahlen  $n \geq 4$  gilt.

**AUFGABE 24.** Zeigen Sie, dass die Summe der ersten  $n$  ungeraden Zahlen gerade  $n^2$  ergibt.



## Mengen, Relationen und Abbildungen

### 2.1. Mengen

Die Beschreibung von Mengen ist ein elementares Werkzeug der Mathematik. Sie ermöglicht es, beliebige Objekte zu gruppieren und Aussagen auf in Mengen beschriebenen Klassen zu beschreiben.

DEFINITION 2.1. Eine **Menge** ist eine nicht geordnete Zuordnung verschiedener Objekte zu einem Ganzen. Die zugeordneten Objekte sind die **Elemente** der Menge. Jedes Objekt kann nur einmal einer Menge zugeordnet sein, aber Element vieler Mengen sein.

Eine Möglichkeit Mengen zu beschreiben, ist die einfache Aufzählung der Elemente:

$$A = \{1, 9, \odot, 4, \heartsuit, 12\}$$

Die Elemente haben in einer Menge keine Reihenfolge, daher spielt diese bei der Beschreibung der Menge keine Rolle. Mit dieser Beschreibung kann nun auch feststellen, dass die Zahl 9 ein Element der Menge  $A$  ist, und die Zahl 7 kein Element der Menge  $A$  ist.

DEFINITION 2.2. Gehört ein **Element**  $e$  zu einer Menge  $M$ , so wird dies als

$$e \in M$$

geschrieben. Gehört es nicht zur Menge  $M$ , so wird die Notation

$$e \notin M$$

verwendet.

Damit lauten die gerade beschriebenen Zusammenhänge:  $9 \in A$ ,  $7 \notin A$ .

Mengen können auch unendlich viele Elemente beinhalten. Bei einfachen Bildungsgesetzen, kann man die Menge mit Punkten illustrieren:

$$B = \{1, 3, 5, 7, 9, \dots\}$$

Die Menge  $B$  scheint die Menge aller positiven ungeraden Zahlen zu beschreiben, ganz sicher ist man sich aber nur, wenn man die Bildungsregel als Prädikat tatsächlich aufschreibt:

$$B = \{ x \mid P(x) \} = \{ x \mid x \text{ ist eine positive ungerade Zahl} \}$$

In dieser Notation gehören alle  $x$  zur Menge, die die darauf folgende Aussage erfüllen. Möchte man eine Menge aus allen Quadratzahlen positiver ungerader Zahlen beschreiben, so könnte man dies so tun:

$$C = \{ x^2 \mid x \text{ ist eine positive ungerade Zahl} \} = \{1, 9, 25, 49, \dots\}$$

Hier wurde jetzt naiv von Zahlen gesprochen, gemeint sind dabei **natürliche Zahlen**, die mit der 1 beginnen und alle Nachfolger beinhalten, die bei einer Erhöhung um 1 entstehen können, wie sie von Peano 1889 beschrieben wurden:

ABBILDUNG 2.1.1. Venn-Diagramme von Vereinigung und Schnitt von  $A$  und  $B$ AXIOM 2.3. Peano-Axiome für **natürliche Zahlen**

- (1) Die 1 ist eine natürliche Zahl.
- (2) Jede natürliche Zahl  $n$  hat einen Nachfolger  $S(n) = n + 1$ .
- (3) Aus  $S(n) = S(m)$  folgt  $n = m$ .
- (4) Die 1 ist kein Nachfolger einer natürlichen Zahl.
- (5) Enthält eine Menge  $X$  die 1 und mit jeder Zahl  $n$  auch den Nachfolger  $S(n)$ , so sind die natürlichen Zahlen eine Teilmenge von  $X$ .

Das 5. Axiom ist schließlich der Grund, warum die **Vollständige Induktion** funktioniert: Sie zeigt die Konklusion zunächst für das erste oder ein erstes Element, und leitet daraus die Aussage für alle weiteren Elemente her, die nach dem 5. Peano-Axiom mindestens die Menge der natürlichen Zahlen umfasst. Als Symbol für die Menge der natürlichen Zahlen wird das Zeichen  $\mathbb{N}$  verwendet:

$$\mathbb{N} = \{1, 2, 3, 4, 5, \dots\}$$

DEFINITION 2.4. Für zwei Mengen  $A, B$  sind **Vereinigung**  $A \cup B$  und **Schnitt**  $A \cap B$  definiert durch:

$$A \cup B = \{x \mid x \text{ ist Element von } A \text{ oder Element von } B\} = \{x \mid x \in A \vee x \in B\}$$

$$A \cap B = \{x \mid x \text{ ist Element von } A \text{ und Element von } B\} = \{x \mid x \in A \wedge x \in B\}$$

In Abbildung 2.1.1 sind Vereinigung und Schnitt zweier Mengen als Venn-Diagramme dargestellt.

Damit werden auch **natürliche Zahlen mit Null** oder **natürliche Zahlen nach DIN**  $\mathbb{N}_0$  und **ganze Zahlen**  $\mathbb{Z}$  definiert:

$$\mathbb{N}_0 = \mathbb{N} \cup \{0\} = \{0, 1, 2, 3, 4, 5, \dots\}$$

$$\mathbb{Z} = \{x, -x \mid x \in \mathbb{N}_0\} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

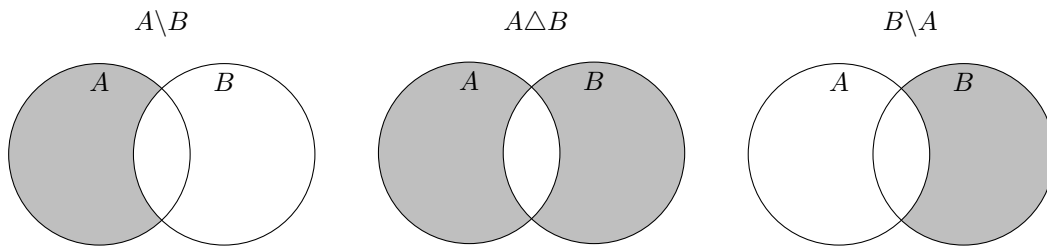
Es kann aber auch passieren, dass bei einem Schnitt zweier Mengen kein Ergebnis übrig bleibt:

DEFINITION 2.5. Die **leere Menge**  $\emptyset$  oder  $\{\}$  bezeichnet die Menge ohne ein einziges Element.

Die Menge aller ganzen oder Bruchzahlen nennen wir **rationale Zahlen**  $\mathbb{Q}$  mit ganzen **Zählern**  $z$  und natürlichen **Nennern**  $n$ :

$$\mathbb{Q} = \left\{ \frac{z}{n} \mid z \in \mathbb{Z}, n \in \mathbb{N} \right\}$$

Hier werden natürlich alle Zahlen mit Nenner 1 mit den entsprechenden ganzen Zahlen identifiziert, beispielsweise  $\frac{5}{1} = 5$ , und Brüche ebenso mit ihren gekürzten oder erweiterten Versionen, wie zum Beispiel  $\frac{4}{6} = \frac{2}{3} = \frac{4000}{6000}$ . Das Komma in der Beschreibung hat die gleiche Bedeutung wie die Konjunktion  $\wedge$ . Die rationalen Zahlen haben in der Informatik eine besondere Bedeutung, da die aktuell am häufigsten verwendeten **Gleitkommazahlen** nach **IEEE 754** Teilmengen der rationalen Zahlen sind, genauer sind es Brüche mit beschränktem Zähler und Zweier-Potenzen  $2^k$  im Nenner.

ABBILDUNG 2.1.2. Venn-Diagramme der Differenzen von  $A$  und  $B$ 

Da die rationalen Zahlen aber sehr spannende Zahlen wie  $\sqrt{2}$  oder die Kreiszahl  $\pi$  auslassen, gibt es die reellen Zahlen. Diese kann man gut als die Menge aller Grenzwerte konvergenter rationaler Folgen definieren, aber diese Begriffe sind nicht Thema dieser Vorlesung. Daher hier eine anschauliche, jedoch äquivalente Definition für eine **reelle Zahl** mit Hilfe von Dezimalzahlen wie 12.34521:

$$\mathbb{R} = \{ x \mid x \text{ ist als, eventuell unendliche, Dezimalzahl darstellbar} \}$$

Besonders interessant sind hier die Zahlen in  $\mathbb{R}$ , die nicht rational sind. Diese können wir mit der einseitigen Mengendifferenz beschreiben. Verwandt dazu sollte auch die symmetrische Mengendifferenz eingeführt werden, die in Abbildung 2.1.2 dargestellt werden.

DEFINITION 2.6. Für zwei Mengen  $A, B$  ist die **einseitige Mengendifferenz**  $A \setminus B$  und die **symmetrische Mengendifferenz**  $A \Delta B$  definiert durch:

$$A \setminus B = \{ x \mid x \in A \wedge x \notin B \}$$

$$A \Delta B = A \setminus B \cup B \setminus A$$

Damit sind  $\mathbb{R} \setminus \mathbb{Q}$  alle **irrationalen Zahlen**, also alle reelle Zahlen, die nicht gleichzeitig rational sind. Beispiele sind dafür  $\sqrt{2}$  oder  $\pi$ .

Eine besonders praktische Schreibweise gibt es für Intervalle auf den reellen Zahlen, wo man durch die Art der Klammern beschreibt, ob die Ränder dazu gehören oder nicht:

$$[a, b] = \{ x \in \mathbb{R} \mid a \leq x \leq b \}$$

$$(a, b] = \{ x \in \mathbb{R} \mid a < x \leq b \}$$

$$[a, b) = \{ x \in \mathbb{R} \mid a \leq x < b \}$$

$$(a, b) = \{ x \in \mathbb{R} \mid a < x < b \}$$

Speziell wird  $[a, b]$  **abgeschlossenes Intervall** von  $a$  nach  $b$  genannt und  $(a, b)$  wird als **offenes Intervall** zwischen  $a$  und  $b$  bezeichnet. Mit Hilfe des Symbols  $\infty$  für **unendlich** werden auch unbeschränkte Intervalle beschrieben:

$$(-\infty, a) = \{ x \in \mathbb{R} \mid x < a \}$$

$$(-\infty, a] = \{ x \in \mathbb{R} \mid x \leq a \}$$

$$[a, \infty) = \{ x \in \mathbb{R} \mid x \geq a \}$$

$$(a, \infty) = \{ x \in \mathbb{R} \mid x > a \}$$

Da es in den reellen Zahlen nicht möglich ist, Wurzeln aus negativen Zahlen zu ziehen, hat man auch die reellen Zahlen erweitert. Dazu führt man eine Konstante  $i$  mit der Eigenschaft ein, dass  $i^2 = -1$

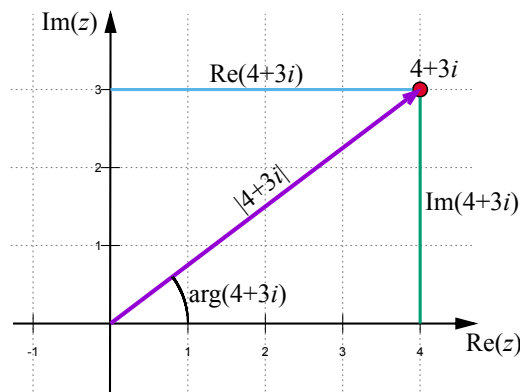


ABBILDUNG 2.1.3. Die komplexe Zahl  $z = 4 + 3i$  in der Gaußschen Zahlenebene

gilt. Damit kann man Wurzeln aus negativen Zahlen als **komplexe Zahl** unter anderem erklären als  $\sqrt{-n} = i \cdot \sqrt{n}$  (oder auch  $-i\sqrt{n}$ , je nach Kontext) und erhält die Menge der **komplexen Zahlen**:

$$\mathbb{C} = \{ x + iy \mid x \in \mathbb{R}, y \in \mathbb{R} \}$$

Von einer komplexen Zahl  $z = x + iy$  wird  $x = \operatorname{Re} z$  als **Realteil** von  $z$  und  $y = \operatorname{Im} z$  als **Imaginärteil** von  $z$  bezeichnet. Abbildung 2.1.3 zeigt die Darstellung einer komplexen Zahl in der komplexen Zahlenebene, auch **Gaußsche Zahlenebene** genannt. Der **Betrag einer komplexen Zahl** ist  $|x + iy| = \sqrt{x^2 + y^2}$ . Beim Rechnen mit komplexen Zahlen ist die **komplexe Konjugation**  $\bar{z} = x - iy$  zu einer komplexen Zahl  $z = x + iy$  sehr wichtig, wo bei einer komplexen Zahl der Wert vor der Konstante  $i$ , genannt imaginärer Teil, negiert wird. Bei der Division durch eine komplexe Zahl kann man das Ergebnis schnell bestimmen, wenn man den Bruch durch die komplexe Konjugierte des Nenners erweitert:

$$\frac{2 + 3i}{1 + 4i} = \frac{(2 + 3i) \cdot (1 - 4i)}{(1 + 4i) \cdot (1 - 4i)} = \frac{2 + 3i - 8i - 12i^2}{1 - 16i^2} = \frac{14 - 5i}{17} = \frac{14}{17} - \frac{5}{17}i$$

Komplexe Zahlen können auch in **Polarkoordinaten** dargestellt werden  $z = x + iy = r \cdot (\cos \varphi + i \sin \varphi)$  mit dem Betrag  $r = |z|$  und dem Argument  $\varphi = \arg z$ , dem Winkel zwischen dem Vektor von Ursprung zum Wert in der komplexen Ebene zur positiven reellen Achse.

Die bisher eingeführten speziellen Zahlenmengen wurden immer erweitert: Die natürlichen Zahlen sind beispielsweise komplett in den ganzen Zahlen enthalten.

**DEFINITION 2.7.** Seien  $A$  und  $B$  Mengen. Dann ist  $A$  genau dann eine **Teilmenge** von  $B$  oder  $B$  **Obermenge** von  $A$ , geschrieben  $A \subseteq B$ , wenn gilt:  $\forall x \in A : x \in B$ .  $A$  ist eine **echte Teilmenge** von  $B$  oder  $B$  **echte Obermenge** von  $A$ , geschrieben  $A \subset B$ , genau dann, wenn  $A \subseteq B$  und  $B \setminus A \neq \emptyset$ .

Damit sind die natürlichen Zahlen eine echte Teilmenge der rationalen Zahlen, geschrieben  $\mathbb{N} \subset \mathbb{Q}$ . Da die rationalen Zahlen auch Teilmenge der reellen Zahlen sind  $\mathbb{Q} \subset \mathbb{R}$ , gilt auch  $\mathbb{N} \subset \mathbb{R}$ .

$$\emptyset \subset \mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

Mit Hilfe der Teilmengen-Beziehung lässt sich die **Gleichheit von Mengen** gut definieren:

**DEFINITION 2.8.** Zwei Mengen  $M$  und  $N$  sind gleich, wenn sie gegenseitig Teilmengen sind:

$$M = N \Leftrightarrow (M \subseteq N) \wedge (N \subseteq M)$$

Aus den bisherigen Definitionen erhalten wir eine Vielzahl von Zusammenhängen:

SATZ 2.9. Seien  $A$ ,  $B$  und  $C$  Mengen. Dann gilt:

- |    |  |                             |
|----|--|-----------------------------|
| 1. | $A \cap B \subseteq A \subseteq A \cup B$  |                             |
| 2. | $A \cap A = A = A \cup A$  | <b>Idempotenz</b>           |
| 3. | $A \cap B = B \cap A$<br>$A \cup B = B \cup A$   | <b>Kommutativität</b>       |
| 4. | $A \cap (B \cap C) = (A \cap B) \cap C$<br>$A \cup (B \cup C) = (A \cup B) \cup C$   | <b>Assoziativität</b>       |
| 5. | $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$<br>$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$                               | <b>Distributivität</b>      |
| 6. | $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$<br>$A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$ | <b>De Morgansche Regeln</b> |

BEWEIS. Exemplarisch von 6a:  $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$ .

Zu zeigen sind zwei Aussagen:  $A \setminus (B \cup C) \subseteq (A \setminus B) \cap (A \setminus C)$  und  $A \setminus (B \cup C) \supseteq (A \setminus B) \cap (A \setminus C)$ :

$A \setminus (B \cup C) \subseteq (A \setminus B) \cap (A \setminus C)$ :

Gegeben ist:  $x \in A \setminus (B \cup C)$

Zu zeigen ist:  $x \in (A \setminus B) \cap (A \setminus C)$

(1) Wenn  $x \in A \setminus (B \cup C)$ , so ist  $x \in A$  und  $x \notin B \cup C$ .

(2) Damit ist  $x \in A$  und  $x \notin B$  und  $x \notin C$ .

(3) Somit ist  $x \in A \setminus B$  und  $x \in A \setminus C$ .

(4) Damit ist  $x \in (A \setminus B) \cap (A \setminus C)$ , was zu zeigen war.

$(A \setminus B) \cap (A \setminus C) \subseteq A \setminus (B \cup C)$ :

Gegeben ist:  $x \in (A \setminus B) \cap (A \setminus C)$

Zu zeigen ist:  $x \in A \setminus (B \cup C)$

(1) Wenn  $x \in (A \setminus B) \cap (A \setminus C)$ , so ist  $x \in A \setminus B$  und  $x \in A \setminus C$ .

(2) Damit ist  $x \in A$  und  $x \notin B$  und  $x \notin C$ .

(3) Also ist  $x \notin B \cup C$ .

(4) Damit ist  $x \in A \setminus (B \cup C)$ .

Die weiteren Aussagen werden entsprechend nachgewiesen. □

Die Anzahl von Elementen in einer Menge wird mit der Kardinalität beschrieben:

DEFINITION 2.10. Die **Kardinalität** oder **Mächtigkeit** von Mengen beschreibt die Größe oder Anzahl der Elemente einer Menge: Für endliche Mengen  $M$  beschreibt  $|M|$  die Anzahl der Elemente in  $M$ .

SATZ 2.11. Seien  $A$  und  $B$  endliche Mengen. Dann gilt:

$$|A \cap B| \leq |A| \leq |A \cup B| \leq |A| + |B|.$$

BEWEIS. Ist  $U \subseteq V$ , so ist  $|U| \leq |V|$ , da alle Elemente in  $U$  auch in  $V$  sind. Daraus folgen die ersten beiden Ungleichungen. Die letzte Ungleichung folgt, da jedes Element in  $A \cup B$  entweder in  $A$  oder  $B$  vorkommen muss, aber eventuell in beiden vorkommt und so doppelt gezählt wird. □

Mengen können auch aus Mengen bestehen. Eine Menge von Mengen wird auch als **Mengensystem** bezeichnet. Die Potenzmenge ist so ein Mengensystem:

DEFINITION 2.12. Zu einer Menge  $M$  ist die **Potenzmenge**  $\mathcal{P}(M)$  die Menge der Teilmengen von  $M$ :

$$\mathcal{P}(M) = \{ U \mid U \subseteq M \}$$

BEISPIEL 2.13. Für  $A = \{1, 4, 7\}$  ist

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{4\}, \{7\}, \{1, 4\}, \{1, 7\}, \{4, 7\}, A\}.$$

SATZ 2.14. Ist  $M$  eine endliche Menge mit  $|M| = n$ , so ist ihre Potenzmenge  $\mathcal{P}(M)$  ebenso endlich mit  $|\mathcal{P}(M)| = 2^n$ .

BEWEIS. In der Übung. □

Ein weiteres Beispiel für Mengensysteme sind Partitionen:

DEFINITION 2.15. Ein Mengensystem  $\mathcal{Z} = \{M_1, \dots, M_n\}$  von paarweisen disjunkten Mengen  $M_1, \dots, M_n$  ist eine **Partition** ihrer Vereinigung  $M$ :

$$\bigcup_{k=1}^n M_k = M_1 \cup \dots \cup M_n = M$$

$$M_i \cap M_j = \emptyset \text{ für } i \neq j$$

BEISPIEL 2.16. Die Zerlegung der natürlichen Zahlen in gerade und ungerade Zahlen ist eine Partition:

$$\mathcal{Z} = \{ \{2n \mid n \in \mathbb{N}\}, \{2n-1 \mid n \in \mathbb{N}\} \} = \{ \{2, 4, 6, \dots\}, \{1, 3, 5, \dots\} \}$$

DEFINITION 2.17. Für zwei Mengen  $A$  und  $B$  bezeichnet  $A \times B$  das **kartesische Produkt**:

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

Die Elemente  $(a, b)$  werden als zweistellige **Tupel** oder **Paare** bezeichnet. Die Elemente des kartesischen Produkts über  $n$  Mengen

$$A_1 \times \dots \times A_n = \{ (a_1, \dots, a_n) \mid a_1 \in A_1, \dots, a_n \in A_n \}$$

werden als  $n$ -stellige **Tupel** bezeichnet. Dreistellige **Tupel** werden auch als **Tripel** bezeichnet.

Bei Zweier-Tupeln besteht eine Verwechslungsgefahr mit Intervallen, es muss also immer genau klar sein, was eine Notation bedeutet. Mit der Kurzschreibweise  $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$  für kartesische Produkte von Mengen mit sich selbst wird beispielsweise der Raum der drei-dimensionalen reellen **Vektoren**  $(x_1, x_2, x_3) \in \mathbb{R}^3$  mit  $x_1, x_2, x_3 \in \mathbb{R}$  definiert. Im Gegensatz zu Mengen mit mehreren Elementen ist bei Tupeln die Reihenfolge relevant und das gleiche Objekt kann an unterschiedlichen Stellen mehrfach auftreten.

SATZ 2.18. Sind  $A$  und  $B$  endliche Mengen mit  $|A| = n$  und  $|B| = m$  Elementen, so ist das kartesische Produkt ebenso endlich und hat  $|A \times B| = n \cdot m$  Elemente.

BEWEIS. Seien die Elemente von  $A$  und  $B$  durchnummeriert

$$A = \{a_1, a_2, \dots, a_n\}, B = \{b_1, b_2, \dots, b_m\},$$

so ist

$$A \times B = \{ (a, b) \mid a \in A, b \in B \} = \{ (a_k, b_l) \mid k = 1, \dots, n, l = 1, \dots, m \}$$

und damit gibt es  $n \cdot m$  unterschiedliche **Tupel**, somit gilt  $|A \times B| = n \cdot m$ . □

BEMERKUNG 2.19. Für das kartesische Produkt von mehr als zwei endlichen Mengen  $A_1, \dots, A_n$  mit Kardinalitäten  $|A_1| = m_1, \dots, |A_n| = m_n$  gilt entsprechend  $|A_1 \times \dots \times A_n| = m_1 \cdot \dots \cdot m_n$ .

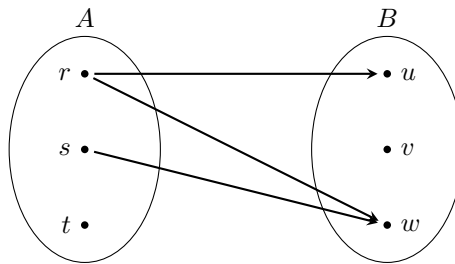
## 2.2. Relationen

DEFINITION 2.20. Eine **Relation**  $R$  zwischen zwei Mengen  $A$  und  $B$  ist eine Teilmenge ihres kartesischen Produkts  $R \subseteq A \times B$ . Je zwei Elemente  $a \in A$  und  $b \in B$  stehen genau dann in Relation zu einander, geschrieben  $a R b$ , wenn  $(a, b) \in R$ .

BEISPIEL 2.21. Es seien  $A = \{r, s, t\}$  und  $B = \{u, v, w\}$ . Dann ist

$$R = \{(r, u), (r, w), (s, w)\} \subseteq A \times B$$

eine Relation zwischen  $A$  und  $B$ , die so dargestellt werden kann:



BEMERKUNG 2.22. Es ist auch möglich  $n$ -stellige Relationen zwischen Mengen  $A_1, \dots, A_n$  als Teilmengen von  $A_1 \times \dots \times A_n$  zu betrachten. Im Folgenden werden aber nur zweistellige oder binäre Relationen innerhalb einer Menge behandelt. Viele der Konzepte können auf Relationen zwischen unterschiedlichen Mengen und auch mehrstellige Relationen erweitert werden. Eine **relationale Datenbank** basiert auch auf dem Grundkonzept von Relationen zwischen Zeilen unterschiedlicher Tabellen.

DEFINITION 2.23. Eigenschaften von Relationen: Sei  $M$  eine Menge und  $R \subseteq M \times M$  eine Relation.

- (1)  $R$  ist **symmetrisch**, wenn für alle  $(x, y) \in R$  auch  $(y, x) \in R$  folgt.
- (2)  $R$  ist **antisymmetrisch**, wenn aus  $(x, y) \in R$  und  $(y, x) \in R$  folgt, dass  $x = y$ .
- (3)  $R$  ist **reflexiv**, wenn für alle  $x \in M$  gilt, dass  $(x, x) \in R$ .
- (4)  $R$  ist **transitiv**, wenn aus  $(x, y) \in R$  und  $(y, z) \in R$  folgt, dass  $(x, z) \in R$ .
- (5)  $R$  ist **linear**, wenn für jedes  $x, y \in M$  gilt:  $(x, y) \in R \vee (y, x) \in R$ .

BEISPIEL 2.24. Für die Menge  $M = \{a, b, c, d\}$  seien die Relationen

$$R = \{(a, a), (a, b), (a, c), (a, d), (b, b), (b, c), (b, d), (c, c), (c, d), (d, d)\}$$

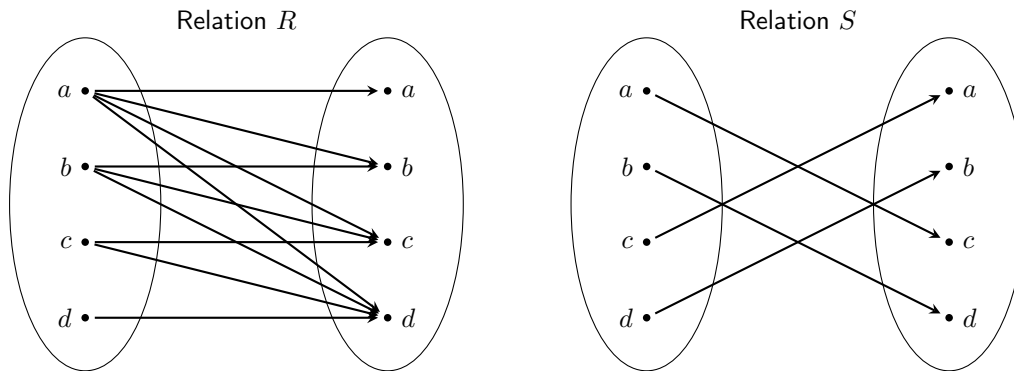
und  $S = \{(a, c), (b, d), (c, a), (d, b)\}$  definiert und in Abbildung 2.2.1 dargestellt.

Die Relation  $R$  ist

- nicht symmetrisch, denn aus  $(a, b) \in R$  folgt nicht  $(b, a) \in R$ ,
- antisymmetrisch, denn aus  $(x, y) \in R$  und  $(y, x) \in R$  folgt, dass  $x = y$ ,
- reflexiv, da  $\{(a, a), (b, b), (c, c), (d, d)\} \subseteq R$ ,
- transitiv, da z.B. mit  $(a, b) \in R$ ,  $(b, c) \in R$  auch  $(a, c) \in R$  folgt,
- linear, da für alle  $x \in M$  und  $y \in M$  entweder  $(x, y) \in R$  oder  $(y, x) \in R$  gilt.

Die Relation  $S$  ist

- symmetrisch, da aus  $(a, c) \in S$  auch  $(c, a) \in S$ , und  $(b, d) \in S$  auch  $(d, b) \in S$  folgt,
- nicht antisymmetrisch, da zwar  $(a, c) \in S$  und  $(c, a) \in S$  aber nicht  $a = c$  ist,
- nicht reflexiv, da beispielsweise  $(a, a) \notin S$ ,
- nicht transitiv, da mit  $(a, c) \in S$  und  $(c, a) \in S$  nicht  $(a, a) \in S$  folgt,
- nicht linear, da weder  $(a, b)$  noch  $(b, a)$  in  $S$  sind.

ABBILDUNG 2.2.1. Relationen  $R$  und  $S$  aus Beispiel 2.24

### 2.2.1. Äquivalenzrelationen.

DEFINITION 2.25. Eine reflexive, symmetrische und transitive Relation ist eine **Äquivalenzrelation**.

BEMERKUNG 2.26. Relationen und besonders Äquivalenzrelationen werden oft durch einen  $\sim$ -Operator dargestellt, also statt  $x R y$  wird die Notation  $x \sim_R y$  oder  $x \sim y$  verwendet. Die drei Bedingungen für eine Äquivalenzrelation  $\sim$  über einer Menge  $M$  sind mit dieser Notation dann:

- (1) Reflexivität:  $\forall x \in M : x \sim x$
- (2) Symmetrie:  $\forall x, y \in M : (x \sim y \Rightarrow y \sim x)$
- (3) Transitivität:  $\forall x, y, z \in M : (x \sim y \wedge y \sim z \Rightarrow x \sim z)$

BEISPIEL 2.27. Einige Beispiele für Äquivalenzrelationen:

- (1) Seien  $g$  und  $h$  Geraden im  $\mathbb{R}^2$ . Die Relation  $g \parallel h$  für  $g$  ist parallel zu  $h$ .  
 Reflexivität: Eine Gerade  $g$  ist zu sich selbst parallel (definieren wir so):  $g \parallel g$ . ✓  
 Symmetrie: Ist  $g \parallel h$ , so auch  $h \parallel g$ . ✓  
 Transitivität: Ist  $g \parallel h$  und  $h \parallel k$ , so ist auch  $g \parallel k$ . ✓
- (2) Seien  $x, y \in \mathbb{Z}$  und in Relation bei gleichem Rest bei Division durch 5 haben:  $x \equiv y \pmod{5}$ .  
 Reflexivität: Es gilt  $x \equiv x \pmod{5}$ . ✓  
 Symmetrie: Mit  $x \equiv y \pmod{5}$  gilt auch  $y \equiv x \pmod{5}$ . ✓  
 Transitivität: Mit  $x \equiv y \pmod{5}$  und  $y \equiv z \pmod{5}$  gilt auch  $x \equiv z \pmod{5}$ . ✓
- (3) Ein **Netzwerk** oder **Graph**  $N$  besteht aus **Knoten** und **Kanten** zwischen jeweils zwei Knoten. Sei  $N$  ein **ungerichteter Graph** und sei darin  $M$  eine Menge von Knoten und  $K$  die Relation der Kanten zwischen den Punkten in einem Netzwerk, also mit  $x K y$  gilt immer auch  $y K x$  wie in Abbildung 2.2.2. Dann ist die Relation  $K$  im Allgemeinen keine Äquivalenzrelation, aber die abgeleitete Relation  $x R y$  für  $x$  ist mit  $y$  über Kanten verbunden, ist eine Äquivalenzrelation:  
 Reflexivität: Es gilt  $x R x$ , da jeder Punkt mit sich verbunden ist. ✓  
 Symmetrie: Ist  $x R y$ , so existiert eine Folge von Kanten  $x K a_1 K \dots K a_n K y$ , die umgekehrt  $y$  mit  $x$  verbindet, also  $y R x$  gilt. ✓  
 Transitivität: Ist  $x R y$  und  $y R z$ , so existieren jeweils von  $x$  nach  $y$  nach  $z$  eine Folge von Kanten, die zusammengehängt  $x$  mit  $z$  verbinden, also gilt  $x R z$ . ✓

DEFINITION 2.28. Sei  $M$  eine Menge und  $R$  eine Äquivalenzrelation. Für ein  $x \in M$  ist

$$[x]_R = \{ y \in M \mid x R y \}$$

die **Äquivalenzklasse** von  $x$  bezüglich  $R$ .



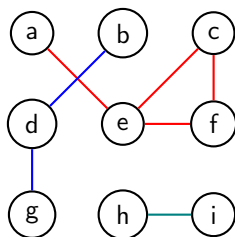


ABBILDUNG 2.2.2. Ungerichteter Graph zu Beispielen 2.27 (3) und 2.31

SATZ 2.29. Sei  $R$  eine Äquivalenzrelation über einer Menge  $M$  und  $x, y \in M$  beliebig.

- (1) Es gilt  $x \in [x]_R$ .
- (2) Gilt  $x R y$ , so ist  $x \in [y]_R$ .
- (3) Ist  $[x]_R \cap [y]_R \neq \emptyset$ , so ist  $[x]_R = [y]_R$ .

BEWEIS. Seien  $x, y \in M$  beliebig.

- (1) Da  $R$  reflexiv, gilt  $x R x$  und damit ist  $x \in [x]_R$ .
- (2) Da  $x R y$  ist wegen Symmetrie  $y R x$  und daher ist  $x \in [y]_R$ .
- (3) Existiert ein  $z \in [x]_R \cap [y]_R$ , so ist  $x R z$  und  $y R z$ , also wegen Symmetrie auch  $z R y$ . Wegen Transitivität gilt dann  $x R y$ . Für die Gleichheit der Mengen ist aus Symmetrie nur eine Richtung, also  $[x]_R \subseteq [y]_R$  zu zeigen. Ist  $a \in [x]_R$ , so ist  $x R a$ . Da  $y R x$  wegen Symmetrie gilt, ist wegen Transitivität auch  $y R a$ . Damit ist  $a \in [y]_R$ .

□

Aus der dritten Aussage von Satz 2.29 folgt, dass Äquivalenzklassen sich entweder vollständig unterscheiden oder gleich sind. Daraus folgt der folgende Satz:

SATZ 2.30. Sei  $R$  Äquivalenzrelation der Menge  $M$ , dann ist das Mengensystem der Äquivalenzklassen

$$\mathcal{K} = \{ [x]_R \mid x \in M \}$$

eine Partition der Menge  $M$ .

BEWEIS. Zu zeigen sind:  $\bigcup_{[x]_R \in \mathcal{K}} [x]_R = M$  und es gilt entweder  $[x]_R = [y]_R$  oder  $[x]_R \cap [y]_R = \emptyset$ .

- (1) Zu zeigen ist:  $\bigcup_{[x]_R \in \mathcal{K}} [x]_R = M$

- (a)  $\bigcup_{[x]_R \in \mathcal{K}} [x]_R \subseteq M$ :

Da nach Definition  $[x]_R = \{ y \in M \mid x R y \}$  ist  $[x]_R \subseteq M$ . Für jedes  $y \in \bigcup_{[x]_R \in \mathcal{K}} [x]_R$  gibt es ein  $x$  mit  $y \in [x]_R \subseteq M$ , damit ist  $y \in M$ , also  $\bigcup_{[x]_R \in \mathcal{K}} [x]_R \subseteq M$ .

- (b)  $M \subseteq \bigcup_{[x]_R \in \mathcal{K}} [x]_R$

Für jedes  $x \in M$  ist  $x \in [x]_R$  nach Satz 2.29 (1). Nach Definition ist  $[x]_R \in \mathcal{K}$ , und damit ist  $x \in \bigcup_{[x]_R \in \mathcal{K}} [x]_R$ .

- (2) Zu zeigen ist: Es gilt entweder  $[x]_R = [y]_R$  oder  $[x]_R \cap [y]_R = \emptyset$ .

- (a) Wenn es ein  $z \in [x]_R \cap [y]_R$  gibt, so ist nach Satz 2.29 (3)  $[x]_R = [y]_R$ .
- (b) Wenn es kein  $z \in [x]_R \cap [y]_R$  gibt, so ist  $[x]_R \cap [y]_R = \emptyset$ .

□

BEISPIEL 2.31. Der ungerichtete Graph mit der Relation  $R$  für Knoten, die über Kanten verbunden sind, aus Beispiel 2.27 (3) und Abbildung 2.2.2 hat drei in der Abbildung eingefärbten Äquivalenzklassen, die auch **Zusammenhangskomponenten** genannt werden. Diese Komponenten teilen den Graphen in drei Teile ein. Diese Partitionierung durch eine Äquivalenzrelation wird auch Quotientenmenge genannt.

DEFINITION 2.32. Sei  $R$  eine Äquivalenzrelation über einer Menge  $M$ . Dann wird das Mengensystem

$$M/R = \{ [x]_R \mid x \in M \}$$

als **Quotientenmenge** oder **Faktormenge** von  $M$  **modulo**  $R$  bezeichnet.

BEISPIEL 2.33. Mit diesen Begriffen können einige wichtige Mengen nun mathematisch sinnvoll beschrieben werden:

- (1) Die Äquivalenzrelation  $R$  über  $\mathbb{Z}$  zum gleichen Rest bei Division durch 5 aus Beispiel 2.27 (2) hat diese Quotientenmenge, die aus den **Restklassen** zur Zahl 5 besteht:

$$\mathbb{Z}/R = \{ [0]_R, [1]_R, [2]_R, [3]_R, [4]_R \}$$

Diese Mengen bezüglich eines Divisors  $n$  werden oft verkürzt als  $\mathbb{Z}_n = \{0, \dots, n-1\}$  durch ihre **Repräsentanten** beschrieben. Dies soll aber nicht verstecken, dass dies nur Repräsentanten ihrer Äquivalenzklassen sind, denn beispielsweise ist in  $\mathbb{Z}_5$  gerade  $4 \equiv 9 \pmod{5}$ , was eigentlich für  $[4]_R = [9]_R$  steht. **Register in 8-Bit Computern** basieren beispielsweise auf  $\mathbb{Z}_{256}$ .

- (2) Die rationalen Zahlen  $\mathbb{Q}$  sind eigentlich die Quotientenmenge von  $\mathbb{Z} \times \mathbb{N}$  bezüglich der Äquivalenzrelation  $R$ :

$$(a, b) R (c, d) \Leftrightarrow a \cdot d = b \cdot c.$$

Damit haben die beiden Brüche  $\frac{2}{3}$  und  $\frac{4}{6}$  die gleiche Bedeutung, da sie nur unterschiedliche Repräsentanten der gleichen Äquivalenzklasse sind. Im **IEEE 754** Standard für **Gleitkommazahlen** wird diese Identifikation unterschiedlicher Binärbrüche durch eine **Normalisierung** hergestellt.

- (3) Die Menge der reellen Zahlen  $\mathbb{R}$  ist die Quotientenmenge konvergenter rationaler Folgen bezüglich der Äquivalenzrelation, dass die beiden Folgen den gleichen Grenzwert haben. Dadurch haben die beiden Zahlen 1 und  $0.9999\dots$  in  $\mathbb{R}$  die gleiche Bedeutung.
- (4) Die Konzepte Wochentag, Kalenderwoche und Monat sind Äquivalenzklassen. Die Äquivalenzklasse „Montag“ zur Äquivalenzrelation der Wochentage in einem Jahr beinhaltet beispielsweise alle Montag in diesem Jahr. Die Quotientenmenge der Tage eines Jahres bezüglich der Äquivalenzrelation Monat ist die Menge der Monate.
- (5) Der **Projektive Raum** kommt in Robotik und Computergrafik zum Einsatz:

$$\mathbb{P}^n = (\mathbb{R}^{n+1} \setminus \{0\}) / \sim \text{ mit } x \sim y \Leftrightarrow \exists \lambda \in \mathbb{R} \setminus \{0\} : x = \lambda y$$

Die Vektoren  $(x_1, \dots, x_n) \in \mathbb{R}^n$  sind in der Äquivalenzklasse  $[(x_1, \dots, x_n, 1)]_{\sim}$  eingebettet, die auch mit  $(x_1 : \dots : x_n : 1)$  als **homogene Koordinaten** notiert wird. Affine Abbildungen, wie  $Ax + b$ , werden hier zu einfachen Matrixmultiplikationen  $Cx$  und vereinfachen Umrechnungen deutlich.

### 2.2.2. Ordnungsrelationen.

DEFINITION 2.34. Eine Relation  $R$  ist

- (1) **Quasiordnung**, wenn  $R$  reflexiv und transitiv ist,
- (2) **Halbordnung**, wenn  $R$  reflexiv, transitiv und antisymmetrisch ist,
- (3) **lineare Ordnung** oder **Vollordnung**, wenn  $R$  reflexiv, transitiv, antisymmetrisch, linear ist.

BEMERKUNG 2.35. Für Ordnungen  $R$  wird statt  $x R y$  auch  $x \preceq y$  geschrieben. Ist  $R$  über Menge  $M$

- (1) reflexiv,  $\forall x \in M : x \preceq x$ ,
- (2) transitiv,  $\forall x, y, z \in M : (x \preceq y \wedge y \preceq z) \Rightarrow x \preceq z$

so ist die Relation Quasiordnung. Ist die Relation zusätzlich

- (3) antisymmetrisch,  $\forall x, y \in M : (x \preceq y \wedge y \preceq x) \Rightarrow x = y$

so ist die Relation Halbordnung. Ist die Relation zusätzlich

- (4) linear,  $\forall x, y \in M : (x \preceq y) \vee (y \preceq x)$

so ist die Relation Vollordnung.

BEISPIEL 2.36. Beispiele für Ordnungen:

- (1) Die Ordnung  $\leq$  ist auf den ganzen Zahlen  $\mathbb{Z}$  eine lineare Ordnung:  
 Reflexivität: Für alle  $x \in \mathbb{Z}$  gilt  $x \leq x$ .  
 Transitivität: Für alle  $x, y, z \in \mathbb{Z}$  mit  $x \leq y$  und  $y \leq z$  ist auch  $x \leq z$ .  
 Antisymmetrie: Für alle  $x, y \in \mathbb{Z}$  mit  $x \leq y$  und  $y \leq x$  ist  $x = y$ .  
 Linearität: Für alle  $x, y \in \mathbb{Z}$  ist  $(x \leq y) \vee (y \leq x)$ .
- (2) Die Ordnung  $\subseteq$  ist auf Mengen wie z.B.  $\mathcal{P}(\mathbb{Z})$  eine Halbordnung:  
 Reflexivität: Für alle Mengen  $A$  gilt  $A \subseteq A$ .  
 Transitivität: Für alle Mengen  $A, B, C$  mit  $A \subseteq B$  und  $B \subseteq C$  ist auch  $A \subseteq C$ .  
 Antisymmetrie: Gilt für zwei Mengen  $A, B$ , dass  $A \subseteq B$  und  $B \subseteq A$ , so ist  $A = B$ .  
 Die Ordnung ist nicht linear, da nicht alle Mengen vergleichbar sind.
- (3) Die Ordnung  $\preceq$  nach Größe von Preisen von Produkten im Supermarkt ist eine Quasiordnung:  
 Reflexivität: Für alle Artikel  $x$  gilt  $x \preceq x$ .  
 Transitivität: Für Artikel  $x, y, z$  mit  $x \preceq y$  und  $y \preceq z$  ist natürlich auch  $x \preceq z$ .  
 Die Ordnung ist nicht antisymmetrisch, da gleicher Preis nicht auf das gleiche Produkt führt.
- (4) Die Relation  $R$  aus Beispiel 2.24 und Abbildung 2.2.1 ist eine lineare Ordnung.

DEFINITION 2.37. Sei  $\preceq$  eine Halbordnung auf einer Menge  $M$ .

- (1) Ein Element  $x \in M$  ist **minimal** bezüglich  $\preceq$ , wenn es kein weiteres Element  $y \in M$  mit  $x \neq y$  gibt mit  $y \preceq x$ .
- (2) Ein Element  $x \in M$  ist **maximal** bezüglich  $\preceq$ , wenn es kein weiteres Element  $y \in M$  mit  $x \neq y$  gibt mit  $x \preceq y$ .
- (3) Das Element  $x \in M$  ist **kleinstes Element** bezüglich  $\preceq$ , wenn  $\forall y : x \preceq y$ .
- (4) Das Element  $x \in M$  ist **größtes Element** bezüglich  $\preceq$ , wenn  $\forall y : y \preceq x$ .

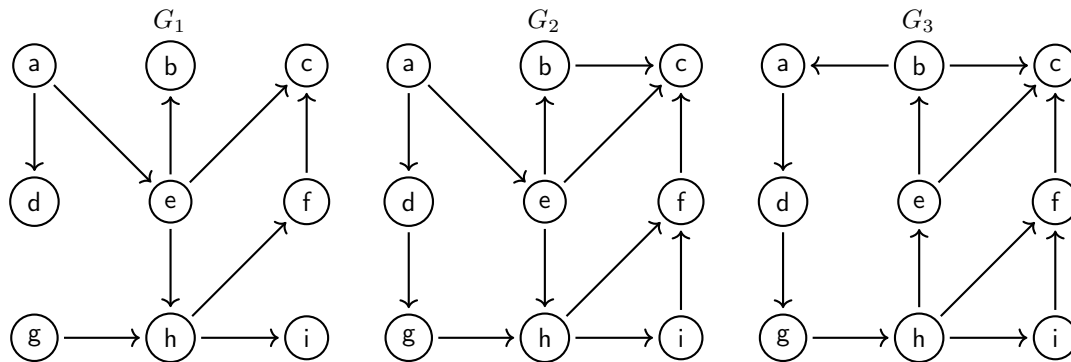


ABBILDUNG 2.2.3. Gerichtete Graphen  $G_1$ ,  $G_2$  und  $G_3$  zu Beispiel 2.38

BEISPIEL 2.38. Ein **gerichteter Graph** ist eine Menge  $M$  von **Knoten** und einer Relation  $\rightarrow$  für **Kanten**, wobei für  $x, y \in M$  genau dann  $x \rightarrow y$  gilt, wenn von  $x$  ein Pfeil zu  $y$  geht. Auf Zusammenhangskomponenten kann eine Quasiordnung  $R$  definiert werden, mit  $x R y$  wenn ein Knoten  $x$  eine gerichtete Verbindung zum Knoten  $y$  besitzt. Abbildung 2.2.3 zeigt drei gerichtete **Graphen**  $G_1$ ,  $G_2$  und  $G_3$  mit unterschiedlichen Eigenschaften:

- (1) Die Relation  $R$  auf dem Graphen  $G_1$  ist reflexiv, transitiv und antisymmetrisch, also sogar eine Halbordnung, aber keine Ordnung, da beispielsweise  $d$  und  $i$  nicht gegenseitig erreichbar und damit nicht vergleichbar sind. Der Graph besitzt zwei minimale Elemente  $a$  und  $g$  und vier maximale Elemente  $i$ ,  $d$ ,  $b$  und  $c$ . Der Graph hat kein größtes oder kleinstes Element.
- (2) Die Relation  $R$  auf dem Graphen  $G_2$  ist reflexiv, transitiv und antisymmetrisch, also eine Halbordnung, aber keine Ordnung, da  $d$  und  $e$  nicht vergleichbar sind. Das Element  $a$  ist minimal und kleinstes Element, das Element  $c$  ist maximales und größtes Element.
- (3) Die Relation  $R$  auf dem Graphen  $G_3$  ist reflexiv und transitiv, aber nicht antisymmetrisch, da es zwischen  $a, d, g, h, e, b$  einen Zyklus gibt. Es gibt kein minimales oder kleinstes Element, und das Element  $c$  ist maximales und größtes Element.

Ist  $R$  eine Halbordnung, so werden die zugehörigen gerichteten Graphen, wo implizite transitive Beziehungen ausgelassen werden, **Hasse-Diagramm** genannt.

SATZ 2.39. Sei  $\preceq$  eine Halbordnung auf der Menge  $M$ .

- (1) Existiert ein kleinstes Element in  $M$  bezüglich  $\preceq$ , so ist es eindeutig.
- (2) Falls ein kleinstes Element existiert, so ist es minimal.
- (3) Falls ein kleinstes Element existiert, so ist es das einzige minimale Element.

Entsprechende Aussagen gelten auch für maximale und größte Elemente.

BEWEIS.

- (1) Seien  $x, y \in M$  kleinste Elemente bezüglich  $\preceq$ . So gilt  $x \preceq y$  und  $y \preceq x$ . Da  $\preceq$  Halbordnung folgt daraus  $x = y$ , also ist das kleinste Element eindeutig.
- (2) Sei  $x$  kleinstes Element. Angenommen es gibt ein Element  $y \in M$  mit  $y \preceq x$ . Da  $\forall z \in M : x \preceq z$ , gilt dies auch für  $y$ , somit ist  $x \preceq y$  und da  $\preceq$  Halbordnung ist, ist  $y = x$ .
- (3) Ist  $x$  kleinstes Element, so ist es nach (2) minimal. Sei  $y$  ein weiteres minimales Element, so gilt  $x \preceq y$ , da  $x$  kleinstes Element. Also muss  $y = x$  sein.

□

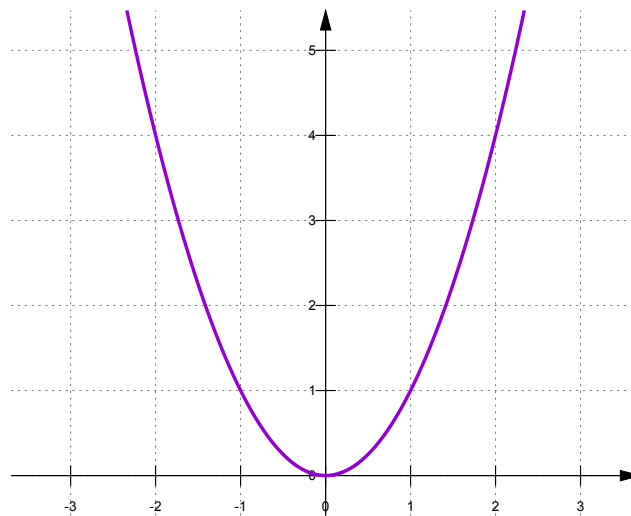


ABBILDUNG 2.3.1. Graph der Quadratfunktion  $f(x) = x^2$  in  $\mathbb{R}^2$

### 2.3. Abbildungen

Auch Abbildungen oder Funktionen können über Mengen und Relationen eingeführt werden:

DEFINITION 2.40. Eine **Abbildung** oder **Funktion** mit Notation  $f : D \rightarrow W$  ist eine Relation auf  $D \times W$ , bei dem jedes Element  $x \in D$  mit genau nur mit einem Element  $f(x) = y \in W$  in Relation steht:

$$f : D \rightarrow W$$

$$x \mapsto f(x) = y$$

Die Menge  $D$  ist die **Definitionsmenge** der Abbildung und die Menge  $W$  ist die **Wertemenge** der Abbildung. Die Teilmenge von  $D \times W$ , die die Relation bestimmt, wird als **Graph der Abbildung** bezeichnet:

$$\text{graph}(f) = \{ (x, f(x)) \mid x \in D \} \subseteq D \times W$$

BEISPIEL 2.41. Beispiele für Abbildungen:

- (1) Die Relation  $S$  in Beispiel 2.24 und Abbildung 2.2.1 ist eine Abbildung, die Relation  $R$  in Beispiel und Abbildung ist hingegen keine Funktion, da beispielsweise  $a$  mit mehreren Elementen in Relation steht.
- (2) Die Quadratfunktion  $f : \mathbb{R} \rightarrow \mathbb{R}, x \mapsto f(x) = x^2$  ist eine Abbildung und ihr Graph ist in Abbildung 2.3.1 dargestellt.

DEFINITION 2.42. Für eine Funktion  $f : A \rightarrow B$  und Teilmengen  $U \subseteq A$  und  $V \subseteq B$  ist die Menge

$$f(U) = \{ f(x) \mid x \in U \}$$

das **Bild** von  $U$  unter  $f$ , und

$$f^{-1}(V) = \{ x \mid f(x) \in V \}$$

das **Urbild** von  $V$  unter  $f$ .

BEISPIEL 2.43. Für die Quadratfunktion  $f : \mathbb{R} \rightarrow \mathbb{R}, x \mapsto f(x) = x^2$  aus Abbildung 2.3.1 ist das Bild vom Intervall  $[1, 2]$  gerade  $f([1, 2]) = [1, 4]$  und das Urbild des Intervalls  $[1, 4]$  ist  $f^{-1}([1, 4]) = [-2, -1] \cup [1, 2]$ .

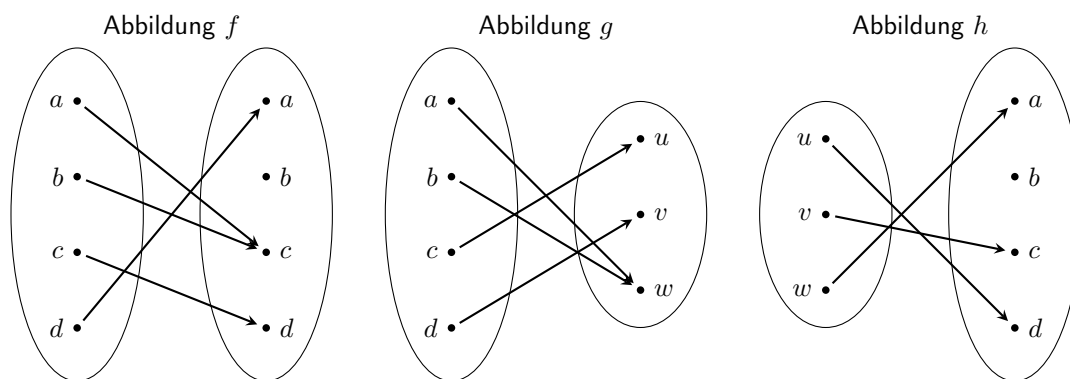


ABBILDUNG 2.3.2. Drei Abbildungen zur Injektivität und Surjektivität im Beispiel 2.45

DEFINITION 2.44. Sei  $f : A \rightarrow B$  eine Abbildung.

- (1)  $f$  ist **injektiv**, wenn für alle  $x, y \in A$  mit  $x \neq y$  folgt  $f(x) \neq f(y)$ .
- (2)  $f$  ist **surjektiv**, wenn das **Bild der Funktion** den Wertebereich umfasst,

$$\text{Bild}(f) = \bigcup_{x \in A} f(x) = B.$$

- (3)  $f$  ist **bijektiv**, wenn  $f$  injektiv und surjektiv ist.

BEISPIEL 2.45.

- (1) Die Abbildung  $f$  in Abbildung 2.3.2 ist weder injektiv noch surjektiv. Die Abbildung  $g$  ist surjektiv, aber nicht injektiv. Die Abbildung  $h$  ist injektiv aber nicht surjektiv. Die Relation  $S$  in Beispiel 2.24 und Abbildung 2.2.1 ist eine Abbildung, sowohl injektiv als auch surjektiv, und damit eine bijektive Abbildung.
- (2) Die Quadratfunktion in Abbildung 2.3.1 ist als Funktion  $\mathbb{R} \rightarrow \mathbb{R}$  weder injektiv noch surjektiv. Als Funktion  $[0, \infty) \rightarrow \infty$  ist sie injektiv und als Funktion  $[0, \infty) \rightarrow [0, \infty)$  ist sie injektiv und surjektiv und damit bijektiv.

Auf endlichen Mengen haben ihre bijektiven Abbildungen besonders viele Anwendungen:

DEFINITION 2.46. Sei  $M$  eine endliche Menge, dann heißen bijektive Abbildungen  $p : M \rightarrow M$  **Permutationen**. Die Menge aller Permutationen über  $M$  ist definiert als:

$$S_M = \{ p : M \rightarrow M \mid p \text{ ist bijektiv} \}$$

Für die Menge  $M = \{1, 2, \dots, n\}$  der Zahlen von 1 bis  $n$  ist  $S_n$  die Menge deren Permutationen.

Da Elemente endlicher Mengen immer durchgezählt werden können, können wir generell  $S_n$  stellvertretend für die Permutationen  $S_M$  von Mengen mit  $n$  Elementen, also  $|M| = n$ , betrachten.

BEISPIEL 2.47. Die Menge  $S_3$  hat 6 Elemente, die in ausführlicher Schreibweise von Urbild in der ersten Zeile und Abbild in der zweiten Zeile geschrieben werden können:

$$\begin{aligned} \sigma_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \\ \sigma_4 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \end{aligned}$$

Beispielsweise ist  $\sigma_3(1) = 2$  und  $\sigma_4(3) = 1$ .

DEFINITION 2.48. Sind  $f : A \rightarrow B$  und  $g : B \rightarrow C$  Abbildungen so ist deren **Verkettung**  $g \circ f$  definiert als Abbildung

$$\begin{aligned} g \circ f : A &\rightarrow C \\ x &\mapsto g(f(x)). \end{aligned}$$

BEISPIEL 2.49. Die Verkettung ist eine natürliche Operation auf den Permutationen, beispielsweise ist in  $S_3$  aus Beispiel 2.47

$$\begin{aligned} (\sigma_3 \circ \sigma_4)(1) &= \sigma_3(\sigma_4(1)) = \sigma_3(2) = 1 \\ (\sigma_3 \circ \sigma_4)(2) &= \sigma_3(\sigma_4(2)) = \sigma_3(3) = 3 \\ (\sigma_3 \circ \sigma_4)(3) &= \sigma_3(\sigma_4(3)) = \sigma_3(1) = 2 \end{aligned}$$

Und damit ist  $\sigma_3 \circ \sigma_4 = \sigma_2$ . Da bei der Verkettung von Permutationen wieder neue Permutationen entstehen, ergibt sich durch Verkettung immer wieder ein Element aus  $S_3$ .

SATZ 2.50. Die Verkettung ist assoziativ, für  $f : A \rightarrow B$ ,  $g : B \rightarrow C$  und  $h : C \rightarrow D$  gilt also

$$(h \circ g) \circ f = h \circ (g \circ f).$$

BEWEIS. Zu zeigen ist, dass für alle  $x \in A$  gilt, dass  $((h \circ g) \circ f)(x) = (h \circ (g \circ f))(x)$  ist.

Da  $(g \circ f)(x) = g(f(x))$  und  $(h \circ g)(z) = h(g(z))$  gilt

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

□

DEFINITION 2.51. Die Funktion  $id_M : M \rightarrow M$  mit  $id(x) = x$  für alle  $x \in M$  ist die **identische Funktion** oder die **Identität** auf der Menge  $M$ .

BEISPIEL 2.52. Im Beispiel 2.47 ist  $\sigma_1 = id$ , und es gilt  $\sigma_1 \circ \sigma_k = \sigma_k = \sigma_k \circ \sigma_1$  für alle  $k = 1, \dots, 6$ . So eine Vertauschbarkeit oder Kommutativität gilt aber hier nicht immer:

$$\sigma_3 \circ \sigma_4 = \sigma_2 \quad \text{aber} \quad \sigma_4 \circ \sigma_3 = \sigma_6$$

Die Verkettung von Funktionen ist also nicht notwendigerweise kommutativ.

SATZ 2.53. Genau dann, wenn eine Funktion  $f : A \rightarrow B$  bijektiv ist, existiert eine **inverse Funktion**

$$f^{-1} : B \rightarrow A$$

mit  $f^{-1} \circ f = id_A$  und  $f \circ f^{-1} = id_B$ .

BEWEIS.

$\Rightarrow$

Gegeben ist:  $f : A \rightarrow B$  ist bijektiv

Zu zeigen ist:  $\exists f^{-1} : (\forall x \in A : f^{-1}(f(x)) = x) \wedge (\forall y \in B : f(f^{-1}(y)) = y)$ .

- (1) Da  $f$  surjektiv ist, gibt es für jedes  $y \in B$  ein  $x_y \in A$  mit  $y = f(x_y)$ .
- (2) Da  $f$  injektiv ist, folgt aus  $f(u) = f(v)$ , dass  $u = v$ , also ist  $x_y$  zu  $y$  eindeutig.
- (3) Jedem  $y \in B$  kann eindeutig  $x_y \in A$  zugeordnet werden, dies sei  $f^{-1}(y) = x_y$ .
- (4) Für jedes  $y \in B$  gilt, dass  $f(x_y) = y$  und  $f^{-1}(y) = x_y$ , also ist  $f(f^{-1}(y)) = y$ .
- (5) Für jedes  $x \in A$  gibt es nach Injektivität ein eindeutiges  $y \in B$  mit  $f(x) = y$ .
- (6) Dieses  $y$  hat nach Konstruktion das zugehörige  $x_y = x$ .
- (7) Daher ist  $f^{-1}(y) = x_y = x$ .
- (8) Also gilt  $f^{-1}(f(x)) = x$ .

⇐

Gegeben ist:  $\exists f^{-1} : \forall x \in A : f^{-1}(f(x)) = x$ .

Zu zeigen ist:  $f : A \rightarrow B$  ist surjektiv und injektiv.

- (1) Es gibt für alle  $y \in B$  ein  $x \in A$  mit  $f(x) = y$ : Wähle  $x = f^{-1}(y)$ .
- (2) Also ist  $f$  surjektiv.
- (3) Seien  $u, v \in A$  mit  $f(u) = f(v)$ , dann ist  $u = f^{-1}(f(u)) = f^{-1}(f(v)) = v$ .
- (4) Damit ist  $f$  injektiv.

□

BEISPIEL 2.54. Da alle Funktionen in  $S_3$  aus Beispiel 2.47 bijektiv sind, haben alle eine Inverse, die ebenfalls als Permutation in  $S_3$  ist:

$$\sigma_1^{-1} = \sigma_1, \sigma_2^{-1} = \sigma_2, \sigma_3^{-1} = \sigma_3, \sigma_4^{-1} = \sigma_5, \sigma_5^{-1} = \sigma_4, \sigma_6^{-1} = \sigma_6$$

Permutationen können alternativ auch kürzer dargestellt werden. Beispielsweise gilt für

$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} : \quad 1 \xrightarrow{\sigma_4} 2 \xrightarrow{\sigma_4} 3 \xrightarrow{\sigma_4} 1 \xrightarrow{\sigma_4} \dots$$

Die Zahlen durchlaufen also immer einen Zyklus 1, 2, 3. Deswegen gibt es auch die Kurzschreibweise  $\sigma_4 = (1\,2\,3)$ . Da egal ist, bei welchem Wert gestartet wird, gilt auch  $\sigma_4 = (2\,3\,1) = (3\,1\,2)$ , aber es ist sinnvoll immer mit der kleinsten Zahl zu beginnen. Die Identität hat keinen Zyklus und heißt deswegen einfach nur *id*. Damit können die Elemente von  $S_3$  in **Zyklusschreibweise** kürzer auch so geschrieben werden:

$$\sigma_1 = id, \sigma_2 = (2\,3), \sigma_3 = (1\,2), \sigma_4 = (1\,2\,3), \sigma_5 = (1\,3\,2), \sigma_6 = (1\,3)$$

Ab  $S_4$  können die Permutationen auch mehrere Zyklen haben, die hintereinander geschrieben werden:

$$\varrho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (1\,3)(2\,4)$$



## 2.4. Aufgaben

AUFGABE 25. Welche Elemente sind in Menge  $A$ :

$$A = (\{x \in \mathbb{R} \mid x^2 < 25\} \cup [-12, 3)) \cap (\mathbb{Z} \setminus \mathbb{N})$$

AUFGABE 26. Finden Sie eine einfachere Beschreibung für die Menge  $A$ :

$$A = \{x \in \mathbb{Z} \mid |x - 4| < 7\} \cap (\{x \in \mathbb{Z} \mid \exists y \in \mathbb{N} : x = y^2\} \triangle (-\infty, 1])$$

AUFGABE 27. Vereinfachen Sie diesen Ausdruck für Mengen  $A$ ,  $B$  und  $C$ :

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

AUFGABE 28. Vereinfachen Sie diesen Ausdruck für Mengen  $A$ ,  $B$  und  $C$ :

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

AUFGABE 29. Ist  $C$  eine Partition der Menge  $A = \{1, 2, 3\}$ ?

$$C = (\mathcal{P}(A) \setminus \mathcal{P}(A \setminus \{1\}))$$

AUFGABE 30. Seien  $A = \{1, 4, 3\}$  und  $B = \{2, 3, 4\}$ . Bestimmen Sie  $|\mathcal{P}(A) \triangle \mathcal{P}(B)|$ .

AUFGABE 31. Auf der Menge  $M = \mathbb{Z} \times \mathbb{N}$  sei die Relation  $R$  definiert durch

$$(a, b) R (c, d) \Leftrightarrow a \cdot d = b \cdot c.$$

Welche Eigenschaften hat sie?

AUFGABE 32. Welche Eigenschaften hat die Relation  $x \mid y$  für  $x$  teilt  $y$  auf den natürlichen Zahlen?

AUFGABE 33. Auf der Menge  $M = \{1, 2, 3, 4\}$  sei die Relation

$$R = \{ (1, 1), (1, 3), (2, 2), (3, 1), (3, 3), (4, 4) \}$$

gegeben. Zeigen Sie, dass  $R$  eine Äquivalenzrelation ist, bestimmen Sie die Äquivalenzklasse  $[3]_R$  und stellen Sie die Quotientenmenge  $M/R$  auf.

AUFGABE 34. Auf der Menge  $M = \{1, 2, 3, 4\}$  sei die Relation

$$R = \{ (1, 4), (1, 1), (3, 2), (2, 2), (4, 4), (3, 3), (4, 1), (2, 3) \}$$

gegeben. Zeigen Sie, dass  $R$  eine Äquivalenzrelation ist, bestimmen Sie die Äquivalenzklasse  $[2]_R$  und stellen Sie die Quotientenmenge  $M/R$  auf.

AUFGABE 35. Auf der Menge  $M = \{1, 2, 3, 4\}$  sei die Relation

$$R = \{ (1, 1), (1, 3), (1, 4), (1, 2), (2, 2), (3, 3), (3, 4), (3, 2), (4, 4) \}$$

gegeben.

- (1) Ist  $R$  eine Ordnung, und was für eine?
- (2) Gibt es minimale, maximale, kleinste oder größte Elemente?

**AUFGABE 36.** Auf der Menge  $M = \{1, 2, 3, 4\}$  sei die Relation

$$R = \{ (1, 1), (2, 1), (2, 2), (2, 3), (2, 4), (3, 1), (3, 3), (3, 4), (4, 1), (4, 3), (4, 4) \}$$

gegeben.

- (1) Ist  $R$  eine Ordnung, und was für eine?
- (2) Gibt es minimale, maximale, kleinste oder größte Elemente?

**AUFGABE 37.** Gegeben seien die Relationen  $U, V, W \subseteq \{1, 2, 3, 4\} \times \{1, 2, 3\}$ :

$$U = \{ (1, 4), (2, 3), (3, 3), (3, 2), (4, 1) \}$$

$$V = \{ (1, 2), (2, 3), (3, 1), (4, 2) \}$$

$$W = \{ (2, 1), (3, 1), (1, 2), (4, 2) \}$$

- (1) Welche der Relationen sind Funktionen?
- (2) Untersuchen Sie die Funktionen auf Injektivität und Surjektivität.

**AUFGABE 38.** Gegeben seien die Relationen  $U, V, W \subseteq \{1, 2, 3\} \times \{1, 2, 3, 4\}$ :

$$U = \{ (1, 4), (2, 3), (3, 1), (2, 3) \}$$

$$V = \{ (1, 2), (2, 3), (1, 2), (2, 3) \}$$

$$W = \{ (2, 1), (3, 4), (1, 2) \}$$

- (1) Welche der Relationen sind Funktionen?
- (2) Untersuchen Sie die Funktionen auf Injektivität und Surjektivität.

**AUFGABE 39.** In  $S_5$  sind diese beiden Permutationen gegeben:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}, \quad \tau = (14)(23)$$

- (1) Schreiben Sie  $\sigma$  in Zykelschreibweise und  $\tau$  in ausführlicher Matrixform.
- (2) Bestimmen Sie  $\sigma^{-1}$  und  $\tau \circ \sigma$ .
- (3) Bestimmen Sie das Urbild von  $\{1, 2, 5\}$  unter  $\tau$ .

**AUFGABE 40.** In  $S_5$  sind diese beiden Permutationen gegeben:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix}, \quad \tau = (142)(35)$$

- (1) Schreiben Sie  $\sigma$  in Zykelschreibweise und  $\tau$  in ausführlicher Matrixform.
- (2) Bestimmen Sie  $\tau^{-1}$  und  $\sigma \circ \tau$ .
- (3) Bestimmen Sie das Bild von  $\{2, 3, 4\}$  unter  $\sigma$ .

## KAPITEL 3

# Gruppen, Ringe und Körper

DEFINITION 3.1. Seien  $A, B, C$  Mengen. Dann ist eine **Verknüpfung** eine Abbildung

$$\begin{aligned} v : A \times B &\rightarrow C, \\ (x, y) &\mapsto v(x, y) \end{aligned}$$

und kann mit einem **Operator**  $x \star_v y = v(x, y)$  oder kürzer  $x \star y = v(x, y)$  geschrieben werden, wenn der Zusammenhang klar ist. Wenn  $A = B = C$ , so ist  $v$  eine Verknüpfung auf  $A$ .

### 3.1. Gruppen

DEFINITION 3.2. Sei  $G$  eine nichtleere Menge und  $\star$  eine Verknüpfung auf  $G$ . Dann ist  $(G, \star)$  eine **Gruppe**, wenn diese Axiome erfüllt sind:

1. **Assoziativität:**  $\forall x, y, z \in G : (x \star y) \star z = x \star (y \star z)$
2. **Neutrales Element:**  $\exists e \in G : \forall x \in G : e \star x = x \star e = x$
3. **Inverse Elemente:**  $\forall x \in G : \exists y \in G : x \star y = y \star x = e$

Gilt zusätzlich noch das 4. Axiom der Kommutativität, so ist die Gruppe eine **kommutative Gruppe** oder **abelsche Gruppe**:

4. **Kommutativität:**  $\forall x, y \in G : x \star y = y \star x$

BEISPIEL 3.3.

- (1) Die ganzen Zahlen bilden mit der Addition  $(\mathbb{Z}, +)$  eine kommutative Gruppe.
- (2) Rationale Zahlen ohne Null bilden mit der Multiplikation  $(\mathbb{Q} \setminus \{0\}, \cdot)$  eine kommutative Gruppe.
- (3) Die Permutationen von  $n$  Elementen bilden mit der Verkettung  $(S_n, \circ)$  eine Gruppe.
- (4) Quadratische  $n \times n$ -Matrizen bilden mit Matrixaddition  $(\mathbb{R}^{n \times n}, +)$  eine kommutative Gruppe.

SATZ 3.4. Wenn  $(G, \star)$  eine Gruppe ist, so gilt:

- (1) Das Element  $e$  ist eindeutig.
- (2) Für jedes  $x \in G$  gibt es genau ein  $y \in G$  mit  $x \star y = y \star x = e$ .

BEWEIS.

- (1) Angenommen es gäbe ein zweites  $e'$  mit  $\forall x \in G : e' \star x = x \star e' = x$ , so wäre  $e = e \star e' = e'$  und damit ist  $e = e'$  eindeutig.
- (2) Sei  $x \in G$  beliebig aber fest. Angenommen es gäbe neben  $y \in G$  mit  $y \star x = x \star y = e$  ein zweites  $y'$  mit  $y' \star x = x \star y' = e$ , so ist

$$y' = e \star y' = (y \star x) \star y' = y \star (x \star y') = y \star e = y$$

also ist  $y' = y$ .

□

BEMERKUNG 3.5. Gruppen werden häufig als additive oder multiplikative Gruppen interpretiert.

- In additiv interpretierten Gruppen wird oft  $+$  als Operator,  $0$  als neutrales Element  $e$  und  $-x$  für das inverse Element  $y$  zu  $x$  verwendet.
- In multiplikativ interpretierten Gruppen wird oft  $\cdot$  oder  $*$  als Operator,  $1$  als neutrales Element  $e$  und  $x^{-1}$  für das inverse Element  $y$  zu  $x$  verwendet.

Die generische Verknüpfung  $\star$  wird ab hier multiplikativ interpretiert.

DEFINITION 3.6. Sei  $(G, \star)$  eine Gruppe. Ist  $H \subseteq G$  und  $(H, \star)$  eine Gruppe, so ist  $(H, \star)$  eine **Untergruppe** von  $(G, \star)$ .

BEISPIEL 3.7. Die Menge der geraden Zahlen  $G = \{2z \mid z \in \mathbb{Z}\}$  bildet mit der Addition  $(G, +)$  eine Gruppe, da dies eine zyklische Gruppe ist, die später eingeführt wird. Da  $(\mathbb{Z}, +)$  eine Gruppe und  $G \subseteq \mathbb{Z}$ , ist  $(G, +)$  eine Untergruppe von  $(\mathbb{Z}, +)$ . Da sogar  $G \subset \mathbb{Z}$  gilt, ist dies auch eine **echte Untergruppe**.

SATZ 3.8. Sei  $(G, \star)$  eine Gruppe. Dann ist  $U \subseteq G$  genau dann Untergruppe  $(U, \star)$  von  $G$ , wenn

- (1)  $U \neq \emptyset$
- (2)  $\forall x, y \in U : x \star y^{-1} \in U$

BEWEIS. Ist  $(U, \star)$  Gruppe, so gelten die Aussagen nach Axiomen 2 und 3.

Ist  $U \subseteq G$  mit  $(G, \star)$  Gruppe,  $U \neq \emptyset$  und  $\forall x, y \in U : x \star y^{-1} \in U$ , so gilt:

- (1) Assoziativität: Da  $(G, \star)$  Gruppe ist, ist die Verknüpfung  $\star$  assoziativ.
- (2) Neutrales Element: Sei  $x \in U \neq \emptyset$ , so gilt nach Prämisse  $x \star x^{-1} = 1 \in U$ .
- (3) Inverses Element: Sei  $y \in U \neq \emptyset$  und  $x = 1$ , so gilt nach Prämisse  $1 \star y^{-1} = y^{-1} \in U$ .

Somit ist  $(U, \star)$  Gruppe und damit Untergruppe von  $(G, \star)$ . □

SATZ 3.9. Sind  $(H, \star)$  und  $(L, \star)$  Untergruppen einer Gruppe  $(G, \star)$ , so ist  $(H \cap L, \star)$  ebenfalls eine Untergruppe von  $(G, \star)$ . Ist  $\mathcal{M}$  ein Mengensystem von Untergruppen von  $G$ , so ist

$$\left( \bigcap_{M \in \mathcal{M}} M, \star \right)$$

ebenfalls eine Untergruppe von  $(G, \star)$ .

BEWEIS. Zu zeigen ist  $H \cap L \subset G$  bzw.  $\bigcap_{M \in \mathcal{M}} M \subset G$ . Dies ist erfüllt, da jede der Mengen nach Vorgabe Teilmenge von  $G$  ist, und dies dann auch für den Schnitt gilt. Es verbleibt zu zeigen, dass  $(H \cap L, \star)$  bzw.  $\left( \bigcap_{M \in \mathcal{M}} M, \star \right)$  Gruppen sind. Für alle Elemente  $x, y, z \in H \cap L$  bzw.  $x, y, z \in \bigcap_{M \in \mathcal{M}} M$  gelten die Aussagen 1-3 bzw. 1-4 in den Einzelmengen. Die neutralen und inversen Elemente sind in  $G$  eindeutig und sind damit in allen Mengen enthalten. Damit sind alle Axiome auch auf den Schnitten erfüllt und damit sind dies Gruppen. □

DEFINITION 3.10. Sei  $(G, \star)$  eine Gruppe und  $H \subseteq G$  eine Teilmenge. Seien im Mengensystem  $\mathcal{M}$  die Mengen aller Untergruppen  $(M, \star)$  von  $G$ , für die  $H \subseteq M$  gilt. Dann ist

$$\langle (H), \star \rangle = \left( \bigcap_{M \in \mathcal{M}} M, \star \right)$$

die von  $H$  **erzeugte Gruppe**. Man sagt auch:  $H$  ist das **Erzeugendensystem** von  $\langle H \rangle$ .

BEISPIEL 3.11. Die Definition über den Schnitt aller Untergruppen, die eine Menge umschließen, klärt nur, dass es sich tatsächlich um eine Gruppe handelt. Praktisch wird man alle Kombinationen und Inversen bilden, um die erzeugte Gruppe zu bestimmen. Seien  $\tau, \sigma \in S_4$  mit  $\tau = (12)$  und  $\sigma = (34)$ . Dann lautet  $\langle \tau, \sigma \rangle = \{id, (12), (34), (12)(34)\}$ .

DEFINITION 3.12. Eine **zyklische Gruppe**  $(\langle a \rangle, \star)$  ist eine von genau einem Element  $a$  erzeugte Gruppe. Ist  $\langle a \rangle$  endlich, so ist die Anzahl der Elemente die **Ordnung** von  $a$ :  $\text{ord}(a) = |\langle a \rangle|$ .

Zur Bestimmung zyklischer Gruppen gibt es eine einfache Darstellung:

SATZ 3.13. Ist  $a \in G$  für eine Gruppe  $(G, \star)$ , so gilt mit  $a^n = \underbrace{a \star \dots \star a}_{n \text{ mal}}$ ,  $a^0 = 1$  und  $a^{-n} = (a^{-1})^n$ , dass  $\langle a \rangle = \{a^z \mid z \in \mathbb{Z}\}$ .

BEWEIS.

(1)  $\langle a \rangle \subseteq A = \{a^z \mid z \in \mathbb{Z}\}$ : Zu zeigen:  $A$  ist Gruppe mit  $a \in A$ , denn dann ist  $\langle a \rangle$  nach Definition als Schnitt aller  $a$  umfassender Gruppen Teilmenge von  $A$ :

(a) Es ist  $A \neq \emptyset$ , da  $a^0 = 1 \in A$ .

(b) Sei  $x, y \in A$  mit  $x = a^k$  und  $y = a^l$ . Dann ist  $y^{-1} = a^{-l}$ , denn

$$y \star a^{-l} = \underbrace{a \star \dots \star a}_{l \text{ mal}} \star \underbrace{a^{-1} \star \dots \star a^{-1}}_{l \text{ mal}} = 1,$$

da sich immer die mittleren beiden  $a \star a^{-1} = 1$  aufheben und  $1 \star a^{-1} = a^{-1}$  ist, bis die letzte 1 übrig bleibt, und damit ist  $y^{-1} = a^{-l}$ . Dann folgt

$$x \star y = a^k \star (a^{-1})^l = \underbrace{a \star \dots \star a}_{n \text{ mal}} \star \underbrace{a^{-1} \star \dots \star a^{-1}}_{l \text{ mal}} = \begin{cases} \underbrace{a \star \dots \star a}_{n-l \text{ mal}}, & \text{wenn } n > l \\ 1, & \text{wenn } n = l \\ \underbrace{a^{-1} \star \dots \star a^{-1}}_{l-n \text{ mal}}, & \text{wenn } n < l \end{cases} = a^{n-l} \in A.$$

Damit ist  $(A, \star)$  eine Untergruppe von  $(G, \star)$  und da  $a = a^1 \in A$ , ist  $A \subseteq \langle a \rangle$ .

(2)  $A = \{a^z \mid z \in \mathbb{Z}\} \subseteq \langle a \rangle$ : Zu zeigen: Jedes  $a^z \in A$  ist in  $\langle a \rangle$ :

(a) Da  $\langle a \rangle$  Gruppe mit  $a \in \langle a \rangle$ , ist  $a \star a \in \langle a \rangle$  und induktiv  $a^n \in \langle a \rangle$  für alle  $n \in \mathbb{N}$ .

(b) Da  $\langle a \rangle$  Gruppe, ist  $a^0 = 1 \in \langle a \rangle$ .

(c) Da  $\langle a \rangle$  Gruppe und  $a \in \langle a \rangle$  ist  $a^{-1} \in \langle a \rangle$  und induktiv  $a^{-n} \in \langle a \rangle$  für alle  $n \in \mathbb{N}$ .

Damit sind alle  $a^z \in \langle a \rangle$  für alle  $z \in \mathbb{Z}$  und damit  $\{a^z \mid z \in \mathbb{Z}\} \subseteq \langle a \rangle$

□

BEISPIEL 3.14. In der Gruppe der  $2 \times 2$ -Matrizen besteht die von  $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$  mit der Matrix-

multiplikation erzeugte zyklische Gruppe aus den folgenden Elementen:

$$\langle A \rangle = \{A, A^1, A^2, A^3\} = \left\{ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

Man kann diese Gruppe auf ein Einheitsquadrat mit den Ecken  $A, B, C, D$  anwenden. Die Matrixmultiplikation dreht dann das Quadrat immer um 90 Grad, so dass die Ecken immer wieder aufeinander abgebildet werden. Diese Gruppe entspricht daher der zyklischen Untergruppe von  $\langle (1234), \circ \rangle$  in  $S_4$ .

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

ABBILDUNG 3.2.1. Additions- und Multiplikationstafel im Restklassen-Ring  $(\mathbb{Z}_6, +, \cdot)$ 

### 3.2. Ringe und Körper

DEFINITION 3.15. Sei  $R$  eine Menge und  $+, \cdot$  Verknüpfungen auf  $R$ . Dann ist  $(R, +, \cdot)$  ein **Ring**, wenn

- (1)  $(R, +)$  eine kommutative Gruppe ist,
- (2) die Verknüpfung  $\cdot$  auf  $R$  assoziativ ist, also für alle  $a, b, c \in R$  gilt, dass

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c,$$

- (3) und für alle  $a, b, c \in R$  die Distributivgesetze gelten:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

$$(a + b) \cdot c = a \cdot c + b \cdot c$$

Das neutrale Element der Gruppe  $(R, +)$  wird mit 0 bezeichnet, und wenn es ein neutrales Element 1 bezüglich der Verknüpfung  $\cdot$  gibt, so wird die Struktur **Ring mit 1** genannt. Ist die Verknüpfung  $\cdot$  kommutativ, so ist  $R$  ein **kommutativer Ring**.

BEISPIEL 3.16.

- (1) Die natürlichen Zahlen  $(\mathbb{Z}, +, \cdot)$  bilden einen kommutativen Ring mit 1, da
  - (a)  $(\mathbb{Z}, +)$  ist kommutative Gruppe ist,
  - (b) die Multiplikation assoziativ ist,
  - (c) die Distributivgesetze erfüllt sind,
  - (d) es ein neutrales Element 1 bezüglich der Multiplikation gibt,
  - (e) und die Multiplikation kommutativ ist.
- (2) Die Menge der Restklassen  $(\mathbb{Z}_n, +, \cdot)$  für  $n \in \mathbb{N}$  bilden mit der Addition und Multiplikation der ganzen Zahlen einen kommutativen Ring mit 1, den so genannten **Restklassen-Ring**. Die Multiplikation und Addition ist dabei unabhängig vom Repräsentanten ist, da für  $a \in [x]_n$ ,  $b \in [y]_n$  also  $a = x + kn$ ,  $b = y + ln$  mit  $k, l \in \mathbb{Z}$  gilt:

$$a + b = (x + kn) + (y + ln) = x + y + (k + l)n \equiv x + y \pmod{n}$$

$$a \cdot b = (x + kn) \cdot (y + ln) = xy + (yk + xl + kln)n \equiv x \cdot y \pmod{n}$$

Damit übertragen sich alle Eigenschaften  $(\mathbb{Z}, +, \cdot)$ . Die Abbildung 3.2.1 zeigt zur Illustration die Additions- und Multiplikationstafel in  $\mathbb{Z}_6$ . Hier ist interessant, dass außer der 1 nur die 5 ein multiplikativ Inverses besitzt und manche „Multiplikationen“ wie  $3 \cdot 4 \equiv 0 \pmod{6}$  ergeben.

DEFINITION 3.17. Sei  $(R, +, \cdot)$  kommutativer Ring mit 1, so ist  $R[x]$  Menge der **Polynome** über  $R$ :

$$R[x] = \{ a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \mid n \in \mathbb{N}_0, a_0, \dots, a_n \in R \}$$

Für ein Polynom  $p(x) = a_n x^n + \dots + a_1 x + a_0$  mit  $a_n \neq 0$  oder  $n = 0$  wird  $n$  als der **Grad des Polynoms** und ein einzelner Term  $a_k x^k$  als **Monom** bezeichnet. Die Polynomaddition  $+$  ist elementweise definiert (hier für  $n \geq m$ )

$$(a_n x^n + \dots + a_0) + (b_m x^m + \dots + b_0) = a_n x^n + \dots + a_{n+1} x^{n+1} + (a_m + b_m) x^m + \dots + (a_0 + b_0)$$

und die Polynommultiplikation  $\cdot$  ist entsprechend über alle Monome mit  $x^p \cdot x^q = x^{p+q}$  definiert als

$$(a_n x^n + \dots + a_0) \cdot (b_m x^m + \dots + b_0) = a_n b_m x^{n+m} + (a_{n-1} b_m + a_n b_{m-1}) x^{n+m-1} + \dots + a_0 b_0.$$

Dabei übertragen sich die algebraischen Eigenschaften des zu Grunde liegenden Rings auf die Polynome:

SATZ 3.18. Ist  $(R, +, \cdot)$  ein kommutativer Ring mit 1, so sind die Polynome  $(R[x], +, \cdot)$  über  $R$  ebenfalls ein kommutativer Ring mit 1.

BEWEIS. Durch Überprüfung der einzelnen Kriterien. □

BEISPIEL 3.19. Eine wichtige Darstellung ist, Binärzahlen als Polynome  $\mathbb{Z}_2[x]$  darzustellen, die zu einer ganz anderen Arithmetik führt, die sehr gut in Schaltkreisen umgesetzt werden kann:

$\begin{array}{r} 110101 \\ + 1010111 \\ \hline 10001100 \end{array}$	$\begin{array}{r} 1x^5 + 1x^4 + 0x^3 + 1x^2 + 0x + 1 \\ + 1x^6 + 0x^5 + 1x^4 + 0x^3 + 1x^2 + 1x + 1 \\ \hline 1x^6 + 1x^5 + 0x^4 + 0x^3 + 0x^2 + 1x + 0 \end{array}$
$\begin{array}{r} 101 \\ \cdot 10111 \\ \hline 101 \\ 101 \\ 101 \\ 101 \\ \hline 1110011 \end{array}$	$\begin{array}{r} (1x^2 + 0x + 1) \\ \cdot (1x^4 + 0x^3 + 1x^2 + 1x + 1) \\ \hline 1x^6 + 0x^5 + 1x^4 \\ 1x^4 + 0x^3 + 1x^2 \\ 1x^3 + 0x^2 + 1x \\ 1x^2 + 0x + 1 \\ \hline 1x^6 + 0x^5 + 0x^4 + 1x^3 + 0x^2 + 1x + 1 \end{array}$

Auf Ringen kann der Begriff der Teilbarkeit definiert werden:

DEFINITION 3.20. Sei  $(R, +, \cdot)$  ein kommutativer Ring. Dann ist  $a \in R$  **Teiler** von  $b \in R$ , geschrieben  $a|b$ , wenn es ein  $k \in R$  gibt mit  $b = k \cdot a$ .

BEISPIEL 3.21. Im Ring der ganzen Zahlen  $(\mathbb{Z}, +, \cdot)$  sind  $\{1, 2, 3, 4, 5, 6, 12, 15, 20, 30\}$  zuzüglich deren Negationen Teiler von 60. Im Ring der Polynome mit ganzzahligen Koeffizienten  $(\mathbb{Z}[x], +, \cdot)$  hat das Polynom  $2x^2 - 8$  unter anderem die Teiler  $\{1, 2, x + 2, x - 2, 2x - 4, 2x + 4, x^2 - 4\}$ , dazu kommen noch die jeweils negierten Terme. Werden nur die natürlichen Zahlen oder die Polynome mit positivem höchsten Koeffizienten betrachtet, so bildet die Teilbarkeit eine Halbordnung und kann daher in einem Hasse-Diagramm wie in Abbildung 3.2.2 dargestellt werden.

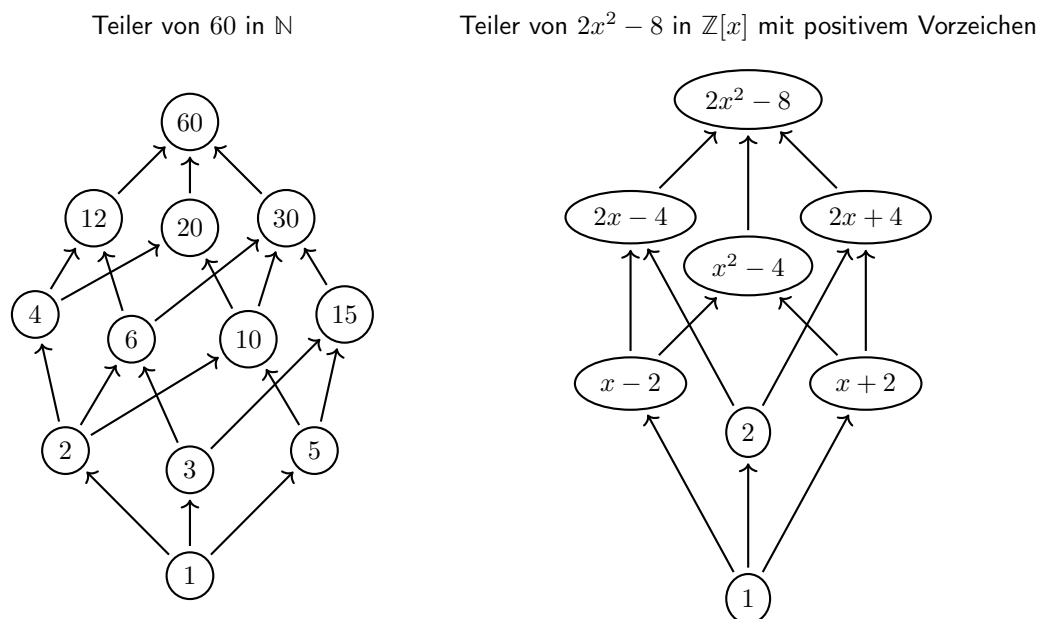


ABBILDUNG 3.2.2. Hasse-Diagramme zur Teilbarkeit zu Beispiel 3.21

In Beispiel 3.16 und Abbildung 3.2.1 war zu sehen, dass neben der 1 nur die 5 ein multiplikativ inverses Element besitzt. Entsprechend haben auch in  $\mathbb{Z}_8$  neben der 1 nur die Zahlen  $\{3, 5, 7\}$  eine multiplikative Inverse. Dafür gibt es einen Grund:

**SATZ 3.22.** Sei  $n \in \mathbb{N}$  und  $x \in \mathbb{Z}_n$ . Dann existiert genau dann ein  $y \in \mathbb{Z}_n$  mit  $x \cdot y \equiv 1 \pmod{n}$ , wenn  $x = 1$  oder  $x$  und  $n$  teilerfremd sind.

**BEWEIS.** Sei  $n \in \mathbb{N}$  und es existiere  $x, y \in \mathbb{Z}_n$  mit  $x \cdot y \equiv 1$ . Zu zeigen ist  $x = 1$  oder  $x$  und  $n$  sind teilerfremd. Ist  $x = 1$ , so ist die Konklusion gezeigt. Sei also  $x \neq 1$ . Für einen Beweis durch Widerspruch sei  $t > 1$  ein Teiler von  $n$  und  $x$ , also  $t|x$  und  $t|n$ . Dann gibt es  $x'$  und  $n'$  mit  $x = t \cdot x'$  und  $n = t \cdot n'$ . Da nun  $x \cdot y \equiv 1 \pmod{n}$  gilt, ist für ein  $k \in \mathbb{Z}$ :

$$\begin{aligned}
 x \cdot y + k \cdot n &= 1 \\
 \Rightarrow t \cdot x' \cdot y + t \cdot n' \cdot k &= 1 \\
 \Rightarrow \underbrace{t}_{>1} \cdot (x' \cdot y + n' \cdot k) &= 1 \qquad \text{Widerspruch!}
 \end{aligned}$$

Dies ist ein Widerspruch, da in  $\mathbb{Z}$  es nicht möglich ist durch Multiplikation einer Zahl, die größer als 1 ist, auf 1 zu kommen.

Sind  $x$  und  $n$  teilerfremd, so bestimmt der euklidische Algorithmus mit Satz 3.30 die Inverse  $y \in \mathbb{Z}_n$ .  $\square$

**DEFINITION 3.23.** Seien  $a, b \in \mathbb{Z}$ . Der **größte gemeinsame Teiler**  $\text{ggT}(a, b)$  ist die größte natürliche Zahl, die  $a$  und  $b$  teilt.

**SATZ 3.24.** Für  $a, b, k \in \mathbb{N}$  und  $a > k \cdot b$  gilt  $\text{ggT}(a, b) = \text{ggT}(b, a - k \cdot b)$ .

**BEWEIS.** Ist  $x = \text{ggT}(a, b)$ , so gibt es  $u, v \in \mathbb{N}$  mit  $a = ux$  und  $b = vx$  mit  $u > kv$  da  $a > kb$ . Dann ist  $x$  Teiler von  $b$  und  $a - kb = ux - kvx = (u - kv) \cdot x$ . Ist umgekehrt  $x = \text{ggT}(b, a - kb)$ , so existieren wiederum  $u, v \in \mathbb{N}$  mit  $b = ux$  und  $a - kb = vx$  und damit teilt  $x$  auch  $b$  und  $a = a - kb + kb = vx + kux = (ku + v) \cdot x$ . Damit teilen sich beide ggT und sind daher die gleiche Zahl, da die Teilbarkeit eine Halbordnung und damit antisymmetrisch auf den natürlichen Zahlen ist.  $\square$



DEFINITION 3.25. Für  $a \in \mathbb{R}$  sei die **Gaußklammer**  $b = \lfloor a \rfloor \in \mathbb{Z}$  die größte ganze Zahl  $b \leq a$ .

BEMERKUNG 3.26. Damit gilt also für  $a, b \in \mathbb{N}$  auch  $\text{ggT}(a, b) = \text{ggT}(b, a - \lfloor \frac{a}{b} \rfloor b)$ . Der Wert  $a - \lfloor \frac{a}{b} \rfloor b$  ist der ganzzahlige Rest von  $a$  nach Division durch  $b$  und wird auch  $a$  modulo  $b$  genannt.

SATZ 3.27. **Euklidischer Algorithmus:** Seien  $a_0, a_1 \in \mathbb{N}$  und  $u_0 = 1, u_1 = 0, v_0 = 0, v_1 = 1$ . Für natürliche  $k$  sei iterativ

$$r_k = \left\lfloor \frac{a_{k-1}}{a_k} \right\rfloor$$

$$a_{k+1} = a_{k-1} - r_k \cdot a_k$$

$$u_{k+1} = u_{k-1} - r_k \cdot u_k$$

$$v_{k+1} = v_{k-1} - r_k \cdot v_k$$

solange  $a_{k+1} > 0$ . Dann ist  $a_k = \text{ggT}(a_0, a_1) = u_k \cdot a_0 + v_k \cdot a_1$ .

BEWEIS. Es werden folgende Aussagen gezeigt:

- (1) Für  $k \in \mathbb{N}$  mit  $a_k, a_{k-1} > 0$  gilt  $a_k > a_{k+1}$ . Damit hat das Verfahren maximal  $a_k$  Schritte.
- (2) Ist  $a_{k+1} \leq 0$ , so ist  $a_{k+1} = 0$ .
- (3) Ist  $a_{k+1} = 0$ , so ist  $a_k = \text{ggT}(a_0, a_1)$ .
- (4) Für  $k \in \mathbb{N}_0$  gilt  $a_k = u_k \cdot a_0 + v_k \cdot a_1$ .

Durch Nachweis dieser Aussagen ist die endliche Ausführbarkeit und Ergebnis bewiesen.

- (1) Angenommen  $a_{k+1} = a_{k-1} - r_k a_k \geq a_k$ , so wähle ganzzahliges  $s = r_k + 1$  mit

$$a_{k-1} - sa_k = a_{k-1} - r_k a_k - 1 \cdot a_k \geq a_k - a_k = 0,$$

also  $a_{k-1} \geq sa_k$  und  $s \leq \frac{a_{k-1}}{a_k}$ . Das ist aber im Widerspruch dazu, dass  $r_k = \left\lfloor \frac{a_{k-1}}{a_k} \right\rfloor$  die größte ganzzahlige Zahl mit  $r_k \leq \frac{a_{k-1}}{a_k}$  sein soll. Also ist  $a_{k+1} < a_k$  und damit auch  $a_{k+1} \leq a_k - 1$  und damit endet das Verfahren spätestens nach  $a_1$  Schritten.

- (2) Für natürliche  $a_{k-1}, a_k > 0$  ist  $a_k \geq 0$ , da  $r_k \leq \frac{a_{k-1}}{a_k}$  und damit  $a_{k-1} - r_k a_k \geq a_{k-1} - \frac{a_{k-1}}{a_k} \cdot a_k = a_{k-1} - a_{k-1} = 0$ . Da das Verfahren aber endet, ist schließlich  $a_{k+1} = 0$ .
- (3) Ist  $k$  so, dass  $a_{k+1} = 0$ , so ist  $a_k > 0$  und mit  $a_{k+1} = 0 = a_{k-1} - r_k a_k$  ist  $a_{k-1} = r_k a_k$ , also teilt  $a_k$  den Wert  $a_{k-1}$ . Da ein Teiler nicht größer als eine Zahl selbst sein kann, ist damit  $a_k = \text{ggT}(a_{k-1}, a_k)$ . Nach Satz 3.24 ist induktiv

$$\text{ggT}(a_0, a_1) = \text{ggT}(a_1, \underbrace{a_0 - r_1 a_1}_{=a_2}) = \text{ggT}(a_2, \underbrace{a_1 - r_2 a_2}_{=a_3}) = \dots = \text{ggT}(a_{k-1}, a_k)$$

und damit ist  $a_k = \text{ggT}(a_0, a_1)$ .

- (4) Vollständige Induktion bis zum Ende der Iteration:

Induktionsstart: Für  $k = 0$  und  $k = 1$  gilt  $a_0 = u_0 a_0 + v_0 a_1$  und  $a_1 = u_1 a_0 + v_1 a_1$ .

Induktionsschritt: Sei  $a_{k-1} = u_{k-1} a_0 + v_{k-1} a_1$  und  $a_k = u_k a_0 + v_k a_1$ . Dann ist

$$\begin{aligned} a_{k+1} &= a_{k-1} - r_k a_k \\ &= (u_{k-1} a_0 + v_{k-1} a_1) - r_k (u_k a_0 + v_k a_1) \\ &= u_{k-1} a_0 + v_{k-1} a_1 - r_k u_k a_0 - r_k v_k a_1 \\ &= (u_{k-1} - r_k u_k) a_0 + (v_{k-1} - r_k v_k) a_1 \\ &= u_{k+1} a_0 + v_{k+1} a_1. \end{aligned}$$

□

BEMERKUNG 3.28. Das in Satz 3.27 dargestellte Verfahren samt Berechnung einer **Linearkombination**  $\text{ggT}(a_0, a_1) = u_k a_0 + v_k a_1$  wird auch als **Erweiterter Euklidischer Algorithmus** bezeichnet.

Das ursprünglich von Euklid um 300 v. Chr. beschriebene Verfahren lautet: Solange  $a_{k-1} > a_k$  berechne  $a_{k+1} = a_{k-1} - a_k$ , oder tausche die Zahlen bis  $a_{k+1} = 0$ . In der Literatur wird normalerweise die daraus optimierte Variante aus den ersten beiden Schritten in der Form  $a_{k+1} = (a_{k-1} \bmod a_k)$  verkürzt geschrieben.

Das Verfahren lässt sich auch sehr elegant rekursiv formulieren, ist dann aber wegen des Aufwands der Aufrufe gegenüber der iterativen Version etwas weniger effizient, und die Berechnung der Koeffizienten  $u_k$  und  $v_k$  ist im erweiterten euklidischen Algorithmus schwerer zu verstehen. Wenn die Koeffizienten  $u_k$  und  $v_k$  nicht iterativ mitberechnet werden, so können sie durch Rücksubstitution der Formeln für  $a_k$  ebenso bestimmt werden.

BEISPIEL 3.29. Berechnung des  $x = \text{ggT}(63, 46)$  und eine Linearkombination  $x = u \cdot 63 + v \cdot 46$ :

$k$	$a_k$	$r_k$	$u_k$	$v_k$	$u_k \cdot a_0 + v_k \cdot a_1$
0	63		1	0	$1 \cdot 63 + 0 \cdot 46$
1	46	$\lfloor \frac{63}{46} \rfloor = 1$	0	1	$0 \cdot 63 + 1 \cdot 46$
2	$63 - 1 \cdot 46 = 17$	$\lfloor \frac{46}{17} \rfloor = 2$	$1 - 1 \cdot 0 = 1$	$0 - 1 \cdot 1 = -1$	$1 \cdot 63 - 1 \cdot 46$
3	$46 - 2 \cdot 17 = 12$	$\lfloor \frac{17}{12} \rfloor = 1$	$0 - 2 \cdot 1 = -2$	$1 - 2 \cdot (-1) = 3$	$-2 \cdot 63 + 3 \cdot 46$
4	$17 - 1 \cdot 12 = 5$	$\lfloor \frac{12}{5} \rfloor = 2$	$1 - 1 \cdot (-2) = 3$	$-1 - 1 \cdot 3 = -4$	$3 \cdot 63 - 4 \cdot 46$
5	$12 - 2 \cdot 5 = 2$	$\lfloor \frac{5}{2} \rfloor = 2$	$-2 - 2 \cdot 3 = -8$	$3 - 2 \cdot (-4) = 11$	$-8 \cdot 63 + 11 \cdot 46$
6	$5 - 2 \cdot 2 = 1$		$3 - 2 \cdot (-8) = 19$	$-4 - 2 \cdot 11 = -26$	$19 \cdot 63 - 26 \cdot 46$

Im nächsten Schritt ist  $a_7 = 0$ . Damit ist  $\text{ggT}(63, 46) = 1 = 19 \cdot 63 - 26 \cdot 46$ . Die Probe in der rechten Spalte kann natürlich weggelassen werden, genauso die Spalte  $r_k$  bei so ausführlicher Rechnung, wie hier. Wird die Linearkombination nicht benötigt, sondern nur der ggT berechnet werden, fallen die Spalten  $u_k$  und  $v_k$  weg.

Mit dem euklidischen Algorithmus kann nun der Beweis von Satz 3.22 vervollständigt werden, da teilerfremde Zahlen 1 als größten gemeinsamen Teiler haben:

SATZ 3.30. Sei  $n \in \mathbb{N}$ ,  $n > 1$  und  $x \in \mathbb{Z}_n$ . Ist  $\text{ggT}(n, x) = 1 = u \cdot n + v \cdot x$ , so gilt für  $y = v$ , wenn  $v > 0$  oder  $y = n + v$  sonst:

$$x \cdot y \equiv 1 \pmod{n}$$

BEWEIS. Die Linearkombination  $1 = u \cdot n + v \cdot x$  ergibt sich aus Satz 3.27. Ist  $v > 0$ , so ist

$$u \cdot n + v \cdot x \equiv v \cdot x \equiv 1 \pmod{n}.$$

Ist  $v < 0$ , so ist für ein  $k \in \mathbb{N}$

$$1 = u \cdot n + v \cdot x = u \cdot n - k \cdot x \cdot n + k \cdot n \cdot x + v \cdot x = (u - k \cdot x) \cdot n + \underbrace{(v + k \cdot n)}_{v'} \cdot x,$$

das  $v' > 0$  und kann wie im ersten Fall verwendet werden.  $v = 0$  ist nicht möglich.  $\square$

BEISPIEL 3.31. Gesucht ist eine **multiplikative Inverse** zu  $46 \in \mathbb{Z}_{63}$ . Nach Beispiel 3.29 ist  $\text{ggT}(63, 46) = 1 = 19 \cdot 63 - 26 \cdot 46$ , also existiert nach Satz 3.30 eine multiplikative Inverse. Da  $-26 < 0$  ist  $y = 63 - 26 = 37$  die gesuchte Zahl:  $46 \cdot 37 = 1702 \equiv 1 \pmod{63}$ .

Also besitzt jede zu  $n$  teilerfremde Zahl  $x$  in  $\mathbb{Z}_n$  eine multiplikative Inverse. Was ist nun, wenn  $n$  eine Primzahl ist? Genau dann ist jede Zahl (außer 0,1)  $x < n$  teilerfremd zu  $n$ :

SATZ 3.32. Genau dann, wenn  $n$  eine Primzahl ist, ist  $(\mathbb{Z}_n \setminus \{0\}, \cdot)$  eine kommutative Gruppe.

BEWEIS. Ist  $n$  eine Primzahl, so haben alle ganzen  $1 < x < n$  nach Satz 3.30 ein inverses Element. Zusätzlich ist die Verknüpfung assoziativ und kommutativ und  $1 \in \mathbb{Z}_n \setminus \{0\}$  ist das neutrale Element, damit ist  $(\mathbb{Z}_n \setminus \{0\}, \cdot)$  eine kommutative Gruppe.

Ist hingegen  $n$  keine Primzahl, so existieren ganze Faktoren  $p \cdot q = n$  mit  $p, q$  zwischen 1 und  $n$ . Damit sind  $p, q \in \mathbb{Z}_n \setminus \{0\}$  als Repräsentanten ihrer Äquivalenzklasse mit  $p \cdot q \equiv 0 \pmod{n}$ . Da aber  $0 \notin \mathbb{Z}_n \setminus \{0\}$ , ist  $\cdot$  dann keine Verknüpfung auf  $\mathbb{Z}_n \setminus \{0\}$  und somit liegt hier sicher keine Gruppe vor.  $\square$

DEFINITION 3.33. Ist  $(R, +, \cdot)$  ein kommutativer Ring mit 1 und ist  $(R \setminus \{0\}, \cdot)$  eine kommutative Gruppe, wird  $(R, +, \cdot)$  als **Körper** bezeichnet.

BEISPIEL 3.34. Beispiele für Körper:

- (1) Ist  $p$  Primzahl, so ist  $(\mathbb{Z}_p, +, \cdot)$  der so genannte **Restklassen-Körper**. Allgemeiner wird für **endliche Körper** wie  $\mathbb{Z}_p$  auch die Schreibweise und Benennung **Feld** oder **Field**  $\mathbb{F}_n$  verwendet, das auch andere endliche Körper mit  $n$  Elementen bezeichnet.
- (2) Die Quotientenmenge  $\mathbb{Z}_2[x]/_{x^2+x+1}$ , nach der Äquivalenzrelation  $0 \equiv x^2 + x + 1$  bzw.  $x^2 \equiv x + 1$  ergibt mit Addition und Polynommultiplikation den Körper  $\mathbb{F}_4$ :

+	0	1	$x$	$x+1$
0	0	1	$x$	$x+1$
1	1	0	$x+1$	$x$
$x$	$x$	$x+1$	0	1
$x+1$	$x+1$	$x$	1	0

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

- (3)  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ ,  $(\mathbb{C}, +, \cdot)$  sind Körper.

### 3.3. Zyklische Codes

Durch **Kanalcodierung** werden Informationen über gestörte Kanäle übertragen oder auf unsicheren Medien gespeichert. Durch hinzugefügte **Redundanz** können Fehler in der Form von veränderten Bits erkannt und teilweise sogar korrigiert werden. Die hier vorgestellten Verfahren werden in dieser Form beispielsweise direkt im USB-Standard, auf SD-Karten, in der Bluetooth-Übertragung und im Ethernet-Protokoll verwendet.

DEFINITION 3.35. Ein **Binärcode** ist eine injektive Abbildung  $c : M \rightarrow \mathbb{Z}_2^N$  für ein  $N \in \mathbb{N}$ . Das Bild des Binärcodes sind die **Codewörter** mit  $N$  Bits.

BEISPIEL 3.36. Ein **Wiederholungscode** wiederholt das Signal mehrfach, und wird beispielsweise auch im Funkverkehr im Fussballschiedswesen („Foul-Foul-Foul“) verwendet wird:

$$c : \mathbb{Z}_2 \rightarrow \mathbb{Z}_2^3$$

$$x \mapsto c(x) = (x, x, x)$$

Also ist  $c(0) = (0, 0, 0)$  und  $c(1) = (1, 1, 1)$ , und die Codewörter lauten  $\{(0, 0, 0), (1, 1, 1)\}$ . Wenn ein Signal gestört wird, und beispielsweise  $(1, 0, 1)$  empfangen wird, so ist unter der Annahme dass höchstens ein Fehler aufgetreten ist, vom korrigierten Codewort  $(1, 1, 1)$  auszugehen, und dass damit 1 ursprünglich kodiert wurde. Der Code kann auch so interpretiert werden, dass  $n = 1$  Datenbit um  $k = 2$  Prüfbits zu einem  $N = n + k = 3$  Bit-Binärcode ergänzt werden.

Um den Unterschied zwischen korrekten Daten und gestörten Daten bezeichnen zu können, wird ein Begriff für den Grad der Änderung benötigt:

DEFINITION 3.37. Sei  $n \in \mathbb{N}$  und seien  $x, y \in \mathbb{Z}_2^n$  zwei Binärvektoren der Länge  $n$ . Dann bezeichnet die **Hammingdistanz**  $H(x, y)$  die Anzahl der unterschiedlichen Bits:

$$H(x, y) = \sum_{k=1}^n \begin{cases} 0, & \text{wenn } x_k = y_k \\ 1, & \text{wenn } x_k \neq y_k \end{cases}$$

Über die geringste Hammingdistanz zu Codewörtern können Fehler korrigiert werden. Haben die Codewörter eines Codes untereinander eine minimale Hammingdistanz von 3, so können einfache Bitveränderungen, also empfangene Daten mit einer Hammingdistanz von 1 zu einem Codewort dahin eindeutig korrigiert werden.

BEISPIEL 3.38. In einem gestörten Kanal mit dem Wiederholungscode aus Beispiel 3.36 werden Bitvektoren  $d^{(k)}$  empfangen. Die Korrektur der gestörten Daten zum korrigierten Code  $y^{(k)}$  und Nachricht  $x^{(k)}$  erfolgt durch Bestimmung des Hamming-Abstands zu den zwei möglichen Codewörtern:

$d^{(k)}$	$H(d^{(k)}, c(0))$	$H(d^{(k)}, c(1))$	$y^{(k)}$	$x^{(k)}$	$d^{(k)}$	$H(d^{(k)}, c(0))$	$H(d^{(k)}, c(1))$	$y^{(k)}$	$x^{(k)}$
000	0	3	000	0	100	1	2	000	0
001	1	2	000	0	101	2	1	111	1
010	1	2	000	0	110	2	1	111	1
011	2	1	111	1	111	3	0	111	1

Nur in zwei der acht Fälle wurde ein fehlerfreier Code empfangen, in allen anderen Fällen konnte der empfangene Code zum von der Hammingdistanz nächsten Code korrigiert werden. Das ist für einen Code für  $n = 1$  Datenbits ein optimales Ergebnis. Für  $n = 2, 3, 4$  Bits könnte man das Verfahren wiederholen und diese in  $N = 6, 9, 12$  Bits kodieren, aber geht das auch mit besserem Verhältnis  $\frac{n}{N}$ , da mit dieser Kodierung nur ein Drittel der möglichen Bandbreite für Nutzdaten zur Verfügung steht?

Es wird vorausgesetzt, dass die Kanäle rein zufällig gestört sind. Damit sollte ein Code auch alle Bits der Codewörter gleichwertig behandeln, damit es nicht „wichtigere“ und „weniger wichtige“ Bits gibt, und so ein gezielter einzelner Treffer im „word-case scenario“ mehr Schaden anrichten kann. Daher ist es grundsätzlich sinnvoll, sich auf zyklische Codes zu beschränken:

DEFINITION 3.39. Ein Binärcode  $c : M \rightarrow \mathbb{Z}_2^N$  ist **zyklisch**, wenn es zu jedem Codewort  $c(x) = y = (y_1, \dots, y_N)$  zu einem  $x \in M$  auch die zyklische Drehung  $y' = (y_2, \dots, y_N, y_1)$  Codewort ist, also ein  $x' \in M$  existiert, so dass  $c(x') = y'$ .

BEISPIEL 3.40. Im Ring  $(\mathbb{Z}_2[x]/_{x^7+1}, +, \cdot)$  der Faktormenge der Polynome über  $\mathbb{Z}_2$  mit Äquivalenz  $0 \equiv x^7 + 1$  oder einfach  $x^7 \equiv 1$  kann der Bitvektor  $(0, 0, 0, 1, 0, 1, 1)$  als

$$p(x) = 0x^6 + 0x^5 + 0x^4 + 1x^3 + 0x^2 + 1x + 1 = x^3 + x + 1$$

abgebildet werden. Die zyklischen Drehungen ergeben sich durch Multiplikationen mit  $x^k$ :

$$\begin{aligned} p(x) &= x^3 + x + 1 && \leftrightarrow (0, 0, 0, 1, 0, 1, 1) \\ x \cdot p(x) &= x^4 + x^2 + x && \leftrightarrow (0, 0, 1, 0, 1, 1, 0) \\ x^2 \cdot p(x) &= x^5 + x^3 + x^2 && \leftrightarrow (0, 1, 0, 1, 1, 0, 0) \\ x^3 \cdot p(x) &= x^6 + x^4 + x^3 && \leftrightarrow (1, 0, 1, 1, 0, 0, 0) \\ x^4 \cdot p(x) &\equiv x^5 + x^4 + 1 && \leftrightarrow (0, 1, 1, 0, 0, 0, 1) \\ x^5 \cdot p(x) &\equiv x^6 + x^5 + x && \leftrightarrow (1, 1, 0, 0, 0, 1, 0) \\ x^6 \cdot p(x) &\equiv x^6 + x^2 + 1 && \leftrightarrow (1, 0, 0, 0, 1, 0, 1) \end{aligned}$$

DEFINITION 3.41. Ein Binärcode  $c : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^N$  ist **linear**, wenn für alle  $x^{(1)}, x^{(2)} \in \mathbb{Z}_2^n$  die Aussage

$$c(x^{(1)} + x^{(2)}) = c(x^{(1)}) + c(x^{(2)})$$

erfüllt ist.

BEMERKUNG 3.42. Damit können lineare Codes  $c : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^N$  durch eine Abbildungsmatrix dargestellt werden. Alternativ kann der Raum  $\mathbb{Z}_2^N$  auch durch  $\mathbb{Z}_2[x]/_{x^{N+1}}$ , also durch Polynome über  $\mathbb{Z}_2$  bis zum Grad  $N - 1$  repräsentiert werden, da hier sowohl zyklische als auch lineare Codes durch Multiplikation und Addition direkt abgebildet werden können, und damit nicht nur eine Darstellung des Codes, sondern auch eine Konstruktion von Codes ermöglicht.

DEFINITION 3.43. Ein Polynom  $p(x)$  ist ein **Generatorpolynom** eines Codes  $c : \mathbb{Z}_2[x]/_{x^{n+1}} \rightarrow \mathbb{Z}_2[x]/_{x^{N+1}}$ , wenn der Code durch diese Polynommultiplikation darstellbar ist:

$$c(q) = q \cdot p$$

Mit dem folgenden, hier nicht bewiesenen Satz, können zyklische Codes erzeugt werden, die als **CRC** oder **Cyclic Redundancy Check** bezeichnet werden:

SATZ 3.44. Ein Polynom  $p(x)$  ist genau dann Generatorpolynom eines zyklischen Codes  $c : \mathbb{Z}_2[x]/_{x^{n+1}} \rightarrow \mathbb{Z}_2[x]/_{x^{N+1}}$  mit der Länge von  $N$  Bits, wenn es Teiler von  $x^N + 1$  ist.

BEISPIEL 3.45. Das Polynom  $p(x) = x^3 + x + 1$  ist Teiler von  $x^7 + 1$ , da

$$x^7 + 1 = (x^3 + x + 1) \cdot (x^4 + x^3 + x + 1).$$

Damit ist  $p(x)$  Generatorpolynom eines zyklischen und linearen Codes mit  $N = 7$  Bits. Mit der Wahl von  $n = 4$  Datenbits haben alle Codewörter die Hammingdistanz von 3, und damit kann ein Bitfehler erfolgreich korrigiert werden. Beispielsweise wird der Bitvektor  $(0, 1, 0, 1)$  als Polynom  $q(x) = x^2 + 1$  dargestellt. Das zugehörige Codewort berechnet sich dann als Polynommultiplikation

$$\begin{aligned} q(x) \cdot p(x) &= (x^2 + 1) \cdot (x^3 + x + 1) \\ &= x^2 \cdot (x^3 + x + 1) + (x^3 + x + 1) \\ &= (x^5 + x^3 + x^2) + (x^3 + x + 1) \equiv x^5 + x^2 + x + 1 \end{aligned}$$

und wird damit als  $(0, 1, 0, 0, 1, 1, 1)$  kodiert. Abbildung 3.3.1 zeigt alle Codewörter des so genannten **(7, 4)-Hammingcode** mit 7 Code- und 4 Nachrichtenbits. Im Gegensatz zum Wiederholungscode mit der dreifachen Menge an Codebits verglichen zu den Nachrichtenbits werden hier nur weniger als doppelt

$x^{(k)}$	$C(x^{(k)})$	$x^{(k)}$	$C(x^{(k)})$
(0, 0, 0, 0)	(0, 0, 0, 0, 0, 0, 0)	(1, 0, 0, 0)	(1, 0, 1, 1, 0, 0, 0)
(0, 0, 0, 1)	(0, 0, 0, 1, 0, 1, 1)	(1, 0, 0, 1)	(1, 0, 1, 0, 0, 1, 1)
(0, 0, 1, 0)	(0, 0, 1, 0, 1, 1, 0)	(1, 0, 1, 0)	(1, 0, 0, 1, 1, 1, 0)
(0, 0, 1, 1)	(0, 0, 1, 1, 1, 0, 1)	(1, 0, 1, 1)	(1, 0, 0, 0, 1, 0, 1)
(0, 1, 0, 0)	(0, 1, 0, 1, 1, 0, 0)	(1, 1, 0, 0)	(1, 1, 1, 0, 1, 0, 0)
(0, 1, 0, 1)	(0, 1, 0, 0, 1, 1, 1)	(1, 1, 0, 1)	(1, 1, 1, 1, 1, 1, 1)
(0, 1, 1, 0)	(0, 1, 1, 1, 0, 1, 0)	(1, 1, 1, 0)	(1, 1, 0, 0, 0, 1, 0)
(0, 1, 1, 1)	(0, 1, 1, 0, 0, 0, 1)	(1, 1, 1, 1)	(1, 1, 0, 1, 0, 0, 1)

ABBILDUNG 3.3.1. Der zyklische und lineare  $(7, 4)$ -Hammingcode zu  $x^3 + x + 1$

so viele Codebits übertragen. Natürlich könnte der Wiederholungscode bis zu vier Bitfehler korrigieren, aber nur, wenn diese jeweils nur einzeln in einzelnen Blöcken auftreten, so dass im „Worst-Case Scenario“ der Wiederholungscode auch nicht mehr als einen Bitfehler erfolgreich korrigieren kann, ebenso wie dieser hier eingeführte Code für vier Nachrichtenbits.

BEISPIEL 3.46. Einige häufig verwendete zyklische Codes mit ihrem Generatorpolynom:

$N$	$n$	$k$	$p(x)$	Bezeichnung	Nutzung
3	1	2	$x^2 + x + 1$	Wiederholungscode	
7	4	3	$x^3 + x + 1$	$(7, 4)$ -Hammingcode	
15	11	4	$x^4 + x + 1$	$(15, 11)$ -Hammingcode / CRC-4	<b>Bluetooth</b>
31	26	5	$x^5 + x^2 + 1$	$(31, 26)$ -Hammingcode / CRC-5	<b>USB</b>
127	120	7	$x^7 + x^3 + 1$	$(127, 120)$ -Hammingcode / CRC-7	<b>SD-Card</b>
$2^{32} - 1$		32	$x^{32} + x^{26} + \dots + x + 1$	CRC-32	<b>Ethernet</b>

Auf CD-ROMs und auch zur frühen Deep-Space Kommunikation werden zyklische Codes verwendet, nur werden hier bei den **Reed-Solomon-Codes** statt Bits ganze Datenblöcke betrachtet, um die Übertragung resistent auch gegen längere Fehlerbursts zu machen.

Bei linearen Codes sind Linearkombinationen von Codewörtern auch immer Codewörter. Unabhängig von der Konstruktion über Generatorpolynome ist es daher ohne Einschränkungen der Leistungsfähigkeit des Codes möglich, die Kodierung so umzuordnen und linear zu kombinieren, so dass die ersten  $k$  Bits des Codes mit den Nachrichtenbits übereinstimmen. Ein Code, wo die Nachrichtbits Teil der codierten Bits sind, wird als **systematischer Code** bezeichnet. Die verbleibenden  $n - k$  Bits sind dann echte Prüfbits, die Fehler anzeigen und eventuell korrigieren können.

Grundsätzlich sind mit längeren Codes bessere Verhältnisse von korrigierbaren Fehlern zu zusätzlicher Redundanz möglich. Dabei ist aber immer abzuwägen, dass längere Codes sowohl einen höheren Aufwand in der Korrektur bedeuten und zusätzlich eine Block-Latenz erzeugen, da ein Block erst geprüft und eventuell korrigiert werden kann, wenn er komplett empfangen wurde.

### 3.4. Kryptographie

Die Kryptographie befasste sich ursprünglich mit Verfahren, um Information geheim zu übertragen. Viele frühere Verfahren bedienten sich gemeinsamen Geheimnissen, die aber einmal erraten oder anderweitig umgangen, die Verfahren nutzlos machen. Die Kryptoanalyse befasst sich daher mit der Frage, wie sicher Verfahren eigentlich sind. Heutzutage werden nur noch Verfahren verwendet, dessen Angreifbarkeit schon intensiv untersucht wurde, um durch eine Abwägung zwischen erforderlicher Sicherheit und damit zu treibendem Aufwand passend verschlüsselt werden kann. Die Algebra und die Zahlentheorie spielen in sehr vielen Verfahren eine zentrale Rolle.

Sehr viele Verfahren basieren auf der Multiplikation und besonders der Potenzierung auf  $\mathbb{Z}_n$  mit bestimmten und in Anwendungen sehr großen  $n \in \mathbb{N}$ , oder wenn  $n = p$  eine große Primzahl ist. In beiden Fällen können Potenzen mit großen Zahlen schnell berechnet werden:

Sei  $a \in \mathbb{Z}_n$  und wir suchen  $y = a^x$  für beispielsweise  $x = 17$ , so ist

$$x = a^{17} = \underbrace{a \cdot \dots \cdot a}_{16 \text{ Multiplikationen}} = a \cdot a^{16} = a \cdot \underbrace{\left( \left( (a^2)^2 \right)^2 \right)^2}_{5 \text{ Multiplikationen}}.$$

Dieses Verfahren nennt sich **binäre Exponentiation** oder das **Square-and-Multiply** Verfahren. Ein Quadrieren ist auch immer nur eine Multiplikation, verdoppelt aber den ursprünglichen Exponenten, und dadurch können sehr schnell auch hohe Potenzen berechnet werden. Beispielsweise verwenden ein Großteil der Schlüssel im RSA-Verfahren den Exponenten  $65537 = 2^{16} + 1$ , der mit nur 16 Multiplikationsschritten berechnet werden kann.

Warum ist nun die Potenzierung so interessant für die Verschlüsselung? Schauen wir uns Potenzen  $2^x$  in  $\mathbb{Z}_{253}$  an:

2, 4, 8, 16, 32, 64, 128, 3, 6, 12, 24, 48, 96, 192, 131, 9, 18, 36, 72, 144, 35, 70, 140, 27, 54, 108, ...

Oder die Potenzen  $3^x$  in  $\mathbb{Z}_{253}$ :

3, 9, 27, 81, 243, 223, 163, 236, 202, 100, 47, 141, 170, 4, 12, 36, 108, 71, 213, 133, 146, 185, ...

Nach den anfänglich bekannten Potenzen werden die Ergebnisse nach dem ersten „wrap-around“ beim Übersteigen von 253 scheinbar zufällig und nicht mehr vorhersagbar, obwohl sie leicht zu berechnen sind. So ist  $100 \cdot 3 = 300 \equiv 47 \pmod{253}$ . Es ist einfach und schnell machbar,  $y \equiv 3^{16} \pmod{253}$  zu berechnen, aber es ist sehr schwer aus der Gleichung  $3^x \equiv 36 \pmod{253}$  das passende  $x$  zu bestimmen. Natürlich ist es möglich, sich für ein festes  $n = 253$  Tabellen wie oben vorab zu erzeugen und dann den so genannten **diskreten Logarithmus** so schnell zu bestimmen, doch verwendet jede Person, jedes Gerät und jedes Verfahren immer unterschiedliche Zahlen für  $n$  und daher ist dieser Angriff nur durchführbar, wenn fehlerhafterweise häufig der gleiche Zahlenraum  $\mathbb{Z}_n$  verwendet wird.

Um sich mit einem Gesprächspartner geheim auszutauschen, wäre es ungemein praktisch, wenn Sie sich öffentlich, also für alle anderen mithörbar, austauschen und auf einen geheimen Schlüssel einigen könnten, ohne dass die Zuhörenden ebenfalls den Schlüssel erhalten. Genau so etwas wird dank der Potenzierung in  $\mathbb{Z}_p$  möglich:

DEFINITION 3.47. **Diffie-Hellman-Schlüsselaustausch** auf  $\mathbb{Z}_p$ :

- (1) Einer der Kommunikationspartner wählt eine Primzahl  $p$  und einen Erzeuger  $\alpha \in \mathbb{Z}_p \setminus \{0, 1\}$ . Die Parameter  $(p, \alpha)$  werden öffentlich an den anderen Partner übersendet.
- (2) Die zwei Kommunikationspartner wählen Zufallszahlen  $a$  und  $b$ , berechnen die Potenzen  $\alpha^a$  und  $\alpha^b$  in  $\mathbb{Z}_p$  und senden das Ergebnis öffentlich zum anderen Partner.
- (3) Jetzt werden die empfangenen Ergebnisse mit der eigenen Zufallszahl potenziert und die beiden erhalten  $(\alpha^a)^b$  bzw.  $(\alpha^b)^a$  in  $\mathbb{Z}_p$ .
- (4) Da  $(\alpha^a)^b = \alpha^{a \cdot b} = (\alpha^b)^a$  gilt, haben beide Kommunikationspartner nun einen gemeinsamen Schlüssel  $\alpha^{a \cdot b}$  für die weitere Kommunikation.

Dieses Verfahren ist die Basis für die Methoden der **Perfect Forward Secrecy**, bei der in festem Abstand auf diesem Wege immer neue Sitzungsschlüssel bestimmt werden, und ein Mitschnitt der übertragenen Daten im Nachhinein keine (einfachen) Rückschlüsse auf die übersendeten Daten ermöglicht. Natürlich funktioniert das nur, wenn immer unterschiedliche  $p$  und große Zahlen verwendet werden, damit ein Angriff zu teuer wird. Im Mai 2015 wurde festgestellt, dass 8.4% der TOP 1M-Webseiten durch eine fehlerhafte Implementation gleiche und zu kleine Primzahlen verwendeten, und damit dieser Sicherheitsmechanismus komplett ausgehebelt werden konnte. Dies war die [Logjam-Attacke](#).

BEISPIEL 3.48. Die Kommunikationspartner Alice und Bob einigen sich auf das Diffie-Hellman-Verfahren auf  $\mathbb{Z}_{233}$  und  $\alpha = 2$ .

	Alice	Bob
1.	Sende öffentlich $p = 233, \alpha = 2$	
2.	Geheime Zufallszahl $a = 28$	Geheime Zufallszahl $b = 17$
	Berechne $\alpha^a = 2^{28} \equiv 117 \pmod{233}$	Berechne $\alpha^b = 2^{17} \equiv 126 \pmod{233}$
	Sende öffentlich 117	Sende öffentlich 126
3.	Berechne $(\alpha^b)^a = 126^{28} \equiv 135 \pmod{233}$	Berechne $(\alpha^a)^b = 117^{17} \equiv 135 \pmod{233}$
4.	Verwende 135 als temporären Schlüssel	

Das Verfahren als solches ist aber gegen eine Man-in-the-Middle-Attacke anfällig: Hier setzt sich ein Angreifer zwischen die Kommunikationspartner und sendet jeweils eigene Werte an die beiden Opfer, und hat im Folgenden den vollen Zugriff auf die Daten.

Diese Attacke kann durch die Verwendung von Signaturen zur Authentifikation verhindert werden: Wenn die übersendeten Zahlen digital signiert werden, würde eine Attacke sofort auffliegen.

Der Schlüsselaustausch kommt bei der Verwendung von symmetrischen Kryptographieverfahren zum Einsatz: Hier verwenden die Sende- und Empfangsseite den gleichen Schlüssel, mit dem das Kryptoverfahren parametrisiert wird. Dies sind sehr effiziente Verfahren, aber die Schlüssel sollten immer nur für kurze Zeit verwendet werden. Bei asymmetrischen Kryptographieverfahren werden unterschiedliche Schlüssel zur Verschlüsselung und Entschlüsselung verwendet. Typischerweise wird der Schlüssel zum Entschlüsseln geheim gehalten und als privater Schlüssel bezeichnet, wogegen der Schlüssel zur Verschlüsselung auch als öffentlicher Schlüssel bezeichnet wird. Natürlich sollte es nicht einfach möglich sein, den privaten Schlüssel aus dem öffentlichen Schlüssel zu berechnen.

Die Grundidee, wie zwei solche Schlüssel und ein Verfahren konstruiert werden kann, liefert uns der folgende Satz:



THEOREM 3.49. *Kleiner Satz von Fermat.*

Sei  $p$  eine Primzahl und  $a \in \mathbb{Z}_p$ . Dann gilt

$$a^p \equiv a \pmod{p}.$$

Ist  $a \neq 0$ , so gelten die direkten Folgerungen

$$a^{p-1} \equiv 1 \pmod{p} \quad \text{und} \quad a^{n(p-1)} \equiv 1 \pmod{p}$$

für alle natürlichen Zahlen  $n \in \mathbb{N}$ .

BEWEIS. Beweis der Aussage  $a^p - a \equiv 0 \pmod{p}$  über vollständige Induktion:

$$a = 0 : \quad 0^p - 0 = 0.$$

$a \rightarrow a + 1$  : Es sei  $a^p - a \equiv 0 \pmod{p}$ , und wir erhalten mit der binomischen Formel

$$\begin{aligned} (a+1)^p - (a+1) &\equiv a^p + \binom{p}{1} a^{p-1} + \dots + \binom{p}{p-1} a + 1 - (a+1) \\ &\equiv \underbrace{a^p - a}_{\equiv 0} + \left[ \binom{p}{1} a^{p-1} + \dots + \binom{p}{p-1} a \right] \end{aligned}$$

Da nun  $\binom{p}{k} \in \mathbb{N}$  und für  $p > k$  der Primfaktor  $p$  nur im Zähler auftaucht, ist

$$\binom{p}{k} = \frac{p(p-1) \cdots (p-k+1)}{1 \cdot 2 \cdots k} = p \cdot \frac{(p-1) \cdots (p-k+1)}{1 \cdot 2 \cdots k}$$

für  $0 < k < p$  durch  $p$  teilbar, und damit gilt  $\binom{p}{k} \equiv 0 \pmod{p}$ . Also ist

$$(a+1)^p - (a+1) \equiv 0 \pmod{p}.$$

□

BEISPIEL 3.50. Mit dem kleinen Satz von Fermat kann in  $\mathbb{Z}_p$  für eine Primzahl  $p$  ein zweigeteilter Schlüssel erzeugt werden: Das Kryptoverfahren soll über Potenzieren im  $\mathbb{Z}_p$  funktionieren. Beispielsweise rechnen wir hier in  $\mathbb{Z}_5$  und der öffentliche Schlüssel soll 7 sein. Nachrichten  $x$  werden als  $x^7$  verschlüsselt. Angenommen wir erhalten die verschlüsselte Nachricht 3. Wie können wir nun die „7. Wurzel“ ziehen, damit wir wieder zur Nachricht gelangen?

Wir suchen zum Entschlüsseln nun ein  $x$  mit  $x^7 \equiv 3 \pmod{5}$ . Mit  $3^k \equiv (x^7)^k \equiv x^{7k} \pmod{5}$  können wir nun ein  $k$  suchen, so dass  $7k = n(p-1) + 1$  gilt. Denn dann ist

$$x^{7k} \equiv x^{n(p-1)+1} \equiv 1 \cdot x \pmod{5}.$$

Mit  $n(p-1) + 1 = 4n + 1 \in \{5, 9, 13, 17, 21, \dots\}$  erhalten wir für  $n = 5$  und  $k = 3$  das Gewünschte:  $7 \cdot 3 = 5 \cdot 4 + 1$ . Und damit ist

$$3^3 \equiv 2 \equiv x \pmod{5}$$

das Ergebnis. Die Kontrolle  $2^7 = 128 = 125 + 3$  zeigt schnell, dass das Ergebnis korrekt ist. In  $\mathbb{Z}_5$  gilt allgemein

$$\sqrt[7]{x} \equiv x^3 \pmod{5}.$$

Der kleine Satz von Fermat ist also hier eine Möglichkeit, mit dem die 7. Wurzel in  $\mathbb{Z}_5$  auf leichtem Weg durch Potenzieren mit 3 berechnet werden kann. Leider ist dieser Trick zu bekannt, und deshalb braucht es Verfahren mit „geheimen“ Tricks. Diese gibt es durch die Erweiterung des kleinen Satzes von Fermat:

DEFINITION 3.51. Die **Eulersche Phi-Funktion** bezeichnet die Anzahl der zu  $n$  teilerfremden ganzen Zahlen in  $1, \dots, n$ :

$$\varphi(n) = |\{a \in \mathbb{N} \mid 1 \leq a \leq n \wedge \text{ggT}(a, n) = 1\}|$$

Beispielsweise ist  $\varphi(6) = 2$ , da nur 1 und 5 die Bedingungen erfüllen. Hingegen ist  $\varphi(7) = 6$ , da 7 zu allen Zahlen 1, 2, 3, 4, 5, 6 teilerfremd ist, nach obiger Definition. Damit lässt sich der folgende Satz formulieren, der hier nicht bewiesen wird:

SATZ 3.52. **Satz von Euler-Fermat.** Sei  $n \in \mathbb{N}$  und  $a \in \mathbb{Z}_n$ . Dann ist

$$a \equiv a^{\varphi(n)+1} \pmod{n}.$$

Ist  $n = p \cdot q$  für zwei Primzahlen  $p \neq q$ , so ist  $\varphi(n) = (p-1)(q-1)$  und es folgt

$$a \equiv a^{(p-1)(q-1)+1} \pmod{n}.$$

Damit kann entsprechend zu den Vorüberlegungen das RSA-Verfahren formuliert werden:

DEFINITION 3.53. Das **RSA-Verfahren**:

- (1) Wählen Sie zwei große unterschiedliche Primzahlen  $p$  und  $q$ .
- (2) Berechnen Sie das Produkt  $n = pq$ .
- (3) Wähle einen zu  $(p-1)(q-1)$  teilerfremden öffentlichen Exponenten  $e \in \mathbb{N}$ , das heißt

$$\text{ggT}(e, (p-1)(q-1)) = 1.$$

- (4) Berechne den geheimen Exponenten  $d \in \mathbb{N}$  mit der Eigenschaft

$$e \cdot d \equiv 1 \pmod{(p-1)(q-1)}.$$

Dann ist  $k_{PUB} = (e, n)$  der öffentliche Schlüssel und  $k_{SEC} = (d, n)$  der zugehörige geheime Schlüssel dieses RSA-Verfahrens.

BEISPIEL 3.54. Wir erwürfeln die zwei Primzahlen  $p = 53$  und  $q = 71$ . Damit erhalten wir

$$n = 53 \cdot 71 = 3763.$$

Als Kandidaten für den öffentlichen Exponenten versuchen wir  $e = 17$ , und berechnen wegen  $(p-1)(q-1) = 52 \cdot 70 = 3640$  den  $\text{ggT}(17, 3640)$  mit dem Euklidischen Algorithmus:

$$\begin{aligned} 3640 &= 214 \cdot 17 + 2 \\ 17 &= 8 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 \end{aligned}$$

Wir erhalten den  $\text{ggT}(17, 3640) = 1$ . Damit ist  $e = 17$  geeignet, und über den erweiterten Euklidischen Algorithmus erhalten wir den geheimen Exponenten  $d$  mit  $e \cdot d \equiv 1 \pmod{(p-1)(q-1) = 3640}$ :

$$\begin{aligned} 1 &= 17 - 8 \cdot 2 \\ &= 17 - 8 \cdot (3640 - 214 \cdot 17) \\ &= -8 \cdot 3640 + 1713 \cdot 17 \end{aligned}$$

Also ist  $17 \cdot 1713 = 1 + 8 \cdot 3640$  bzw.  $17 \cdot 1713 \equiv 1 \pmod{3640}$ , also ist  $d = 1713$  der gesuchte geheime Exponent. Jetzt heißt es  $p$  und  $q$  zu vergessen, und  $k_{PUB} = (17, 3763)$  zu veröffentlichen und  $k_{SEC} = (1713, 3763)$  sicher abzuspeichern.

Will uns nun jemand die Nachricht  $m = 255$  senden, so berechnet die Person mit dem öffentlichen Schlüssel  $k_{PUB} = (17, 3763)$ :

$$c = m^{17} = 255^{17} \equiv 2137 \pmod{3763}$$

Sobald wir die Nachricht  $c = 2137$  erhalten, verwenden wir den geheimen Exponenten, um zur Nachricht zurück zu gelangen

$$c^{1713} = 2137^{1713} \equiv 255 \pmod{3763}$$

und erhalten wie erhofft die Nachricht  $m = 255$  als Ergebnis.

### 3.5. Aufgaben

**AUFGABE 41.** Die Menge  $M = \{a, b, c, d\}$  soll mit der Operation  $*$  eine Gruppe bilden. Ergänzen Sie die Verknüpfungstafel und bestimmen Sie, ob die resultierende Gruppe kommutativ ist:

$x * y$	$y = a$	$y = b$	$y = c$	$y = d$
$x = a$				$c$
$x = b$		$b$		
$x = c$	$b$			
$x = d$			$a$	

**AUFGABE 42.** Die Menge  $M = \{a, b, c, d\}$  soll mit der Operation  $*$  eine Gruppe bilden. Ergänzen Sie die Verknüpfungstafel und bestimmen Sie, ob die resultierende Gruppe kommutativ ist:

$x * y$	$y = a$	$y = b$	$y = c$	$y = d$
$x = a$				$a$
$x = b$		$d$		
$x = c$	$b$			
$x = d$				

**AUFGABE 43.** Bestimmen Sie alle Elemente von  $\langle (12)(34), (13)(24) \rangle$ . Ist die resultierende Gruppe kommutativ?

**AUFGABE 44.** Bestimmen Sie alle Elemente von  $\langle (13), (1234) \rangle$ . Ist die resultierende Gruppe kommutativ?

**AUFGABE 45.** Bestimmen Sie in  $(\mathbb{Z}_8, +)$  die Ordnung aller Elemente.

**AUFGABE 46.** Bestimmen Sie in  $(\mathbb{Z}_{12}, +)$  die Ordnung aller Elemente.

**AUFGABE 47.** Erstellen Sie bezüglich  $3x^2 - 6x$  das Hassediagramm zur Teilbarkeit in  $\mathbb{Z}[x]$  durch Terme mit positivem Vorzeichen.

**AUFGABE 48.** Erstellen Sie bezüglich  $2x^2 + 6x + 4$  das Hassediagramm zur Teilbarkeit in  $\mathbb{Z}[x]$  durch Terme mit positivem Vorzeichen.

**AUFGABE 49.** Bestimmen Sie durch den euklidischen Algorithmus den  $x = \text{ggT}(81, 57)$  und zwei ganze Zahlen  $u, v$  mit  $x = 81u + 57v$ .

**AUFGABE 50.** Bestimmen Sie durch den euklidischen Algorithmus den  $x = \text{ggT}(98, 77)$  und zwei ganze Zahlen  $u, v$  mit  $x = 98u + 77v$ .

**AUFGABE 51.** Bestimmen Sie in  $\mathbb{Z}_{94}$  eine positive multiplikative Inverse zu 41.

**AUFGABE 52.** Bestimmen Sie in  $\mathbb{Z}_{99}$  eine positive multiplikative Inverse zu 70.

**AUFGABE 53.** Berechnen Sie in  $\mathbb{Z}_2[x]/_{x^4+1}$ :

- (1)  $(x^2 + x) + (x^3 + x + 1)$
- (2)  $(x^2 + 1) \cdot (x^3 + x + 1)$

**AUFGABE 54.** Berechnen Sie in  $\mathbb{Z}_2[x]/_{x^5+x+1}$ :

- (1)  $(x + 1) + (x^2 + 1) + (x^3 + x + 1)$
- (2)  $(x + 1)^3 \cdot (x^3 + x^2 + 1)$

**AUFGABE 55.** Bestimmen Sie in  $\mathbb{Z}_2[x]/_{x^6+1}$  alle Polynome  $x^k \cdot (x^3 + x + 1)$ ,  $k \in \mathbb{N}$  und deren binäre Repräsentation.

**AUFGABE 56.** Bestimmen Sie in  $\mathbb{Z}_2[x]/_{x^6+1}$  alle Polynome  $x^k \cdot (x^4 + x + 1)$ ,  $k \in \mathbb{N}$  und deren binäre Repräsentation.

**AUFGABE 57.** Zeigen Sie, dass  $x^3 + x^2 + 1$  in  $\mathbb{Z}_2[x]/_{x^7+1}$  ein Generatorpolynom eines zyklischen Codes ist, und bestimmen Sie den binären Code von  $(1, 0, 0, 1)$ .

**AUFGABE 58.** Zeigen Sie, dass  $x^4 + x^2 + x + 1$  in  $\mathbb{Z}_2[x]/_{x^7+1}$  ein Generatorpolynom eines zyklischen Codes ist, und bestimmen Sie den binären Code von  $(0, 1, 0, 1)$ .

**AUFGABE 59.** Alice und Bob möchten mit dem Diffie-Hellman Verfahren einen geheimen Sitzungsschlüssel vereinbaren. Sie entscheiden sich, das Verfahren auf  $\mathbb{Z}_{17}$  mit  $\alpha = 11$  durchzuführen. Alice wählt die Zufallszahl  $a = 7$  und Bob die Zufallszahl  $b = 9$ . Welche Nachrichten schicken sich Alice und Bob und was wird ihr Sitzungsschlüssel sein?

**AUFGABE 60.** Alice und Bob wollen sich mit dem Diffie-Hellman-Verfahren auf einen gemeinsamen Schlüssel einigen. Im Vorfeld haben sie abgesprochen, dass sie in  $\mathbb{Z}_{11}$  rechnen werden, und  $\alpha = 2$  verwenden. Alice hat sich das Geheimnis  $a = 3$ , Bob das Geheimnis  $b = 4$  ausgedacht.

**AUFGABE 61.** RSA-Schlüsselberechnung: Sie haben die zwei Primzahlen  $p = 61$  und  $q = 83$  bestimmt, und versuchen Ihr Glück mit den Kandidaten 27, 29 und 65537 für den öffentlichen Exponenten  $e$ . Prüfen Sie mit dem Euklidischen Algorithmus, welcher Exponent in Frage kommt, und berechnen Sie für diese den zugehörigen geheimen Exponenten  $d$ .

**AUFGABE 62.** Es seien  $p = 13$  und  $q = 19$  zwei geheime Primzahlen mit Produkt  $p \cdot q = 247$ . Zeigen Sie, dass  $e = 5$  als Exponent für einen geheimen RSA-Schlüssel in  $\mathbb{Z}_{247}$  in Frage kommt. Bestimmen Sie den zugehörigen Exponenten des öffentlichen Schlüssels und schreiben Sie das Schlüsselpaar auf.



## Boolesche Algebra und logische Schaltungen

Das Konzept der Booleschen Algebra umfasst verschiedene Strukturen, die bis jetzt schon Thema waren:

DEFINITION 4.1. Eine **Boolesche Algebra**  $(B, \oplus, \odot, \neg, 0, 1)$  besteht aus einer Menge  $B$  mit Elementen  $0, 1$  und den Verknüpfungen der Addition  $\oplus$ , und Multiplikation  $\odot$  auf  $B$  und dem Komplement  $\neg : B \rightarrow B$  mit folgenden Eigenschaften für alle  $a, b, c \in B$ :

<b>Assoziativität</b>	$x \oplus (y \oplus z) = (x \oplus y) \oplus z$	$x \odot (y \odot z) = (x \odot y) \odot z$
<b>Kommutativität</b>	$x \oplus y = y \oplus x$	$x \odot y = y \odot x$
<b>Distributivität</b>	$x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$	$x \oplus (y \odot z) = (x \oplus y) \odot (x \oplus z)$
<b>Identität</b>	$x \oplus 0 = x$	$x \odot 1 = x$
<b>Komplement</b>	$x \oplus \neg x = 1$	$x \odot \neg x = 0$

Einige wichtige Beispiele für Boolesche Algebren:

BEISPIEL 4.2.

- (1) Sei  $D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$  die Menge der positiven Teiler der Zahl 30, das **kleinste gemeinsame Vielfache** zweier Zahlen definiert als  $\text{kgV}(a, b) = \frac{ab}{\text{ggT}(a, b)}$ , und das Komplement hier durch  $\neg a = \frac{30}{a}$  definiert. Dann ist die Struktur  $(D_{30}, \text{kgV}, \text{ggT}, \neg, 1, 30)$  die Boolesche **Teileralgebra**. Beispielsweise ist in  $D_{30}$ :

$$\begin{aligned}
 6 \oplus 15 &= \text{kgV}(6, 15) = 30 = 15 \oplus 6 & 2 \oplus 10 &= \text{kgV}(2, 10) = 10 = 10 \oplus 2 \\
 6 \odot 15 &= \text{ggT}(6, 15) = 3 = 15 \odot 6 & 2 \odot 10 &= \text{ggT}(2, 10) = 2 = 10 \odot 2 \\
 \neg 6 &= \frac{30}{6} = 5 & \neg 2 &= \frac{30}{2} = 15 \\
 6 \oplus \neg 6 &= 6 \oplus 5 = \text{kgV}(6, 5) = 30 = 1 & 2 \oplus \neg 2 &= 2 \oplus 15 = \text{kgV}(2, 15) = 30 = 1 \\
 6 \odot \neg 6 &= 6 \odot 5 = \text{ggT}(6, 5) = 1 = 0 & 2 \odot \neg 2 &= 2 \odot 15 = \text{ggT}(2, 15) = 1 = 0
 \end{aligned}$$

- (2) Sei  $M$  eine endliche, nichtleere Menge: Dann ist deren **Potenzmenge**  $\mathcal{P}(M)$  mit Vereinigung und Schnitt und dem **Mengenkomplement**  $\neg A = M \setminus A$  in der Form  $(\mathcal{P}(M), \cup, \cap, \neg, \emptyset, M)$  die Boolesche **Mengenalgebra**. Beispielsweise ist für  $M = \{2, 3, 5\}$ :

$$\begin{aligned}
 \{2, 3\} \oplus \{3, 5\} &= \{2, 3\} \cup \{3, 5\} = \{2, 3, 5\} \\
 \{2, 3\} \odot \{3, 5\} &= \{2, 3\} \cap \{3, 5\} = \{3\} \\
 \neg \{2, 3\} &= \{2, 3, 5\} \setminus \{2, 3\} = \{5\} \\
 \{2, 3\} \oplus \neg \{2, 3\} &= \{2, 3\} \oplus \{5\} = \{2, 3, 5\} = 1 \\
 \{2, 3\} \odot \neg \{2, 3\} &= \{2, 3\} \odot \{5\} = \emptyset = 0
 \end{aligned}$$

- (3) Die kleinste Boolesche Algebra ist die **Schaltalgebra**  $(\mathbb{Z}_2, \vee, \wedge, \neg, 0, 1)$  mit  $\neg x = 1 - x$ , wobei falsch mit 0 und wahr mit 1 identifiziert wird.

Tatsächlich ist der Zusammenhang zwischen  $D_{30}$  und  $\{2, 3, 5\}$  nicht zufällig, sondern diese beiden Booleschen Algebren stehen in einem direktem Zusammenhang: Existiert zwischen den Mengen  $X, Y$  zweier algebraischen Strukturen

$$(X, \oplus_X, \odot_X, \neg_X, 0_X, 1_X), (Y, \oplus_Y, \odot_Y, \neg_Y, 0_Y, 1_Y),$$

eine bijektive Abbildung  $f : X \rightarrow Y$ , bei der alle Operationen der Struktur nach Anwendung von  $f$  erhalten bleiben, also

$$f(a \oplus_X b) = f(a) \oplus_Y f(b),$$

$$f(a \odot_X b) = f(a) \odot_Y f(b),$$

$$f(\neg_X a) = \neg_Y f(a),$$

$$f(0_X) = 0_Y,$$

$$f(1_X) = 1_Y,$$

so nennt man diese bijektive Abbildung eine **Isomorphie** und die beiden Strukturen isomorph zu einander. Hier wäre das Produkt der Elemente der Mengen mit der Zuordnung der leeren Menge auf die Zahl 1 eine entsprechende Isomorphie zwischen  $M = \{2, 3, 5\}$  und  $D_{30}$ . Für jede Boolesche Algebra gibt es nach dem von M. H. Stone 1936 aus der Topologie bewiesenen Darstellungssatz eine isomorphe Mengenalgebra:

**THEOREM 4.3. (Darstellungssatz)** Sei  $(B, \oplus, \odot, \neg, 0, 1)$  eine boolesche Algebra. Dann gibt es eine Menge  $M$ , so dass die boolesche Algebra  $(\mathcal{P}(M), \cup, \cap, \neg, \emptyset, M)$  zu  $(B, \oplus, \odot, \neg, 0, 1)$  isomorph ist.

Auch wenn dieser Darstellungssatz entsprechend auch für unendliche Mengen  $B$  oder  $M$  gilt, so sind im endlichen Fall die  $n = |M|$  Elemente von  $M = \{m_1, \dots, m_n\}$  durchzählbar. Damit ist jede Teilmenge  $A$  von  $M$  repräsentierbar durch einen Vektor aus  $\mathbb{Z}_2^n$ , wobei jeder Eintrag in  $x = (x_1, \dots, x_n)$ , also beispielsweise  $x_k$  mit 1 oder 0 bezeichnet, ob das jeweilige durchgezählte Element  $m_k$  aus  $M$  in  $A$  vorhanden ist oder nicht. Auf  $\mathbb{Z}_2^n$  kann dann ebenso durch elementweise Anwendung der Operationen in  $\mathbb{Z}_2$  eine zu  $M$  isomorphe boolesche Algebra definiert werden.

Zwar definieren allgemeine boolesche Algebren viele Zustände zwischen  $0$  und  $1$ , die auch als falsch und wahr interpretiert werden können, aber diese können im endlichen Fall mit dem Darstellungssatz und diesen Überlegungen vollständig durch Vektoren in  $\mathbb{Z}_2^n$  isomorph abgebildet werden. Daher werden für praktische Anwendungen nur noch Boolesche Algebren über  $\mathbb{Z}_2$  oder den Vektoren  $\mathbb{Z}_2^n$  im Sinne mehrerer  $\mathbb{Z}_2$ -Variablen betrachtet und begrifflich oft synonym verwendet.

#### 4.1. Boolesche Funktionen und Normalformen

**DEFINITION 4.4.** Eine Funktion  $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$  ist eine **boolesche Funktion**. Eine Variable  $x \in \mathbb{Z}_2$  ist eine **boolesche Variable**.

**SATZ 4.5.** Jede boolesche Funktion  $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$  wird eindeutig durch ihre **Wahrheitstafel** mit der Identifikation von 0 zu falsch und 1 zu wahr dargestellt und jede Wahrheitstafel definiert eine boolesche Funktion.

**BEWEIS.** Jede Funktion ist eindeutig durch die Bilder der Elemente aus ihrer Definitionsmenge definiert und umgekehrt erfüllt eine vollständig ausgefüllte Wahrheitstafel mit  $2^n$  Einträgen die Bedingungen für eine Funktion  $\mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$ .  $\square$

**KOROLLAR 4.6.** Es gibt  $2^{(2^n)}$  unterschiedliche  $n$ -stellige boolesche Funktionen  $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$ .



BEWEIS. Es gibt  $m = 2^n$  Elemente in  $\mathbb{Z}_2^n$ . Jedes Element kann auf 0 oder 1 abgebildet werden, damit gibt es insgesamt  $2^m = 2^{(2^n)}$  unterschiedliche boolesche Funktionen.  $\square$

Boolesche Funktionen können auch durch boolesche Ausdrücke konstruiert werden:

DEFINITION 4.7. Auf der Booleschen Algebra  $(\mathbb{Z}_2, \vee, \wedge, \neg, 0, 1)$  seien  $x_1, \dots, x_n$  boolesche Variablen. Dann ist  $E(x_1, \dots, x_n)$  ein **boolescher Ausdruck**, wenn

$$(1) \ E(x_1, \dots, x_n) = a \text{ für } a \in \{0, 1, x_1, \dots, x_n\}, \text{ oder}$$

$$(2) \ E(x_1, \dots, x_n) = \begin{cases} \neg G(x_1, \dots, x_n), & \text{oder} \\ G(x_1, \dots, x_n) \vee H(x_1, \dots, x_n), & \text{oder} \\ G(x_1, \dots, x_n) \wedge H(x_1, \dots, x_n) \end{cases}$$

für boolesche Ausdrücke  $G(x_1, \dots, x_n)$  und  $H(x_1, \dots, x_n)$ .

Da alle logischen Junktoren auf die elementaren Junktoren  $\vee, \wedge, \neg$  zurückgeführt werden können, werden oft auch Ausdrücke mit anderen Junktoren boolesche Ausdrücke genannt. Weiterhin kann auch die Negation kürzer als  $\neg x = \bar{x}$  geschrieben werden.

Die Anzahl  $n$ -stelliger boolescher Funktionen steigt für  $n$  zwar stark an, aber die Anzahl boolescher Ausdrücke übersteigt jedes  $n$  leicht, da sogar ohne Änderung der Funktion beliebig beispielsweise „ $\vee 0$ “ an einen Ausdruck angehängt werden kann. Es macht also viel Sinn, strukturierte Darstellungen für boolesche Ausdrücke zu suchen:

SATZ 4.8. **Boolesche Normalformen.** Sei  $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$  eine boolesche Funktion, und die Notation  $a^{(0)} = \neg a$  und  $a^{(1)} = a$ . Dann hat  $f$  zwei bis auf Kommutativität eindeutige Darstellungen als

(1) **Disjunktive Normalform (DNF)** als boolescher Ausdruck

$$f(x_1, \dots, x_n) = \bigvee_{(a_1, \dots, a_n) \in f^{-1}(\{1\})} \left( x_1^{(a_1)} \wedge \dots \wedge x_n^{(a_n)} \right),$$

(2) und als **Konjunktive Normalform (KNF)** als boolescher Ausdruck

$$f(x_1, \dots, x_n) = \bigwedge_{(a_1, \dots, a_n) \in f^{-1}(\{0\})} \left( x_1^{(\neg a_1)} \vee \dots \vee x_n^{(\neg a_n)} \right).$$

Ist  $f^{-1}(\{1\}) = \emptyset$ , so ist die DNF konstant 0, und bei  $f^{-1}(\{0\}) = \emptyset$  die KNF konstant 1.

BEWEIS.

(1) Zu zeigen ist: Für  $x \in \mathbb{Z}_2^n$  gilt  $f(x) = \bigvee_{(a_1, \dots, a_n) \in f^{-1}(\{1\})} \left( x_1^{(a_1)} \wedge \dots \wedge x_n^{(a_n)} \right)$ .

- Sei  $x \in \mathbb{Z}_2^n$  und  $f(x) = 1$ . Dann ist  $x \in f^{-1}(\{1\})$  und für beliebiges  $k = 1, \dots, n$  ist  $x_k^{(x_k)} = 1$ , denn wenn  $x_k = 1$ , so ist  $x_k^{(1)} = x_k = 1$  und ist  $x_k = 0$ , so ist  $x_k^{(0)} = \neg x_k = \neg 0 = 1$ . Also sind sämtliche  $x_k^{(x_k)}$  im Ausdruck  $x_1^{(a_1)} \wedge \dots \wedge x_n^{(a_n)}$  für  $a = x$  gleich 1 und damit ist der Ausdruck 1. Da alle diese Ausdrücke mit Disjunktion verbunden sind, reicht dies, damit die gesamte rechte Seite 1 wird, und das war zu zeigen.
- Sei  $x \in \mathbb{Z}_2^n$  und  $f(x) = 0$ . Dann ist  $x \notin f^{-1}(\{1\})$ . Für alle Terme  $y \in f^{-1}(\{1\})$  auf der rechten Seite gibt es mindestens ein  $k \in \{1, \dots, n\}$  mit  $x_k \neq y_k$  und für diesen gilt  $x_k^{(y_k)} = 0$ , denn ist  $x_k = 0$ , so ist  $y_k = 1$  und  $x_k^{(y_k)} = x_k^{(1)} = x_k = 0$  und ist  $x_k = 1$ , so ist  $y_k = 0$  und  $x_k^{(y_k)} = x_k^{(0)} = \neg x_k = \neg 1 = 0$ . Damit ist der Term  $x_1^{(a_1)} \wedge \dots \wedge x_n^{(a_n)}$  für alle  $y = a$  gleich 0. Da dies für alle  $y \in f^{-1}(\{1\})$  gilt, gilt dies für alle über Disjunktion verbundene Terme und damit für die gesamte rechte Seite, was zu zeigen war.

(2) Zu zeigen ist: Für  $x \in \mathbb{Z}_2^n$  gilt  $f(x_1, \dots, x_n) = \bigwedge_{(a_1, \dots, a_n) \in f^{-1}(\{0\})} (x_1^{(\neg a_1)} \vee \dots \vee x_n^{(\neg a_n)})$ .

- Sei  $x \in \mathbb{Z}_2^n$  und  $f(x) = 0$ . Dann ist  $x \in f^{-1}(\{0\})$  und für beliebiges  $k = 1, \dots, n$  ist  $x_k^{(\neg x_k)} = 0$ , denn wenn  $x_k = 1$ , so ist  $x_k^{(0)} = \neg x_k = 0$  und ist  $x_k = 0$ , so ist  $x_k^{(1)} = \neg x_k = 0$ . Also sind sämtliche  $x_k^{(x_k)}$  im Ausdruck  $x_1^{(\neg a_1)} \vee \dots \vee x_n^{(\neg a_n)}$  für  $a = x$  gleich 0 und damit ist der Ausdruck 0. Da alle diese Ausdrücke mit Konjunktion verbunden sind, reicht dies, damit die gesamte rechte Seite 0 wird, und das war zu zeigen.
- Sei  $x \in \mathbb{Z}_2^n$  und  $f(x) = 1$ . Dann ist  $x \notin f^{-1}(\{0\})$ . Für alle Terme  $y \in f^{-1}(\{0\})$  auf der rechten Seite gibt es mindestens ein  $k \in \{1, \dots, n\}$  mit  $x_k \neq y_k$  und für diesen gilt  $x_k^{(y_k)} = 1$ , denn ist  $x_k = 0$ , so ist  $y_k = 1$  und  $x_k^{(\neg y_k)} = x_k^{(0)} = x_k = 1$  und ist  $x_k = 1$ , so ist  $y_k = 0$  und  $x_k^{(\neg y_k)} = x_k^{(1)} = \neg x_k = 1$ . Damit ist der Term  $x_1^{(\neg a_1)} \vee \dots \vee x_n^{(\neg a_n)}$  für alle  $y = a$  gleich 1. Da dies für alle  $y \in f^{-1}(\{0\})$  gilt, gilt dies für alle über Konjunktion verbundene Terme und damit für die gesamte rechte Seite, was zu zeigen war.

□

BEISPIEL 4.9. Die boolesche Funktion

$$f(x_1, x_2, x_3) = (x_1 \vee (\overline{x_3} \wedge x_2)) \wedge (\overline{x_2} \vee (x_3 \wedge x_1))$$

hat die folgende Wahrheitstafel:

$x_1$	$x_2$	$x_3$	$f(x_1, x_2, x_3)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	1

Damit lautet die disjunktive Normalform (mit Zuordnung der Funktionswerte zu den Termen)

$$f(x_1, x_2, x_3) = \underbrace{(x_1 \wedge \overline{x_2} \wedge \overline{x_3})}_{f(1,0,0)=1} \vee \underbrace{(x_1 \wedge \overline{x_2} \wedge x_3)}_{f(1,0,1)=1} \vee \underbrace{(x_1 \wedge x_2 \wedge x_3)}_{f(1,1,1)=1},$$

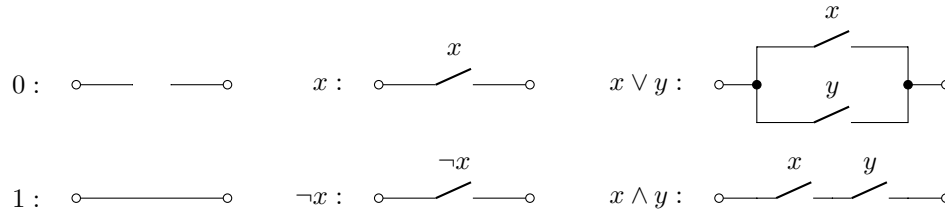
und die konjunktive Normalform lautet (mit entsprechender Zuordnung)

$$f(x_1, x_2, x_3) = \underbrace{(x_1 \vee x_2 \vee x_3)}_{f(0,0,0)=0} \wedge \underbrace{(x_1 \vee x_2 \vee \overline{x_3})}_{f(0,0,1)=0} \wedge \underbrace{(x_1 \vee \overline{x_2} \vee x_3)}_{f(0,1,0)=0} \wedge \underbrace{(x_1 \vee \overline{x_2} \vee \overline{x_3})}_{f(0,1,1)=0} \wedge \underbrace{(\overline{x_1} \vee \overline{x_2} \vee x_3)}_{f(1,1,0)=0}.$$

## 4.2. Logische Schaltungen

Boolesche Ausdrücke sind gleichbedeutend als idealisierte elektrische **Schaltwerke** darstellbar, der Wert 0 bedeutet, dass keine Verbindung besteht und kein Strom durch die Schaltung fließen kann, der Wert 1 entspricht einer Verbindung, dass also hier ein Strom zwischen Anfang und Ende fließen kann. Boolesche Variablen steuern hier Schalter als **Schließer** oder negiert als **Öffner**.

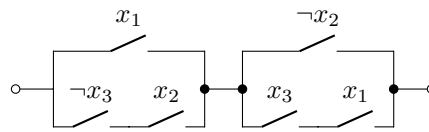
DEFINITION 4.10. Die **Schaltungsdiagramme** der booleschen Schaltalgebra  $(\mathbb{Z}_2, \vee, \wedge, \neg, 0, 1)$ :



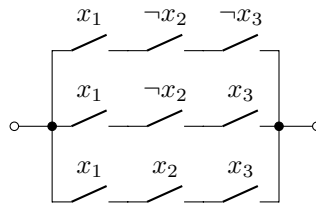
Auf Basis dieser Elemente können beliebige boolesche Ausdrücke in Schaltungen überführt werden und entsprechend aufgebaute Schaltungen als boolesche Ausdrücke interpretiert werden. Dabei können

BEISPIEL 4.11. Die Darstellungen aus Beispiel 4.9 als Schaltungen:

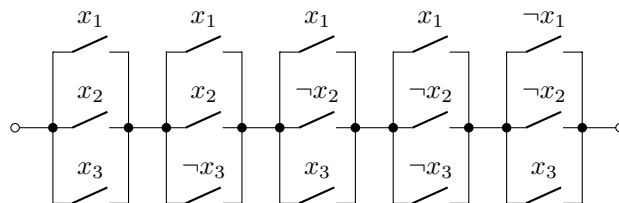
$$f(x_1, x_2, x_3) = (x_1 \vee (\overline{x_3} \wedge x_2)) \wedge (\overline{x_2} \vee (x_3 \wedge x_1)) :$$



$$f(x_1, x_2, x_3) = (x_1 \wedge \overline{x_2} \wedge \overline{x_3}) \vee (x_1 \wedge \overline{x_2} \wedge x_3) \vee (x_1 \wedge x_2 \wedge x_3) :$$



$$f(x_1, x_2, x_3) = (x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee x_2 \vee \overline{x_3}) \wedge (x_1 \vee \overline{x_2} \vee x_3) \wedge (x_1 \vee \overline{x_2} \vee \overline{x_3}) \wedge (\overline{x_1} \vee \overline{x_2} \vee x_3) :$$



In der praktischen **Digitaltechnik** werden logische Schaltungen natürlich nicht mit abstrakten Schaltern sondern mit Transistoren in der Form von Logikgattern umgesetzt. In Abbildung 4.2.1 ist ein npn-Transistor in typischer Verstärkungsschaltung dargestellt, an dessen **Kollektor** (C) am n-dotierten Anschluss über einen Widerstand  $R_C$  der Pluspol der Versorgungsspannung, und an dessen **Emitter** (E) am anderen n-dotierten Anschluss der Minuspol der Betriebsspannung angeschlossen ist. Der **Basisanschluss** (B) liegt am dazwischenliegenden p-dotierten Material. Soweit keine Spannung  $U_e$  am Eingang der Basis anliegt, blockiert der Übergang von Kollektor nach Basis, da die anliegende Spannung hier mit Pluspol am n-dotierten Material in Sperrrichtung anliegt. Die Spannung  $U_a$  beträgt die Versorgungsspannung.

Die p-dotierte Halbleiterschicht an der Basis ist so dünn gehalten, so dass bei Anlegen einer Spannung  $U_e$  an der Basis gegenüber dem Emitter, also in dessen Durchlassrichtung, ab der Durchlassspannung

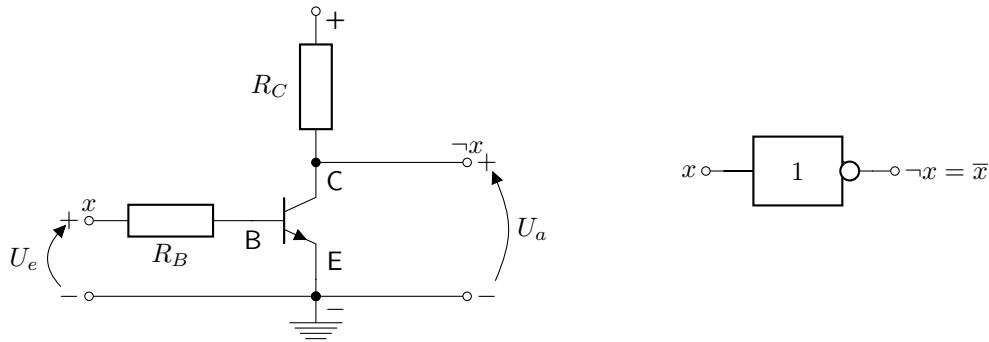


ABBILDUNG 4.2.1. Schaltung und Symbol eines NOT-Gatters

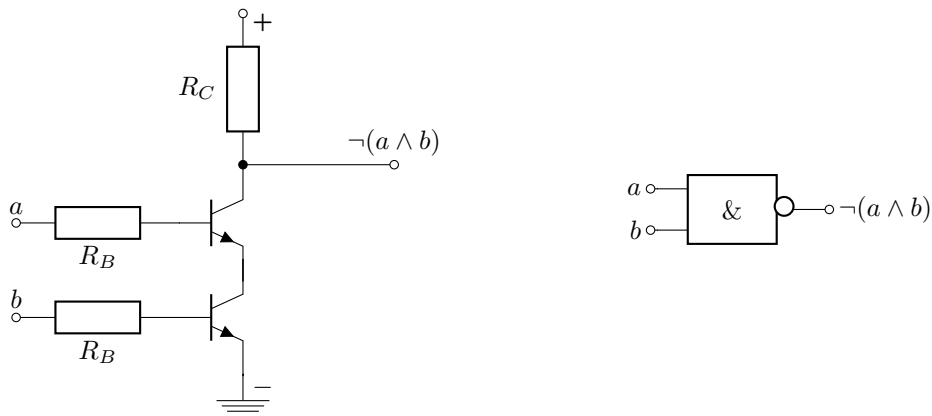


ABBILDUNG 4.2.2. Schaltung und Symbol eines NAND-Gatters

die Grenzschicht in der p-Schicht verschwindet, und damit auch in Richtung Kollektor leitend wird. Durch die geringe Dicke der p-dotierten Schicht an der Basis, ist auch der resultierende Strom  $I_B$  von Basis zu Emmitter ein Bruchteil der Stromes  $I_C$  vom Kollektor zum Emmitter. Das Verhältnis  $\beta$  in  $I_C = \beta \cdot I_B$  ist der **Stromverstärkungsfaktor** des Transistors und liegt typisch bei Werten zwischen 50 bis 200.

Liegt also an  $U_e$  eine hinreichend hohe Spannung an, so wird der Transistor von Kollektor nach Emmitter leitend, und die Spannung an  $U_a$  verschwindet. Versteht man nun die Spannung  $U_e$  als Eingang und die Spannung  $U_a$  als Ausgang, so invertiert die Schaltung die Eingangsschaltung. Dieses Gatter wird daher als **NOT-Gatter** bezeichnet: Eine angelegte Spannung am Eingang wird als  $x = 1$  gewertet und wird am Ausgang auf  $\neg x = 0$ , also keiner Spannung, abgebildet und umgekehrt. Die Schaltfunktion des NOT-Gatters ist also  $\text{NOT } x = \neg x$ .

In Abbildung 4.2.2 sind zwei Transistoren in Reihe geschaltet, die so ein **NAND-Gatter** für „Nicht-Und“ ergeben. Das NAND-Gatter der Variablen  $a$  und  $b$  hat also die Schaltfunktion  $a \text{ NAND } b = \neg(a \wedge b) = \overline{a \wedge b}$ . Die Abbildung 4.2.3 zeigt die wichtigsten **Logikgatter** mit deren Schaltungssymbolen und Schaltfunktionen. Mit diesen Gattern werden alle logischen Ausdrücke in Schaltkreisen umgesetzt werden, und Schaltkreise können mit Hilfe der Aussagenlogik beschrieben werden.

Die Abbildung 4.2.4 zeigt die Umsetzung des Ausgangsterms aus Beispiel 4.9 mit Logikgattern. Hier müssen die Leitungen zu den Logikgattern mit berücksichtigt werden, die in Schaltwerken einfach nur durch die Bezeichnungen an den Schaltern definiert wurden. Dadurch werden die Darstellungen schnell deutlich komplizierter, können aber so direkt in reale Schaltungen umgesetzt werden.


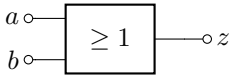
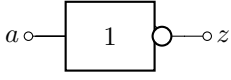

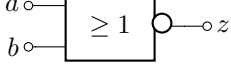
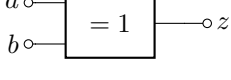
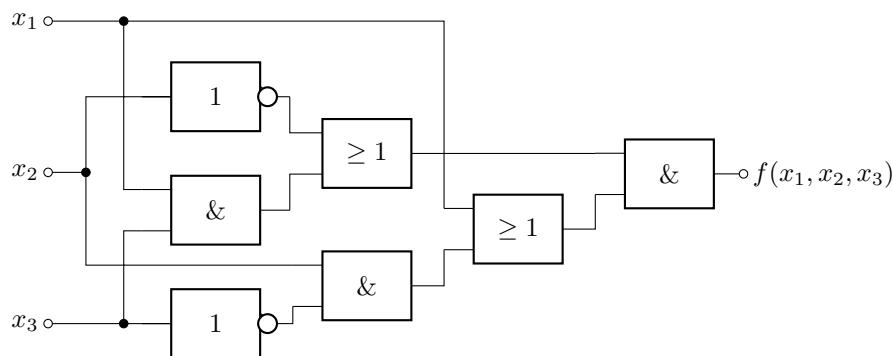
Name	Symbol	Schaltfunktion
AND		$z = a \wedge b$
OR		$z = a \vee b$
NOT		$z = \neg a = \bar{a}$
NAND		$z = \overline{a \wedge b}$
NOR		$z = \overline{a \vee b}$
XOR		$z = (a \wedge \bar{b}) \vee (\bar{a} \wedge b)$

ABBILDUNG 4.2.3. Logikgatter nach IEC 60617-12 und deren Schaltfunktionen

ABBILDUNG 4.2.4.  $f(x_1, x_2, x_3) = (x_1 \vee (\bar{x}_3 \wedge x_2)) \wedge (\bar{x}_2 \vee (x_3 \wedge x_1))$  mit Logikgattern

### 4.3. KV-Diagramme

Während boolesche Ausdrücke und Wahrheitstabeln mit Hilfe von Normalformen in bis auf Kommutativität der Terme eindeutige boolesche Darstellungen überführt werden können, so ist in Beispielen 4.9 und 4.11 erkennbar, dass die Normalformen nur selten eine sinnvolle Form zur Umsetzung oder Auswertung sind. Für die systematische Vereinfachung von booleschen Ausdrücken gibt es die im Folgenden vorgestellten **Karnaugh-Veitch-Diagramme**, kurz **KV-Diagramme** für bis zu vier Boolesche Variablen, und den **Quine-McCluskey-Algorithmus** für mehr Variablen.

In KV-Diagrammen werden bis zu zwei Variablen je in Spalten und Zeilen so aufgeteilt, dass sich von einer Zeile zur nächsten oder einer Spalte zur nächsten immer nur höchstens eine Variable in ihre Negation ändert. Dabei wird das Diagramm wiederholt vorgestellt, als wäre es auf einem Torus abgebildet: Damit schließt sich die Spalte ganz links an die Spalte ganz rechts an, die Zeile unten an die Zeile oben und umgekehrt.

Das Diagramm wird dann mit Werten einer Wahrheitstafel, oder für in der disjunktiven Normalform auftretenden Termen mit 1 und sonst 0 gefüllt. In diesem Diagramm werden nun eine möglichst kleine Anzahl zusammenhängender möglichst großer Blöcke der Größen  $1 \times 1$ ,  $1 \times 2$ ,  $1 \times 4$ ,  $2 \times 1$ ,  $2 \times 2$ ,  $2 \times 4$  oder  $4 \times 4$  mit gleicher Belegung gesucht, die auch über die Ränder hinweg gehen und sich überschneiden können. Je weniger Blöcke, um so weniger Terme werden auftreten, je größer die Blöcke, um so kürzer wird der jeweilige Term:

		$x_1 x_2$			
		00	01	11	10
$x_3 x_4$	00	1	0	0	1
	01	1	1	1	1
	11	1	1	1	1
	10	1	0	0	1

Bei der **Minterm-Methode** werden Blöcke mit 1 gesammelt und jeder Block nach den erforderlichen Termen untersucht: Hier ergibt dies für den Block in der Mitte, dass hier immer  $x_2 = 1$  und  $x_4 = 1$  gilt, und damit durch den Term  $x_2 \wedge x_4$  ausgedrückt werden kann. Der den Rand überschneidende Block wird durch  $x_2 = 0$  vollständig charakterisiert und wird durch  $\overline{x_2}$  ausgedrückt. Damit ist der minimale Ausdruck hier  $(x_2 \wedge x_4) \vee \overline{x_2}$ .

		$x_1 x_2$			
		00	01	11	10
$x_3 x_4$	00	1	0	1	0
	01	0	0	1	0
	11	1	0	1	1
	10	1	0	1	0

Bei der **Maxterm-Methode** werden Blöcke mit 0 gesammelt und jeder Block nach den erforderlichen Termen untersucht: Der lange Balken über 4 Zeilen wird durch  $x_1 = 0$  und  $x_2 = 1$  definiert und negiert durch  $x_1 \vee \overline{x_2}$  charakterisiert. Der Block rechts oben wird definiert durch  $x_3 = 0$ ,  $x_1 = 1$  und  $x_2 = 0$  und damit negiert durch  $\overline{x_1} \vee x_2 \vee x_3$  dargestellt. Der überschneidende Block hat  $x_2 = 0$ ,  $x_3 = 0$ ,  $x_4 = 1$  und entspricht so negiert  $x_2 \vee x_3 \vee \overline{x_4}$ . Der Einzelblock  $x_1 = 1$ ,  $x_2 = 0$ ,  $x_3 = 1$  und  $x_4 = 0$  wird damit zu  $\overline{x_1} \vee x_2 \vee \overline{x_3} \vee x_4$ . Insgesamt ergibt das Diagramm den Ausdruck

$$(x_1 \vee \overline{x_2}) \wedge (\overline{x_1} \vee x_2 \vee x_3) \wedge (x_2 \vee x_3 \vee \overline{x_4}) \wedge (\overline{x_1} \vee x_2 \vee \overline{x_3} \vee x_4).$$

BEISPIEL 4.12. Aus der disjunktiven Normalform

$$f(x_1, x_2, x_3) = (x_1 \wedge \overline{x_2} \wedge \overline{x_3}) \vee (x_1 \wedge \overline{x_2} \wedge x_3) \vee (x_1 \wedge x_2 \wedge x_3)$$

der Beispiele 4.9 und 4.11 resultieren die Belegungen

	$x_1$	$x_2$	$x_3$
$x_1 \wedge \overline{x_2} \wedge \overline{x_3} :$	1	0	0
$x_1 \wedge \overline{x_2} \wedge x_3 :$	1	0	1
$x_1 \wedge x_2 \wedge x_3 :$	1	1	1

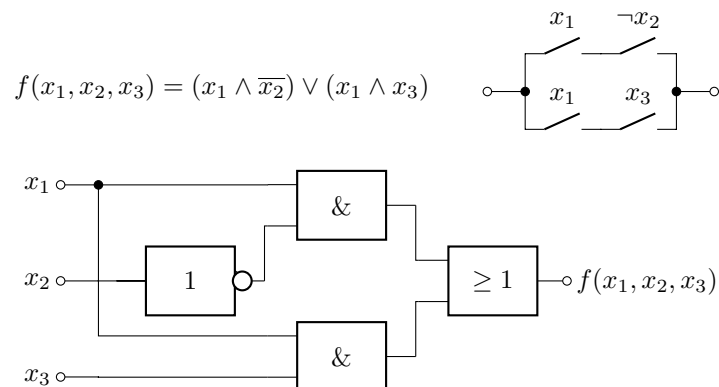
und damit ergibt sich das folgende KV-Diagramm:

		$x_1 x_2$			
		00	01	11	10
$x_3$	0	0	0	0	1
	1	0	0	1	1

Das Diagramm kann sinnvoll sowohl nach Minterm- und Maxterm-Methode aufgeteilt werden: Bei der Minterm-Methode werden möglichst wenige möglichst große Blöcke mit 1 gesucht:

		$x_1 x_2$			
		00	01	11	10
$x_3$	0	0	0	0	1
	1	0	0	1	1

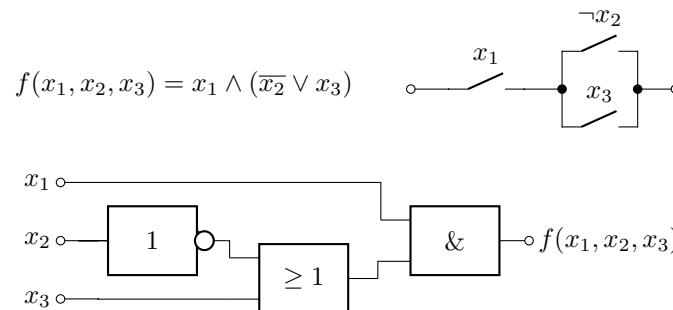
Hier ergibt sich aus dem Block  $x_1 = 1, x_2 = 0$  der Term  $x_1 \wedge \overline{x_2}$  und aus  $x_1 = 1, x_3 = 1$  der Term  $x_1 \wedge x_3$  und damit eine disjunktive Minimalform mit Schaltung und Logikgattern:



Bei der Maxterm-Methode werden möglichst wenige möglichst große Blöcke mit 0 gesucht:

		$x_1 x_2$			
		00	01	11	10
$x_3$	0	0	0	0	1
	1	0	0	1	1

Hier ergibt sich aus dem Block  $x_1 = 0$  der negierte Term  $x_1$  und aus  $x_2 = 1, x_3 = 0$  der negierte Term  $\overline{x_2} \vee x_3$  und damit eine konjunktive Minimalform mit zugehöriger Schaltung:



Beide Darstellungen sind deutliche Vereinfachungen gegenüber der früheren Darstellung oder dem Logikgatter aus Abbildung 4.2.3.

In vielen Anwendungen gibt es Einträge im KV-Diagramm, die beliebig gewählt werden können. Diese Einträge können opportun zu allen Blöcken bei Bedarf hinzugezählt werden:

		$x_1 x_2$			
		00	01	11	10
$x_3 x_4$	00	0	0	1	0
	01	1	-	-	-
	11	1	1	-	-
	10	0	0	-	0

		$x_1 x_2$			
		00	01	11	10
$x_3 x_4$	00	0	0	1	0
	01	1	-	-	-
	11	1	1	-	-
	10	0	0	-	0

$$f(x_1, x_2, x_3, x_4) = x_4 \vee (x_1 \wedge x_2)$$

$$f(x_1, x_2, x_3, x_4) = (x_1 \vee x_4) \wedge (\overline{x_1} \vee x_2)$$



### 4.4. Aufgaben

**AUFGABE 63.** Bestimmen Sie für die Boolesche Teileralgebra  $D_{70}$  die Werte  $2 \oplus 14$ ,  $\neg 14$  und  $35 \odot 10$ .

**AUFGABE 64.** Bestimmen Sie für die Boolesche Teileralgebra  $D_{42}$  die Werte  $6 \oplus 21$ ,  $\neg 14$  und  $6 \odot 42$ .

**AUFGABE 65.** Mit der Relation  $a \preceq b \Leftrightarrow a \odot b = a$  ergibt sich eine Teilordnung auf einer Booleschen Algebra. Erstellen Sie daraus ein Hassediagramm aller Elemente in  $D_{70}$ .

**AUFGABE 66.** Mit der Relation  $a \preceq b \Leftrightarrow a \odot b = a$  ergibt sich eine Teilordnung auf einer Booleschen Algebra. Erstellen Sie daraus ein Hassediagramm aller Elemente in der Booleschen Mengenalgebra zu  $\mathcal{P}(\{r, g, b\})$ .

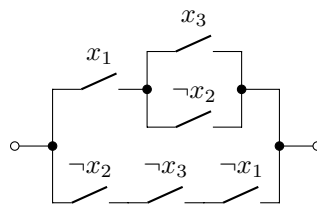
**AUFGABE 67.** Zeigen Sie, dass es in einer Booleschen Algebra  $B$  nur ein Element  $e \in B$  gibt, so dass für alle  $x \in B$  gilt:  $x \oplus e = x$ .

**AUFGABE 68.** Zeigen Sie, dass es in einer Booleschen Algebra  $B$  für jedes Element  $x \in B$  die Gleichung  $x \odot x = x$  gilt.

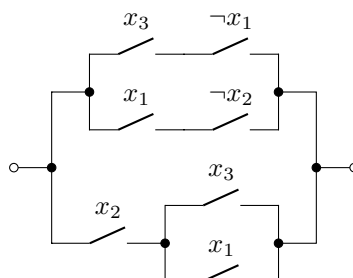
**AUFGABE 69.** Erstellen Sie eine Schaltung, die aus dezimal einstelligen 4-Bit Binärzahlen die einstelligen Primzahlen 2, 3, 5, 7 signalisiert.

**AUFGABE 70.** Erstellen Sie eine Schaltung, die einen Wiederholungscode-Decoder mit Korrektur aus Beispiel 3.38 realisiert.

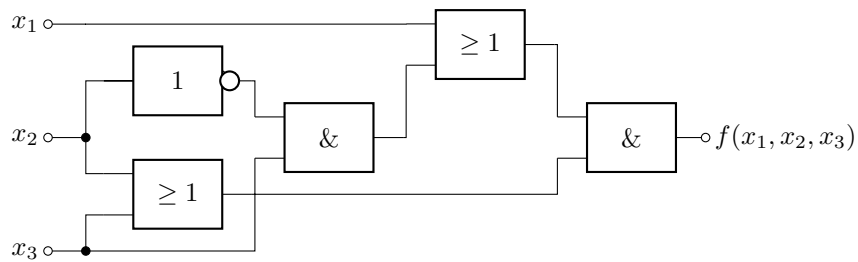
**AUFGABE 71.** Formulieren Sie den zugehörigen booleschen Ausdruck zum gegebenen Schaltungsdiagramm, bestimmen Sie die disjunktiven und konjunktiven Normalformen. Können Sie mit Hilfe eines KV-Diagramms eine vereinfachte Schaltung ableiten?



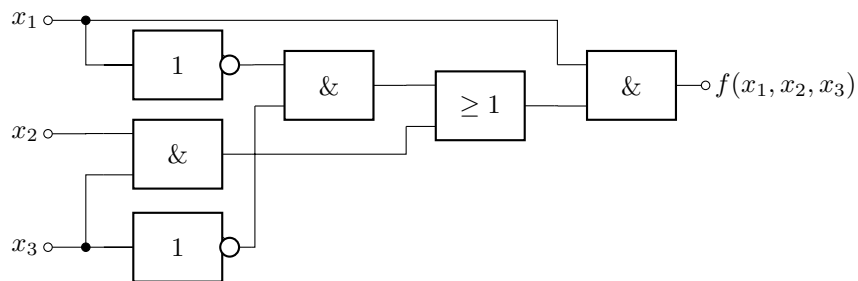
**AUFGABE 72.** Formulieren Sie den zugehörigen booleschen Ausdruck zum gegebenen Schaltungsdiagramm, bestimmen Sie die disjunktiven und konjunktiven Normalformen. Können Sie mit Hilfe eines KV-Diagramms eine vereinfachte Schaltung ableiten?



**AUFGABE 73.** Formulieren Sie die folgende logische Gatterschaltung als booleschen Ausdruck und als Schaltungsdiagramm. Ermitteln Sie mit einem KV-Diagramm eine Minimalform und stellen Sie diese als Schaltung und mit Logikgattern dar:



**AUFGABE 74.** Formulieren Sie die folgende logische Gatterschaltung als booleschen Ausdruck und als Schaltungsdiagramm. Ermitteln Sie mit einem KV-Diagramm eine Minimalform und stellen Sie diese als Schaltung und mit Logikgattern dar:



## Literaturverzeichnis

- [1] ARENS, T., F. HETTLICH, C. KARPFINGER, U. KOCKELKORN, K. LICHTENEGGER und H. STACHEL: *Arbeitsbuch Mathematik: Aufgaben, Hinweise, Lösungen und Lösungswege*. Springer Berlin Heidelberg, 2015.
- [2] ARENS, T., F. HETTLICH, C. KARPFINGER, U. KOCKELKORN, K. LICHTENEGGER und H. STACHEL: *Mathematik*. Springer Berlin Heidelberg, 2015.
- [3] ARENS, T., F. HETTLICH, C. KARPFINGER, U. KOCKELKORN, K. LICHTENEGGER und H. STACHEL: *Ergänzungen und Vertiefungen zu Arens et al., Mathematik*. Springer Berlin Heidelberg, 2017.
- [4] BREITNER, JOACHIM: *Visual theorem proving with the Incredible Proof Machine*. In: *International Conference on Interactive Theorem Proving*, Seiten 123–139. Springer, 2016.
- [5] EBBINGHAUS, H.-D., FLUM, J. und T. WOLFGANG: *Einführung in die mathematische Logik*. Springer Spektrum, 2018.
- [6] GRIESER, DANIEL: *Mathematisches Problemlösen und Beweisen*. Springer, 2017.
- [7] HUTH, MICHAEL und MARK RYAN: *Logic in Computer Science: Modelling and reasoning about systems*. Cambridge university press, 2004.
- [8] MEINEL, CHRISTOPH und MARTIN MUNDHENK: *Mathematische Grundlagen der Informatik*. Springer, 2011.



# Index

8-Bit Computer, 34

## A

Abbildung, 37  
abelsche Gruppe, 43  
abgeschlossenes Intervall, 27  
Adsorption, 9  
Allquantor, 16, 17  
antisymmetrisch, 31  
Äquivalenz, 19  
Äquivalenzklasse, 32  
Äquivalenzrelation, 32  
Assoziativität, 9, 29, 43, 63  
Auslöschung, 22  
Aussage, 5

## B

Basis, 67  
Betrag einer komplexen Zahl, 28  
Beweis durch Gegenbeispiel, 21  
Beweis durch Widerspruch, 21  
bijektiv, 38  
Bild, 37  
Bild der Funktion, 38  
Binärcode, 51  
binäre Exponentiation, 55  
Bluetooth, 54  
Boolesche Algebra, 63  
boolesche Funktion, 64  
Boolesche Normalformen, 65  
boolesche Variable, 64  
boolescher Ausdruck, 65

## C

Codewörter, 51  
CRC, 53  
Cyclic Redundancy Check, 53

## D

Darstellungssatz, 64  
De Morgansche Regeln, 9, 29  
Definition, 5  
Definitionsmenge, 37  
Diffie-Hellman-Schlüsselaustausch, 56  
Digitaltechnik, 67

direkter Beweis, 20  
Disjunktion, 7, 13  
Disjunktive Normalform, 65  
diskreten Logarithmus, 55  
Distributivität, 9, 29, 63  
DNF, 65  
Doppelte Negation, 9

## E

echte Obermenge, 28  
echte Teilmenge, 28  
echte Untergruppe, 44  
einseitige Mengendifferenz, 27  
Element, 25  
Elementare Aussagen, 6  
Emitter, 67  
endliche Körper, 51  
Erweiterter Euklidischer Algorithmus, 50  
Erzeugendensystem, 44  
erzeugte Gruppe, 44  
Ethernet, 54  
Euklidischer Algorithmus, 49  
Eulersche Phi-Funktion, 58  
ex falso quodlibet, 14  
Existenzquantor, 16, 18

## F

Faktormenge, 34  
falsch, 5  
Falsche Aussage, 14  
Feld, 51  
Field, 51  
Funktion, 37

## G

ganze Zahlen, 26  
Gaußklammer, 49  
Gaußsche Zahlenebene, 28  
Generatorpolynom, 53  
gerichteter Graph, 36  
Gleichheit von Mengen, 28  
Gleitkommazahlen, 26, 34  
Grad des Polynoms, 47  
Graph, 32, 36  
Graph der Abbildung, 37

größte gemeinsame Teiler, 48  
größtes Element, 35  
Gruppe, 43

**H**

Halbordnung, 35  
Hammingcode, 53  
Hammingdistanz, 52  
Hasse-Diagramm, 36, 48  
homogene Koordinaten, 34

**I**

Idempotenz, 9, 29  
identische Funktion, 39  
Identität, 39, 63  
IEC 60617-12, 69  
IEEE 754, 26, 34  
Imaginärteil, 28  
Implikation, 8, 12  
Incredible Proof Machine, 10  
Indirekter Beweis, 15, 20  
injektiv, 38  
Inverse Elemente, 43  
inverse Funktion, 39  
irrationale Zahl, 27  
Isomorphie, 64

**J**

Junktor, 6

**K**

Kalkül, 10  
Kanalcodierung, 51  
Kanten, 32, 36  
Kardinalität, 29  
Karnaugh-Veitch-Diagramme, 69  
kartesische Produkt, 30  
kleinste gemeinsame Vielfache, 63  
kleinstes Element, 35  
KNF, 65  
Knoten, 32, 36  
Kollektor, 67  
kommutative Gruppe, 43  
kommutativer Ring, 46  
Kommutativität, 9, 29, 43, 63  
Komplement, 63  
komplexe Konjugation, 28  
komplexe Zahl, 28  
Konjunktion, 7, 11  
Konjunktive Normalform, 65  
Konklusion, 10  
Kontradiktion, 9  
Körper, 51  
KV-Diagramme, 69

**L**

leere Menge, 26

linear, 31, 53  
lineare Ordnung, 35  
Linearkombination, 50  
Logikgatter, 68  
Logische Äquivalenz, 8

**M**

Mächtigkeit, 29  
maximal, 35  
Maxterm-Methode, 70  
Menge, 25  
Mengenalgebra, 63  
Mengenkomplement, 63  
Mengensystem, 29  
minimal, 35  
Minterm-Methode, 70  
modulo, 34  
Modus Ponens, 12  
Modus Tollens, 14  
Monom, 47  
multiplikative Inverse, 51

**N**

NAND-Gatter, 68  
natürliche Zahlen, 25, 26  
natürliche Zahlen mit Null, 26  
natürliche Zahlen nach DIN, 26  
Negation, 7  
Nenner, 26  
Netzwerk, 32  
Neutrales Element, 43  
Neutralität, 9  
Normalisierung, 34  
NOT-Gatter, 68

**O**

Obermenge, 28  
Oder, 7  
offenes Intervall, 27  
Öffner, 66  
Operator, 43  
Ordnung, 45

**P**

Paar, 30  
Partition, 30  
Perfect Forward Secrecy, 56  
Permutationen, 38  
Polarkoordinaten, 28  
Polynom, 47  
Potenzmenge, 30, 63  
Prädikat, 16  
Präposition, 10  
Projektive Raum, 34

**Q**

Quantor, 16

Quasiordnung, 35

Quine-McCluskey-Algorithmus, 69

Quotientenmenge, 34

## R

rationale Zahl, 26

Realteil, 28

Redundanz, 51

Reed-Solomon-Code, 54

reelle Zahl, 27

reflexiv, 31

Register, 34

Relation, 31

relationale Datenbank, 31

Repräsentant, 34

Restklasse, 34

Restklassen-Körper, 51

Restklassen-Ring, 46

Ring, 46

Ring mit 1, 46

RSA-Verfahren, 58

## S

Satz von Euler-Fermat, 58

Schaltalgebra, 63

Schaltungsdiagramme, 67

Schaltwerke, 66

Schließer, 66

Schnitt, 26

SD-Card, 54

Square-and-Multiply, 55

Stromverstärkungsfaktor, 68

surjektiv, 38

symmetrisch, 31

symmetrische Mengendifferenz, 27

systematischer Code, 54

## T

Tautologie, 9

Teiler, 47

Teileralgebra, 63

Teilmenge, 28

Tertium Non Datur, 15

transitiv, 12, 31

Tripel, 30

Tupel, 30

## U

Und, 7

unendlich, 27

ungerichteter Graph, 32

Untergruppe, 44

Urbild, 37

USB, 54

## V

Vektor, 30

Vereinigung, 26

Verkettung, 39

Verknüpfung, 43

Vollordnung, 35

Vollständige Induktion, 21, 26

## W

wahr, 5

Wahrheitstafel, 6, 64

Wertemenge, 37

Wiederholungscode, 52

## Z

Zähler, 26

Zusammengesetzte Aussagen, 6

Zusammenhangskomponenten, 34

zyklisch, 52

zyklische Gruppe, 45

Zyklusschreibweise, 40