

Vorlesungsnotizen

# **Mathematik 1**

(für den Lehramtsstudiengang Sekundarstufe)

Wintersemester 2020/21

Thomas Schmidt

Stand: 6. April 2021



# Mathematik 1: Inhaltsverzeichnis

<b>Inhaltsverzeichnis</b>	<b>1</b>
<b>Vorwort zur Thematik</b>	<b>3</b>
<b>1 Grundlagen aus Logik und Mengenlehre</b>	<b>5</b>
1.1 Aussagenlogik und Wahrheitstafeln . . . . .	5
1.2 Prädikatenlogik und Quantoren . . . . .	8
1.3 Zum Aufbau der Mathematik und logischen Schlüssen . . . . .	10
1.4 Grundlagen der Mengenlehre . . . . .	11
<b>2 Abbildungen, Relationen, Zahlen</b>	<b>21</b>
2.1 Abbildungen . . . . .	21
2.2 Natürliche und ganze Zahlen, Induktion und Rekursion . . . . .	36
Einschub: Beweisstrategien . . . . .	46
2.3 Relationen . . . . .	49
2.3.1 Ordnungsrelationen . . . . .	54
2.3.2 Äquivalenzrelationen . . . . .	60
2.4 Rationale Zahlen . . . . .	67
2.5 Mächtigkeit von Mengen . . . . .	69
<b>3 Algebraische Grundstrukturen</b>	<b>75</b>
3.1 Verknüpfungen, Halbgruppen und Gruppen . . . . .	75
3.2 Ringe und Körper . . . . .	88
3.3 Homomorphismen, Unter- und Faktorstrukturen . . . . .	99
<b>4 Reelle und komplexe Zahlen</b>	<b>109</b>
4.1 Reelle Zahlen . . . . .	109
(Fortsetzung Kapitel 4 in Mathematik 2) . . . . .	
<b>Literaturverzeichnis</b>	<b>117</b>

**Warnung: Diese Notizen umfassen nicht den vollständigen Vorlesungsstoff!**  
Falls Sie Fehler (jeglicher Art) finden oder sonstige Hinweise haben, bitte ich Sie, mir dies entweder persönlich oder unter [thomas.schmidt@math.uni-hamburg.de](mailto:thomas.schmidt@math.uni-hamburg.de) mitzuteilen.



# Vorwort zur Thematik

Der **Vorlesungszyklus Mathematik 1 bis 4** für das Lehramt der Sekundarstufe deckt (vor allem) **Themen aus den Bereichen Analysis und lineare Algebra** ab. Diese Bereiche sind grundlegend für die Mathematik und werden auch im Studium des Kernfachs Mathematik als Erstes unterrichtet. Die lineare Algebra ist dabei eine allgemeine Lehre „linearer Strukturen“, zu der unter anderem der Umgang mit linearen Gleichungssystemen, linearen Abbildungen, Vektoren und Matrizen zählt und an die sich die sogenannte analytische Geometrie mit Punkten, Geraden und Ebenen im Raum andockt. Die Analysis ist die Lehre vom mathematischen Umgang mit dem Unendlichen, der letztlich immer mittels Grenzübergängen und Grenzwerten erfolgt. Zentrale Themen der Analysis sind reelle und komplexe Zahlen, Grenzwerte, Ableitungen und Integrale. In der **Vorlesung Mathematik 1** liegt der Schwerpunkt zunächst auf allgemeinen **Grundlagen der Mathematik**, die nicht unbedingt einem der genannten Bereiche zuzuordnen sind, und dann auf ersten **Themen der Analysis**.

Das **Ziel** der Vorlesungen Mathematik 1 bis 4 ist, eine **fachwissenschaftliche Einführung** in das mathematische Arbeiten mit präzise definierten Begriffen, Lehrsätzen und vollständigen Beweisen zu geben. Im Schulunterricht der Sekundarstufe relevante Themen werden dabei in größerer Ausführlichkeit behandelt. Daneben sollen ein deutlich über den Schulstoff hinausgehendes **mathematisches Hintergrundwissen**, die **Fähigkeit zur eigenständigen Einarbeitung** in mathematische Themen und Konzepte, ein gewisser **Überblick** über mathematische Gebiete sowie ein Gefühl für die **Mathematik als lebendige Wissenschaft** vermittelt werden.



# Kapitel 1

## Grundlagen aus Logik und Mengenlehre

In diesem initialen Kapitel geht es um Aspekte der mathematischen Logik, der mathematischen Arbeitsweise und der Mengenlehre, die als Grundlage der gesamten modernen Mathematik betrachtet werden und den streng mathematische Aufbau aller weiteren Theorie erst ermöglichen. Die Beschäftigung mit den Grundlagen ist dabei keineswegs einfach, da man auch sehr einleuchtende Sachverhalte weiter hinterfragen und begründen muss.

Hier werden wir sowohl die Logik als auch die Mengenlehre hauptsächlich von einem (mehr oder weniger) naiven Standpunkt betrachten, der für ein Mathematik-Studium und das wissenschaftliche Arbeiten in den allermeisten mathematischen Gebieten ausreicht. Es sind heutzutage auch fundiertere Zugänge zu Logik und Mengenlehre bekannt (sowie prinzipiell andere Herangehensweisen an die Grundlagen). Solche Aspekte können wir hier aber bestenfalls andeuten. Bevor man sie im Detail verstehen kann, braucht man erst einmal mehr Erfahrung mit dem mathematischen Denken und Arbeiten.

### 1.1 Aussagenlogik und Wahrheitstabeln

Grundlegend für (fast) alle Gebiete der modernen Mathematik ist der Umgang mit (Elementar-) **Aussagen**, die entweder als **wahr** (**w**) oder als **falsch** (**f**) zu betrachten sind und denen einer dieser beiden sogenannten Wahrheitswerte zugeordnet wird. Insbesondere bewegen sich mathematische Aussagen nicht in Grauzonen. Ein Satz wie „Die Zahl 10 ist groß.“ erfüllt also nicht den Anspruch einer mathematischen Aussage, denn ab wie groß man von „groß“ spricht wird nicht ersichtlich. (Wenn man „groß“ natürlich im Vorfeld festgelegt/definiert hat, dann ist es etwas anderes.) Dagegen sind „Die Zahl 10 ist größer als die Zahl 15.“ und „Die Zahl 10 ist mindestens so groß wie die Zahl 10.“ Beispiele für sinnvolle mathematische Aussagen, von denen die erste natürlich falsch, die zweite wahr ist. Dass eine **Aussage gilt**, ist eine alternative mathematische Sprechweise dafür, dass die Aussage wahr ist.

Aussagen können im Rahmen der **Aussagenlogik** durch **logische Grundoperationen** verneint und auf verschiedene Weisen zusammengesetzt werden. Formal notiert man verneinte und zusammengesetzte Aussagen mit Hilfe von **Junktoren** genannten logischen Symbolen, die vor oder zwischen die Aussage(n) geschrieben werden. Die fünf wichtigsten Grundoperationen und die Anwendung der zugehörigen Junktoren mit Platzhaltern  $A$  und  $B$  für Aussagen sind in folgender Tabelle zusammengefasst (*wobei die Operationen, Schreib- und Sprechweisen innerhalb*

eines Feldes Alternativen gleicher Bedeutung sind):

Operation	Junktoren	Bedeutung, Sprechweisen
Verneinung Negation	$\neg A$	nicht $A$
logisches Und Konjunktion	$A \wedge B$	$A$ und $B$
logisches Oder Disjunktion	$A \vee B$	$A$ oder $B$
Folgerung	$A \implies B$	Aus $A$ folgt $B$ . $B$ folgt aus $A$ .
Implikation	$B \impliedby A$	$A$ impliziert $B$ . $B$ wird von $A$ impliziert.
Konditional	$A \rightarrow B$	Sei $A$ (gegeben). Dann (gilt) $B$ .
Subjunktion	$B \leftarrow A$	$A$ (ist) hinreichend für $B$ . $B$ (ist) notwendig für $A$ .
Äquivalenz	$A \iff B$	$A$ (ist) äquivalent (zu) $B$ $A$ gleichbedeutend mit $B$
Bikonditional	$A \leftrightarrow B$	$A$ (gilt) genau dann, wenn $B$ (gilt). $A$ ist notwendig und hinreichend für $B$ .

Die Wahrheitswerte der verneinten und zusammengesetzten Aussagen ergeben sich dabei einzig und allein aus den Wahrheitswerten von  $A$  und  $B$  und werden durch folgende (in Anbetracht der Sprechweisen naheliegende) **Wahrheitstabellen** festgelegt:

$A$	$\neg A$	$A$	$B$	$A \wedge B$	$A \vee B$	$A \implies B$	$A \iff B$
w	f	w	w	w	w	w	w
w	f	w	f	f	w	f	f
f	w	f	w	f	w	w	f
f	w	f	f	f	f	w	w

Hervorzuheben ist hierbei insbesondere, dass das logische Oder nicht exklusiv ist, das heißt,  $A \vee B$  ist *auch* dann wahr, wenn  $A, B$  beide wahr sind (zusätzlich zu den „echten Oder-Fällen“ natürlich, in denen eine der Aussagen  $A, B$  wahr, eine falsch ist).

Daneben mag zunächst überraschen, dass die Implikation  $A \implies B$  bei falscher Prämisse  $A$  (dritte/vierte Zeile Tabellenkörper) als wahr festgelegt wird, also „aus Falschem alles folgt“. Beispiele sind etwa „3 ist ungerade  $\implies 2 \cdot 4 = 8$ “ (wahr), „3 ist ungerade  $\implies 2 \cdot 4 = 7$ “ (falsch), „3 ist gerade  $\implies 2 \cdot 4 = 8$ “ (wahr) und „3 ist gerade  $\implies 2 \cdot 4 = 7$ “ (wahr). Um dies zu verstehen, kann man auch an das Sprichwort „Wer  $A$  sagt, der muss auch  $B$  sagen.“ denken, das als Implikation aus den Teilaussagen „ $A$  wird gesagt.“ und „ $B$  wird gesagt.“ zusammengesetzt ist (wobei die zeitliche Reihenfolge, in der etwas gesagt wird, hier keine Rolle spielen soll). Wenn man  $A$  und  $B$  sagt (erste Zeile), ist dies im Sinn des Sprichworts „richtig“. Wenn man  $A$  nicht sagt, ergibt sich keine Verpflichtung. Man kann dann  $B$  sagen (dritte Zeile) oder auch nicht (vierte Zeile); beides wäre „richtig“. Die einzige Möglichkeit, gemäß Sprichwort „falsch“ zu handeln, ist in der Tat die, dass zwar  $A$ , aber nicht  $B$  gesagt wird (zweite Zeile).

Natürlich kann man mehrere verschiedene (oder auch gleiche) Junktoren kombinieren — wobei die Reihenfolge der Auswertung genau wie bei den Grundrechenarten im Allgemeinen durch Klammern anzuzeigen ist — und kann für jede logische Formel aus endlich vielen Aussagen und

endlich vielen Junktoren Wahrheitstabeln ableiten. Auf die weitere Ausführung von Beispielen wird hier verzichtet.

Es kommt vor, dass verschiedene logische Formeln in allen Fällen mit dem gleichen Wahrheitswert belegt sind. **Beispiele für gleichbelegte Formeln**, gebildet aus Aussagen  $A, B, C$ , sind die Kommutativ- und Assoziativgesetzte (wobei gb. für gleichbelegt steht):

$$\begin{array}{ll} A \wedge B \text{ gb. mit } B \wedge A, & A \vee B \text{ gb. mit } B \vee A, \\ (A \wedge B) \wedge C \text{ gb. mit } A \wedge (B \wedge C), & (A \vee B) \vee C \text{ gb. mit } A \vee (B \vee C). \end{array}$$

Dementsprechend kann man bei Formeln dieser Gestalt die Reihenfolge der Aussagen vertauschen und auf Klammerung verzichten. **Weitere Beispiele für gleichbelegte Formeln** sind:

$$\begin{array}{ll} (A \vee B) \wedge C \text{ gb. mit } (A \wedge C) \vee (B \wedge C), & (A \wedge B) \vee C \text{ gb. mit } (A \vee C) \wedge (B \vee C), \\ A \implies B \text{ gb. mit } (\neg A) \vee B, & A \iff B \text{ gb. mit } (A \wedge B) \vee (\neg(A \vee B)). \end{array}$$

Die beiden Regeln der oberen Zeile kann man sich dabei als eine Art „Distributivgesetze“ für  $\wedge$  und  $\vee$  merken. Mit der unteren Zeile können die Pfeil-Symbole  $\implies$  und  $\iff$  durch  $\neg$ ,  $\wedge$  und  $\vee$  ausgedrückt werden und erweisen sich im Prinzip als redundant. In der Tat ist die Pfeil-Notation aber sehr, sehr intuitiv und in der Praxis dennoch unverzichtbar.

Es kann sich beim Ausfüllen einer Wahrheitstafel auch herausstellen, dass eine logische Formel für alle möglichen Kombinationen von Wahrheitswerten der Einzelaussagen stets wahr ist. Solche Formeln heißen **Tautologien**. Dass eine Formel eine Tautologie ist, drückt man manchmal durch die (eigentlich nicht völlig korrekten) Sprechweisen aus, dass die Formel (generell) wahr ist oder (generell) gilt. Bekannte und naheliegende **Beispiele für Tautologien**, gebildet aus Aussagen  $A, B, C$ , sind:

$$\begin{array}{ll} (\neg(\neg A)) \iff A & \text{(Gesetz der doppelten Negation),} \\ A \vee (\neg A) & \text{(Satz vom ausgeschlossenen Dritten),} \\ (A \wedge B) \implies (A \vee C), & \\ \left. \begin{array}{l} (\neg(A \wedge B)) \iff ((\neg A) \vee (\neg B)) \\ (\neg(A \vee B)) \iff ((\neg A) \wedge (\neg B)) \\ (\neg(A \implies B)) \iff (A \wedge (\neg B)) \end{array} \right\} & \text{(De Morgansche Gesetze zur Nega-} \\ & \text{tion der Konjunktion und Disjunktion),} \\ & \text{(Negation der Implikation).} \end{array}$$

**Weitere Beispiele für Tautologien**, an die sich später diskutierte Schluß- und Beweistechniken anlehnen, sind:

$$\begin{array}{ll} (A \wedge (A \implies B)) \implies B & \text{(Modus ponens),} \\ ((A \implies B) \wedge (B \implies C)) \implies (A \implies C) & \text{(Transitivität der Implikation),} \\ (A \implies B) \iff ((\neg B) \implies (\neg A)) & \text{(Kontrapositions-Prinzip),} \\ (A \iff B) \iff ((A \implies B) \wedge (B \implies A)) & \text{(Charakterisierung der Äquivalenz} \\ & \text{durch „Hin“- und „Rück“-Implikation).} \end{array}$$

Die Tautologien der Form  $(\dots) \iff (\dots)$  bedeuten dabei gemäß der Wahrheitstafel für die Äquivalenz, dass die linke und die rechte Teilformel stets denselben Wahrheitswert haben, somit (logisch) gleichbelegt/gleichbedeutend/äquivalent sind und beliebig durch einander ausgetauscht werden können. Dies gilt natürlich genauso für die zuvor schon erwähnten Beispiele gleichbelegter Formeln, bei denen man einfach „gb. mit“ durch den Junktor  $\iff$  ersetzen kann und darf, um sie ebenfalls als Tautologien der gerade besprochenen Form zu schreiben.

## 1.2 Prädikatenlogik und Quantoren

In der mathematischen Praxis kommt man mit der Aussagenlogik allein nicht weit, sondern benötigt schnell die allgemeinere **Prädikatenlogik** oder **Quantorenlogik**. **Prädikate** sind dabei Aussagen mit freien Variablen. Ein Beispiel ist „ $x$  ist größer als die Zahl 15.“ mit einer freien Variable  $x$ . Freie Variablen sind Platzhalter für (noch) unbestimmte Objekte oder Zahlen, und solange diese nicht bestimmt sind, man etwa im Beispiel den Wert von  $x$  nicht kennt, solange kann man über wahr oder falsch nicht sinnvoll entscheiden. Somit kann und soll Prädikaten erst einmal kein Wahrheitswert zugeordnet werden. Erst wenn man für die freien Variablen sinnvoll konkrete Objekte oder Zahlen einsetzt, z.B. die Zahl 10 für  $x$ , erst dann ergeben sich wieder individuelle Aussagen, die als wahr oder falsch zu betrachten sind.

Man kann mit einem Prädikat allerdings auch auf andere Art Aussagen ohne freie Variablen bilden. Beispielsweise lässt sich mit dem Prädikat „ $x$  ist größer als die Zahl 15.“ einerseits die Aussage „Alle natürlichen Zahlen sind größer als die Zahl 15.“ bilden und andererseits die Aussage „Es gibt eine natürliche Zahl, die größer als die Zahl 15 ist.“. (Erstere ist natürlich falsch, letztere wahr; dies hier aber nur nebenbei!) Dies sind tatsächlich Beispiele für das Hinzufügen von **Quantoren**, den entscheidenden logischen Operatoren der Prädikatenlogik, die bei einem Prädikat  $P(x)$  mit einer freien Variable  $x$  die Variable „binden“ und zu einer Aussage ohne freie Variable führen. Die Kombination aus Prädikat und Quantor liefert wieder eine „einfache“ Aussage mit Wahrheitswert. In der Praxis gibt man in Kombination mit dem Quantor auch eine Grundmenge<sup>1</sup>  $M$  von Zahlen oder Objekten an, die man für die Variable  $x$  einzusetzen erlaubt, und man sagt dann, dass  $x$  in  $M$  „läuft“. Im eben betrachteten Beispiel war diese Grundmenge  $M$  die Menge der natürlichen Zahlen.

Zu Schreib- und Sprechweisen für die beiden maßgeblichen und im Beispiel schon betrachteten Quantoren halten wir fest:

Quantor	Schreibweisen	Bedeutung, Sprechweisen
All-Quantor	$\forall x \in M: P(x)$	Für alle/beliebiges $x$ aus $M$ gilt $P(x)$ .
	$\bigwedge_{x \in M} P(x)$	Sei $x$ aus $M$ (beliebig). Dann gilt $P(x)$ .
Existenz-Quantor	$\exists x \in M: P(x)$	Es gibt ein $x$ aus $M$ mit $P(x)$ .
	$\bigvee_{x \in M} P(x)$	Für ein $x$ aus $M$ gilt $P(x)$ .

Naheliegenderweise wird hierbei die Aussage  $\forall x \in M: P(x)$  als wahr betrachtet, wenn  $P(x)$  für jede Zahl/jedes Objekt aus der Grundmenge  $M$ , die/das an Stelle von  $x$  eingesetzt wird, wahr

<sup>1</sup>Tatsächlich werden hier Quantoren unter Verwendung von Mengen und im nächsten Abschnitt Mengen unter Verwendung von Quantoren erklärt. Damit dreht man sich genau genommen im Kreis. Eine konsistente Einführung der Begriffe erfordert eigentlich ein vorsichtigeres Vorgehen: Man würde dazu an dieser Stelle nur die „Mengenfreien“ Aussagen  $\forall x: P(x)$  und  $\exists x: P(x)$  einführen, wobei im Hintergrund ein sogenanntes Diskursuniversum von zulässigen Objekten steht, die für die Variable  $x$  eingesetzt werden können. Im nächsten Schritt könnte man dann axiomatisch Mengen und die Elementbeziehung  $\in$  einführen — unter Verwendung solcher Quantoren über das Diskursuniversum der Mengen. Schließlich würde man  $\forall x \in M: P(x)$  und  $\exists x \in M: P(x)$  als abkürzende Schreibweisen für  $\forall x: (x \in M \implies P(x))$  und  $\exists x: (x \in M \implies P(x))$  erklären. Sind diese Grundlagen einmal geklärt, so laufen alle fortan relevanten Quantoren aber tatsächlich über Grundmengen  $M$ . Zudem ist ein rigoroser Aufbau der Logik und Mengenlehre an dieser Stelle sowieso nicht in Reichweite, weshalb man sich über mehr als den oben diskutierten praktisch relevanten Fall mit Grundmenge  $M$  kaum Gedanken machen muss.

ist. In allen anderen Fällen gilt  $\forall x \in M: P(x)$  als falsch. Analog betrachtet man  $\exists x \in M: P(x)$  als wahr, wenn es eine Zahl/ein Objekt in der Grundmenge  $M$  gibt, deren/dessen Einsetzen zu einer wahren Aussage  $P(x)$  führt. In allen anderen Fällen gilt  $\exists x \in M: P(x)$  als falsch. Betont sei dabei, dass mit einer Zahl/einem Objekt/einem  $x$  jetzt und fortan immer *mindestens* eine Zahl/*mindestens* ein Objekt/*mindestens* ein  $x$  gemeint ist; diese Interpretation ist in der Mathematik allgemein üblich.

Die Symbole  $\forall$  (umgedrehtes A) und  $\exists$  (gespiegeltes E) erinnern dabei an die Namen der Quantoren. Daneben verwendet man auch die „vergrößerten“ Und- und Oder-Junktoren  $\wedge$  und  $\vee$ , denn in der Tat kann man sich den All-Quantor als ein „großes Und“ über alle Aussagen vorstellen, die aus  $P(x)$  durch Einsetzen von Zahlen/Objekten aus  $M$  entstehen. Analog entspricht der Existenz-Quantor einem „großen Oder“.

Gelegentlich wird auch die Notation  $\exists! x \in M: P(x)$  mit einem Existenz-und-Eindeutigkeits-Quantor  $\exists!$  verwendet, um auszudrücken, dass  $P(x)$  für genau ein Objekt (also für ein einziges, aber kein weiteres) aus  $M$  wahr ist.

Für die **Negation von Quantoren** gelten die folgenden einleuchtenden Gesetzmäßigkeiten („große“ Versionen der de Morganschen Gesetze aus Abschnitt 1.1)

$$\begin{aligned}(\neg(\forall x \in M: P(x))) &\iff (\exists x \in M: (\neg P(x))), \\(\neg(\exists x \in M: P(x))) &\iff (\forall x \in M: (\neg P(x))),\end{aligned}$$

die in einem ähnlichen Sinn wie die früheren Formeln der Aussagenlogik Tautologien sind. In Worten besagt die erste Regel, dass „ $P(x)$  gilt nicht für alle  $x$  aus  $M$ .“ gleichbedeutend mit „Für ein  $x$  aus  $M$  gilt  $P(x)$  nicht.“ ist. Die zweite Regel drückt aus, dass „Für kein  $x$  aus  $M$  gilt  $P(x)$ .“ gleichbedeutend mit „Für alle  $x$  aus  $M$  gilt  $P(x)$  nicht.“ ist.

Natürlich treten in der Mathematik auch **Prädikate mit mehreren freien Variablen** auf, wobei die Variablen dann durch mehrere Quantoren gebunden werden können. Beispielsweise kann man aus einem Prädikat  $P(x, y)$  mit zwei freien Variablen  $x$  und  $y$  und aus Quantoren über Grundmengen  $M$  und  $N$  unter anderem die Aussagen  $\forall x \in M: \forall y \in N: P(x, y)$  und  $\exists y \in N: \forall x \in M: P(x, y)$  bilden.

Es ist dabei wichtig zu wissen, dass zwei Quantoren gleichen Typs (also  $\forall$  mit  $\forall$  und  $\exists$  mit  $\exists$ ) in der Reihenfolge vertauscht werden dürfen, ohne dass sich die Bedeutung der Aussage ändert. Beispielsweise ist  $\forall x \in M: \forall y \in N: P(x, y)$  äquivalent zu  $\forall y \in N: \forall x \in M: P(x, y)$  und — in Vorgriff auf Notation des Abschnitts 1.4 — übrigens auch äquivalent zu  $\forall (x, y) \in M \times N: P(x, y)$ . Die Vertauschung eines All-Quantors mit einem Existenz-Quantor ist dagegen nicht (ohne Unterschied in der Bedeutung) möglich: Tatsächlich bedeutet  $\forall x \in M: \exists y \in N: P(x, y)$ , dass zu jedem  $x \in M$  ein von  $x$  abhängiges  $y \in N$  existiert, so dass  $P(x, y)$  gilt. Dagegen symbolisiert  $\exists y \in N: \forall x \in M: P(x, y)$  die Existenz eines  $y \in N$  (jetzt wirklich nur ein einziges  $y$ , das nicht von einem  $x$  abhängen darf), so dass für alle  $x \in M$  Gültigkeit von  $P(x, y)$  besteht. Man kann sich den Unterschied zwischen diesen beiden Aussagen klarmachen, indem man für  $P(x, y)$  das einfache Prädikat „ $y$  ist größer als  $x$ “ einsetzt (und als Mengen  $M$  und  $N$  die Menge der natürlichen Zahlen): Die Aussage  $\forall x \in M: \exists y \in N: P(x, y)$  bedeutet dann „Für alle natürlichen Zahlen  $x$  gibt es eine natürliche Zahl  $y$ , die größer ist als die zuerst gegebene Zahl  $x$ .“ und ist richtig. Die Aussage  $\exists y \in N: \forall x \in M: P(x, y)$  dagegen bedeutet „Es gibt eine natürliche Zahl  $y$ , die größer ist als alle natürlichen Zahlen  $x$ .“ und ist falsch. (Dass sich wie in diesem prägnanten Beispiel unterschiedliche Wahrheitswerte ergeben, ist aber nur *eine* Möglichkeit. Für andere Prädikate  $P(x, y)$  kommt es auch vor, dass die betrachteten Aussagen den gleichen Wahrheitswert haben.)

Wie sich die Negationsregeln auf Formeln mit mehreren Quantoren auswirken, kann man

schließlich anhand des Beispiels (Formel ist Tautologie)

$$(\neg(\forall x \in M: \exists y \in N: P(x, y))) \iff (\exists x \in M: \forall y \in N: (\neg P(x, y)))$$

verstehen: Beim Hereinziehen der Negation wird jeder der Quantoren „umgemodelt“.

### 1.3 Zum Aufbau der Mathematik und logischen Schlüssen

Der **Grundanspruch der Mathematik als Wissenschaft** ist der, nur von einem begrenzten System von Grundannahmen, sogenannten **Axiomen**, auszugehen und alle Aussagen und Lehrsätze der Theorie durch lückenlose Argumentation mittels **logischer Schlüsse** aus den Axiomen abzuleiten. Die für die Herleitung einer Aussage benötigte Argumentation nennt man einen **Beweis** und spricht davon, die Aussage zu **zeigen**, zu **beweisen**, nachzuweisen oder zu verifizieren.

Hierzu können

- **Definitionen** (allgemein vereinbarte Abkürzungen oder Festlegungen)

getroffen und bereits bewiesene Aussagen verwendet werden. Für Gleichheiten beziehungsweise Äquivalenzen, die per Definition festgelegt werden, verwendet man dabei die Symbole  $:=$ ,  $=:$  beziehungsweise  $:\iff$ ,  $\iff$ :, wobei der Doppelpunkt auf der Seite der neu eingeführten Bildung steht. Es kommt gelegentlich vor, dass bei einer Definition *nicht direkt* ersichtlich ist, warum ein eingeführtes Objekt in allen zulässigen Fällen sinnvoll erklärt oder von der richtigen Bauart ist. In solchen Situationen ist zusammen mit der Definition die sogenannte **Wohldefiniertheit** zu zeigen, das heißt, es ist im Zusammenhang mit der Definition auch die Sinnhaftigkeit des eingeführten Objekts zu beweisen.

Einmal bewiesene Aussagen bezeichnet man, je nach Bedeutung (deren Einschätzung etwas subjektiv sein mag), als

- **Sätze** (wesentliche Erkenntnisse),
- **Hauptsätze/Theoreme** (Sätze von besonders weitreichender Bedeutung),
- **Lemmata/Hilfssätze** (kleinere/größere Hilfsresultate von eher spezieller Natur),
- **Propositionen** (Hilfsresultate von etwas allgemeinerem Nutzen),
- **Korollare** (vergleichsweise direkte Folgerungen aus anderen Resultaten).

Das wohl wichtigste **Grundprinzip des Beweisens/logischen Schließens** (das sich an den Modus ponens aus Abschnitt 1.1 anlehnt) besteht darin, bei zwei gegebenen Aussagen  $A$  und  $B$  aus der Wahrheit von einerseits  $A$  und andererseits  $A \implies B$  auf die Wahrheit von  $B$  zu schließen. Dies erklärt zu einem gewissen Grad auch die Notation  $A \implies B$  mit dem Pfeilsymbol: Gilt die Implikation, so kann man eben von  $A$  auf/zu  $B$  schließen. Nützlich ist solch ein logischer Schluss beispielsweise dann, wenn  $A \implies B$  gemäß einem (bereits bewiesenen) mathematischen Satz gilt und die Wahrheit von  $A$  deutlich leichter zu prüfen ist als die von  $B$ .

Als konkretes Beispiel könnte der Satz die (vermutlich) aus der Schule bekannte Regel zur Teilbarkeit durch 3 sein, die man in der Form

$$\forall x \in \mathbb{N}: ((3 \text{ teilt die Quersumme von } x) \iff (3 \text{ teilt } x))$$

mit der Menge  $\mathbb{N}$  der natürlichen Zahlen schreiben kann und die ein generell anwendbares, **notwendiges und hinreichendes Kriterium** für Teilbarkeit durch 3 darstellt. Möchte man

hiermit 873 auf Teilbarkeit durch 3 prüfen, so lässt sich dies logisch wie folgt aufdröseln: Zunächst setzt man 873 für  $x$  ein und erhält nach Berechnung der Quersumme 18 von 873, dass „(3 teilt 18)  $\iff$  (3 teilt 873)“ gilt. Somit sind die Implikationen „(3 teilt 18)  $\implies$  (3 teilt 873)“ und „(3 teilt 18 nicht)  $\implies$  (3 teilt 873 nicht)“ beide wahr (vergleiche mit Abschnitt 1.1). Nun folgt der eigentliche logische Schluss im obigen Sinn: Da „3 teilt 18“ wahr ist (kleines Einmaleins) und die erste der beiden genannten Implikationen wahr ist, lässt sich schließen, dass „3 teilt 873“ wahr ist. Damit ist die Teilbarkeitsfrage in diesem Fall geklärt. Stellt man für eine andere Zahl anstelle von 873 fest, dass 3 die Quersumme nicht teilt, so läuft der Schluss natürlich analog, dann aber über die zweite Implikation, die das „nicht“ enthält.

Bei zukünftigen Schlüssen und Beweisen werden wir viel weniger ins Detail gehen und den begrifflichen und formalen Aufwand dadurch deutlich verringern. Nichtsdestotrotz kann es immer mal wieder nützen, den gerade am Beispiel erläuterten Ablauf eines typischen logischen Schlusses zu durchdringen und im Hinterkopf zu behalten.

## 1.4 Grundlagen der Mengenlehre

In diesem Abschnitt werden grundlegende Definitionen und Notationen der Mengenlehre eingeführt. Wie schon zu Kapitelanfang angedeutet, beschränken wir uns dabei größtenteils auf eine Betrachtung vom Standpunkt der **naiven Mengenlehre**. Weiterführendes zur axiomatischen Fundierung der Mengenlehre und zu Gründen, warum es einer solchen bedarf, wird am Ende dieses Abschnitts kurz und im Kleingedruckten angerissen.

Grundlegend für die Mengenlehre ist in jedem Fall die Vorstellung, dass **eine Menge unterscheidbare mathematische Objekte als Elemente enthält**, wobei die **Elementbeziehung** durch das Symbol  $\in$  zum Ausdruck gebracht wird. Diese Grundvorstellung, die nicht weiter formalisiert werden kann, gilt es zu akzeptieren. Die folgende Definition verbindet diese Vorstellung mit Grundnotationen und der Festlegung, dass die Gleichheit von Mengen (nur) an ihren Elementen hängt und somit Mengen durch ihre Elemente vollständig charakterisiert sind:

**Definitionen (Mengen, Mengen-Gleichheit, Mengen-Inklusion).** *Als eine Menge  $M$  betrachtet man jede „Ansammlung“ (endlich oder unendlich vieler) „wohlunterscheidbarer mathematischer Objekte“ und erklärt die Aussage  $x \in M$  (lies:  $x$  Element (von)  $M$ ) für wahr, wenn das Objekt  $x$  in  $M$  enthalten ist. Darauf aufbauend definiert man für Mengen  $M$  und  $N$ :*

- Die **Mengen-Inklusion**  $M \subset N$  (lies:  $M$  **Teilmenge** von  $N$ ; oder:  $M$  enthalten in  $N$ ) beziehungsweise äquivalent  $N \supset M$  (lies:  $N$  **Obermenge** von  $M$ ; oder:  $N$  enthält  $M$ ) bedeutet, dass jedes Element von  $M$  auch Element von  $N$  ist, also  $\forall x \in M: x \in N$  gilt.
- Die **Mengen-Gleichheit**  $M = N$  bedeutet, dass  $M \subset N$  und  $N \subset M$  gelten, also  $M$  und  $N$  dieselben Elemente enthalten.
- Die **echte oder strikte Mengen-Inklusion**  $M \subsetneq N$  beziehungsweise äquivalent  $N \supsetneq M$  bedeutet, dass  $M \subset N$ , aber nicht  $M = N$  gilt.

Für die logischen Negationen von  $x \in M$ ,  $M \subset N$ ,  $N \supset M$ ,  $M = N$  schreibt man naheliegenderweise  $x \notin M$ ,  $M \not\subset N$ ,  $N \not\supset M$ ,  $M \neq N$ .

Bei der Mengen-Inklusion ist auch Gleichheit erlaubt, es gilt also  $M \subset M$  (was natürlich auch als  $M \supset M$  geschrieben werden kann) für jede Menge  $M$ . Analog zu den Ungleichheitszeichen  $\leq$  und  $\geq$  bei Zahlen werden deshalb in mancher Literatur die alternativen Symbole  $\subseteq$ ,  $\supseteq$ ,  $\subsetneq$ ,  $\supsetneq$  für

die Mengen-Inklusion verwendet. Für die strikte Mengen-Inklusion sind auch  $\subsetneq$ ,  $\supsetneq$  gebräuchlich — und seltener auch nur  $\subset$ ,  $\supset$ . In dieser Vorlesung halten wir uns aber an die etwas anderen Konventionen der obigen Definition.

Insbesondere ist es nach der Definition sinnlos zu fragen, ob eine Menge dasselbe Objekt (beispielsweise dieselbe Zahl) mehrfach enthält, denn das Konzept der Menge sieht nur vor, dass ein Objekt entweder als Element enthalten ist oder eben nicht. Ein Objekt ist in einer Menge nicht „zweimal“ oder „dreimal“ enthalten, jedenfalls nicht in dem Sinn, dass es sich um eine andere Menge handeln würde als bei nur „einmaligem“ Enthaltensein.

Die **Veranschaulichung von Mengen** und Mengen-Inklusionen kann man *in geeigneten Fällen* mit Bereichen oder Umrissen in der Zeichenebene angehen: Besonders in Fällen mit endlich vielen Elementen ist es üblich, die **Elemente in einem Bereich/Umriss von schematischer Bedeutung** einzutragen oder zumindest anzudeuten. Eine *zweite Darstellungsweise*, die besonders im geometrischen Kontext nutzt, mutet zunächst ähnlich an, *unterscheidet sich* aber doch *deutlich*: Bei dieser betrachtet man alle **durch den Bereich/Umriss umschlossenen Koordinatenpunkte als Elemente** der veranschaulichten Menge. Hierbei handelt es sich also um Mengen mit unendlich vielen, nicht explizit angedeuteten Elementen, und es kommt auf die genaue Form des Bereichs/Umrisses dann entscheidend an. Beispiele zur Darstellung der Mengen-Inklusion auf beide Weisen (bei der ersten einmal mit konkreten Elementen, einmal mit angedeuteten) zeigt Abbildung 1.

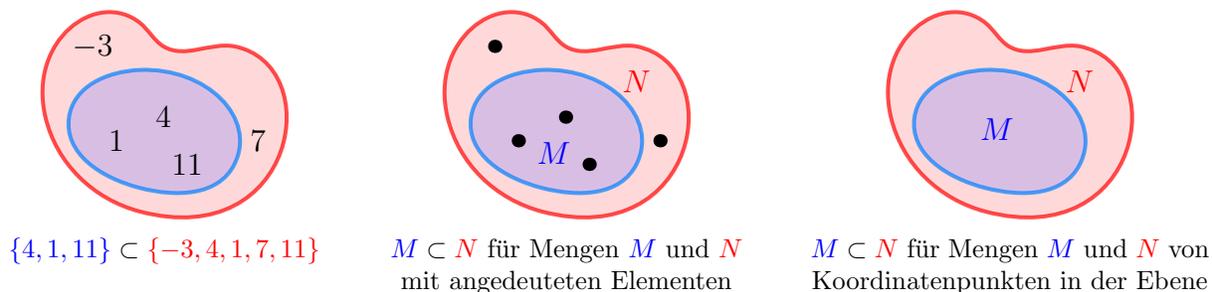


Abb. 1: Graphische Darstellungen der Mengen-Inklusion

Bei Darstellungen mit expliziten/angedeuteten Elementen sind Bereiche ohne Elemente belanglos. Ragt also der blaue Bereich wie in den ersten beiden Bildern der Abbildung 2 aus dem roten heraus, ohne dass dort ein Element steht, so gilt im Prinzip dieselbe Mengen-Inklusion, die damit aber irritierend und weniger günstig als in Abbildung 1 wiedergegeben ist. Stellt man dagegen wie im dritten Bild der Abbildung 2 Mengen von Koordinatenpunkten dar, so verhindern die Punkte (und damit Elemente) im herausragenden Bereich offensichtlich die Inklusion.

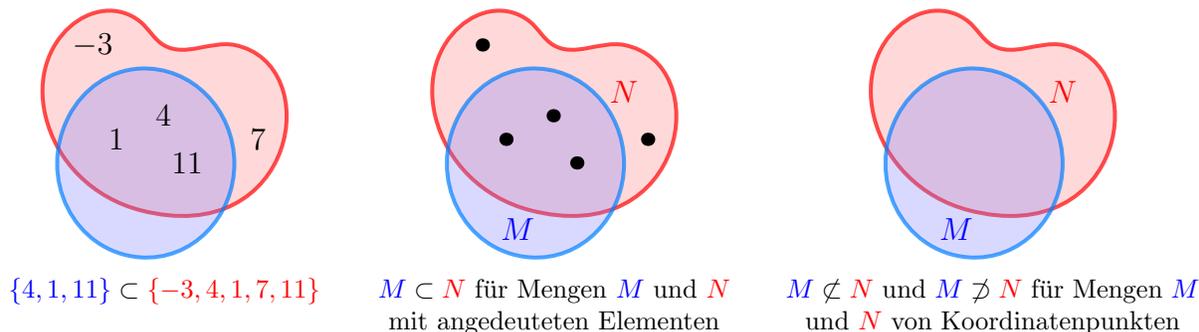


Abb. 2: Unterschiede in der Mengen-Darstellung

Um Mengen konkret (durch Angabe ihrer Elemente) zu beschreiben, listet man die Elemente wie folgt zwischen geschweiften Klammern auf:

**Notationen** (zur Angabe von Mengen durch Angabe der Elemente). *Man schreibt ...*

- $\emptyset$  für die Menge, die kein Element enthält, die sogenannte **leere Menge**,
- $\{x\}$  für die Menge, die das Objekt  $x$  als einziges Element enthält,
- $\{x, y\}$  für die Menge, die genau die zwei Objekte  $x$  und  $y$  als Elemente enthält,
- allgemeiner  $\{x_1, x_2, x_3, \dots, x_{n-1}, x_n\}$  mit irgendeiner natürlichen Zahl  $n$  für die Menge, die genau die  $n$  Objekte  $x_1, x_2, x_3, \dots, x_{n-1}, x_n$  als Elemente enthält,
- $\{x_1, x_2, x_3, \dots, \}$  für die Menge, die genau die unendlich vielen Objekte  $x_1, x_2, x_3, \dots$  als Elemente enthält,

Die Formulierung, dass „genau“ die genannten Elemente enthalten sind, bedeutet dabei, dass außer den Objekten in der (eventuell mit Pünktchen angedeuteten) Liste keine weiteren Objekte Element der Menge sind.

Wird hierbei dasselbe Objekt mehrfach gelistet, so hat dies gemäß den oben schon gemachten Bemerkungen keine andere Auswirkung als eine nur einfache Nennung. Im einfachsten Fall bedeutet dies beispielsweise  $\{x, x\} = \{x\}$ .

**Beispiele.** Beispiele für Mengen mit konkret angegebenen Elementen sind:

- $\{5, 13\}$  (Menge mit den zwei Elementen 5 und 13),
- $\{\text{rot, grün, blau}\}$  (Menge der RGB-Grundfarben; 3 Elemente),
- $\{+, -, \cdot, :\}$  (Menge der Grundrechenarten; 4 Elemente),
- $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F\}$  (Menge der Hexadezimal-Ziffern; 16 Elemente),
- $\{-7, -6, -5, \dots, 17, 18\}$  (Menge der ganzen Zahlen von  $-7$  bis  $18$ ; 26 Elemente),
- $\{1, 2, 3, 4, \dots\}$  (Menge der natürlichen Zahlen; unendlich viele Elemente),
- $\{\{1, 2, 3, 4, \dots\}, \{+, -, \cdot, :\}, \{5, 13\}, \{2, 5, -\}\}$   
(Mengensystem mit 4 Mengen als Elementen; dargestellt in Abbildung 3),

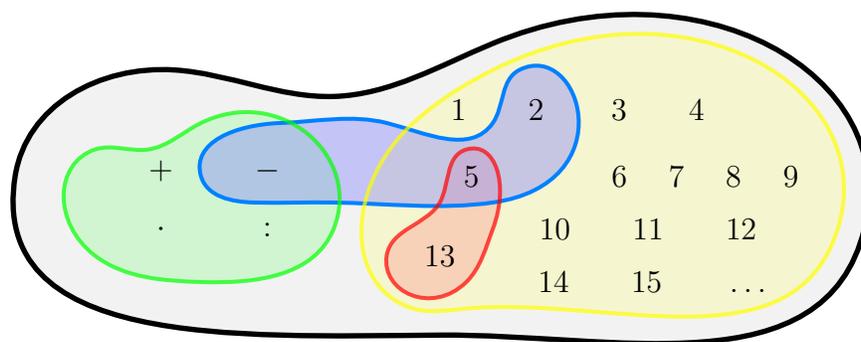


Abb. 3: Darstellung des Mengensystems  $\{\{1, 2, 3, 4, \dots\}, \{+, -, \cdot, :\}, \{5, 13\}, \{2, 5, -\}\}$

- $\{2, 3, 5, 7, 11, 13, 17, 19, 23, \dots\}$  (Menge der Primzahlen; unendlich viele Elemente),
- $\{ , ! , " , \# , \$ , \% , \& , ' , ( , ) , 0 , 1 , 2 , 3 , \dots , x , y , z , \{ , | , \} , \sim \}$   
(Menge der ASCII-Zeichen ohne Steuerzeichen; 95 Elemente).

Geht man nur vom Bild aus, so könnte es sich in Abbildung 3 aber genauso gut um das Mengensystem  $\{\{\{5, 13\}, 1, 2, 3, 4, \dots\}, \{+, -, \cdot, :\}, \{2, 5, -\}\}$  handeln. Insofern ist bei derartigen Bildern eine gewisse Vorsicht geboten. Auch Notationen mit Pünktchen können problematisch sein, wenn die eigentliche Bildungsregel nicht angegeben wird und nicht jedermann unbedingt (direkt) zur gleichen Interpretation kommt. Dennoch sind Pünktchen so praktisch, dass wir sie mit etwas Vorsicht weiterhin verwenden. Mit den im Folgenden definierten Grundoperationen ergeben sich aber automatisch auch andere Möglichkeiten zur Angabe von Mengen:

**Definitionen. Grundoperationen** mit Mengen  $M, N$  und einem Mengensystem  $\mathcal{S}$  (also einer Menge  $\mathcal{S}$  von Mengen) sind:

- (1) **Aussonderungen:** Ist  $P(x)$  ein Prädikat, für dessen Variable  $x$  die Elemente von  $M$  sinnvoll eingesetzt werden können, so enthält die Aussonderungsmenge  $\{x \in M \mid P(x)\}$  genau die Elemente  $x$  von  $M$ , für die  $P(x)$  gilt.
- (2) **Vereinigungen:** Die Vereinigungsmenge  $M \cup N$  von  $M$  und  $N$  enthält alle Elemente von  $M$  und alle Elemente von  $N$  und sonst keine weiteren Elemente. Für jedes  $x$  ist also  $x \in M \cup N$  gleichbedeutend mit  $(x \in M) \vee (x \in N)$  ist.

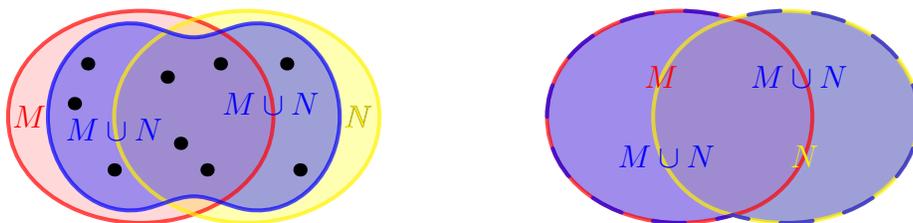


Abb. 4: Graphische Darstellungen der Vereinigungsmenge  $M \cup N$

Allgemeiner ist die Vereinigungsmenge  $\bigcup \mathcal{S} = \bigcup_{M \in \mathcal{S}} M = \bigcup \{M \mid M \in \mathcal{S}\}$  (drei gleichbedeutende Schreibweisen) die Menge, deren Elemente genau die Elemente der Elemente von  $\mathcal{S}$  sind. Für jedes  $x$  ist also  $x \in \bigcup_{M \in \mathcal{S}} M$  gleichbedeutend mit  $\exists M \in \mathcal{S} : x \in M$ .

- (3) **(Durch-)Schnitte:** Die Schnittmenge  $M \cap N$  von  $M$  und  $N$  ist die Menge, die alle gemeinsamen Elemente von  $M$  und  $N$  und sonst keine weiteren Elemente enthält. Für jedes  $x$  ist also  $x \in M \cap N$  gleichbedeutend mit  $(x \in M) \wedge (x \in N)$ .



Abb. 5: Graphische Darstellungen der Schnittmenge  $M \cap N$

Allgemeiner ist die Schnittmenge  $\bigcap \mathcal{S} = \bigcap_{M \in \mathcal{S}} M = \bigcap \{M \mid M \in \mathcal{S}\}$  die Menge, die genau die Elemente enthält, die in allen Elementen von  $\mathcal{S}$  enthalten sind. Für jedes  $x$  ist also  $x \in \bigcap_{M \in \mathcal{S}} M$  gleichbedeutend mit  $\forall M \in \mathcal{S}: x \in M$ .

- (4) **Mengen-Differenzen:** Die Differenzmenge  $M \setminus N := \{x \in M \mid x \notin N\}$  ist die Menge genau der Elemente von  $M$ , die keine Elemente von  $N$  sind.

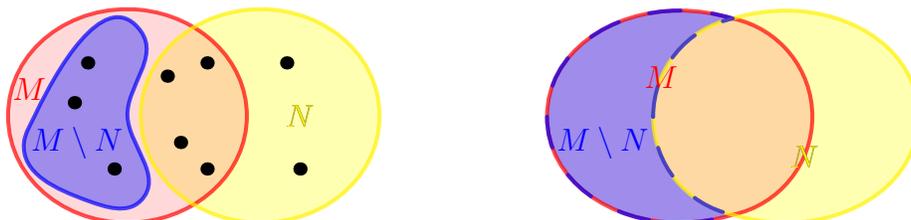


Abb. 6: Graphische Darstellungen der Differenzmenge  $M \setminus N$

Die symmetrische Differenzmenge ist  $M \Delta N := (M \setminus N) \cup (N \setminus M) = (M \cup N) \setminus (M \cap N)$ .

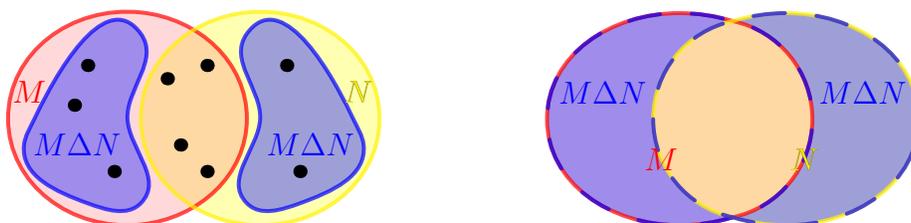


Abb. 7: Graphische Darstellungen der symmetrischen Differenzmenge  $M \Delta N$

Aus Regeln für die logischen Operatoren  $\vee$  und  $\wedge$  ergeben sich entsprechende Regeln für den Umgang mit den Mengen-Operatoren  $\cup$  und  $\cap$ . Für  $\cup$  beispielsweise gelten die Kommutativ- und Assoziativgesetze

$$M \cup N = N \cup M \quad \text{und} \quad (M_1 \cup M_2) \cup M_3 = M_1 \cup (M_2 \cup M_3) = \bigcup_{M \in \{M_1, M_2, M_3\}} M,$$

für  $\cap$  gelten diese analog, für das Zusammenspiel gelten die „Distributivgesetze“

$$(M_1 \cup M_2) \cap N = (M_1 \cap N) \cup (M_2 \cap N) \quad \text{und} \quad (M_1 \cap M_2) \cup N = (M_1 \cup N) \cap (M_2 \cup N).$$

Insbesondere kann man beim Zusammentreffen von ausschließlich Vereinigungen oder ausschließlich Schnitten (aber nicht beim Zusammenspiel der beiden) auf Klammern verzichten und gebräuchliche Schreibweisen wie

$$\bigcup_{i=m}^n M_i := M_m \cup M_{m+1} \cup \dots \cup M_n = \bigcup_{M \in \{M_m, M_{m+1}, \dots, M_n\}} M,$$

$$\bigcap_{i=m}^n M_i := M_m \cap M_{m+1} \cap \dots \cap M_n = \bigcap_{M \in \{M_m, M_{m+1}, \dots, M_n\}} M$$

für beliebige ganze Zahlen  $m, n$  mit  $m \leq n$  erklären (wenn nötig ergänzt um die sinnvolle Konvention  $\bigcup_{i=m}^n M_i := \emptyset$  im Fall  $m > n$ ). Ist allgemeiner für jedes Element  $i$  einer Menge  $I$ , genannt Indexmenge, eine Menge  $M_i$  gegeben<sup>2</sup> und ist  $\mathcal{S}$  ein/das Mengensystem, das als Elemente genau all diese  $M_i$  enthält, so verwenden wir

$$\bigcup_{i \in I} M_i := \bigcup_{M \in \mathcal{S}} M \quad \text{und} \quad \bigcap_{i \in I} M_i := \bigcap_{M \in \mathcal{S}} M$$

auch für beliebige Indexmengen  $I$  (wenn nötig ergänzt um  $\bigcup_{i \in \emptyset} M_i := \emptyset$ ).

Unter Verwendung der Schnittmenge definieren wir außerdem:

**Definition (disjunkte Mengen).** Zwei Mengen  $M$  und  $N$  heißen (zueinander) **disjunkt**, wenn

$$M \cap N = \emptyset$$

gilt. Allgemeiner heißen endliche viele Mengen  $M_1, M_2, \dots, M_n$  (mit natürlicher Zahl  $n$ ) bzw. unendliche viele Mengen  $M_1, M_2, M_3, \dots$  (**paarweise**) **disjunkt**, wenn  $M_i \cap M_j = \emptyset$  für alle  $i, j \in \{1, 2, \dots, n\}$  mit  $i \neq j$  bzw. alle  $i, j \in \{1, 2, 3, \dots\}$  mit  $i \neq j$  gilt. Analog heißen die in einem Mengensystem  $\mathcal{S}$  enthaltenen Mengen (**paarweise**) **disjunkt**, wenn  $M \cap N = \emptyset$  für alle  $M, N \in \mathcal{S}$  mit  $M \neq N$  gilt.

Das Adjektiv „paarweise“ wird dabei des Öfteren hinzugesetzt, um noch klarer zu stellen, dass für Disjunktheit mehrerer Mengen  $M_1, M_2, \dots, M_n$  nur der Schnitt  $M_i \cap M_j$  von je zweien leer sein muss und eben *nicht* der Gesamt-Schnitt  $M_1 \cap M_2 \cap \dots \cap M_n$ . Jeder andere Begriff von Disjunktheit mehrerer Mengen ist aber unüblich, so dass man auf das Wort „paarweise“ normalerweise auch verzichten kann.

Für **disjunkte** Mengen  $M$  und  $N$  bezeichnet man  $M \cup N$  als **disjunkte Vereinigung**(smenge) von  $M$  und  $N$  und schreibt für  $M \cup N$  auch

$$M \dot{\cup} N.$$

Der Unterschied zwischen  $\cup$  und  $\dot{\cup}$  besteht also einzig darin, dass  $\dot{\cup}$  nur zwischen disjunkten Mengen verwendet werden darf und durch seine Verwendung die Disjunktheit dann mit anzeigt. Analog verwendet man die Notationen  $\dot{\bigcup}_{i=m}^n M_i$  und  $\dot{\bigcup}_{M \in \mathcal{S}} M$ . Gelegentlich wird das Symbol  $\dot{\cup}$  allerdings auch bei (möglicherweise) nicht disjunkten Mengen verwendet, um anzuzeigen, dass die Mengen vor der Vereinigung durch Ersetzung/Umbenennung von Elementen disjunkt gemacht werden. Seltener werden für disjunkte Vereinigungen anstelle obiger Notation auch die Schreibweisen  $M + N$ ,  $\sum_{i=m}^n M_i$  und  $\sum_{M \in \mathcal{S}} M$  gebraucht.

Auch für Mengen-Differenzen und ihr Zusammenspiel mit Vereinigungen und Schnitten lassen sich verschiedene allgemeingültige Regeln angeben, die teils in den Lernwerkstätten und Übungen behandelt werden. Hier halten wir vor allem eine etwas andere Sichtweise auf Differenzmengen fest:

**Definition (Komplementärmengen, Komplemente von Mengen).** Für eine fixierte Menge  $\mathcal{X}$ , genannt die Grundmenge, und eine Teilmenge  $M$  von  $\mathcal{X}$  nennt man  $M^c := \mathcal{X} \setminus M$  das **Komplement** von  $M$  (in  $\mathcal{X}$ ).

<sup>2</sup>Später werden wir in dieser Situation von einer Familie  $(M_i)_{i \in I}$  von Mengen oder äquivalent von einer Abbildung  $I \rightarrow \mathcal{S}$ ,  $i \mapsto M_i$  sprechen.

Da bei der Komplement-Notation nur noch  $M$  und nicht mehr  $\mathcal{X}$  auftritt, ist die Schreibweise  $M^c$  mit Bedacht zu verwenden und nur dann sinnvoll, wenn die zugrundeliegende Menge  $\mathcal{X}$  klar ist und nicht variiert. Ein Vorteil der Komplement-Notation ist aber, dass mengentheoretische Folgerungen aus den Verneinungsregeln der Abschnitte 1.1 und 1.2 sehr prägnant angegeben werden können: Tatsächlich gelten für Teilmengen  $M, N, M_i$  einer fixierten Grundmenge  $\mathcal{X}$  die Regel

$$(M^c)^c = M$$

und die mengentheoretischen **de Morganschen Gesetze**

$$\begin{aligned} (M \cup N)^c &= M^c \cap N^c, & (M \cap N)^c &= M^c \cup N^c, \\ \left( \bigcup_{i \in I} M_i \right)^c &= \bigcap_{i \in I} M_i^c, & \left( \bigcap_{i \in I} M_i \right)^c &= \bigcup_{i \in I} M_i^c \end{aligned}$$

(mit beliebiger Indexmenge  $I$  und ergänzender Konvention  $\bigcap_{i \in \emptyset} M_i := \mathcal{X}$ ). Mit anderen Worten werden **Vereinigungen unter Komplement-Bildung zu Schnitten und umgekehrt**.

Als Nächstes wird die Liste der Grundoperationen mit Mengen noch etwas erweitert:

**Definition (kartesische Produkte).** Seien  $M$  und  $N$  Mengen. Die Produktmenge  $M \times N$  von  $M$  und  $N$  ist die Menge aller (**geordneten**) **Paare**  $(x, y)$  mit  $x \in M$  und  $y \in N$ . Dabei wird die Gleichheit  $(x, y) = (\tilde{x}, \tilde{y})$  von Paaren als gleichbedeutend mit  $(x = \tilde{x}) \wedge (y = \tilde{y})$  definiert.

**Beispiel.** Es ist  $\{2, 4, 7\} \times \{4, 3\} = \{(2, 4), (2, 3), (4, 4), (4, 3), (7, 4), (7, 3)\}$ .

Im Zusammenhang mit geordneten Paaren und kartesischen Produkten sei zunächst betont, dass  $(x, y)$  *nicht* dasselbe ist wie  $(y, x)$  (außer natürlich im Fall  $x = y$ ). Dementsprechend ist auch  $M \times N$  *nicht* dasselbe wie  $N \times M$  (außer wenn  $M = N$  oder  $M = \emptyset$  oder  $N = \emptyset$ ). Es kommt also auf die Reihenfolge entscheidend an; dies ist gerade das Wesen des *geordneten* Paares und des kartesischen Produkts.

Man kann das kartesische Produkt im Fall von Mengen  $M$  und  $N$  von Zahlen auf der Zahlengeraden veranschaulichen, indem man die in  $M \times N$  enthaltenen Paare genau wie in der Schulmathematik als Koordinatenpunkte in der Zeichenebene interpretiert. Trägt man  $M$  auf der ersten und  $N$  auf der zweiten Achse des ebenen Koordinatensystems auf (womit man tatsächlich  $M \times \{0\}$  und  $\{0\} \times N$  zeichnet), so ergibt sich das kartesische Produkt  $M \times N$  in der in Abbildung 8 veranschaulichten Weise.

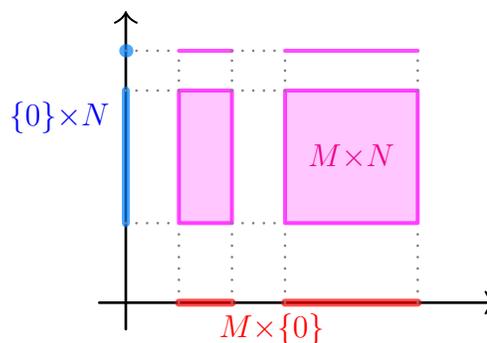


Abb. 8: Kartesisches Produkt  $M \times N$  von Mengen  $M, N$  der Zahlengeraden

Neben geordneten Paaren  $(x_1, x_2)$  braucht man oft auch **Tripel**  $(x_1, x_2, x_3)$ , **Quadrupel**  $(x_1, x_2, x_3, x_4)$  und allgemein für eine beliebige natürliche Zahl  $n$  sogenannte  **$n$ -Tupel**  $(x_1, x_2, \dots, x_n)$ . Diese betrachtet man als Elemente des kartesischen Produkts mehrerer Mengen:

**Definitionen (mehrfache kartesische Produkte).** Seien  $n$  eine natürliche Zahl<sup>3</sup> und  $M_1,$

<sup>3</sup>Im formal eingeschlossenen Fall  $n = 1$  trifft man die sehr naheliegende Konvention, dass ein 1-Tupel  $(x_1)$  nichts anderes als das Element  $x_1$  und ein 1-faches kartesische Produkt  $M_1$  nichts anderes als die Menge  $M_1$  ist. Dies ergibt sich auch aus Notationsgründen mehr oder weniger automatisch.

$M_2, \dots, M_n$  Mengen. Das  $n$ -fache kartesische Produkt

$$M_1 \times M_2 \times \dots \times M_n$$

(manchmal auch als  $\times_{i=1}^n M_i$  oder  $\prod_{i=1}^n M_i$  notiert) ist die Menge der  $n$ -Tupel  $(x_1, x_2, \dots, x_n)$  mit  $x_i \in M_i$  für alle  $i \in \{1, 2, \dots, n\}$ . Dabei wird die Gleichheit  $(x_1, x_2, \dots, x_n) = (\tilde{x}_1, \tilde{x}_2, \dots, \tilde{x}_n)$  von  $n$ -Tupeln als gleichbedeutend mit  $\forall i \in \{1, 2, \dots, n\}: x_i = \tilde{x}_i$  definiert.

Besonders häufig braucht man tatsächlich das  $n$ -fache kartesische Produkt

$$M^n := \underbrace{M \times M \times \dots \times M}_{n \text{ Faktoren}}$$

einer Menge  $M$  mit sich selbst. Zu allermeist ist es bei solchen Bildungen üblich,  $((x_1, x_2), x_3) = (x_1, (x_2, x_3)) = (x_1, x_2, x_3)$  zu verstehen, also derartige iterierte Paare mit Tripeln zu identifizieren. Dementsprechend gilt dann

$$(M_1 \times M_2) \times M_3 = M_1 \times (M_2 \times M_3) = M_1 \times M_2 \times M_3,$$

und man kann auf Klammerung verzichten.

Vor diesem Hintergrund können wir das kartesische Produkt  $M \times N$  auch im Fall einer Menge  $M$  von Koordinatenpunkten in der Ebene und einer Menge  $N$  von Zahlen auf der Zahlengeraden veranschaulichen. In diesem Fall enthält  $M \times N$  Tripel  $(x, y, z) = ((x, y), z)$  aus ebenen Koordinaten  $(x, y)$  und einer weiteren Zahl  $z$ , wobei die Tripel insgesamt als räumliche Koordinaten interpretiert werden können. In einer 3D-Skizze ist somit  $M$  (beziehungsweise  $M \times \{0\}$ ) in der Ebene der ersten beiden Achsen und  $N$  (beziehungsweise  $\{(0, 0)\} \times N$ ) auf der dritten Achse zu zeichnen. Das Produkt  $M \times N$  ergibt sich dann, wie in Abbildung 9 dargestellt, als Zylinder-artige Menge von Koordinatenpunkten im 3-dimensionalen Raum.

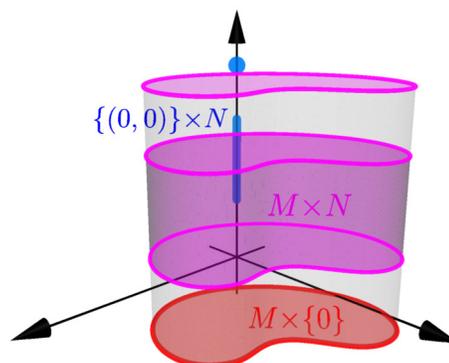


Abb. 9: Kartesisches Produkt  $M \times N$  einer Menge  $M$  der Ebene mit einer Menge  $N$  der Zahlengeraden

Auf zwei letzte Grundoperationen mit Mengen wird hier nur kurz eingegangen:

**Definition (Potenzmenge).** Sei  $M$  eine Menge. Die Potenzmenge  $\mathcal{P}(M)$  von  $M$  ist das Mengensystem, das genau die Teilmengen von  $M$  (inklusive  $\emptyset$  und  $M$  selbst) als Elemente enthält.

Die wohl einfachste Potenzmenge ist  $\mathcal{P}(\emptyset) = \{\emptyset\}$  (bemerke aber  $\{\emptyset\} \neq \emptyset$ ), ein konkreteres Beispiel ist  $\mathcal{P}(\{6, 28, 496\}) = \{\emptyset, \{6\}, \{28\}, \{496\}, \{6, 28\}, \{6, 496\}, \{28, 496\}, \{6, 28, 496\}\}$ . Allgemein kann mit etwas Kombinatorik gezeigt werden (dazu später): Hat  $M$  genau  $n$  verschiedene Elemente (für eine nicht-negative ganze Zahl  $n$ ), so hat  $\mathcal{P}(M)$  genau  $2^n$  verschiedene Elemente.

**Axiom (Auswahl).** Sei  $\mathcal{S}$  ein System disjunkter nicht-leerer Mengen. Dann gibt es eine Teilmenge  $A$  von  $\bigcup_{M \in \mathcal{S}} M$ , so dass  $A$  mit jeder in  $\mathcal{S}$  enthaltenen Menge  $M$  genau ein Element gemeinsam hat.

Bei der Auswahloperation handelt es sich tatsächlich um eine Ausformulierung des sogenannten Auswahlaxioms der Mengenlehre, also um eine Grundannahme der Mathematik, die (für unsere und die allermeisten Zwecke) nicht zu hinterfragen ist. Die Annahme betrifft dabei nur die pure Existenz von Auswahlmengen  $A$  mit der beschriebenen Eigenschaft. Wie die Auswahl eventuell zustande kommt und ob sie konkreter angegeben werden kann, ist unerheblich. Etwas mehr hierzu wird unten im Kleingedruckten noch gesagt. Tatsächlich ist ein genaueres Verständnis des Auswahlaxioms an dieser Stelle aber nicht erforderlich.

Schließlich soll auch auf **Grenzen der naiven Mengenlehre** mit der Grundvorstellung einer Menge als Ansammlung von Objekten hingewiesen werden: Tatsächlich würde man im naiven Rahmen zunächst davon ausgehen, dass man auch das Mengensystem  $\mathcal{S}$  aller Mengen (manchmal Allmenge genannt) bilden kann. Dies ist aber hochproblematisch, denn durch Aussonderung könnte man auch die Menge  $\mathcal{R} := \{M \in \mathcal{S} \mid M \notin M\}$  bilden, und die Frage, ob  $\mathcal{R}$  sich selbst enthält, ergäbe den Widerspruch  $\mathcal{R} \in \mathcal{R} \iff \mathcal{R} \notin \mathcal{R}$ . Dieser als **Russellsches Paradoxon** bekannte Widerspruch hat maßgeblich zur Entwicklung eines modernen Mengenbegriffs beigetragen und das Verständnis dafür geprägt, dass die naive Mengenlehre nicht ausreicht und man tatsächlich ein **präzises Axiomensystem als Grundlage** der Mengenlehre braucht, in dessen Rahmen die Bildung einer Menge aller Mengen **nicht zulässig** ist.

Als präzise Grundlage der Mengenlehre und damit der Mathematik hat sich letztlich (trotz gewisser Unvollständigkeitsprobleme) das **Zermelo-Fraenkel-Axiomensystem der Mengenlehre**, benannt nach den Mathematikern E. Zermelo (1871–1953) und A. Fraenkel (1891–1965), bewährt. Dieses Axiomensystem ist heutzutage sehr weitgehend akzeptiert und ähnelt an vielen Stellen oben schon diskutierten Bildungen. Eine detaillierte Behandlung der Axiome geht über den Vorlesungsstoff hinaus. Es soll allerdings auch nicht fälschlicherweise der Eindruck entstehen, dass die Axiome unzugänglich wären oder nicht ohne Weiteres hingeschrieben werden könnten. Daher seien die Axiome für den interessierten Leser zumindest im Kleingedruckten festgehalten:

Die **Zermelo-Fraenkel-Axiome der Mengenlehre** fundieren eine Mathematik, in der alle mathematischen Objekte Mengen sind und insbesondere auch als Elemente von Mengen nur Mengen in Frage kommen. Die Axiome basieren auf einer Prädikatenlogik erster Stufe mit Gleichheitsrelation  $=$ , wobei alle Quantoren über das sogenannte Diskursuniversum aus allen Mengen laufen. Daneben wird nur auf die undefinierte Elementrelation  $\in$  aufgebaut (auf deren Grundlage  $\notin$  und  $\subset$  wie früher in diesem Abschnitt definiert werden). Die genauen Axiome lauten dann wie folgt, wobei die zweiten eingeklammerten Absätze nicht zum Axiomensystem gehören, sondern Zusatz Erläuterungen geben:

- **Extensionalitätsaxiom:** Zwei Mengen  $M$  und  $N$  sind genau dann gleich, wenn sie dieselben Elemente enthalten. Mit anderen Worten ist die Gleichheit  $M = N$  gleichbedeutend mit  $\forall x: (x \in M \iff x \in N)$ .

(Wir hatten dies zuvor als Definition der Mengen-Gleichheit betrachtet. Da die Gleichheit aber schon in der zugrunde gelegten Prädikatenlogik definiert ist, kann man sich diese Charakterisierung der Gleichheit genau genommen nur als Axiom und nicht als Definition „wünschen“.)

- **Leermengenaxiom:** Es existiert eine Menge  $\emptyset$  ohne Elemente, die also  $\forall x: x \notin \emptyset$  erfüllt.

(Wegen des Extensionalitätsaxioms ist  $\emptyset$  dabei eindeutig bestimmt. Das Leermengenaxiom ist das einzige Axiom, das die Existenz einer konkreten Menge fordert. Alle anderen Mengen können — was zunächst erstaunlich scheinen mag — mit Hilfe der anderen Axiome aus der leeren Menge gebildet werden.)

- **Paarmengenaxiom:** Für alle Mengen  $a$  und  $b$  existiert eine Menge  $\{a, b\}$ , die genau  $a$  und  $b$  als Elemente enthält, für die also  $\forall x: (x \in \{a, b\} \iff x = a \vee x = b)$  gilt.

(Man kann die Menge  $\{a, b\}$  als ein *ungeordnetes* Paar von  $a$  und  $b$  auffassen, denn die Gleichheit  $\{a, b\} = \{\tilde{a}, \tilde{b}\}$  solcher Mengen bedeutet *entweder*  $a = \tilde{a} \wedge b = \tilde{b}$  *oder*  $a = \tilde{b} \wedge b = \tilde{a}$ . Hierauf aufbauend kann man aber auch das *geordnete* Paar  $(a, b)$  und das kartesische Produkt mengentheoretisch definieren. Dazu setzt man  $(a, b) := \{a, \{a, b\}\}$  oder — was technisch ein kleinen Vorteil hat —  $(a, b) := \{\{a\}, \{a, b\}\}$  und weist anhand dieser Definition nach, dass die Gleichheit geordneter Paare  $(a, b) = (\tilde{a}, \tilde{b})$  tatsächlich wie gewünscht  $a = \tilde{a} \wedge b = \tilde{b}$  bedeutet.)

- **Vereinigungsaxiom:** Für jede Menge  $\mathcal{S}$  (von Mengen) existiert eine mit  $\bigcup \mathcal{S}$  bezeichnete Menge, deren Elemente genau die Elemente der Elemente von  $\mathcal{S}$  sind, für die mit anderen Worten also  $\forall x: (x \in \bigcup \mathcal{S} \iff \exists M \in \mathcal{S}: x \in M)$  gilt.

- **Unendlichkeitsaxiom:** Es existiert eine sogenannte induktive Menge, die zum einen die leere Menge  $\emptyset$  als Element enthält und zum anderen für jedes ihrer Elemente  $x$  auch  $x \cup \{x\}$  als Element enthält (wobei  $\{x\} := \{x, x\}$  und  $x \cup \{x\} := \bigcup\{x, \{x\}\}$  gemäß den vorigen Axiomen existieren).  
(Dieses Axiom sichert die Existenz unendlicher Mengen und spielt vor allem bei der Konstruktion der natürlichen Zahlen  $\mathbb{N}$ , der wohl grundlegendsten unendlichen Menge, eine entscheidende Rolle.)
- **Potenzmengenaxiom:** Zu jeder Menge  $M$  existiert die sogenannte Potenzmenge  $\mathcal{P}(M)$ , die genau die Teilmengen von  $M$  als Elemente enthält, also  $\forall T: (T \subset M \iff T \in \mathcal{P}(M))$  erfüllt.
- **Fundierungsaxiom/Regularitätsaxiom:** Jede Menge  $M$  außer der leeren Menge enthält ein Element  $N$  mit  $M \cap N = \emptyset$  (wobei man vor Einführung der Schnittmenge statt  $M \cap N = \emptyset$  eigentlich  $\forall x: (x \notin M \vee x \notin N)$  schreiben muss).  
(Dieses Axiom sichert, dass keine unendliche Kette von ineinander enthalten Mengen des Typs  $M_1 \ni M_2 \ni M_3 \ni \dots$  existieren kann (denn dann würde die unendliche Menge  $M = \{M_1, M_2, M_3, \dots\}$  dem Axiom widersprechen). Das Axiom führt auch dazu, dass  $N \notin N$  für jede Menge  $N$  gilt (denn bei Existenz von  $N$  mit  $N \in N$  würde  $M = \{N\}$  dem Axiom widersprechen).)
- **Aussonderungssaxiom:** Für jede Menge  $M$  und jedes Prädikat  $P(y)$  mit einer freien Variable  $y$  gibt es eine Menge  $\{y \in M \mid P(y)\}$ , deren Elemente genau die Elemente  $x$  von  $M$  sind, für die  $P(x)$  gilt. Diese Menge  $\{y \in M \mid P(y)\}$  erfüllt also  $\forall x: (x \in \{y \in M \mid P(y)\} \iff x \in M \wedge P(x))$  ist wahr).  
(Insbesondere können als Konsequenz des Axioms auch Schnittmengen und — wie vorne schon gesehen — Mengendifferenzen definiert werden.)
- **Ersetzungssaxiom:** Ist  $M$  eine Menge, so kann jedes Element  $x$  von  $M$  durch eine beliebige von  $x$  abhängige Menge  $N_x$  ersetzt und auf diese Weise eine neue Menge  $\{N_x \mid x \in M\}$  gebildet werden.
- **Auswahlaxiom:** Für jede Menge  $\mathcal{S}$  von paarweise disjunkten nicht-leeren Mengen (d.h.  $\forall M \in \mathcal{S}: M \neq \emptyset$  und  $\forall M, N \in \mathcal{S}: M \neq N \implies M \cap N = \emptyset$ ) kann eine Menge  $A$  gebildet werden, die genau ein Element aus jedem Element von  $\mathcal{S}$  enthält (und sonst keine weiteren Elemente).  
(Dieses Axiom ermöglicht es, aus jeder in  $\mathcal{S}$  enthaltenen Menge je ein Element auszuwählen und aus diesen Elementen eine neue Menge zu bilden. Der entscheidende Punkt ist dabei, dass solch eine Auswahl in sehr großer Allgemeinheit ermöglicht wird. Falls eine „konkrete Regel“ für die Auswahl angegeben werden kann oder falls  $\mathcal{S}$  nur endlich viele Mengen als Elemente hat, wird das Auswahlaxiom nicht benötigt und die Auswahl kann auch mit den anderen Axiomen bewerkstelligt werden. Das Auswahlaxiom greift aber selbst dann, wenn  $\mathcal{S}$  unendlich viele Elemente hat und keine Regel für die Auswahl konstruktiv angegeben werden kann. Bei früheren Kontroversen um die Konstruktivität mathematischer Beweise stand daher auch die Sinnhaftigkeit des Auswahlaxioms zur Debatte. Heutzutage wird das Axiom aber von einer überwiegenden Mehrheit der Mathematiker akzeptiert, und in vielen Bereichen der modernen Mathematik kann nicht darauf verzichtet werden.)

Die historische Entwicklung von der naiven Mengenlehre des späten 19. Jahrhunderts zu dem in der obigen Form um das Jahr 1930 komplettierten Axiomensystem war übrigens ein langer Prozess mit vielen Beteiligten. Einen ersten Hinweis, dass die naive Mengenlehre an ihre Grenzen stößt, mag man tatsächlich in einer als **prägnante Anekdote** überlieferten Konversation zwischen den Mathematikern und Gründervätern der Mengenlehre G. Cantor (1845–1918) und R. Dedekind (1831–1916) sehen: „Dedekind äußerte hinsichtlich des Begriffs der Menge, er stelle sich eine Menge vor wie einen geschlossenen Sack, der ganz bestimmte Dinge enthalte, die man aber nicht sähe, und von denen man nichts wisse, außer daß sie vorhanden und bestimmt seien. Einige Zeit später gab Cantor seine Vorstellung einer Menge zu erkennen: Er richtete seine kolossale Figur hoch auf, beschrieb mit erhobenem Arm eine großartige Geste und sagte mit einem ins Unbestimmte gerichteten Blick: „Eine Menge stelle ich mir vor wie einen Abgrund.““ (Überlieferung nach F. Bernstein [2]).

## Kapitel 2

# Abbildungen, Relationen, Zahlen

In diesem und den nächsten Kapiteln beschäftigen wir uns viel mit den grundlegenden, auch aus der Schule bekannten **Zahlbereichen** (Mengen von Zahlen)

$$\begin{aligned}\mathbb{N} &= \{1, 2, 3, \dots\} \text{ (natürliche Zahlen)}, \mathbb{N}_0 = \{0, 1, 2, \dots\}, \\ \mathbb{Z} &= \{0, 1, -1, 2, -2, 3, -3, \dots\} \text{ (ganze Zahlen)}, \\ \mathbb{Q} &\text{ (rationale Zahlen; Brüche mit Zähler aus } \mathbb{Z}, \text{ Nenner aus } \mathbb{N}), \\ \mathbb{R} &\text{ (reelle Zahlen; Zahlen der Zahlengeraden)}\end{aligned}$$

und den **Rechengrundgesetzen** auf diesen Bereichen. Für die Zahlbereiche gelten die Inklusionen

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

wobei die ganz rechts genannten komplexen Zahlen  $\mathbb{C}$  erst in Mathematik 2 eingeführt werden.

Das **Ziel dieses Kapitels** ist zweigeteilt: Zum einen werden allgemeine, für die Mathematik **fundamentale Konzepte wie Abbildungen/Funktionen und Relationen** eingeführt. Zum anderen werden mit Hilfe dieser Konzepte **präzise Konstruktionen der Zahlbereiche**  $\mathbb{N}$ ,  $\mathbb{N}_0$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$  nur auf Grundlage der (Axiome der) Mengenlehre gegeben und damit die Existenz dieser Zahlbereiche bewiesen werden. Die Konstruktion von  $\mathbb{R}$  (und  $\mathbb{C}$ ), die etwas mehr Analysis braucht, wird auf das spätere Kapitel 4 vertagt.

### 2.1 Abbildungen

Die **gleichbedeutenden Begriffe Abbildung und Funktion** sind in der Mathematik sehr grundlegend. Tendenziell bevorzugt man die Bezeichnung Funktion in etwas konkreteren Situationen (etwa, wenn man wie in der Schulmathematik Terme angeben und Funktionsgraphen zeichnen kann), während die Bezeichnung Abbildung häufig im Abstrakten verwendet wird. Eine scharfe Trennung oder einen echten Unterschied in der Bedeutung gibt es aber nicht.

Tatsächlich lässt sich der Begriff wie folgt fassen:

**Definition (Abbildungen).** *Seien  $\mathcal{X}$  und  $\mathcal{Y}$  beliebige Mengen. Eine **Funktion** oder **Abbildung**  $f$  von  $\mathcal{X}$  nach  $\mathcal{Y}$  oder in die Menge  $\mathcal{Y}$  ist eine (Zuordnungs-)Vorschrift<sup>1</sup>, die jedem Element  $x$  von  $\mathcal{X}$  ein eindeutiges Element  $y$  von  $\mathcal{Y}$  zuordnet. Man sagt,  $f$  bilde das Element  $x$  auf das zugehörige*

---

<sup>1</sup>Den Begriff „(Zuordnungs-)Vorschrift“ können und werden wir in Abschnitt 2.3 noch präzisieren.

Element  $y$  ab, dieses  $y$  sei das Bild von  $x$  unter  $f$  oder dieses  $y$  sei der (**Funktions-**) Wert von  $f$  an der Stelle  $x$  oder zum **Argument**  $x$ . Man nennt  $\mathcal{X}$  die Definitionsmenge oder den **Definitionsbereich** und  $\mathcal{Y}$  das Ziel oder den **Zielbereich** von  $f$ . Im Fall  $\mathcal{X} = \mathcal{Y}$  spricht man von einer **Selbstabbildung**.

Besonders betont sei bei dieser Definition das **zentrale Existenz- und Eindeutigkeitsprinzip**, gemäß dem zu einem beliebigen Element  $x$  von  $\mathcal{X}$  genau ein zugehöriges Element  $y$  von  $\mathcal{Y}$  existiert. Sowohl die Nicht-Existenz des Elements  $y$  als auch die Existenz mehr als eines Elements  $y$  (zum gleichen  $x$ ) werden ausgeschlossen.

**Notationen** (bei Abbildungen). Seien  $\mathcal{X}, \mathcal{Y}$  Mengen und  $f$  eine Abbildung von  $\mathcal{X}$  nach  $\mathcal{Y}$ .

- (1) Dass  $f$  Definitionsbereich  $\mathcal{X}$  und Ziel  $\mathcal{Y}$  hat, also eine Abbildung von  $\mathcal{X}$  nach  $\mathcal{Y}$  ist, drückt man durch die Notation  $f: \mathcal{X} \rightarrow \mathcal{Y}$  aus.
- (2) Ordnet  $f$  einem Element  $x \in \mathcal{X}$  den Funktionswert  $y \in \mathcal{Y}$  zu, so schreibt man  $f(x)$  für  $y$  oder notiert  $x \xrightarrow{f} y$  beziehungsweise kurz  $x \mapsto y$ .

(Dabei ist es Konvention, den Pfeil  $\rightarrow$  bei Angabe von Definitionsbereich und Ziel, aber den etwas anderen Pfeil  $\mapsto$  für Zuordnungen der Elemente zu nutzen).

**Beispiele** (von Abbildungen). In der Praxis gibt man eine Abbildung  $f$  von  $\mathcal{X}$  nach  $\mathcal{Y}$  konkret an, indem man neben  $\mathcal{X}, \mathcal{Y}$  den Funktionsterm  $f(x)$  oder die Zuordnung  $x \mapsto f(x)$  beziehungsweise  $x \mapsto y$  für alle  $x \in \mathcal{X}$  eindeutig spezifiziert. Wir betrachten hierzu folgende Beispiele:

- (1) Eine Abbildung

$$f: \{1, 2, 4, 5\} \rightarrow \{-3, -2, 0, 4, 10\}$$

ist durch die Zuordnungen

$$1 \mapsto -2, \quad 2 \mapsto -2, \quad 4 \mapsto 4, \quad 5 \mapsto 10$$

gegeben und wird weiter unten in Abbildung 10 graphisch dargestellt. Die gleiche Zuordnungsvorschrift kann auch anders angegeben werden, z.B. durch  $f(x) := x^2 - 3x$  oder durch  $f(x) := \begin{cases} -2 & \text{falls } x < 3 \\ 6x - 20 & \text{falls } x > 3 \end{cases}$  für alle  $x \in \{1, 2, 4, 5\}$ . Wie zuletzt eine **geschweifte Klammer für Fallunterscheidungen** zu verwenden, ist allgemein üblich und bedeutet an dieser Stelle einerseits  $f(x) := -2$  im Fall  $x < 3$  und andererseits  $f(x) := 6x - 20$  im Fall  $x > 3$ .

- (2) Eine andere Abbildung

$$f: \{\emptyset, 5, \mathbb{N}\} \rightarrow \mathbb{Q}$$

erhält man durch die Festlegungen

$$f(\emptyset) := \frac{3}{2}, \quad f(5) := 4, \quad f(\mathbb{N}) := -\frac{1}{12}.$$

- (3) Eine weitere Abbildung

$$f: \mathbb{N} \rightarrow \mathbb{N}$$

wird durch

$$f(n) := n^2 \quad \text{für alle } n \in \mathbb{N}$$

definiert. Diese Abbildung ordnet  $1 \mapsto 1$ ,  $2 \mapsto 4$ ,  $3 \mapsto 9$ ,  $4 \mapsto 16$  zu. Da es unendlich viele Zahlen in  $\mathbb{N}$  gibt, reichen diese vier Beispiele (oder jede andere endliche Anzahl) aber nicht aus, um die Abbildung in Gänze zu beschreiben. Zum Beispiel haben 1, 2, 3, 4 dieselben Funktionswerte wie unter  $f$  auch unter  $g: \mathbb{N} \rightarrow \{0, 1, 4, 9, 16\}$  mit  $g(n) := \begin{cases} n^2 & \text{falls } n \leq 4 \\ 0 & \text{falls } n \geq 5 \end{cases}$  für alle  $n \in \mathbb{N}$  und unter  $h: \mathbb{N} \rightarrow \mathbb{N}$  mit  $h(n) := n^2 + (n-1)(n-2)(n-3)(n-4)$  für alle  $n \in \mathbb{N}$ , doch ab 5 unterscheiden sich die Werte von  $f$ ,  $g$  und  $h$ .

- (4) Man kann die Addition natürlicher Zahlen als Abbildung

$$f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$$

auffassen, die durch

$$f((m, n)) := m+n \quad \text{für alle } (m, n) \in \mathbb{N} \times \mathbb{N}$$

festgelegt ist. Dies ist ein erstes Beispiel einer **Abbildung von zwei Variablen**, die beispielsweise  $(1, 2) \mapsto 3$  und  $(4, 2) \mapsto 6$  zuordnet und von beiden Einträgen  $m$  und  $n$  der einzusetzenden Paare  $(m, n)$  abhängt. Zur Vereinfachung der Notation schreiben wir bei solchen Abbildungen zukünftig  $f(m, n)$  statt  $f((m, n))$ . Übrigens ist es durchaus üblich, die hier betrachtete Abbildung  $+$  statt  $f$  zu nennen, und analog dazu auch bei anderen Abbildungen, die sich direkt aus einer Rechenoperation ergeben, das Rechensymbol als Name der Abbildung zu verwenden.

- (5) Eine Funktion

$$f: \mathbb{R} \rightarrow \mathbb{R}$$

erhält man durch die Festlegung

$$f(x) := x^3 - x \quad \text{für alle } x \in \mathbb{R}.$$

In alternativer verbreiteter Schreibweise kann diese Funktion auch als  $f: \mathbb{R} \rightarrow \mathbb{R}$ ,  $x \mapsto x^3 - x$  angegeben werden.

- (6) Eine weitere Funktion

$$f: \mathcal{X} \rightarrow \mathcal{Y} \quad \text{von } \mathcal{X} := \{x \in \mathbb{R} \mid 1 \leq x < \frac{11}{2}\} \text{ nach } \mathcal{Y} := \{y \in \mathbb{R} \mid -\frac{1}{2} < y < \frac{13}{2}\}$$

wird durch

$$f(x) := -x^2 + 6x - 3 \quad \text{für alle } x \in \mathcal{X}$$

definiert und weiter unten in den Abbildungen 13 und 14 (teilweise) graphisch dargestellt. Um die *Wohldefiniertheit* dieser Funktion  $f$  sicherzustellen, muss man allerdings noch zeigen, dass  $-\frac{1}{2} < -x^2 + 6x - 3 < \frac{13}{2}$  für alle  $x \in \mathcal{X}$  gilt: Tatsächlich erhält man durch Umschreiben  $-x^2 + 6x - 3 = 6 - (x-3)^2$  und Rechnen mit Ungleichungen (Dazu ab Kapitel 4 mehr!) aber sogar  $-\frac{1}{4} = 6 - \left(\frac{5}{2}\right)^2 < -x^2 + 6x - 3 \leq 6$  für alle  $x \in \mathcal{X}$ , womit die Wohldefiniertheit von  $f$  gesichert ist. Nebenbei sehen wir, dass  $g(x) := -x^2 + 6x - 3$  für  $x \in \mathcal{X}$  auch eine Funktion  $g: \mathcal{X} \rightarrow \mathcal{Z}$  in den kleineren Zielbereich  $\mathcal{Z} := \{z \in \mathbb{R} \mid -\frac{1}{4} < z \leq 6\} \subsetneq \mathcal{Y}$  ergibt.

- (7) „**Gegenbeispiele**“: Die Versuche,  $f: \mathbb{N} \rightarrow \mathbb{N}$  durch  $f(n) := n^2 - n$  für alle  $n \in \mathbb{N}$  oder  $g: \mathbb{N}_0 \rightarrow \mathbb{N}_0$  durch  $g(0) := n$  und  $g(n) := 0$  für alle  $n \in \mathbb{N}$  zu definieren, geben allerdings *keine* wohldefinierten Abbildungen, da  $f(1)$  nicht im Zielbereich  $\mathbb{N}$  liegt und  $g(0)$  nicht eindeutig definiert ist. (Auch  $g(0) := \mathbb{N}$  geht nicht, da zwar  $\mathbb{N} \subset \mathbb{N}_0$ , aber eben nicht  $\mathbb{N} \in \mathbb{N}_0$  gilt). Weiterhin ist auch  $h: \mathbb{R} \rightarrow \mathbb{R}$ ,  $x \mapsto \frac{1}{x}$  *keine* wohldefinierte Funktion, da  $\frac{1}{0}$  nicht erklärt

und deshalb der Funktionswert  $h(0)$  nicht definiert ist. (Die Variante  $\tilde{h}: \mathbb{R} \setminus \{0\} \rightarrow \mathbb{R}, x \mapsto \frac{1}{x}$  vermeidet dieses Problem natürlich und ist wohldefiniert.)

Erste Möglichkeiten zur **Veranschaulichung einer Abbildung** werden in den Abbildungen 10, 11, 12 und 13 gezeigt. Die entscheidende Abbildungseigenschaft verlangt dabei, dass **bei jedem Element des Definitionsbereichs  $\mathcal{X}$  genau ein Zuordnungspfeil beginnt** und zum zugehörigen Element im Ziel weist. Dagegen bestehen für ein Element des Ziels prinzipiell alle Möglichkeiten: Dort können kein Pfeil, ein Pfeil, mehrere Pfeile oder im Extremfall einer konstanten Abbildung auch alle Pfeile enden. Enthält der Definitionsbereich  $\mathcal{X}$  wie in Abbildung 10 und 11 nur endlich viele Elemente, so kann die Abbildung durch solche Zuordnungspfeile vollständig dargestellt werden. Dagegen kann man für Definitionsbereiche  $\mathcal{X}$  mit unendlich vielen Elementen, wie schon bei Beispiel (3) gesagt, nur einige Fälle, aber nie die gesamte Zuordnungsvorschrift auf diese Weise darstellen. Abbildung 12 zeigt dies für den Definitionsbereich  $\mathbb{N} \times \mathbb{N}$ . Abbildung 13 zeigt es für Teilmengen von  $\mathbb{R}$ , die als Punktmengen auf der Zahlengeraden veranschaulicht werden (wobei die schwarzen Punkte in Abbildung 13 nur Beispiel-Elemente und *nicht* alle Elemente der Mengen  $\mathcal{X}$  und  $\mathcal{Y}$  darstellen).

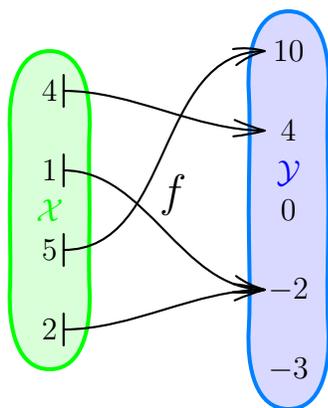


Abb. 10: Die Abbildung  $f$  aus Beispiel (1) von  $\mathcal{X} = \{1, 2, 4, 5\}$  nach  $\mathcal{Y} = \{-3, -2, 0, 4, 10\}$

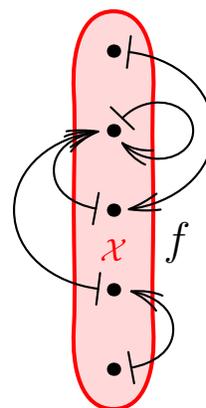


Abb. 11: Eine Selbstabbildung  $f: \mathcal{X} \rightarrow \mathcal{X}$  einer 5-elementigen Menge  $\mathcal{X}$

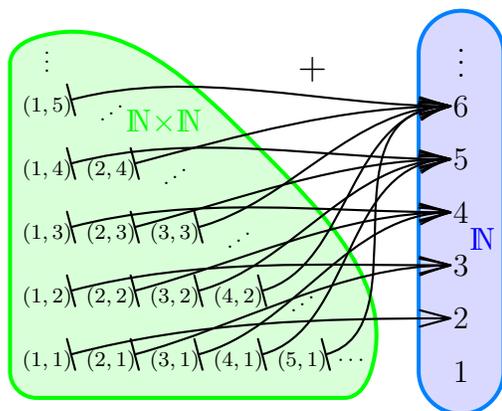


Abb. 12: Die Addition  $+$  als Abbildung des Beispiels (4) von  $\mathbb{N} \times \mathbb{N}$  nach  $\mathbb{N}$

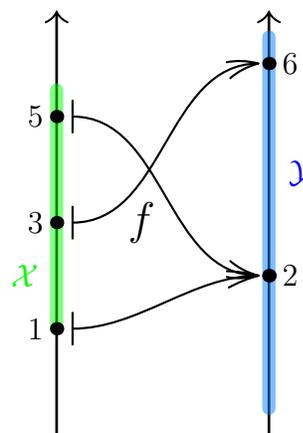


Abb. 13: Die Funktion  $f$  aus Beispiel (6) bildet 3 Punkte von  $\mathcal{X} \subset \mathbb{R}$  nach  $\mathcal{Y} \subset \mathbb{R}$  ab.

Natürlich müssen Definitionsbereich und Ziel einer Abbildung nicht unbedingt disjunkt sein, sondern können gemeinsame Elemente enthalten (wie es mit Ausnahme der Additions-Abbildung tatsächlich bei allen obigen Beispielen und Bildern der Fall ist). Normalerweise stellt man diese beiden Mengen dennoch nicht überlappend dar und trägt gemeinsame Elemente, so wie in den Abbildungen 10 und 13, zweimal separat ein. Sogar wenn Definitionsbereich und Ziel übereinstimmen, zieht man es der Übersichtlichkeit halber meist vor, zwei Kopien derselben Menge einzuzichnen. Gelegentlich weicht man hiervon aber auch ab und verwendet alternative Darstellungen wie die der Abbildung 11.

Speziell für eine Funktion  $f: \mathcal{X} \rightarrow \mathcal{Y}$  von  $\mathcal{X} \subset \mathbb{R}$  nach  $\mathcal{Y} \subset \mathbb{R}$  kann man oft auch den **(Funktions-)Graph**

$$G_f := \{(x, y) \in \mathcal{X} \times \mathcal{Y} \mid f(x) = y\} \subset \mathbb{R}^2$$

als Menge von Koordinatenpunkten der Ebene darstellen. Man trägt dazu den Definitionsbereich

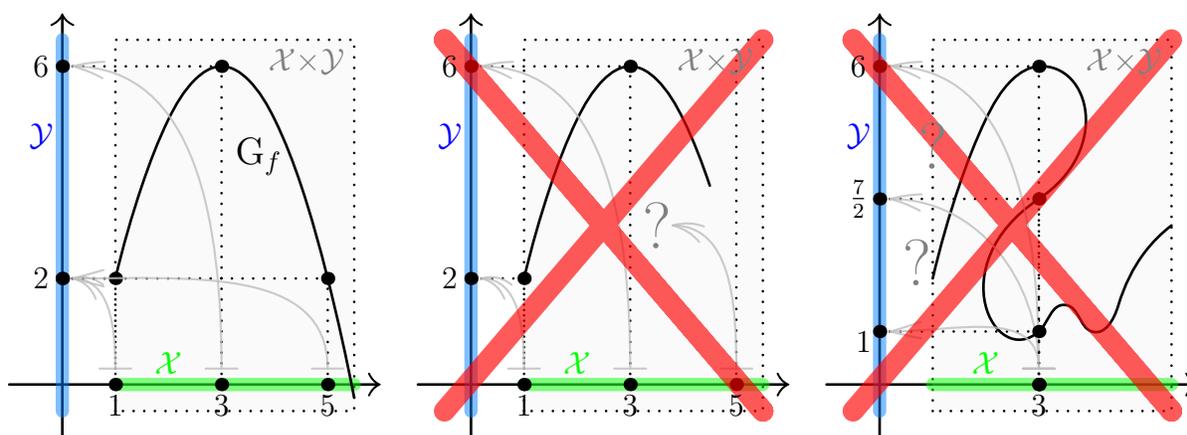


Abb. 14: Der Graph  $G_f$  der Funktion  $f$  aus Beispiel (6) von  $\mathcal{X} = \{x \in \mathbb{R} \mid 1 \leq x < \frac{11}{2}\}$  nach  $\mathcal{Y} = \{y \in \mathbb{R} \mid -\frac{1}{2} < y < \frac{13}{2}\}$  und zwei Kurven, die *nicht* Graph einer Funktion von  $\mathcal{X}$  nach  $\mathcal{Y}$  sind

$\mathcal{X}$  auf der ersten, den Zielbereich  $\mathcal{Y}$  auf der zweiten Achse des ebenen Koordinatensystems ein und bekommt als Darstellung von  $G_f$  in gutartigen Fällen eine Kurve durch alle Punkte der Form  $(x, f(x))$  mit  $x \in \mathcal{X}$ . Die definierende Eigenschaft der Funktion verlangt dabei, dass sich wie im ersten Bild der Abbildung 14 über jedem Punkt  $x \in \mathcal{X}$  (den wir jetzt immer mit  $(x, 0) \in \mathcal{X} \times \{0\}$  identifizieren) genau ein Punkt von  $G_f$  befindet. Dass sich wie in den beiden anderen Bildern über einem Punkt von  $\mathcal{X}$  kein Punkt oder mehrere Punkte der Kurve befinden, dass die Kurve also „aufhört“ oder unter/über sich selbst „zurück läuft“ ist für einen Funktionsgraph als Kurve somit nicht möglich. Der **entscheidende Vorteil der Graphendarstellung** ist der, dass man an  $G_f$  *alle* zu  $f$  gehörigen Zuordnungen ablesen kann (vergleiche die grauen Pfeile in Abbildung 14) und nicht nur die Zuordnung einiger Beispiel-Elemente. Daher wird mit  $G_f$  (jedenfalls im Rahmen der Zeichengenauigkeit) die **gesamte Zuordnungsvorschrift dargestellt**.

Auch für eine Funktion  $f: \mathcal{X} \rightarrow \mathcal{Z}$  von einem 2-dimensionalen Definitionsbereich  $\mathcal{X} \subset \mathbb{R}^2$  nach  $\mathcal{Z} \subset \mathbb{R}$ , also eine **Funktion von zwei Variablen**, kann man die Zuordnung einzelner Elemente mittels Pfeilen verdeutlichen oder in gutartigen Fällen die Funktion insgesamt durch ihren (Funktions-)Graph

$$G_f := \{(x, y, z) \in \mathcal{X} \times \mathcal{Z} \mid f(x, y) = z\} \subset \mathbb{R}^3$$

darstellen (wobei wir wie in Abschnitt 1.4 wieder  $((x, y), z) = (x, y, z)$  und  $\mathbb{R}^2 \times \mathbb{R} = \mathbb{R}^3$  identifizieren). Beide Möglichkeiten werden für eine Beispiel-Funktion<sup>2</sup> in Abbildung 15 gezeigt. Dabei bildet der Graph jetzt eine Fläche im 3-dimensionalen Raum durch alle Punkte der Form  $(x, y, f(x, y))$  mit  $(x, y) \in \mathcal{X}$ , es befindet sich aber nach wie vor über jedem Punkt  $(x, y) \in \mathcal{X}$  (natürlich identifiziert mit  $(x, y, 0) \in \mathcal{X} \times \{0\}$ ) genau ein Punkt von  $G_f$ .

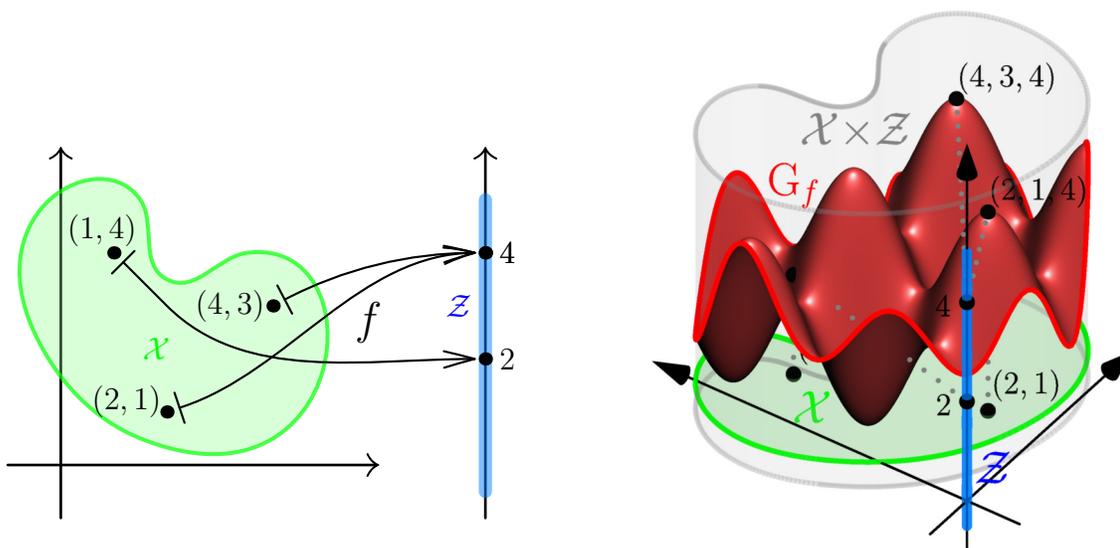


Abb. 15: Abbildung einiger Beispiel-Punkte und Graph  $G_f$  bei einer Funktion  $f: \mathcal{X} \rightarrow \mathcal{Z}$  von einem 2-dimensionalen Definitionsbereich  $\mathcal{X} \subset \mathbb{R}^2$  nach  $\mathcal{Z} = \{z \in \mathbb{R} \mid -\frac{1}{2} < z < 5\} \subset \mathbb{R}$

Als letzten Fall betrachten wir Darstellungen einer Funktion  $f: \mathcal{X} \rightarrow \mathcal{Y}$  von  $\mathcal{X} \subset \mathbb{R}$  in einen 2-dimensionalen Zielbereich  $\mathcal{Y} \subset \mathbb{R}^2$ . Im gutartigen Fall spricht man bei einer solchen Funktion von einer **Kurve**  $f$  in  $\mathbb{R}^2$  und stellt oft das Bild

$$f(\mathcal{X}) := \{(y, z) \in \mathcal{Y} \mid \exists x \in \mathcal{X} : f(x) = (y, z)\} \subset \mathbb{R}^2$$

von  $f$  dar, obwohl es für eine Gesamtdarstellung der Funktion auch hier den (Funktions-)Graph

$$G_f := \{(x, y, z) \in \mathcal{X} \times \mathcal{Y} \mid f(x) = (y, z)\} \subset \mathbb{R}^3,$$

braucht. Ein Beispiel für beide Darstellungsweisen wird in Abbildung 16 gezeigt. Tatsächlich enthält in diesem Fall das Bild  $f(\mathcal{X})$  schon relativ viel Information über die Funktion und kann zudem in der Ebene  $\mathbb{R}^2$  leichter gezeichnet, interpretiert und verstanden werden als der Graph  $G_f$ , der im Raum  $\mathbb{R}^3$  darzustellen ist. Das Bild muss sich übrigens nicht unbedingt so gutartig wie in Abbildung 16 verhalten, sondern kann sich auch in sogenannten Selbstschnitten „überkreuzen“ und/oder „auf sich selbst zurück laufen“. Beim Graph dagegen sind Selbstschnitte oder Ähnliches ausgeschlossen. Vielmehr hat dieser die Eigenschaft, dass sich in jedem der parallelen Ebenenstücke  $\{x\} \times \mathcal{Y}$  mit  $x \in \mathcal{X}$  genau ein Punkt von  $G_f$  befindet.

<sup>2</sup>Tatsächlich ist die in Abbildung 15 geplottete Funktion auf dem dargestellten Definitionsbereich  $\mathcal{X} \subset \mathbb{R}^2$  durch  $f(x, y) := 2 - 2 \sin((x+y)\frac{\pi}{2}) \sin((x-y)\frac{3\pi}{8})$  für  $(x, y) \in \mathcal{X}$  gegeben. Die hier verwendete Sinus-Funktion  $\sin$  und die Kreiszahl  $\pi$  werden in der Vorlesung aber erst deutlich später eingeführt.

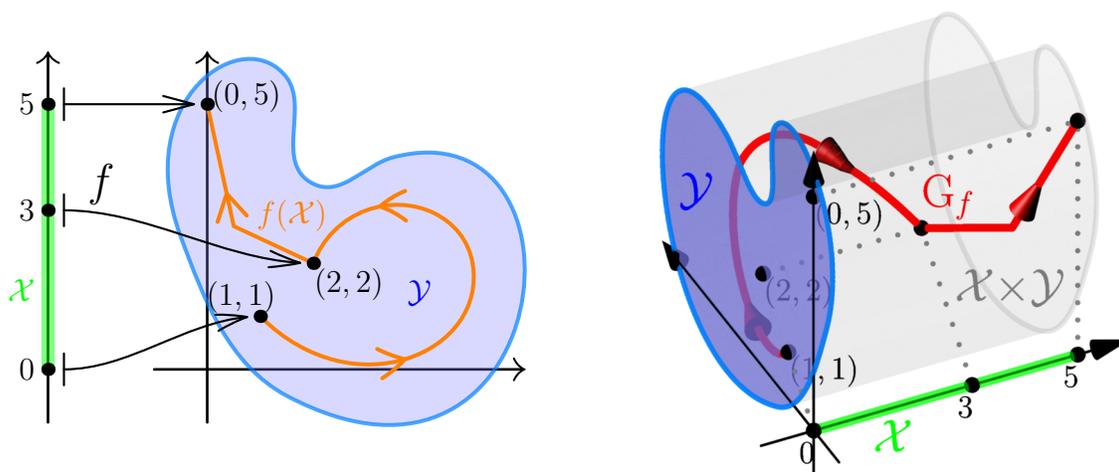


Abb. 16: Abbildung einiger Beispiel-Punkte, das Bild  $f(\mathcal{X})$  und der Graph  $G_f$  bei einer Funktion  $f: \mathcal{X} \rightarrow \mathcal{Y}$  von  $\mathcal{X} = \{x \in \mathbb{R} \mid 0 \leq x \leq 5\} \subset \mathbb{R}$  in einen 2-dimensionalen Zielbereich  $\mathcal{Y} \subset \mathbb{R}^2$

Übrigens ist der Graph  $G_f$  einer Funktion  $f: \mathcal{X} \rightarrow \mathcal{Y}$  immer auch das Bild der Graphenabbildung  $\mathcal{X} \rightarrow \mathcal{X} \times \mathcal{Y}$ ,  $x \mapsto (x, f(x))$ . Insofern haben wir mit den Graphen  $G_f$  der Abbildungen 16 bzw. 15 auch schon Beispiele für *Bilder* von Funktionen von einem 1- bzw. 2-dimensionalen Definitionsbereich  $\mathcal{X}$  in den 3-dimensionalen Zielbereich  $\mathcal{X} \times \mathcal{Y} \subset \mathbb{R}^3$  gesehen.

Als nächstes führen wir Konzepte im Umfeld der gerade schon diskutierten Begriffe Bild und Graph präzise und allgemein ein:

**Definitionen (Bilder, Urbilder, Graphen).** Sei  $f: \mathcal{X} \rightarrow \mathcal{Y}$  eine Abbildung von einer Menge  $\mathcal{X}$  in eine Menge  $\mathcal{Y}$ .

(I) Das **Bild einer Teilmenge**  $A \subset \mathcal{X}$  unter  $f$  erklärt man als

$$f(A) := \{y \in \mathcal{Y} \mid \exists x \in A: f(x) = y\} \subset \mathcal{Y}.$$

Oft wird dies auch (etwas informeller) als  $f(A) = \{f(x) \mid x \in A\}$  geschrieben. Für einzelne  $x \in \mathcal{X}$  ist das Bild  $f(\{x\}) = \{f(x)\}$ . Speziell heißt  $\text{Bild}(f) := f(\mathcal{X}) \subset \mathcal{Y}$  das **Bild der Abbildung**  $f$ .

(II) Das **Urbild einer Teilmenge**  $B \subset \mathcal{Y}$  unter  $f$  erklärt man als

$$f^{-1}(B) := \{x \in \mathcal{X} \mid f(x) \in B\} \subset \mathcal{X}.$$

Für einzelne  $y \in \mathcal{Y}$  gilt damit<sup>3</sup>  $f^{-1}(\{y\}) = \{x \in \mathcal{X} \mid f(x) = y\}$ . Die definierende Eigenschaft der Abbildung erzwingt generell  $f^{-1}(\mathcal{Y}) = \mathcal{X}$  und auch  $f^{-1}(\text{Bild}(f)) = \mathcal{X}$ .

(III) Den (**Funktions-**)**Graph**  $G_f$  von  $f$  erklärt man als

$$G_f := \{(x, y) \in \mathcal{X} \times \mathcal{Y} \mid f(x) = y\} \subset \mathcal{X} \times \mathcal{Y}.$$

Oft wird dies auch (etwas informeller) als  $G_f = \{(x, f(x)) \mid x \in \mathcal{X}\}$  geschrieben, und anstelle von  $G_f$  notiert man gleichbedeutend auch  $\text{Graph}(f)$ .

<sup>3</sup>In mancher Literatur wird für das Urbild  $f^{-1}(\{y\})$  auch  $f^{-1}(y)$  geschrieben. Wir vermeiden dies aber fürs Erste, um Verwechslungen mit der demnächst eingeführten Umkehrfunktion  $f^{-1}$  vorzubeugen.

Eine Veranschaulichung des Bilds  $f(A)$  und des Urbilds  $f^{-1}(B)$  gelingt in einfachen Fällen wie in Abbildung 17.

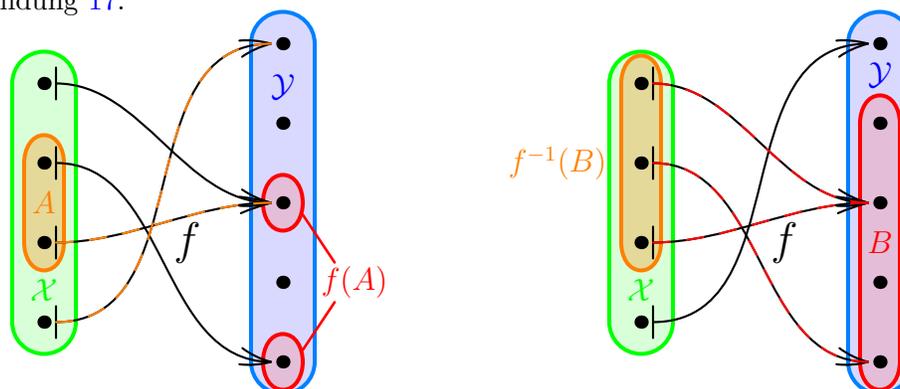


Abb. 17: Bild  $f(A)$  von  $A \subset \mathcal{X}$  und Urbild  $f^{-1}(B)$  von  $B \subset \mathcal{Y}$  unter einer Abbildung  $f: \mathcal{X} \rightarrow \mathcal{Y}$

**Bemerkungen** (zu Bildern, Urbildern und Graphen).

- (1) Das Bild einer Abbildung  $f: \mathcal{X} \rightarrow \mathcal{Y}$  ist die Menge  $B$  mit den wenigsten möglichen Elementen, so dass noch  $G_f \subset \mathcal{X} \times B$  gilt. Das Bild *kann* eine *echte* Teilmenge des Ziels sein.
- (2) Für eine Abbildung  $f: \mathcal{X} \rightarrow \mathcal{Y}$  und  $A \subset \mathcal{X}$ ,  $B \subset \mathcal{Y}$  sagt man,  $f$  bilde (Elemente) von  $A$  *nach*  $B$  ab, wenn  $f(A) \subset B$  gilt. Stärker sagt man,  $f$  bilde  $A$  *auf*  $B$  ab, wenn  $f(A) = B$  gilt (wobei der Unterschied sich in der Präposition „auf“ anstelle von „nach“ niederschlägt). Insbesondere bildet  $f$  immer von  $\mathcal{X}$  *nach*  $\mathcal{Y}$  und  $\mathcal{X}$  *auf*  $f(\mathcal{X}) = \text{Bild}(f)$  ab.
- (3) Manchmal spricht man bei einer Abbildung auch vom Wertebereich/Bildbereich und meint entweder Bild oder Ziel. Wir vermeiden diese Begriffe aufgrund der Doppeldeutigkeit vorerst.
- (4) **Achtung!** Obwohl das Urbild mit dem Symbol  $f^{-1}(\dots)$  notiert wird, ist das Urbild auch in Fällen definiert, in denen die demnächst eingeführte Umkehrfunktion  $f^{-1}$  *nicht* existiert.

Erste Regeln für (Ur-)Bilder lesen wir direkt aus den Definitionen ab: Für  $A_1 \subset A_2 \subset \mathcal{X}$  gilt stets  $f(A_1) \subset f(A_2)$  und für  $B_1 \subset B_2 \subset \mathcal{Y}$  stets  $f^{-1}(B_1) \subset f^{-1}(B_2)$ . Des Weiteren gilt:

**Satz (Regeln für Bilder und Urbilder von Vereinigungen und Schnitten).** Sei  $f: \mathcal{X} \rightarrow \mathcal{Y}$  eine Abbildung von einer Menge  $\mathcal{X}$  in eine Menge  $\mathcal{Y}$ . Für Teilmengen  $A_1, A_2$  von  $\mathcal{X}$  und  $B_1, B_2$  von  $\mathcal{Y}$  gelten dann stets:

$$\begin{aligned} f(A_1 \cup A_2) &= f(A_1) \cup f(A_2), & f(A_1 \cap A_2) &\subset f(A_1) \cap f(A_2), \\ f^{-1}(B_1 \cup B_2) &= f^{-1}(B_1) \cup f^{-1}(B_2), & f^{-1}(B_1 \cap B_2) &= f^{-1}(B_1) \cap f^{-1}(B_2). \end{aligned}$$

Dass beim Bild des Schnitts tatsächlich nur „ $\subset$ “ und nicht „ $=$ “ gelten kann, sieht man schon an einer Abbildung  $f: \{a_1, a_2\} \rightarrow \{y\}$  mit  $a_1 \neq a_2$ , denn dann ist  $f(\{a_1\} \cap \{a_2\}) = f(\emptyset) = \emptyset$ , aber  $f(\{a_1\}) \cap f(\{a_2\}) = \{f(a_1)\} \cap \{f(a_2)\} = \{f(y)\} \cap \{f(y)\} = \{f(y)\}$ .

Zum Beweis des Satzes nutzen wir typische Techniken, um Mengen-Inklusionen und Mengengleichheiten nachzuweisen:

*Beweis.* Wir behandeln erst das Bild der Vereinigung: Für  $i \in \{1, 2\}$  gilt  $A_1 \cup A_2 \supset A_i$ , nach Vorbemerkung zum Satz dann auch  $f(A_1 \cup A_2) \supset f(A_i)$  und daher  $f(A_1 \cup A_2) \supset f(A_1) \cup f(A_2)$ .

Als Nächstes zeigen wir die umgekehrte Inklusion  $f(A_1 \cup A_2) \subset f(A_1) \cup f(A_2)$  gemäß Definition der Inklusion: Sei  $y \in f(A_1 \cup A_2)$ . Nach Definition des Bilds gibt es dann  $x \in A_1 \cup A_2$  mit  $f(x) = y$ . Dabei ist  $x \in A_1$  oder  $x \in A_2$ . Im ersten Fall folgt  $y = f(x) \in f(A_1)$ , im zweiten Fall  $y = f(x) \in f(A_2)$ . In beiden Fällen gilt also  $y \in f(A_1) \cup f(A_2)$ . Damit ist die Inklusion  $f(A_1 \cup A_2) \subset f(A_1) \cup f(A_2)$  und insgesamt auch  $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$  gezeigt.

Beim Bild des Schnitts erhält man aus  $A_1 \cap A_2 \subset A_i$  für  $i \in \{1, 2\}$  mit der Vorbemerkung  $f(A_1 \cup A_2) \subset f(A_i)$  und insgesamt  $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$ .

Die Regel für das Urbild der Vereinigung ergibt sich durch schrittweise Äquivalenzumformung<sup>4</sup> mit der Definition von Urbild und Vereinigung durch

$$\begin{aligned} x \in f^{-1}(B_1 \cup B_2) &\iff f(x) \in B_1 \cup B_2 \iff (f(x) \in B_1) \vee (f(x) \in B_2) \\ &\iff (x \in f^{-1}(B_1)) \vee (x \in f^{-1}(B_2)) \iff x \in f^{-1}(B_1) \cup f^{-1}(B_2) \end{aligned}$$

für  $x \in \mathcal{X}$ . Beim Urbild des Schnitts geht man analog vor (mit  $\cap$  statt  $\cup$  und  $\wedge$  statt  $\vee$ ).  $\square$

Sehr wichtige Eigenschaften von Abbildungen, die ab jetzt immer wieder auftreten, sind:

**Definitionen (Abbildungseigenschaften).** Sei  $f: \mathcal{X} \rightarrow \mathcal{Y}$  eine Abbildung von einer Menge  $\mathcal{X}$  in eine Menge  $\mathcal{Y}$ .

- (I) Man nennt  $f$  **injektiv** oder eine **Injektion**, wenn zu jedem  $y \in \mathcal{Y}$  höchstens ein  $x \in \mathcal{X}$  mit  $f(x) = y$  existiert, mit anderen Worten also, wenn für alle  $x, \tilde{x} \in \mathcal{X}$  die Implikation

$$f(\tilde{x}) = f(x) \implies \tilde{x} = x$$

gilt. Man nennt injektive Abbildungen auch Einbettungen und zeigt Injektivität von  $f$  gelegentlich durch die Notation  $f: \mathcal{X} \hookrightarrow \mathcal{Y}$  an.

- (II) Man nennt  $f$  **surjektiv** oder eine **Surjektion**, wenn zu jedem  $y \in \mathcal{Y}$  mindestens ein  $x \in \mathcal{X}$  mit  $f(x) = y$  existiert, mit anderen Worten also, wenn  $\text{Bild}(f) = \mathcal{Y}$  gilt. Gelegentlich zeigt man Surjektivität von  $f$  durch die Notation  $f: \mathcal{X} \twoheadrightarrow \mathcal{Y}$  an.

- (III) Man nennt  $f$  **bijektiv** oder eine **Bijektion**, wenn zu jedem  $y \in \mathcal{Y}$  genau ein  $x \in \mathcal{X}$  mit  $f(x) = y$  existiert, mit anderen Worten also, wenn  $f$  sowohl injektiv als auch surjektiv ist.

In **graphischen Darstellungen mit Zuordnungspfeilen** bedeuten Injektivität, Surjektivität bzw. Bijektivität, dass bei jedem Element des Ziels  $\mathcal{Y}$  höchstens ein, mindestens ein bzw. genau ein Pfeil endet. Für Definitions- und Zielbereiche  $\mathcal{Y}$  mit endlich vielen Elementen wird dies in den oberen Bildern der Abbildung 18 dargestellt. Wenn nicht alle (eventuell unendlich vielen) Elemente und/oder Zuordnungspfeile graphisch dargestellt werden können, gilt das Gesagte sinngemäß für alle prinzipiell in Frage kommenden Elemente und Pfeile.

Auch **am Graph**  $G_f$  einer Funktion  $f: \mathcal{X} \rightarrow \mathcal{Y}$  mit  $\mathcal{X} \subset \mathbb{R}$  und  $\mathcal{Y} \subset \mathbb{R}$  kann man die Abbildungseigenschaften ablesen, was beispielhaft in den unteren Bildern der Abbildung 18 gezeigt wird: Injektivität bedeutet, dass sich auf jeder horizontalen Geraden in einer „Höhe“  $y \in \mathcal{Y}$  höchstens ein Punkt von  $G_f$  befindet. (Dies kann sich in gutartigen Fällen nur so manifestieren, dass die Graphenkurve  $G_f$  von links nach rechts durchgehend steigt oder fällt.) Surjektivität liegt vor, wenn es auch immer mindestens einen solchen Punkt gibt, also jede horizontale Gerade einer „Höhe“  $y \in \mathcal{Y}$  den Graph  $G_f$  tatsächlich trifft. Bijektivität erfordert beides zusammen.

<sup>4</sup>Aneinandergereihte Äquivalenzen  $S_1 \iff S_2 \iff S_3 \iff \dots \iff S_{n-1} \iff S_n$  für Aussagen  $S_1, S_2, \dots, S_n$  verwenden wir ab jetzt immer als abkürzende Schreibweise mit der auch bei Äquivalenzumformungen verbreiteten Bedeutung, dass die auftretenden Aussagen wechselseitig äquivalent sind. In der ursprünglichen Notation der Aussagenlogik müssten wir hierfür streng genommen  $(S_1 \iff S_2) \wedge (S_2 \iff S_3) \wedge \dots \wedge (S_{n-1} \iff S_n)$  schreiben.

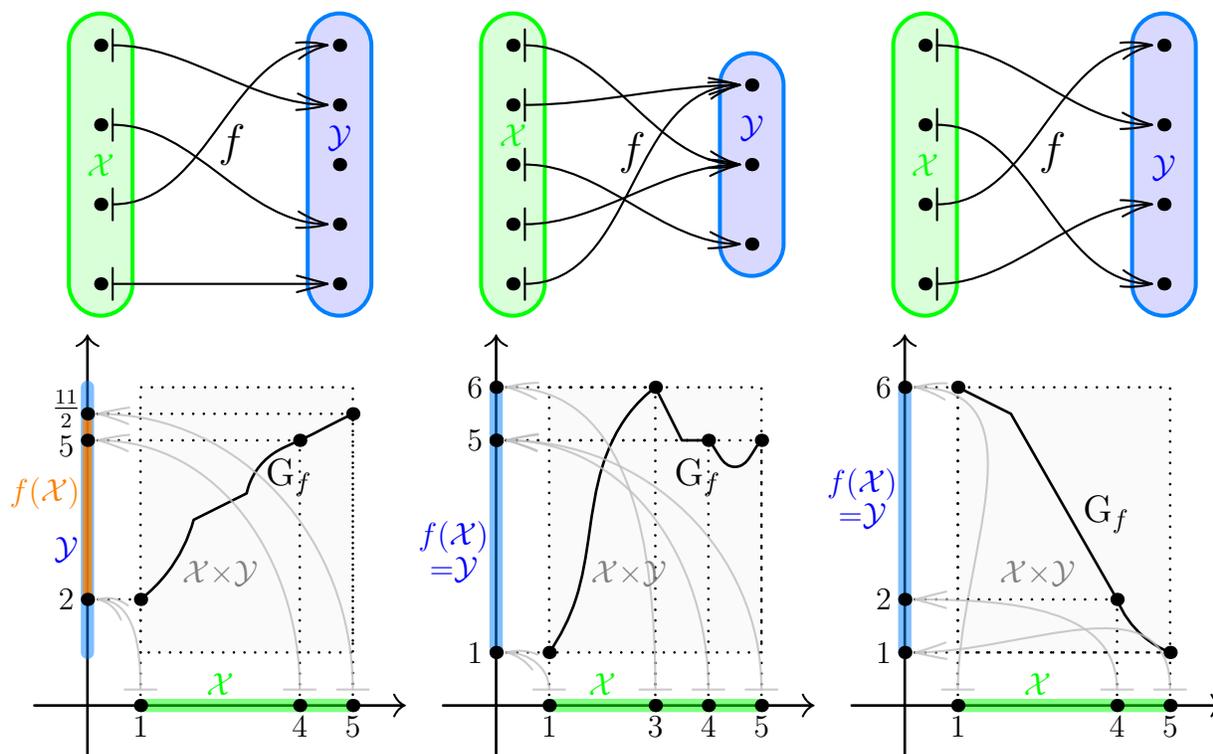


Abb. 18: Injektionen (links), Surjektionen (mittig) und Bijektionen (rechts)  $f: \mathcal{X} \rightarrow \mathcal{Y}$  für endliche Mengen  $\mathcal{X}$  und  $\mathcal{Y}$  (oben) und in Graphendarstellung für  $\mathcal{X} = \{x \in \mathbb{R} \mid 1 \leq x \leq 5\}$  und  $\mathcal{Y} = \{y \in \mathbb{R} \mid 1 \leq y \leq 6\}$  (unten), links unten mit Bild  $f(\mathcal{X}) = \{y \in \mathbb{R} \mid 2 \leq y \leq \frac{11}{2}\} \subsetneq \mathcal{Y}$

**Bemerkungen** (zu Injektionen, Surjektionen und Bijektionen).

- (1) Ob eine Abbildung injektiv/surjektiv/bijektiv ist, hängt auch bei (wie in der Schule) durch Funktionsterme gegebenen Funktionen entscheidend davon ab, mit welchem Definitionsbereich und Ziel diese betrachtet werden.
- (2) Für eine **Injektion**, **Surjektion** bzw. **Bijektion**  $\mathcal{X} \rightarrow \mathcal{Y}$  zwischen Mengen  $\mathcal{X}$  und  $\mathcal{Y}$  mit endlich vielen Elementen ist zwingend erforderlich, dass  $\mathcal{Y}$  **mindestens so viele, höchstens so viele bzw. genau so viele Elemente** enthält wie  $\mathcal{X}$ .

In Fällen mit unendlich vielen Elementen kann man natürlich nicht durchzählen. Wie in Abschnitt 2.5 noch Thema sein wird, kann man aber auch die „Größe“ von Mengen mit unendlich vielen Elementen zu einem gewissen Grad über Injektionen, Surjektionen, Bijektionen vergleichen.

- (3) Aus einer beliebigen Abbildung  $f: \mathcal{X} \rightarrow \mathcal{Y}$  kann man durch Verkleinerung des Ziels stets die Surjektion  $\tilde{f}: \mathcal{X} \rightarrow \text{Bild}(f)$  mit  $\tilde{f}(x) := f(x)$  für alle  $x \in \mathcal{X}$  gewinnen. Ist  $f$  surjektiv, so ist dabei  $\tilde{f} = f$ . Ist  $f$  injektiv, so ist  $\tilde{f}$  sogar bijektiv.
- (4) Bei einer **Bijektion**  $f: \mathcal{X} \rightarrow \mathcal{Y}$  erfolgt eine **Eins-zu-eins-Zuordnung** (der Elemente) von  $\mathcal{X}$  und  $\mathcal{Y}$ , bei einer Injektion entsprechend eine Eins-zu-eins-Zuordnung (der Elemente) von  $\mathcal{X}$  und  $\text{Bild}(f)$ . Manchmal nutzt man dies, um die einander zugeordneten Mengen und Elemente vollständig miteinander zu identifizieren.

**Beispiele** (von Injektionen und Surjektionen). Bei den zuvor betrachteten Beispielen von Abbildungen liegen folgende Eigenschaften vor:

- Die Abbildungen  $f$  aus den Beispielen (2) und (3) sind injektiv, aber nicht surjektiv.
- Dagegen ist  $f$  aus Beispiel (5) surjektiv, aber (z.B. wegen  $f(1) = 0 = f(0)$ ) nicht injektiv.
- Die Abbildungen  $f$  der Beispiele (1), (4) und (6) sind weder injektiv noch surjektiv. (Bei der Additions-Abbildung  $f$  des Beispiels (4) scheitert Surjektivität aber insofern nur knapp, dass  $\text{Bild}(f) = \mathbb{N} \setminus \{1\}$  sich nur um das eine Element 1 vom Ziel  $\mathbb{N}$  unterscheidet.)

Die Abbildungseigenschaften werden von nun immer wieder auftreten und häufig eine wichtige Rolle spielen. Eng verbunden mit Bijektivität ist folgender Begriff:

**Definition (Umkehrfunktionen).** Seien  $\mathcal{X}$  und  $\mathcal{Y}$  Mengen sowie  $f: \mathcal{X} \rightarrow \mathcal{Y}$  eine Abbildung. Eine Abbildung  $g: \mathcal{Y} \rightarrow \mathcal{X}$  heißt **Umkehrfunktion** oder **Umkehrabbildung** von/zu  $f$ , wenn folgende Äquivalenz für alle  $x \in \mathcal{X}$  und  $y \in \mathcal{Y}$  gilt:

$$f(x) = y \iff g(y) = x.$$

Prinzipiell bedeutet dies nichts anderes, als dass die Umkehrfunktion aus der Funktion durch Umkehrung aller Zuordnungspfeile entsteht. Diese für das Konzept entscheidende Anschauung wird in einem einfachen Fall durch Abbildung 19 verdeutlicht. Bei einer Funktion  $f: \mathcal{X} \rightarrow \mathcal{Y}$  von  $\mathcal{X} \subset \mathbb{R}$  nach  $\mathcal{Y} \subset \mathbb{R}$  geht der Graph  $G_g = \{(y, x) \in \mathbb{R}^2 \mid (x, y) \in G_f\}$  der Umkehrfunktion  $g: \mathcal{Y} \rightarrow \mathcal{X}$  wie in Abbildung 20 aus dem Graph  $G_f$  von  $f$  durch Spiegelung an der ersten Winkelhalbierenden des Koordinatensystems hervor.

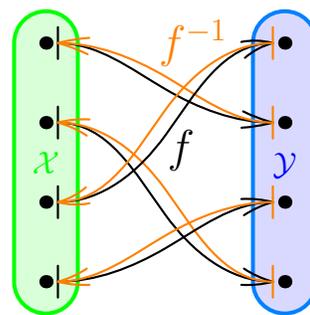


Abb. 19: Die Umkehrabbildung  $f^{-1}: \mathcal{Y} \rightarrow \mathcal{X}$  einer Bijektion  $f: \mathcal{X} \rightarrow \mathcal{Y}$

**Bemerkung & Notation** (zu/für Umkehrfunktionen). Seien  $\mathcal{X}$  und  $\mathcal{Y}$  Mengen. Falls überhaupt eine Umkehrfunktion zu  $f: \mathcal{X} \rightarrow \mathcal{Y}$  existiert, ist diese eindeutig bestimmt und wird mit  $f^{-1}: \mathcal{Y} \rightarrow \mathcal{X}$  bezeichnet.

*Beweis der Eindeutigkeit.* Für zwei Umkehrfunktionen  $g: \mathcal{Y} \rightarrow \mathcal{X}$  und  $\tilde{g}: \mathcal{Y} \rightarrow \mathcal{X}$  zu  $f$  ergibt die Definition  $g(y) = x \iff \tilde{g}(y) = x$  für alle  $x \in \mathcal{X}, y \in \mathcal{Y}$ . Für  $y \in \mathcal{Y}$  führt die Wahl  $x := g(y) \in \mathcal{X}$  zur Äquivalenz  $g(y) = g(y) \iff \tilde{g}(y) = g(y)$ . Da die linke Seite trivial gilt, gilt auch  $\tilde{g}(y) = g(y)$  für alle  $y \in \mathcal{Y}$ , und damit ist  $\tilde{g} = g$ .  $\square$

**Bemerkung.** Die Notationen für Umkehrfunktion und Urbild sind insoweit konsistent, dass bei Existenz der Umkehrfunktion  $f^{-1}$  die Gleichheit  $f^{-1}(\{y\}) = \{f^{-1}(y)\}$  (mit Urbild links und Umkehrfunktion rechts) für alle  $y \in \mathcal{Y}$  gilt.

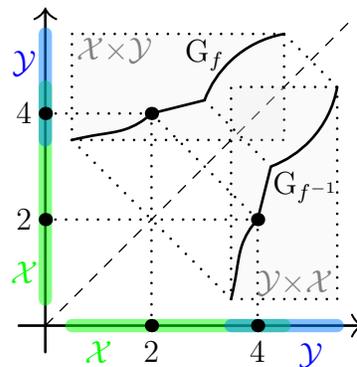


Abb. 20: Graphen  $G_f$  und  $G_{f^{-1}}$  von  $f: \mathcal{X} \rightarrow \mathcal{Y}$  und  $f^{-1}: \mathcal{Y} \rightarrow \mathcal{X}$  für  $\mathcal{X}, \mathcal{Y} \subset \mathbb{R}$

**Satz (Bijektivität entspricht Umkehrbarkeit).** Seien  $\mathcal{X}$  und  $\mathcal{Y}$  Mengen und  $f: \mathcal{X} \rightarrow \mathcal{Y}$  eine Abbildung. Dann gilt:

$$f \text{ ist bijektiv.} \iff \text{Es gibt eine Umkehrabbildung zu } f.$$

*Beweis.* „ $\implies$ “: Sei  $f$  bijektiv und sei  $y \in \mathcal{Y}$  beliebig. Zu  $y$  gibt es wegen der Bijektivität von  $f$  ein eindeutiges  $x \in \mathcal{X}$  mit  $f(x) = y$ . Wir definieren eine Abbildung  $g: \mathcal{Y} \rightarrow \mathcal{X}$  durch die Festlegung  $g(y) := x$  für beliebiges  $y \in \mathcal{Y}$  und das erwähnte eindeutig zugehörige  $x$  mit  $f(x) = y$ . Damit gilt offensichtlich die Äquivalenz  $f(x) = y \iff g(y) = x$  für alle  $x \in \mathcal{X}$  und  $y \in \mathcal{Y}$ , also ist  $g$  eine Umkehrabbildung zu  $f$ .

„ $\impliedby$ “: Sei  $g: \mathcal{Y} \rightarrow \mathcal{X}$  eine Umkehrabbildung zu  $f$  und sei  $y \in \mathcal{Y}$  beliebig. Per definierender Eigenschaft der Abbildung  $g$  gibt es zu  $y$  genau ein  $x \in \mathcal{X}$  mit  $g(y) = x$ . Nach der Definition der Umkehrabbildung ist aber  $g(y) = x$  äquivalent zu  $f(x) = y$ . Also gibt es zu  $y$  auch genau ein  $x \in \mathcal{X}$  mit  $f(x) = y$ . Dies bedeutet per Definition, dass  $f$  bijektiv ist.  $\square$

Einige spezielle Abbildungen existieren für beliebige Mengen und können auch als weitere Beispiele von Abbildungen angesehen werden:

**Definitionen & Beispiele** (von speziellen Abbildungen).

- (1) Für jede Menge  $\mathcal{X}$  ist die **Identität** oder **identische Abbildung**  $\text{id}_{\mathcal{X}}: \mathcal{X} \rightarrow \mathcal{X}$  von  $\mathcal{X}$  durch  $\text{id}_{\mathcal{X}}(x) := x$  für alle  $x \in \mathcal{X}$  gegeben. Diese Abbildung nimmt die Zuordnung  $x \mapsto x$  für alle  $x \in \mathcal{X}$  vor, ordnet also — wie in Abbildung 21 — jedem Element von  $\mathcal{X}$  wieder das Element selbst zu. Die Identität ist stets bijektiv.

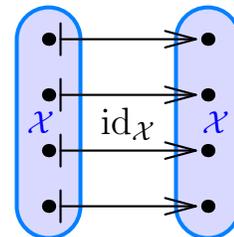


Abb. 21: Die Identität einer Menge  $\mathcal{X}$  mit 4 Elementen

- (2) Für Mengen  $\mathcal{X}, \mathcal{Y}$  und ein **fixiertes** Element  $y \in \mathcal{Y}$  heißt  $\mathcal{X} \rightarrow \mathcal{Y}$ ,  $x \mapsto y$  die **konstante Abbildung** von  $\mathcal{X}$  nach  $\mathcal{Y}$  mit (konstantem Funktions-) Wert  $y$ . Ist  $f: \mathcal{X} \rightarrow \mathcal{Y}$  die konstante Abbildung mit Wert  $y$ , so notiert man<sup>5</sup>  $f \equiv y$  und liest dies als „ $f$  konstant gleich  $y$ “.
- (3) Für eine fixierte Teilmenge  $A \subset \mathcal{X}$  einer (Grund-)Menge  $\mathcal{X}$  wird die **charakteristische Funktion** oder **Indikatorfunktion**  $\mathbb{1}_A: \mathcal{X} \rightarrow \{0, 1\}$  der Menge  $A$  durch  $\mathbb{1}_A(x) := \begin{cases} 1 & \text{falls } x \in A \\ 0 & \text{falls } x \notin A \end{cases}$  für alle  $x \in \mathcal{X}$  definiert.

Etwas anders betrachtet kann man auch für ein fixiertes Element  $x \in \mathcal{X}$  einer (Grund-)Menge  $\mathcal{X}$  eine Abbildung  $\delta_x: \mathcal{P}(\mathcal{X}) \rightarrow \{0, 1\}$  durch  $\delta_x(A) := \mathbb{1}_A(x)$  für alle  $A \in \mathcal{P}(\mathcal{X})$  erhalten.

Wir kommen nun zu weiteren Grundoperationen mit Abbildungen:

**Definition (Komposition von Abbildungen).** Seien  $\mathcal{X}, \mathcal{Y}$  und  $\mathcal{Z}$  Mengen sowie  $f: \mathcal{X} \rightarrow \mathcal{Y}$  und  $g: \mathcal{Y} \rightarrow \mathcal{Z}$  Abbildungen. Dann ist die **Komposition**, auch **Verkettung** oder **Hintereinanderausführung** genannt, von  $f$  und  $g$  die Abbildung

$$g \circ f: \mathcal{X} \rightarrow \mathcal{Z}$$

mit

$$(g \circ f)(x) := g(f(x)) \quad \text{für alle } x \in \mathcal{X}.$$

**Beispiel.** Für  $f: \mathbb{N} \rightarrow \mathbb{Z}$  mit  $f(n) := 7 - 3n$  für  $n \in \mathbb{N}$  und  $g: \mathbb{Z} \rightarrow \mathbb{Q}$  mit  $g(z) := z^2 - 3z + 4^z$  für  $z \in \mathbb{Z}$  ist  $g \circ f: \mathbb{N} \rightarrow \mathbb{Q}$  durch  $(g \circ f)(n) = (7 - 3n)^2 - 3(7 - 3n) + 4^{7 - 3n}$  für  $n \in \mathbb{N}$  gegeben.

Anschaulich bedeutet die Komposition, dass man erst den Zuordnungen von  $f$ , dann denen von  $g$  folgt und auf diese Weise die Zuordnungen von  $g \circ f$  erhält; dazu vergleiche Abbildung 22.

<sup>5</sup>Das „normale“ Gleichheitszeichen wird an dieser Stelle bewusst vermieden, da die Abbildung  $f$  und das Element  $y$  des Zielbereichs verschiedene Objekte sind. Alternativ kann man  $f(x) = y$  für alle  $x \in \mathcal{X}$  ausschreiben und auf die Verwendung von „ $\equiv$ “ verzichten.

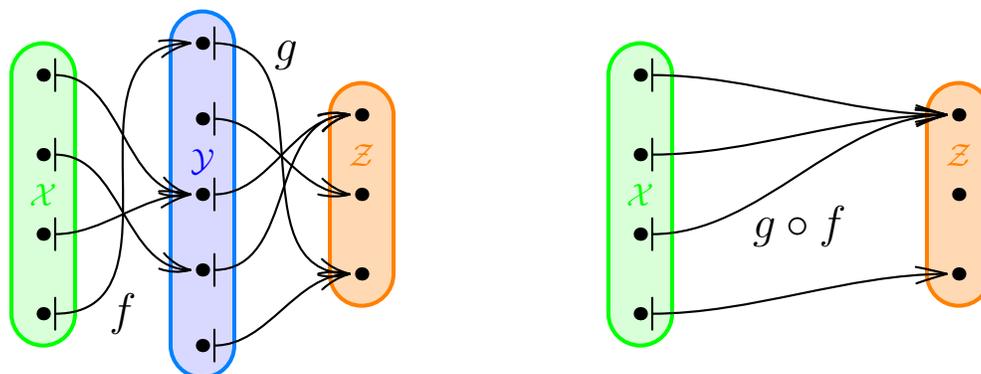


Abb. 22: Die Komposition  $g \circ f: \mathcal{X} \rightarrow \mathcal{Z}$  von  $f: \mathcal{X} \rightarrow \mathcal{Y}$  und  $g: \mathcal{Y} \rightarrow \mathcal{Z}$

Sowohl anschaulich einleuchtend als auch problemlos zu beweisen ist dann:

**Satz (über Assoziativität der Komposition).** Für Mengen  $\mathcal{W}, \mathcal{X}, \mathcal{Y}, \mathcal{Z}$  sowie Abbildungen  $f: \mathcal{W} \rightarrow \mathcal{X}$ ,  $g: \mathcal{X} \rightarrow \mathcal{Y}$  und  $h: \mathcal{Y} \rightarrow \mathcal{Z}$  gilt

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

*Beweis.* Für  $w \in \mathcal{W}$  ergibt sich mit der Definition der Komposition

$$((h \circ g) \circ f)(w) = (h \circ g)(f(w)) = h(g(f(w))) = h((g \circ f)(w)) = (h \circ (g \circ f))(w). \quad \square$$

**Bemerkung** (zur Nicht-Kommutativität der Komposition). Die Frage, ob die Komposition kommutativ ist, ob also  $g \circ f$  gleich  $f \circ g$  ist, macht nur für Selbstabbildungen  $f, g$  einer Menge  $\mathcal{X}$  Sinn. Die Antwort ist aber auch in diesem Fall im Allgemeinen „Nein!“. Zum Beispiel gilt für die konstanten Abbildungen  $f: \{0, 1\} \rightarrow \{0, 1\}$  mit  $f \equiv 0$  und  $g: \{0, 1\} \rightarrow \{0, 1\}$  mit  $g \equiv 1$  offensichtlich  $0 \equiv f \circ g \neq g \circ f \equiv 1$ .

Übrigens liegt selbst für bijektive  $f, g: \mathcal{X} \rightarrow \mathcal{X}$  im Allgemeinen keine Kommutativität vor: Zum Beispiel bei  $f, g: \{1, 2, 3\} \rightarrow \{1, 2, 3\}$  mit  $f(1) := 2$ ,  $f(2) := 1$ ,  $f(3) := 3$  und  $g(1) := 1$ ,  $g(2) := 3$ ,  $g(3) := 2$  ist  $3 = (g \circ f)(1) \neq (f \circ g)(1) = 2$ .

**Satz** (Abbildungseigenschaften und Komposition). Seien  $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$  Mengen sowie  $f: \mathcal{X} \rightarrow \mathcal{Y}$  und  $g: \mathcal{Y} \rightarrow \mathcal{Z}$  Abbildungen. Dann gelten:

$$\begin{array}{ll} f, g \text{ beide injektiv} \implies g \circ f \text{ injektiv,} & g \circ f \text{ injektiv} \implies f \text{ injektiv,} \\ f, g \text{ beide surjektiv} \implies g \circ f \text{ surjektiv,} & g \circ f \text{ surjektiv} \implies g \text{ surjektiv,} \\ f, g \text{ beide bijektiv} \implies g \circ f \text{ bijektiv,} & g \circ f \text{ bijektiv} \implies f \text{ injektiv, } g \text{ surjektiv.} \end{array}$$

*Beweis.* Die ersten beiden Zeilen werden in den Lernwerkstätten und Übungen behandelt. Die dritte folgt direkt daraus.  $\square$

**Definition (inverse Abbildungen).** Seien  $\mathcal{X}, \mathcal{Y}$  Mengen sowie  $f: \mathcal{X} \rightarrow \mathcal{Y}$  und  $g: \mathcal{Y} \rightarrow \mathcal{X}$  Abbildungen. Dann heißen  $f$  und  $g$  **zueinander invers** und  $g$  heißt **inverse Abbildung**, **inverse Funktion** oder kurz **Inverse** von/zu  $f$ , wenn gelten:

$$g \circ f = \text{id}_{\mathcal{X}} \quad \text{und} \quad f \circ g = \text{id}_{\mathcal{Y}}.$$

**Bemerkung** (zu Inversen). Seien  $\mathcal{X}, \mathcal{Y}$  Mengen. Falls überhaupt eine Inverse zu  $f: \mathcal{X} \rightarrow \mathcal{Y}$  existiert, ist diese eindeutig bestimmt.

*Beweis der Eindeutigkeit.* Sind  $g: \mathcal{Y} \rightarrow \mathcal{X}$  und  $\tilde{g}: \mathcal{Y} \rightarrow \mathcal{X}$  zwei Inverse zu  $f$ , so folgt

$$g = g \circ \text{id}_{\mathcal{Y}} = g \circ (f \circ \tilde{g}) = (g \circ f) \circ \tilde{g} = \text{id}_{\mathcal{X}} \circ \tilde{g} = \tilde{g}. \quad \square$$

Tatsächlich ist die Inverse nichts anderes als die Umkehrfunktion:

**Satz (Umkehrfunktionen sind dasselbe wie Inverse).** Seien  $\mathcal{X}, \mathcal{Y}$  Mengen. Genau dann ist  $g: \mathcal{Y} \rightarrow \mathcal{X}$  die Umkehrfunktion von  $f: \mathcal{X} \rightarrow \mathcal{Y}$ , wenn  $g$  die Inverse zu  $f$  ist.

*Beweis.* „ $\implies$ “: Ist  $g$  die Umkehrabbildung zu  $f$ , so ergibt Einsetzen von  $y = f(x)$  bzw.  $x = g(y)$  in der Definition, dass  $g(f(x)) = x$  für alle  $x \in \mathcal{X}$  und  $f(g(y)) = y$  für alle  $y \in \mathcal{Y}$  gelten. Damit ist  $g$  auch die Inverse zu  $f$ .

„ $\impliedby$ “: Ist  $g$  die Inverse zu  $f$ , so sind  $g \circ f = \text{id}_{\mathcal{X}}$  und  $f \circ g = \text{id}_{\mathcal{Y}}$  beide bijektiv. Nach dem vorigen Satz ist dann  $f$  injektiv und surjektiv, also auch bijektiv. Damit existiert die Umkehrfunktion  $f^{-1}$  von  $f$ . Nach „ $\implies$ “ ist  $f^{-1}$  invers zu  $f$ . Per Eindeutigkeit der Inversen ist  $g = f^{-1}$ , also ist  $g$  die Umkehrfunktion zu  $f$ .  $\square$

Insbesondere sind **Bijektivität, Umkehrbarkeit** (d.h. die Umkehrfunktion existiert) **und Invertierbarkeit** (d.h. die Inverse existiert) einer Abbildung alle drei **exakt gleichbedeutend**.

Zum Abschluss des Abschnitts sammeln wir noch einige weitere Grunddefinitionen bei Abbildungen ein. Zum Beispiel kann man den Definitionsbereich immer (künstlich) verkleinern und bei Werten in einem kartesischen Produkt in die sogenannten Komponenten aufspalten:

**Definition (Einschränkungen).** Seien  $\mathcal{X}, \mathcal{Y}$  Mengen. Die **Einschränkung** einer Abbildung  $f: \mathcal{X} \rightarrow \mathcal{Y}$  auf eine Teilmenge  $A$  des Definitionsbereichs  $\mathcal{X}$  ist die Abbildung

$$f|_A: A \rightarrow \mathcal{Y}$$

mit dem kleineren Definitionsbereich  $A$ , aber der auf diesem unveränderten Zuordnungsvorschrift  $f|_A(x) := f(x)$  für alle  $x \in A$ .

**Definitionen & Bemerkungen** (zu kartesischen Produkten und Abbildungen). Sei  $n \in \mathbb{N}$ , und seien  $\mathcal{X}, \mathcal{Y}, \mathcal{X}_1, \mathcal{Y}_1, \mathcal{X}_2, \mathcal{Y}_2, \dots, \mathcal{X}_n, \mathcal{Y}_n$  Mengen.

(1) Für  $i \in \{1, 2, \dots, n\}$  wird die ***i*-te Projektion**

$$p_i: \mathcal{X}_1 \times \mathcal{X}_2 \times \dots \times \mathcal{X}_n \rightarrow \mathcal{X}_i$$

des  $n$ -fachen kartesischen Produkts  $\mathcal{X}_1 \times \mathcal{X}_2 \times \dots \times \mathcal{X}_n$  durch die Festlegung  $p_i(x_1, x_2, \dots, x_n) := x_i$  für alle  $(x_1, x_2, \dots, x_n) \in \mathcal{X}_1 \times \mathcal{X}_2 \times \dots \times \mathcal{X}_n$  definiert; für  $n=2$  vgl. Abbildung 23. Es wird auch  $p_{\mathcal{X}_i}$  statt  $p_i$  notiert.

Auch allgemein nutzt man  $x_i$  mit  $i \in \{1, 2, \dots, n\}$  als Standard-Bezeichnung für den Eintrag  $p_i(x)$  des Tupels  $x \in \mathcal{X}_1 \times \mathcal{X}_2 \times \dots \times \mathcal{X}_n$ . Mit anderen Worten versteht man auch dann  $x = (x_1, x_2, \dots, x_n)$ , wenn die Einträge des Tupels  $x$  noch nicht explizit benannt wurden.

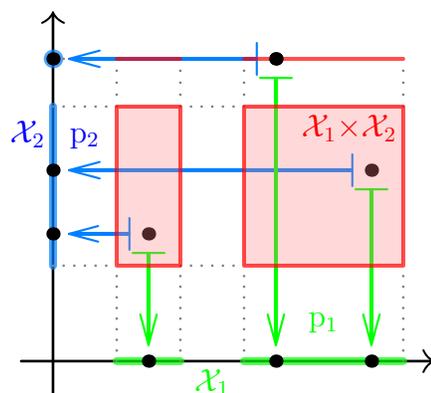


Abb. 23: Das Produkt  $\mathcal{X}_1 \times \mathcal{X}_2$  und die Projektionen  $p_1: \mathcal{X}_1 \times \mathcal{X}_2 \rightarrow \mathcal{X}_1$  und  $p_2: \mathcal{X}_1 \times \mathcal{X}_2 \rightarrow \mathcal{X}_2$  für  $\mathcal{X}_1, \mathcal{X}_2 \subset \mathbb{R}$

(2) *Eine Funktion*

$$f: \mathcal{X} \rightarrow \mathcal{Y}_1 \times \mathcal{Y}_2 \times \dots \times \mathcal{Y}_n$$

mit Werten im  $n$ -fachen kartesischen Produkt  $\mathcal{Y}_1 \times \mathcal{Y}_2 \times \dots \times \mathcal{Y}_n$  entspricht eins-zu-eins einzelnen Funktionen  $f_1: \mathcal{X} \rightarrow \mathcal{Y}_1$ ,  $f_2: \mathcal{X} \rightarrow \mathcal{Y}_2$ ,  $\dots$ ,  $f_n: \mathcal{X} \rightarrow \mathcal{Y}_n$  mit

$$f(x) = (f_1(x), f_2(x), \dots, f_n(x)) \quad \text{für alle } x \in \mathcal{X}.$$

Man nennt  $f_1, f_2, \dots, f_n$  die **Komponenten(funktionen)** von  $f$  und kann jedes  $f_i$  mit  $i \in \{1, 2, \dots, n\}$  als  $f_i = p_i \circ f$  mit der  $i$ -ten Projektion  $p_i$  von  $\mathcal{Y}_1 \times \mathcal{Y}_2 \times \dots \times \mathcal{Y}_n$  schreiben (woraus die Existenz und Eindeutigkeit von  $f_1, f_2, \dots, f_n$  zu gegebenem  $f$  klar wird).

In Analogie zu Elementen der (Ziel-)Mengen schreibt man die Funktion mit Komponenten  $f_1, f_2, \dots, f_n$  als  $(f_1, f_2, \dots, f_n)$  und verwendet  $f_1, f_2, \dots, f_n$  als Standard-Bezeichnungen für die Komponenten einer Funktion  $f$  mit Werten in  $\mathcal{Y}_1 \times \mathcal{Y}_2 \times \dots \times \mathcal{Y}_n$ .

Besonders häufig arbeitet man im Fall  $\mathcal{Y}_1 = \mathcal{Y}_2 = \dots = \mathcal{Y}_n = \mathcal{Y}$ , also für eine Funktion

$$f: \mathcal{X} \rightarrow \mathcal{Y}^n,$$

mit den  $n$  Komponentenfunktionen  $f_1, f_2, \dots, f_n: \mathcal{X} \rightarrow \mathcal{Y}$  der Funktion  $f$ .

- (3) Die **Diagonalabbildung**  $\mathcal{X} \rightarrow \mathcal{X}^n$ ,  $x \mapsto (x, x, \dots, x)$  kann auch als die Abbildung  $(\text{id}_{\mathcal{X}}, \text{id}_{\mathcal{X}}, \dots, \text{id}_{\mathcal{X}}): \mathcal{X} \rightarrow \mathcal{X}^n$ , deren Komponenten alle  $\text{id}_{\mathcal{X}}$  sind, geschrieben werden. Sie ist stets injektiv.
- (4) Das **kartesische Produkt von Abbildungen**  $f_1: \mathcal{X}_1 \rightarrow \mathcal{Y}_1$ ,  $f_2: \mathcal{X}_2 \rightarrow \mathcal{Y}_2$  ist die Abbildung  $f_1 \times f_2: \mathcal{X}_1 \times \mathcal{X}_2 \rightarrow \mathcal{Y}_1 \times \mathcal{Y}_2$ , die durch  $(f_1 \times f_2)(x_1, x_2) := (f_1(x_1), f_2(x_2))$  für alle  $(x_1, x_2) \in \mathcal{X}_1 \times \mathcal{X}_2$  definiert wird. Die Komponenten von  $f_1 \times f_2$  sind  $p_{\mathcal{Y}_1} \circ (f_1 \times f_2) = f_1 \circ p_{\mathcal{X}_1}: \mathcal{X}_1 \times \mathcal{X}_2 \rightarrow \mathcal{Y}_1$  und  $p_{\mathcal{Y}_2} \circ (f_1 \times f_2) = f_2 \circ p_{\mathcal{X}_2}: \mathcal{X}_1 \times \mathcal{X}_2 \rightarrow \mathcal{Y}_2$  mit den Projektionen  $p_{\mathcal{X}_1}, p_{\mathcal{X}_2}$  und  $p_{\mathcal{Y}_1}, p_{\mathcal{Y}_2}$  der kartesischen Produkte  $\mathcal{X}_1 \times \mathcal{X}_2$  und  $\mathcal{Y}_1 \times \mathcal{Y}_2$ . Die Produkt-Bildung  $\times$  bei Abbildungen ist assoziativ und ist analog für eine beliebige endliche Zahl von Funktionen (statt zweien) sinnvoll.

Als letztes besprechen wir noch kurz Mengen von Abbildungen:

**Definition (Mengen von Abbildungen).** Sind  $\mathcal{X}, \mathcal{Y}$  Mengen, so schreiben wir  $\text{Abb}(\mathcal{X}, \mathcal{Y})$  oder  $\mathcal{Y}^{\mathcal{X}}$  für die **Menge der Abbildungen von  $\mathcal{X}$  nach  $\mathcal{Y}$** . Speziell im Fall  $\mathcal{X} = \mathcal{Y}$  von Selbstabbildungen kürzen wir gelegentlich  $\text{Abb}(\mathcal{X}) := \text{Abb}(\mathcal{X}, \mathcal{X})$  ab.

**Bemerkungen** (zur Identifikation von (Mengen von) Abbildungen). Sei  $n \in \mathbb{N}$ , und seien  $\mathcal{X}, \mathcal{Y}, \mathcal{Y}_1, \mathcal{Y}_2, \dots, \mathcal{Y}_n$  Mengen.

- (1) Für jeden **Definitionsbereich**  $\mathcal{X} = \{x_1, x_2, \dots, x_n\}$  mit genau  $n$  verschiedenen **Elementen**  $x_1, x_2, \dots, x_n$  ist

$$\text{Abb}(\mathcal{X}, \mathcal{Y}) \rightarrow \mathcal{Y}^n, f \mapsto (f(x_1), f(x_2), \dots, f(x_n))$$

eine Bijektion. Daher kann man eine Abbildung  $f \in \text{Abb}(\mathcal{X}, \mathcal{Y})$  auf dem  $n$ -elementigen Definitionsbereich  $\mathcal{X}$  auch als  $n$ -Tupel  $(f(x_1), f(x_2), \dots, f(x_n)) \in \mathcal{Y}^n$  ihrer Werte betrachten und bekommt in diesem Fall eine naheliegende **Identifikation von  $\text{Abb}(\mathcal{X}, \mathcal{Y})$  mit  $\mathcal{Y}^n$** . In Anlehnung hieran kann man sich eine Abbildung  $f \in \text{Abb}(\mathbb{N}, \mathcal{Y})$  mit Definitionsbereich  $\mathbb{N}$  als „unendliches Tupel“  $(f(x_1), f(x_2), f(x_3), \dots)$  ihrer Werte vorstellen — ein Objekt, das wir so nicht definiert haben, das aber für  $\text{Abb}(\mathbb{N}, \mathcal{Y})$  die Schreibweise  $\mathcal{Y}^{\mathbb{N}}$  nahelegt. Hierdurch wird für  $\text{Abb}(\mathcal{X}, \mathcal{Y})$  auch bei allgemeinen Definitionsbereich  $\mathcal{X}$  die in der vorigen Definition eingeführte und an eine Potenz erinnernde Schreibweise  $\mathcal{Y}^{\mathcal{X}}$  motiviert.

- (2) Der oben erwähnten Eins-zu-Eins-Entsprechung zwischen Funktionen mit Werten in Produkt  $\mathcal{Y}_1 \times \mathcal{Y}_2 \times \dots \times \mathcal{Y}_n$  und dem Tupel ihrer Komponentenfunktionen liegt tatsächlich eine Bijektion

$$\text{Abb}(\mathcal{X}, \mathcal{Y}_1 \times \mathcal{Y}_2 \times \dots \times \mathcal{Y}_n) \rightarrow \text{Abb}(\mathcal{X}, \mathcal{Y}_1) \times \text{Abb}(\mathcal{X}, \mathcal{Y}_2) \times \dots \times \text{Abb}(\mathcal{X}, \mathcal{Y}_n)$$

oder mit anderen Worten (und vielleicht intuitiver)

$$(\mathcal{Y}_1 \times \mathcal{Y}_2 \times \dots \times \mathcal{Y}_n)^{\mathcal{X}} \rightarrow \mathcal{Y}_1^{\mathcal{X}} \times \mathcal{Y}_2^{\mathcal{X}} \times \dots \times \mathcal{Y}_n^{\mathcal{X}}$$

zugrunde, die die Zuordnung  $f \mapsto (f_1, f_2, \dots, f_n)$  vornimmt (mit den Komponenten  $f_i$  von  $f$ ). Dies ermöglicht eine häufig verwendete Identifikation, die wir teils in die Notation für die Komponenten eingebaut haben. Deutlicher noch sieht man dies an der zugehörigen Umkehrabbildung, die  $(f_1, f_2, \dots, f_n) \mapsto (f_1, f_2, \dots, f_n)$  zuordnet, wobei das Tupel der Einzelfunktionen  $f_1, f_2, \dots, f_n$  (links) und die Funktion mit Komponenten  $f_1, f_2, \dots, f_n$  (rechts) in unserer Notation nicht mehr unterscheidbar sind.

## 2.2 Natürliche und ganze Zahlen, Induktion und Rekursion

Natürlich wurde die Menge  $\mathbb{N} = \{1, 2, 3, \dots\}$  der natürlichen Zahlen bereits verwendet und ist Ihnen geläufig. Dennoch möchte man  $\mathbb{N}$  in der Mathematik präziser als durch eine Auflistung mit Pünktchen einführen, und prinzipiell kann man den Aufbau der Mathematik dann auch so gestalten, dass  $\mathbb{N}$  vor seiner Einführung nicht vorkommt. (Die Einhaltung einer derartigen konsequenten Reihenfolge wäre aber an vielen Stellen so umständlich, dass dies für eine Vorlesung nicht in Frage kommt.) Die präzise Einführung von  $\mathbb{N}$  mag zunächst penibel und überflüssig scheinen, wird aber den richtigen Rahmen für das **wichtige Beweisverfahren der vollständigen Induktion, rekursive Definitionen** und die Eingrenzung der entscheidenden Eigenschaften von  $\mathbb{N}$  bieten. Tatsächlich fordern wir zur Einführung von  $\mathbb{N}$  folgendes Axiom:

**Axiom (Peano-Axiome der natürlichen Zahlen).** *Es gibt eine Menge  $\mathbb{N}$ , eine injektive Abbildung  $S: \mathbb{N} \rightarrow \mathbb{N}$  und ein Element  $1 \in \mathbb{N} \setminus S(\mathbb{N})$ , so dass für alle Teilmengen  $M$  von  $\mathbb{N}$  gilt: Ist  $1 \in M$  und  $S(M) \subset M$ , so folgt  $M = \mathbb{N}$ .*

Es handelt sich hierbei um eine kurze und prägnante Zusammenfassung eines fünf separate Axiome umfassenden Axiomensystems, das auf G. Peano (1858–1932) zurückgeht. Wir diskutieren die Original-Axiome und erläutern damit zugleich das Vorausgehende:

- Die erste Forderung  $1 \in \mathbb{N}$  sichert überhaupt die **Existenz einer natürlichen Zahl 1**.
- Das zweite Axiom postuliert für jede natürliche Zahl  $n \in \mathbb{N}$  die **Existenz und Eindeutigkeit eines Nachfolgers**  $S(n) \in \mathbb{N}$ , den wir normalerweise als  $n+1$  bezeichnen. Dieses Axiom ist oben in der Wohldefiniertheit der Abbildung  $S: \mathbb{N} \rightarrow \mathbb{N}$  enthalten.
- Das dritte Axiom  $1 \notin S(\mathbb{N})$  besagt, dass 1 nicht Nachfolger einer natürlichen Zahl ist und begründet die **herausgehobene Rolle der 1** als erste natürliche Zahl.
- Peanos viertes Axiom fordert  $S(m) = S(n) \implies m = n$  für alle  $m, n \in \mathbb{N}$ , entspricht oben der Injektivität von  $S$  und sichert die **Eindeutigkeit des Vorgängers** jeder natürlichen Zahl (sofern es überhaupt einen Vorgänger gibt).
- Das letzte Axiom schließlich enthält die oben gestellte Forderung für Teilmengen  $M$  von  $\mathbb{N}$  und kann in Worten so formuliert werden, dass aus  $1 \in M$  und der Gültigkeit der Implikation  $n \in M \implies S(n) \in M$  für alle  $n \in \mathbb{N}$  schon  $M = \mathbb{N}$  folgt. Dieses Postulat ist als **Induktionsaxiom** bekannt, sichert unter anderem, dass in  $\mathbb{N}$  nicht „zu viele“ Zahlen enthalten sind, und wird in Folge noch sehr genau diskutiert.

Natürlich beschreiben diese Axiome nichts anderes als die gewohnte Struktur der natürlichen Zahlen, wobei die **Sukzessions- oder Nachfolge-Abbildung**  $S$  in Abbildung 24 veranschaulicht wird, einfach dem „Weiterzählen“ von einer natürlichen Zahl zur nächsten entspricht und die formale Einführung der 1-stelligen Zahlen durch

$$2 := S(1), \quad 3 := S(2), \quad 4 := S(3), \quad 5 := S(4), \quad 6 := S(5), \quad 7 := S(6), \quad 8 := S(7), \quad 9 := S(8)$$

ermöglicht.

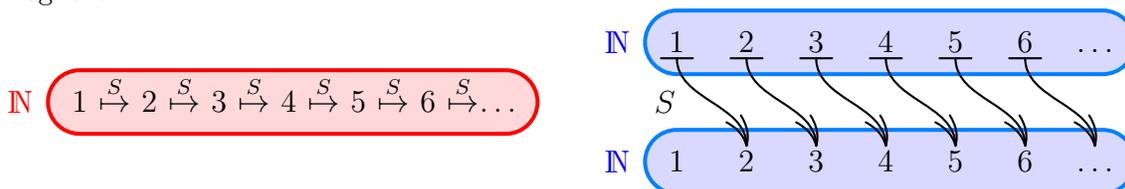


Abb. 24:  $\mathbb{N}$  und die Nachfolge-Abbildung  $S: \mathbb{N} \rightarrow \mathbb{N}$  (zwei Möglichkeiten der Veranschaulichung)

Auch wenn all dies mehr oder weniger vertraut scheinen mag, sei an dieser Stelle trotzdem die Warnung angebracht, dass bei  $\mathbb{N}$  als Menge mit unendlich vielen Elementen ganz anderes passieren kann als bei Mengen mit nur endlich vielen Elementen. So erhält man aus der Injektion  $S: \mathbb{N} \rightarrow \mathbb{N}$  zum einen die Bijektion  $\tilde{S}: \mathbb{N} \rightarrow S(\mathbb{N})$ , durch die man die Elemente von  $\mathbb{N}$  und  $S(\mathbb{N})$  eins-zu-eins identifizieren kann. Zum anderen ist aber doch  $S(\mathbb{N}) \subsetneq \mathbb{N}$ , denn  $\mathbb{N}$  enthält das Element 1 „mehr“ als  $S(\mathbb{N})$ . Genau diese paradox scheinende Eigenschaft des Unendlichen illustriert das **berühmte Gedankenspiel des Hilbert-Hotels**: In diesem Hotel gibt es unendlich viele Zimmer, für jede natürliche Zahl als Raumnummer eines. Sind alle Zimmer belegt, so ist dieses besondere Hotel aber dennoch nicht voll. Kommt nämlich in dieser Situation ein neuer Gast an, so bittet man alle bereits eingezogenen Gäste, aus ihrem derzeitigen Zimmer  $n$  in das Nachfolge-Zimmer  $S(n)$  zu ziehen, sozusagen entlang der Umzugswege im zweiten Bild der Abbildung 24. Damit wird Zimmer 1 frei und kann durch den neuen Gast bezogen werden.

Weitere Eigenschaften von  $\mathbb{N}$  (und  $S$ ) können wir aus den Axiomen folgern. Zum Beispiel sind bei  $\{n \in \mathbb{N} \mid S(n) \neq n\}$  gemäß dem dritten und vierten Axiom die Voraussetzungen des Induktionsaxioms erfüllt. Letzteres zeigt dann, dass die angegebene Menge ganz  $\mathbb{N}$  ist und sich daher **jedes  $n \in \mathbb{N}$  von seinem Nachfolger unterscheidet**. In ähnlicher Weise gibt die Anwendung des Induktionsaxioms auf  $S(\mathbb{N}) \cup \{1\}$  für jede Zahl  $n \in \mathbb{N}$  außer 1 die **Existenz eines Vorgängers**  $p \in \mathbb{N}$  mit  $S(p) = n$  (der gemäß dem vierten Axiom außerdem eindeutig ist). Schon hieran kann man die Wichtigkeit des Induktionsaxioms erkennen, auf das wir demnächst noch genau eingehen und ohne das man solche einleuchtenden Folgerungen tatsächlich nicht<sup>6</sup> zur Verfügung hätte.

Ist  $\mathbb{N}$  einmal eingeführt, so ist der Aufwand zur Definition von  $\mathbb{N}_0$  und  $\mathbb{Z}$  eher gering:

**Definition (natürliche Zahlen mit Null und ganze Zahlen).** Wir setzen

$$\mathbb{N}_0 := \mathbb{N} \cup \{0\}$$

mit einer fixierten Zahl  $0 \notin \mathbb{N}$  und

<sup>6</sup>Alle Peano-Axiome außer dem Induktionsaxiom sind auch für  $\mathbb{N}$  mit  $S(n) := n+2$  für alle ungeraden  $n \in \mathbb{N}$  und  $S(n) := n$  für alle geraden  $n \in \mathbb{N}$  erfüllt. In diesem Modell wären aber anders als üblich alle geraden Zahlen ihr eigener Nachfolger. Zudem sind die Peano-Axiome außer dem Induktionsaxiom auch für die positiven reellen Zahlen  $\mathbb{R}_+ := \{x \in \mathbb{R} \mid x > 0\}$  anstelle von  $\mathbb{N}$  mit  $S(x) := x+1$  für alle  $x \in \mathbb{R}_+$  erfüllt und ebenso für  $\mathbb{N}$  mit  $S(n) := n+2$  für alle  $n \in \mathbb{N}$ . Dabei gäbe es neben 1 aber weitere Zahlen, die keinen Vorgänger besitzen, zum Beispiel  $\frac{1}{2}$  im ersten und 2 im zweiten Fall.

$$\mathbb{Z} := \mathbb{N}_0 \dot{\cup} (-\mathbb{N})$$

mit einer „Kopie“<sup>7</sup>  $-\mathbb{N}$  von  $\mathbb{N}$ , so dass die Abbildung  $\mathbb{N} \rightarrow -\mathbb{N}$ , die jedem  $n \in \mathbb{N}$  ein neues Element  $-n \in (-\mathbb{N}) \setminus \mathbb{N}_0$  zuordnet, bijektiv ist. Wir nennen die Zahlen aus  $\mathbb{N}$  auch die positiven ganzen Zahlen, die aus  $-\mathbb{N}$  die negativen ganzen Zahlen. Das Negative  $-z \in \mathbb{Z}$  einer ganzen Zahl  $z \in \mathbb{Z}$  definieren wir ergänzend (nachdem es für positive  $z$  schon eingeführt ist) durch  $-0 := 0$  und  $-(-n) := n$  für  $n \in \mathbb{N}$ . Die Nachfolge-Abbildung setzen wir durch die Festlegungen  $S(0) := 1$ ,  $S(-1) := 0$  und  $S(-S(n)) := -n$  für  $n \in \mathbb{N}$  (natürlich unter Beibehalt von  $S(n)$  für  $n \in \mathbb{N}$ ) zu einer bijektiven Abbildung  $S: \mathbb{Z} \rightarrow \mathbb{Z}$  fort.

Wir halten fest, dass für jede Zahl  $z \in \mathbb{Z}$  ein eindeutiger Nachfolger  $S(z) \in \mathbb{Z}$  und ein eindeutiger Vorgänger  $S^{-1}(z) \in \mathbb{Z}$  (mit der Umkehrabbildung  $S^{-1}: \mathbb{Z} \rightarrow \mathbb{Z}$  der Bijektion  $S: \mathbb{Z} \rightarrow \mathbb{Z}$ ) existieren und  $S^{-1}(z) \neq z \neq S(z)$  erfüllen. (Letzteres folgt leicht aus  $S(n) \neq n$  für alle  $n \in \mathbb{N}$ ).

**Bemerkung** (zur Einführung von  $\mathbb{N}_0$ ). Übrigens erfüllt anstelle von  $(\mathbb{N}, 1)$  auch  $(\mathbb{N}_0, 0)$  die Peano-Axiome (mit  $S: \mathbb{N}_0 \rightarrow \mathbb{N}_0$  erweitert durch  $S(0) := 1$ ). Insofern gibt es zwischen  $\mathbb{N}$  und  $\mathbb{N}_0$  bisher, wo wir nur die Nachfolge-Abbildung  $S$  und ein Anfangselement 1 bzw. 0 betrachten, keinen strukturellen Unterschied, und wir hätten alternativ auch  $\mathbb{N}_0$  axiomatisch einführen und  $\mathbb{N} := \mathbb{N}_0 \setminus \{0\}$  setzen können. Sobald wir die Grundrechenarten angehen, entstehen aber selbstverständlich strukturelle Unterschiede zwischen 1 und 0 und somit zwischen  $\mathbb{N}$  und  $\mathbb{N}_0$ .

Auf dem Induktionsaxiom fußt das **fundamentale Beweisprinzip der vollständigen Induktion (VI) zum Nachweis einer von  $n \in \mathbb{N}$  abhängigen Aussage**<sup>8</sup>  $A(n)$  für alle  $n \in \mathbb{N}$ , bei dem man wie folgt vorgeht:

$$\left. \begin{array}{l} \text{Induktionsanfang: Zeige } \boxed{A(1)}. \\ \text{Induktionsschritt: Zeige die Implikation } \boxed{A(n) \implies A(n+1)} \text{ für alle } n \in \mathbb{N}. \end{array} \right\} \text{ (VI)}$$

Dabei haben wir schon einmal  $n+1 := S(n)$  als die allgemein übliche und mittelfristig einfach bessere Bezeichnung für die auf  $n$  folgende natürliche Zahl verwendet.

**Bemerkungen** (zum Beweisprinzip der vollständigen Induktion).

- (1) Der **Induktionsanfang** wird auch Induktionsverankerung genannt. Er lässt sich oft vergleichsweise einfach und schnell erledigen, darf aber natürlich nicht vergessen werden.
- (2) Für den **Induktionsschritt** fixiert man ein beliebiges  $n \in \mathbb{N}$ . Man betrachtet die **Induktionsannahme** oder Induktionsvoraussetzung  $A(n)$  als gegeben und leitet dann unter Verwendung dieser Annahme die **Induktionsbehauptung**  $A(n+1)$  her.
- (3) Dass das Beweisverfahren funktioniert und tatsächlich die Gültigkeit von  $A(n)$  für alle  $n \in \mathbb{N}$  sicherstellt, ist **durch das Induktionsaxiom gerechtfertigt**: Sind Induktionsanfang und Induktionsschritt gemacht, so wissen wir für die Menge  $M := \{n \in \mathbb{N} \mid A(n) \text{ gilt}\}$  einerseits

<sup>7</sup>Die etwas vage Einführung von  $-\mathbb{N}$  als „Kopie“ kann mengentheoretisch untermauert werden, indem man nur von einem neuen (Vorzeichen-)Objekt  $\ominus$  ausgeht,  $-\mathbb{N} := \{\ominus\} \times \mathbb{N}$  setzt und dann für  $n \in \mathbb{N}$  die Notation  $-n := (\ominus, n) \in -\mathbb{N}$  festlegt. Wir werden  $\ominus$  und diese Konstruktion aber nie wieder explizit brauchen, sondern mit dem in der Definition Gesagten auskommen.

<sup>8</sup>Genauer ist  $A(n)$  ein Prädikat mit freier Variable  $n$ , für die natürliche Zahlen eingesetzt werden können, und das Ziel ist der Nachweis der Aussage  $\forall n \in \mathbb{N}: A(n)$ .

$1 \in M$  und andererseits  $n \in M \implies S(n) \in M$ . Wir können daher per Induktionsaxiom schließen, dass  $M = \mathbb{N}$  ist. Nach Wahl von  $M$  bedeutet dies, dass  $A(n)$  für alle  $n \in \mathbb{N}$  gilt.

(Diese Argumentation braucht jetzt, nachdem wir sie einmal gemacht haben, natürlich *nicht* bei jedem Induktionsbeweis wiederholt zu werden.)

- (4) **Induktionsbeweise sind nicht konstruktiv**, da man schon vor Beginn des Beweises wissen muss, wie die zu zeigende Aussage  $A(n)$  für alle  $n \in \mathbb{N}$  aussieht. Um ein „Gefühl“ zu bekommen und eine sinnvolle Vermutung  $A(n)$  aufstellen zu können, experimentiert man typischerweise mit den ersten paar natürlichen Zahlen. Ein fehlerfreier und erfolgreicher Induktionsbeweis zementiert dann, dass eine Aussage  $A(n)$ , die man für die ersten paar natürlichen Zahlen  $n$  verifiziert hat, tatsächlich und unwiderruflich für *alle* natürlichen Zahlen  $n$  gilt. Mit etwas mehr Erfahrung kann man manchmal auch mit möglichen Induktionsschritten experimentieren, um sinnvoll eine Vermutung  $A(n)$  aufstellen zu können. Wie man zur Vermutung findet, ist tatsächlich nicht vorgeschrieben und muss auch nicht (unbedingt) dokumentiert werden.
- (5) **Achtung! Vollständige Induktion ist kein Allheilmittel, und man muss *nicht jede* von  $n \in \mathbb{N}$  abhängige Aussage  $A(n)$  mit vollständiger Induktion beweisen.** Oft kann man solche Aussagen  $A(n)$  auch für jedes  $n \in \mathbb{N}$  ohne Verwendung der vorigen Aussagen  $A(1), A(2), \dots, A(n-1)$  zeigen und braucht dann keinen Induktionsbeweis anzusetzen. Insbesondere ist dies der Fall, wenn man beim Versuch eines Induktionsschritts feststellt, dass man die Induktionsbehauptung ohne Verwendung der Induktionsannahme zeigen kann. Auch wenn man formal nichts falsch gemacht hat, empfiehlt es sich in dieser Situation trotzdem, das Argument noch einmal neu und induktionsfrei aufzuschreiben.

**Beispiele** (Beispiele für Beweise mit vollständiger Induktion). Unter leichtem Vorgriff auf noch einzuführende Konzepte und Rechenregeln geben wir Beispiele der Anwendung von (VI):

- (1) Wir wollen zeigen:

Für alle  $n \in \mathbb{N}$  ist  $3^{2n} - 2^n$  durch 7 teilbar.

*Beweis.* Wir argumentieren durch vollständige Induktion nach  $n \in \mathbb{N}$ .

*Induktionsanfang für  $n = 1$ :* Die Behauptung reduziert sich wegen  $3^{2 \cdot 1} - 2^1 = 7$  zu „7 ist durch 7 teilbar“ und ist offensichtlich richtig.

*Induktionsschritt von  $n$  auf  $n+1$  für  $n \in \mathbb{N}$ :* Wir möchten von der Induktionsannahme „ $3^{2n} - 2^n$  ist durch 7 teilbar“ auf die Induktionsbehauptung „ $3^{2n+2} - 2^{n+1}$  ist durch 7 teilbar“ schließen. Dazu schreiben wir

$$3^{2n+2} - 2^{n+1} = 9 \cdot 3^{2n} - 9 \cdot 2^n + 9 \cdot 2^n - 2 \cdot 2^n = 9 \cdot (3^{2n} - 2^n) + 7 \cdot 2^n,$$

wobei einerseits nach Induktionsannahme  $3^{2n} - 2^n$  und damit auch  $9 \cdot (3^{2n} - 2^n)$  durch 7 teilbar ist und andererseits  $7 \cdot 2^n$  wegen des Faktors 7 durch 7 teilbar ist. Mit den beiden Summanden ist auch die Summe  $3^{2n+2} - 2^{n+1}$  durch 7 teilbar und die Induktionsbehauptung gezeigt.  $\square$

- (2) Wir wollen zeigen, dass (wie Ihnen vielleicht schon aufgefallen ist) die sukzessive Addition der ungeraden Zahlen die Quadratzahlen ergibt, genauer

$$1+3+5+\dots+(2n-3)+(2n-1) = n^2 \quad \text{für alle } n \in \mathbb{N}.$$

*Beweis.* Wir argumentieren durch vollständige Induktion nach  $n \in \mathbb{N}$ .

*Induktionsanfang für  $n = 1$ :* Die Behauptung reduziert sich zu  $1 = 1^2$  und gilt offensichtlich.

*Induktionsschritt von  $n$  auf  $n+1$  für  $n \in \mathbb{N}$ :* Wir möchten von der Induktionsannahme  $1+3+5+\dots+(2n-3)+(2n-1) = n^2$  auf die Induktionsbehauptung  $1+3+5+\dots+(2n-1)+(2n+1) = (n+1)^2$  schließen. Dazu rechnen wir unter Verwendung der Induktionsannahme im zweiten Schritt

$$\begin{aligned} 1+3+5+\dots+(2n-1)+(2n+1) &= (1+3+5+\dots+(2n-3)+(2n-1)) + (2n+1) \\ &= n^2 + (2n+1) = n^2+2n+1 = (n+1)^2 \end{aligned}$$

und erhalten die Induktionsbehauptung.  $\square$

In der praktischen Anwendung treten auch etliche **Varianten des Induktionsprinzips** auf: Zum Beispiel kann man eine Aussage  $A(z)$  für alle  $z \in \{z_0, z_0+1, z_0+2, \dots\}$  mit fixiertem  $z_0 \in \mathbb{Z}$  (häufig auch  $z_0 = 0$ ) nachweisen, indem man den Induktionsanfang bei  $A(z_0)$  und Induktionsschritt für alle  $z \in \{z_0, z_0+1, z_0+2, \dots\}$  von  $A(z)$  zu  $A(z+1)$  durchführt. Man kann die Variable beim Induktionsschritt selbstverständlich anders benennen und den Schritt etwa von  $A(z-1)$  zu  $A(z)$  für alle  $z \in \{z_0+1, z_0+2, z_0+3, \dots\}$  durchführen. Man kann mehrere Einzelfälle als Induktionsanfang behandeln oder beim Induktionsschritt in Zweischritten von  $A(z)$  zu  $A(z+2)$  übergehen (nützlich etwa dann, wenn für gerade und ungerade  $z$  unterschiedliches Vorgehen geboten ist). Explizit erwähnen wir folgende **Variante mir „allen“ Induktionsannahmen**, die ebenfalls den Nachweis von  $A(n)$  für alle  $n \in \mathbb{N}$  erlaubt:

**Induktionsanfang:** Zeige  $A(1)$ .  
**Induktionsschritt:** Zeige  $A(1) \wedge A(2) \wedge \dots \wedge A(n) \implies A(n+1)$  für alle  $n \in \mathbb{N}$ .  $\left. \vphantom{\begin{array}{l} \text{Induktionsanfang:} \\ \text{Induktionsschritt:} \end{array}} \right\} (\widetilde{\text{VI}})$

Da man hier mehr Annahmen zur Verfügung hat, bietet  $(\widetilde{\text{VI}})$  **beim Induktionsschritt mehr Flexibilität** als  $(\text{VI})$ . Tatsächlich sind die beiden Prinzipien aber gleichwertig, denn  $(\widetilde{\text{VI}})$  kann durch Anwendung des Original-Prinzips  $(\text{VI})$  auf  $\widetilde{A}(n) := A(1) \wedge A(2) \wedge \dots \wedge A(n)$  aus diesem abgeleitet werden.

**Entscheidend ist bei allen Varianten** des Induktionsprinzips aber vor allem, dass **durch Induktionsanfang und -schritt ein Dominoeffekt entsteht**, dass etwa durch  $A(z_0)$ , den Schritt von  $A(z_0)$  zu  $A(z_0+1)$ , den Schritt von  $A(z_0+1)$  zu  $A(z_0+2)$ , den Schritt von  $A(z_0+2)$  zu  $A(z_0+3)$ ,  $\dots$  alle gewünschten  $A(z)$  abgedeckt werden. Statt verschiedene Varianten auswendig zu lernen, sollte man tatsächlich besser an dieses Zusammenspiel von Induktionsanfang und Induktionsschritt im Hinterkopf behalten und sich überlegen, dass es funktioniert.

**Weiteres Beispiel.** Es folgt ein Beispiel zur Anwendung von  $(\widetilde{\text{VI}})$  (oder eigentlich einer weiteren kleinen Variante davon mit Induktionsanfang bei  $n = 2$ ):

(3) Wir möchten die **Existenz der Primfaktorzerlegung** zeigen:

Für alle  $n \in \mathbb{N} \setminus \{1\}$  gibt es  $k \in \mathbb{N}$  und Primzahlen  $p_1, p_2, \dots, p_k \in \mathbb{N}$  mit  $n = p_1 p_2 \dots p_k$ .

*Beweis.* Wir argumentieren durch vollständige Induktion nach  $n \in \mathbb{N} \setminus \{1\}$ .

*Induktionsanfang für  $n = 2$ :* Für  $n = 2$  gilt die Behauptung mit  $k = 1$  und der Primzahl 2.

*Induktionsschritt von  $2, 3, \dots, n-1$  auf  $n$  für  $n \in \mathbb{N} \setminus \{1, 2\}$ :* Wir haben als Induktionsannahme, dass die behauptete Darstellung für  $1, 2, \dots, n-1$  jeweils existiert. Wir möchten daraus die Existenz der entsprechenden Darstellung von  $n$  ableiten. Im Fall, dass  $n$  eine Primzahl ist, ist die Darstellung trivial (mit  $k = 1, p_1 = n$ ). Im Fall, dass  $n$  keine Primzahl ist, können wir  $n = ab$  mit  $a, b \in \{2, 3, \dots, n-1\}$  schreiben. Gemäß Induktionsannahme gibt es daher einerseits  $k \in \mathbb{N}$  und Primzahlen  $p_1, p_2, \dots, p_k \in \mathbb{N}$  mit  $a = p_1 p_2 \dots p_k$ , andererseits  $\ell \in \mathbb{N}$  und Primzahlen  $q_1, q_2, \dots, q_\ell \in \mathbb{N}$  mit  $b = q_1 q_2 \dots q_\ell$ . Setzen wir  $p_{k+i} := q_i$  für alle  $i \in \{1, 2, \dots, \ell\}$ , so ergibt sich mit

$$n = ab = (p_1 p_2 \dots p_k)(q_1 q_2 \dots q_\ell) = p_1 p_2 \dots p_{k+\ell}$$

die behauptete Darstellung von  $n$  (mit  $k+\ell \in \mathbb{N}$  anstelle von  $k$ ). Wir erhalten also die Induktionsbehauptung.  $\square$

Eine Version des Induktionsprinzips zur **Erklärung eines von  $n \in \mathbb{N}$  abhängigen Objekts  $X_n$**  für alle  $n \in \mathbb{N}$  ist das **Prinzip der rekursiven Definition**, das wir schematisch wie folgt festhalten:

$$\left. \begin{array}{l} \textbf{Rekursionsanfang:} \text{ Definiere } X_1. \\ \textbf{Rekursionsschritt:} \text{ Für alle } n \in \mathbb{N} \text{ definiere } X_{n+1} \text{ unter Rückgriff auf } X_n. \end{array} \right\} \text{ (RD)}$$

Hierbei ist (nur jetzt ein Mal, nicht bei jeder Anwendung) zu überlegen, dass das Objekt  $X_n$  durch diese Festlegungen tatsächlich für *alle*  $n \in \mathbb{N}$  *definiert* wird. Genau dies ergibt aber die Anwendung des Induktionsprinzips (VI) auf die  $n$ -abhängige Aussage „ $X_n$  ist (wohl)definiert“ (jedenfalls sofern beim Rekursionsschritt  $X_{n+1}$  für gegebenes  $X_n$  immer wohldefiniert ist). Analog zum Induktionsprinzip besitzt auch (RD) Varianten mit Rekursionsanfang bei beliebigem  $z_0 \in \mathbb{Z}$ , mehreren Einzelfällen als Rekursionsanfang, Rekursionsschritt mit Rückgriff auf mehrere Vorgänger-Objekte, et cetera. Damit wird es möglich, viele naheliegende Definitionen präziser als mit Pünktchen (oder auch überhaupt erst) hinzuschreiben:

**Beispiele** (zur rekursiven Definition von Rechenoperationen auf  $\mathbb{Z}$ ).

- (1) Ausgehend von der bijektiven Nachfolge-Abbildung  $S: \mathbb{Z} \rightarrow \mathbb{Z}$  kann man die **Summe**  $z+n \in \mathbb{Z}$  und die **Differenz**  $z-n \in \mathbb{Z}$  von  $z \in \mathbb{Z}$  und  $n \in \mathbb{N}_0$  erklären, dies aber auf verschiedene Weisen hinschreiben: Mit Pünktchen lauten die Definitionen

$$z + n := \underbrace{S(S(S(\dots(S(z))\dots))}_{n \text{ Anwendungen von } S} \quad \text{und} \quad z - n := \underbrace{S^{-1}(S^{-1}(S^{-1}(\dots(S^{-1}(z))\dots))}_{n \text{ Anwendungen von } S^{-1}}.$$

Mit dem Rekursionsprinzip können wir dieselben Definitionen ganz präzise und frei von Andeutungen durch Pünktchen für alle  $z \in \mathbb{Z}$  durch

$$z \pm 0 := z, \quad z + S(n) := S(z+n) \text{ für } n \in \mathbb{N}_0, \quad z - S(n) := S^{-1}(z-n) \text{ für } n \in \mathbb{N}_0$$

treffen. Wenn im Vorfeld  $z+1 := S(z)$ ,  $z-1 := S^{-1}(z)$  vereinbart wird, können beide Varianten etwas vertrauter hingeschrieben werden, nämlich mit Pünktchen als

$$z + n := (\dots(\underbrace{((z+1)+1)+1}_{n \text{ Summanden } 1})\dots) \quad \text{und} \quad z - n := (\dots(\underbrace{(((z-1)-1)-1)\dots}_{n \text{ Subtrahenden } 1})\dots)$$

und mit Rekursion als

$$z \pm 0 := z, \quad z + (n+1) := (z+n) + 1 \text{ für } n \in \mathbb{N}_0, \quad z - (n+1) := (z-n) - 1 \text{ für } n \in \mathbb{N}_0.$$

Um  $z \pm \tilde{z} \in \mathbb{Z}$  sogar für beliebige  $z, \tilde{z} \in \mathbb{Z}$  zu erklären, vereinbart man im Nachhinein noch

$$z + (-n) := z - n \text{ für } n \in \mathbb{N} \quad \text{und} \quad z - (-n) := z + n \text{ für } n \in \mathbb{N}.$$

(2) Ausgehend von der Summe kann das **Produkt**

$$n \cdot z := nz := \underbrace{(\dots((z+z)+z)+\dots)}_{n \text{ Summanden } z} + z \in \mathbb{Z}$$

von  $n \in \mathbb{N}_0$  und  $z \in \mathbb{Z}$  erklärt werden. Die Präzisierung dieser Pünktchen-Definition durch Rekursion für alle  $z \in \mathbb{Z}$  ist

$$0z := 0 \quad \text{und} \quad (n+1)z := (nz) + z \text{ für } n \in \mathbb{N}_0.$$

Um  $z\tilde{z} \in \mathbb{Z}$  sogar für beliebige  $z, \tilde{z} \in \mathbb{Z}$  zu erklären, ergänzt man die Festlegung

$$(-n)z := n(-z) \text{ für } n \in \mathbb{N}.$$

(3) Mit Hilfe des Produkts können **Potenzen**

$$z^n := \underbrace{(\dots((z \cdot z) \cdot z) \cdot \dots)}_{n \text{ Faktoren } z} \cdot z \in \mathbb{Z}$$

mit Basis  $z \in \mathbb{Z}$  und Exponent  $n \in \mathbb{N}$  definiert werden. Die präzisere rekursive Definition für jedes  $z \in \mathbb{Z}$  lautet

$$z^1 := z \quad \text{und} \quad z^{n+1} := z^n \cdot z \text{ für } n \in \mathbb{N}.$$

Ergänzend definiert man

$$z^0 := 1 \text{ (zumindest) für } z \in \mathbb{Z} \setminus \{0\}.$$

Der Ausdruck  $0^0$  **bleibt generell undefiniert** (begründet zum Beispiel dadurch, dass man die Regeln  $z^0 = 1$  für alle  $z \in \mathbb{Z} \setminus \{0\}$  und  $0^n = 0$  *nicht beide* konsistent fortsetzen kann). Später wird es sich *in manchen Zusammenhängen* als sinnvoll erweisen,  $0^0$  als 1 festzulegen.

Auf Basis der Definitionen kann man die **Kommutativität und Assoziativität der Addition und Multiplikation**, die **Distributivgesetze** und weitere bekannte Rechenregeln ( $z-z=0$ , Klammer-Regeln, binomische Formel, et cetera) für den (symbolischen) Umgang mit ganzen Zahlen herleiten. Zu einem großen Teil kann dies mit Induktionsbeweisen nachgewiesen werden, was hier (abgesehen von einem Beispiel in den Übungen) aber ausgespart werden soll. Wir treffen ab jetzt außerdem die üblichen Konventionen zur **Klammereinsparung**: Es gilt **Punkt- vor Strich-Rechnung**, und die dadurch und durch Assoziativität überflüssigen Klammern werden weggelassen. **Quotienten**  $z:n = z/n = \frac{z}{n} \in \mathbb{Z}$  von  $z \in \mathbb{Z}$  und  $n \in \mathbb{Z} \setminus \{0\}$  können im Rahmen der ganzen Zahlen natürlich nur dann definiert werden, wenn  $z$  durch  $n$  teilbar ist. Formal würde man den Quotienten  $\frac{z}{n}$  an dieser Stelle daher als die eindeutige Zahl  $q \in \mathbb{Z}$ , sofern eine solche denn existiert, mit  $nq = z$  festlegen.

**Weitere Beispiele** (für rekursive Definitionen).

(4) Die **Fakultät**

$$n! := n(n-1) \cdot \dots \cdot 3 \cdot 2 \cdot 1 \in \mathbb{N}$$

von  $n \in \mathbb{N}_0$  wird rekursiv definiert durch

$$0! := 1, \quad (n+1)! := (n+1)(n!) \text{ für } n \in \mathbb{N}_0.$$

Beispiele sind  $0! = 1! = 1$ ,  $2! = 2$ ,  $3! = 6$ ,  $4! = 24$ ,  $5! = 120$ ,  $6! = 720$ ,  $7! = 5040$ ,  $8! = 40320$ .

(5) Die **Fibonacci-Zahlen**  $F_n \in \mathbb{N}_0$  mit  $n \in \mathbb{N}_0$  können tatsächlich nicht so einfach mit Pünktchen hingeschrieben werden. Sie sind rekursiv durch

$$F_0 := 0, \quad F_1 := 1 \quad \text{und} \quad F_{n+1} := F_{n-1} + F_n \text{ für alle } n \in \mathbb{N}$$

definiert. Die ersten Fibonacci-Zahlen sind  $F_0 = 0$ ,  $F_1 = 1$ ,  $F_2 = 1$ ,  $F_3 = 2$ ,  $F_4 = 3$ ,  $F_5 = 5$ ,  $F_6 = 8$ ,  $F_7 = 13$ ,  $F_8 = 21$ ,  $F_9 = 34$ ,  $F_{10} = 55$ . Überraschenderweise kann man (z.B. mit vollständiger Induktion) auch die für alle  $n \in \mathbb{N}$  gültige geschlossene **Formel von Binet**

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

beweisen. Etwas mehr zu Beweis und Hintergrund dieser Formel folgt in den Übungen.

(6) Für  $k \leq \ell$  in  $\mathbb{Z}$  wird die Summe von  $\ell - k + 1$  Zahlen  $a_k, a_{k+1}, \dots, a_{\ell-1}, a_\ell \in \mathbb{Z}$  mit dem **Summenzeichen**  $\sum$  (nach dem Sigma genannten griechischen Buchstaben  $\Sigma$ ) als

$$\sum_{i=k}^{\ell} a_i := a_k + a_{k+1} + \dots + a_{\ell-1} + a_\ell \in \mathbb{Z}$$

abgekürzt. Rekursiv kann man für gegebene  $a_i \in \mathbb{Z}$  erst

$$\sum_{i=0}^0 a_i := a_0 \quad \text{und} \quad \sum_{i=0}^n a_i := \left( \sum_{i=0}^{n-1} a_i \right) + a_n \text{ für } n \in \mathbb{N},$$

darauf aufbauend dann

$$\sum_{i=k}^{\ell} a_i := \sum_{i=0}^{\ell-k} a_{k+i} \text{ für } k \leq \ell \text{ in } \mathbb{Z}$$

definieren. Spezialfälle sind Summen von Einsen  $\sum_{i=k}^{\ell} 1 = \ell - k + 1$  und Produkte  $nz = \sum_{i=1}^n z$ .

(7) Analog wird für  $k \leq \ell$  in  $\mathbb{Z}$  das Produkt von  $a_k, a_{k+1}, \dots, a_{\ell-1}, a_\ell \in \mathbb{Z}$  mit dem **Produktzeichen**  $\prod$  (nach dem Pi genannten griechischen Buchstaben  $\Pi$ ) als

$$\prod_{i=k}^{\ell} a_i := a_k a_{k+1} \cdot \dots \cdot a_{\ell-1} a_\ell \in \mathbb{Z}$$

abgekürzt. Die rekursive Definition kann genau wie beim Summenzeichen ausgeschrieben werden. Spezialfälle sind Potenzen  $z^n = \prod_{i=1}^n z$  und Fakultäten  $n! = \prod_{i=1}^n i$ .

In Ergänzung zu (6) und (7) notiert man auch  $\sum_{i \in I} a_i := \sum_{j=1}^n a_{i_j}$  und  $\prod_{i \in I} a_i := \prod_{j=1}^n a_{i_j}$  für jede endliche Indexmenge  $I = \{i_1, i_2, \dots, i_n\}$  mit  $n \in \mathbb{N}$  Elementen. Ergänzend nutzt man für „leere“ Summen und Produkte die Konventionen  $\sum_{i=k}^{\ell} a_i := 0$ ,  $\prod_{i=k}^{\ell} a_i := 1$  im Fall  $k > \ell$  sowie  $\sum_{i \in \emptyset} a_i := 0$ ,  $\prod_{i \in \emptyset} a_i := 1$ . Wichtiger fürs Rechnen mit Summen- und Produktzeichen sind die Regeln für **Indexverschiebung** (mit  $k, \ell \in \mathbb{Z}$ ,  $v, a_i \in \mathbb{Z}$ ; entspricht Substitution  $j = i+v$ )

$$\sum_{i=k}^{\ell} a_i = \sum_{j=k+v}^{\ell+v} a_{j-v}, \quad \prod_{i=k}^{\ell} a_i = \prod_{j=k+v}^{\ell+v} a_{j-v},$$

**Indexlaufumkehr** (mit  $k, \ell \in \mathbb{Z}$ ,  $a_i \in \mathbb{Z}$ ; entspricht Substitution  $j = k+\ell-i$ )

$$\sum_{i=k}^{\ell} a_i = \sum_{j=k}^{\ell} a_{k+\ell-j}, \quad \prod_{i=k}^{\ell} a_i = \prod_{j=k}^{\ell} a_{k+\ell-j}$$

und **Verhalten bei Summen und Produkten** (mit Indexmenge  $I$ ,  $a_i, b_i, z \in \mathbb{Z}$ ,  $n \in \mathbb{N}$ )

$$\begin{aligned} \sum_{i \in I} (a_i + b_i) &= \left( \sum_{i \in I} a_i \right) + \left( \sum_{i \in I} b_i \right), & \prod_{i \in I} (a_i + b_i) &= \left( \prod_{i \in I} a_i \right) \left( \prod_{i \in I} b_i \right), \\ \sum_{i \in I} (z a_i) &= z \sum_{i \in I} a_i, & \prod_{i \in I} (a_i^n) &= \left( \prod_{i \in I} a_i \right)^n. \end{aligned}$$

Diese Regeln (und die bei der Notation mit Indexmengen implizit unterstellte Unabhängigkeit von der Reihenfolge, in der die Elemente nummeriert werden) liegen in Anbetracht der Pünktchen-Definitionen so nahe, dass wir hier auf Beweise dazu verzichten.

Stattdessen diskutieren wir als Nächstes die Ihnen allen bekannte Darstellung ganzer Zahlen, bei denen Ziffern an unterschiedlichen Positionen unterschiedliches Gewicht besitzen, also die Darstellung in sogenannten Stellenwertsystemen:

**Beispiele und Bemerkungen** (zu Stellenwertsystemen).

- (1) Im **Dezimalsystem/dekadisches System/Zehnersystem** werden die bereits erklärten 1-stelligen Zahlen  $0, 1, 2, 3, 4, 5, 6, 7, 8, 9 \in \mathbb{N}_0$  als Ziffern verwendet. Allgemeiner erhält man eine  $(n+1)$ -stellige Zahl mit  $n \in \mathbb{N}_0$  durch Hintereinanderschreiben solcher Ziffern  $z_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$  und unter Verwendung der **Basis 10** :=  $S(9)$  als

$$z_n z_{n-1} \dots z_2 z_1 z_0 := \sum_{i=0}^n z_i \cdot 10^i \in \mathbb{N}_0,$$

wobei das Hintereinanderschreiben von Ziffern ohne dazwischen gestelltes Symbol hier ausnahmsweise **nicht für das Produkt** steht. Man kann dies als rekursive Definition betrachten, bei der der Rekursionsanfang mit der Definition der 1-stelligen Zahlen bereits erfolgt ist und im Rekursionsschritt für jedes  $n \in \mathbb{N}$  die  $(n+1)$ -stellige Zahl  $z_m := z \cdot 10^n + m$  mit Ziffer  $z \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$  und  $n$ -stelliger natürlicher Zahl  $m$  definiert wird.

**Werden Ziffern ohne Verknüpfungszeichen und Erläuterung verwendet und/oder hintereinander geschrieben, so ist standardmäßig immer dieses System gemeint.**

- (2) In **Stellenwertsystemen mit beliebiger Basis**  $b \in \mathbb{N} \setminus \{1\}$  arbeitet man mit  $b$  Ziffern. Man verwendet (jedenfalls heutzutage und in unserem Kulturkreis) im Fall  $b \leq 10$  normalerweise die  $b$  ersten Ziffern  $0, 1, 2, \dots, b-2, b-1 \in \mathbb{Z}$  des Dezimalsystems in üblicher Bedeutung und muss für  $b > 10$  Ziffersymbole für die Dezimalzahlen  $10, 11, 12, \dots, b-2, b-1 \in \mathbb{Z}$  hinzufügen. Für jedes  $n \in \mathbb{N}_0$  werden  $(n+1)$ -stellige Zahlen mit (im jeweiligen System zulässigen) Ziffern  $z_i$  in Analogie zum Dezimalsystem durch

$$(z_n z_{n-1} \dots z_2 z_1 z_0)_b := \sum_{i=0}^n z_i \cdot b^i \in \mathbb{N}_0$$

erklärt (wobei die als Subskript anzugebende Basis  $b$  gemäß Dezimalsystem benannt wird). An verschiedenen Stellen übliche Basen sind  $b = 2$  (Binärsystem/Dualsystem/Zweiersystem),  $b = 3$  (Ternärsystem),  $b = 8$  (Oktalsystem/Achtersystem),  $b = 10$  (Dezimalsystem aus (1)),  $b = 12$  (Duodezimalsystem/Zwölfersystem),  $b = 16$  (Hexadezimalsystem/Sechzehnersystem). Beim letztgenannten System sind als Zusatz-Ziffern  $A := 10, B := 11, C := 12, D := 13, E := 14, F := 15$  weitgehend üblich.

**Beispiel.** Nachrechnen zeigt  $(11111100100)_2 = (2202211)_3 = (3744)_8 = 2020 = (1204)_{12} = (7E4)_{16}$ .

Wie für die Basis 10 ist auch für beliebige Basen  $b \in \mathbb{N} \setminus \{1\}$  richtig, dass jede natürliche Zahl eine Zifferndarstellung in dieser Basis hat und verschiedene Zifferndarstellungen ohne führende Null-Ziffern zu verschiedenen natürlichen Zahlen gehören. Streng genommen müsste man auch dies natürlich beweisen, worauf wir hier aber verzichten.

Zum Abschluss dieses Abschnitts sei angemerkt, dass **man die natürlichen Zahlen auch allein aus den Axiomen der Mengenlehre** aus Abschnitt 1.4 konstruieren kann, womit sich die Peano-Axiome tatsächlich von zusätzlichen Postulaten zu herleitbaren Eigenschaften wandeln. Mit anderen Worten können die Existenz der natürlichen Zahlen und ihre Grundeigenschaften rein mengentheoretisch unterbaut werden, was im Detail aber über den Vorlesungsstoff hinausgeht und hier nur im Kleingedruckten ausgeführt wird:

**Satz (Existenz von  $\mathbb{N}$ ).** *Es existieren eine Menge  $\mathbb{N}$ , ein Abbildung  $S$  und ein Element  $1$ , die die Peano-Axiome erfüllen.*

*Beweis.* Gemäß dem Unendlichkeitsaxiom gibt es eine Menge  $U$  mit  $\emptyset \in U$  und  $\forall x \in U: x \cup \{x\} \in U$ . Wir erklären  $\mathbb{N}$  als Durchschnitt aller Teilmengen von  $U$ , die diese Eigenschaften von  $U$  teilen, definieren  $S: \mathbb{N} \rightarrow \mathbb{N}$  durch  $S(n) := n \cup \{n\}$  für alle  $n \in \mathbb{N}$ , und setzen  $1 := \emptyset \in \mathbb{N}$ . Wegen  $S(n) = n \cup \{n\} \neq \emptyset = 1$  für alle  $n \in \mathbb{N}$  ist dann  $1 \notin S(\mathbb{N})$ .

Zum Nachweis der Injektivität von  $S$  seien  $m, n \in \mathbb{N}$  mit  $m \cup \{m\} = n \cup \{n\}$ . Wäre  $m \neq n$ , so müssten  $m \in n$  und  $n \in m$  gelten, und die Paarmenge  $\{m, n\}$  widerspräche dem Fundierungsaxiom. Also muss  $m = n$  sein, und  $S$  ist injektiv.

Ist schließlich  $M \subset \mathbb{N}$  mit  $1 \in M$  und  $S(M) \subset M$ , so ist auch  $M \subset U$  mit  $\emptyset \in M$  und  $\forall x \in M: x \cup \{x\} \in M$ . Damit ist  $M$  eine der Mengen, als deren Durchschnitt  $\mathbb{N}$  erklärt wurde. Es folgt also  $\mathbb{N} \subset M$  und insgesamt  $M = \mathbb{N}$ .

Damit haben  $\mathbb{N}$ ,  $S$  und  $1$  alle benötigten Eigenschaften. □

Etwas weniger formell bedeutet die Konstruktion dieses Beweises, dass wir die natürlichen Zahlen als

$$1 := \emptyset, \quad 2 := 1 \cup \{1\}, \quad 3 := 2 \cup \{2\}, \quad 4 := 3 \cup \{3\}, \quad 5 := 4 \cup \{4\}, \quad \dots$$

und konkreter als

$$1 := \emptyset, \quad 2 := \{\emptyset\}, \quad 3 := \{\emptyset, \{\emptyset\}\}, \quad 4 := \{\emptyset, \{\emptyset, \{\emptyset\}\}\}, \quad 5 := \{\emptyset, \{\emptyset, \{\emptyset, \{\emptyset\}\}\}, \{\emptyset, \{\emptyset, \{\emptyset, \{\emptyset\}\}\}\}\}, \quad \dots$$

erhalten haben.

Des Weiteren lässt sich auch eine Eindeutigkeitseigenschaft der natürlichen Zahlen formal herleiten:

**Satz ((strukturelle) Eindeutigkeit von  $\mathbb{N}$ ).** *Sind die Peano-Axiome einerseits für  $(\mathbb{N}, S, 1)$ , andererseits für  $(\tilde{\mathbb{N}}, \tilde{S}, \tilde{1})$  erfüllt, so können  $\mathbb{N}$  und  $\tilde{\mathbb{N}}$  durch eine Bijektion  $f: \mathbb{N} \rightarrow \tilde{\mathbb{N}}$  identifiziert werden, die  $f(1) = \tilde{1}$  und  $f \circ S = \tilde{S} \circ f$  erfüllt.*

Da wir alle weiteren Operationen mit natürlichen Zahlen wie Addition, Multiplikation, et cetera nur aus der Nachfolgeabbildung und der Eins konstruiert haben, sind  $\mathbb{N}$  und  $\tilde{\mathbb{N}}$  damit auch im Hinblick auf solche Operationen **strukturell vollständig äquivalent** und unterscheiden sich höchstens durch „Benennungen konkreter Zahlen“.

*Beweisskizze.* Wir definieren  $f(n) \in \tilde{\mathbb{N}}$  für alle  $n \in \mathbb{N}$ , indem wir  $f(1) := \tilde{1}$  und rekursiv  $f(S(n)) := \tilde{S}(f(n))$  für alle  $n \in \mathbb{N}$  festsetzen. Über das Induktionsaxiom von  $(\mathbb{N}, S, 1)$  ist damit die Wohldefiniertheit einer Abbildung  $f: \mathbb{N} \rightarrow \tilde{\mathbb{N}}$  gesichert, die per Definition  $f(1) = \tilde{1}$  und  $f \circ S = \tilde{S} \circ f$  erfüllt.

Um Surjektivität von  $f$  nachzuweisen, beobachten wir einerseits  $\tilde{1} \in f(\mathbb{N})$  und andererseits  $\tilde{n} \in f(\mathbb{N}) \implies \tilde{S}(\tilde{n}) \in f(\mathbb{N})$  (wobei letzteres gilt, weil  $\tilde{n} \in f(\mathbb{N})$  ja  $\tilde{n} = f(n)$  für ein  $n \in \mathbb{N}$  und damit auch  $\tilde{S}(\tilde{n}) = \tilde{S}(f(n)) = f(S(n))$  bedeutet). Aufgrund dieser Beobachtungen gibt das Induktionsaxiom von  $(\tilde{\mathbb{N}}, \tilde{S}, \tilde{1})$  schon  $f(\mathbb{N}) = \tilde{\mathbb{N}}$ , und damit ist  $f$  surjektiv.

Der Nachweis der Injektivität von  $f$  braucht Vorbereitungen. Wir benutzen, dass Addition und Subtraktion auf  $\mathbb{N}$  und  $\mathbb{Z}$  wie zuvor besprochen rekursiv eingeführt werden können und Standard-Rechenregeln genügen. Da wir für  $\tilde{\mathbb{N}}$  die gleichen Axiome wie für  $\mathbb{N}$  haben, können wir auch auf  $\tilde{\mathbb{N}}$  eine Addition  $\tilde{+}$  rekursiv einführen und erhalten analoge Eigenschaften. Jetzt ergibt sich aus der Vertauschbarkeit  $f \circ S = \tilde{S} \circ f$  von  $f$  mit  $S, \tilde{S}$  die Vertauschbarkeit von  $f$  mit  $+, \tilde{+}$  in der Form  $f(m+n) = f(m)\tilde{+}f(n)$  für alle  $m, n \in \mathbb{N}$ . Um dies formal einzusehen, führt man bei festem  $m \in \mathbb{N}$  aufbauend auf der rekursiven Definition von  $+, \tilde{+}$  und  $f$  vollständige Induktion nach  $n \in \mathbb{N}$  durch. (Wir gehen dazu nicht ins Detail.)

Zum eigentlichen Nachweis der Injektivität von  $f$  sei  $f(m) = f(n)$  für gewisse  $m, n \in \mathbb{N}$ . Ist  $m \neq n$ , so gilt entweder  $n-m \in \mathbb{N}$  oder  $m-n \in \mathbb{N}$ . Wir betrachten im Fall  $n-m \in \mathbb{N}$  erst den Subfall  $m=1$ . In diesem ist  $n \neq 1$ , und mit  $\tilde{1} = f(1) = f(n) = f(n-1)\tilde{+}\tilde{1}$  (Rechenregeln und Vertauschbarkeit von  $f$  mit Addition verwendet) erhalten wir den Widerspruch, dass  $\tilde{1}$  ein Nachfolger ist. Im Subfall  $m \neq 1$  bekommen wir auf ähnliche Weise  $\tilde{1}\tilde{+}f(m-1) = f(m) = f(n) = f(n-m)\tilde{+}\tilde{1}\tilde{+}f(m-1)$ . Elimination des letzten Summanden  $f(m-1)$  auf beiden Seiten der resultierenden Gleichung führt erneut auf den Widerspruch, dass  $\tilde{1}$  ein Nachfolger ist. Damit ist der Fall  $n-m \in \mathbb{N}$  ausgeschlossen. Dieselbe Argumentation mit vertauschten Rollen von  $m$  und  $n$  schließt aber auch  $m-n \in \mathbb{N}$  aus. Daher muss  $m = n$  gelten, und damit ist  $f$  injektiv.

Insgesamt haben wir gezeigt, dass  $f$  eine Bijektion mit den gewünschten Eigenschaften ist.  $\square$

## Einschub: Beweisstrategien

Vorausgeschickt sei die Warnung, dass es **kein Patentrezept** zum Finden eines mathematischen Beweises gibt. Gerade aufwändige Beweise kann man nur über Erfahrung, Intuition, Umformulieren des Problems, Betrachtung aus verschiedenen Blickwinkeln und das Ausprobieren verschiedener Ansätze angehen. Und am Ende kann man trotz allem scheitern.

Dennoch seien hier **Hinweise zu generellen Strategien und häufigen Vorgehensweisen** zusammengetragen. Zu einem großen Teil lehnen sich die Hinweise aber eng an Definitionen an, kamen auf die ein oder andere Weise schon vor und bringen über die systematische Zusammenstellung hinaus **wenig wirklich Neues**.

**Strategien (für Beweise).** Generell hängt das Vorgehen bei einem Beweis stark von der behaupteten Aussage ab. Es folgen Hinweise sowohl für spezielle Fälle als auch allgemeiner Natur.

(1) Beweise von **Aussagen mit Teilaussagen**  $A, B$ :

- **Implikation**  $A \implies B$ : Dies ist der Prototyp eines logischen Schlusses. Es gibt hierfür drei prinzipielle Möglichkeiten:

Beim **direkten Beweis** nimmt man  $A$  als wahr an und argumentiert, dass  $B$  dann ebenfalls wahr sein muss; vergleiche mit Abschnitt 1.3.

Der **Beweis durch Kontraposition** nutzt das Kontrapositions-Prinzip aus Abschnitt 1.1: Man zeigt  $(\neg B) \implies (\neg A)$ , geht also von  $\neg B$  aus und schließt auf  $\neg A$ .

Beim **indirekten Beweis** oder **Widerspruchsbeweis**, auch **Reductio ad absurdum** genannt, nimmt man  $A$  und zudem die **Widerspruchsannahme**  $\neg B$  als wahr an (typische Formulierung: „Angenommen, es gilt/ist ...“) und zeigt, dass hieraus eine Absurdität/ein Widerspruch entsteht. (Dieses Vorgehen ist übrigens durch die Definition der Implikation selbst gerechtfertigt: Man führt  $A \wedge (\neg B)$  als den einzigen Fall, in dem  $A \implies B$  falsch ist, zum Widerspruch und schließt diesen somit aus.)

Die logischen Verneinungen bei Kontraposition und indirektem Beweis betreffen oft Aussagen mit Quantoren. In solchen Fällen denke man an die zugehörigen Regeln aus Abschnitt 1.2 (auch dann, wenn die Quantoren in Worten und nicht als Formelzeichen auftreten).

- **Äquivalenz  $A \iff B$ :** Meist zeigt man die Hin-Richtung „ $\implies$ “ und die Rück-Richtung „ $\impliedby$ “ separat. Dafür kann jede der gerade besprochenen Strategien zum Einsatz kommen. Seltener, aber nicht völlig ungewöhnlich ist, eine Äquivalenz durch Aneinandersetzen bekannter oder einfacher Äquivalenzen (z.B. Äquivalenzumformungen)  $A \iff H_1, H_1 \iff H_2, H_2 \iff H_3, \dots, H_{n-1} \iff H_n, H_n \iff B$  (mit Hilfsaussagen  $H_1, H_2, \dots, H_n$ ) zu zeigen.
- (2) In fast jedem Zusammenhang kommen **Fallunterscheidungen** in Betracht, bei denen im Beweis Fälle mit verschiedenen Annahme einzeln abgearbeitet werden. Entscheidend ist natürlich, dass die Fälle die Gesamtheit aller Möglichkeiten abdecken müssen.
- (3) **Existenz- und Eindeutigkeitsbeweise:**
- Zu **Existenzbeweisen** lässt sich wenig Allgemeines sagen. Nur um auf eine Existenzaussage der Form  $\exists x \in \mathcal{X}: \forall y \in \mathcal{Y}: P(x, y)$  zu schließen, bietet sich manchmal ein indirekter Beweis an, da die Widerspruchsannahme für jedes  $x \in \mathcal{X}$  ein  $y_x \in \mathcal{Y}$  mit  $\neg P(x, y_x)$  gibt und man mit den „Gegenbeispielen“  $y_x$  eventuell gut argumentieren kann. Aber so etwas wird erst viel (!) später mal vorkommen.
  - Bei **Eindeutigkeitsbeweisen** ist für zwei Objekte  $x, y$  mit gewissen behaupteten Eigenschaften die Gleichheit  $x = y$  zu zeigen. Dies kann direkt oder indirekt geschehen. Bei letzterem nimmt man an, dass  $x, y$  mit  $x \neq y$  die behaupteten Eigenschaften haben und erzeugt einen Widerspruch.
- (4) Beweise von **Aussagen über Mengen  $M, N$ :**
- **Mengen-Inklusion  $M \subset N$ :** Oft zeigt man „zu Fuß“ die Implikation  $x \in M \implies x \in N$ . Dies kann direkt, durch Kontraposition (entspricht Nachweis  $N^c \subset M^c$ , wenn  $M, N \subset \mathcal{X}$  für Grundmenge  $\mathcal{X}$ ) oder durch Widerspruch (entspricht Nachweis  $M \setminus N \subset \emptyset$ ) geschehen. Oft kann man auch abstrakt ohne Betrachtung einzelner Elemente argumentieren, zum Beispiel durch Zusammensetzen schon bekannter Inklusionen.
  - **Mengen-Gleichheit  $M = N$ :** Meist zeigt man die Inklusionen „ $\subset$ “ und „ $\supset$ “ separat. Seltener kann man direkt die Äquivalenz  $x \in M \iff x \in N$  nachweisen oder abstrakter argumentieren.
  - Das **Widerlegen** solcher Aussagen ist viel einfacher. Um  $M \not\subset N$  bzw.  $M \neq N$  zu zeigen, muss man *nur ein Element*  $x \in M \setminus N$  bzw.  $x \in M \Delta N$  („ein Gegenbeispiel“) angeben.
- (5) Zu Beweisen von **Aussagen über Zahlen  $x, y$**  lässt sich nur weniger aussagekräftig sagen:
- Gelegentlich weist man eine Ungleichung  $x \leq y$  für  $x, y \in \mathbb{R}$  nach, indem man  $x \leq y + \varepsilon$  für alle  $\varepsilon \in \mathbb{R}$  mit  $\varepsilon > 0$  (oder nur für alle  $\varepsilon \in \mathbb{Q}$  mit  $\varepsilon > 0$ ) zeigt. Genaueres dazu später noch!
  - Gelegentlich weist man eine Gleichheit  $x = y$  nach, indem man „ $\leq$ “ und „ $\geq$ “ separat zeigt.
- Anders als bei Mengen sind die beschriebenen Vorgehensweisen hier aber nicht kanonisch.
- (6) Beweise von **Aussagen über  $n$ -Tupel  $x, y$**  (z.B. Paare oder Tripel):
- **Gleichheit  $x = y$  von  $n$ -Tupeln:** Oft zeigt man „zu Fuß“  $x_i = y_i$  für alle  $i \in \{1, 2, \dots, n\}$ .
- (7) Beweise von **Aussagen über Abbildungen  $f, g: \mathcal{X} \rightarrow \mathcal{Y}$ :**
- **Gleichheit  $f = g$  von Abbildungen:** Vorab ist zu prüfen, dass  $f$  und  $g$  gleichen Definitionsbereich  $\mathcal{X}$  und je nach genauer Auffassungsweise (Dazu in Abschnitt 2.3 noch!) gleichen Zielbereich  $\mathcal{Y}$  haben. Man zeigt dann oft „zu Fuß“  $f(x) = g(x)$  für alle  $x \in \mathcal{X}$ .

- **Injektivität von  $f$ :** Oft zeigt man „zu Fuß“ die Implikation  $f(x) = f(\tilde{x}) \implies x = \tilde{x}$  für alle  $x, \tilde{x} \in \mathcal{X}$ . Dies kann direkt, per Kontraposition ( $x \neq \tilde{x} \implies f(x) \neq f(\tilde{x})$ ) oder indirekt ( $f(x) = f(\tilde{x})$  für  $x \neq \tilde{x}$  führt zum Widerspruch) geschehen und ist ein spezieller Fall eines Eindeutigkeitsbeweises.
- **Surjektivität von  $f$ :** Oft gibt man sich ein beliebiges  $y \in \mathcal{Y}$  vor und zeigt „zu Fuß“ die Existenz eines  $x \in \mathcal{X}$  mit  $f(x) = y$ . Dies ist ein spezieller Fall eines Existenzbeweises.
- **Bijektivität von  $f$ :** Oft zeigt man Injektivität von  $f$  und Surjektivität von  $f$  separat.
- Das **Widerlegen** ist meist wieder einfacher: Für  $f \neq g$  muss man nur *ein*  $x \in \mathcal{X}$  mit  $f(x) \neq g(x)$  angeben, für Nicht-Injektivität von  $f$  *zwei*  $x, \tilde{x} \in \mathcal{X}$  mit  $x \neq \tilde{x}$ ,  $f(x) = f(\tilde{x})$ , für Nicht-Surjektivität von  $f$  *ein*  $y \notin \text{Bild}(f)$  (was allerdings  $f(x) \neq y$  für *alle*  $x \in \mathcal{X}$  bedeutet).

Oft kann man anstelle der Beweise „zu Fuß“ auch abstrakter ohne Betrachtung einzelner Elemente argumentieren, zum Beispiel über die Komposition und bereits bekannte Eigenschaften gewisser Abbildungen.

- (8) Beweise von „ **$n$ -abhängigen“ Aussagen  $A(n)$**  für alle  $n \in \mathbb{N}$  (oder von  $z$ -abhängigen Aussagen für alle  $z \in \{z_0, z_0+1, z_0+2, \dots\}$ ):

- Das **Prinzip der vollständigen Induktion** wurde in Abschnitt 2.2 besprochen.
- Das **Prinzip des kleinsten Gegenbeispiels** ist eine **indirekte Variante des Induktionsprinzips**, die aber **relativ selten** benötigt wird. Man zeigt dabei den Induktionsanfang  $A(1)$  und macht die Widerspruchsannahme, dass  $A(n)$  *nicht* für alle  $n \in \mathbb{N}$  gilt. Diese Annahme erzwingt, dass einer der Induktionsschritte beim Induktionsprinzip der Form (VI) scheitern muss. Es gibt also ein  $n \in \mathbb{N}$ , so dass  $A(1), A(2), \dots, A(n)$  alle wahr sind, aber  $A(n+1)$  falsch (und somit  $n+1$  das hypothetische „kleinste Gegenbeispiel“) ist. Kann man auf dieser Grundlage einen Widerspruch herleiten, so hat man  $A(n)$  für alle  $n \in \mathbb{N}$  gezeigt.

- (9) Ab und zu kann man bei Beweisen **Ausdehnungsprozeduren** einsetzen, also eine Aussage im ersten Schritt für spezielle Objekte bzw. eine Variable in einer Teilmenge zeigen, im zweiten Schritt unter Rückgriff auf den ersten für etwas weniger spezielle Objekte bzw. eine größere Teilmenge und erst im  $n$ -ten Schritt irgendwann allgemein bzw. für die ganze Menge. Bei Aussagen über Zahlen kann sich dies zum Beispiel so gestalten, dass man eine Aussage erst für natürliche Zahlen, dann für ganze Zahlen, dann für rationale Zahlen und schließlich für reelle Zahlen nachweist.

- (10) In einem Beweis können die bisher genannten **Techniken beliebig kombiniert** oder auch dieselbe Technik mehrfach angewandt werden. **Allgemeine Tipps**, um einen Beweis zu finden und/oder zu verifizieren sind:

- Das **Ziel des Beweises bewusst aufschreiben**, zum Beispiel als „Zu zeigen: ...“ oder „Behauptung: ...“! Dies ist am Anfang der Lösung einer Beweisaufgabe immer gern gesehen.
- Eine **formale Prüfung der Aussage** vornehmen, etwa, ob gleichgesetzte Objekte überhaupt vom gleichen Typ (Zahl, Paar,  $n$ -Tupel, Menge, Abbildung) sind, Argumente im Definitionsbereich einer Abbildung liegen, bei der Komposition von Abbildungen das Ziel der inneren Abbildung gleich dem Definitionsbereich der äußeren Abbildung ist! Man kann dabei auch Grenzfälle abklopfen, zum Beispiel den, dass eine Menge leer oder die ganze Grundmenge ist, eine Zahl den größten oder kleinsten möglichen Wert (z.B. Null) annimmt, et cetera. Auch wenn die Aussagen der Vorlesung und der Übungen in der Regel (formal) korrekt sind, so hilft die Prüfung doch oft beim besseren Verständnis der Ausgangssituation.

- Sich beim Beweis einer Implikation  $A \implies B$  von **Anfang und Ende annähern**, also sowohl überlegen, was mit  $A$  gezeigt werden kann, als auch, was denn reichen würde, um damit  $B$  zu zeigen!
- Wenn der allgemeine Fall nicht in Reichweite scheint, dann zuerst einen **einfachen Fall oder wichtigen Modellfall** betrachten und erst danach dessen Lösung verallgemeinern!
- Teilstücke der Argumentation **immer wieder durchgehen, kritisch hinterfragen und auf Korrektheit prüfen**, auch anhand von speziellen Grenz- und Modellfällen!

Je schwieriger und umfangreicher der Beweis und sein Kontext sich gestalten, desto wichtiger werden gerade die letztgenannten Tipps.

## 2.3 Relationen

Relationen treten in der Mathematik in vielfältiger Gestalt auf. Wir beginnen hier mit dem abstrakten Konzept und wenden uns danach den wichtigen Spezialfällen zu.

**Definitionen (Relationen).** Seien  $\mathcal{X}$  und  $\mathcal{Y}$  beliebige Mengen.

- (I) Eine (zweistellige) **Relation**  $R$  zwischen (den Elementen von)  $\mathcal{X}$  und  $\mathcal{Y}$  ist ein Tripel  $(\mathcal{X}, \mathcal{Y}, G)$  mit einer Teilmenge  $G$  des kartesischen Produkts  $\mathcal{X} \times \mathcal{Y}$ . Wir nennen  $G$  den **Graph der Relation**  $R$  und schreiben für diesen  $G_R$ . Eine Relation zwischen  $\mathcal{X}$  und  $\mathcal{X}$  bezeichnen wir als Relation zwischen den Elementen von  $\mathcal{X}$  oder Relation auf  $\mathcal{X}$ .
- (II) Die Menge aller Relationen zwischen  $\mathcal{X}$  und  $\mathcal{Y}$  (die formal gleich  $\{\mathcal{X}\} \times \{\mathcal{Y}\} \times \mathcal{P}(\mathcal{X} \times \mathcal{Y})$  ist) bezeichnen wir mit  $\text{Rel}(\mathcal{X}, \mathcal{Y})$ . Wir kürzen  $\text{Rel}(\mathcal{X}) := \text{Rel}(\mathcal{X}, \mathcal{X})$  ab.

**Bemerkung.** Für beliebige  $n \in \mathbb{N}$  kann man eine  **$n$ -stellige Relation** zwischen Mengen  $\mathcal{X}_1, \mathcal{X}_2, \dots, \mathcal{X}_n$  als Tupel  $(\mathcal{X}_1, \mathcal{X}_2, \dots, \mathcal{X}_n, T)$  mit einer Teilmenge  $T$  des  $n$ -fachen kartesischen Produkts  $\mathcal{X}_1 \times \mathcal{X}_2 \times \dots \times \mathcal{X}_n$  erklären. Wir behandeln nur den zuvor betrachteten und mit Abstand wichtigsten Fall  $n = 2$ .

Das wesentliche Objekt in der Definition einer Relation ist der letzte Eintrag des Tupels, also bei  $R \in \text{Rel}(\mathcal{X}, \mathcal{Y})$  der in Abbildung 25 gezeigte Graph  $G_R \subset \mathcal{X} \times \mathcal{Y}$ . Die wahre Bedeutung von Relationen erschließt sich aber tatsächlich weniger aus der Definition und mehr aus folgenden Sprech-, Schreib- und Betrachtungsweisen:

**Notation & Betrachtungsweise (für/bei Relationen).**

Seien  $\mathcal{X}, \mathcal{Y}$  Mengen,  $x \in \mathcal{X}$ ,  $y \in \mathcal{Y}$  und  $R \in \text{Rel}(\mathcal{X}, \mathcal{Y})$ . Wir sagen und schreiben im Fall  $(x, y) \in G_R$ , dass  $x$  mit  $y$  bezüglich  $R$  in Relation steht, oder, dass die Aussage  $x R y$  gilt. Sehr oft interpretieren wir eine **Relation nicht als Tupel oder Teilmenge, sondern als eine gewisse Beziehung zwischen Elementen**  $x$  und  $y$ ; vergleiche mit Abbildung 26. Die Beziehung kommt zum Ausdruck, indem wir  $R$  in der gerade eingeführten **Infix-Notation**  $x R y$  zwischen  $x$  und  $y$  schreiben. In Zukunft werden wir anstelle von  $R$  nicht nur andere Buchstaben, sondern häufig auch anders geartete Symbole verwenden.

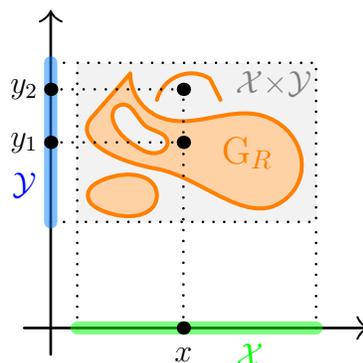


Abb. 25: Der Graph  $G_R$  eines  $R \in \text{Rel}(\mathcal{X}, \mathcal{Y})$  mit  $\mathcal{X}, \mathcal{Y} \subset \mathbb{R}$  sowie  $x \in \mathcal{X}$  und  $y_1, y_2 \in \mathcal{Y}$  mit  $x R y_1$ , aber  $\neg(x R y_2)$ .

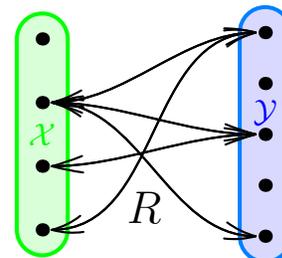


Abb. 26: Darstellung einer Relation  $R$  zwischen Mengen  $\mathcal{X}$  und  $\mathcal{Y}$  mit endlich vielen Elementen

**Beispiele** (von Relationen).

- (0) Für beliebige Mengen  $\mathcal{X}, \mathcal{Y}$  enthält  $\text{Rel}(\mathcal{X}, \mathcal{Y})$  die Leer-Relation  $R = (\mathcal{X}, \mathcal{Y}, \emptyset)$  (für die  $x R y$  nie gilt) und die All-Relation  $R = (\mathcal{X}, \mathcal{Y}, \mathcal{X} \times \mathcal{Y})$  (für die  $x R y$  immer gilt). Diese Extremfälle sind aber selten relevant.

- (1) Durch

$$y \stackrel{\cong}{\sim} z \iff z-y \text{ ist gerade}, \quad y \stackrel{\cup}{\sim} z \iff z-y \text{ ist ungerade}$$

für  $y, z \in \mathbb{Z}$  werden zwei Relationen  $\stackrel{\cong}{\sim}, \stackrel{\cup}{\sim} \in \text{Rel}(\mathbb{Z})$  erklärt, von denen für jedes  $(y, z) \in \mathbb{Z}^2$  eine gilt und eine nicht. Zum Beispiel gelten  $2 \stackrel{\cong}{\sim} 4$ ,  $(-2) \stackrel{\cup}{\sim} 5$ ,  $(-7) \stackrel{\cong}{\sim} (-7)$  und  $9 \stackrel{\cup}{\sim} 0$ . Die Graphen dieser beiden Relationen sind die Mengen  $G_{\cong} = \{(y, z) \in \mathbb{Z}^2 \mid z-y \text{ ist gerade}\}$  und  $G_{\cup} = \{(y, z) \in \mathbb{Z}^2 \mid z-y \text{ ist ungerade}\}$ .

- (2) Für jede Menge  $M$  ist die **Gleichheit „=“ von Elementen** eine Relation  $(M, M, G_=)$  auf  $M$  mit Graph  $G_= = \Delta_M := \{(x, y) \in M^2 \mid x = y\}$ .
- (3) Für jede Grundmenge  $\mathcal{X}$  geben die **Gleichheit, Ungleichheit und (strikte) Inklusion von Mengen**, also alle Symbole  $\square \in \{=, \neq, \subset, \supset, \subsetneq, \supsetneq\}$ , Relationen zwischen Teilmengen von  $\mathcal{X}$  oder mit anderen Worten Relationen auf  $\mathcal{P}(\mathcal{X})$ .
- (4) Für jede Grundmenge  $\mathcal{X}$  und jedes Mengensystem  $\mathcal{S}$  (z.B.  $\mathcal{S} = \mathcal{P}(\mathcal{X})$ ) ist die **Element-Beziehung „ $\in$ “** eine Relation auf  $\mathcal{X} \times \mathcal{S}$  mit Graph  $G_{\in} = \{(x, M) \in \mathcal{X} \times \mathcal{S} \mid x \in M\}$ . Analog kann man „ $\ni$ “ als Relation auf  $\mathcal{S} \times \mathcal{X}$  verstehen.
- (5) Die **Gleichheit, Ungleichheit und Kleiner-/Größer-(gleich-)Beziehungen zwischen Zahlen**, also alle Symbole  $\square \in \{=, \neq, <, >, \leq, \geq\}$ , geben Relationen auf jedem Zahlbereich  $\mathbb{B} \in \{\mathbb{N}, \mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}\}$ . Dabei sind Gleichheit und Ungleichheit generell definiert. Auch die anderen Symbole sind Ihnen prinzipiell vertraut. Präzise können „ $<$ “ und „ $>$ “ durch

$$z > y \iff y < z \iff z-y \in \mathbb{N} \quad \text{für } y, z \in \mathbb{Z}$$

erklärt und später auf  $y, z \in \mathbb{Q}$  bzw.  $y, z \in \mathbb{R}$  verallgemeinert werden. Darauf aufbauend bedeuten  $y \leq z$  und  $z \geq y$  natürlich nichts anderes als  $(y < z) \vee (y = z)$ .

- (6) Die **Gleichheit, Ungleichheit und Kleiner-/Größer-(gleich-)Beziehungen zwischen Abbildungen**, also alle Symbole  $\square \in \{=, \neq, <, >, \leq, \geq\}$ , geben Relationen auf Mengen  $\text{Abb}(\mathcal{X}, \mathbb{B})$  von Abbildungen (mit beliebiger Menge  $\mathcal{X}$  und  $\mathbb{B} \in \{\mathbb{N}, \mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}\}$ ), wobei man für  $f, g \in \text{Abb}(\mathcal{X}, \mathbb{B})$  die meisten genannten Symbole  $\square$  standardmäßig im punktweisen Sinn

$$f \square g \iff f \square g \text{ auf } \mathcal{X} \iff \forall x \in \mathcal{X}: f(x) \square g(x)$$

versteht. Lediglich bei der Ungleichheit  $f \neq g$  hängt es tatsächlich vom Kontext ab, ob sie wie gerade beschrieben als  $\forall x \in \mathcal{X}: f(x) \neq g(x)$  oder als logisches Gegenteil  $\exists x \in \mathcal{X}: f(x) \neq g(x)$  der Gleichheit  $f = g$  zu verstehen ist. Speziell für konstante  $g \equiv y$  unterscheidet man hierfür manchmal die Notationen  $f \neq y$  für  $\forall x \in \mathcal{X}: f(x) \neq y$  und  $f \not\equiv y$  für  $\exists x \in \mathcal{X}: f(x) \neq y$ . Aus demselben Grund, i.W. dem Unterschied zwischen  $\forall x$  und  $\exists x$ , ist hier die „ $<$ “-Relation *nicht* das Gegenteil der „ $\geq$ “-Relation und die „ $>$ “-Relation *nicht* das Gegenteil der „ $\leq$ “-Relation.

- (7) Die **Teilbarkeitsrelation „ $\mid$ “** ist auf jedem ganzzahligen Zahlbereich  $\mathbb{B} \in \{\mathbb{N}_0, \mathbb{N}, \mathbb{Z}\}$  sinnvoll. Dabei bedeutet  $t \mid z$  mit  $t, z \in \mathbb{B}$ , dass  $t$  ein Teiler von  $z$  ist, oder als Formel

$$t \mid z \iff \exists d \in \mathbb{B}: td = z \quad \text{für } t, z \in \mathbb{B}.$$

- (8) Für jede feste Grundmenge  $\mathcal{X}$  ist **Disjunktheit von Teilmengen** eine Relation auf  $\mathcal{P}(\mathcal{X})$ .
- (9) Jede Funktion  $f: \mathcal{X} \rightarrow \mathcal{Y}$  zwischen Mengen  $\mathcal{X}, \mathcal{Y}$  induziert eine Relation  $R \in \text{Rel}(\mathcal{X}, \mathcal{Y})$  mit gleichem Graph  $G_R = G_f$  (wobei  $G_f = \{(x, y) \in \mathcal{X} \times \mathcal{Y} \mid f(x) = y\}$  definiert war) oder äquivalent mit

$$x R y \iff f(x) = y \quad \text{für alle } x \in \mathcal{X}, y \in \mathcal{Y}.$$

Die Relation  $R$  erbt von der Funktion  $f$  die entscheidende Eigenschaft, dass zu jedem  $x \in \mathcal{X}$  *genau* ein  $y \in \mathcal{Y}$  mit  $x R y$  existiert.

Tatsächlich kommt jede Relation  $R \in \text{Rel}(\mathcal{X}, \mathcal{Y})$  mit der „Genau-ein- $y$ -Eigenschaft“ des Beispiels (9) durch eine eindeutig bestimmte Abbildung  $f: \mathcal{X} \rightarrow \mathcal{Y}$  zustande, denn man kann den Funktionswert  $f(x)$  als das eindeutige, zu  $x \in \mathcal{X}$  gehörige  $y \in \mathcal{Y}$  mit  $x R y$  festsetzen. Wir erhalten eine 1-zu-1-Korrespondenz zwischen Abbildungen  $\mathcal{X} \rightarrow \mathcal{Y}$  und Relationen in  $\text{Rel}(\mathcal{X}, \mathcal{Y})$  mit der „Genau-ein- $y$ -Eigenschaft“ und **können Abbildungen fortan als spezielle Relationen auffassen**. Dies können wir auch benutzen, um den Begriff der Abbildung aus Abschnitt 2.1 — wo, wir erinnern uns, der nicht formal definierte Begriff „Zuordnungsvorschrift“ einging — völlig präzise auf den Punkt zu bringen und mengentheoretisch zu unterfüttern:

**Präzisierung (des Abbildungsbegriffs).** *Seien  $\mathcal{X}$  und  $\mathcal{Y}$  Mengen. Eine Abbildung  $f: \mathcal{X} \rightarrow \mathcal{Y}$  von  $\mathcal{X}$  nach  $\mathcal{Y}$  ist eine Relation  $R \in \text{Rel}(\mathcal{X}, \mathcal{Y})$ , bei der zu jedem  $x \in \mathcal{X}$  genau ein  $y \in \mathcal{Y}$  mit  $x R y$  existiert. Für jedes  $x \in \mathcal{X}$  wird das eindeutige  $y$  mit  $x R y$  als  $f(x)$  bezeichnet.*

**Bemerkungen** (zum Abbildungsbegriff).

- (1) **Beim praktischen Umgang mit Abbildungen ist die Präzisierung des Begriffs selten relevant.** Sie zeigt aber, dass auch der Abbildungsbegriff mengentheoretisch unterfüttert und allein<sup>9</sup> auf die Axiome der Mengenlehre gegründet werden kann. Manchmal hilft die Präzisierung auch beim Umgang mit Grenzfällen. Sie klärt etwa, dass von leerem Definitionsbereich  $\emptyset$  in beliebiges Ziel  $\mathcal{Y}$  genau eine Abbildung existiert, die leere Abbildung  $\emptyset \rightarrow \mathcal{Y}$ , die der Leer-Relation (die in diesem Fall zugleich die All-Relation ist) entspricht.
- (2) Durch die Präzisierung des Abbildungsbegriffs wird die **Gleichheit  $f_1 = f_2$  von Abbildungen  $f_1 \in \text{Abb}(\mathcal{X}_1, \mathcal{Y}_1)$  und  $f_2 \in \text{Abb}(\mathcal{X}_2, \mathcal{Y}_2)$**  auf die Gleichheit von Tripeln und (Teil-)Mengen zurückgeführt und stellt sich als **gleichbedeutend mit  $\mathcal{X}_1 = \mathcal{X}_2$ ,  $\mathcal{Y}_1 = \mathcal{Y}_2$  und  $f_1(x) = f_2(x)$  für alle  $x \in \mathcal{X}_1$**  heraus. Dies haben wir in Abschnitt 2.1, dem Einschub zu Beweisstrategien und obigem Beispiel (6) teils schon benutzt, hatten dort aber eher nur Gleichheit von Abbildungen mit *a priori* gleichem Definitionsbereich und Ziel angesprochen. Manchmal möchte man für die Gleichheit tatsächlich auch nur  $\mathcal{X}_1 = \mathcal{X}_2$  und  $f_1(x) = f_2(x)$  für alle  $x \in \mathcal{X}_1$  verlangen, eine eventuelle Nicht-Übereinstimmung  $\mathcal{Y}_1 \neq \mathcal{Y}_2$  der Zielbereiche aber außen vor lassen, was formal durch die Definition einer Relation  $R \in \text{Rel}(\mathcal{X}, \mathcal{Y})$  nur als Paar  $(\mathcal{X}, G)$  mit  $G \subset \mathcal{X} \times \mathcal{Y}$  ohne explizite Berücksichtigung von  $\mathcal{Y}$  erreicht werden kann. Fürs Erste bleiben wir aber bei der gegebenen Definition mit Berücksichtigung von  $\mathcal{Y}$ . Später wird sich der geeignete Standpunkt aus dem Kontext ergeben.
- (3) Man nennt eine Relation  $R$  zwischen Mengen  $\mathcal{X}$  und  $\mathcal{Y}$  linkstotal, wenn jedes  $x \in \mathcal{X}$  mit *mindestens* einem  $y \in \mathcal{Y}$  bezüglich  $R$  in Relation steht. Man nennt sie rechtseindeutig, wenn jedes  $x \in \mathcal{X}$  mit *höchstens* einem  $y \in \mathcal{Y}$  bezüglich

<sup>9</sup>Allerdings braucht man Abbildungen schon zur präzisen semantischen Erklärung von Belegungen logischer Formeln. Dies gehört *vor* die Mengenlehre und macht es — so jedenfalls der Wissensstand des Dozenten — erforderlich, sich in der Logik trotz allem auf einen naiveren, metatheoretischen Abbildungsbegriff zu stützen.

$R$  in Relation steht. Beide Bedingungen zusammen ergeben die obige Forderung, dass jedes  $x$  mit *genau* einem  $y$  in Relation steht, wir können also festhalten: **Eine Funktion  $\mathcal{X} \rightarrow \mathcal{Y}$  ist nichts anderes als eine linkstotale und rechtseindeutige Relation zwischen  $\mathcal{X}$  und  $\mathcal{Y}$ .**

- (4) Für jede linkstotale Relation  $R$  zwischen Mengen  $\mathcal{X}$  und  $\mathcal{Y}$  gibt es mindestens eine Abbildung  $f: \mathcal{X} \rightarrow \mathcal{Y}$  mit  $G_f \subset G_R$ .

Dies ergibt sich durch Anwendung des Auswahlaxioms aus Abschnitt 1.4 auf das System der disjunkten nicht-leeren Mengen  $G_R \cap (\{x\} \times \mathcal{Y})$  mit  $x \in \mathcal{X}$  und Festlegung von  $f(x)$  mit  $x \in \mathcal{X}$  als  $y$ -Eintrag des ausgewählten Paares  $(x, y)$  aus  $G_R \cap (\{x\} \times \mathcal{Y})$ . Tatsächlich ist obige Aussage sogar äquivalent zum Auswahlaxiom, denn für ein System  $\mathcal{S}$  disjunkter nicht-leerer Mengen kann man sie auf die linkstotale Relation  $R \in \text{Rel}(\mathcal{S}, \bigcup_{M \in \mathcal{S}} M)$  mit  $G_R := \bigcup_{M \in \mathcal{S}} (\{M\} \times M)$  anwenden und erhält erst eine Abbildung  $f: \mathcal{S} \rightarrow \bigcup_{M \in \mathcal{S}} M$  mit  $G_f \subset G_R$  und daraus dann die Auswahlmenge  $A := \text{Bild}(f) \subset \bigcup_{M \in \mathcal{S}} M$  mit  $A \cap M = \{f(M)\}$  für jedes  $M \in \mathcal{S}$ .  $\square$

Als Nächstes führen wir Grundoperationen mit Relationen ein, die teils schon bekannte Operationen mit Abbildungen verallgemeinern:

**Definitionen (Grundoperationen mit Relationen).** Seien  $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$  beliebige Mengen.

- (1) Die **Komposition von Relationen**  $R \in \text{Rel}(\mathcal{X}, \mathcal{Y})$  und  $S \in \text{Rel}(\mathcal{Y}, \mathcal{Z})$  ist die Relation  $S \circ R := RS \in \text{Rel}(\mathcal{X}, \mathcal{Z})$  mit

$$x(RS)z \iff \exists y \in \mathcal{Y}: (xRy \wedge ySz) \quad \text{für alle } x \in \mathcal{X}, z \in \mathcal{Z}.$$

- (2) Die **Umkehrrelation** zu  $R \in \text{Rel}(\mathcal{X}, \mathcal{Y})$  ist die Relation  $R^{-1} \in \text{Rel}(\mathcal{Y}, \mathcal{X})$  mit

$$yR^{-1}x \iff xRy \quad \text{für alle } x \in \mathcal{X}, y \in \mathcal{Y}.$$

- (3) Die **komplementäre Relation** zu  $R \in \text{Rel}(\mathcal{X}, \mathcal{Y})$  ist die Relation  $R^c \in \text{Rel}(\mathcal{X}, \mathcal{Y})$  mit

$$xR^c y \iff \neg(xRy) \quad \text{für alle } x \in \mathcal{X}, y \in \mathcal{Y}.$$

Dies bedeutet, dass  $G_{R^c}$  das Komplement von  $G_R$  in  $\mathcal{X} \times \mathcal{Y}$  ist, also  $G_{R^c} = (G_R)^c$  gilt.

**Bemerkungen** (zu den Grundoperationen mit Relationen). Seien  $\mathcal{W}, \mathcal{X}, \mathcal{Y}, \mathcal{Z}$  Mengen.

- (1) Die Komposition von Relationen verallgemeinert die Komposition von Abbildungen.

Die Umkehrrelation verallgemeinert die Umkehrfunktion und existiert immer. Im Gegensatz zu Funktionen ist also auf der Ebene von Relationen die Umkehrbarkeit stets gegeben.

Die Komplement-Bildung hat bei Abbildungen kein Analogon.

- (2) Die Komposition ist assoziativ: Für  $R \in \text{Rel}(\mathcal{W}, \mathcal{X})$ ,  $S \in \text{Rel}(\mathcal{X}, \mathcal{Y})$ ,  $T \in \text{Rel}(\mathcal{Y}, \mathcal{Z})$  gilt

$$(RS)T = R(ST).$$

- (3) Die Umkehrung und die Komplement-Bildung sind involutorisch: Für  $R \in \text{Rel}(\mathcal{X}, \mathcal{Y})$  gilt

$$(R^{-1})^{-1} = R = (R^c)^c.$$

**Beispiele** (zu den Grundoperationen mit Relationen).

- (1) Für die Relationen des früheren Beispiels (1) gelten  $(\overset{\text{g}}{\underset{\sim}{\text{g}}})^{-1} = \overset{\text{g}}{\underset{\sim}{\text{g}}}$ ,  $(\overset{\text{u}}{\underset{\sim}{\text{u}}})^{-1} = \overset{\text{u}}{\underset{\sim}{\text{u}}}$ ,  $(\overset{\text{g}}{\underset{\sim}{\text{g}}})^c = \overset{\text{u}}{\underset{\sim}{\text{u}}}$ ,  $(\overset{\text{u}}{\underset{\sim}{\text{u}}})^c = \overset{\text{g}}{\underset{\sim}{\text{g}}}$ .

- (2) Für die Relationen aus den Beispielen (2), (3), (4), (5), (6) vom Abschnittanfang gelten: **Umkehrrelationen zu  $=, \neq, \subset, \subsetneq, \in, <, \leq$  sind  $=, \neq, \supset, \supsetneq, \ni, >, \geq$**  (sofern definiert, aber ansonsten egal, ob zwischen Elementen, Mengen, Zahlen, Abbildungen). **Komplementär zu  $=, \subset, \in, <, \leq$  sind  $\neq, \not\subset, \notin, \geq, >$**  (sofern definiert bei Elementen, Mengen, Zahlen — aber, wie in Beispiel (6) erklärt, nicht unbedingt bei Abbildungen).
- (3) Die **nächstkleinere ganze Zahl** zu einer reellen Zahl  $x \in \mathbb{R}$ , also die eindeutige Zahl  $z \in \mathbb{Z}$  mit  $z \leq x < z+1$ , schreibt man mit der sogenannten **Gauß-Klammer** als  $[x] \in \mathbb{Z}$ . Die **Abrunden-Funktion**  $A: \mathbb{R} \rightarrow \mathbb{Z}, x \mapsto [x]$  ist surjektiv, aber nicht injektiv und nicht bijektiv und als Funktion nicht umkehrbar. Die Umkehrrelation existiert aber immer und ist in diesem Fall die Relation  $A^{-1} \in \text{Rel}(\mathbb{Z}, \mathbb{R})$  mit  $G_{A^{-1}} = \{(z, r) \in \mathbb{Z} \times \mathbb{R} \mid z \leq r < z+1\}$ . Die Graphen von  $A$  und  $A^{-1}$  werden in Abbildung 27 gezeigt.

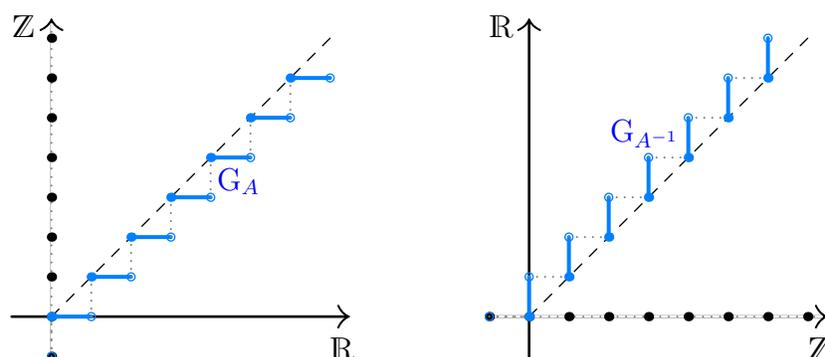


Abb. 27: Der Graph  $G_A$  der Abrunden-Funktion  $A \in \text{Abb}(\mathbb{R}, \mathbb{Z})$  und der Graph  $G_{A^{-1}}$  ihrer Umkehrrelation  $A^{-1} \in \text{Rel}(\mathbb{Z}, \mathbb{R})$

Die beiden wirklich wichtigen Klassen von Relationen werden nun in Kürze über die Gültigkeit (einiger) der folgenden Eigenschaften definiert.

**Definitionen (Relationseigenschaften).** Eine Relation  $R$  auf einer Menge  $\mathcal{X}$  heißt ...

- (1) **reflexiv**, wenn  $x R x$  für alle  $x \in \mathcal{X}$  gilt,
- (2) **symmetrisch**, wenn für alle  $x, y \in \mathcal{X}$  gilt:

$$x R y \implies y R x,$$

- (3) **asymmetrisch**, wenn es **kein** Paar  $(x, y) \in \mathcal{X}^2$  mit  $x R y$  und  $y R x$  gibt,
- (4) **antisymmetrisch**, wenn für alle  $x, y \in \mathcal{X}$  gilt:

$$(x R y \text{ und } y R x) \implies x = y,$$

- (5) **transitiv**, wenn für alle  $x, y, z \in \mathcal{X}$  gilt:

$$(x R y \text{ und } y R z) \implies x R z.$$

**Bemerkungen** (zu den Relationseigenschaften). Für  $R \in \text{Rel}(\mathcal{X})$  sieht man problemlos:

- (1) Ist  $R$  symmetrisch, so gilt für alle  $x, y \in \mathcal{X}$  automatisch auch:  $x R y \iff y R x$ . Deshalb ist  $R$  genau dann symmetrisch, wenn  $R^{-1} = R$  gilt.

- (2) Asymmetrie und Symmetrie von  $R$  schließen einander aus (außer wenn  $R = \emptyset$ ).
- (3) Asymmetrie und Reflexivität von  $R$  schließen einander aus (außer wenn  $\mathcal{X} = \emptyset$ ). Antisymmetrie kann man als schwächere Form von Asymmetrie sehen, die Reflexivität noch erlaubt.
- (4) Alle fünf gerade definierten Eigenschaften übertragen sich von  $R$  auf  $R^{-1}$  (und wegen  $(R^{-1})^{-1} = R$  natürlich auch von  $R^{-1}$  auf  $R$ ).

### 2.3.1 Ordnungsrelationen

Wir können nun eine wichtige Klasse von Relationen definieren und diskutieren:

**Definitionen (Ordnungsrelationen).**

- (I) Eine **Ordnungsrelation, partielle Ordnung oder Halbordnung** auf einer Menge  $\mathcal{X}$  ist eine **reflexive, antisymmetrische und transitive** Relation auf  $\mathcal{X}$ .
- (II) Eine **strikte Ordnungsrelation, strikte partielle Ordnung oder strikte Halbordnung** auf einer Menge  $\mathcal{X}$  ist eine **asymmetrische und transitive** Relation auf  $\mathcal{X}$ .

**Bemerkungen** (zu Ordnungsrelationen).

- (1) **Achtung!** Eine strikte Ordnungsrelation ist nicht etwa eine Ordnungsrelation mit Zusatzeigenschaft. Vielmehr kann  $R \in \text{Rel}(\mathcal{X})$  auf  $\mathcal{X} \neq \emptyset$ , weil Reflexivität und Asymmetrie einander ja ausschließen, **nie zugleich Ordnungsrelation und strikte Ordnungsrelation** sein.
- (2) Es besteht aber eine **1-zu-1-Korrespondenz zwischen Ordnungsrelationen und strikten Ordnungsrelationen** durch folgende zueinander inverse Operationen: Zu jeder Ordnungsrelation  $\leq$  auf  $\mathcal{X}$  gehört eine strikte Ordnungsrelation  $\triangleleft$  auf  $\mathcal{X}$  mit „weggelassenen Gleichheitsfällen“, also mit  $x \triangleleft y \iff (x \leq y \wedge x \neq y)$  für  $x, y \in \mathcal{X}$ . Umgekehrt gehört zu jeder strikten Ordnungsrelation  $\triangleleft$  auf  $\mathcal{X}$  eine Ordnungsrelation  $\leq$  auf  $\mathcal{X}$  mit „hinzugefügten Gleichheitsfällen“, also mit  $x \leq y \iff (x \triangleleft y \vee x = y)$  für  $x, y \in \mathcal{X}$ .
- (3) Da sich alle relevanten Eigenschaften übertragen, ist die Umkehrrelation einer (strikten) Ordnungsrelation wieder eine (strikte) Ordnungsrelation.

**Beispiele** (für Ordnungsrelationen). In den früheren Beispielen (2), (3), (5), (6), (7) gilt:

- (1) Die Relationen  $=, \subset, \supset, \leq, \geq$  **sind Ordnungsrelationen**, aber (außer auf leerer Grundmenge) keine strikten Ordnungsrelationen.
- (2) Die Relationen  $\subsetneq, \supsetneq, <, >$  **sind strikte Ordnungsrelationen**, aber (außer auf leerer Grundmenge) keine Ordnungsrelationen.
- (3) Die Ungleichheitsrelation  $\neq$  ist symmetrisch, ist aber (jedenfalls auf einer Grundmenge mit mindestens zwei Elementen) weder reflexiv noch asymmetrisch noch antisymmetrisch noch transitiv und damit weder Ordnungsrelation noch strikte Ordnungsrelation.
- (4) Für die Praxis wenig relevante, aber vielleicht illustrative Beispiele mit Parameter  $\delta \in \mathbb{R}$ ,  $\delta > 0$  sind die strikte (!) Ordnungsrelation  $\leq^\delta \in \text{Rel}(\mathbb{R})$  und die Ordnungsrelation  $\leq_\delta \in \text{Rel}(\mathbb{R})$ , die durch  $x \leq^\delta y \iff x + \delta \leq y$  und  $x \leq_\delta y \iff (x + \delta < y \vee x = y)$  für  $x, y \in \mathbb{R}$  definiert sind. Anschaulich spielt  $\delta$  hier die Rolle eines Mindestabstands: Auf der Zahlengeraden bedeutet  $x \leq^\delta y$ , dass  $y$  um mindestens  $\delta$  rechts von  $x$  liegen muss, und  $x \leq_\delta y$ , dass  $y$  um mehr als  $\delta$  rechts von  $x$  liegen oder alternativ exakt gleich  $x$  sein muss.

- (5) Die Teilbarkeitsrelationen „|“ auf  $\mathbb{N}$  und  $\mathbb{N}_0$  sind Ordnungsrelationen, aber keine strikten Ordnungsrelationen. Die Teilbarkeitsrelation „|“ auf  $\mathbb{Z}$  dagegen ist zwar reflexiv und transitiv, aber weder asymmetrisch noch antisymmetrisch (wie man z.B. an  $(-1)|1$  und  $1|(-1)$  sieht) und damit weder Ordnungsrelation noch strikte Ordnungsrelation.

**Definitionen (Totalordnungen und Ketten).** Sei  $\mathcal{X}$  eine Menge.

- (I) Eine Ordnungsrelation  $\leq$  auf  $\mathcal{X}$  heißt eine **Totalordnung, totale Ordnung oder lineare Ordnung** auf einer Teilmenge  $T$  von  $\mathcal{X}$ , wenn  $(x \leq y) \vee (y \leq x)$  für alle  $x, y \in T$  gilt. Wir nennen  $T$  dann eine **total/linear geordnete Teilmenge** von  $\mathcal{X}$  oder eine **Kette** in  $\mathcal{X}$ .
- (II) Wir verwenden dieselben Begriffe für eine strikte Ordnungsrelation  $\triangleleft$  auf  $\mathcal{X}$ , wenn sie für die „nicht-strikte“ Ordnungsrelation  $\leq$  auf  $\mathcal{X}$  mit  $x \leq y \iff ((x \triangleleft y) \vee (x = y))$  für alle  $x, y \in \mathcal{X}$  erfüllt sind. Speziell ist  $\triangleleft$  genau dann eine **strikte Totalordnung**, wenn für alle  $x, y \in T$  eine (und dann automatisch genau eine) der drei Aussagen  $x \triangleleft y, y \triangleleft x, x = y$  gilt.

**Bemerkungen** (zu Totalordnungen). Sei  $\mathcal{X}$  eine Menge.

- (1) Bei einer Totalordnung  $\leq$  auf  $\mathcal{X}$  können zwei Elemente  $x, y \in \mathcal{X}$  stets auf irgendeine Weise verglichen werden: Es gilt stets  $x \leq y$  oder  $y \leq x$ . Bei einer allgemeinen Ordnungsrelation dagegen kann es passieren (vergleiche die folgenden Beispiele), dass für zwei Elemente  $x, y \in \mathcal{X}$  weder  $x \leq y$  noch  $y \leq x$  gilt, also überhaupt kein Vergleich zwischen  $x$  und  $y$  gezogen werden kann. Diese Möglichkeit, dass man in manchen Fällen eben gar nicht vergleichen kann, ist der Grund, warum man auch von *nur partiellen* Ordnungen oder *Halbordnungen* spricht. Analog verhält es sich natürlich bei strikten Ordnungsrelationen.
- (2) Die Umkehrrelation einer (strikten) Totalordnung ist eine (strikte) Totalordnung. Dies folgt nach vorigen Bemerkungen quasi durch „scharfes Ansehen“ der Totalordnungs-Eigenschaft.
- (3) In den Übungen zeigen Sie für Komplemente:  $\leq \in \text{Rel}(\mathcal{X})$  ist genau dann eine Totalordnung auf  $\mathcal{X}$ , wenn  $\leq^c$  eine strikte Totalordnung auf  $\mathcal{X}$  ist. Umgekehrt damit auch:  $\triangleleft \in \text{Rel}(\mathcal{X})$  ist genau dann eine strikte Totalordnung auf  $\mathcal{X}$ , wenn  $\triangleleft^c$  eine Totalordnung auf  $\mathcal{X}$  ist.

**Beispiele** (für Totalordnungen und nicht-totale Ordnungen).

- (1) Die Relationen  $\leq, \geq$  sind **Totalordnungen** und  $<, >$  **strikte Totalordnungen** auf den reellen Zahlen  $\mathbb{R}$ , insbesondere auch auf  $\mathbb{N}, \mathbb{N}_0, \mathbb{Z}, \mathbb{Q}$  und jeder Teilmenge  $T \subset \mathbb{R}$ .
- (2) **Zwischen Paaren, Tripeln oder Tupeln** von Zahlen oder mit anderen Worten auf  $\mathbb{B}^n$  mit  $\mathbb{B} \in \{\mathbb{N}, \mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}\}$  und  $n \in \mathbb{N} \setminus \{1\}$  gibt es **keine kanonische Totalordnung** oder jedenfalls keine, die so kanonisch wäre wie  $\leq$  oder  $\geq$  zwischen einzelnen Zahlen.

Für  $n = 2$  kann man zwar Ordnungsrelationen  $\leq_{\text{komp}}$  und  $\leq_{\text{komp}}$  auf  $\mathbb{B}^2$  **komponentenweise** durch

$$\begin{aligned} x \leq_{\text{komp}} y &\iff (x_1 \leq y_1, x_2 \leq y_2) && \text{für } x, y \in \mathbb{B}^2, \\ x \leq_{\text{komp}} y &\iff ((x_1 < y_1, x_2 < y_2) \vee (x_1 = y_1, x_2 = y_2)) && \text{für } x, y \in \mathbb{B}^2 \end{aligned}$$

erklären, aber  $\leq_{\text{komp}}$  und  $\leq_{\text{komp}}$  sind **keine Totalordnungen** auf  $\mathbb{B}^2$ . Nichtsdestotrotz gibt es für diese Relationen aber Ketten in  $\mathbb{B}^2$  wie  $\{(3, 2), (6, 2), (7, 4), (8, 9)\}$  (nur für  $\leq_{\text{komp}}$ ) und  $\{x \in \mathbb{B}^2 \mid x_1 = x_2\}$  (für  $\leq_{\text{komp}}$  und  $\leq_{\text{komp}}$ ), bei denen eine (strikte) Ordnung der Elemente bezüglich beider Einträge *zugleich* vorliegt oder vorgenommen werden kann.

Alternativ erhält man durch die sogenannte **lexikographische Ordnung** (die sich an die übliche Sortierung von Worten zunächst nach dem ersten Buchstaben, dann nach dem zweiten, dem dritten und den folgenden anlehnt)

$$x \leq_{\text{lex}} y \iff ((x_1 < y_1) \vee (x_1 = y_1, x_2 \leq y_2)) \quad \text{für } x, y \in \mathbb{B}^2$$

**tatsächlich eine Totalordnung**  $\leq_{\text{lex}}$  auf  $\mathbb{B}^2$ , bei der die Priorisierung allein aufgrund des ersten Eintrags aber nicht unbedingt natürlich anmutet.

Selbstverständlich kann man bei diesen Bildungen auch die Umkehrrelationen, die zugehörigen strikten Ordnungsrelationen und Verallgemeinerungen auf  $\mathbb{B}^n$  mit beliebigem  $n \in \mathbb{N} \setminus \{1\}$  betrachten und erhält dafür weitgehend analoge Eigenschaften.

- (3) Die Relationen  $\leq, \geq, <, >$  auf  $\text{Abb}(\mathcal{X}, T)$  mit  $T \subset \mathbb{R}$ , also **zwischen Abbildungen**, sind dagegen **keine (strikten) Totalordnungen**, jedenfalls sofern  $\mathcal{X}$  und  $T$  mindestens zwei Elemente haben: Sind nämlich  $f, g \in \text{Abb}(\mathcal{X}, T)$  mit  $f(x) < g(x)$  für ein  $x \in \mathcal{X}$  und  $g(\tilde{x}) < f(\tilde{x})$  für ein anderes  $\tilde{x} \in \mathcal{X}$ , so gilt weder  $f \leq g$  noch  $g \leq f$  (bzw. weder  $f < g$  noch  $g < f$  noch  $f = g$ ). Nichtsdestotrotz gibt es für diese Relationen aber Ketten in  $\text{Abb}(\mathcal{X}, T)$ , etwa die Teilmenge aller *konstanten* Abbildungen  $\mathcal{X} \rightarrow T$ .
- (4) Die Relationen  $\subset, \supset, \subsetneq, \supsetneq$  sind **keine (strikten) Totalordnungen** auf  $\mathcal{P}(\mathcal{X})$ , sofern die Grundmenge  $\mathcal{X}$  zwei verschiedene Elemente  $x \neq \tilde{x}$  enthält, denn für  $\{x\}, \{\tilde{x}\} \in \mathcal{P}(\mathcal{X})$  gilt dann weder  $\{x\} \subset \{\tilde{x}\}$  noch  $\{\tilde{x}\} \subset \{x\}$  (bzw. weder  $\{x\} \subsetneq \{\tilde{x}\}$  noch  $\{\tilde{x}\} \subsetneq \{x\}$  noch  $\{x\} = \{\tilde{x}\}$ ). Es gibt aber für diese Relationen (viele) Ketten in  $\mathcal{P}(\mathcal{X})$ , z.B. ist für  $\mathcal{X} = \mathbb{N}$  das Mengensystem

$$\{\emptyset, \{-3\}, \{-3, 5\}, \{-3, 5, 0\}, \{-3, 5, 0, 8, -2\}, \{-3, 5, 0, 8, -2, 4\}, \{-3, 5, 0, 8, -2, 4, 1, 2, 3\}\}$$

ein **Beispiel einer Kette in  $\mathcal{P}(\mathbb{N})$** . Es gibt in  $\mathcal{P}(\mathbb{N})$  neben solchen endlichen auch unendliche Ketten von analoger Natur.

**Definitionen (Schranken und größte/kleinste/maximale/minimale Elemente).** Sei  $\trianglelefteq$  eine Ordnungsrelation auf einer Menge  $\mathcal{X}$  und  $T$  eine Teilmenge von  $\mathcal{X}$ .

- (I) Wir nennen  $s \in \mathcal{X}$  eine **obere Schranke** bzw. **untere Schranke** für  $T$  in  $\mathcal{X}$ , wenn  $x \trianglelefteq s$  bzw.  $s \trianglelefteq x$  für alle  $x \in T$  gilt. Ist eine obere Schranke bzw. untere Schranke für  $T$  selbst Element von  $T$ , so heißt sie ein **größtes Element** bzw. **kleinstes Element** von  $T$ .
- (II) Wir nennen  $m \in T$  ein **maximales Element** bzw. **minimales Element** von  $T$ , wenn für jedes  $x \in T$  mit  $m \trianglelefteq x$  bzw.  $x \trianglelefteq m$  schon  $x = m$  gilt.

**Bemerkungen** (zu den vorausgehenden Begriffen). Sei  $\trianglelefteq$  Ordnungsrelation auf  $\mathcal{X}$  und  $T \subset \mathcal{X}$ .

- (1) **Falls ein größtes/kleinstes Element** von  $T$  existiert, ist dieses immer **eindeutig** und ist auch das **eindeutige maximale/minimale Element** von  $T$  und die **kleinste obere/größte untere Schranke** für  $T$  (wobei  $s_* \in \mathcal{X}$  kleinste obere/größte untere Schranke für  $T$  heißt, wenn  $s_*$  selbst obere/untere Schranke für  $T$  ist und  $s_* \trianglelefteq s$  bzw.  $s \trianglelefteq s_*$  für alle oberen/unteren Schranken  $s \in \mathcal{X}$  für  $T$  erfüllt).

*Beweis.* Es existiere ein größtes Element  $g \in T$  von  $T$ . Wir begründen, dass ...

- dieses größte Element eindeutig ist: Ist auch  $\tilde{g} \in T$  ein größtes Element von  $T$ , so gilt sowohl  $g \trianglelefteq \tilde{g}$  als auch  $\tilde{g} \trianglelefteq g$ , und die Antisymmetrie von  $\trianglelefteq$  gibt  $\tilde{g} = g$ .

- $g$  die kleinste obere Schranke für  $T$  ist: Per Definition ist  $g$  obere Schranke für  $T$  und  $g \leq s$  für jede obere Schranke  $s \in \mathcal{X}$  für  $T$ . Also ist  $g$  die kleinste obere Schranke für  $T$ .
- $g$  das eindeutige maximale Element von  $T$  ist: Da jedes  $x \in T$  mit  $g \leq x$  zusätzlich  $x \leq g$  und dann per Antisymmetrie auch  $x = g$  erfüllt, ist  $g$  ein maximales Element von  $T$ . Ist auch  $m \in T$  ein maximales Element, so gilt mit  $m \leq g$  sofort auch  $m = g$ . Daher ist  $g$  tatsächlich das eindeutige maximale Element von  $T$ .

Existiert stattdessen ein kleinstes Element von  $T$ , so kann man analog argumentieren oder durch Übergang zu  $\leq^{-1}$  auf das Vorige reduzieren.  $\square$

- (2) **Für total geordnetes  $T$  sind maximale/minimale Elemente von  $T$  dasselbe wie größte/kleinste Elemente von  $T$ .** Insbesondere greift (1) dann auch für ein maximales/minimales Element.

*Beweis.* Gemäß Bemerkung (1) ist ein größtes Element von  $T$  stets auch ein maximales Element von  $T$ . Wir zeigen, dass umgekehrt ein maximales Element  $m \in T$  von  $T$  stets auch ein größtes Element von  $T$  ist: Sei dazu  $x \in T$  beliebig. Da  $T$  total geordnet ist, gilt entweder  $x \leq m$  oder  $m \leq x$ . Im zweiten Fall folgt  $x = m$  per Maximalität von  $m$  und damit  $x \leq m$  gemäß der Reflexivität von  $\leq$ . Also gilt tatsächlich  $x \leq m$  für jedes  $x \in T$ , und  $m$  ist ein größtes Element von  $T$ .

Analog oder durch Übergang zu  $\leq^{-1}$  behandelt man kleinste und minimale Elemente.  $\square$

**Beispiele** (von größten und maximalen Elementen).

- (1) Bezüglich der Totalordnung  $\leq$  auf  $\mathbb{R}$  ist das größte/kleinste Element einer Teilmenge im üblichen Sinn zu verstehen, zum Beispiel ist 5 das größte Element von  $\{x \in \mathbb{R} \mid x < 0\} \cup \{5\} \cup \{2\}$ . Es gibt Teilmengen ohne größtes Element, aber mit oberer Schranke, etwa  $\{x \in \mathbb{R} \mid x < 0\}$ , und auch Teilmengen ohne obere Schranke, zum Beispiel  $\mathbb{N}$ .
- (2) Ein größtes/kleinstes Element bezüglich der Totalordnung  $\geq$  ist ein kleinstes/größtes Element im herkömmlichen Sinn. Um Verwirrung zu vermeiden, wendet man die obigen Begriffe in diesem Wortlaut daher nur auf  $\leq$  und ähnliche, „nach oben gerichtete“ Relationen an.
- (3) Wir betrachten  $T := \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2)\} \subset \mathbb{N}^2$  bezüglich der Ordnungsrelationen  $\leq_{\text{komp}}$ ,  $\leq_{\text{lex}}$  aus einem früheren Beispiel (2). Dieses  $T$  hat bezüglich  $\leq_{\text{komp}}$  genau  $(1, 4)$  und  $(2, 2)$  als maximale Elemente und  $(2, 4)$  als kleinste obere Schranke, hat bezüglich  $\leq_{\text{komp}}$  genau  $(1, 2)$ ,  $(1, 3)$ ,  $(1, 4)$  und  $(2, 2)$  als maximale Elemente und  $(3, 5)$  als kleinste obere Schranke und hat bezüglich der Totalordnung  $\leq_{\text{lex}}$  das größte Element  $(2, 2)$ .
- (4) Bezüglich der Ordnungsrelation  $\subset$  hat die Teilmenge  $T := \{\{1\}, \{1, 2\}, \{1, 2, 3\}, \{2, 3\}, \{2, 4\}\}$  von  $\mathcal{P}(\{1, 2, 3, 4, 5\})$  genau  $\{1, 2, 3\}$  und  $\{2, 4\}$  als maximale Elemente. Obere Schranken für  $T$  sind genau  $\{1, 2, 3, 4\}$  und  $\{1, 2, 3, 4, 5\}$ . Ein größtes Element von  $T$  gibt es nicht.
- (5) Betrachten wir  $T := \{x \in \mathbb{R} \mid x \leq 0\}$  bezüglich der Ordnungsrelation  $\leq^\delta \in \text{Rel}(\mathbb{R})$  mit Parameter  $\delta \in \mathbb{R}$ ,  $\delta > 0$ , aus einem früheren Beispiel (4), so sind die maximalen Elemente für  $T$  genau die  $m \in \mathbb{R}$  mit  $-\delta \leq m \leq 0$  und die oberen Schranken für  $T$  genau die  $m \in \mathbb{R}$  mit  $m > \delta$ . Ein größtes Element von  $T$  gibt es nicht.

Es folgt ein allgemeines Resultat über Ordnungsrelationen, dessen Bedeutung sich nicht unbedingt auf den ersten Blick erschließt, das aber später wichtige Anwendungen hat:

**Lemma (Zornsches Lemma).** *Sei  $\leq$  eine Ordnungsrelation auf einer Menge  $\mathcal{X}$ . Wenn für jede Kette in  $\mathcal{X}$  eine obere Schranke in  $\mathcal{X}$  existiert, dann gibt es ein maximales Element von  $\mathcal{X}$ .*

Der Beweis des Zornschen Lemmas verwendet ganz wesentlich das Auswahlaxiom der Mengenlehre und kann entweder mit Hilfe sogenannter Ordinalzahlen oder elementar geführt werden. Beides geht über den Vorlesungsstoff hinaus, weshalb wir die elementare Argumentation nur als Kleingedrucktes angeben:

*Beweis.* Sei  $\mathcal{K}$  das Mengensystem aller Ketten in  $\mathcal{X}$ , auf dem wir die Mengen-Inklusion „ $\subset$ “ als Ordnungsrelation betrachten.

Wir zeigen zunächst, dass die Behauptung des Lemmas folgt, sobald die Existenz eines maximalen Elements von  $\mathcal{K}$  nachgewiesen ist. Sei also  $M \in \mathcal{K}$  ein maximales Element von  $\mathcal{K}$ . Dann existiert für die Kette  $M$  in  $\mathcal{X}$  nach Voraussetzung des Lemmas eine obere Schranke  $s$  in  $\mathcal{X}$ . Um zu zeigen, dass  $s$  auch ein maximales Element von  $\mathcal{X}$  ist, sei weiter  $x \in \mathcal{X}$  mit  $s \preceq x$ . Dann ist auch  $M \cup \{x\}$  eine Kette in  $\mathcal{X}$  (denn Reflexivität gibt  $x \preceq x$ , die Schrankeneigenschaft von  $s$  gibt  $m \preceq s$  für alle  $m \in M$  und mit Transitivität folgt  $m \preceq x$  für alle  $m \in M$ ). Also ist  $M \cup \{x\} \in \mathcal{K}$ , und wegen der Maximalität von  $M$  folgt  $M = M \cup \{x\}$ , also  $x \in M$ . Wegen der Schrankeneigenschaft von  $s$  bedeutet dies  $x \preceq s$  und wegen Antisymmetrie von  $\preceq$  dann  $x = s$ . Damit ist  $s$  das gewünschte maximale Element von  $\mathcal{X}$ .

Im Hauptteil des Beweises zeigen wir nun die Existenz eines maximalen Elements  $M$  von  $\mathcal{K}$ . Dazu verwenden wir erst das Auswahlaxiom, um auf die Existenz einer Auswahl-Abbildung  $f: \mathcal{P}(\mathcal{X}) \setminus \{\emptyset\} \rightarrow \mathcal{X}$  mit  $f(T) \in T$  für alle nicht-leeren  $T \subset \mathcal{X}$  zu schließen. (Genauer kann die Existenz von  $f$  dadurch begründet werden, dass Bemerkung (4) zum Abbildungsbegriff aus dem aktuellen Abschnitt 2.3 auf die umgekehrte Element-Relation „ $\ni$ “ zwischen  $\mathcal{P}(\mathcal{X}) \setminus \{\emptyset\}$  und  $\mathcal{X}$  angewandt wird.) Als Nächstes vereinbaren wir für Ketten  $T \in \mathcal{K}$  die Notation  $\hat{T} := \{x \in \mathcal{X} \mid T \cup \{x\} \in \mathcal{K}\}$  und definieren dann eine Abbildung  $g: \mathcal{K} \rightarrow \mathcal{K}$ , die eine Kette wenn möglich um ein mit Hilfe von  $f$  ausgewähltes Element erweitert, durch

$$g(T) := \begin{cases} T & \text{falls } T \text{ maximales Element von } \mathcal{K} \\ T \cup \{f(\hat{T} \setminus T)\} & \text{andernfalls} \end{cases}$$

für alle  $T \in \mathcal{K}$ . Formal ist die Abbildung  $g$  wohldefiniert, weil es für nicht-maximales  $T$  eine Kette  $\tilde{T} \in \mathcal{K}$  mit  $T \subsetneq \tilde{T}$  gibt und mit  $T \subsetneq \tilde{T} \subset \hat{T}$  dann  $\hat{T} \setminus T \neq \emptyset$ , Wohldefiniertheit von  $f(\hat{T} \setminus T) \in \hat{T} \setminus T$  und  $T \cup \{f(\hat{T} \setminus T)\} \in \mathcal{K}$  sichergestellt sind.

Für den weiteren Beweis nennen wir ein System von Ketten  $\mathcal{T} \subset \mathcal{K}$  einen **Turm**, wenn es folgende Eigenschaften hat:

- (A) Es gilt  $\emptyset \in \mathcal{T}$ .
- (B) Für jedes  $T \in \mathcal{T}$  ist  $g(T) \in \mathcal{T}$ .
- (C) Für jede Kette (von Ketten)  $\mathcal{S} \subset \mathcal{T}$  ist  $\bigcup \mathcal{S} \in \mathcal{T}$ .

Nun argumentieren wir in aufeinander aufbauenden Schritten:

- 1) *Behauptung.* Das Mengensystem  $\mathcal{K}$  aller Ketten ist ein Turm.

Die Eigenschaften (A) und (B) sind für  $\mathcal{K}$  klar. Für (C) ist zu zeigen, dass für eine Kette von Ketten  $\mathcal{S} \subset \mathcal{K}$  auch  $\bigcup \mathcal{S}$  eine Kette ist, also  $\bigcup \mathcal{S} \in \mathcal{K}$  gilt. Seien dazu  $x, \tilde{x} \in \bigcup \mathcal{S}$ . Es gibt dann  $T, \tilde{T} \in \mathcal{S}$  mit  $x \in T$  und  $\tilde{x} \in \tilde{T}$ , und wegen der Ketteneigenschaft von  $\mathcal{S}$  gilt  $T \subset \tilde{T}$  oder  $\tilde{T} \subset T$ . Somit gilt  $x, \tilde{x} \in \tilde{T}$  oder  $x, \tilde{x} \in T$ . Als Elemente einer Kette ( $\tilde{T}$  oder  $T$ ) erfüllen  $x, \tilde{x}$  dann  $x \preceq \tilde{x}$  oder  $\tilde{x} \preceq x$ . Damit ist  $\bigcup \mathcal{S}$  eine Kette.

- 2) *Behauptung.* Ein beliebiger Durchschnitt von Türmen ist wieder ein Turm.

Dies ist klar, das sich die drei Eigenschaften (A), (B), (C) problemlos auf den Durchschnitt übertragen.

- 3) In Anbetracht der Schritte 1) und 2) können wir einen „kleinsten“ Turm  $\mathcal{T}_0$  als Durchschnitt aller Türme  $\mathcal{T} \subset \mathcal{K}$  erhalten. Damit definieren wir

$$\mathcal{V} := \{V \in \mathcal{T}_0 \mid \forall T \in \mathcal{T}_0: ((T \subset V) \vee (V \subset T))\} \quad \text{und} \quad \mathcal{T}_V := \{T \in \mathcal{T}_0 \mid (T \subset V) \vee (g(V) \subset T)\} \text{ für } V \in \mathcal{V}.$$

- 4) *Behauptung.* Für jedes  $V \in \mathcal{V}$  ist  $\mathcal{T}_V$  ein Turm.

Die Eigenschaft (A) ist klar. Für (B) betrachten wir  $T \in \mathcal{T}_V \subset \mathcal{T}_0$  und bemerken  $g(T) \in \mathcal{T}_0$  (da  $\mathcal{T}_0$  ein Turm ist). Es tritt nun einer der drei Fälle  $T \subset V \subset g(T)$ ,  $T \not\subset V$ ,  $V \not\subset g(T)$  ein. Im Fall  $T \subset V \subset g(T)$  gilt, da sich  $g(T)$  von  $T$  um höchstens ein Element unterscheidet,  $(V = g(T)) \vee (T = V)$  und damit insbesondere  $(g(T) \subset V) \vee (g(V) \subset g(T))$ , was  $g(T) \in \mathcal{T}_V$  bedeutet. Im Fall  $T \not\subset V$  gilt wegen  $T \in \mathcal{T}_V$  notwendig  $g(V) \subset T \subset g(T)$  und  $g(T) \in \mathcal{T}_V$ . Im Fall  $V \not\subset g(T)$  gilt wegen  $V \in \mathcal{V}$  notwendig  $g(T) \subset V$  und damit  $g(T) \in \mathcal{T}_V$ . Also gilt  $g(T) \in \mathcal{T}_V$  in allen Fällen, und die Eigenschaft (B) ist für  $\mathcal{T}_V$  gezeigt. Für die Eigenschaft (C) betrachten wir eine Kette von Ketten  $\mathcal{S} \subset \mathcal{T}_V \subset \mathcal{T}_0$  und bemerken  $\bigcup \mathcal{S} \in \mathcal{T}_0$  (da  $\mathcal{T}_0$  ein Turm ist). Nach Definition von  $\mathcal{T}_V$  gilt entweder  $\exists T \in \mathcal{S}: g(V) \subset T$ , somit  $g(V) \subset \bigcup \mathcal{S}$  und  $\bigcup \mathcal{S} \in \mathcal{T}_V$ , oder es gilt  $\forall T \in \mathcal{S}: T \subset V$ , somit  $\bigcup \mathcal{S} \subset V$  und erneut  $\bigcup \mathcal{S} \in \mathcal{T}_V$ . Damit ist (C) für  $\mathcal{T}_V$  gezeigt.

- 5) *Behauptung.* Für alle  $V \in \mathcal{V}$  gilt  $\mathcal{T}_V = \mathcal{T}_0$ .

Dies folgt, da einerseits  $\mathcal{T}_V$  gemäß 4) ein Turm mit  $\mathcal{T}_V \subset \mathcal{T}_0 \subset \mathcal{K}$  und andererseits  $\mathcal{T}_0$  der Schnitt aller Türme  $\subset \mathcal{K}$  ist.

- 6) *Behauptung.* Auch  $\mathcal{V}$  ist ein Turm.

Die Eigenschaft (A) ist klar. Für (B) betrachten wir  $V \in \mathcal{V} \subset \mathcal{T}_0$  und bemerken wieder  $g(V) \in \mathcal{T}_0$ . Für jedes  $T \in \mathcal{T}_0$  gilt dann  $T \subset V$  oder  $V \subsetneq T$ . Im ersten Fall folgt trivial  $T \subset g(V)$ . Im zweiten Fall benutzen wir  $T \in \mathcal{T}_0 \stackrel{5)}{=} \mathcal{T}_V$  und erhalten  $g(V) \subset T$ . Insgesamt gilt für alle  $T \in \mathcal{T}_0$  also  $(T \subset g(V)) \vee (g(V) \subset T)$ , wir erhalten  $g(V) \in \mathcal{V}$ , und die Eigenschaft (B) ist für  $\mathcal{V}$  gezeigt. Für die Eigenschaft (C) betrachten wir eine Kette (von Ketten)  $\mathcal{S} \subset \mathcal{V} \subset \mathcal{T}_0$  und bemerken wieder  $\bigcup \mathcal{S} \in \mathcal{T}_0$ . Nach Definition von  $\mathcal{V}$  gilt für jedes  $T \in \mathcal{T}_0$  entweder  $\exists V \in \mathcal{S}: T \subset V$  und somit  $T \subset \bigcup \mathcal{S}$ , oder es gilt  $\forall V \in \mathcal{S}: V \subset T$  und somit  $\bigcup \mathcal{S} \subset T$ . Insgesamt gilt  $\forall T \in \mathcal{T}_0: ((T \subset \bigcup \mathcal{S}) \vee (\bigcup \mathcal{S} \subset T))$ , womit  $\bigcup \mathcal{S} \in \mathcal{V}$  und (C) für  $\mathcal{V}$  gezeigt sind.

7) *Behauptung.* Es gilt  $\mathcal{V} = \mathcal{T}_0$ .

Dies folgt, da einerseits  $\mathcal{V}$  gemäß 6) ein Turm mit  $\mathcal{V} \subset \mathcal{T}_0 \subset \mathcal{K}$  und andererseits  $\mathcal{T}_0$  der Schnitt aller Türme  $\subset \mathcal{K}$  ist.

8) *Behauptung.*  $\mathcal{T}_0$  ist eine Kette (von Ketten).

Für  $T, V \in \mathcal{T}_0 \stackrel{7)}{=} \mathcal{V}$  gilt  $(T \subset V) \vee (V \subset T)$  nach Definition von  $\mathcal{V}$ .

9) *Behauptung.* Es gibt ein maximales Element  $M$  von  $\mathcal{K}$ .

Da  $\mathcal{T}_0$  nach 8) eine Kette von Ketten und per Definition ein Turm ist, folgt  $M := \bigcup_{T \in \mathcal{T}_0} T \in \mathcal{T}_0$  gemäß Eigenschaft (C) des Turms  $\mathcal{T}_0$ . Weiter gilt  $g(M) \in \mathcal{T}_0$  gemäß Eigenschaft (B) des Turms  $\mathcal{T}_0$ , und gemäß Konstruktion von  $M$  ergibt sich  $g(M) \subset M$ . Nach Konstruktion von  $g$  gilt aber andererseits  $T \subsetneq g(T)$ , wann immer  $T \in \mathcal{K}$  nicht-maximales Element von  $\mathcal{K}$  ist. Somit verbleibt für  $M \in \mathcal{T}_0 \subset \mathcal{K}$  nur die Möglichkeit, dass  $M$  maximales Element von  $\mathcal{K}$  ist.

Damit ist der Beweis komplett.  $\square$

Als Nächstes kommen wir zu **Ordnungseigenschaften der natürlichen und ganzen Zahlen** bezüglich der Totalordnung  $\leq$  und der zugehörigen strikten Totalordnung  $<$ . Wir halten fest (wobei wir jetzt „kleinste Zahl“ für „kleinstes Element“ verwenden):

In  $\mathbb{N}$  bzw.  $\mathbb{N}_0$  ist 1 bzw. 0 die kleinste Zahl. Eine größte Zahl gibt es in  $\mathbb{N}$  und  $\mathbb{N}_0$  nicht. (\*)

In  $\mathbb{Z}$  gibt es weder eine kleinste noch eine größte Zahl.

Diese einleuchtenden Aussagen lassen sich auch auf Grundlage der bisherigen Definitionen verifizieren: Zum Beispiel übersetzt man die Aussage, dass 1 die kleinste Zahl in  $\mathbb{N}$  ist, mit den Definitionen des kleinsten Elements und der Relation  $\leq$  auf  $\mathbb{Z}$  (siehe das frühere Beispiel (5)) in die zu ihr äquivalenten Aussagen  $\forall n \in \mathbb{N}: 1 \leq n$  und  $\forall n \in \mathbb{N}: n-1 \in \mathbb{N}_0$ . Letztere erkennt man dann aufgrund des früher zu Nachfolgern und Vorgängern ganzer Zahlen Gesagten als richtig. Dass es keine größte Zahl in  $\mathbb{N}$  gibt, liegt natürlich einfach an  $n+1 > n$  für alle  $n \in \mathbb{N}$ . Mit denselben Argumenten bestätigt man die anderen obigen Aussagen sowie für jedes  $z \in \mathbb{Z}$ , dass

$z+1$  die kleinste Zahl in  $\{y \in \mathbb{Z} \mid z < y\}$  und  $z-1$  die größte Zahl in  $\{y \in \mathbb{Z} \mid y < z\}$  (\*\*)

ist. Eng verwandt ist auch:

**Proposition** (über **größte und kleinste Elemente in Mengen ganzer Zahlen**). *In jeder nicht-leeren Teilmenge von  $\mathbb{Z}$ , die eine obere Schranke in  $\mathbb{Z}$  besitzt, existiert eine größte Zahl, und in jeder nicht-leeren Teilmenge von  $\mathbb{Z}$ , die eine untere Schranke in  $\mathbb{Z}$  besitzt, existiert eine kleinste Zahl. Insbesondere haben  $\mathbb{N}$  und  $\mathbb{N}_0$  die (unten weiter diskutierte) Wohlordnungseigenschaft, gemäß der in jeder ihrer nicht-leeren Teilmengen eine kleinste Zahl existiert.*

*Beweis.* Wir zeigen erst die Existenz kleinster Zahlen in  $T$  für  $\emptyset \neq T \subset \mathbb{Z}$  mit unterer Schranke  $z_0$  für  $T$  in  $\mathbb{Z}$ . Dazu argumentieren wir indirekt: Angenommen, es gibt *keine* kleinste Zahl in  $T$ . Dann zeigen wir durch Induktion, dass jedes  $z \in \{z_0, z_0+1, z_0+2, \dots\}$  untere Schranke für  $T$  ist. Der Induktionsanfang für  $z = z_0$  ist per Voraussetzung gegeben. Für den Induktionsschritt sei  $z \in \mathbb{Z}$  untere Schranke für  $T$ , also  $T \subset \{y \in \mathbb{N} \mid z \leq y\}$ . Zudem ist aber  $z \notin T$  (denn sonst wäre  $z$  kleinste Zahl in  $T$ ) und damit sogar  $T \subset \{y \in \mathbb{N} \mid z < y\} = \{y \in \mathbb{N} \mid z+1 \leq y\}$ , wobei die Gleichheit aus (\*\*) resultiert. Dies bedeutet, dass  $z+1$  untere Schranke für  $T$  und der Induktionsschritt komplett ist. Insgesamt sind dann aber alle unteren Schranken  $z_0, z_0+1, z_0+2, \dots \notin T$ , da man sonst eine kleinste Zahl in  $T$  bekäme. Dies steht im Widerspruch zu  $T \neq \emptyset$  und beweist insgesamt die Existenz der kleinsten Zahl in  $T$ .

Die Existenz der größten Zahl in  $T$  für  $\emptyset \neq T \subset \mathbb{Z}$  mit oberer Schranke ergibt sich analog oder durch Anwendung des Vorigen auf  $\{-z \mid z \in \mathbb{Z}\}$ .

Die Wohlordnungseigenschaft von  $\mathbb{N}$  und  $\mathbb{N}_0$  folgt, da dort gemäß (\*) 1 bzw. 0 kleinstes Element und damit untere Schranken für jede Teilmenge ist.  $\square$

**Definition (Wohlordnungen).** Eine Ordnungsrelation auf einer Menge  $\mathcal{X}$  heißt eine **Wohlordnung** auf  $\mathcal{X}$ , wenn sie eine totale Ordnung auf ganz  $\mathcal{X}$  ist und bezüglich ihr jede nicht-leere Teilmenge von  $\mathcal{X}$  ein kleinstes Element besitzt.

Gemäß der vorigen Proposition ist die Standard-Ordnung „ $\leq$ “ eine Wohlordnung auf  $\mathbb{N}$  und  $\mathbb{N}_0$ . Auf  $\mathbb{Z}$  ist „ $\leq$ “ zwar keine Wohlordnung, man kann auf  $\mathbb{Z}$  und jeder Menge, die in Bijektion zu  $\mathbb{N}$  steht, aber ohne Probleme eine Wohlordnung erzeugen. Auf  $\mathbb{Z}$  sieht eine mögliche Wohlordnung  $\trianglelefteq$  zum Beispiel so aus, dass

$$0 \trianglelefteq 1 \trianglelefteq -1 \trianglelefteq 2 \trianglelefteq -2 \trianglelefteq 3 \trianglelefteq -3 \trianglelefteq 4 \trianglelefteq -4 \trianglelefteq \dots$$

gilt. Auf  $\mathbb{R}$  und anderen „großen“ Mengen dagegen kann man eine Wohlordnung nicht konstruktiv erhalten. Ihre pure Existenz ist dennoch sichergestellt durch:

**Satz (Wohlordnungssatz von Zermelo).** Für jede Menge  $\mathcal{X}$  gibt es eine Wohlordnung auf  $\mathcal{X}$ .

Der Beweis basiert auf dem Zornschen Lemma und wendet dieses Lemma in typischer Manier an:

*Beweisskizze.* Wir betrachten die Menge von Definitionsbereichen und Graphen von Wohlordnungen

$$\mathcal{W} := \{(D, G) \in \mathcal{P}(\mathcal{X}) \times \mathcal{P}(\mathcal{X}^2) \mid (D, D, G) \text{ ist eine Wohlordnung auf } D\}$$

(wobei das Tripel  $(D, D, G)$  wie ursprünglich definiert für die Relation auf  $D$  mit Graph  $G \subset D^2$  steht) und erklären eine Ordnungsrelation  $\in \in \text{Rel}(\mathcal{W})$  durch

$$(D, G) \in (\tilde{D}, \tilde{G}) \iff ((D \subset \tilde{D}) \wedge (G \subset \tilde{G}) \wedge (\forall x \in D: \forall y \in \tilde{D} \setminus D: (x, y) \in \tilde{G}))$$

für alle  $(D, G), (\tilde{D}, \tilde{G}) \in \mathcal{W}$ . Grob gesagt bedeutet  $(D, G) \in (\tilde{D}, \tilde{G})$  damit, dass die Relation  $\tilde{R} = (\tilde{D}, \tilde{D}, \tilde{G})$  die Relation  $R = (D, D, G)$  so fortsetzt, dass die Elemente von  $\tilde{D} \setminus D$  bezüglich  $\tilde{R}$  „größer oder gleich“ den Elementen von  $D$  sind.

Wir zeigen nun, dass die Voraussetzung des Zornschen Lemmas für  $\mathcal{W}$  mit der Relation  $\in$  erfüllt ist, dass also für jede Kette  $\mathcal{K} \subset \mathcal{W}$  eine obere Schranke in  $\mathcal{W}$  existiert. Dazu setzen wir für eine solche Kette  $D_{\mathcal{K}} := \bigcup \{D \mid (D, G) \in \mathcal{K}\} \subset \mathcal{P}(\mathcal{X})$  und  $G_{\mathcal{K}} := \bigcup \{G \mid (D, G) \in \mathcal{K}\} \subset \mathcal{P}(\mathcal{X}^2)$ . Damit ist  $G_{\mathcal{K}} \subset (D_{\mathcal{K}})^2$  der Graph einer Relation  $R_{\mathcal{K}} \in \text{Rel}(D_{\mathcal{K}})$ , und es ist nicht schwer zu sehen, dass  $R_{\mathcal{K}}$  eine Totalordnung auf  $D_{\mathcal{K}}$  ist (denn zum Nachweis von Reflexivität, Antisymmetrie, Transitivität und Totalordnungs-Eigenschaft operiert man mit höchstens drei Elementen von  $D_{\mathcal{K}}$  und kann sich mit der Ketteneigenschaft immer darauf zurückziehen, dass diese alle im Definitionsbereich  $D$  nur eines  $(D, G) \in \mathcal{K}$  liegen). Etwas schwieriger ist der folgende Nachweis, dass  $R_{\mathcal{K}}$  sogar eine Wohlordnung ist: Sei  $\emptyset \neq T \subset D_{\mathcal{K}}$ . Wir wählen  $t \in T$ . Dann gilt  $t \in D$  für ein  $(D, G) \in \mathcal{K}$ , und  $T \cap D \neq \emptyset$  besitzt bezüglich der Wohlordnung  $(D, D, G)$  ein kleinstes Element  $x \in T \cap D$ . Wir zeigen, dass dieses  $x$  schon das kleinste Element von  $T$  bezüglich  $R_{\mathcal{K}}$  ist. Sei dazu  $y \in T \subset D_{\mathcal{K}}$ . Dann gilt  $y \in \tilde{D}$  für ein  $(\tilde{D}, \tilde{G}) \in \mathcal{K}$ . Wir unterscheiden nun die Fälle  $y \in D$  und  $y \notin D$ . Im Fall  $y \in D$  ist  $y \in T \cap D$  und gemäß Wahl von  $x$  somit  $(x, y) \in G \subset G_{\mathcal{K}}$ . Im Fall  $y \notin D$  erinnern wir uns, dass  $\mathcal{K}$  eine Kette ist. Da  $y \in \tilde{D} \setminus D$  ja  $\tilde{D} \subset D$  und damit  $(\tilde{D}, \tilde{G}) \in (\tilde{D}, G)$  ausschließt, muss  $(D, G) \in (\tilde{D}, \tilde{G})$  gelten. Die letzte Bedingung aus der Definition von  $\in$  liefert für  $x \in D$  und  $y \in \tilde{D} \setminus D$  dann  $(x, y) \in \tilde{G} \subset G_{\mathcal{K}}$ . Somit ist  $(x, y) \in G_{\mathcal{K}}$  oder mit anderen Worten  $x R_{\mathcal{K}} y$  in allen Fällen gezeigt,  $x$  ist also bezüglich  $R_{\mathcal{K}}$  kleinstes Element von  $T$ . Insgesamt erhalten wir, dass  $R_{\mathcal{K}}$  eine Wohlordnung auf  $D_{\mathcal{K}}$ , also  $(D_{\mathcal{K}}, G_{\mathcal{K}}) \in \mathcal{W}$  ist. Man prüft nun problemlos, dass  $(D, G) \in (D_{\mathcal{K}}, G_{\mathcal{K}})$  für alle  $(D, G) \in \mathcal{K}$  gilt und somit  $(D_{\mathcal{K}}, G_{\mathcal{K}})$  eine obere Schranke für  $\mathcal{K}$  ist.

Insgesamt ist die Voraussetzung des Zornschen Lemmas erfüllt, und dieses liefert nun die Existenz eines maximalen Elements  $(D, G)$  von  $\mathcal{W}$ , für das  $R = (D, D, G)$  eine Wohlordnung auf  $D \subset \mathcal{X}$  ist. Angenommen, es ist  $D \subsetneq \mathcal{X}$ . Dann könnten wir ein  $x_0 \in \mathcal{X} \setminus D$  wählen, dieses  $x_0$  durch die Festlegungen  $D_0 := D \cup \{x_0\}$ ,  $G_0 := G \cup (D_0 \times \{x_0\})$  als neues größtes Element hinzufügen und erhielten  $(D_0, G_0) \in \mathcal{W}$  mit  $(D, G) \in (D_0, G_0)$ , aber  $(D_0, G_0) \neq (D, G)$ . Da dies im Widerspruch zur Maximalität von  $(D, G)$  stünde, muss tatsächlich  $D = \mathcal{X}$  gelten. Dies bedeutet aber, dass  $R$  tatsächlich eine Wohlordnung auf ganz  $\mathcal{X}$  ist.  $\square$

Tatsächlich stellen sich das **Auswahlaxiom**, das **Zornsche Lemma** und der **Wohlordnungssatz** sogar als **zueinander äquivalent** heraus. Da wir mit den vorausgehenden Beweisen schon gesehen haben, dass das Auswahlaxiom das Zornsche Lemma und das Wohlordnungssatz implizieren, ist für die Äquivalenz nur noch zu zeigen, dass der Wohlordnungssatz das Auswahlaxiom impliziert. Da mittels Wohlordnung sehr kanonisch (kleinste) Elemente ausgewählt werden können, ist letzteres tatsächlich vergleichsweise einfach: Für ein beliebiges System  $\mathcal{S}$  disjunkter nicht-leerer Mengen liefert der Wohlordnungssatz die Existenz einer Wohlordnung auf  $\bigcup \mathcal{S}$ , und bezüglich dieser existiert in jeder Menge  $M \in \mathcal{S}$ , die ja nicht-leere Teilmenge von  $\bigcup \mathcal{S}$  ist, ein kleinstes Element  $x_M$  (das durch seine Eigenschaft zu einem gewissen Grad konstruktiv charakterisiert ist). Gemäß dem Ersetzungsaxiom kann nun die Menge  $\{x_M \mid M \in \mathcal{S}\}$  gebildet werden. Diese hat dann die Auswahl-eigenschaft, dass sie mit jeder der in  $\mathcal{S}$  enthaltenen Mengen genau ein Element gemeinsam hat.

### 2.3.2 Äquivalenzrelationen

Die zweite wichtige Klasse spezieller Relationen ist folgende:

**Definition (Äquivalenzrelationen).** Eine **Äquivalenzrelation** auf einer Menge  $\mathcal{X}$  ist eine **reflexive, symmetrische und transitive** Relation auf  $\mathcal{X}$ .

**Bemerkung.** Für die Umkehrrelation und Selbst-Komposition einer Äquivalenzrelation  $\sim$  gelten stets  $\sim^{-1} = \sim$  (folgt aus Symmetrie) und  $\sim\sim = \sim$  (folgt aus Reflexivität und Transitivität).

Wir werden in Kürze konkrete Beispiele von Äquivalenzrelationen diskutieren, beschäftigen uns aber zuvor mit der entscheidenden abstrakten Eigenschaft, dass sogenannte Äquivalenzklassen gebildet werden können und die nützlichen Eigenschaften des nächsten Satzes aufweisen:

**Definitionen (Äquivalenzklassen und Quotienten).** Sei  $\sim$  eine Äquivalenzrelation auf einer Menge  $\mathcal{X}$ .

(I) Die **Äquivalenzklasse** von  $x \in \mathcal{X}$  bezüglich  $\sim$  (oder auch: von  $\sim$  zu  $x \in \mathcal{X}$ ) ist

$$[x]_{\sim} := \{y \in \mathcal{X} \mid y \sim x\} \subset \mathcal{X}.$$

Ist die betrachtete Äquivalenzrelation im Kontext klar, so notieren wir auch  $[x]$  für  $[x]_{\sim}$ .

(II) Die **Quotientenmenge**  $\mathcal{X}/\sim$  (lies:  $\mathcal{X}$  modulo  $\sim$ ) von  $\mathcal{X}$  bezüglich der Äquivalenzrelation  $\sim$  ist die **Menge aller Äquivalenzklassen** von  $\sim$ , also

$$\mathcal{X}/\sim := \{[x]_{\sim} \mid x \in \mathcal{X}\} \subset \mathcal{P}(\mathcal{X}).$$

(III) Die **kanonische Projektion** oder **Quotientenabbildung** von  $\mathcal{X}$  nach  $\mathcal{X}/\sim$  ist die stets surjektive Abbildung

$$p_{\sim}: \mathcal{X} \rightarrow \mathcal{X}/\sim, x \mapsto [x]_{\sim}.$$

Ergibt sich die Äquivalenzrelation aus dem Kontext, so schreiben wir auch  $p$  für  $p_{\sim}$ .

**Satz (zu Äquivalenzrelationen und Äquivalenzklassen).** Sei  $\mathcal{X}$  eine Menge mit  $x, y \in \mathcal{X}$ . Für eine Äquivalenzrelation  $\sim$  auf  $\mathcal{X}$  gilt

$$\boxed{y \sim x \iff y \in [x]_{\sim} \iff [y]_{\sim} = [x]_{\sim} \iff [y]_{\sim} \cap [x]_{\sim} \neq \emptyset}$$

und für die komplementäre Relation  $\not\sim := \sim^c$  dementsprechend

$$y \not\sim x \iff y \notin [x]_{\sim} \iff [y]_{\sim} \neq [x]_{\sim} \iff [y]_{\sim} \cap [x]_{\sim} = \emptyset.$$

*Beweis.* Wir zeigen nur die obere Zeile von Äquivalenzen, da sich die untere durch Negation daraus ergibt. Da  $y \sim x \iff y \in [x]_{\sim}$  per Definition der Äquivalenzklasse  $[x]_{\sim}$  gilt, werden wir tatsächlich nur als Ringschluss die drei Implikationen in

$$y \sim x \xrightarrow{(1)} [y]_{\sim} = [x]_{\sim} \xrightarrow{(2)} [y]_{\sim} \cap [x]_{\sim} \neq \emptyset \xrightarrow{(3)} y \sim x$$

nachweisen:

- Implikation (1): Es gelte  $y \sim x$ . Wir verifizieren  $[y]_{\sim} \subset [x]_{\sim}$  und  $[y]_{\sim} \supset [x]_{\sim}$  separat. Für „ $\subset$ “ sei  $z \in [y]_{\sim}$ , also  $z \sim y$ . Zusammen mit  $y \sim x$  und Transitivität von  $\sim$  folgt  $z \sim x$ , also wie benötigt  $z \in [x]_{\sim}$ . Für „ $\supset$ “ bemerken wir, dass per Symmetrie von  $\sim$  auch  $x \sim y$  gilt, und greifen dann auf „ $\subset$ “ mit vertauschten Rollen von  $x$  und  $y$  zurück.
- Implikation (2): Hierfür ist nur  $[x]_{\sim} \neq \emptyset$  sicherzustellen. Dies ist aber gegeben, weil Reflexivität  $x \sim x$  und damit  $x \in [x]_{\sim}$  garantiert.

- Implikation (3): Sei  $z \in [y]_{\sim} \cap [x]_{\sim}$ , also  $z \sim x$  und  $z \sim y$ . Per Symmetrie gilt auch  $y \sim z$ . Mit Transitivität folgt aus  $y \sim z$  und  $z \sim x$  dann  $y \sim x$ .  $\square$

**Bemerkungen** (zu Äquivalenzklassen). Insbesondere ergibt sich aus dem Satz:

- (1) Jede Äquivalenzklasse  $[x]_{\sim}$  kann auch als  $[y]_{\sim}$  mit beliebigem  $y \in [x]_{\sim}$  geschrieben werden. Man hat bei der Darstellung einer Äquivalenzklasse durch ein Element und die eckigen Klammern in der Regel also eine Wahl, welches Element man nennt. Man sagt daher häufig, dass ein  $y \in [x]_{\sim}$  (wie auch  $x$  selbst) ein **Repräsentant der Äquivalenzklasse**  $[x]_{\sim}$  ist.
- (2) Verschiedene Äquivalenzklassen sind stets disjunkt, also ist die Quotientenmenge  $\mathcal{X}/\sim$  ein System disjunkter Mengen. Da jedes Element  $x \in \mathcal{X}$  in einer Äquivalenzklasse liegt (nämlich in  $x \in [x]_{\sim}$ ), bedeutet dies insgesamt

$$\mathcal{X} = \dot{\bigcup}(\mathcal{X}/\sim) = \dot{\bigcup}\{[x]_{\sim} \mid x \in \mathcal{X}\}.$$

Mit anderen Worten bringt eine Äquivalenzrelation stets eine **Partition/(disjunkte) Zerlegung der Grundmenge in Äquivalenzklassen** mit sich.

Auch umgekehrt erhält man aus einer Partition  $\mathcal{X} = \dot{\bigcup}\{M \mid M \in \mathcal{S}\}$  einer Menge  $\mathcal{X}$  mittels eines Systems  $\mathcal{S}$  disjunkter Mengen, durch die Festlegung

$$x \underset{\mathcal{S}}{\in} y \iff \exists M \in \mathcal{S}: (x \in M \wedge y \in M) \quad \text{für } x, y \in \mathcal{X}$$

eine Äquivalenzrelation  $\underset{\mathcal{S}}{\in} \in \text{Rel}(\mathcal{X})$ .

Dabei ergeben sich als Äquivalenzklassen von  $\underset{\mathcal{S}}{\in}$  gerade die in  $\mathcal{S}$  enthaltenen Mengen, und aus einer Partition in Äquivalenzklassen erhält man die Äquivalenzrelation zurück, es gelten also stets  $\mathcal{X}/\underset{\mathcal{S}}{\in} = \mathcal{S}$  und  $\underset{\mathcal{X}/\underset{\mathcal{S}}{\in}}{\sim} = \sim$ . Somit sind die beschriebenen Übergänge von Äquivalenzrelation zu Partition und von Partition zu Äquivalenzrelation zueinander invers, und man kann **Äquivalenzrelationen auf  $\mathcal{X}$  tatsächlich 1-zu-1 mit Partitionen von  $\mathcal{X}$  identifizieren**, wenn man möchte.

**Beispiele (von Äquivalenzrelationen).**

- (0) Die All-Relation auf  $\mathcal{X}$  ist eine (triviale) Äquivalenzrelation. Bei dieser ist  $[x] = \mathcal{X}$  für alle  $x \in \mathcal{X}$ , ganz  $\mathcal{X}$  ist also die einzige Äquivalenzklasse.
- (1) Die Gleichheitsrelation „ $=$ “ des früheren Beispiels (2) ist eine Äquivalenzrelation auf  $M$  und kann als stark vereinfachter Prototyp einer solchen Relation angesehen werden. Bei  $=$  haben alle Äquivalenzklassen  $[x]_{=} = \{x\}$  mit  $x \in M$  genau ein Element. Die Quotientenabbildung  $M \rightarrow M/=$  ist bijektiv und erlaubt die kanonische Identifikation von  $M/=$  mit  $M$ .
- (2) **Sehr zentrale Beispiele von Äquivalenzrelationen** sind die **Modulo- $n$ -Relationen**  $\overset{n}{\sim}$  auf  $\mathbb{Z}$ , die für jede feste Zahl  $n \in \mathbb{Z}$  durch

$$y \overset{n}{\sim} x \iff n \mid (y-x) \iff \exists z \in \mathbb{Z}: y-x = nz \quad \text{für } x, y \in \mathbb{Z}$$

erklärt werden (und deren Reflexivität, Symmetrie und Transitivität man leicht prüft). Typischerweise betrachtet man nur  $n \in \mathbb{N} \setminus \{1\}$ , da  $\overset{-n}{\sim} = \overset{n}{\sim}$  gilt,  $\overset{0}{\sim}$  die Gleichheitsrelation und  $\overset{1}{\sim}$  die All-Relation ist. Außerdem ist  $\overset{2}{\sim}$  die Relation  $\overset{\mathcal{E}}{\sim}$  des früheren Beispiels (1) (wohingegen die Relation  $\overset{2}{\sim}$  von früher *keine* Äquivalenzrelation und hier irrelevant ist). Man verwendet bei den Modulo-Relationen die **allgemeinen Schreibweisen**

$$y = x \pmod n \quad \text{für} \quad y \overset{n}{\sim} x$$

(gelesen „ $y$  gleich  $x$  modulo  $n$ “ oder „ $y$  kongruent  $x$  modulo  $n$ “) und

$$\mathbb{Z}/n\mathbb{Z} \quad \text{für} \quad \mathbb{Z}/n.$$

Konkret gelten beispielsweise  $25 = 7 \pmod{9}$  und  $3 \cdot 6385 + 4 = -11 \pmod{3}$ .

Die **Äquivalenzklassen modulo 2** sind

$$\begin{aligned} [0]_{\mathbb{Z}/2\mathbb{Z}} &= \{\dots, -6, -4, -2, 0, 2, 4, 6, \dots\} = [2]_{\mathbb{Z}/2\mathbb{Z}} = [-2]_{\mathbb{Z}/2\mathbb{Z}}, \\ [1]_{\mathbb{Z}/2\mathbb{Z}} &= \{\dots, -5, -3, -1, 1, 3, 5, 7, \dots\} = [3]_{\mathbb{Z}/2\mathbb{Z}} = [-1]_{\mathbb{Z}/2\mathbb{Z}} \end{aligned}$$

und geben die in Abbildung 28 gezeigte Zerlegung  $\mathbb{Z} = [0]_{\mathbb{Z}/2\mathbb{Z}} \dot{\cup} [1]_{\mathbb{Z}/2\mathbb{Z}}$  von  $\mathbb{Z}$  in die **Mengen der geraden und ungeraden Zahlen**.

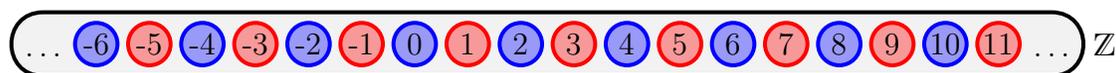


Abb. 28: Die Zerlegung  $\mathbb{Z} = [0]_{\mathbb{Z}/2\mathbb{Z}} \dot{\cup} [1]_{\mathbb{Z}/2\mathbb{Z}}$  der ganzen Zahlen modulo 2

Die **Äquivalenzklassen modulo 3** sind

$$\begin{aligned} [0]_{\mathbb{Z}/3\mathbb{Z}} &= \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\} = [3]_{\mathbb{Z}/3\mathbb{Z}} = [-3]_{\mathbb{Z}/3\mathbb{Z}}, \\ [1]_{\mathbb{Z}/3\mathbb{Z}} &= \{\dots, -8, -5, -2, 1, 4, 7, 10, \dots\} = [4]_{\mathbb{Z}/3\mathbb{Z}} = [-2]_{\mathbb{Z}/3\mathbb{Z}}, \\ [2]_{\mathbb{Z}/3\mathbb{Z}} &= \{\dots, -7, -4, -1, 2, 5, 8, 11, \dots\} = [5]_{\mathbb{Z}/3\mathbb{Z}} = [-1]_{\mathbb{Z}/3\mathbb{Z}} \end{aligned}$$

und geben die in Abbildung 29 gezeigte Zerlegung  $\mathbb{Z} = [0]_{\mathbb{Z}/3\mathbb{Z}} \dot{\cup} [1]_{\mathbb{Z}/3\mathbb{Z}} \dot{\cup} [2]_{\mathbb{Z}/3\mathbb{Z}}$  in drei Äquivalenzklassen mit je unendlich vielen Elementen, die **bei Division durch 3 Rest 0, 1 bzw. 2** ergeben.

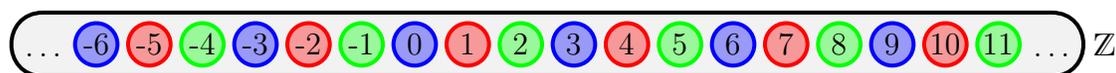


Abb. 29: Die Zerlegung  $\mathbb{Z} = [0]_{\mathbb{Z}/3\mathbb{Z}} \dot{\cup} [1]_{\mathbb{Z}/3\mathbb{Z}} \dot{\cup} [2]_{\mathbb{Z}/3\mathbb{Z}}$  der ganzen Zahlen modulo 3

Analog ist  $\mathbb{Z}$  in Äquivalenzklassen modulo 4, 5, 6, 7, 8, 9, ... zerlegt. Ein Beispiel für eine **Äquivalenzklasse modulo 9** ist

$$[7]_{\mathbb{Z}/9\mathbb{Z}} = \{\dots, -38, -29, -20, -11, -2, 7, 16, 25, 34, 43, 52, 61, 70, 79, \dots\}.$$

(3) Ein Beispiel einer Äquivalenzrelation  $\overset{\#}{\sim}$  auf  $\mathbb{N}$  erhält man durch

$$m \overset{\#}{\sim} n \iff m \text{ und } n \text{ besitzen gleich viele Teiler in } \mathbb{N} \quad \text{für } m, n \in \mathbb{N}.$$

Beispiele von Äquivalenzklassen bezüglich  $\overset{\#}{\sim}$  sind

$\{1\}$	(genau 1 Teiler),
$\{2, 3, 5, 7, 11, 13, 17, 19, \dots\}$	(genau 2 Teiler; Primzahlen $p \in \mathbb{P}$ ),
$\{4, 9, 25, 49, 121, 169, \dots\}$	(genau 3 Teiler; Zahlen $p^2$ mit $p \in \mathbb{P}$ ),
$\{6, 8, 10, 14, 15, 21, 22, \dots\}$	(genau 4 Teiler; Zahlen $p^3$ oder $pq$ mit $p \neq q$ in $\mathbb{P}$ ),
$\{16, 81, 625, 2401, 14641, \dots\}$	(genau 5 Teiler; Zahlen $p^4$ mit $p \in \mathbb{P}$ ),
$\{12, 18, 20, 28, 32, 44, 45, \dots\}$	(genau 6 Teiler; Zahlen $p^5$ oder $p^2q$ mit $p \neq q$ in $\mathbb{P}$ ).

Insgesamt zerlegt die Äquivalenzrelation  $\#^T$  die natürlichen Zahlen— wie in Abbildung 30 angedeutet — in die Äquivalenzklasse  $\{1\}$  mit einem Element und unendlich viele weitere Äquivalenzklassen mit jeweils unendlich vielen Elementen.

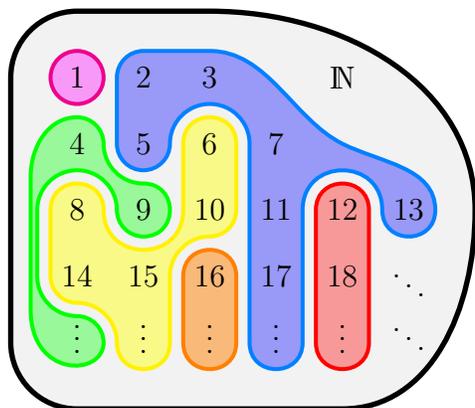


Abb. 30: Die Zerlegung von  $\mathbb{N}$  in die Äquivalenzklassen der Relation  $\#^T$

(4) Für jede Menge  $\mathcal{X}$  wird durch

$$f \propto g \iff \exists \gamma \in \mathbb{R} \setminus \{0\} : \forall x \in \mathcal{X} : g(x) = \gamma f(x) \quad \text{für } f, g \in \text{Abb}(\mathcal{X}, \mathbb{R})$$

eine Äquivalenzrelation  $\propto$  auf  $\text{Abb}(\mathcal{X}, \mathbb{R})$  definiert. Im Fall  $\mathcal{X} = \mathbb{R}$  enthält die Äquivalenzklasse von  $\text{id}_{\mathbb{R}}$  bezüglich  $\propto$  alle linearen Funktionen  $\mathbb{R} \rightarrow \mathbb{R}$ ,  $x \mapsto mx$  mit (Steigungs-)Parameter  $m \in \mathbb{R} \setminus \{0\}$ , und die Äquivalenzklasse von  $\mathbb{R} \rightarrow \mathbb{R}$ ,  $x \mapsto x^2$  bezüglich  $\propto$  enthält alle quadratischen Funktionen  $\mathbb{R} \rightarrow \mathbb{R}$ ,  $x \mapsto ax^2$  mit (Öffnungs-)Parameter  $a \in \mathbb{R} \setminus \{0\}$ .

(5) Bezüglich der Äquivalenzrelationen  $\stackrel{123}{\equiv}$  auf  $\mathcal{P}(\mathbb{N})$  mit

$$M \stackrel{123}{\equiv} N \iff M \cap \{1, 2, 3\} = N \cap \{1, 2, 3\} \quad \text{für } M, N \subset \mathbb{N}$$

enthält die Äquivalenzklasse der Menge der ungeraden Zahlen

$$[\{1, 3, 5, 7, 9, \dots\}] = \{M \in \mathcal{P}(\mathbb{N}) \mid 1 \in M, 2 \notin M, 3 \in M\}$$

sowohl endliche Mengen wie  $\{1, 3\}$ ,  $\{1, 3, 8\}$ ,  $\{1, 3, 7, 19\}$ ,  $\{1, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\}$  als auch unendliche Mengen wie  $\mathbb{N} \setminus \{2\}$ ,  $\mathbb{P} \Delta \{1, 2\}$  und  $\{1, 3, 5, 7, 9, \dots\}$  selbst. Insgesamt besteht  $\mathcal{P}(\mathbb{N}) / \stackrel{123}{\equiv}$  aus 8 Äquivalenzklassen mit jeweils unendlich vielen Elementen.

(6) Bezüglich der Äquivalenzrelationen  $\cong$  auf  $\mathcal{P}(\mathbb{N})$  mit

$$M \cong N \iff M \Delta N \text{ hat nur endlich viele Elemente} \quad \text{für } M, N \subset \mathbb{N}$$

enthält die Äquivalenzklasse der Menge  $\mathbb{P} \subset \mathbb{N}$  der Primzahlen

$$[\mathbb{P}] = \{\mathbb{P} \Delta \{n_1, n_2, n_3, \dots, n_k\} \mid k \in \mathbb{N}_0, n_1, n_2, n_3, \dots, n_k \in \mathbb{N}\}$$

nur unendliche Mengen wie zum Beispiel  $\{19, 23, 29, 31, 37, 41, \dots\}$  (Primzahlen ab 19) und  $\{1, 3, 5, 7, \dots, 101, 103, 107, 109, 113, 127, \dots\}$  (ungerade Zahlen bis 103, Primzahlen ab 107). Hier enthält  $\mathcal{P}(\mathbb{N}) / \cong$  unendlich viele Äquivalenzklassen mit je unendlich vielen Elementen.

(7) Jede Funktion  $f: \mathcal{X} \rightarrow \mathcal{Y}$  zwischen Mengen  $\mathcal{X}$  und  $\mathcal{Y}$  induziert eine Äquivalenzrelation  $\overset{f}{\sim}$  auf  $\mathcal{X}$  durch

$$x \overset{f}{\sim} y \iff f(x) = f(y) \quad \text{für alle } x, y \in \mathcal{X}.$$

(Reflexivität, Symmetrie, Transitivität besagen hier  $f(x) = f(x)$ ,  $f(x) = f(y) \implies f(y) = f(x)$  und  $(f(x) = f(y) \wedge f(y) = f(z)) \implies f(x) = f(z)$  für alle  $x, y, z \in \mathcal{X}$  und gelten offensichtlich.)

Spezialfälle dieser Bildung haben wir in den Beispielen (3) und (5) gesehen: Die Relation  $\overset{\#T}{\sim}$  ergibt sich für die Funktion  $f: \mathbb{N} \rightarrow \mathbb{N}$ , die  $n \in \mathbb{N}$  auf die Anzahl der Teiler von  $n$  abbildet. Die Relation  $\overset{123}{\sim}$  ergibt sich für  $f: \mathcal{P}(\mathbb{N}) \rightarrow \mathcal{P}(\{1, 2, 3\})$ ,  $M \mapsto M \cap \{1, 2, 3\}$ .

Etwas allgemeiner kann man übrigens auch für  $f: \mathcal{X} \rightarrow \mathcal{Y}$  und für eine beliebige Äquivalenzrelation  $\cong$  auf dem Ziel  $\mathcal{Y}$  anstelle der Gleichheitsrelation durch

$$x \overset{f}{\sim} y \iff f(x) \cong f(y) \quad \text{für alle } x, y \in \mathcal{X}$$

eine Äquivalenzrelation  $\overset{f}{\sim}$  auf  $\mathcal{X}$  erhalten.

Mit **Äquivalenzrelationen** bringt man in der Mathematik ganz allgemein und formal korrekt zum Ausdruck, dass man **in Relation stehende Elemente miteinander und mit ihrer Äquivalenzklasse identifizieren** kann, jedenfalls im Hinblick auf gewisse, an der entsprechenden Stelle relevante Eigenschaften. Ist speziell für Elemente  $x \in \mathcal{X}$  nur der Funktionswert  $f(x) \in \mathcal{Y}$  unter einer fixierten Abbildung  $f: \mathcal{X} \rightarrow \mathcal{Y}$  relevant, so wird genau dies im nächsten Satz formalisiert:

**Satz** (über die **Faktorisierung einer Abbildung bezüglich einer Äquivalenzrelation**).  
Seien  $\mathcal{X}$  und  $\mathcal{Y}$  Mengen,  $\sim$  eine Äquivalenzrelation auf  $\mathcal{X}$  und  $f: \mathcal{X} \rightarrow \mathcal{Y}$  eine Abbildung mit der Eigenschaft

$$y \sim x \implies f(y) = f(x) \quad \text{für alle } x, y \in \mathcal{X}.$$

Dann gibt es genau eine Abbildung  $f_*: \mathcal{X}/\sim \rightarrow \mathcal{Y}$  mit

$$f_*([x]) = f(x) \quad \text{für alle } x \in \mathcal{X}.$$

*Beweis.* Wir zeigen, dass  $f_*: \mathcal{X}/\sim \rightarrow \mathcal{Y}$  durch  $f_*([x]) := f(x)$  für  $x \in \mathcal{X}$  wohldefiniert wird, dass also für  $x, y \in \mathcal{X}$  aus  $[y] = [x]$  stets  $f(y) = f(x)$  folgt. Da  $[y] = [x]$  gemäß dem vorigen Satz  $y \sim x$  bedeutet, ist genau dies aber durch die vorausgesetzte Eigenschaft gesichert. Mit der Wohldefiniertheit ist dann auch die Existenz und Eindeutigkeit von  $f_*$  klar.  $\square$

**Beispiel** (zum Satz über die Faktorisierung). Wir betrachten die Abbildung  $r: \mathbb{Z} \rightarrow \{0, 1, 2\}$ , die ganze Zahlen auf ihren Rest bei Division durch 3 abbildet, also  $r(x) = x \bmod 3$  mit  $r(x) \in \{0, 1, 2\}$  oder mit anderen Worten  $x = 3[x/3] + r(x)$  für alle  $x \in \mathbb{Z}$  erfüllt. Die zugehörige Relation  $\overset{r}{\sim}$  im Sinn von Beispiel (7) ist die Modulo-3-Relation.

Da  $(y = x \bmod 6) \implies (y = x \bmod 3) \implies r(y) = r(x)$  gilt, greift der Satz sowohl für die Modulo-6- als auch die Modulo-3-Relation und gibt eine eindeutige Abbildung  $r_*: \mathbb{Z}/6\mathbb{Z} \rightarrow \{0, 1, 2\}$  mit  $r_*([x]_{\mathbb{Z}/6\mathbb{Z}}) = r(x)$  beziehungsweise  $r_*: \mathbb{Z}/3\mathbb{Z} \rightarrow \{0, 1, 2\}$  mit  $r_*([x]_{\mathbb{Z}/3\mathbb{Z}}) = r(x)$  für alle  $x \in \mathbb{Z}$ . Konkret sieht man an

$$\begin{aligned} r(-2) = 1, \quad r(-1) = 2, \quad r(0) = 0, \quad r(1) = 1, \quad r(2) = 2, \quad r(3) = 0, \quad r(4) = 1, \\ r_*([-2]) = 1, \quad r_*([-1]) = 2, \quad r_*([0]) = 0, \quad r_*([1]) = 1, \quad r_*([2]) = 2, \quad r_*([3]) = 0, \quad r_*([4]) = 1 \end{aligned}$$

(für Äquivalenzklassen entweder modulo 6 oder modulo 3), dass der Übergang von  $r$  zu  $r_*$  naheliegend und eher eine Formalität ist. Entscheidend ist aber, dass z.B. mit  $4 = -2 \bmod 6$

auch  $[4] = [-2]$  ist und dies  $r(4) = r(-2)$  erzwingt: Wäre nämlich *mal hypothetisch*  $r(4) \neq r(-2)$ , so könnte man den Wert von  $r_*$  auf  $[4] = [-2]$  nicht wie benötigt festlegen. Dass auf diese Weise tatsächlich keine Probleme entstehen (weil die Abbildung nämlich auf allen Elementen einer Äquivalenzklasse denselben Wert hat), das wird in diesem Beispiel durch die erwähnten Implikationen  $(y = x \bmod 6) \implies (y = x \bmod 3) \implies r(y) = r(x)$  sichergestellt — und genauso im allgemeinen Fall durch die Voraussetzung  $y \sim x \implies f(y) = f(x)$ .

Tatsächlich kann die hier betrachtete Abbildung  $r$  nach allen Modulo- $n$ -Relationen mit durch 3 teilbarem  $n$  faktorisieren, aber nicht nach irgendwelchen anderen Modulo-Relationen: Die Faktorisierung modulo 2 scheitert zum Beispiel daran, dass dann tatsächlich  $[0] = [2]$ , aber  $r(0) = 0 \neq r(2) = 2$  ist und kein sinnvoller Wert von  $r_*$  auf  $[0] = [2]$  festgelegt werden kann.

**Bemerkungen** (zum Satz über die Faktorisierung).

(1) Die Voraussetzung  $y \sim x \implies f(y) = f(x)$  für alle  $x, y \in \mathcal{X}$  bedeutet, dass  $f$  auf Äquivalenzklassen von  $\sim$  konstant ist. Mit  $\overset{f}{\sim}$  aus Beispiel (7) kann die diese Voraussetzung äquivalent als  $x \sim y \implies x \overset{f}{\sim} y$  für alle  $x, y \in \mathcal{X}$  oder auch als  $G_\sim \subset G_{\overset{f}{\sim}}$  geschrieben werden. Insbesondere ist  $\overset{f}{\sim}$  die Relation mit den größten Äquivalenzklassen und dem größten Graph, für die der Satz anwendbar ist.

(2) Im Satz ist ...

- $f_*$  genau dann injektiv, wenn  $\sim = \overset{f}{\sim}$  (also  $y \sim x \iff f(y) = f(x)$  für alle  $x, y \in \mathcal{X}$ ) gilt,
- $\text{Bild}(f_*) = \text{Bild}(f)$  und insbesondere  $f_*$  genau dann surjektiv, wenn  $f$  surjektiv ist.

*Beweis.* Ist  $f_*$  injektiv, so erhalten wir  $f(y) = f(x) \implies y \sim x$  für alle  $x, y \in \mathcal{X}$  aus den Schlüssen  $f(y) = f(x) \rightsquigarrow f_*([y]) = f_*([x]) \rightsquigarrow [y] = [x] \rightsquigarrow y = x$ . Da die Umkehr-Implikation im Satz vorausgesetzt wird, ist damit  $y \sim x \iff f(y) = f(x)$  für alle  $x, y \in \mathcal{X}$  gezeigt.

Gilt  $y \sim x \iff f(y) = f(x)$  für alle  $x, y \in \mathcal{X}$ , so erhalten wir  $f_*([y]) = f_*([x]) \implies [y] = [x]$  für alle  $x, y \in \mathcal{X}$  durch die Schlüsse  $f_*([y]) = f_*([x]) \rightsquigarrow f(y) = f(x) \rightsquigarrow y \sim x \rightsquigarrow [y] = [x]$ . Damit ist  $f_*$  injektiv.

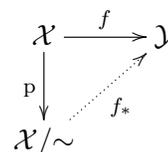
Die Gleichheit  $\text{Bild}(f_*) = \text{Bild}(f)$  liest man aus  $f_*([x]) = f(x)$  für alle  $x \in \mathcal{X}$  ab und erhält dann auch die Aussage zur Surjektivität.  $\square$

(3) Die Schlussfolgerung des Satzes kann **abstrakter** so formuliert werden, dass **genau eine Abbildung  $f_*: \mathcal{X}/\sim \rightarrow \mathcal{Y}$  mit**

$$\boxed{f_* \circ p = f}$$

(für die Quotientenabbildung  $p: \mathcal{X} \rightarrow \mathcal{X}/\sim$ ) existiert. Damit wird die Abbildung  $f$  gewissermaßen in die „Faktoren“  $f_*$  und  $p$  zerlegt, was die Verwendung des Begriffs „Faktorisierung“ (teils) erklärt. Insbesondere können wir durch die Wahl  $\sim = \overset{f}{\sim}$  und gemäß der vorigen Bemerkung **jede Abbildung  $f$  als Hintereinanderausführung der Surjektion  $p$  und der Injektion  $f_*$**  schreiben.

Man kann sich die Situation des Satzes anhand des rechts gezeigten Diagramms verdeutlichen und merken. Die Gleichheit  $f = f_* \circ p$  bringt man dabei auch so zum Ausdruck, dass man von einem **kommutativen Diagramm** spricht, d.h. einem Diagramm, in dem der direkte Weg von  $\mathcal{X}$  nach  $\mathcal{Y}$  mit  $f$  derselben Abbildung entspricht wie der Weg von  $\mathcal{X}$  über  $\mathcal{X}/\sim$  nach  $\mathcal{Y}$  mit  $p$  und  $f_*$ .



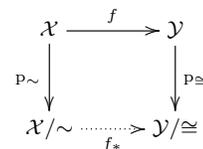
- (4) Wie in Beispiel (7) kann man auch im Satz eine beliebige Äquivalenzrelation  $\cong$  auf dem Ziel  $\mathcal{Y}$  zulassen und erhält dann folgende **leicht allgemeinere Version**: Seien  $\mathcal{X}$  und  $\mathcal{Y}$  Mengen,  $\sim$  eine Äquivalenzrelation auf  $\mathcal{X}$  und  $\cong$  eine Äquivalenzrelation auf  $\mathcal{Y}$  sowie  $f: \mathcal{X} \rightarrow \mathcal{Y}$  eine Abbildung mit der Eigenschaft

$$y \sim x \implies f(y) \cong f(x) \quad \text{für alle } x, y \in \mathcal{X}$$

was mit anderen Worten  $y \sim x \implies y \stackrel{f}{\sim} x$  für die Relation  $\stackrel{f}{\sim}$  aus Beispiel (7) bedeutet. Dann gibt es genau eine Abbildung  $f_*: \mathcal{X}/\sim \rightarrow \mathcal{Y}/\cong$ , die

$$f_*([x]_{\sim}) = [f(x)]_{\cong} \quad \text{für alle } x \in \mathcal{X}$$

oder mit anderen Worten  $f_* \circ p_{\sim} = p_{\cong} \circ f$  erfüllt und das rechts gezeigte Diagramm kommutativ macht.



## 2.4 Rationale Zahlen

In diesem Abschnitt diskutieren wir eine Möglichkeit zur **formalen Einführung der rationalen Zahlen**, also der Brüche mit ganzzahligem Zähler und Nenner, letzterer ungleich Null. Die Darstellung solcher Brüche ist bekanntlich nicht eindeutig, zum Beispiel ist  $\frac{3}{2} = \frac{6}{4} = \frac{-18}{-10}$ , es können also die drei Zähler-Nenner-Paare  $(3, 2)$ ,  $(6, 4)$ ,  $(-18, -10)$  (und viele weitere) zur Darstellung desselben Bruchs herangezogen werden. Der Zusammenhang, dass zwei Paare denselben Bruch darstellen, gibt tatsächlich eine Äquivalenzrelation auf Zähler-Nenner-Paaren, und verschiedene Zähler-Nenner-Paare können als verschiedene Repräsentanten desselben Bruchs betrachtet werden. Deshalb liegt es nahe, mit einer geeigneten Äquivalenzrelation zu arbeiten:

**Proposition.** *Durch die Festlegung*

$$(z, n) \stackrel{\mathcal{Q}}{\sim} (y, m) \iff mz = ny \quad \text{für alle } (z, n), (y, m) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$$

ist eine Äquivalenzrelation auf  $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$  gegeben.

*Beweis.* Wir zeigen die definierenden Eigenschaften (wobei  $(z, n), (y, m), (x, \ell) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ ):

- Reflexivität:  $(z, n) \stackrel{\mathcal{Q}}{\sim} (z, n)$  bedeutet  $nz = nz$  und gilt für alle  $(z, n) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ .
- Symmetrie: Es gilt sogar  $(z, n) \stackrel{\mathcal{Q}}{\sim} (y, m) \iff (y, m) \stackrel{\mathcal{Q}}{\sim} (z, n)$ , denn die ausgeschriebene linke Seite  $mz = ny$  und die ausgeschriebene rechte Seite  $ny = mz$  besagen dasselbe.
- Transitivität: Wir zeigen  $((z, n) \stackrel{\mathcal{Q}}{\sim} (y, m) \wedge (y, m) \stackrel{\mathcal{Q}}{\sim} (\ell, x)) \implies (z, n) \stackrel{\mathcal{Q}}{\sim} (\ell, x)$ : Die Prämisse bedeutet  $mz = ny$  und  $ly = mx$ , und daraus folgt  $mlz = \ell mz = \ell ny = nly = nm x = mn x$ . Wegen  $m \neq 0$  erhalten wir  $\ell z = nx$ , also wie erforderlich  $(z, n) \stackrel{\mathcal{Q}}{\sim} (\ell, x)$ .  $\square$

**Definition (rationale Zahlen).** *Wir definieren die Menge der rationalen Zahlen*

$$\mathbb{Q} := (\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})) / \mathcal{Q}$$

als die Quotientenmenge der Äquivalenzrelation  $\mathcal{Q}$  aus der vorausgehenden Proposition und vereinbaren die Schreibweisen

$$z : n := z/n := \frac{z}{n} := [(z, n)] \quad \text{mit } z \in \mathbb{Z}, n \in \mathbb{Z} \setminus \{0\}$$

für die Äquivalenzklassen dieser Relation. Wir identifizieren außerdem jede ganze Zahl  $z \in \mathbb{Z}$  mit der Äquivalenzklasse  $\frac{z}{1} \in \mathbb{Q}$  und fassen in dieser Weise  $\mathbb{Z}$  als Teilmenge von  $\mathbb{Q}$  auf.

Dass diese Definition sinnvoll ist, liegt vor allem daran, dass sich aus ihr sofort die grundlegende Kürzungs-/Erweiterungs-Regel

$$\frac{z}{n} = \frac{mz}{mn} \quad \text{für } z \in \mathbb{Z}, m, n \in \mathbb{Z} \setminus \{0\}$$

ergibt (denn diese Regel bedeutet per Definition der Äquivalenzrelation nichts anderes als die offensichtliche Gleichheit  $mnz = nmz$ ).

Das Rechnen mit rationalen Zahlen kann nun wie folgt eingeführt werden:

**Definitionen (der Grundrechenarten auf rationalen Zahlen).** *Addition, Subtraktion, Multiplikation und Division rationaler Zahlen werden unter Verwendung der Addition, Subtraktion und Multiplikation ganzer Zahlen durch*

$$\frac{z}{n} \pm \frac{y}{m} := \frac{mz \pm ny}{nm}, \quad \frac{z}{n} \cdot \frac{y}{m} := \frac{zy}{nm}, \quad \frac{z}{n} \Big/ \frac{y}{m} := \frac{zm}{ny}$$

für  $y, z \in \mathbb{Z}, m, n \in \mathbb{Z} \setminus \{0\}$  (bei der Division auch  $y \in \mathbb{Z} \setminus \{0\}$ ) definiert.

Dass diese Festlegungen tatsächlich nur von den Äquivalenzklassen  $\frac{z}{n}, \frac{y}{m}$  und nicht den (Einträgen der) verwendeten Repräsentanten  $(z, n), (y, m)$  abhängen, ist zunächst überhaupt nicht klar. Daher ist hier — wie es für das Arbeiten mit Äquivalenzklassen sehr typisch ist — **Wohldefiniertheit zu zeigen:**

*Beweis für die Wohldefiniertheit der Grundrechenarten.* Für die Wohldefiniertheit der Addition und Subtraktion zeigen wir, dass sich aus  $\frac{z}{n} = \frac{z'}{n'}$  und  $\frac{y}{m} = \frac{y'}{m'}$  stets  $\frac{mz \pm ny}{nm} = \frac{m'z' \pm n'y'}{n'm'}$  ergibt. Dazu schreiben wir die Prämisse mit der Definition der Äquivalenzrelation  $\mathcal{Q}$  um in  $n'z = nz'$  und  $m'y = my'$  und bekommen dann  $n'm'(mz \pm ny) = m'mn'z \pm n'nm'y = mn'm'z' \pm nm'n'y' = mn(m'z' \pm n'y')$ , was wie erforderlich  $\frac{mz \pm ny}{nm} = \frac{m'z' \pm n'y'}{n'm'}$  bedeutet. Für die Wohldefiniertheit der Multiplikation zeigen wir, dass aus  $\frac{z}{n} = \frac{z'}{n'}$  und  $\frac{y}{m} = \frac{y'}{m'}$  stets  $\frac{zy}{nm} = \frac{z'y'}{n'm'}$  folgt. Dazu nutzen wir wieder  $n'z = nz'$  und  $m'y = my'$ , rechnen  $n'm'zy = n'zm'y = nz'my' = nmz'y'$  und bekommen wie gewünscht  $\frac{zy}{nm} = \frac{z'y'}{n'm'}$ . Die Wohldefiniertheit der Division prüft man ganz ähnlich.  $\square$

Insbesondere gelten nach diesen Definitionen für  $y, z \in \mathbb{Z}, n \in \mathbb{Z} \setminus \{0\}$  stets

$$\frac{z}{1} \pm \frac{y}{1} = \frac{z \pm y}{1}, \quad \frac{z}{1} \cdot \frac{y}{1} = \frac{zy}{1}, \quad \frac{z}{1} \Big/ \frac{y}{1} = \frac{z}{y}.$$

Die ersten beiden Gleichungen besagen dabei, dass die Addition, Subtraktion und Multiplikation auf  $\mathbb{Q}$  und  $\mathbb{Z}$  **konsistent mit** der (in der Definition vereinbarten) **Auffassung von  $\mathbb{Z}$  als Teilmenge von  $\mathbb{Q}$**  zusammenpassen. Die dritte Gleichung besagt, dass die Division von  $z \in \mathbb{Z}$  durch  $n \in \mathbb{Z} \setminus \{0\}$  in  $\mathbb{Q}$  die Äquivalenzklasse  $\frac{z}{n}$  gibt, oder anders herum, dass die  $\mathbb{Q}$  ausmachenden Äquivalenzklassen  $\frac{z}{n}$  die Quotienten  $z/n$  der gerade eingeführten Division sind. Dies macht die **Unterscheidung zwischen Äquivalenzklassen und Quotienten fortan unnötig** und erklärt und rechtfertigt, warum wir das Symbol „/“ in beiden Zusammenhängen verwendet haben. (Übrigens besteht auch mit der früher am Rande und nur für den Fall  $z = nq$  erwähnten Division in  $\mathbb{Z}$  natürlich Konsistenz, da in diesem Fall  $\frac{z}{1} \Big/ \frac{n}{1} = \frac{q}{1}$  gilt.)

Aus den Definitionen lassen sich auch auf  $\mathbb{Q}$  die **Kommutativität und Assoziativität der Addition und Multiplikation**, die **Distributivgesetze** und weitere bekannte Rechenregeln ableiten. Davon, solche Rechenregeln im Detail nachzuweisen, sehen wir hier ab.

Schließlich können auch die **Standard-Ordnungsrelationen** „<“, „>“, „≤“, „≥“ **auf rationale Zahlen erweitert** werden: Wir erklären dazu zuerst die strikten Totalordnungen < und > auf  $\mathbb{Q}$  durch

$$\frac{z}{n} > \frac{y}{m} \iff \frac{y}{m} < \frac{z}{n} \iff ny < mz \quad \text{für } y, z \in \mathbb{Z}, m, n \in \mathbb{N}$$

(so nur für *positive Nenner* aus  $\mathbb{N}$  — was aber völlig ausreicht, da  $\frac{z}{n}$  mit  $z \in \mathbb{Z}, n \in -\mathbb{N}$  auch als  $\frac{-z}{-n}$  mit  $-z \in \mathbb{Z}, -n \in \mathbb{N}$  geschrieben werden kann). Die zugehörigen (nicht-strikten) Totalordnungen  $\leq$  und  $\geq$  auf  $\mathbb{Q}$  ergeben sich durch  $q \geq p \iff p \leq q \iff (p < q \vee p = q)$  für  $p, q \in \mathbb{Q}$ . Dass diese Festlegungen wohldefiniert sind und man in der Tat totale (strikte) Ordnungsrelationen erhält, prüft man ausgehend von den entsprechenden Eigenschaften auf  $\mathbb{Z}$  recht problemlos. Außerdem besteht auch hier insofern Konsistenz, dass  $\frac{y}{1} < \frac{z}{1} \iff y < z$  für alle  $y, z \in \mathbb{Z}$  gilt. Genauer gehen wir auf den Umgang und das Rechnen mit Ungleichungen in Abschnitt 4.1 im Kontext der reellen Zahlen ein.

Tatsächlich ist diese Konstruktion der rationalen Zahlen  $\mathbb{Q}$  ein illustratives Beispiel für den Umgang mit Äquivalenzrelationen, und wir werden auch im nächsten Abschnitt noch einmal darauf zurückkommen. **Soweit es den praktischen Umgang mit rationalen Zahlen und das Rechnen mit Brüchen angeht, unterfüttert die beschriebene Konstruktion aber vor allem die bekannten und üblichen Rechenregeln**, während man auf die Konstruktion selbst im Weiteren nicht mehr zurückgreifen muss.

## 2.5 Mächtigkeit von Mengen

Die **Mächtigkeit oder Kardinalität einer Menge verallgemeinert die Anzahl der Elemente** der Menge, bleibt aber auch für Mengen mit unendliche vielen Elementen sinnvoll und **erlaubt einen Vergleich verschiedener „Grade von Unendlichkeit“**. Um dies präzise fassen zu können, erweist es sich als sinnvoll, zuerst den Vergleich von Mächtigkeiten einzuführen:

**Definitionen ((Gleich-)Mächtigkeit von Mengen).** *Seien  $M$  und  $N$  Mengen.*

- (I) *Man nennt  $M$  und  $N$  **gleichmächtig** oder **von gleicher Kardinalität**, notiert  $|M| = |N|$ , wenn es eine Bijektion von  $M$  nach  $N$  gibt.*
- (II) *Man nennt  $N$  **mindestens gleichmächtig** zu  $M$ , notiert  $|N| \geq |M|$ , und  $M$  **höchstens gleichmächtig** zu  $N$ , notiert  $|M| \leq |N|$ , wenn es eine Injektion von  $M$  nach  $N$  gibt.*
- (III) *Man nennt  $N$  (echt) **mächtiger** als  $M$ , notiert  $|N| > |M|$ , und  $M$  (echt) **weniger mächtig** als  $N$ , notiert  $|M| < |N|$ , wenn  $|M| \leq |N|$ , aber nicht  $|M| = |N|$  gilt.*

**Bemerkungen** (zur (Gleich-)Mächtigkeit von Mengen).

- (1) Für **endliche Mengen**  $M$  und  $N$  bedeutet  $N$  gleichmächtig/mindestens gleichmächtig/echt mächtiger zu/als  $M$ , dass  $N$  **genau so viele/mindestens so viele/echt mehr Elemente** als  $M$  hat. Dies unterstreicht, dass man bei der Notation  $|M|$  die Anzahl der Elemente von  $M$  im Hinterkopf haben sollte (auch wenn wir die Mächtigkeit  $|M|$  nicht definiert haben, sondern nur die Gleichmächtigkeit  $|M| = |N|$ ).

(2) Für die Gleichmächtigkeit beliebiger Mengen  $M$ ,  $N$  und  $L$  zeigt man leicht

$$|M| = |M|, \quad |M| = |N| \iff |N| = |M|, \quad (|L| = |M| \wedge |M| = |N|) \implies |L| = |N|.$$

Damit ist Gleichmächtigkeit eine Äquivalenzrelation auf der Potenzmenge  $\mathcal{P}(\mathcal{X})$  jeder fixierten Menge  $\mathcal{X}$ . (Ohne eine Grundmenge  $\mathcal{X}$  zu fixieren, können wir dagegen nicht formal sauber von einer Äquivalenzrelation sprechen, da wir die Menge aller Mengen als Grundmenge bräuchten und diese nicht existiert; vergleiche mit Abschnitt 1.4.)

(3) Für den Vergleich von Mächtigkeiten beliebiger Mengen  $M$ ,  $N$  und  $L$  gelten generell die an (strikte) Ordnungsrelationen erinnernden Regeln

$$\begin{aligned} |M| \leq |M|, \quad (|M| \leq |N| \wedge |N| \leq |M|) &\implies |M| = |N|, \quad \neg(|M| < |N| \wedge |N| < |M|), \\ (|L| \leq |M| \wedge |M| \leq |N|) &\implies |L| \leq |N|, \quad (|L| < |M| \wedge |M| < |N|) \implies |L| < |N|. \end{aligned}$$

Während die linken Regeln in beiden Zeilen einfach einzusehen sind, handelt es sich bei der mittleren Regel der oberen Zeile tatsächlich um einen bekannten **Satz von Cantor-Schröder-Bernstein**, dessen Beweis bei Interesse unten im Kleingedruckten nachgelesen werden kann und eine etwas trickreiche Konstruktion einer Bijektion  $M \rightarrow N$  aus einer Injektion  $M \rightarrow N$  und einer Injektion  $N \rightarrow M$  erfordert. Die rechten Regeln in beiden Zeilen ergeben sich dann aus diesem Satz (übrigens auch in schärferen Versionen, bei denen eines der „<“-Zeichen durch „ $\leq$ “ ersetzt wird).

Alles in allem können damit für jede fixierte Menge  $\mathcal{X}$  die Mindestens-Gleichmächtigkeit und Höchstens-Gleichmächtigkeit als Ordnungsrelationen auf  $\mathcal{P}(\mathcal{X})$  modulo der Gleichmächtigkeit angesehen werden und die echt größere und echt geringe Mächtigkeit als strikte Ordnungsrelationen auf  $\mathcal{P}(\mathcal{X})$ .

(4) Eine etwas fortgeschrittenere Argumentation mit dem Wohlordnungssatz zeigt auch die Totalordnungseigenschaft, dass stets genau eine der drei Möglichkeiten  $|\mathcal{X}| \leq |\mathcal{Y}|$ ,  $|\mathcal{Y}| \leq |\mathcal{X}|$ ,  $|\mathcal{X}| = |\mathcal{Y}|$  eintritt.

Alles in allem gelten damit für den Vergleich von Mächtigkeiten dieselben Regeln wie für den Vergleich von Zahlen, so dass die eingeführte Notation mit den Symbolen  $=$ ,  $\leq$ ,  $\geq$ ,  $<$ ,  $>$  sich als sehr sinnvoll und suggestiv erweist.

Als Nächstes geben wir wie angekündigt:

*Beweis der Regel  $(|M| \leq |N| \wedge |N| \leq |M|) \implies |M| = |N|$ , also des Satzes von Cantor-Schröder-Bernstein.* Es gelte sowohl  $|M| \leq |N|$  als auch  $|N| \leq |M|$ . Per Definition gibt es dann Injektionen  $f: M \rightarrow N$  und  $g: N \rightarrow M$ , und aus letzterer erhalten wir durch Verkleinerung des Zielbereichs eine Bijektion  $\tilde{g}: N \rightarrow \text{Bild}(g)$  mit Umkehrbijektion  $\tilde{g}^{-1}: \text{Bild}(g) \rightarrow N$ . Wir definieren  $A_n \subset M$  für alle  $n \in \mathbb{N}_0$  durch den Rekursionsanfang  $A_0 := M \setminus \text{Bild}(g)$  und den Rekursionsschritt  $A_{n+1} := g(f(A_n))$  für alle  $n \in \mathbb{N}_0$ . Damit können wir  $A_* := \bigcup_{n \in \mathbb{N}_0} A_n$  setzen und  $h: M \rightarrow N$  durch

$$h(x) := \begin{cases} f(x) & \text{für } x \in A_* \\ \tilde{g}^{-1}(x) & \text{für } x \notin A_* \end{cases}$$

(also ein gewisses „Zusammenstückeln“ von  $f$  und  $\tilde{g}^{-1}$ ) für alle  $x \in M$  definieren, denn im Fall  $x \notin A_*$  liegt  $x$  insbesondere in  $M \setminus A_0 = \text{Bild}(g)$ , wo  $\tilde{g}^{-1}$  definiert ist.

Um Injektivität von  $h$  zu zeigen, betrachten wir  $x, y \in M$  mit  $h(y) = h(x)$  und unterscheiden Fälle: Im Fall  $x, y \in A_*$  gilt  $f(y) = f(x)$ , und  $y = x$  folgt per Injektivität von  $f$ . Im Fall  $x, y \notin A_*$  gilt  $\tilde{g}^{-1}(y) = \tilde{g}^{-1}(x)$ , und  $y = x$  folgt aus der Bijektivität von  $\tilde{g}^{-1}$ . Im Fall  $x \in A_*$ ,  $y \notin A_*$  gilt  $\tilde{g}^{-1}(y) = f(x)$ . Es gibt dann ein  $n \in \mathbb{N}_0$  mit  $x \in A_n$  und folglich  $y = \tilde{g}(f(x)) = g(f(x)) \in A_{n+1} \subset A_*$ . Damit ist ein Widerspruch erreicht und das Auftreten dieses Falls tatsächlich ausgeschlossen. Analog sieht man, dass auch der Fall  $x \notin A_*$ ,  $y \in A_*$  nicht eintreten kann. Damit ist wie benötigt  $y = x$  in allen (möglichen) Fällen gezeigt.

Um Surjektivität von  $h$  zu zeigen, sei  $y \in N$ . Da  $\tilde{g}^{-1}$  bijektiv ist, können wir  $y = \tilde{g}^{-1}(x)$  mit  $x \in \text{Bild}(g) = M \setminus A_0$  schreiben. Wir unterscheiden wieder Fälle: Im Fall  $x \notin A_*$  erhalten wir direkt  $y = h(x) \in \text{Bild}(h)$ . Im Fall  $x \in A_*$  muss  $x \in A_n = g(f(A_{n-1}))$  für ein  $n \in \mathbb{N}$  gelten (denn wir hatten  $A_* = \bigcup_{n \in \mathbb{N}_0} A_n$  gewählt, und  $x \notin A_0$  ergab sich bei der Wahl von  $x$ ). Es gibt also ein  $x' \in A_{n-1}$  mit  $x = g(f(x'))$ , und wir erhalten  $y = \tilde{g}^{-1}(x) = \tilde{g}^{-1}(g(f(x'))) = \tilde{g}^{-1}(\tilde{g}(f(x'))) = f(x')$  mit  $x' \in A_*$ . Dies bedeutet auch in diesem Fall  $y = h(x') \in \text{Bild}(h)$ . Damit ist, wie für Surjektivität benötigt,  $y \in \text{Bild}(h)$  in allen Fällen gezeigt.

Insgesamt ist  $h: M \rightarrow N$  injektiv und surjektiv, also auch bijektiv, und es gilt  $|M| = |N|$ .  $\square$

Aufbauend auf (dem Vergleich von) Mächtigkeiten können wir einige weitere Begriffe spezifizieren:

### Definitionen & Bemerkungen (zu (un)endlichen Mengen).

(1) Mit dem Konzept der Gleichmächtigkeit können wir präzisieren, dass eine Menge  $M \dots$

- genau  $n \in \mathbb{N}_0$  Elemente hat, notiert  $|M| = n$ , wenn  $|M| = |\{1, 2, 3, \dots, n-1, n\}|$  gilt<sup>10</sup>,
- **endlich** ist, notiert  $|M| < \infty$ , wenn ein  $n \in \mathbb{N}_0$  mit  $|M| = n$  existiert,
- **unendlich** ist, wenn sie nicht endlich ist.

Gemäß dem Auswahlaxiom (oder einer Folgerung daraus) kann man in jeder unendlichen Menge  $M$  rekursiv  $x_1 \in M$ ,  $x_2 \in M \setminus \{x_1\}$ ,  $x_3 \in M \setminus \{x_1, x_2\}$ ,  $x_4 \in M \setminus \{x_1, x_2, x_3\}$ ,  $\dots$  wählen, daraus eine Injektion  $\mathbb{N} \rightarrow M$ ,  $n \mapsto x_n$  erhalten und so  $|\mathbb{N}| \leq |M|$  einsehen. Damit sind die natürlichen Zahlen gewissermaßen die kleinste unendliche Menge.

(2) Eine alternative, äquivalente Definition (un)endlicher Mengen geht auf Dedekind zurück und kommt ohne expliziten Rückgriff auf die (Struktur der) natürlichen Zahlen aus. Dabei erklärt man eine Menge  $M$  als unendlich, wenn eine echte Teilmenge  $T \subsetneq M$  mit  $|T| = |M|$  existiert, und andernfalls als endlich. Inspiriert wird diese Definition durch die schon in Abschnitt 2.2 erwähnte Eigenschaft, dass die Nachfolge-Abbildung eine Bijektion von  $\mathbb{N}$  auf  $\mathbb{N} \setminus \{1\}$  ist und damit  $|\mathbb{N} \setminus \{1\}| = |\mathbb{N}|$  für die echte Teilmenge  $\mathbb{N} \setminus \{1\} \subsetneq \mathbb{N}$  gilt.

Vor allem bietet das Konzept der Gleichmächtigkeit aber eine Möglichkeit, auch unendliche Menge nach „Größenvergleich“ mit  $\mathbb{N}$  zu unterscheiden:

**Definition ((Über-)Abzählbarkeit).** Eine Menge  $M$  heißt...

- (**höchstens**) **abzählbar**, wenn  $|M| \leq |\mathbb{N}|$  gilt,
- **abzählbar (unendlich)**, wenn  $|M| = |\mathbb{N}|$  gilt,
- **überabzählbar**, wenn  $|M| > |\mathbb{N}|$  gilt.

**Bemerkungen (zu (Über-)Abzählbarkeit).**

(1) **Abzählbarkeit** einer Menge  $M$  bedeutet, dass man die Elemente von  $M$  mit natürlichen Zahlen nummerieren und in der Form  $M = \{x_1, x_2, x_3, \dots, x_{n-1}, x_n\}$  (endliche Liste im Fall  $|M| < |\mathbb{N}|$  mit  $n = |M| \in \mathbb{N}_0$ ) oder  $M = \{x_1, x_2, x_3, \dots\}$  (unendliche Liste im Fall  $|M| = |\mathbb{N}|$ ) nacheinander „aufzählen“ kann (wobei im unendlichen Fall  $|M| = |\mathbb{N}|$  das Aufzählen nie endet, aber zumindest feststeht, wann jedes einzelne Element dran wäre).

(2) Neben  $\mathbb{N}$  selbst ist die Menge  $\mathbb{Z}$  der ganzen Zahlen abzählbar unendlich, denn man kann eine Bijektion  $\mathbb{N} \rightarrow \mathbb{Z}$  zum Beispiel durch Nummerierung aller ganzen Zahlen in der Reihenfolge

$$0, 1, -1, 2, -2, 3, -3, 4, -4, \dots$$

erhalten.

(3) Das erste Cantorsche Diagonalverfahren zeigt, dass die kartesischen Produkte  $\mathbb{N}^2$ ,  $\mathbb{Z}^2$  und die Menge  $\mathbb{Q}$  der rationalen Zahlen abzählbar unendlich sind. Dazu konstruiert man erst eine Bijektion  $\mathbb{N} \rightarrow \mathbb{N}^2$ , für die eine Formel bereits auf Übungsblatt 4 angegeben wurden, hinter der aber letztlich die Grundidee steht, die Paare in  $\mathbb{N}^2$  gemäß dem in Abbildung 31 gezeigten Diagonalschema zu nummerieren:

<sup>10</sup>Im Fall  $n = 0$  verstehen wir  $\{1, 2, 3, \dots, n-1, n\} = \emptyset$ , so dass  $|M| = 0$  genau  $M = \emptyset$  bedeutet.

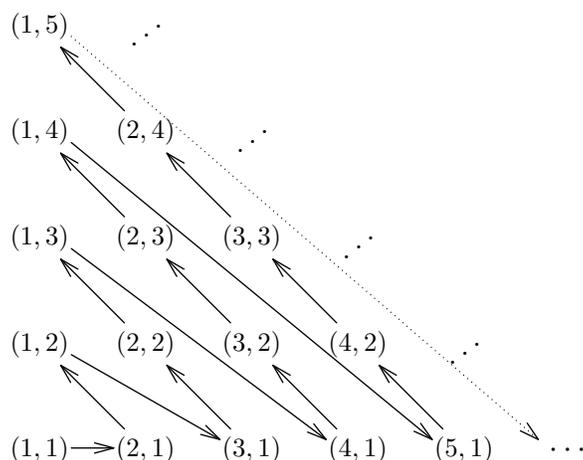


Abb. 31: Die Nummerierung von  $\mathbb{N}^2$  durch das erste Cantorsche Diagonalverfahren (wobei die Pfeile keine Abbildungspfeile sind, sondern nur die Reihenfolge andeuten)

Ist damit  $|\mathbb{N}^2| = |\mathbb{N}|$  gezeigt, so kann dies mit  $|\mathbb{Z}| = |\mathbb{N}|$  und folglich  $|\mathbb{Z}^2| = |\mathbb{N}^2|$  zu  $|\mathbb{Z}^2| = |\mathbb{N}|$  zusammengesetzt werden. Weiter folgt nun  $|\mathbb{Q}| = |\mathbb{N}|$ , denn zu einem gilt mit  $\mathbb{N} \subset \mathbb{Q}$  natürlich  $|\mathbb{N}| \leq |\mathbb{Q}|$ , zum anderen ergibt sich mit der Konstruktion  $\mathbb{Q} = (\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})) / \sim$  des Abschnitts 2.4 und dem Vorausgehenden, dass  $|\mathbb{Q}| \leq |\mathbb{Z}^2| = |\mathbb{N}|$  gilt.

- (4) Beim **zweiten Cantorschen Diagonalverfahren** handelt es sich um ein Widerspruchargument zum Nachweis, dass die **Menge  $\mathbb{R}$  der reellen Zahlen** und ihre Teilmenge  $\mathbb{I} := \{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$  tatsächlich **überabzählbar** sind. Man verwendet dazu (worauf wir in Mathematik 2 noch genauer eingehen), dass jedes  $x \in \mathbb{I}$  eine Darstellung  $0, z_1 z_2 z_3 \dots$  mit unendlich vielen Nachkomma-Ziffern  $z_1, z_2, z_3, \dots \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$  hat. *Angekommen*, man könnte in dieser Darstellung nun alle  $x \in \mathbb{I}$  in einer Reihenfolge

$$\begin{aligned} x_1 &= 0, \mathbf{z_{11}} z_{12} z_{13} z_{14} \dots \\ x_2 &= 0, z_{21} \mathbf{z_{22}} z_{23} z_{24} \dots \\ x_3 &= 0, z_{31} z_{32} \mathbf{z_{33}} z_{34} \dots \\ x_4 &= 0, z_{41} z_{42} z_{43} \mathbf{z_{44}} \dots \\ &\vdots \quad \vdots \quad \vdots \quad \vdots \end{aligned}$$

aufzählen. Dann könnte man für jeden Index  $i \in \mathbb{N}$  eine von der fett gedruckten Ziffer  $z_{ii}$  auf der Diagonale verschiedene Ziffer  $z_i^* \in \{1, 2, 3, 4, 5, 6, 7, 8\} \setminus \{z_{ii}\}$  wählen und erhielte  $x^* := 0, z_1^* z_2^* z_3^* z_4^* \dots \in \mathbb{I}$ . Die Zahl  $x^*$  unterscheidet sich wegen  $z_i^* \neq z_{ii}$  an der  $i$ -ten Nachkommastelle von der  $i$ -ten Zahl auf der Liste, unterscheidet sich also<sup>11</sup> von *jeder* Zahl auf der Liste und kommt auf der Liste nicht vor. *Widerspruch!* Also können die  $x \in \mathbb{I}$  und erst recht alle  $x \in \mathbb{R}$  nicht nummeriert werden,  $\mathbb{I}$  und  $\mathbb{R}$  sind in der Tat überabzählbar.

- (5) Tatsächlich sind  $\mathbb{R}$  und  $\mathbb{I}$  gleichmächtig zur Potenzmenge  $\mathcal{P}(\mathbb{N})$ . Dies kann man mit Hilfe von unendlichen *dyadischen* Nachkomma-Darstellungen einsehen.

<sup>11</sup>An dieser Stelle ist etwas Vorsicht geboten, da bei der unendlichen Darstellung von Zahlen mit eigentlich nur endlich vielen Nachkomma-Stellen die Doppeldeutigkeit  $0, z_1 z_2 \dots z_{k-1} z_k 0000 \dots = 0, z_1 z_2 \dots z_{k-1} (z_k - 1) 9999 \dots$  besteht. Um trotzdem sicher sein zu können, dass  $x^*$  nicht auf der Liste vorkommt, wurden bei der Wahl der  $z_i^*$  die Ziffern 0 und 9 ausgeschlossen.

**Ausblick (Mehr zu Kardinalitäten).**

- (1) Im Prinzip kann die Mächtigkeit einer Menge nicht nur verglichen, sondern auch als eigenständige Eigenschaft einer einzelnen Menge definiert und betrachtet werden. Dazu ordnet man jeder Äquivalenzklasse<sup>12</sup> von gleichmächtigen Mengen  $M$  als Kenngröße eine gewisse Mächtigkeit/Kardinalität/Kardinalzahl  $\aleph$  zu, die die Anzahl der Elemente verallgemeinert, und notiert für diese auch bei unendlichen Mengen  $|M| = \aleph$  (mit dem Aleph  $\aleph$ , dem ersten Buchstaben des phönizischen und hebräischen Alphabets). Da solche Kardinalzahlen aber letztlich auch nur Äquivalenzklassen gleichmächtiger Mengen anzeigen, bringt diese Betrachtungsweise gegenüber der Gleichmächtigkeit und dem Vergleich von Mächtigkeiten kaum einen echten Gewinn. Für die kleinste unendliche Kardinalität, die Kardinalität von  $\mathbb{N}$  und allen abzählbar unendlichen Mengen ist die Bezeichnung  $\aleph_0$  üblich, die nächstgrößere<sup>13</sup> Kardinalität, also die kleinste überabzählbare Kardinalität, nennt man  $\aleph_1$ .
- (2) Die berühmte **Kontinuumshypothese** fragt nun, ob tatsächlich  $|\mathbb{R}| = \aleph_1$  gilt oder nicht, ob also die nächstgrößere Kardinalität nach  $|\mathbb{N}|$  schon die Kardinalität  $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$  des sogenannten Kontinuums  $\mathbb{R}$  ist oder es noch Zwischenstufen gibt. Dieses 1878 von Cantor formulierte Problem war über viele Jahrzehnte eine fundamentale offene Frage der Mathematik und wurde erst durch aufsehenerregende (Meta-)Sätze der berühmten Mathematiker K. Gödel (1906–1978) und P. Cohen (1934–2007) aus den Jahren 1938 und 1963 gelöst: Das erstaunliche Fazit lautet, dass die Frage der Kontinuumshypothese **im Rahmen des Zermelo-Fraenkel-Axiomensystems der Mengenlehre unentscheidbar** ist und auf Basis dieses Systems nicht beantwortet werden kann. Genauer können sowohl die Gültigkeit als auch die Nicht-Gültigkeit der Kontinuumshypothese in konsistenter Weise als Zusatzannahmen zum Axiomensystem hinzugefügt werden. Das Auftreten eines solchen prinzipiell unentscheidbaren Problems ist überraschend und zu einem gewissen Grad schockierend. Dennoch handelt es sich um einen Fakt der mathematischen Theorie, mit dem man (fortan) leben muss. **In der Praxis treten unentscheidbare Probleme glücklicherweise sehr selten auf**, und in den allermeisten mathematischen Disziplinen sind die Gültigkeit oder Nicht-Gültigkeit der Kontinuumshypothese und anderer unentscheidbarer Probleme kaum von Belang.
- (3) Zum Abschluss dieses Abschnitts behandeln wir einen bekannten Satz von Cantor, demzufolge man durch Bildung der Potenzmenge immer noch größere Mächtigkeiten erhält und es daher bei der Mächtigkeit von Mengen kein Limit gibt:

**Satz (von Cantor).** Für jede Menge  $M$  gilt  $|\mathcal{P}(M)| > |M|$ .

Ausgehend von  $|M| = n \implies |\mathcal{P}(M)| = 2^n$  für endliche Mengen  $M$  (was prinzipiell schon bei der ursprünglichen Einführung der Potenzmenge erwähnt wurde) schreibt man für die Mächtigkeit  $|\mathcal{P}(M)|$  der Potenzmenge auch allgemein  $2^{|M|}$ . Damit lautet der Satz von Cantor  $2^{|M|} > |M|$ , und die Kontinuumshypothese fragt nach  $2^{|\mathbb{N}|} = \aleph_1$ .

<sup>12</sup>Die Äquivalenzklassen können, weil eben die Menge aller Mengen nicht existiert, nicht als Mengen gebildet werden. Abstrakt kann man sich eine „Ansammlung“ aller zu einer gegebenen Menge gleichmächtigen Mengen aber trotzdem vorstellen, und im verallgemeinerten Sinn sogenannter Klassen existiert diese Ansammlung auch als formales Objekt.

<sup>13</sup>Tatsächlich ergibt sich mit dem Wohlordnungssatz, dass die Kardinalzahlen nicht nur die Totalordnungs-, sondern auch die Wohlordnungseigenschaft haben. Nur deshalb kann man von einer nächstgrößeren Kardinalität überhaupt sprechen.

Der elegante Beweis des Satzes lehnt sich an die Grundidee des Russellschen Paradoxons an:

*Beweis des Satzes von Cantor.* Da  $M \rightarrow \mathcal{P}(M)$ ,  $x \mapsto \{x\}$  eine Injektion ist, gilt  $|M| \leq |\mathcal{P}(M)|$ . Um  $|M| < |\mathcal{P}(M)|$  zu zeigen, bleibt also  $|M| = |\mathcal{P}(M)|$  oder m.a.W. die Existenz einer Bijektion  $f: M \rightarrow \mathcal{P}(M)$  auszuschließen. *Angenommen*, es gäbe solch eine Bijektion  $f$ . Dann ließe sich die Teilmenge  $T := \{x \in M \mid x \notin f(x)\} \in \mathcal{P}(M)$  bilden, und wegen der Surjektivität von  $f$  gäbe es ein  $a \in M$  mit  $f(a) = T$ . Nun erhielte man einerseits im Fall  $a \in T$ , dass  $a \notin f(a)$ , also  $a \notin T$  gelten müsste, andererseits im Fall  $a \notin T$ , dass  $a \in f(a)$ , also  $a \in T$  gelten müsste. Damit ist in jedem Fall ein *Widerspruch* erreicht. Also existiert keine Bijektion  $f: M \rightarrow \mathcal{P}(M)$ , womit  $|M| < |\mathcal{P}(M)|$  gezeigt ist.  $\square$

Unter anderem gibt der Satz von Cantor auch die Existenz einer Menge  $G$  mit  $|G| > |\mathcal{P}^k(\mathbb{N})|$  für alle  $k \in \mathbb{N}_0$ , wobei sich  $\mathcal{P}^k(\mathbb{N})$  durch  $k$ -fache Bildung der Potenzmenge in der Form  $\mathcal{P}^k(\mathbb{N}) := \mathcal{P}(\mathcal{P}(\dots \mathcal{P}(\mathbb{N}) \dots))$  ergibt. Man erhält dieses  $G$  einfach als  $G := \mathcal{P}(\bigcup_{k \in \mathbb{N}_0} \mathcal{P}^k(\mathbb{N}))$ .

Tatsächlich gibt es der Kardinalitäten insgesamt sogar „zu viele“, um diese in einer Menge zusammenfassen zu können, d.h. genauer, dass eine Menge  $\mathcal{K}$  aller Kardinalitäten nicht existiert. Gäbe es nämlich eine solche Menge  $\mathcal{K}$ , so ließe sich auch eine Vereinigungsmenge  $G := \bigcup_{\aleph \in \mathcal{K}} M_{\aleph}$  bilden, die Mengen  $M_{\aleph}$  jeder Kardinalität  $|M_{\aleph}| = \aleph$  als Teilmengen enthält. Insbesondere enthielte  $G$  eine Teilmenge der Kardinalität  $|\mathcal{P}(G)|$ , was  $|\mathcal{P}(G)| \leq |G|$  bedeutete und damit im Widerspruch zum Satz von Cantor stände.

# Kapitel 3

## Algebraische Grundstrukturen

In diesem Kapitel werden wir das **Konzept eines Zahlbereichs samt Rechenart(en)** **dar- auf sehr weitgehend verallgemeinern**. Dies ist nützlich, um gemeinsame Eigenschaften der Zahlbereiche und der Rechenarten sowie weiterer, ähnlich gearteter Operationen einordnen, be- schreiben und abstrahieren zu können.

### 3.1 Verknüpfungen, Halbgruppen und Gruppen

Wir beginnen mit der Einführung von Verknüpfungen, die Rechenarten verallgemeinern:

**Definitionen (Verknüpfungen und deren Grundeigenschaften).**

(I) *Unter einer (zweistelligen inneren) **Verknüpfung** auf einer Menge  $G$  verstehen wir eine Abbildung  $*$ :  $G \times G \rightarrow G$ . Wir verwenden (ähnlich wie bei Relationen) die Infix-Notation  $g * h$  statt  $*(g, h)$  für das Bild von  $(g, h) \in G \times G$  unter der Verknüpfung  $*$ .*

(II) *Wir nennen eine Verknüpfung  $*$  auf einer Menge  $G$  **assoziativ**, wenn*

$$(g * h) * k = g * (h * k) \quad \text{für alle } g, h, k \in G$$

*gilt.*

(III) *Wir nennen eine Verknüpfung  $*$  auf einer Menge  $G$  **kommutativ**, wenn*

$$g * h = h * g \quad \text{für alle } g, h \in G$$

*gilt.*

**Beispiele (von Verknüpfungen).**

(1) **Verknüpfungen auf endlichen Mengen** können durch **Verknüpfungstabellen** genannte Tabellen angegeben werden, indem man man  $g * h$  in das Feld in der zu  $g$  gehörigen Zeile und zu  $h$  gehörigen Spalte einträgt. Zum Beispiel sind eine Verknüpfung  $\tau$  auf  $\{2, 3, 5, 7\}$  und eine Verknüpfung  $\times$  auf einer beliebigen 3-elementigen Menge  $\{e, \alpha, \beta\}$  wie folgt gegeben:

$\tau$	2	3	5	7
2	5	2	7	3
3	2	3	5	7
5	7	5	7	2
7	3	7	2	5

$\times$	e	$\alpha$	$\beta$
e	e	$\alpha$	$\beta$
$\alpha$	$\alpha$	$\alpha$	$\alpha$
$\beta$	$\beta$	$\beta$	$\beta$

Dabei ist  $\tau$  nicht assoziativ (z.B.  $(2 \tau 2) \tau 5 = 7 \neq 2 \tau (2 \tau 5) = 3$ ), aber kommutativ (was man bei gleicher Reihenfolge in Eingangsspalte und Kopfzeile an Spiegelsymmetrie bezüglich der Diagonalen erkennt). Dagegen ist  $\times$  assoziativ (denn die Verknüpfung mehrerer Elemente gibt unabhängig von der Klammerung das am weitesten links stehende Element  $\neq e$ , falls ein solches existiert, und  $e$  sonst), aber nicht kommutativ ( $\alpha \times \beta = \alpha \neq \beta \times \alpha = \beta$ ).

Die Darstellung einer Verknüpfung durch solche Tafeln wird aber schon **bei relativ wenigen Elementen unübersichtlich** und wird daher **beim praktischen Umgang mit Verknüpfungen eher selten** verwendet.

- (2) Die **Addition**  $+$  und die **Multiplikation**  $\cdot$  sind assoziative und kommutative Verknüpfungen auf jedem der Zahlbereiche  $\mathbb{N}$ ,  $\mathbb{N}_0$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ .
- (3) Die **Subtraktion**  $-$  ist keine Verknüpfung auf  $\mathbb{N}$  oder  $\mathbb{N}_0$  (z.B.  $1-2 \notin \mathbb{N}_0$ ). Sie ist eine Verknüpfung auf  $\mathbb{Z}$ ,  $\mathbb{Q}$  und  $\mathbb{R}$ , ist dort aber weder assoziativ (z.B.  $(0-0)-1 \neq 0-(0-1)$ ) noch kommutativ (z.B.  $0-1 \neq 1-0$ ).
- (4) Die **Division**  $:$  (die wir normalerweise mit dem Schrägstrich oder Bruchstrich notieren) ist keine Verknüpfung auf irgendeinem Zahlbereich, der 0 enthält, (Division durch 0 undefiniert) und auch nicht auf  $\mathbb{N}$  oder  $\mathbb{Z} \setminus \{0\}$  (z.B.  $\frac{1}{2} \notin \mathbb{Z}$ ). Sie ist eine Verknüpfung auf  $\mathbb{Q} \setminus \{0\}$  und  $\mathbb{R} \setminus \{0\}$ , ist dort aber weder assoziativ (z.B.  $\frac{1/1}{2} \neq \frac{1}{1/2}$ ) noch kommutativ (z.B.  $\frac{1}{2} \neq \frac{2}{1}$ ).
- (5) Das Potenzieren  $(m, n) \mapsto m^n$  ist eine Verknüpfung auf  $\mathbb{N}$  und, sobald man irgendeine Konvention für  $0^0 \in \mathbb{N}_0$  festlegt, auch auf  $\mathbb{N}_0$ , ist aber weder assoziativ (z.B.  $2^{(1^2)} \neq (2^1)^2$ ) noch kommutativ (z.B.  $2^1 \neq 1^2$ ).
- (6) Für jede Menge  $\mathcal{X}$  ist die **Komposition o von Selbstabbildungen** eine Verknüpfung auf  $\text{Abb}(\mathcal{X})$ . Diese Verknüpfung ist assoziativ, aber für  $|\mathcal{X}| \geq 2$  nicht kommutativ (siehe Satz und Bemerkung in Abschnitt 2.1). Die Komposition ist auch eine assoziative Verknüpfung auf gewissen Teilmengen von  $\text{Abb}(\mathcal{X})$ , z.B. auf der Menge der Injektionen  $\mathcal{X} \rightarrow \mathcal{X}$ , der Menge der Surjektionen  $\mathcal{X} \rightarrow \mathcal{X}$  und der Menge der Bijektionen  $\mathcal{X} \rightarrow \mathcal{X}$ .
- (7) Für jede Menge  $\mathcal{X}$  sind die **Mengen-Operationen** Vereinigung ( $\cup$ ), Durchschnitt ( $\cap$ ), Differenz ( $\setminus$ ) und symmetrische Differenz ( $\Delta$ ) Verknüpfungen auf der Potenzmenge  $\mathcal{P}(\mathcal{X})$ . Dabei sind  $\cup$ ,  $\cap$  und  $\Delta$  kommutativ und assoziativ (vergleiche mit Abschnitt 1.4), während  $\setminus$  für  $|\mathcal{X}| \geq 1$  weder assoziativ (z.B.  $(\{x\} \setminus \{x\}) \setminus \emptyset \neq \{x\} \setminus (\emptyset \setminus \{x\})$ ) noch kommutativ (z.B.  $\{x\} \setminus \emptyset \neq \emptyset \setminus \{x\}$ ) ist.
- (8) Etwas ungewöhnliche Beispiele für Verknüpfungen sind der größte gemeinsame Teiler und das kleinste gemeinsame Vielfache zweier natürlicher Zahlen. Man kann (per Primfaktorzerlegung) zeigen, dass es sich um assoziative und kommutative Verknüpfungen auf  $\mathbb{N}$  handelt.

Oftmals nützlich im Zusammenhang mit verschiedenen Verknüpfungen ist:

**Notation** (für Verknüpfungen und (Teil-)Mengen). Sei  $*$  eine Verknüpfung auf einer Menge  $G$ . Für  $g \in G$  und  $A, B \subset G$  verwenden wir häufig die auf Mengen erweiterten Infix-Notationen

$$g * A := \{g * a \mid a \in A\}, \quad A * g := \{a * g \mid a \in A\}, \quad A * B := \{a * b \mid (a, b) \in A \times B\}$$

für die Bilder der kartesischen Produkte  $\{g\} \times A$ ,  $A \times \{g\}$  und  $A \times B$  unter  $*$ .

**Bemerkungen und Beispiele** (zur auf Mengen erweiterten Notation für Verknüpfungen).

- (1) Tatsächlich wird mit der Definition von  $A * B$  eine Verknüpfung auf  $\mathcal{P}(G)$  erklärt, die genau dann assoziativ beziehungsweise kommutativ ist, wenn die Verknüpfung  $*$  auf  $G$  dies ist.
- (2) Speziell ist die sich aus der Addition  $+$  auf einem Zahlbereich  $\mathbb{B} \in \{\mathbb{N}, \mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}\}$  ergebende Verknüpfung  $+$  auf  $\mathcal{P}(\mathbb{B})$  mit  $A+B = \{a+b \mid (a, b) \in A \times B\}$  als **Minkowski-Addition** von Mengen bekannt.
- (3) Konkret ergibt sich beispielsweise aus  $A = \{0, 4, 7\}$  und  $B = \{1, -5\}$  durch Multiplikation und Subtraktion  $3A-B = \{-1, 5, 11, 17, 20, 26\}$ .
- (4) Die eingeführte Notation ist sehr nützlich und erlaubt es beispielsweise, die Mengen der geraden beziehungsweise ungeraden Zahlen in  $\mathbb{N}$  und  $\mathbb{Z}$  prägnant als  $2\mathbb{N}$  und  $2\mathbb{Z}$  beziehungsweise  $2\mathbb{N}-1$  und  $2\mathbb{Z}+1 = 2\mathbb{Z}-1$  zu schreiben.
- (5) Dass bei Verwendung solcher Notationen **etwas Vorsicht** geboten ist, erkennt man aber daran, dass schon für  $A \subset \mathbb{N}$  meistens  $A+A \neq 2A$  und  $A-A \neq \{0\}$  gelten: Beispielsweise für  $A = \{1, 2\}$  ergibt sich  $A+A = \{2, 3, 4\}$ , aber  $2A = \{2, 4\}$ . Weiterhin gilt  $\mathbb{N}-\mathbb{N} = \mathbb{Z}$ .

**Notationen** (für Verknüpfungen von Tupeln und Abbildungen). Sei  $*$  eine Verknüpfung auf einer Menge  $G$ .

- (1) Für jedes  $n \in \mathbb{N}$  definieren wir die **komponentenweise** Anwendung der Verknüpfung  $*$  auf **Tupeln** durch

$$x * y := (x_1 * y_1, x_2 * y_2, \dots, x_n * y_n) \in G^n \quad \text{für } x, y \in G^n.$$

- (2) Für jede Menge  $\mathcal{X}$  definieren wir die **punktweise** Anwendung der Verknüpfung  $*$  auf **Abbildungen**  $f_1, f_2: \mathcal{X} \rightarrow G$  durch

$$(f_1 * f_2)(x) := f_1(x) * f_2(x) \in G \quad \text{für alle } x \in \mathcal{X}$$

und legen damit eine Abbildung  $f_1 * f_2: \mathcal{X} \rightarrow G$  fest.

**Bemerkungen** (zu Verknüpfungen von Tupeln und Abbildungen).

- (1) Mit dieser Definition von  $x * y$  und von  $f_1 * f_2$  erhalten wir eine Verknüpfung auf dem kartesischen Produkt  $G^n$  und eine Verknüpfung auf der Menge  $\text{Abb}(\mathcal{X}, G)$  der Abbildungen  $\mathcal{X} \rightarrow G$ . Beide diese Verknüpfungen sind (wenn  $\mathcal{X} \neq \emptyset$ ) genau dann assoziativ beziehungsweise kommutativ, wenn  $*$  auf  $G$  dies ist.
- (2) Insbesondere sind hiermit die **komponentenweise Summe/Differenz**  $x \pm y$ , das **komponentenweise Produkt**  $x \cdot y$ , der **komponentenweise Quotient**  $\frac{x}{y}$  von **Tupeln**  $x, y \in \mathbb{B}^n$  und die **komponentenweise Summe/Differenz**  $f_1 \pm f_2$ , das **komponentenweise Produkt**  $f_1 \cdot f_2$ , der **komponentenweise Quotient**  $\frac{f_1}{f_2}$  von **Abbildungen**  $f_1, f_2: \mathcal{X} \rightarrow \mathbb{B}$  erklärt, jedenfalls soweit die Rechenoperationen Verknüpfungen auf den Zahlbereichen  $\mathbb{B} \in \{\mathbb{N}, \mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Z} \setminus \{0\}, \mathbb{Q} \setminus \{0\}, \mathbb{R} \setminus \{0\}\}$  sind.

**Definitionen (neutrale/inverse Elemente).** Sei  $*$  eine Verknüpfung auf einer Menge  $G$ .

- (I) Wir nennen  $e \in G$  ein **neutrales Element** (für/von  $*$ ), wenn  $e * g = g = g * e$  für alle  $g \in G$  gilt.
- (II) Falls ein neutrales Element  $e \in G$  für  $*$  existiert, so nennen wir  $h \in G$  ein zu  $g \in G$  (bezüglich  $*$ ) **inverses Element** oder **Inverses** zu/von  $g \in G$ , wenn  $h * g = e = g * h$  gilt. Existiert ein Inverses zu  $g \in G$ , so heißt  $g$  (in  $G$ ) **invertierbar**.

**Bemerkungen & Notation** (zu/bei neutralen/inversen Elementen). Sei  $*$  eine Verknüpfung auf einer Menge  $G$ .

- (1) Existiert ein **neutrales Element**  $e \in G$  für  $*$ , so ist dieses stets **eindeutig**. Ist nämlich  $e' \in G$  ein weiteres neutrales Element für  $*$ , so folgt aus der Definition  $e' = e' * e = e$ . Daher ist es beim Umgang mit inversen Elementen nicht nötig, das neutrale Element explizit zu benennen (solange es existiert).
- (2) Existiert ein **inverses Element**  $h \in G$  zu  $g \in G$  und ist  $*$  zumindest assoziativ, so ist das inverse Element  $h$  zu  $g$  **eindeutig**. Ist nämlich  $h' \in G$  ein weiteres inverses Element zu  $g$ , so folgt per Definition  $h' = h' * e = h' * (g * h) = (h' * g) * h = e * h = h$ . (Dasselbe Argument haben wir für die Komposition von Abbildungen schon in Abschnitt 2.1 benutzt.)
- (3) Bei assoziativer Verknüpfung  $*$  wird die **Notation**  $g^{-1} \in G$  für das **inverse Element** (falls existent) zu  $g \in G$  sinnvoll. Wir halten fest, dass  $g^{-1}$  per Definition  $g^{-1} * g = e = g * g^{-1}$  erfüllt und folgende **allgemeine Regeln für Inverse** gelten:

$$\begin{aligned} e^{-1} &= e && \text{für das neutrale Element } e \in G, \\ (g^{-1})^{-1} &= g && \text{für invertierbares } g \in G, \\ (g * h)^{-1} &= h^{-1} * g^{-1} && \text{für invertierbare } g, h \in G. \end{aligned}$$

Für die letzte Regel rechnet man dabei mit den Definitionen und Assoziativität nach, dass  $h^{-1} * g^{-1} * g * h = h^{-1} * e * h = h^{-1} * h = e = g * g^{-1} = g * e * g^{-1} = g * h * h^{-1} * g^{-1}$  gilt.

- (4) Manchmal werden auch **linksneutrale Elemente**  $\ell \in G$  mit  $\ell * g = g$  für alle  $g \in G$  und **rechtsneutrale Elemente**  $r \in G$  mit  $g * r = g$  für alle  $g \in G$  betrachtet. Solche Elemente sind im Allgemeinen nicht eindeutig bestimmt. Sobald aber ein linksneutrales Element  $\ell$  und ein rechtsneutrales Element  $r$  existieren, sind beide eindeutig, stimmen überein und sind damit auch das eindeutige neutrale Element. Das ergibt sich aus  $\ell = \ell * r = r$ .
- (5) Ebenso werden (Existenz des neutralen Elements  $e$  vorausgesetzt) manchmal **Linksinverse**  $h \in G$  zu  $g \in G$  mit  $h * g = e$  und **Rechtsinverse**  $h \in G$  zu  $g \in G$  mit  $g * h = e$  betrachtet. Linksinverse und Rechtsinverse zu  $g$  sind im Allgemeinen nicht eindeutig bestimmt. Sobald aber ein Linksinverses  $h'$  und ein Rechtsinverses  $h$  zu einem  $g$  existieren und  $*$  assoziativ ist, sind beide eindeutig, stimmen überein und sind damit auch das eindeutige Inverse zu  $g$ . Das zeigt die Rechnung aus Bemerkung (2) (für ein Linksinverses  $h'$  und ein Rechtsinverses  $h$ ).

**Definitionen (Halbgruppen, Gruppen).**

- (I) Eine **Halbgruppe** ist ein Paar  $(G, *)$  aus einer Menge  $G$  und einer **assoziativen** Verknüpfung  $*$  auf  $G$ . Gibt es für  $*$  ein neutrales Element, so spricht man von einer **Halbgruppe mit neutralem Element**.
- (II) Eine **Gruppe**  $(G, *)$  ist eine Halbgruppe mit neutralem Element, bei der zu jedem Element  $g \in G$  ein inverses Element  $g^{-1} \in G$  existiert.

- (III) Eine Halbgruppe oder Gruppe  $(G, *)$  heißt **kommutativ** oder **abelsch**, wenn  $*$  eine kommutative Verknüpfung ist.

**Bemerkung.** Später verzichtet man sehr häufig auf die explizite Angabe der Verknüpfung  $*$ , die sich oft aus dem Kontext ergibt, und spricht nur davon, dass die zugrundeliegende Menge  $G$  eine (Halb-)Gruppe ist. Ist speziell die Verknüpfung eine Addition oder Multiplikation (gewisser Objekte), so spricht man von einer **additiven (Halb-)Gruppe**  $G$  oder **multiplikativen (Halb-)Gruppe**  $G$ . Auch beim Umgang mit allgemeinen (Halb-)Gruppen mit beliebiger Verknüpfung  $*$  stellt man sich  $*$  häufig als „eine Art Multiplikation“ vor und benutzt daran angelehnte Schreibweisen (zum Beispiel für Potenzen; dazu demnächst).

**Beispiele (von Halbgruppen und Gruppen).**

- (1) Mit den Verknüpfungstafeln (die erste gegenüber der für  $\tau$  im früheren Beispiel (1) nur bei der Verknüpfung von 5 mit sich modifiziert, die zweite unverändert)

⊗	2	3	5	7
2	5	2	7	3
3	2	3	5	7
5	7	5	3	2
7	3	7	2	5

und

×	e	α	β
e	e	α	β
α	α	α	α
β	β	β	β

wird  $(\{2, 3, 5, 7\}, \otimes)$  zu einer abelschen Gruppe mit neutralem Element 3 und den Inversen  $2^{-1}=7, 7^{-1}=2, 5^{-1}=5$  sowie  $(\{e, \alpha, \beta\}, \times)$  zu einer nicht-kommutativen Halbgruppe mit neutralem Element  $e$  und nicht-invertierbaren Elementen  $\alpha, \beta$ . Die Eigenschaft des neutralen Elements erkennt man in der Verknüpfungstafel daran, dass die zugehörige Spalte und Zeile Kopien der Eingangsspalte und Kopfzeile sind. Für die Verknüpfungstafel einer Gruppe ist neben der Existenz des neutralen Elements erforderlich (aber noch nicht ausreichend<sup>1</sup>), dass jedes Element in jeder Zeile und jeder Spalte genau einmal auftritt.

Wie schon bei Verknüpfungen gesagt, ist die **Angabe solcher Tafeln in der Praxis aber weniger üblich und hilfreich.**

- (2) Für die üblichen Zahlbereiche  $\mathbb{B}$  mit der Addition  $+$  und der Multiplikation  $\cdot$  sind  $(\mathbb{B}, +)$  und  $(\mathbb{B}, \cdot)$ , wie in folgender Tabelle angegeben, **kommutative Halbgruppen (kHG)**, **kommutative Halbgruppen mit neutralem Element (kHG-n)** oder sogar **kommutative Gruppen (kG)** (wobei jeweils die stärkste Eigenschaft angegeben wird):

	$\mathbb{N}$	$\mathbb{N}_0$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{Z} \setminus \{0\}$	$\mathbb{Q} \setminus \{0\}$	$\mathbb{R} \setminus \{0\}$
$+$	kHG	kHG-n	kG		—			
$\cdot$	kHG-n					kG		

Das **neutrale Element der Addition** ist immer  $0$ , das **neutrale Element der Multiplikation** ist immer  $1$ . Das **additiv Inverse** zu  $x \in \mathbb{B}$  ist  $-x$ , das **multiplikativ Inverse** zu  $x \in \mathbb{B} \setminus \{0\}$  ist  $\frac{1}{x}$ .

<sup>1</sup>In der Tat definiert nebenstehende Verknüpfungstafel eine kommutative Verknüpfung  $\star$  auf  $\{e, \alpha, \beta, \gamma, \delta, \varepsilon\}$  mit neutralem Element  $e$ , wobei jedes Element in jeder Zeile und Spalte genau einmal auftritt, wegen  $(\delta \star \gamma) \star \beta = \delta \neq \delta \star (\gamma \star \beta) = \beta$  aber dennoch keine Assoziativität und keine Gruppe vorliegt:

*	e	α	β	γ	δ	ε
e	e	α	β	γ	δ	ε
α	α	e	δ	β	ε	γ
β	β	δ	e	ε	γ	α
γ	γ	β	ε	e	α	δ
δ	δ	ε	γ	α	e	β
ε	ε	γ	α	δ	β	e

All dies ergibt sich sofort aus den üblichen Rechenregeln in den Zahlbereichen.

- (3) **Produkt-(Halb-)Gruppen:** Für jedes  $n \in \mathbb{N}$  und jede (Halb-)Gruppe  $(G, *)$  ist auch  $(G^n, *)$  mit der komponentenweisen Verknüpfung  $*$  eine (Halb-)Gruppe, auf die sich auch Kommutativität und/oder Existenz des neutralen Elements überträgt.

Etwas allgemeiner ergibt sich auch als Produkt von  $n \in \mathbb{N}$  (Halb-)Gruppen  $(G_1, *)$ ,  $(G_2, *)$ ,  $\dots$ ,  $(G_n, *)$  eine (Halb-)Gruppe  $(G_1 \times G_2 \times \dots \times G_n, *)$ , deren Verknüpfung durch  $(g_1, g_2, \dots, g_n) * (g'_1, g'_2, \dots, g'_n) := (g_1 * g'_1, g_2 * g'_2, \dots, g_n * g'_n)$  für  $(g_1, g_2, \dots, g_n), (g'_1, g'_2, \dots, g'_n) \in G_1 \times G_2 \times \dots \times G_n$  komponentenweise erklärt ist; vgl. Aufgabe 22(a) auf Blatt 10.

- (4) **Abbildungs-(Halb-)Gruppen:** Für jede Menge  $\mathcal{X}$  und jede (Halb-)Gruppe  $(G, *)$  ist auch  $(\text{Abb}(\mathcal{X}, G), *)$  mit der punktweisen Verknüpfung  $*$  eine (Halb-)Gruppe, auf die sich auch Kommutativität und/oder Existenz des neutralen Elements überträgt. Speziell sind  $(\text{Abb}(\mathcal{X}, \mathbb{B}), +)$  und  $(\text{Abb}(\mathcal{X}, \mathbb{B}), \cdot)$  insoweit (Halb-)gruppen wie  $(\mathbb{B}, +)$  und  $(\mathbb{B}, \cdot)$ .

**(Halb-)Gruppen von Selbstabbildungen:** Auch ist für jede Menge  $\mathcal{X}$  auch  $(\text{Abb}(\mathcal{X}), \circ)$ , die Menge der **Selbstabbildungen** von  $\mathcal{X}$  mit der **Komposition**  $\circ$ , eine (für  $|\mathcal{X}| \geq 2$  nicht kommutative) Halbgruppe mit neutralem Element  $\text{id}_{\mathcal{X}}$ . Die Menge der Bijektionen  $\mathcal{X} \rightarrow \mathcal{X}$  ist mit  $\circ$  sogar eine (für  $|\mathcal{X}| \geq 3$  nicht kommutative) Gruppe, in der das Inverse einer Bijektion deren Umkehrabbildung ist.

Die Menge der Injektionen  $\mathcal{X} \rightarrow \mathcal{X}$  und die Menge der Surjektionen  $\mathcal{X} \rightarrow \mathcal{X}$  stimmen übrigens für endliches  $\mathcal{X}$  mit der Menge der Bijektionen  $\mathcal{X} \rightarrow \mathcal{X}$  überein, werden für unendliches  $\mathcal{X}$  aber durch  $\circ$  zu nicht-kommutativen Halbgruppen mit neutralem Element, in denen für jedes Element ein Linksinverses beziehungsweise Rechtsinverses existiert, dieses für nicht-invertierbare Elemente aber nicht eindeutig ist.

- (5) **(Halb-)Gruppen von Mengen:** Für jede Menge  $\mathcal{X}$  sind  $(\mathcal{P}(\mathcal{X}), \cup)$  und  $(\mathcal{P}(\mathcal{X}), \cap)$  kommutative Halbgruppen mit neutralem Element  $\emptyset$  beziehungsweise  $\mathcal{X}$ . Weiterhin ist  $(\mathcal{P}(\mathcal{X}), \Delta)$  sogar eine kommutative Gruppe mit neutralem Element  $\emptyset$  und der (bei dieser Betrachtungsweise ungewohnten Eigenschaft), dass mit  $M \Delta M = \emptyset$  für alle  $M \subset \mathcal{X}$  jedes Element zu sich selbst invers ist.
- (6) Mit dem größten gemeinsamen Teiler zweier natürlicher Zahlen wird  $\mathbb{N}$  zu einer kommutativen Halbgruppe, mit dem kleinsten gemeinsamen Vielfachen zweier natürlicher Zahlen sogar zu einer kommutativen Halbgruppe mit neutralem Element 1.
- (7) **Weitere, sehr wichtige Beispiele** von (Halb-)Gruppen ergeben sich aus dem **Modulo-Rechnen** sowie dem Umgang und Rechnen mit **Permutationen, Polynomen, Vektoren oder Matrizen**. Diese werden teils im Folgenden, teils erst in Mathematik 2 behandelt.

**Satz & Definition** (zu den **Gruppen des Restklassenrings**  $\mathbb{Z}_n$ ). Sei  $n \in \mathbb{N}$ .

- (I) Wir bezeichnen die Menge der Modulo- $n$ -Äquivalenzklassen künftig auch als den **Modulo- $n$ -Restklassenring**

$$\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\sim.$$

Die Äquivalenzklasse eines  $x \in \mathbb{Z}$  wird auch die **Restklasse** von  $x$  modulo  $n$  genannt und besitzt die alternative Darstellung  $[x]_{\mathbb{Z}_n} = x + n\mathbb{Z} \in \mathbb{Z}_n$ .

- (II) Die Addition und die Multiplikation geben durch

$$[x]_{\mathbb{Z}_n} + [y]_{\mathbb{Z}_n} := [x+y]_{\mathbb{Z}_n} \quad \text{und} \quad [x]_{\mathbb{Z}_n} \cdot [y]_{\mathbb{Z}_n} := [xy]_{\mathbb{Z}_n} \quad \text{für } x, y \in \mathbb{Z}$$

wohldefinierte Verknüpfungen auf  $\mathbb{Z}_n$ . Im Fall der Addition kann  $[x]_{\mathbb{Z}_n} + [y]_{\mathbb{Z}_n}$  äquivalent als Minkowski-Addition von Teilmengen von  $\mathbb{Z}$  interpretiert werden.

(III) Mit diesen Verknüpfungen ist  $(\mathbb{Z}_n, +)$  eine abelsche Gruppe mit neutralem Element  $[0]_{\mathbb{Z}_n}$  und Inverse  $[-x]_{\mathbb{Z}_n}$  zu  $[x]_{\mathbb{Z}_n}$  sowie  $(\mathbb{Z}_n, \cdot)$  eine kommutative Halbgruppe mit neutralem Element  $[1]_{\mathbb{Z}_n}$ . Kürzen wir  $\mathbb{Z}_p^\times := \mathbb{Z}_p \setminus \{[0]_{\mathbb{Z}_p}\}$  ab, so ist darüber hinaus  $(\mathbb{Z}_p^\times, \cdot)$  genau für die Primzahlen  $p \in \mathbb{N}$  eine abelsche Gruppe.

*Beweis von Teil (I) des Satzes.* Nach Definition von Modulo-Relationen und Äquivalenzklassen gilt  $[x]_{\mathbb{Z}_n} = \{y \in \mathbb{Z} \mid y \stackrel{n}{\sim} x\} = \{y \in \mathbb{Z} \mid y - x = nz \text{ für ein } z \in \mathbb{Z}\} = \{x + nz \mid z \in \mathbb{Z}\} = x + n\mathbb{Z}$ .  $\square$

*Beweis von Teil (II) des Satzes.* Für die Wohldefiniertheit der Addition ist  $[x'] = [x] \wedge [y'] = [y] \implies [x' + y'] = [x + y]$  für die Äquivalenzklassen bezüglich der Modulo- $n$ -Relation zu zeigen. Zum Nachweis reicht die Beobachtung, dass, wenn  $x' - x$  und  $y' - y$  durch  $n$  teilbar sind, stets auch  $(x' + y') - (x + y) = (x' - x) + (y' - y)$  durch  $n$  teilbar ist. Bei Interpretation als Minkowski-Addition, ergibt sich mit Teil (I), Kommutativität, Assoziativität und der Beobachtung  $n\mathbb{Z} + n\mathbb{Z} = n\mathbb{Z}$  die identische Vorschrift  $[x]_{\mathbb{Z}_n} + [y]_{\mathbb{Z}_n} = (x + n\mathbb{Z}) + (y + n\mathbb{Z}) = x + y + n\mathbb{Z} + n\mathbb{Z} = x + y + n\mathbb{Z} = [x + y]_{\mathbb{Z}_n}$ .

Für die Wohldefiniertheit der Multiplikation ist analog  $[x'] = [x] \wedge [y'] = [y] \implies [x'y'] = [xy]$  zu zeigen. Dies ist aber ebenfalls gegeben, weil Teilbarkeit von  $x' - x$  und  $y' - y$  durch  $n$  die Teilbarkeit von  $x'y' - xy = (x' - x)y' + x(y' - y)$  durch  $n$  nach sich zieht.  $\square$

Den Beweis von Teil (III) des Satzes gehen wir erst nach einigen Beispielen hierzu an:

**Beispiele (zu den Gruppen des Restklassenrings  $\mathbb{Z}_n$ ).**

(1) Für Restklassen in  $\mathbb{Z}_2$  und  $\mathbb{Z}_7$  gelten

$$[3] + [-5] = [-2] \text{ in } \mathbb{Z}_2, \quad [1] + [1] = [0] \text{ in } \mathbb{Z}_2, \quad [3] \cdot [5] = [1] \text{ in } \mathbb{Z}_7.$$

Dies bedeutet letztlich dasselbe wie

$$3 - 5 = -2 \pmod{2}, \quad 1 + 1 = 0 \pmod{2}, \quad 3 \cdot 5 = 1 \pmod{7},$$

was wir auch in Abschnitt 2.3.2 schon hinschreiben konnten. Jetzt verstehen wir aber genauer, wie weit diese Art des Rechnens trägt.

(2) Da  $\mathbb{Z}_n$  aus den  $n$  Restklassen  $[0] = n\mathbb{Z}$ ,  $[1] = 1 + n\mathbb{Z}$ ,  $[2] = 2 + n\mathbb{Z}$ ,  $\dots$ ,  $[n-2] = (n-2) + n\mathbb{Z}$ ,  $[n-1] = (n-1) + n\mathbb{Z}$  besteht (was man formal durch Division mit Rest einsieht), lassen sich die Addition und die Multiplikation auf  $\mathbb{Z}_n$  für festes  $n \in \mathbb{N}$  durch Verknüpfungstabellen vollständig angeben. Wir zeigen hier die Verknüpfungstabellen

• für $\mathbb{Z}_2$ :	<table border="1" style="border-collapse: collapse; margin: auto;"> <tr><td style="padding: 2px 5px;">+</td><td style="padding: 2px 5px;">[0]</td><td style="padding: 2px 5px;">[1]</td></tr> <tr><td style="padding: 2px 5px;">[0]</td><td style="padding: 2px 5px;">[0]</td><td style="padding: 2px 5px;">[1]</td></tr> <tr><td style="padding: 2px 5px;">[1]</td><td style="padding: 2px 5px;">[1]</td><td style="padding: 2px 5px;">[0]</td></tr> </table>	+	[0]	[1]	[0]	[0]	[1]	[1]	[1]	[0]	<table border="1" style="border-collapse: collapse; margin: auto;"> <tr><td style="padding: 2px 5px;">·</td><td style="padding: 2px 5px;">[0]</td><td style="padding: 2px 5px;">[1]</td></tr> <tr><td style="padding: 2px 5px;">[0]</td><td style="padding: 2px 5px;">[0]</td><td style="padding: 2px 5px;">[0]</td></tr> <tr><td style="padding: 2px 5px;">[1]</td><td style="padding: 2px 5px;">[0]</td><td style="padding: 2px 5px;">[1]</td></tr> </table>	·	[0]	[1]	[0]	[0]	[0]	[1]	[0]	[1]																																
+	[0]	[1]																																																		
[0]	[0]	[1]																																																		
[1]	[1]	[0]																																																		
·	[0]	[1]																																																		
[0]	[0]	[0]																																																		
[1]	[0]	[1]																																																		
• für $\mathbb{Z}_3$ :	<table border="1" style="border-collapse: collapse; margin: auto;"> <tr><td style="padding: 2px 5px;">+</td><td style="padding: 2px 5px;">[0]</td><td style="padding: 2px 5px;">[1]</td><td style="padding: 2px 5px;">[2]</td></tr> <tr><td style="padding: 2px 5px;">[0]</td><td style="padding: 2px 5px;">[0]</td><td style="padding: 2px 5px;">[1]</td><td style="padding: 2px 5px;">[2]</td></tr> <tr><td style="padding: 2px 5px;">[1]</td><td style="padding: 2px 5px;">[1]</td><td style="padding: 2px 5px;">[2]</td><td style="padding: 2px 5px;">[0]</td></tr> <tr><td style="padding: 2px 5px;">[2]</td><td style="padding: 2px 5px;">[2]</td><td style="padding: 2px 5px;">[0]</td><td style="padding: 2px 5px;">[1]</td></tr> </table>	+	[0]	[1]	[2]	[0]	[0]	[1]	[2]	[1]	[1]	[2]	[0]	[2]	[2]	[0]	[1]	<table border="1" style="border-collapse: collapse; margin: auto;"> <tr><td style="padding: 2px 5px;">·</td><td style="padding: 2px 5px;">[0]</td><td style="padding: 2px 5px;">[1]</td><td style="padding: 2px 5px;">[2]</td></tr> <tr><td style="padding: 2px 5px;">[0]</td><td style="padding: 2px 5px;">[0]</td><td style="padding: 2px 5px;">[0]</td><td style="padding: 2px 5px;">[0]</td></tr> <tr><td style="padding: 2px 5px;">[1]</td><td style="padding: 2px 5px;">[0]</td><td style="padding: 2px 5px;">[1]</td><td style="padding: 2px 5px;">[2]</td></tr> <tr><td style="padding: 2px 5px;">[2]</td><td style="padding: 2px 5px;">[0]</td><td style="padding: 2px 5px;">[2]</td><td style="padding: 2px 5px;">[1]</td></tr> </table>	·	[0]	[1]	[2]	[0]	[0]	[0]	[0]	[1]	[0]	[1]	[2]	[2]	[0]	[2]	[1]																		
+	[0]	[1]	[2]																																																	
[0]	[0]	[1]	[2]																																																	
[1]	[1]	[2]	[0]																																																	
[2]	[2]	[0]	[1]																																																	
·	[0]	[1]	[2]																																																	
[0]	[0]	[0]	[0]																																																	
[1]	[0]	[1]	[2]																																																	
[2]	[0]	[2]	[1]																																																	
• für $\mathbb{Z}_4$ :	<table border="1" style="border-collapse: collapse; margin: auto;"> <tr><td style="padding: 2px 5px;">+</td><td style="padding: 2px 5px;">[0]</td><td style="padding: 2px 5px;">[1]</td><td style="padding: 2px 5px;">[2]</td><td style="padding: 2px 5px;">[3]</td></tr> <tr><td style="padding: 2px 5px;">[0]</td><td style="padding: 2px 5px;">[0]</td><td style="padding: 2px 5px;">[1]</td><td style="padding: 2px 5px;">[2]</td><td style="padding: 2px 5px;">[3]</td></tr> <tr><td style="padding: 2px 5px;">[1]</td><td style="padding: 2px 5px;">[1]</td><td style="padding: 2px 5px;">[2]</td><td style="padding: 2px 5px;">[3]</td><td style="padding: 2px 5px;">[0]</td></tr> <tr><td style="padding: 2px 5px;">[2]</td><td style="padding: 2px 5px;">[2]</td><td style="padding: 2px 5px;">[3]</td><td style="padding: 2px 5px;">[0]</td><td style="padding: 2px 5px;">[1]</td></tr> <tr><td style="padding: 2px 5px;">[3]</td><td style="padding: 2px 5px;">[3]</td><td style="padding: 2px 5px;">[0]</td><td style="padding: 2px 5px;">[1]</td><td style="padding: 2px 5px;">[2]</td></tr> </table>	+	[0]	[1]	[2]	[3]	[0]	[0]	[1]	[2]	[3]	[1]	[1]	[2]	[3]	[0]	[2]	[2]	[3]	[0]	[1]	[3]	[3]	[0]	[1]	[2]	<table border="1" style="border-collapse: collapse; margin: auto;"> <tr><td style="padding: 2px 5px;">·</td><td style="padding: 2px 5px;">[0]</td><td style="padding: 2px 5px;">[1]</td><td style="padding: 2px 5px;">[2]</td><td style="padding: 2px 5px;">[3]</td></tr> <tr><td style="padding: 2px 5px;">[0]</td><td style="padding: 2px 5px;">[0]</td><td style="padding: 2px 5px;">[0]</td><td style="padding: 2px 5px;">[0]</td><td style="padding: 2px 5px;">[0]</td></tr> <tr><td style="padding: 2px 5px;">[1]</td><td style="padding: 2px 5px;">[0]</td><td style="padding: 2px 5px;">[1]</td><td style="padding: 2px 5px;">[2]</td><td style="padding: 2px 5px;">[3]</td></tr> <tr><td style="padding: 2px 5px;">[2]</td><td style="padding: 2px 5px;">[0]</td><td style="padding: 2px 5px;">[2]</td><td style="padding: 2px 5px;">[0]</td><td style="padding: 2px 5px;">[2]</td></tr> <tr><td style="padding: 2px 5px;">[3]</td><td style="padding: 2px 5px;">[0]</td><td style="padding: 2px 5px;">[3]</td><td style="padding: 2px 5px;">[2]</td><td style="padding: 2px 5px;">[1]</td></tr> </table>	·	[0]	[1]	[2]	[3]	[0]	[0]	[0]	[0]	[0]	[1]	[0]	[1]	[2]	[3]	[2]	[0]	[2]	[0]	[2]	[3]	[0]	[3]	[2]	[1]
+	[0]	[1]	[2]	[3]																																																
[0]	[0]	[1]	[2]	[3]																																																
[1]	[1]	[2]	[3]	[0]																																																
[2]	[2]	[3]	[0]	[1]																																																
[3]	[3]	[0]	[1]	[2]																																																
·	[0]	[1]	[2]	[3]																																																
[0]	[0]	[0]	[0]	[0]																																																
[1]	[0]	[1]	[2]	[3]																																																
[2]	[0]	[2]	[0]	[2]																																																
[3]	[0]	[3]	[2]	[1]																																																

Man erkennt insbesondere, dass die Multiplikation zwar auf  $\mathbb{Z}_2^\times$  und  $\mathbb{Z}_3^\times$  eine Verknüpfung ist, aber wegen  $[2] \cdot [2] = [0]$  nicht auf  $\mathbb{Z}_4^\times$ .

*Beweis von Teil (III) des Satzes.* Da die Wohldefiniertheit der Verknüpfungen durch Teil (II) gesichert ist, ergeben sich die für alle  $n \in \mathbb{N}$  gültigen (Halb-)Gruppeneigenschaften von  $(\mathbb{Z}_n, +)$  und  $(\mathbb{Z}_n, \cdot)$  sofort aus denen von  $(\mathbb{Z}, +)$  und  $(\mathbb{Z}, \cdot)$ .

Ist  $p \in \mathbb{N}$  keine Primzahl, so ist zunächst  $\mathbb{Z}_1^\times = \emptyset$  im Fall  $p = 1$  wegen Nicht-Existenz des neutralen Elements keine Gruppe. In den anderen Nicht-Primzahl-Fällen können wir  $p = xy$  mit  $x, y \in \{2, 3, \dots, p-1\}$  schreiben. Da für  $[x], [y] \in \mathbb{Z}_p^\times$  dann  $[x] \cdot [y] = [p] = [0] \notin \mathbb{Z}_p^\times$  eintritt, ist  $\cdot$  nur auf  $\mathbb{Z}_p$ , aber nicht auf  $\mathbb{Z}_p^\times$  wohldefinierte Verknüpfung, und  $(\mathbb{Z}_p^\times, \cdot)$  ist keine Gruppe.

Es bleibt also die Gruppeneigenschaft von  $(\mathbb{Z}_p^\times, \cdot)$  im Fall einer Primzahl  $p \in \mathbb{P}$  zu verifizieren. Dazu zeigen wir für jede Restklasse  $[y] \in \mathbb{Z}_p^\times$  mit  $y \in \mathbb{Z}$  zuerst die Existenz eines multiplikativ Inversen in  $\mathbb{Z}_p$ . Wir schreiben dazu  $[y] = [x]$  mit Hilfe eines Repräsentanten  $x \in \{1, 2, 3, \dots, p-2, p-1\}$ , der sich als Rest bei der Division von  $y$  durch  $p$  ergibt (wobei der Rest 0 ausgeschlossen ist, da andernfalls  $[y] = [0]$  wäre). Wir zeigen nun indirekt, dass  $[0], [x], [2x], [3x], \dots, [(p-2)x], [(p-1)x]$ , also mit anderen Worten die Restklassen  $[nx]$  mit  $n \in \{0, 1, 2, \dots, p-2, p-1\}$ , in  $\mathbb{Z}_p$  alle verschieden sind. Andernfalls müsste nämlich  $[kx] = [\ell x]$  für  $k, \ell \in \{0, 1, 2, \dots, p-2, p-1\}$  mit  $k < \ell$  gelten, und für  $m := \ell - k \in \{1, 2, 3, \dots, p-2, p-1\}$  bekämen wir  $[mx] = [0]$ , mit anderen Worten also  $p|(mx)$ . Mit der Eindeutigkeit der Primfaktorzerlegung (deren Beweis bisher noch nicht vorgestellt wurde, aber vielleicht später noch nachgetragen wird) ergäbe sich, dass die Primzahl  $p$  ein Primfaktor von  $m$  oder einer von  $x$  sein müsste, also  $p|m$  oder  $p|x$  gälte. Beides ist aber ausgeschlossen, da  $m$  und  $x$  in  $\{0, 1, 2, \dots, p-2, p-1\}$  sind. Damit sind  $[nx]$  mit  $n \in \{0, 1, 2, \dots, p-2, p-1\}$  in der Tat  $p$  verschiedene Elemente von  $\mathbb{Z}_p$ . Da  $\mathbb{Z}_p$  genau die  $p$  Elemente  $[0], [1], [2], \dots, [p-2], [p-1]$  enthält, muss somit  $[nx] = [1]$  für ein  $n \in \{1, 2, \dots, p-2, p-1\}$  gelten (wobei  $n = 0$  wegen  $[0x] = [0] \neq [1]$  ausgeschlossen ist). Per Definition der Multiplikation gilt somit auch  $[n] \cdot [x] = [1] = [x] \cdot [n]$  für  $[n] \in \mathbb{Z}_p^\times$ , also ist  $[n]$  das gesuchte Inverse zu  $[y] = [x]$ . An dieser Stelle können wir nun mit einem kurzen allgemeinen Argument folgern, dass für beliebige  $[y], [z] \in \mathbb{Z}_p^\times$  auch  $[y] \cdot [z] \neq [0]$  ist, weshalb die Multiplikation überhaupt eine Verknüpfung auf  $\mathbb{Z}_p^\times$  ist: Wäre nämlich  $[y] \cdot [z] = [0]$ , so ergäbe sich mit dem Inversen  $[n]$  zu  $[y]$  der Widerspruch  $[z] = [n] \cdot [y] \cdot [z] = [n] \cdot [0] = [0]$ . Mit der gerade begründeten Verknüpfungseigenschaft und der Existenz der Inversen ist dann klar, dass  $(\mathbb{Z}_p^\times, \cdot)$  eine abelsche Gruppe ist (denn die restlichen benötigten Eigenschaften vererben sich von  $(\mathbb{Z}_p, \cdot)$ ).  $\square$

Anhand dieser Beispiele diskutieren wir kurz einige allgemeine Begriffe bei Gruppen:

**Definitionen.** Sei  $(G, *)$  eine Halbgruppe und  $g \in G$ .

- (I) Wir erklären „**Potenzen**“  $g^n$  von  $g$  mit Exponent  $n \in \mathbb{N}$  rekursiv durch  $g^1 := g$  und  $g^{n+1} := g * g^n$  für  $n \in \mathbb{N}$ . Hat  $(G, *)$  ein neutrales Element  $e$ , so sei zudem  $g^0 := e$ .
- (II) Gilt  $g^2 = g$ , so heißt  $g$  **idempotent**.

Man beachte, dass diese Definition prinzipiell auch auf additive Gruppen wie  $(\mathbb{Z}, +)$ ,  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$  und  $(\mathbb{Z}_n, +)$  angewandt werden kann. Dort entsprechen die „Potenzen“ allerdings Vielfachen, die man in der üblichen Schreibweise als  $nx$  beziehungsweise  $[nx]$  notiert.

**Bemerkungen und Beispiele** (zu idempotenten Elementen).

- (1) Ist  $g$  idempotent, so folgt mit vollständiger Induktion  $g^n = g$  für alle  $n \in \mathbb{N}$ .

- (2) Hat  $(G, *)$  ein neutrales Element, so ist dieses stets idempotent und weitere Idempotente, falls existent, sind nicht invertierbar (denn für jedes invertierbare Idempotent  $g \in G$  gilt  $g = g^{-1} * g^2 = g^{-1} * g = e$ ). In einer Gruppe ist daher das neutrale Element immer das einzige idempotente Element.
- (3) In den Halbgruppen  $(\mathbb{Z}, \cdot)$ ,  $(\mathbb{Q}, \cdot)$ ,  $(\mathbb{R}, \cdot)$  ist neben dem neutralen Element 1 einzig 0 idempotent. In  $(\mathbb{Z}_n, \cdot)$  sind [1] und [0] immer idempotent, für  $n = 6$  ist [3] mit  $[3] \cdot [3] = [9] = [3]$  in  $(\mathbb{Z}_6, \cdot)$  ein weiteres Beispiel eines Idempotents.

Als Nächstes führen wir eine **grundlegende Klasse von Gruppen mit besonders gutartiger und einfacher Struktur** ein:

**Definition (zyklische Gruppen).** Eine Gruppe  $(G, *)$  mit neutralem Element  $e$  heißt **zyklisch** von Ordnung  $n \in \mathbb{N}$ , wenn  $G = \{e, g, g^2, g^3, \dots, g^{n-1}\}$  für ein  $g \in G$  mit  $g^n = e \neq g^k$  für alle  $k \in \{1, 2, \dots, n-1\}$  gilt. Ein solches Element  $g$  heißt ein **Erzeuger** der Gruppe  $(G, *)$ .

**Bemerkungen** (zu zyklischen Gruppen).

- (1) Für einen Erzeuger  $g$  in einer zyklischen Gruppe  $(G, *)$  der Ordnung  $n$  sind  $e, g, g^2, g^3, \dots, g^{n-1}$  alle verschieden (weil aus  $g^\ell = g^k$  für  $0 \leq k < \ell < n$  schon  $g^{\ell-k} = e$  folgt). Insbesondere ist daher  $|G| = n$ .
- (2) Es kann in einer zyklischen Gruppe mehrere Erzeuger geben (Beispiel unten).
- (3) Zyklische Gruppen sind stets abelsch, denn in der Darstellung mit einem Erzeuger  $g$  erhält man die Kommutativität  $g^k g^\ell = g^{k+\ell} = g^\ell g^k$  für alle  $k, \ell \in \{0, 1, 2, \dots, n-1\}$ .
- (4) Man könnte dieselbe Definition auch allgemeiner für eine Halbgruppe mit neutralem Element treffen und bekäme automatisch eine Gruppe, denn das Inverse zu  $g^k$  mit  $k \in \{0, 1, 2, \dots, n-1\}$  ist  $g^{n-k}$ .

**Bemerkungen und Beispiele** (zu den zyklischen Gruppen  $(\mathbb{Z}_n, +)$  und  $(\mathbb{Z}_p^\times, \cdot)$ ).

- (1) Die Gruppe  $(\mathbb{Z}_7^\times, \cdot)$  ist zyklisch von Ordnung 6 mit genau [3] und [5] = [3]<sup>-1</sup> als Erzeugern, denn [3]<sup>1</sup> = [3], [3]<sup>2</sup> = [2], [3]<sup>3</sup> = [6], [3]<sup>4</sup> = [4], [3]<sup>5</sup> = [5], [3]<sup>6</sup> = [1] und [5]<sup>1</sup> = [5], [5]<sup>2</sup> = [4], [5]<sup>3</sup> = [6], [5]<sup>4</sup> = [2], [5]<sup>5</sup> = [3], [5]<sup>6</sup> = [1] geben jeweils alle Elemente von  $\mathbb{Z}_7^\times$ , während für die anderen vier Elemente [1]<sup>1</sup> = [2]<sup>3</sup> = [4]<sup>3</sup> = [6]<sup>2</sup> = [1] eintritt.
- (2) Die Gruppe  $(\mathbb{Z}_4, +)$  ist zyklisch von Ordnung 4 mit genau [1] und [3] als Erzeugern, denn [1·1] = [1], [2·1] = [2], [3·1] = [3], [4·1] = [0] und [1·3] = [3], [2·3] = [2], [3·3] = [1], [4·3] = [0] sind jeweils alle Elemente von  $\mathbb{Z}_4$ , während für die anderen beiden Elemente [1·0] = [2·2] = [0] eintritt.
- (3) Allgemein gilt:
- Für jedes  $n \in \mathbb{N}$  ist die **additive Gruppe**  $(\mathbb{Z}_n, +)$  des Restklassenrings  $\mathbb{Z}_n$  zyklisch von Ordnung  $n$  mit Erzeuger [1].  
(Begründung: Mit [1·1] = [1], [2·1] = [2], ..., [(n-1)·1] = [n-1], [n·1] = [0] erhalten wir alle Elemente von  $\mathbb{Z}_n$ .)
  - In  $(\mathbb{Z}_p, +)$  mit einer Primzahl  $p \in \mathbb{P}$  sind sogar alle Elemente außer [0] Erzeuger.  
(Begründung: Dies ergibt sich aus dem Beweis des letzten Satzes, in dem wir gesehen hatten, dass für jedes  $x \in \mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$  die  $p$  Restklassen [x], [2x], [3x], ..., [(p-1)x], [px] = [0] alle verschieden sind und daher die  $p$  Elemente von  $\mathbb{Z}_p$  sein müssen.)

- Für jede Primzahl  $p \in \mathbb{P}$  ist die **multiplikative Gruppe**  $(\mathbb{Z}_p^\times, \cdot)$  des Restklassenrings  $\mathbb{Z}_p$  zyklisch von Ordnung  $p-1$ .  
(Das ergibt sich mit Methoden der Algebra, die über diese Vorlesung hinausgehen.)

Als nächstes Thema behandeln wir **Permutationen**. Mit solchen formalisiert man in der Mathematik oft **Veränderungen einer Reihenfolge**. Wir erwähnen Permutationen an dieser Stelle aber vor allem wegen Permutationsgruppen wie den **symmetrischen Gruppen**  $S_n$  und den alternierenden Gruppen  $A_n$ .

**Definitionen (Permutationen, symmetrische Gruppen).**

- (I) Eine **Permutation** einer endlichen Menge  $\mathcal{X}$  ist eine bijektive Selbstabbildung von  $\mathcal{X}$ .
- (II) Für  $n \in \mathbb{N}$  schreiben wir  $S_n$  für die Menge der Permutationen von  $\{1, 2, \dots, n\}$  und nennen  $(S_n, \circ)$  die **symmetrische Gruppe** vom Grad  $n$ .
- (III) Permutationen  $\pi \in S_n$  mit  $n \in \mathbb{N}$  notieren wir manchmal in der Form

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

(mit einer weiteren Permutation  $\sigma \in S_n$ ).

**Bemerkungen** (zu Permutationen und symmetrischen Gruppen).

- (1) Man kann die Betrachtung von Permutationen **eigentlich immer auf den Modellfall** von  $S_n$  **über der Grundmenge  $\{1, 2, \dots, n\}$  reduzieren**, da jede endliche Menge  $\mathcal{X}$  durch eine Bijektion mit  $\{1, 2, \dots, n\}$  für  $n := |\mathcal{X}|$  identifiziert werden kann.
- (2) Dass  $(S_n, \circ)$  (und allgemein die Menge der Bijektionen  $\mathcal{X} \rightarrow \mathcal{X}$  mit der Komposition  $\circ$ ) tatsächlich eine Gruppe ist, haben wir früher schon beobachtet. Diese Gruppe ist *nur* für  $n \in \{1, 2\}$  (beziehungsweise  $|\mathcal{X}| \in \{1, 2\}$ ) abelsch.
- (3) Es gibt, wie wir in Mathematik 2 begründen, genau  $n!$  Permutationen einer  $n$ -elementigen Menge, es gilt also  $|S_n| = n!$ .

**Beispiel** (einer Permutation von 5 Elementen). Die Permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix} = \begin{pmatrix} 4 & 2 & 5 & 1 & 3 \\ 1 & 4 & 5 & 2 & 3 \end{pmatrix} \in S_5$$

ist die Bijektion  $\pi: \{1, 2, 3, 4, 5\} \rightarrow \{1, 2, 3, 4, 5\}$  mit  $1 \xrightarrow{\pi} 2$ ,  $2 \xrightarrow{\pi} 4$ ,  $3 \xrightarrow{\pi} 3$ ,  $4 \xrightarrow{\pi} 1$ ,  $5 \xrightarrow{\pi} 5$ .

**Definitionen (Transpositionen, Zykel).** Sei  $\pi$  eine Permutation einer endlichen Menge  $\mathcal{X}$ .

- (I) Wir nennen  $\pi$  die **Transposition** von  $a, b \in \mathcal{X}$  mit  $a \neq b$  (in  $\mathcal{X}$ ), wenn  $\pi(a) = b$ ,  $\pi(b) = a$  und  $\pi(x) = x$  für alle  $x \in \mathcal{X} \setminus \{a, b\}$  gelten.

- (II) Wir nennen  $\pi$  einen **Zykel** der Länge  $\ell \in \mathbb{N}$  oder einen  $\ell$ -Zykel (in  $\mathcal{X}$ ), wenn es ein  $a \in \mathcal{X}$  mit  $\pi^\ell(a) = a \neq \pi^k(a)$  für alle  $k \in \{1, 2, \dots, \ell-1\}$  und  $\pi(x) = x$  für alle  $x \in \mathcal{X} \setminus \{a, \pi(a), \pi^2(a), \dots, \pi^{\ell-1}(a)\}$  gibt. Für solche Zykel wird manchmal in Zykelschreibweise  $\pi = (a \ \pi(a) \ \pi^2(a) \ \dots \ \pi^{\ell-1}(a))$  notiert.

**Bemerkungen** (zu Transpositionen und Zykeln).

- (1) Ein Zykel der Länge 1 ist die Identität, ein Zykel der Länge 2 ist eine Transposition.
- (2) Eine Transposition  $\pi$  ist selbstinvers. Für einen Zykel  $\pi$  der Länge  $\ell$  in  $\mathcal{X}$  gilt  $\pi^\ell = \text{id}_{\mathcal{X}}$ .

**Beispiele** (der **symmetrischen Gruppen vom Grad 2 und 3**). Wir betrachten folgende noch gut überschaubare Beispiele zwischen  $S_1 = \{\text{id}\}$  und  $S_4$  mit  $|S_4| = 4! = 24$ :

- (1) Die  $2! = 2$  Elemente der **symmetrischen Gruppe**  $(S_2, \circ)$  sind die Identität  $\text{id}$  und eine Transposition  $\tau$  mit den Darstellungen

$$\text{id} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \quad \text{und} \quad \tau = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

Offensichtlich ist  $\tau$  selbstinvers und  $(S_2, \circ)$  zyklisch von Ordnung 2. In Zykelschreibweise kann man  $\tau = (1 \ 2) = (2 \ 1)$  schreiben.

- (2) Die  $3! = 6$  Elemente der **symmetrischen Gruppe**  $(S_3, \circ)$  sind die Identität  $\text{id}$ , drei Transpositionen  $\tau_1, \tau_2, \tau_3$  und zwei 3-Zykel  $\sigma_1, \sigma_2$  mit den Darstellungen

$$\begin{aligned} \text{id} &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, & \tau_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, & \tau_2 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \\ \tau_3 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, & \sigma_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, & \sigma_2 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}. \end{aligned}$$

Bezüglich der Komposition, der Verknüpfung der Gruppe, hängen die Elemente zum Beispiel durch  $\sigma_1 = \tau_2 \circ \tau_1 = \tau_3 \circ \tau_2 = \tau_1 \circ \tau_3 = \sigma_2^2 = \sigma_2^{-1}$  zusammen. In Zykelschreibweise kann man z.B.  $\tau_1 = (1 \ 2) = (2 \ 1)$ ,  $\tau_2 = (1 \ 3) = (3 \ 1)$  und  $\sigma_1 = (1 \ 2 \ 3) = (2 \ 3 \ 1) = (3 \ 1 \ 2)$  schreiben.

Zur Einführung einer weiteren Gruppe von Permutationen und für wichtige Anwendungen später in der linearen Algebra brauchen wir:

**Satz** (zur Darstellbarkeit von Permutationen durch Transpositionen). *Sei  $\pi$  eine Permutation einer endlichen Menge  $\mathcal{X}$ .*

- (I) *Dann kann  $\pi$  als Komposition  $\pi = \tau_1 \circ \tau_2 \circ \dots \circ \tau_{m-1} \circ \tau_m$  einer endlichen Zahl  $m \in \mathbb{N}_0$  von Transpositionen  $\tau_1, \tau_2, \dots, \tau_{m-1}, \tau_m$  in  $\mathcal{X}$  geschrieben werden.*
- (II) *Die Parität (gerade oder ungerade) der Zahl  $m$  in (I) oder mit anderen Worten die Restklasse  $[m]_{\mathbb{Z}_2} \in \mathbb{Z}_2$  ist durch  $\pi$  eindeutig bestimmt.*

**Definitionen** (Parität/Vorzeichen von Permutationen, alternierende Gruppen).

- (I) *Wir nennen eine Permutation  $\pi$  einer endlichen Menge  $\mathcal{X}$  eine **gerade beziehungsweise ungerade Permutation**, wenn die Parität von  $m$  in Teil (II) des Satzes gerade beziehungsweise ungerade ist. Das **Vorzeichen**  $\text{sgn}(\pi) \in \{-1, 1\}$  einer Permutation  $\pi$  erklären wir für gerade Permutationen  $\pi$  zu 1, für ungerade Permutationen  $\pi$  zu  $-1$ .*

(II) Für  $n \in \mathbb{N}$  setzen wir

$$A_n := \{\pi \in S_n \mid \pi \text{ ist gerade}\} = \{\pi \in S_n \mid \operatorname{sgn}(\pi) = 1\},$$

und nennen  $(A_n, \circ)$  die **alternierende Gruppe vom Grad  $n$** .

**Bemerkungen** (zum Vorzeichen von Permutationen und der alternierenden Gruppe).

- (1) Für Permutationen  $\pi$  und  $\sigma$  von  $\mathcal{X}$  gelten  $\operatorname{sgn}(\pi^{-1}) = \operatorname{sgn}(\pi)$  und  $\operatorname{sgn}(\sigma \circ \pi) = \operatorname{sgn}(\sigma) \operatorname{sgn}(\pi)$ .  
(Begründung für letzteres: Sind  $\sigma$  bzw.  $\pi$  Kompositionen von  $\ell$  bzw.  $m$  Transpositionen, so ist  $\sigma \circ \pi$  Komposition von  $\ell+m$  Transpositionen. Im Fall  $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\pi)$  haben  $\ell, m$  gleiche Parität,  $\ell+m$  ist gerade, und es gilt  $\operatorname{sgn}(\sigma \circ \pi) = 1 = \operatorname{sgn}(\sigma) \operatorname{sgn}(\pi)$ . Im Fall  $\operatorname{sgn}(\sigma) = -\operatorname{sgn}(\pi)$  dagegen haben  $\ell, m$  verschiedene Parität,  $\ell+m$  ist ungerade, und es gilt  $\operatorname{sgn}(\sigma \circ \pi) = -1 = \operatorname{sgn}(\sigma) \operatorname{sgn}(\pi)$ .)
- (2) Insbesondere folgt aus Bemerkung (1), dass für  $\pi, \sigma \in A_n$  auch  $\pi^{-1} \in A_n$  und  $\sigma \circ \pi \in A_n$  gelten. Erst dies (zusammen mit früheren Beobachtungen) stellt sicher, dass  $(A_n, \circ)$  in der Tat eine Gruppe ist. Die Gruppe  $(A_n, \circ)$  ist *nur* für  $n \in \{1, 2, 3\}$  abelsch.
- (3) Für  $n \in \mathbb{N} \setminus \{1\}$  enthält die Teilmenge  $A_n$  von  $S_n$  die Hälfte der Permutationen aus  $S_n$ , es gilt also  $|A_n| = \frac{1}{2}|S_n| = \frac{n!}{2}$ .  
(Begründung: Sei  $\tau \in S_n$  eine beliebige Transposition, die als solche insbesondere selbstinvers mit  $\operatorname{sgn}(\tau) = -1$  ist. Mit der vorausgehenden Bemerkung (1) und den Gruppeneigenschaften von  $(S_n, \circ)$  folgt, dass  $A_n \rightarrow S_n \setminus A_n, \pi \mapsto \tau \circ \pi$  eine wohldefinierte Bijektion von  $A_n$  nach  $S_n \setminus A_n$  ist. Damit gilt  $|A_n| = |S_n \setminus A_n| = |S_n| - |A_n|$ , und durch Auflösen ergibt sich  $|A_n| = \frac{1}{2}|S_n|$ .)

**Beispiele** (der **alternierenden Gruppen vom Grad 3 und 4**). Wir betrachten folgende noch überschaubare Beispiele zwischen  $A_1 = \{\operatorname{id}\}$ ,  $A_2 = \{\operatorname{id}\}$  und  $A_5$  mit  $|A_5| = \frac{5!}{2} = 60$ :

- (1) Die  $\frac{3!}{2} = 3$  Elemente der **alternierenden Gruppe  $(A_3, \circ)$**  sind die Identität  $\operatorname{id}$  und die beiden als Elemente von  $(S_3, \circ)$  schon betrachteten 3-Zykel  $\sigma_1$  und  $\sigma_2$ . Es gelten  $\sigma_1^2 = \sigma_2$ ,  $\sigma_2^2 = \sigma_1$  und  $\sigma_1 \circ \sigma_2 = \operatorname{id} = \sigma_2 \circ \sigma_1$ . Insbesondere ist  $(A_3, \circ)$  zyklisch von Ordnung 3.
- (2) Die  $\frac{4!}{2} = 12$  Elemente der **alternierenden Gruppe  $(A_4, \circ)$**  sind die Identität  $\operatorname{id}$ , acht 3-Zykel  $\eta_1, \eta_2, \eta_3, \eta_4, \eta_5, \eta_6, \eta_7, \eta_8$  und drei Kompositionen  $\vartheta_1, \vartheta_2, \vartheta_3$  von je zwei „getrennten“ Transpositionen mit den Darstellungen

$$\begin{aligned} \operatorname{id} &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, & \eta_1 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, & \eta_2 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, & \eta_3 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \\ \eta_4 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}, & \eta_5 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}, & \eta_6 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}, & \eta_7 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}, \\ \eta_8 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}, & \vartheta_1 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, & \vartheta_2 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, & \vartheta_3 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}. \end{aligned}$$

Dass  $(A_4, \circ)$  nicht abelsch ist, sieht man beispielsweise an  $\eta_1 \circ \vartheta_1 = \eta_5$  und  $\vartheta_1 \circ \eta_1 = \eta_8$ .

Es verbleibt, den Beweis des letzten Satzes durchzuführen:

*Beweis von Teil (I) des Satzes.* Wir argumentieren per vollständiger Induktion nach  $|\mathcal{X}| \in \mathbb{N}_0$ :

Den Induktionsanfang für  $|\mathcal{X}| = 0$  erledigt die Beobachtung, dass dann  $\mathcal{X} = \emptyset$  ist, dass die (formal) bijektive leere Abbildung die einzige Abbildung  $\emptyset \rightarrow \emptyset$  und die einzige Permutation von  $\emptyset$  ist, und, dass die leere Abbildung (formal) die Komposition von 0 Transpositionen ist.

Für den Induktionsschluss von  $|\mathcal{X}|-1$  zu  $|\mathcal{X}|$  sei  $|\mathcal{X}| \in \mathbb{N}$  und  $\pi$  Permutation von  $\mathcal{X}$ . Wir wählen  $x_1 \in \mathcal{X}$ . Im Fall  $\pi(x_1) = x_1$  sei  $\tau_1 := \text{id}_{\mathcal{X}}$ , im Fall  $\pi(x_1) \neq x_1$  sei  $\tau_1 := (x_1 \pi(x_1))$  die Transposition von  $\mathcal{X}$  mit  $\tau_1(x_1) = \pi(x_1)$  und  $\tau_1(\pi(x_1)) = x_1$ . So oder so folgt  $(\tau_1 \circ \pi)(x_1) = x_1$ , und wegen Bijektivität erhalten wir  $(\tau_1 \circ \pi)(x) \in \mathcal{X} \setminus \{x_1\}$  für alle  $x \in \mathcal{X} \setminus \{x_1\}$ . Wir können daher die Permutation  $\tilde{\pi}$  von  $\mathcal{X} \setminus \{x_1\}$  mit  $\tilde{\pi}(x) = (\tau_1 \circ \pi)(x)$  für alle  $x \in \mathcal{X} \setminus \{x_1\}$  bilden und  $\tilde{\pi}$  nach Induktionsannahme für ein  $m \in \mathbb{N}$  als Komposition von  $m-1$  Transpositionen schreiben. Wir erweitern diese zu  $m-1$  Transpositionen  $\tau_2, \tau_3, \dots, \tau_m$  auf  $\mathcal{X}$  mit  $\tau_2(x_1) = \tau_3(x_1) = \dots = \tau_m(x_1) = x_1$  und bekommen  $\tau_1 \circ \pi = \tau_2 \circ \tau_3 \circ \dots \circ \tau_{m-1} \circ \tau_m$ . Da  $\tau_1$  selbstinvers ist (Eigenschaft von  $\text{id}_{\mathcal{X}}$  und jeder Transposition), erhalten wir  $\pi = \tau_1^{-1} \circ \tau_2 \circ \tau_3 \circ \dots \circ \tau_{m-1} \circ \tau_m = \tau_1 \circ \tau_2 \circ \tau_3 \circ \dots \circ \tau_{m-1} \circ \tau_m$ . Damit ist  $\pi$  die Komposition der Transpositionen  $\tau_1, \tau_2, \dots, \tau_{m-1}, \tau_m$  (im Fall  $\pi(x_1) = x_1$  nach Weglassen von  $\tau_1 = \text{id}_{\mathcal{X}}$ ), und die Induktionsbehauptung ist gezeigt.  $\square$

*Beweis von Teil (II) des Satzes.* Wir nehmen der Einfachheit halber  $\mathcal{X} = \{1, 2, \dots, n\}$  an (können aber für allgemeines  $\mathcal{X}$  eine beliebige Totalordnung auf  $\mathcal{X}$  einführen und damit analog argumentieren). Wir betrachten die Menge

$$\text{FS}(\pi) := \{(i, j) \in \{1, 2, \dots, n\}^2 \mid i < j, \pi(i) > \pi(j)\}$$

der sogenannten Fehlstände oder Inversionen eine Permutation  $\pi \in S_n$  und argumentieren mit der **Zahl der Fehlstände/Inversionen**  $|\text{FS}(\pi)| \in \mathbb{N}_0$ . Für diesen Beweis entscheidend ist nun:

**Behauptung:** Für eine beliebige Permutation  $\pi \in S_n$  und eine Transposition  $\tau \in S_n$  haben die Zahlen der Fehlstände  $|\text{FS}(\tau \circ \pi)|$  und  $|\text{FS}(\pi)|$  unterschiedliche Parität.

Zum Nachweis dieser Behauptung benutzen wir zunächst, dass die Transposition  $\tau$  per Definition die Form  $\tau = (k \ell)$  mit  $k, \ell \in \{1, 2, \dots, n\}$ ,  $k \neq \ell$ , hat. Da  $k$  und  $\ell$  vertauscht werden können, behandeln wir *ohne Einschränkung* (typische Formulierung an solch einer Stelle!) nur den Fall  $k < \ell$ . Für ein Paar  $(i, j) \in \{1, 2, \dots, n\}^2$  mit  $i < j$  und  $\{\pi(i), \pi(j)\} =: \{x, y\}$  mit  $x < y$  unterscheiden wir folgende Fälle:

- (a) Fall  $x, y \notin \{k, \ell\}$ : Dann ist  $\tau(x) = x$ ,  $\tau(y) = y$ , also  $\tau(\pi(i)) = \pi(i)$ ,  $\tau(\pi(j)) = \pi(j)$ , und es folgt  $(i, j) \in \text{FS}(\tau \circ \pi) \iff (i, j) \in \text{FS}(\pi)$ .
- (b) Fall  $x < k$ ,  $y \in \{k, \ell\}$  sowie Fall  $x \in \{k, \ell\}$ ,  $\ell < y$ : Neben  $x < y$  gilt dann  $\tau(x) < \tau(y)$ , es folgen  $\tau(\pi(i)) > \tau(\pi(j)) \iff \pi(i) > \pi(j)$  und  $(i, j) \in \text{FS}(\tau \circ \pi) \iff (i, j) \in \text{FS}(\pi)$ .
- (c) Fall  $x = k < y < \ell$  sowie Fall  $k < x < \ell = y$ : Neben  $x < y$  gilt dann  $\tau(x) > \tau(y)$ , es folgen  $\tau(\pi(i)) > \tau(\pi(j)) \iff \pi(i) < \pi(j)$  und  $(i, j) \in \text{FS}(\tau \circ \pi) \iff (i, j) \notin \text{FS}(\pi)$ .
- (d) Fall  $x = k$ ,  $y = \ell$ : Dann ist  $\tau(x) = y$ ,  $\tau(y) = x$ , also  $\tau(\pi(i)) = \pi(j)$ ,  $\tau(\pi(j)) = \pi(i)$ , und es folgt  $(i, j) \in \text{FS}(\tau \circ \pi) \iff (i, j) \notin \text{FS}(\pi)$ .

In den Fällen (a), (b) entnehmen wir, dass Fehlstände  $(i, j)$  von  $\pi$  bei  $\tau \circ \pi$  weiterbestehen. In den Fällen (c), (d) treten bei  $\tau \circ \pi$  gegenüber  $\pi$  Fehlstände hinzu oder fallen weg. Die Situation (c) tritt dabei (da es  $\ell - k - 1$  natürliche Zahlen zwischen  $k$  und  $\ell$  gibt) für genau  $2(\ell - k - 1)$  Paare  $(x, y) \in \{1, 2, \dots, n\}^2$  mit  $x < y$  und dementsprechend auch für  $2(\ell - k - 1)$  Paare  $(i, j) \in \{1, 2, \dots, n\}^2$  mit  $i < j$  ein. Die Situation (d) liegt für genau ein Paar  $(i, j)$  mit  $i < j$  (nämlich das mit  $\{\pi(i), \pi(j)\} = \{k, \ell\}$ ) vor. Insgesamt ist damit  $|\text{FS}(\tau \circ \pi) \Delta \text{FS}(\pi)| = 2(\ell - k - 1) + 1$  ungerade, wegen  $|A| + |B| = |A \Delta B| + 2|A \cap B|$  ist auch  $|\text{FS}(\tau \circ \pi)| + |\text{FS}(\pi)|$  ungerade, also muss von  $|\text{FS}(\tau \circ \pi)|$  und  $|\text{FS}(\pi)|$  eins gerade, eins ungerade sein. Dies zeigt die obige Behauptung.

Da  $|\text{FS}(\text{id})| = 0$  für die Identität  $\text{id} \in S_n$  gerade ist, folgt für Transpositionen  $\tau_1, \tau_2, \tau_3 \in S_n$  iterativ, dass  $|\text{FS}(\tau_1)|$  ungerade ist,  $|\text{FS}(\tau_2 \circ \tau_1)|$  gerade ist,  $|\text{FS}(\tau_3 \circ \tau_2 \circ \tau_1)|$  ungerade ist, und so weiter. Tatsächlich ergibt vollständige Induktion, dass die Komposition einer geraden beziehungsweise ungeraden Anzahl von Transpositionen stets gerades beziehungsweise ungerades Vorzeichen hat. Ist für  $\pi \in S_n$  also  $|\text{FS}(\pi)|$  gerade, so kann  $\pi = \tau_1 \circ \tau_2 \circ \dots \circ \tau_{m-1} \circ \tau_m$  nur für gerades  $m \in \mathbb{N}_0$  gelten. Ist  $|\text{FS}(\pi)|$  ungerade, so kann selbiges nur für ungerades  $m \in \mathbb{N}_0$  gelten. Dies zeigt die behauptete Eindeutigkeit der Parität von  $m$ .  $\square$

## 3.2 Ringe und Körper

Nachdem wir Gruppen als algebraische Strukturen mit *einer* Verknüpfung kennengelernt haben, kommen wir nun zu **algebraischen Strukturen mit zwei Verknüpfungen**, die in den wichtigsten Modellfällen durch **Addition und Multiplikation** gegeben sind.

**Definitionen (Ringe).**

(I) Ein **Ring** ist ein Tripel  $(R, +, \cdot)$  aus einer Menge  $R$  und Verknüpfungen  $+$  und  $\cdot$  auf  $R$ , so dass ...

- $(R, +)$  eine abelsche Gruppe ist,
- $(R, \cdot)$  eine Halbgruppe mit neutralem Element ist
- und folgende **Distributivgesetze** gelten:

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z), \quad (x + y) \cdot z = (x \cdot z) + (y \cdot z) \quad \text{für alle } x, y, z \in R.$$

(II) Bezüglich der **Addition**  $+$  beziehungsweise in der **additiven Gruppe**  $(R, +)$  eines Rings  $(R, +, \cdot)$  bezeichnet man das neutrale Element als die **Null**  $0$  oder das **Nullelement**  $0_R$  von  $(R, +, \cdot)$  und das Inverse zu  $x \in R$  als das **additiv Inverse**  $-x \in R$  zu  $x$ .

(III) Bezüglich der **Multiplikation**  $\cdot$  beziehungsweise in der **multiplikativen Gruppe**  $(R, \cdot)$  eines Rings  $(R, +, \cdot)$  bezeichnet man das neutrale Element als die **Eins**  $1$  oder das **Eins-element**  $1_R$  von  $(R, +, \cdot)$ , ein invertierbares Element  $x \in R$  (was bei Ringen sowieso immer als multiplikativ invertierbar zu verstehen ist) als eine **Einheit** von  $R$  und sein Inverses als das **multiplikativ Inverse**  $x^{-1} \in R$  zu  $x$ .

(IV) Ein Ring heißt **kommutativ**, wenn neben seiner additiven Gruppe  $(R, +)$  auch seine multiplikative Halbgruppe  $(R, \cdot)$  kommutativ ist.

**Notationen & Folgerungen (zum Rechnen in einem Ring).** Sei  $(R, +, \cdot)$  ein Ring.

(1) Wir verwenden beim Rechnen mit Elementen von  $R$  **dieselben Konventionen zur Notationsvereinfachung wie bei Zahlen**. Konkret gehören dazu das **Weglassen des Multiplikationspunkts** ( $xy := x \cdot y$  für  $x, y \in R$ ; sofern keine Mehrdeutigkeit entsteht), die Einführung der **Subtraktion** ( $x - y := x + (-y)$  für  $x, y \in R$ ), die Konvention **Punkt-vor Strich-Rechnung** (derzufolge etwa die Klammern auf den rechten Seiten der Distributivgesetze entfallen können) und die üblichen **Konventionen zur Einsparung von** aufgrund Assoziativität unnötigen **Klammern**. Zudem verwendet man für  $x \in R$ ,  $n \in \mathbb{N}_0$  die Notation  $x^n$ , für invertierbares  $x$  auch  $x^{-n} := (x^{-1})^n$ , für **Potenzen** der multiplikativen Halbgruppe.

(2) Ist  $(R, +, \cdot)$  ein Ring, so gelten für alle  $x, y \in R$  die Regeln

$$0+x = x = x+0, \quad 1x = x = x1, \quad 0x = 0 = x0, \quad (-x)y = -(xy) = x(-y).$$

Insbesondere ist das Nullelement  $0$  nicht invertierbar (außer im Nullring mit  $1 = 0$ ; dazu siehe unten), und wir können in Zukunft ohne Mehrdeutigkeit  $-xy$  notieren.

(Begründungen: Die ersten beiden Regeln gelten per Definition des Null- und des Einselements. Die dritte Regel ergibt sich durch  $0x = 0x+x-x = (0+1)x-x = 1x-x = x-x = 0$  und eine analoge Rechnung. Zum Nachweis der vierten Regel reichen wegen der Kommutativität der Addition die Rechnungen  $xy+(-x)y = (x-x)y = 0y = 0$  und  $xy+x(-y) = x(y-y) = x0 = 0$ .)

**Beispiele (von Ringen).** Aus den in Abschnitt 3.1 betrachteten Beispielen von additiven und multiplikativen (Halb-)Gruppen ergeben sich nach Verifikation der Distributivgesetze Beispiele von Ringen:

(0) Der **Nullring** ist der (bis auf Umbenennung des Elements eindeutige) Ring  $(\{0\}, +, \cdot)$  mit nur einem Element  $1=0$ . Dies ist der einzige Ring mit  $1 = 0$  (denn aus  $1 = 0$  und der vorausgehenden Folgerung (2) ergibt sich  $x = 1x = 0x = 0$  für jedes Ringelement  $x$ ).

(1) Die **ganzen Zahlen**  $(\mathbb{Z}, +, \cdot)$ , die **rationalen Zahlen**  $(\mathbb{Q}, +, \cdot)$ , die **reellen Zahlen**  $(\mathbb{R}, +, \cdot)$  und die **Restklassenringe**  $(\mathbb{Z}_n, +, \cdot)$  mit  $n \in \mathbb{N}$  sind **kommutative Ringe**.

(2) **Produkt-Ringe:** Für jedes  $n \in \mathbb{N}$  und jeden (kommutativen) Ring  $(R, +, \cdot)$  ist auch  $(R^n, +, \cdot)$  mit den komponentenweisen Verknüpfungen  $+$  und  $\cdot$  ein (kommutativer) Ring mit Nullelement  $0_{R^n} = (0_R, 0_R, \dots, 0_R)$  und Einselement  $1_{R^n} = (1_R, 1_R, \dots, 1_R)$ .

Allgemeiner ist für jedes  $n \in \mathbb{N}$  und (kommutative) Ringe  $(R_1, +, \cdot), (R_2, +, \cdot), \dots, (R_n, +, \cdot)$  auch  $(R_1 \times R_2 \times \dots \times R_n, +, \cdot)$  mit den komponentenweisen Verknüpfungen ein (kommutativer) Ring.

(3) **Abbildungs-Ringe:** Für jede Menge  $\mathcal{X}$  und jeden (kommutativen) Ring  $(R, +, \cdot)$  ist auch  $(\text{Abb}(\mathcal{X}, R), +, \cdot)$  mit den punktweisen Verknüpfungen  $+$  und  $\cdot$  ein (kommutativer) Ring.

Dagegen ergibt  $(\text{Abb}(R), +, \circ)$  mit der Komposition  $\circ$  für  $R \neq \{0_R\}$  *keinen* Ring: Zwar ist  $(\text{Abb}(R), +)$  abelsche Gruppe,  $(\text{Abb}(R), \circ)$  ist Halbgruppe mit neutralem Element, und das „rechte“ Distributivgesetz  $(f+g) \circ h = f \circ h + g \circ h$  gilt für alle  $f, g, h \in \text{Abb}(R)$ . Das „linke“ Distributivgesetz  $f \circ (g+h) = f \circ g + f \circ h$  gilt aber zum Beispiel für  $f \equiv 1_R$ , nicht, da dann  $f \circ (g+h) \equiv 1_R$  verschieden von  $f \circ g + f \circ h \equiv 1_R + 1_R$  ist (denn  $R \neq \{0_R\}$  bedeutet  $1_R \neq 1_R + 1_R$ ).

(4) **Mengen-Ringe:** Für jede Menge  $\mathcal{X}$  ist  $(\mathcal{P}(\mathcal{X}), \Delta, \cap)$  ein kommutativer Ring (mit Nullelement  $\emptyset$ , Einselement  $\mathcal{X}$  und  $M \Delta M = \emptyset$  für alle  $M \in \mathcal{P}(\mathcal{X})$ ).

(5) Als **weitere wichtige Beispiele** von Ringen lernen wir später in diesem Abschnitt **Polynom-Ringe** und als typische nicht-kommutative Ringe in Abschnitt 3.3 **Endomorphismenringe** und in Mathematik 2 **Matrizen-Ringe** kennen.

**Bemerkungen (zu Ringen).**

(1) **In einem Ring**  $(R, +, \cdot)$  kann man sehr weitgehend **wie im Bereich  $\mathbb{Z}$  der ganzen Zahlen rechnen**. Insbesondere können für eine Indexmenge  $I$  und  $a_i \in R$  das Summenzeichen  $\sum_{i \in I} a_i$  und im kommutativen Fall auch das Produktzeichen  $\prod_{i \in I} a_i$  wie in Abschnitt 2.2 sinnvoll erklärt werden.

- (2) **In einem Ring  $(R, +, \cdot)$  besitzen neben 0 und 1 alle ganzen Zahlen Entsprechungen**, die man als  $2_R := 1_R + 1_R \in R$ ,  $3_R := 2_R + 1_R \in R$  und allgemein als  $n_R := \sum_{i=1}^n 1_R \in R$ ,  $(-n)_R := -(n_R) \in R$  für  $n \in \mathbb{N}_0$  erhält.

Sind die Elemente  $z_R$  mit  $z \in \mathbb{Z}$  alle voneinander verschieden, so kann man  $z \in \mathbb{Z}$  mit  $z_R \in R$  identifizieren und so  $\mathbb{Z}$  als **Teilmenge von  $R$**  auffassen. Man spricht in diesem Fall<sup>2</sup> von einem **Ring der Charakteristik 0**. Zum Beispiel haben  $(\mathbb{B}, +, \cdot)$ ,  $(\mathbb{B}^n, +, \cdot)$ ,  $(\text{Abb}(\mathcal{X}, \mathbb{B}), +, \cdot)$  mit  $\mathbb{B} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}\}$  Charakteristik 0.

Sind andernfalls die  $z_R$  mit  $z \in \mathbb{Z}$  *nicht* alle verschieden, so gibt es ein kleinstes  $n \in \mathbb{N}$  mit  $n_R = 0_R$ , man kann  $[z]_{\mathbb{Z}_n} \in \mathbb{Z}_n$  mit  $z_R \in R$  identifizieren und so  $\mathbb{Z}_n$  als **Teilmenge von  $R$**  auffassen. In diesem Fall spricht man von einem **Ring der (endlichen) Charakteristik  $n \in \mathbb{N}$** . Zum Beispiel haben  $(\mathbb{Z}_n, +, \cdot)$ ,  $(\mathbb{Z}_n^k, +, \cdot)$ ,  $(\text{Abb}(\mathcal{X}, \mathbb{Z}_n), +, \cdot)$  Charakteristik  $n$  und  $(\mathcal{P}(\mathcal{X}), \Delta, \cap)$  mit  $\mathcal{X} \neq \emptyset$  Charakteristik 2. (Charakteristik 1 hat übrigens nur der Nullring.)

- (3) Manche Autoren fordern bei Definition eines Rings nicht allgemein, dass ein neutrales Element 1 der multiplikativen Halbgruppe existieren muss, und bezeichnen einen Ring, bei dem dies doch der Fall ist, explizit als Ring mit Eins oder unitären Ring. Wir bleiben aber bei der obigen Konvention, gemäß der jeder Ring ein Ring mit Eins ist.

**Definitionen (Teiler, Nullteiler, Integritätsringe).** Sei  $(R, +, \cdot)$  ein **kommutativer Ring**.

- (I) Wir nennen  $y \in R$  einen **Teiler** von  $z \in R$  (in  $R$ ) und notieren  $y|z$  (in  $R$ ), wenn ein  $x \in R$  mit  $xy = z$  existiert.
- (II) Wir nennen  $y \in R \setminus \{0\}$  einen **Nullteiler** (in  $R$ ), wenn ein  $x \in R \setminus \{0\}$  mit  $xy = 0$  existiert. Gibt es in  $R \setminus \{0\}$  keinen Nullteiler, so nennen wir  $(R, +, \cdot)$  **nullteilerfrei**.
- (III) Ist  $(R, +, \cdot)$  nullteilerfrei mit  $R \neq \{0\}$ , so sprechen wir von einem **Integritätsring** oder **Integritätsbereich**.

**Bemerkung (zu Nullteilern).** In einem kommutativen Ring  $(R, +, \cdot)$  ist wegen  $0y = 0$  jedes Element  $y \in R$  ein Teiler von 0. Dies macht ein  $y \in R$  mit  $y \neq 0$  aber noch nicht unbedingt zum Nullteiler, denn dafür ist  $xy = 0$  eben auch mit  $x \neq 0$  erforderlich.

**Beispiele (von Integritätsringen).**

- (1) Die **ganzen Zahlen**  $(\mathbb{Z}, +, \cdot)$ , die **rationalen Zahlen**  $(\mathbb{Q}, +, \cdot)$  und die **reellen Zahlen**  $(\mathbb{R}, +, \cdot)$  sind **Integritätsringe**.  
Dagegen ist  $(\mathbb{B}^2, +, \cdot)$  mit  $\mathbb{B} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}\}$  und den komponentenweisen Verknüpfungen *kein* Integritätsring, denn dort gilt  $(1, 0) \cdot (0, 1) = (0, 0) = 0_{\mathbb{B}^2}$ . Aus dem gleichen Grund sind auch  $(\mathbb{B}^n, +, \cdot)$  mit  $n \geq 2$  und  $(\text{Abb}(\mathcal{X}, \mathbb{B}), +, \cdot)$  mit  $|\mathcal{X}| \geq 2$  *keine* Integritätsringe.
- (2) Der **Restklassenring**  $(\mathbb{Z}_n, +, \cdot)$  mit  $n \in \mathbb{N}$  ist genau dann ein Integritätsring, wenn  $n$  eine Primzahl ist. Die folgt aus den Resultaten des Abschnitts 3.1 zur multiplikativen Gruppe  $(\mathbb{Z}_n^\times, \cdot)$  (und wird auch aus dem Folgenden noch klarer). Ist  $n \in \mathbb{N} \setminus \{1\}$  *keine* Primzahl, also  $n = ab$  mit  $a, b \in \{2, 3, \dots, n-1\}$ , so sieht man dies auch sofort an  $[a]_{\mathbb{Z}_n} [b]_{\mathbb{Z}_n} = [n]_{\mathbb{Z}_n} = [0]_{\mathbb{Z}_n}$ , womit  $[a]_{\mathbb{Z}_n}$  und  $[b]_{\mathbb{Z}_n}$  Nullteiler in  $\mathbb{Z}_n$  sind.

<sup>2</sup>Gleichbedeutend mit „Charakteristik 0“ wird in der Literatur gelegentlich auch „Charakteristik  $\infty$ “ benutzt. Unter „endlicher Charakteristik“ versteht man aber so oder so nur Charakteristiken aus  $\mathbb{N}$ , also *nicht* 0 beziehungsweise  $\infty$ .

**Bemerkungen** (zu Nullteilerfreiheit/Integritätsringen).

- (1) Dass ein kommutativer Ring
- $(R, +, \cdot)$
- nullteilerfrei ist, bedeutet, dass die Implikation

$$xy = 0 \implies x = 0 \vee y = 0 \quad \text{bzw. äquivalent} \quad x \neq 0 \wedge y \neq 0 \implies xy \neq 0$$

für alle  $x, y \in R$  gilt.

- (2) Als vielleicht wichtigste Konsequenz gilt in nullteilerfreien Ringen und Integritätsringen
- $(R, +, \cdot)$
- die
- Kürzungsregel**

$$xz = yz \implies x = y \quad \text{für alle } x, y \in R, z \in R \setminus \{0\}$$

(auch dann, wenn  $z$  nicht invertierbar ist!). Um die Kürzungsregel einzusehen, schreibt man  $xz = yz$  äquivalent als  $(x-y)z = 0$  und benutzt dann die vorige Bemerkung (1).

- (3) Da man für einen Integritätsring
- $(R, +, \cdot)$
- (wie für jeden Ring) immer
- $\mathbb{Z}$
- oder
- $\mathbb{Z}_n$
- als Teilmenge von
- $R$
- auffassen kann und
- $(\mathbb{Z}_n, +, \cdot)$
- aber nur für Primzahlen
- $n$
- Integritätsring ist, stellt sich heraus, dass die Charakteristik eines Integritätsrings stets Null oder eine (endliche) Primzahl ist.

**Definitionen** (Schiefkörper und Körper).

- (I) Ein **Schiefkörper** oder **Divisionsring** ist ein Ring  $(K, +, \cdot)$  mit  $K \neq \{0\}$ , in dem jedes Element von  $K \setminus \{0\}$  multiplikativ invertierbar ist, mit anderen Worten ein Ring  $(K, +, \cdot)$ , für den  $(K \setminus \{0\}, \cdot)$  eine Gruppe ist.
- (II) Ein **Körper** ist ein kommutativer Schiefkörper, mit anderen Worten ein Ring  $(K, +, \cdot)$ , für den  $(K \setminus \{0\}, \cdot)$  eine abelsche Gruppe ist.

**Beispiele** (von (Schief-)Körpern).

- (1) Die
- rationalen Zahlen**
- $(\mathbb{Q}, +, \cdot)$
- und die
- reellen Zahlen**
- $(\mathbb{R}, +, \cdot)$
- sind
- Körper**
- .

Aus dem gleichen Grund wie bei Integritätsringen sind aber  $(\mathbb{Q}^n, +, \cdot)$ ,  $(\mathbb{R}^n, +, \cdot)$  mit  $n \geq 2$  und  $(\text{Abb}(\mathcal{X}, \mathbb{Q}), +, \cdot)$ ,  $(\text{Abb}(\mathcal{X}, \mathbb{R}), +, \cdot)$  mit  $|\mathcal{X}| \geq 2$  keine Körper.

- (2) Der kommutative
- Restklassenring**
- $(\mathbb{Z}_n, +, \cdot)$
- mit
- $n \in \mathbb{N}$
- ist genau dann ein (Schief-)Körper, wenn
- $n$
- eine Primzahl ist. Den Beweis hierfür haben wir schon in Abschnitt 3.1 gesehen, als dort gezeigt wurde, dass
- $(\mathbb{Z}_n \setminus \{0\}, \cdot)$
- genau für Primzahlen
- $n \in \mathbb{N}$
- eine abelsche Gruppe ist. Man erhält also
- für Primzahlen  $p$  einen endlichen Körper  $(\mathbb{Z}_p, +, \cdot)$  mit genau  $p$  Elementen und Charakteristik  $p$**
- und schreibt in Anlehnung an den englischsprachigen Fachbegriff „field“ für Körper auch
- $\mathbb{F}_p$
- für
- $\mathbb{Z}_p$
- .

- (3) Der vielleicht bekannteste Schiefkörper, der kein Körper ist, ist der
- $\mathbb{R}$
- (und
- $\mathbb{C}$
- ) erweiternde Zahlbereich der sogenannten Quaternionen, auf den wir an dieser Stelle aber nicht näher eingehen.

**Bemerkungen** (zu (Schief-)Körpern).

- (1) Ein **Körper**  $(K, +, \cdot)$  ist die **algebraische Struktur mit den besten Eigenschaften** der beiden Verknüpfungen. Wenn wir rekapitulieren, bedeutet dies insgesamt<sup>3</sup>, dass ...
- $(K, +)$  eine abelsche Gruppe ist (im Einzelnen: Assoziativität, Kommutativität, neutrales Element 0, inverse Elemente),
  - $(K \setminus \{0\}, \cdot)$  eine abelsche Gruppe ist (im Einzelnen: Assoziativität, Kommutativität, neutrales Element, inverse Elemente)
  - und die Distributivgesetze für alle Element von  $K$  gelten.
- (2) Man kann daher **in einem Körper**  $(K, +, \cdot)$  sehr weitgehend **wie in den Bereichen  $\mathbb{Q}$  und  $\mathbb{R}$  der rationalen und reellen Zahlen rechnen**. Speziell lässt sich über das zu Ringen Gesagte hinaus die **Division**  $\frac{x}{y} := x/y := xy^{-1}$  für alle  $x, y \in K$  mit  $y \neq 0$  erklären.
- (3) **Jeder Körper ist** insbesondere ein **Integritätsring** (denn für  $y \in K \setminus \{0\}$  mit  $xy = 0$  für  $x \in K$  folgt  $x = xy y^{-1} = 0y^{-1} = 0$ , so dass  $y$  kein Nullteiler sein kann).
- (4) Die **Charakteristik eines Körpers** oder auch eines Schiefkörpers ist stets **Null oder eine (endliche) Primzahl**.

Ein weiteres zentrales Beispiel für eine Ringstruktur ergibt das **Rechnen mit Polynomen**:

**Motivation (Addition und Multiplikation von Polynomen, Koeffizientenfolgen)**. Wir möchten **Polynome** (in einer Unbestimmten  $X$ ) wie beispielsweise

$$\begin{aligned} p &:= 2X^2 - 3X + 4 = 0X^3 + 2X^2 + (-3)X + 4, \\ q &:= 3X^3 + 6X^2 + X = 3X^3 + 6X^2 + 1X + 0 \end{aligned}$$

als **symbolische Ausdrücke** addieren wie in

$$p + q = (0+3)X^3 + (2+6)X^2 + (-3+1)X + (4+0) = 3X^3 + 8X^2 - 2X + 4$$

und multiplizieren wie in

$$\begin{aligned} pq &= (0 \cdot 3)X^6 + (2 \cdot 3 + 0 \cdot 6)X^5 + (-3 \cdot 3 + 2 \cdot 6 + 0 \cdot 1)X^4 + (4 \cdot 3 - 3 \cdot 6 + 2 \cdot 1 + 0 \cdot 0)X^3 \\ &\quad + (4 \cdot 6 - 3 \cdot 1 + 2 \cdot 0)X^2 + (4 \cdot 1 - 3 \cdot 0)X + (4 \cdot 0) \\ &= 6X^5 + 3X^4 - 4X^3 + 21X^2 + 4X. \end{aligned}$$

Um diese Rechenoperationen allgemein und formal einführen zu können, identifizieren wir  $p$  und  $q$  mit ihren jeweiligen **Koeffizientenfolgen**  $a: \mathbb{N}_0 \rightarrow \mathbb{Z}, i \mapsto a_i$  und  $b: \mathbb{N}_0 \rightarrow \mathbb{Z}, i \mapsto b_i$ , die wir uns als unendliche Tupel  $(a_0, a_1, a_2, a_3, a_4, a_5, a_6, \dots) = (4, -3, 2, 0, 0, 0, \dots) \in \mathbb{Z}^{(\mathbb{N}_0)}$  und  $(b_0, b_1, b_2, b_3, b_4, b_5, b_6, \dots) = (0, 1, 6, 3, 0, 0, \dots) \in \mathbb{Z}^{(\mathbb{N}_0)}$  mit nur endlich vielen Nicht-Null-Einträgen vorstellen. (Zur Notation  $\mathbb{Z}^{(\mathbb{N}_0)}$  siehe dabei die folgende Definition.)

<sup>3</sup>Zur multiplikativen Struktur eines Körpers  $(K, +, \cdot)$  wurde oben nur festgehalten, dass  $(K \setminus \{0\}, \cdot)$  abelsche Gruppe sein soll, und man mag sich fragen, ob es dann nicht vorkommen kann, dass  $(K, \cdot)$  wegen Problemen mit 0 nicht einmal Halbgruppe ist (wie für einen Ring und damit einen Körper  $(K, +, \cdot)$  erforderlich). Wenn aber die additiven Eigenschaften und Distributivgesetze wie oben für alle Elemente inklusive 0 gefordert werden, kann dies tatsächlich nicht vorkommen. Dies liegt daran, dass zum einen  $0x = 0 = x0$  für  $x \in K \setminus \{0\}$  wie in Bemerkung (2) zu Ringen folgt und zum anderen  $0 \cdot 0 = 0 \cdot 0 + 0 \cdot 0 - 0 \cdot 0 = (0+0) \cdot 0 - 0 \cdot 0 = 0 \cdot 0 - 0 \cdot 0 = 0$  sein muss. Somit verhalten sich alle Multiplikationen mit 0 ausreichend gutartig, dass  $(K, \cdot)$  automatisch zu einer Halbgruppe wird.

Formal lassen sich diese Überlegungen zum symbolischen Rechnen mit Polynomen in folgende algebraische Konstruktion umsetzen:

**Definitionen (Polynome, Polynomring).** Sei  $(R, +, \cdot)$  ein Ring.

(I) Wir setzen

$$R[X] := R^{(\mathbb{N}_0)} := \{a \in \text{Abb}(\mathbb{N}_0, R) \mid a_i \neq 0 \text{ nur für endliche viele } i \in \mathbb{N}_0\},$$

wobei wir  $a_i \in R$  für den Funktionswert von  $i \in \mathbb{N}_0$  unter  $a$  schreiben und  $a \in R[X]$  auch durch Aufzählung der Funktionswerte in der Form  $a = (a_0, a_1, a_2, a_3, \dots)$  angeben.

(II) Wir nennen  $a = (a_0, a_1, a_2, a_3, \dots) \in R[X]$  ein **Polynom** über dem Grundring  $(R, +, \cdot)$  in der Unbestimmten  $X$ , den Eintrag  $a_i \in R$  den **Koeffizient**  $i$ -ter Ordnung von  $a$  und  $(a_0, a_1, a_2, a_3, \dots) \in R^{(\mathbb{N}_0)}$  (genau genommen nichts anderes als  $a$  selbst) die **Koeffizientenfolge** von  $a$ .

(III) Wir erklären die **Summe**  $a+b \in R[X]$  und das **Produkt**  $ab \in R[X]$  von **Polynomen**  $a, b \in R[X]$  durch

$$(a+b)_k := a_k + b_k, \quad (ab)_k := \sum_{i=0}^k a_i b_{k-i} \quad \text{für } k \in \mathbb{N}_0$$

(wohldefiniert, da  $(a+b)_k \neq 0$  und  $(ab)_k \neq 0$  nur für endliche viele  $k \in \mathbb{N}_0$  eintreten).

(IV) Wir nennen  $(R[X], +, \cdot)$  mit den gerade definierten Verknüpfungen den **Polynomring** über dem Grundring  $(R, +, \cdot)$  in der **Unbestimmten**  $X$ .

**Proposition.** Für jeden (kommutativen) Ring  $(R, +, \cdot)$  ist der Polynomring  $(R[X], +, \cdot)$  über  $(R, +, \cdot)$  ein (kommutativer) Ring mit  $0_{R[X]} = (0_R, 0_R, 0_R, 0_R, \dots)$ ,  $1_{R[X]} = (1_R, 0_R, 0_R, 0_R, \dots)$  und additiv Inversen  $-(a_0, a_1, a_2, a_3, \dots) = (-a_0, -a_1, -a_2, -a_3, \dots)$  zu  $(a_0, a_1, a_2, \dots) \in R[X]$ .

*Beweis.* Dass  $(R[X], +)$  (mit  $0_{R[X]}$  und Inversen wie angegeben) eine abelsche Gruppe ist, folgt problemlos daraus, dass  $(\text{Abb}(\mathbb{N}_0, R), +)$  diese Eigenschaft hat, die Null in  $R[X]$  liegt und Inverse zu Elementen von  $R[X]$  in  $R[X]$  bleiben. Es gilt daher nur, die multiplikativen Eigenschaften und Distributivgesetze des Polynomrings zu verifizieren: Die benötigte Eigenschaft von  $1_{R[X]}$  entnehmen wir aus der Definition der Multiplikation (wo bei Multiplikation mit  $1_{R[X]}$  von links oder rechts einzig der Summand für  $i = 0$  bzw.  $i = k$  ungleich Null ist und bleibt). Für multiplikative Assoziativität machen wir die Rechnung (für  $a, b, c \in R[X]$ ,  $k \in \mathbb{N}_0$ )

$$\begin{aligned} ((ab)c)_k &= \sum_{j=0}^k \sum_{i=0}^j a_i b_{j-i} c_{k-j} = \sum_{0 \leq i \leq j \leq k} a_i b_{j-i} c_{k-j} = \sum_{i=0}^k \sum_{j=i}^k a_i b_{j-i} c_{k-j} \\ &= \sum_{i=0}^k \sum_{j=0}^{k-i} a_i b_j c_{k-i-j} = (a(bc))_k \end{aligned}$$

mit Umsortierung der Summationsindizes und Indexverschiebung, wobei  $\sum_{0 \leq i \leq j \leq k}$  für  $\sum_{(i,j) \in I_k}$  mit der Indexmenge  $I_k := \{(\bar{i}, \bar{j}) \in \mathbb{N}_0^2 \mid \bar{i} \leq \bar{j} \leq k\}$  steht. Die Distributivgesetze des Polynomrings ergeben sich auf naheliegender Weise durch Ausmultiplizieren von Summen in  $(R, +, \cdot)$ .

Ist schließlich  $(R, +, \cdot)$  kommutativ, so bekommen wir multiplikative Kommutativität im Polynomring durch die Rechnung (für  $a, b \in R[X]$ ,  $k \in \mathbb{N}_0$ )

$$(ab)_k = \sum_{i=0}^k a_i b_{k-i} = \sum_{i=0}^k b_{k-i} a_i = \sum_{i=0}^k b_i a_{k-i} = (ba)_k$$

mit Indexlaufumkehr. Damit sind alle benötigten Eigenschaften gezeigt.  $\square$

Ihren **wahren Sinn**, nämlich wie in der Motivation symbolisch rechnen zu dürfen, entfaltet die Definition aber **erst in Anbetracht folgender Festlegungen und Beobachtungen**.

**Notationen & Folgerungen** (bei **Polynomen**). Sei  $(R, +, \cdot)$  ein Ring.

- (I) Durch **Identifikation** der Elemente  $r \in R$  des **Grundrings** mit  $(r, 0, 0, 0, \dots) \in R[X]$  verstehen wir

$$R \subset R[X].$$

Wir bezeichnen die Elemente von  $R$  in diesem Zusammenhang als **Konstanten** oder **konstante Polynome** und bekommen  $r(a_0, a_1, a_2, a_3, \dots) = (ra_0, ra_1, ra_2, ra_3, \dots)$  sowie  $(a_0, a_1, a_2, a_3, \dots)r = (a_0r, a_1r, a_2r, a_3r, \dots)$  für  $r \in R$  und  $(a_0, a_1, a_2, a_3, \dots) \in R[X]$ .

- (II) Wir verstehen die **Unbestimmte selbst als Polynom**

$$X := (0, 1, 0, 0, 0, \dots) \in R[X]$$

mit  $pX = Xp$  für alle  $p \in R[X]$  und erhalten induktiv, dass das **Monom**  $rX^k$  der Ordnung  $k \in \mathbb{N}_0$  mit Koeffizient  $r \in R$  die Koeffizientenfolge  $(0, 0, \dots, 0, 0, r, 0, 0, 0, \dots) \in R[X]$  mit genau  $k$  Nullen vor einem  $r$  als dem einzigen Nicht-Null-Koeffizienten besitzt.

- (III) Damit können wir jedes **Polynom**  $p = (a_0, a_1, a_2, a_3, \dots) \in R[X] \setminus \{0\}$  in **Standard-Form**<sup>4</sup>

$$p = a_\ell X^\ell + a_{\ell-1} X^{\ell-1} + \dots + a_2 X^2 + a_1 X + a_0 = \sum_{i=0}^{\ell} a_i X^i$$

schreiben, wobei  $\ell$  die größte Zahl in  $\mathbb{N}_0$  mit  $a_\ell \neq 0$  sei (die existiert, weil mindestens ein Koeffizient, aber insgesamt nur endliche viele Koeffizienten ungleich Null sind). Wir nennen hierbei  $a_\ell$  den **Leitkoeffizient** oder **führenden Koeffizient** und  $\text{grad}(p) := \ell \in \mathbb{N}_0$  den **Grad** des Polynoms  $p$ . Für das Nullpolynom  $0_{R[X]}$  treffen wir die Konvention, dass sein Grad  $-\infty$  sei. Ein Polynom mit Leitkoeffizient 1 heißt auch **normiertes Polynom**.

- (IV) Direkt aus der Definition als Koeffizientenfolgen ergibt sich für Polynome die Möglichkeit des **Koeffizientenvergleichs**: Aus der Gleichheit  $\sum_{i=0}^{\ell} a_i X^i = \sum_{i=0}^m b_i X^i$  von Polynomen in  $R[X]$  mit Leitkoeffizienten  $a_\ell \neq 0 \neq b_m$  folgen die Übereinstimmungen  $\ell = m$  der Grade und  $a_i = b_i$  der Koeffizienten für alle  $i \in \{1, 2, \dots, \ell\}$ .

- (V) An dieser Stelle erhalten wir für

$$p = \sum_{i=0}^{\ell} a_i X^i \in R[X] \quad \text{und} \quad q = \sum_{i=0}^m b_i X^i \in R[X]$$

<sup>4</sup>Die Potenzen von  $X^i$  sind wie in einem allgemeinen Ring zu verstehen. Insbesondere ist  $X^0 = 1 \in R \subset R[X]$ .

ganz allgemein die durch die anfängliche Motivation nahegelegten **Rechenregeln für Summe und Produkt von Polynomen**

$$p + q = \sum_{k=0}^{\max\{\ell, m\}} (a_k + b_k) X^k, \quad pq = \sum_{k=0}^{\ell+m} \left( \sum_{i=0}^k a_i b_{k-i} \right) X^k = \sum_{k=0}^{\ell+m} \left( \sum_{i=\max\{0, k-m\}}^{\min\{k, \ell\}} a_i b_{k-i} \right) X^k,$$

wobei  $\max\{x, y\}$  bzw.  $\min\{x, y\}$  die größere bzw. kleinere von zwei Zahlen  $x, y \in \mathbb{R}$  bezeichnet und wir natürlich  $a_{\ell+1} = a_{\ell+2} = a_{\ell+3} = \dots = 0$  sowie  $b_{m+1} = b_{m+2} = b_{m+3} = \dots = 0$  verstehen.

Wir halten noch fest:

**Bemerkungen (zu Polynomringen).**

- (1) Für einen Integritätsring  $(R, +, \cdot)$  ist auch der Polynomring  $(R[X], +, \cdot)$  ein Integritätsring. (Begründung: Für Polynome  $p = \sum_{i=0}^{\ell} a_i X^i \in R[X] \setminus \{0\}$  und  $q = \sum_{i=0}^m b_i X^i \in R[X] \setminus \{0\}$  mit Leitkoeffizienten  $a_{\ell} \neq 0 \neq b_m$  ergibt sich als Leitkoeffizient  $(\ell+m)$ -ter Ordnung von  $p+q$  gemäß Obigem  $\sum_{i=\max\{0, \ell\}}^{\min\{\ell+m, \ell\}} a_i b_{\ell+m-i} = a_{\ell} b_m \neq 0$ . Damit ist  $pq \neq 0$  in  $R[X]$ .)
- (2) Selbst für einen Körper  $K$  ist der Polynomring  $K[X]$  *nie* ein Körper, denn das Polynom  $X$  ist (wie auch jedes andere Polynom vom Grad  $\geq 1$ ) nicht invertierbar.

In der Schulmathematik werden Polynome eher als Funktionen oder Funktionsterme betrachtet. Dies ist kein Widerspruch zum Obigen, denn auch bei der hiesigen Betrachtungsweise sind Polynome eng mit einer zugehörigen Polynomfunktion verbunden:

**Definition (Polynomfunktionen, Nullstellen).** Sei  $(R, +, \cdot)$  ein kommutativer Ring. Die zu einem Polynom  $p = \sum_{i=0}^{\ell} a_i X^i \in R[X]$  gehörige **Polynomfunktion**  $\hat{p}: R \rightarrow R$  ist durch

$$\hat{p}(r) := \sum_{i=0}^{\ell} a_i r^i \in R \quad \text{für alle } r \in R$$

gegeben. Wir nennen  $r \in R$  eine **Nullstelle** von  $p \in R[X]$  (und auch von  $\hat{p} \in \text{Abb}(R)$ ), wenn  $\hat{p}(r) = 0_R$  gilt.

**Bemerkungen (zu Polynomfunktionen).** Sei  $(R, +, \cdot)$  ein kommutativer Ring.

- (1) In gutartigen Fällen kann man Polynome und Polynomfunktionen identifizieren, tut dies später des Öfteren und verzichtet dementsprechend auf das Dach-Symbol bei Polynomfunktionen. Für den Moment jedoch betonen wir den **Unterschied zwischen Polynomen und Polynomfunktionen**: Das **Polynom**  $p = \sum_{i=0}^{\ell} a_i X^i \in R[X]$  ist formal als Koeffizientenfolge definiert und als **Objekt symbolischen Rechnens mit einer Unbestimmten  $X$**  zu verstehen. Die **Polynomfunktion**  $\hat{p} \in \text{Abb}(R)$  ist als **Abbildung**  $R \rightarrow R$  definiert (die übrigens ganz anders abbildet als die Koeffizientenfolge  $\mathbb{N}_0 \rightarrow R$  von  $p$  und mit dieser nicht unmittelbar zusammenhängt).

Noch etwas anderes ist der **Funktionsterm**  $\hat{p}(r) = \sum_{i=0}^{\ell} a_i r^i$  **der Polynomfunktion**  $\hat{p}$ , der für jedes einzelne  $r \in R$  selbst Element von  $R$  ist. Zwar besteht die Funktion  $\hat{p}$  im Wesentlichen in der Zuordnungsregel  $r \mapsto \sum_{i=0}^{\ell} a_i r^i$  oder mit anderen Worten  $\hat{p}(r) = \sum_{i=0}^{\ell} a_i r^i$  für alle  $r \in R$ , die Gleichsetzung  $\hat{p} = \sum_{i=0}^{\ell} a_i r^i$  ohne „ $(r)$ “ links ist aber formal *nicht* korrekt.

- (2) Die **Addition und Multiplikation im Polynomring  $R[X]$  entsprechen der punktweisen Addition und Multiplikation von Polynomfunktionen** in dem Sinn, dass

$$\widehat{p+q} = \widehat{p} + \widehat{q} \quad \text{und} \quad \widehat{pq} = \widehat{p}\widehat{q} \quad \text{in } \text{Abb}(R)$$

für alle  $p, q \in R[X]$  gelten. Diese Übereinstimmung bedeutet letztlich, dass man auch mit (formal eingeführten) Polynomen mit denselben Rechenregeln wie im Ring  $(R, +, \cdot)$  rechnen kann — und speziell bei Polynomen über Zahlbereichen einfach mit den üblichen Rechenregeln. Dies ist tatsächlich auch der **Hauptgrund, die Definitionen wie oben zu treffen**.

(Begründung: Die Gleichheit  $\widehat{p+q} = \widehat{p} + \widehat{q}$  ist klar, da auch  $p+q$  komponentenweise definiert wurde. Die Gleichheit  $\widehat{pq} = \widehat{p}\widehat{q}$  zeigen wir, indem wir  $p = \sum_{i=0}^{\ell} a_i X^i$ ,  $q = \sum_{j=0}^m b_j X^j$  schreiben und mit der Kommutativität von  $(R, +, \cdot)$  nachrechnen, dass

$$\begin{aligned} (\widehat{p}\widehat{q})(x) &= \widehat{p}(x)\widehat{q}(x) = \left( \sum_{i=0}^{\ell} a_i x^i \right) \left( \sum_{j=0}^m b_j x^j \right) = \sum_{i=0}^{\ell} \sum_{j=0}^m a_i b_j x^{i+j} \\ &= \sum_{i=0}^{\ell} \sum_{k=i}^{i+m} a_i b_{k-i} x^k = \sum_{0 \leq i \leq k \leq i+m \leq \ell+m} a_i b_{k-i} x^k = \sum_{k=0}^{\ell+m} \sum_{i=\max\{0, k-m\}}^{\min\{k, \ell\}} a_i b_{k-i} x^k = \widehat{p}\widehat{q}(x) \end{aligned}$$

für alle  $x \in R$  gilt.)

- (3) Als Konsequenz der vorigen Bemerkung bildet die Menge der Polynomfunktionen  $R \rightarrow R$  mit der punktweisen Addition und Multiplikation ebenfalls einen kommutativen Ring.

Wie bei ganzen Zahlen besteht auch bei Polynomen die Möglichkeit zur Division mit Rest und bringt einige nützliche Konsequenzen:

**Satz (zu Polynomdivision, Linearfaktoren, Nullstellen).** Sei  $(K, +, \cdot)$  ein Körper.

- (I) **Polynomdivision:** Für Polynome  $p, q \in K[X]$  mit  $q \neq 0$  gibt es eindeutig bestimmte Polynome  $r, s \in K[X]$  mit<sup>5</sup>  $\text{grad}(r) < \text{grad}(q)$ , so dass  $p = s \cdot q + r$  gilt.
- (II) **Abspalten von Linearfaktoren:** Ist  $x_0 \in K$  eine Nullstelle von  $p \in K[X]$ , so kann  $p$  als  $p = s \cdot (X - x_0)$  mit  $s \in K[X]$  geschrieben werden.
- (III) Ein Polynom  $p$  über  $K$  vom Grad  $n \in \mathbb{N}_0$  hat höchstens  $n$  verschiedene Nullstellen in  $K$ .
- (IV) Hat  $K$  unendlich viele Elemente, so ist ein Polynom über  $K$  durch die zugehörige Polynomfunktion eindeutig bestimmt.

*Beweis von Teil (I) des Satzes.* Wir zeigen zuerst Existenz von  $r$  und  $s$ : Im Fall  $\text{grad}(q) > \text{grad}(p)$  können wir  $r := p$  und  $s := 0$  wählen und erhalten trivial  $p = s \cdot q + r$  mit  $\text{grad}(r) = \text{grad}(p) < \text{grad}(q)$ . Für  $\text{grad}(q) \leq \text{grad}(p)$  zeigen wir die Existenz durch Induktion nach  $\text{grad}(p) \in \mathbb{N}_0$ . Beim Induktionsanfang für  $\text{grad}(p) = 0$  ist auch  $\text{grad}(q) = 0$  und damit  $q \in K \setminus \{0\}$ , so dass wir  $p = s \cdot q + r$  für  $r := 0$  und  $s := pq^{-1}$  erhalten. Für den Induktionsschritt habe  $p \in K[X]$  Grad  $\ell \in \mathbb{N}$  und Leitkoeffizient  $a_{\ell}$  sowie  $q \in K[X]$  Grad  $m \in \mathbb{N}_0$  und Leitkoeffizient  $b_m$ , insbesondere  $b_m \neq 0$ , und es sei  $m \leq \ell$ . Dann verschwindet bei  $\tilde{p} := p - a_{\ell} b_m^{-1} X^{\ell-m} q \in K[X]$  der Koeffizient  $\ell$ -ter Ordnung, es gilt also  $\text{grad}(\tilde{p}) < \ell$ . Per Induktionsannahme gibt es daher  $r, \tilde{s} \in K[X]$  mit  $\text{grad}(r) < \text{grad}(q)$ , so dass  $\tilde{p} = \tilde{s} \cdot q + r$  gilt. Durch Umformen erhalten wir

<sup>5</sup>Wir erlauben  $r = 0$  mit  $\text{grad}(r) = -\infty < \text{grad}(q) \in \mathbb{N}_0$ .

daraus  $p = (\tilde{s} + a_\ell b_m^{-1} X^{\ell-m}) \cdot q + r$ , also die Induktionsbehauptung für das bereits eingeführte  $r$  und  $s := \tilde{s} + a_\ell b_m^{-1} X^{\ell-m} \in K[X]$ .

Um Eindeutigkeit von  $r$  und  $s$  nachzuweisen, ist für  $r, \tilde{r}, s, \tilde{s} \in K[X]$  mit  $\text{grad}(r) < \text{grad}(q)$ ,  $\text{grad}(\tilde{r}) < \text{grad}(q)$  und  $\tilde{s} \cdot q + \tilde{r} = s \cdot q + r$  zu zeigen, dass  $\tilde{r} = r$ ,  $\tilde{s} = s$  sein muss. Dazu schreiben wir die Gleichung als  $(\tilde{s} - s) \cdot q = r - \tilde{r}$  und bemerken im Fall  $\tilde{s} \neq s$ , dass  $\text{grad}((\tilde{s} - s) \cdot q) \geq \text{grad}(q)$  gilt (Grad des Produkts ist Summe der Grade; benutzt Nullteilerfreiheit). Andererseits gilt aber  $\text{grad}(r - \tilde{r}) < \text{grad}(q)$ , und wir erreichen einen Widerspruch. Also muss  $\tilde{s} = s$  sein, und dann folgt sofort auch  $\tilde{r} = r$ .  $\square$

*Beweis von Teil (II) des Satzes.* Aus Teil (I) mit  $q := X - x_0 \in K[X]$  lesen wir  $p = s \cdot (X - x_0) + r$  für  $r, s \in K[X]$  mit  $\text{grad}(r) < \text{grad}(q) = 1$ , also  $r \in K$  ab. Durch Einsetzen von  $x_0$  erhalten wir  $0 = \hat{p}(x_0) = \hat{s}(x_0) \cdot 0 + r = r$ , also gilt wie behauptet  $p = s \cdot (X - x_0)$ .  $\square$

*Beweis von Teil (III) des Satzes.* Wir argumentieren indirekt: Sei  $p \in K[X]$  ein Polynom mit  $\text{grad}(p) = n \in \mathbb{N}_0$  und  $(n+1)$  verschiedenen Nullstellen  $x_1, x_2, \dots, x_n, x_{n+1} \in K$ . Dann erreichen wir durch  $(n+1)$ -malige Anwendung von Teil (II) des Satzes die Form  $p = s \prod_{i=1}^{n+1} (X - x_i)$  mit  $s \in K[X]$ . Im Fall  $s \neq 0$  folgt  $\text{grad}(p) \geq n+1$ , im Fall  $s = 0$  folgt  $\text{grad}(p) = -\infty$ . Wir erhalten also in jedem Fall einen Widerspruch zu  $\text{grad}(p) = n \in \mathbb{N}_0$ , und die Behauptung ist bewiesen.  $\square$

*Beweis von Teil (IV) des Satzes.* Wären  $p, q \in K[X]$  verschiedene Polynome mit  $p(x) = q(x)$  für alle  $x \in K$ , so hätte  $p - q \in K[X] \setminus \{0\}$  mit  $\text{grad}(p - q) \in \mathbb{N}_0$  unendlich viele Nullstellen in  $K$  und stünde im Widerspruch zu Teil (III) des Satzes.  $\square$

**Bemerkung.** Die Teile (III) und (IV) Satzes gelten nicht nur über Körpern, sondern allgemeiner über Integritätsringen. Der Beweis von Teil (III) muss dort modifiziert werden, was aber hier nur ergänzend im Kleingedruckten dargestellt wird:

*Beweis von Teil (III) des Satzes über einem allgemeinen Integritätsring  $(R, +, \cdot)$ .* Wir zeigen per Induktion nach  $n \in \mathbb{N}_0$ , dass ein Polynom  $p \in R[X]$  mit  $\text{grad}(p) = n$  höchstens  $n$  verschiedene Nullstellen in  $R$  besitzt: Beim Induktionsanfang für  $n = 0$  ist  $p = r \in R \setminus \{0\}$  konstant und besitzt keine Nullstelle (da  $\hat{p} \equiv r \neq 0$ ). Für den Induktionsschritt betrachten wir  $p = \sum_{i=0}^n a_i X^i \in R[X]$  mit  $\text{grad}(p) = n \in \mathbb{N}$ . Hat  $p$  überhaupt eine Nullstelle  $x_0 \in R$ , so erhalten wir mit einer auch in kommutativen Ringen gültigen Summenformel (siehe Aufgabe 9(c) auf Blatt 5)

$$\hat{p}(x) = \hat{p}(x) - \hat{p}(x_0) = \sum_{i=1}^n a_i (x^i - x_0^i) = (x - x_0) \sum_{i=1}^n \sum_{j=0}^{i-1} a_i x_0^{i-1-j} x^j = (x - x_0) \sum_{j=0}^{n-1} b_j x^j$$

für  $b_j := \sum_{i=j+1}^n a_i x_0^{i-1-j} \in R$ . Da  $R$  nullteilerfrei ist, hat das Polynom  $\sum_{j=0}^{n-1} b_j X^j \in R[X]$  mit Leitkoeffizient  $b_{n-1} = a_n \neq 0$  und Grad  $n-1$  in  $R \setminus \{x_0\}$  exakt dieselben Nullstellen wie  $p$ , und nach Induktionsannahme hat es insgesamt höchstens  $n-1$  Nullstellen in  $R$ . Dies impliziert, dass  $p$  selbst mit der einzig möglichen zusätzlichen Nullstelle  $x_0$  höchstens  $n$  Nullstellen in  $R$  besitzt. Damit ist die Induktionsbehauptung gezeigt und der Beweis komplett.  $\square$

**Verfahren (Polynomdivision).** Mit Teil (I) des Satzes geht das **Rechenverfahren der Polynomdivision** einher, mit dem man für gegebene Polynome  $p, q \in K[X]$ ,  $q \neq 0$ , über einem Körper  $K$  den Multiplikator  $s$  und den Rest  $r$  mit  $p = s \cdot q + r$  und  $\text{grad}(r) < \text{grad}(q)$  bestimmt. Man baut dabei exakt auf der Idee des vorgestellten Induktionsbeweises auf und bestimmt durch Division des Leitmonoms  $a_\ell X^\ell$  von  $p$  durch das Leitmonom  $b_m X^m$  von  $q$  zunächst das Leitmonom  $a_\ell b_m^{-1} X^{\ell-m}$  von  $s$ . Nun betrachtet man die „Korrektur“  $\tilde{p} = p - a_\ell b_m^{-1} X^{\ell-m} \cdot q$  und dividiert im nächsten Schritt das Leitmonom von  $\tilde{p}$  durch  $b_m X^m$ , um den nächsten Term von  $s$  zu erhalten. Danach folgt die nächste Korrektur, und so weiter. Als konkretes Beispiel führen wir dieses

Verfahren hier für  $p := X^4 - 4X^3 + 4X^2 - 2$  und  $q := 2X^2 - 4X - 6$  in  $\mathbb{Q}[X]$  wie folgt durch:

$$\begin{array}{r} (X^4 - 4X^3 + 4X^2 - 2) : (2X^2 - 4X - 6) = \frac{1}{2}X^2 - X - \frac{1}{2} + \frac{-4X - 5}{2X^2 - 4X - 6} \\ \underline{-(X^4 - 2X^3 - 3X^2)} \\ -2X^3 + 3X^2 \\ \underline{-(-2X^3 + 4X^2 + 6X)} \\ -X^2 - 2X \\ \underline{-(-X^2 + 2X + 3)} \\ -4X - 5 \end{array}$$

Dabei wird in jedem Schritt ein farbiges Leitmonom der linken Seite durch das Leitmonom  $2X^2$  von  $q$  (das in jedem Schritt gleich bleibt) dividiert, um das farblich entsprechende Monom auf der rechten Seite zu erhalten. Dieses Monom wird dann mit ganz  $q = 2X^2 - 4X - 6$  multipliziert, um das immer noch farblich entsprechende Korrekturpolynom links zu erhalten. Nach Subtraktion der Korrektur beginnt der nächste Schritt. Da sich der Grad des Polynoms links in jedem Schritt verringert, ist dieser Grad nach endlich vielen Schritten  $< \text{grad}(q)$ , womit das Verfahren endet und das verbleibende, hier violett gefärbte Polynom den Rest  $r$  bildet. Insgesamt haben wir im Beispielfall  $s = \frac{1}{2}X^2 - X - \frac{1}{2}$  und  $r = -4X - 5$  gefunden und mit anderen Worten

$$X^4 - 4X^3 + 4X^2 - 2 = \left(\frac{1}{2}X^2 - X - \frac{1}{2}\right) \cdot (2X^2 - 4X - 6) + (-4X - 5)$$

eingesehen.

Zum Abschluss dieses Abschnitts halten wir fest, dass die Konstruktion des Polynomrings über einem Grundring iteriert werden kann (was aber tatsächlich nur deshalb funktioniert, weil wir die Bildung allgemein über Ringen und nicht nur über Körpern vorgenommen haben):

**Bemerkung** (zu **Polynomen in mehreren Unbestimmten**). Ein **Polynom** über einem Ring  $(R, +, \cdot)$  **in zwei Unbestimmten**  $X$  und  $Y$  hat die Form

$$\sum_{\substack{i \in \{0, 1, 2, \dots, \ell\} \\ j \in \{0, 1, 2, \dots, m\}}} a_{ij} X^i Y^j := \sum_{j=0}^m \left( \sum_{i=0}^{\ell} a_{ij} X^i \right) Y^j \in (R[X])[Y]$$

mit Koeffizienten  $a_{ij} \in R$ . Man schreibt daher

$$R[X, Y] := (R[X])[Y]$$

und nennt  $R[X, Y]$  den Polynomring über  $R$  in zwei Unbestimmten  $X$  und  $Y$  (für die übrigens auch bei nicht-kommutativem Grundring stets  $XY = YX$  und allgemeiner  $pX = Xp$ ,  $pY = Yp$  für alle  $p \in R[X, Y]$  gelten). Iteration dieser Vorgehensweise ergibt den Polynomring  $R[X_1, X_2, \dots, X_n] := (\dots ((R[X_1])[X_2]) \dots)[X_n]$  über  $R$  in  $n \in \mathbb{N}$  Unbestimmten  $X_1, X_2, \dots, X_n$ . Genauer können wir auf das Rechnen mit Polynomen mehrerer Variablen an dieser Stelle aber nicht eingehen.

### 3.3 Homomorphismen, Unter- und Faktorstrukturen

#### Definitionen (Homomorphismen).

- (I) Ein (**Gruppen-)**Homomorphismus von einer Gruppe  $(G, *)$  in eine Gruppe  $(H, \otimes)$  ist eine Abbildung  $\varphi: G \rightarrow H$  mit  $\varphi(g_1 * g_2) = \varphi(g_1) \otimes \varphi(g_2)$  für alle  $g_1, g_2 \in G$ .
- (II) Ein (**Ring-)**Homomorphismus von einem Ring  $(R, +, \cdot)$  in einen Ring  $(S, \oplus, \odot)$  ist eine Abbildung  $\varphi: R \rightarrow S$  mit  $\varphi(x+y) = \varphi(x) \oplus \varphi(y)$  und  $\varphi(x \cdot y) = \varphi(x) \odot \varphi(y)$  für alle  $x, y \in R$  sowie  $\varphi(1_R) = 1_S$ . Sind  $(R, +, \cdot)$  und  $(S, \oplus, \odot)$  sogar Körper, so spricht man von einem **Körperhomomorphismus**.
- (III) Wir vereinbaren<sup>6</sup> für Gruppen, Ringe, Körper gleichermaßen: Ein **Monomorphismus**, **Epimorphismus** bzw. **Isomorphismus** ist ein injektiver, surjektiver bzw. bijektiver Homomorphismus. Gibt es zwischen zwei Gruppen/Ringen/Körpern einen Isomorphismus, so heißen diese (zueinander) **isomorph**. Ein **Endomorphismus** ist ein Homomorphismus mit gleichem Definitionsbereich und Ziel bezüglich der gleichen Verknüpfungen darauf. Ein **Automorphismus** ist ein bijektiver Endomorphismus. Die Mengen aller Homo- und aller Isomorphismen  $\mathcal{X} \rightarrow \mathcal{Y}$  notieren wir als  $\text{Hom}(\mathcal{X}, \mathcal{Y})$  und  $\text{Iso}(\mathcal{X}, \mathcal{Y})$ , für Endo- und Automorphismen vereinbaren wir  $\text{End}(\mathcal{X}) := \text{Hom}(\mathcal{X}, \mathcal{X})$  und  $\text{Aut}(\mathcal{X}) := \text{Iso}(\mathcal{X}, \mathcal{X})$ .

#### Bemerkungen (zu Homomorphismen).

- (1) **Homomorphismen sind Struktur-erhaltende Abbildungen.** Im Fall eines Isomorphismus kann man die Elemente in Definitionsbereich und Ziel 1-zu-1 identifizieren und mit einander entsprechenden Elementen in Definitionsbereich und Ziel auch genauso „rechnen“. Daher **erhalten Isomorphismen alle algebraischen Eigenschaften**, und zueinander isomorphe Gruppen/Ringe/Körper verhalten sich in algebraischer Hinsicht völlig gleich.
- (2) Ein Gruppenhomomorphismus  $\varphi: G \rightarrow H$  erfüllt automatisch  $\varphi(e_G) = e_H$  für die neutralen Elemente  $e_G \in G$  und  $e_H \in H$  sowie  $\varphi(g)^{-1} = \varphi(g^{-1})$  für alle  $g \in G$ .  
(Nachweis: Mit  $\varphi(e_G) = \varphi(e_G) \otimes \varphi(e_G) \otimes \varphi(e_G)^{-1} = \varphi(e_G * e_G) \otimes \varphi(e_G)^{-1} = \varphi(e_G) \otimes \varphi(e_G)^{-1} = e_H$  erhalten wie die Behauptung über die neutralen Elemente. Für die Regel zu den Inversen rechnen wir dann  $\varphi(g) \otimes \varphi(g^{-1}) = \varphi(g * g^{-1}) = \varphi(e_G) = e_H$  und  $\varphi(g^{-1}) \otimes \varphi(g) = \varphi(g^{-1} * g) = \varphi(e_G) = e_H$ .)
- (3) Ein Ring- beziehungsweise Körperhomomorphismus  $\varphi: R \rightarrow S$  ist insbesondere Gruppenhomomorphismus von  $(R, +)$  in  $(S, \oplus)$  und erfüllt neben  $\varphi(1_R) = 1_S$  automatisch  $\varphi(0_R) = 0_S$ ,  $-\varphi(x) = \varphi(-x)$  für  $x \in R$  sowie  $\varphi(x)^{-1} = \varphi(x^{-1})$  für invertierbare  $x \in R$ . Im Körperfall ist  $\varphi$  auch Gruppenhomomorphismus von  $(R \setminus \{0\}, \cdot)$  in  $(S \setminus \{0\}, \odot)$  mit  $\varphi(x)^{-1} = \varphi(x^{-1})$  für alle  $x \in R \setminus \{0\}$ . Dies folgt aus der vorigen Bemerkung beziehungsweise analog zu dieser.  
(Die Forderung  $\varphi(1_R) = 1_S$  in der Definition kann man aber nicht weglassen. Dass diese nicht aus den anderen Bedingungen folgt, erkennt man am Beispiel der Nullabbildung  $\varphi: R \rightarrow S, x \mapsto 0_S$ .)

#### Beispiele (von Homomorphismen).

- (0) Die identische Abbildung ist für jede Gruppe/jeden Ring/jeden Körper ein Automorphismus.

<sup>6</sup>In der fortgeschrittenen Algebra (Kategorientheorie) sind auch alternative Definitionen der verschiedenen Typen von Morphismen gebräuchlich, die den obigen verwandt, aber nicht in allen Fällen vollständig äquivalent zu diesen sind.

- (1) Für  $\mathbb{B} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}\}$  ist die Abbildung  $\mathbb{B} \rightarrow \mathbb{B}$ ,  $x \mapsto -3x$  ein Gruppenendomorphismus von  $(\mathbb{B}, +)$ , denn es gilt  $-3(x+y) = -3x + (-3y)$  für  $x, y \in \mathbb{B}$ . Für  $\mathbb{B} \in \{\mathbb{Q}, \mathbb{R}\}$  handelt es sich sogar um einen Gruppenautomorphismus
- (2) Für  $\mathbb{B} \in \{\mathbb{Q}, \mathbb{R}\}$  ist die Abbildung  $\mathbb{B} \setminus \{0\} \rightarrow \mathbb{B} \setminus \{0\}$ ,  $x \mapsto x^2$  ein Gruppenendomorphismus von  $(\mathbb{B} \setminus \{0\}, \cdot)$ , denn es gilt  $(xy)^2 = x^2 y^2$  für  $x, y \in \mathbb{B} \setminus \{0\}$ .
- (3) Die Abbildung  $\mathbb{Z} \rightarrow \mathbb{Q} \setminus \{0\}$ ,  $x \mapsto 2^x$  ist ein Gruppenmonomorphismus von der additiven Gruppe  $(\mathbb{Z}, +)$  in die multiplikative Gruppe  $(\mathbb{Q} \setminus \{0\}, \cdot)$ , denn es gilt  $2^{x+y} = 2^x 2^y$  für  $x, y \in \mathbb{Z}$ .
- (4) Für jedes  $n \in \mathbb{N}$  ist die Quotientenabbildung  $\mathbb{Z} \rightarrow \mathbb{Z}_n$ ,  $x \mapsto [x]_{\mathbb{Z}_n}$  des Restklassenrings  $\mathbb{Z}_n$  ein Ringepimorphismus, denn es gelten  $[x+y]_{\mathbb{Z}_n} = [x]_{\mathbb{Z}_n} + [y]_{\mathbb{Z}_n}$  und  $[xy]_{\mathbb{Z}_n} = [x]_{\mathbb{Z}_n} [y]_{\mathbb{Z}_n}$  für alle  $x, y \in \mathbb{Z}$  sowie  $[1]_{\mathbb{Z}_n} = 1_{\mathbb{Z}_n}$ .
- (5) Die Einbettung  $\mathbb{Q} \rightarrow \mathbb{R}$ ,  $x \mapsto x$  von  $\mathbb{Q}$  in  $\mathbb{R}$  ist ein Körpermonomorphismus.
- (6) Für jeden Ring  $(R, +, \cdot)$  ist die Vertauschung der Einträge  $\varphi: R^2 \rightarrow R^2$ ,  $(x_1, x_2) \mapsto (x_2, x_1)$  ein Ringautomorphismus. Allgemeiner ist für  $n \in \mathbb{N}$  und  $\pi \in S_n$  die **Koordinatenpermutation**  $\varphi_\pi: R^n \rightarrow R^n$ ,  $(x_1, x_2, \dots, x_n) \mapsto (x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(n)})$  ein Ringautomorphismus.
- (7) Für jeden kommutativen Ring  $(R, +, \cdot)$  ist die Abbildung  $R[X] \rightarrow \text{Abb}(R)$ ,  $p \mapsto \hat{p}$  ein Ringhomomorphismus und ebenso für jedes feste  $r \in R$  die Abbildung  $R[X] \rightarrow R$ ,  $p \mapsto \hat{p}(r)$ . Bei beiden Bildungen spricht man auch vom Einsetzungshomomorphismus.

(Für einen Integritätsring  $R$  mit unendlich vielen Elementen ist die erste Variante sogar Ringmonomorphismus. Das folgt aus dem letzten Satz in Abschnitt 3.2 und der darauf folgenden Bemerkung.)

### Bemerkungen (zu Homomorphismengruppen).

- (1) Für eine Gruppe  $(G, *)$  wird  $\text{Aut}(G)$  **mit Komposition** zu einer Gruppe, der **Automorphismengruppe** von  $(G, *)$ .  
 (Nachweis: Für  $\varphi, \psi \in \text{Aut}(G)$  rechnen wir  $\psi \circ \varphi \in \text{Aut}(G)$  mit  $\psi(\varphi(g_1 * g_2)) = \psi(\varphi(g_1) * \varphi(g_2)) = \psi(\varphi(g_1)) * \psi(\varphi(g_2))$  für  $g_1, g_2 \in G$  nach. Zudem ergibt sich  $\varphi^{-1} \in \text{Aut}(G)$  für die Umkehrfunktion  $\varphi^{-1}$  aus  $\varphi^{-1}(g_1 * g_2) = \varphi^{-1}(\varphi(\varphi^{-1}(g_1)) * \varphi(\varphi^{-1}(g_2))) = \varphi^{-1}(\varphi(\varphi^{-1}(g_1) * \varphi^{-1}(g_2))) = \varphi^{-1}(g_1) * \varphi^{-1}(g_2)$  für alle  $g_1, g_2 \in G$ .)
- (2) Für eine Gruppe  $(G, *)$  und eine abelsche Gruppe  $(H, \otimes)$  werden  $\text{Hom}(G, H)$  und  $\text{End}(H)$  **mit punktweiser Verknüpfung**  $\otimes$  auch abelsche Gruppen. Man spricht von **Homo- bzw. Endomorphismengruppen**.  
 (Nachweis: Für  $\varphi, \psi \in \text{Hom}(G, H)$  zeigen wir  $\varphi \otimes \psi \in \text{Hom}(G, H)$  durch die auf Kommutativität von  $\otimes$  gegründete Rechnung  $(\varphi \otimes \psi)(g_1 * g_2) = \varphi(g_1 * g_2) \otimes \psi(g_1 * g_2) = \varphi(g_1) \otimes \varphi(g_2) \otimes \psi(g_1) \otimes \psi(g_2) = \varphi(g_1) \otimes \psi(g_1) \otimes \varphi(g_2) \otimes \psi(g_2) = (\varphi \otimes \psi)(g_1) \otimes (\varphi \otimes \psi)(g_2)$  für  $g_1, g_2 \in G$ . Dass die konstante Abbildung  $G \rightarrow H$  auf das neutrale Element in  $H$  das neutrale Element in  $\text{Hom}(G, H)$  ist, ist klar. Schließlich können wir Inverse zu  $\varphi \in \text{Hom}(G, H)$  als punktweise Inverse  $\varphi^{-1}$  erhalten, denn die Rechnung  $\varphi^{-1}(g_1 * g_2) = \varphi(g_1 * g_2)^{-1} = (\varphi(g_1) \otimes \varphi(g_2))^{-1} = \varphi(g_2)^{-1} \otimes \varphi(g_1)^{-1} = \varphi(g_1)^{-1} \otimes \varphi(g_2)^{-1}$  unter erneuter Verwendung der Kommutativität von  $\otimes$  ergibt  $\varphi^{-1} \in \text{Hom}(G, H)$ .)
- (3) Für eine (meist additiv notierte) abelsche Gruppe  $(G, +)$  wird  $(\text{End}(G), +, \circ)$  mit punktweiser Addition und Komposition sogar ein Ring, der **Endomorphismenring** von  $(G, +)$ . Anders als bei  $(\text{Abb}(G), +, \circ)$  (was gemäß Abschnitt 3.2 *kein* Ring ist) ergibt sich für Endomorphismen  $\varphi, \psi, \chi \in \text{End}(G)$  nämlich das „linke“ Distributivgesetz  $\varphi \circ (\psi + \chi) = \varphi \circ \psi + \varphi \circ \chi$  durch die Rechnung  $(\varphi \circ (\psi + \chi))(g) = \varphi(\psi(g) + \chi(g)) = \varphi(\psi(g)) + \varphi(\chi(g)) = (\varphi \circ \psi + \varphi \circ \chi)(g)$

für  $g \in G$  mit der Homomorphismus-Eigenschaft von  $\varphi$ . Die anderen benötigten Eigenschaften folgen aus Bemerkung (2) oder sind leicht zu prüfen.

### Definitionen (Kern eines Homomorphismus).

- (I) Der **Kern eines Gruppenhomomorphismus**  $\varphi: G \rightarrow H$  zwischen Gruppen  $(G, *)$  und  $(H, \otimes)$  ist

$$\text{Kern}(\varphi) := \varphi^{-1}(\{e_H\}) = \{g \in G \mid \varphi(g) = e_H\} \subset G$$

mit dem neutralen Element  $e_H$  von  $(H, \otimes)$ .

- (II) Der **Kern eines Ringhomomorphismus**  $\varphi: R \rightarrow S$  zwischen Ringen  $(R, +, \cdot)$  und  $(S, \oplus, \odot)$  ist

$$\text{Kern}(\varphi) := \varphi^{-1}(\{0_S\}) = \{x \in R \mid \varphi(x) = 0_S\} \subset R.$$

Insbesondere findet diese Definition **auch** auf **Körperhomomorphismen** Anwendung.

**Bemerkung.** Wegen  $\varphi(e_G) = e_H$  für das neutrale Element  $e_G$  von  $(G, *)$  gilt in (I) stets  $e_G \in \text{Kern}(\varphi)$  und wegen  $\varphi(0_R) = 0_S$  in (II) stets  $0_R \in \text{Kern}(\varphi)$ .

Am Kern lässt sich erkennen, ob ein Homomorphismus ein Monomorphismus ist (und so wird diese Eigenschaft in Zukunft dann auch wirklich fast immer gezeigt):

### Satz (Kern und Injektivität).

- (I) Für einen Homomorphismus  $\varphi: G \rightarrow H$  von Gruppen  $(G, *)$  und  $(H, \otimes)$  gilt:

$$\varphi \text{ injektiv} \iff \text{Kern } \varphi = \{e_G\}.$$

- (II) Für einen Homomorphismus  $\varphi: R \rightarrow S$  von Ringen  $(R, +, \cdot)$  und  $(S, \oplus, \odot)$  gilt:

$$\varphi \text{ injektiv} \iff \text{Kern } \varphi = \{0_R\}.$$

- (III) Ein Homomorphismus  $\varphi: K \rightarrow L$  von Körpern  $(K, +, \cdot)$  und  $(L, \oplus, \odot)$  ist immer injektiv.

*Beweis.* Teil (I) wird in den Übungen gezeigt. Teil (II) folgt durch Anwendung von Teil (I) auf die additiven Gruppen. Für Teil (III) reicht es,  $\text{Kern}(\varphi) \subset \{0_K\}$  für jeden Körperhomomorphismus  $\varphi: K \rightarrow L$  zu zeigen (denn nach der Bemerkung ist dies gleichbedeutend mit  $\text{Kern}(\varphi) = \{0_K\}$  und gibt gemäß Teil (II) Injektivität). Dazu sei  $x \in \text{Kern}(\varphi)$ , also  $x \in K$  mit  $\varphi(x) = 0_L$ . Wäre  $x \neq 0_K$ , so bekämen wir mit  $1_L = \varphi(1_K) = \varphi(xx^{-1}) = \varphi(x) \odot \varphi(x^{-1}) = 0_L \odot \varphi(x^{-1}) = 0_L$  einen Widerspruch. Also ist  $x = 0_K$ , und  $\text{Kern}(\varphi) \subset \{0_K\}$  ist gezeigt.  $\square$

Als nächsten erklären wir Unterstrukturen von Gruppen, Ringen und Körpern, mit denen wir ohne eine solche explizite Benennung tatsächlich schon oft umgegangen sind:

### Definitionen (algebraische Unterstrukturen).

- (I) Eine **Untergruppe**  $U$  einer Gruppe  $(G, *)$  ist eine Teilmenge  $U$  von  $G$  mit  $e_G \in U$  (für das neutrale Element  $e_G$  von  $(G, *)$ ) sowie  $g * h \in U$  und  $g^{-1} \in U$  für alle  $g, h \in U$ .

- (II) Ein **Unterring**  $U$  eines Rings  $(R, +, \cdot)$  ist eine Untergruppe  $U$  von  $(R, +)$  mit  $1 \in U$  und  $xy \in U$  für alle  $x, y \in U$ .
- (III) Ein **Unterkörper** oder **Teilkörper**  $U$  eines Körpers  $(K, +, \cdot)$  ist ein Unterring  $U$  von  $(K, +, \cdot)$  mit  $x^{-1} \in U$  für alle  $x \in U \setminus \{0\}$ .

**Beispiele** (für algebraische **Unterstrukturen**).

- (1) Für jedes  $n \in \mathbb{N}$  ist  $n\mathbb{Z}$  Untergruppe von  $(\mathbb{Z}, +)$ , aber für  $n \in \mathbb{N} \setminus \{1\}$  wegen  $1 \notin n\mathbb{Z}$  kein Unterring von  $(\mathbb{Z}, +, \cdot)$ .
- (2)  $\mathbb{Z}$  ist Unterring von  $(\mathbb{Q}, +, \cdot)$ , und  $\mathbb{Q}$  ist Unterkörper von  $(\mathbb{R}, +, \cdot)$ .
- (3) Für jedes  $n \in \mathbb{N}$  ist  $A_n$  Untergruppe von  $(S_n, \circ)$ .
- (4) Für eine Gruppe  $(G, *)$  und eine abelsche Gruppe  $(H, \otimes)$  sind  $\text{Aut}(G)$  Untergruppe von  $(\{f \in \text{Abb}(G) \mid f \text{ bijektiv}\}, \circ)$  und  $(\text{Hom}(G, H), *)$  Untergruppe von  $(\text{Abb}(G, H), *)$ .
- (5) Für hier **stets additiv** betrachtete Restklassengruppen kann  $\mathbb{Z}_2$  wegen  $\mathbb{Z}_2 \not\subset \mathbb{Z}_3$ ,  $\mathbb{Z}_2 \not\subset \mathbb{Z}_4$ ,  $\mathbb{Z}_2 \not\subset \mathbb{Z}_2^2$  schon formal keine Untergruppe von  $\mathbb{Z}_3$ ,  $\mathbb{Z}_4$  oder  $\mathbb{Z}_2^2$  sein. Interessanter ist aber, ob die algebraische Struktur von  $\mathbb{Z}_2$  in  $\mathbb{Z}_3$ ,  $\mathbb{Z}_4$  oder  $\mathbb{Z}_2^2$  enthalten ist, ob  $\mathbb{Z}_2$  also zumindest isomorph zu einer Untergruppe ist. Die Antwort lautet, dass  $\mathbb{Z}_2$  *nicht* isomorph zu irgendeiner Untergruppe von  $\mathbb{Z}_3$  ist, aber isomorph zur Untergruppe  $\{[0]_{\mathbb{Z}_4}, [2]_{\mathbb{Z}_4}\}$  von  $\mathbb{Z}_4$  und auch zu jeder der drei Untergruppen  $\{([0]_{\mathbb{Z}_2}, [0]_{\mathbb{Z}_2}), ([0]_{\mathbb{Z}_2}, [1]_{\mathbb{Z}_2})\}$ ,  $\{([0]_{\mathbb{Z}_2}, [0]_{\mathbb{Z}_2}), ([1]_{\mathbb{Z}_2}, [0]_{\mathbb{Z}_2})\}$ ,  $\{([0]_{\mathbb{Z}_2}, [0]_{\mathbb{Z}_2}), ([1]_{\mathbb{Z}_2}, [1]_{\mathbb{Z}_2})\}$  von  $\mathbb{Z}_2^2$  ist.

**Bemerkungen** (zu algebraischen **Unterstrukturen**).

- (1) In jeder Gruppe  $(G, *)$  ist die **triviale Untergruppe**  $\{e_G\}$  die kleinste und ganz  $G$  die größte Untergruppe.  
In jedem Ring  $(R, +, \cdot)$  ist der **Grundring**  $R_0 := \{z_R \mid z \in \mathbb{Z}\}$  der kleinste und ganz  $R$  der größte Unterring. Dabei ist  $R_0$  stets isomorph zu  $\mathbb{Z}$  (wenn  $(R, +, \cdot)$  Charakteristik 0 hat) oder zu  $\mathbb{Z}_n$  (wenn  $(R, +, \cdot)$  Charakteristik  $n \in \mathbb{N}$  hat).  
In jedem Körper  $(K, +, \cdot)$  ist der **Primkörper**  $K_0 := \{z_K \cdot n_K^{-1} \mid n, z \in \mathbb{Z}, n_K \neq 0 \text{ in } K\}$  der kleinste und ganz  $K$  der größte Teilkörper. Dabei ist  $K_0$  stets isomorph zu  $\mathbb{Q}$  (wenn  $(K, +, \cdot)$  Charakteristik 0 hat) oder zu  $\mathbb{F}_p$  (wenn  $(K, +, \cdot)$  Charakteristik  $p \in \mathbb{P}$  hat) ist.
- (2) Dass  $U \subset G$  Untergruppe einer Gruppe  $(G, *)$  ist, ist auch durch  $U \neq \emptyset$  und  $g^{-1} * h \in U$  für alle  $g, h \in U$  charakterisiert. Dass  $U \subset K$  Unterkörper eines Körpers  $(K, +, \cdot)$  ist, ist charakterisiert durch  $U \setminus \{0\} \neq \emptyset$  und  $x - y \in U$  für alle  $x, y \in U$  sowie  $x^{-1}y \in U$  für alle  $x, y \in U \setminus \{0\}$ .
- (3) Die **Terminologie ist sinnvoll**, da mit ihr für eine Untergruppe  $U$  von  $(G, *)$  **auch  $(U, *)$  Gruppe**, für einen Unterring  $U$  von  $(R, +, \cdot)$  **auch  $(U, +, \cdot)$  Ring**, für einen Unterkörper  $U$  von  $(K, +, \cdot)$  **auch  $(U, +, \cdot)$  Körper** ist.
- (4) Man schreibt kurz, dass  $U \subset G$  Untergruppe,  $U \subset R$  Unterring,  $U \subset K$  Unterkörper ist.
- (5) Die definierenden Eigenschaften einer Untergruppe  $U$  von  $(G, *)$  (neben  $e_G \in U$ ) werden auch so ausgedrückt, dass  $U$  **unter** der **Verknüpfung**  $*$  und unter Inversenbildung **abgeschlossen** ist. Analog ist ein Unterring unter Addition, additiver Inversenbildung und Multiplikation abgeschlossen, ein Unterkörper zusätzlich unter multiplikativer Inversenbildung.

**Satz & Definition (erzeugte Unterstrukturen).** Für jede Teilmenge  $A \subset G$  in einer Gruppe  $(G, *)$  gibt es eine bezüglich Mengen-Inklusion kleinste Untergruppe  $U \subset G$  mit  $A \subset U$ . Dieses  $U$  heißt die von  $A$  **erzeugte Untergruppe** und wird mit  $\langle A \rangle$  bezeichnet. Für  $n \in \mathbb{N}$  und  $g_1, g_2, \dots, g_n \in G$  wird  $\langle g_1, g_2, \dots, g_n \rangle := \langle \{g_1, g_2, \dots, g_n\} \rangle$  vereinbart. Analog versteht man **erzeugte Unterringe und Unterkörper**.

*Beweis.* Es ist Existenz von  $U = \langle A \rangle$  zu beweisen. Da es mit  $G$  selbst zumindest eine Untergruppe  $V$  von  $(G, *)$  mit  $A \subset V$  gibt, ist  $\mathcal{S}_A := \{V \subset G \mid V \text{ Untergruppe von } (G, *), A \subset V\}$  nicht leer, und wir können  $U := \bigcap \mathcal{S}_A \subset G$  setzen. Da  $A \cup \{e_G\} \subset U$  gilt und die (Abgeschlossenheits-)Eigenschaften von Untergruppen bei beliebigem Durchschnitt erhalten bleiben, ist  $U \in \mathcal{S}_A$  das gesuchte kleinste Element von  $\mathcal{S}_A$ . Für Unterringe und -körper argumentiert man analog.  $\square$

**Bemerkungen** (zu **Erzeugung** algebraischer (Unter-)Strukturen).

- (1) Der **Beweis besteht aus einem absoluten Standard-Argument**, um die Existenz einer kleinsten (oft von einer Teilmenge erzeugten) Menge mit gewissen Durchschnitts-stabilen Eigenschaften zu begründen. Versionen dieses Arguments werden Sie im Lauf des Studiums an vielen Stellen wiedersehen.
- (2) Ist die von einem einzelnen  $g \in G$  erzeugte Untergruppe  $\langle g \rangle$  in einer Gruppe  $(G, *)$  endlich, so ist  $(\langle g \rangle, *)$  zyklisch von Ordnung  $|\langle g \rangle|$  und hat  $g$  (im für zyklische Gruppen erklärten Sinn) als Erzeuger. Tatsächlich kann eine zyklische Gruppe äquivalent als eine Gruppe  $(G, *)$  definiert werden, für die  $|G| < \infty$  gilt und für die ein einzelnes  $g \in G$  mit  $\langle g \rangle = G$  existiert.

**Beispiele** (zur **Erzeugung** von Unterstrukturen).

- (1) In der additiven Gruppe  $(\mathbb{Z}, +)$  und ist  $\langle x \rangle = x\mathbb{Z}$  für jedes  $x \in \mathbb{Z}$ , im Ring  $(\mathbb{Z}, +, \cdot)$  ist  $\langle x \rangle = \mathbb{Z}$  für jedes  $x \in \mathbb{Z}$  und sogar  $\langle \emptyset \rangle = \mathbb{Z}$  (denn jeder Unterring muss ja 1 enthalten).
- (2) Im Polynomring  $(\mathbb{Z}[X], +, \cdot)$  wird der von  $X^3 \in \mathbb{Z}[X]$  erzeugte Unterring

$$\langle X^3 \rangle = \{a_\ell X^{3\ell} + a_{\ell-1} X^{3(\ell-1)} + \dots + a_1 X^3 + a_0 \mid \ell \in \mathbb{N}_0, a_i \in \mathbb{Z}\}$$

gelegentlich als  $\mathbb{Z}[X^3]$  aufgefasst — wobei, wenn man die Definition über Koeffizientenfolgen genau nimmt,  $\langle X^3 \rangle$  *nur isomorph* zu  $\mathbb{Z}[X^3] = \mathbb{Z}[X]$  ist.

Ein zu Unterstrukturen duales Konzept sind sogenannte Faktorstrukturen, an deren Definition wir uns nun unter Rückgriff auf Quotienten einer Äquivalenzrelation annähern:

**Satz & Definition.** Für jede Untergruppe  $U$  einer Gruppe  $(G, *)$  wird durch

$$x \overset{U}{\sim} y \iff x^{-1} * y \in U \quad \text{für } x, y \in G$$

eine Äquivalenzrelation  $\overset{U}{\sim}$  auf  $G$  definiert, bei der  $|[y]_{\overset{U}{\sim}}| = |[x]_{\overset{U}{\sim}}|$  für alle  $x, y \in G$  gilt, also alle Äquivalenzklassen

$$[x]_{G:U} := [x]_{\overset{U}{\sim}} = x * U$$

mit  $x \in G$  gleiche Kardinalität haben. Wir nennen die Äquivalenzklassen bezüglich  $\overset{U}{\sim}$  auch (Links-) **Nebenklassen** und vereinbaren die Bezeichnung

$$G:U := G/\overset{U}{\sim} = \{[x]_{G:U} \mid x \in G\}$$

für die Quotientenmenge. Insbesondere greift dies bei einem Ring oder Körper  $(R, +, \cdot)$  für jede Untergruppe  $U$  von  $(R, +)$  mit der durch  $x \overset{U}{\sim} y \iff x - y \in U$  gegebenen Äquivalenzrelation.

*Beweis.* Wir verifizieren zunächst die definierenden Eigenschaften der Äquivalenzrelation  $\sim_U$ : Reflexivität liegt vor, weil  $x^{-1} * x = e_G \in U$  für alle  $x \in G$  gilt. Symmetrie ist erfüllt, weil für  $x, y \in G$  aus  $x^{-1} * y \in U$  schon  $y^{-1} * x = (x^{-1} * y)^{-1} \in U$  folgt. Transitivität ergibt sich, weil für  $x, y, z \in G$  aus  $x^{-1} * y \in U$  und  $y^{-1} * z \in U$  auch  $x^{-1} * z = (x^{-1} * y) * (y^{-1} * z) \in U$  folgt.

Die Gleichheit  $[x]_{\sim_U} = x * U$  ergibt sich aus  $x \sim_U y \iff x^{-1} * y \in U \iff y \in x * U$  für  $y \in G$ .

Weiter erhalten wir für feste  $x, y \in G$  durch  $\lambda(z) := y * x^{-1} * z$  für  $z \in G$  eine Abbildung  $\lambda: [x]_{\sim_U} \rightarrow [y]_{\sim_U}$  (denn  $z \in [x]_{\sim_U} = x * U$  impliziert  $y * x^{-1} * z \in y * x^{-1} * x * U = y * U = [y]_{\sim_U}$ ). Analog gibt  $\mu(z) := x * y^{-1} * z$  eine Abbildung  $\mu: [y]_{\sim_U} \rightarrow [x]_{\sim_U}$ , die die Umkehrabbildung zu  $\lambda$  ist. Somit ist  $\lambda$  eine Bijektion  $[x]_{\sim_U} \rightarrow [y]_{\sim_U}$ , und es gilt  $|[y]_{\sim_U}| = |[x]_{\sim_U}|$ .  $\square$

**Bemerkung.** Sei  $U$  eine Untergruppe einer Gruppe  $(G, *)$ . Eine sehr ähnliche Äquivalenzrelation auf  $G$  erhält man durch die Festlegung  $x \sim_{\circ} y \iff y * x^{-1}$  für  $x, y \in G$ . Die Äquivalenzklassen  $[x]_{\sim_{\circ}} = U * x$  von  $\sim_{\circ}$  heißen (Rechts-)Nebenklassen. Sie verhalten sich weitgehend analog zu den Linksnebenklassen, stimmen im nicht-abelschen Fall aber nicht unbedingt mit diesen überein.

Als ein naheliegendes Beispiel für den Nutzen von Nebenklassen beweisen wir den Satz von Lagrange über grundlegende Kennzahlen (die wir vorher noch kurz definieren) von Gruppen, Untergruppen und ihren Elementen:

**Definitionen (Ordnung von Gruppen und Gruppenelementen).**

- (I) Eine Gruppe  $(G, *)$  heißt **endlich**, wenn  $|G| < \infty$  ist, und  $|G| \in \mathbb{N}$  heißt dann die **Ordnung der Gruppe**  $(G, *)$ .
- (II) Die **Ordnung eines Elements**  $g \in G$  in einer Gruppe  $(G, *)$  ist (wenn existent) eine Zahl  $m \in \mathbb{N}$  mit  $g^m = e_G$  und  $g^k \neq e_G$  für alle  $k \in \{1, 2, \dots, m-1\}$  (wobei  $e_G$  das neutrale Element von  $(G, *)$  bezeichnet).

**Satz (von Lagrange).** Für eine endliche Gruppe  $(G, *)$  sind die Ordnungen der Untergruppen von  $G$  und die Ordnungen der Elemente von  $G$  alle Teiler der Ordnung  $|G|$  der Gruppe.

*Beweis.* Sei  $U$  eine Untergruppe von  $(G, *)$ . Nach dem vorigen Satz enthält jede Nebenklasse  $[x]_{G:U} \in G:U$  genau so viele Elemente wie  $U = [e_G]_{G:U} \in G:U$ , es gilt also  $|N| = |U|$  für alle Nebenklassen  $N \in G:U$ . Da  $G$  die disjunkte Vereinigung der  $|G:U|$  Nebenklassen in  $|G:U|$  ist, ergibt sich mit  $|G| = |G:U| |U|$ , dass  $|U|$  ein Teiler von  $|G|$  ist. Dies zeigt die Behauptung über die Ordnungen der Untergruppen.

Ein Element  $g \in G$  hat wegen  $|G| < \infty$  zunächst eine Ordnung  $m \in \mathbb{N}$  (denn andernfalls wäre  $g^k \neq e_G$  für alle  $k \in \mathbb{N}$  und damit wären  $g, g^2, g^3, g^4, g^5, \dots$  unendliche viele verschiedene Elemente von  $G$ ). Nun muss die von  $g$  erzeugte Untergruppe  $\langle g \rangle$  gleich  $\{e_G, g, g^2, g^3, \dots, g^{m-1}\}$  sein und  $|\langle g \rangle| = m$  erfüllen. Nach dem schon Gezeigten ist daher  $m$  ein Teiler von  $|G|$  und auch die Behauptung über die Ordnungen der Elemente verifiziert.  $\square$

**Beispiele (für Ordnungen von Gruppen, Untergruppen und Elementen).** Wir klassifizieren alle Elemente und Untergruppen nach ihrer Ordnung ...

- (1) in der additiven **Restklassengruppe**  $(\mathbb{Z}_{12}, +)$  mit  $|\mathbb{Z}_{12}| = 12$ :

Ordnung	1	2	3	4	6	12
Elemente	$[0]$	$[6]$	$[4], [8]$	$[3], [9]$	$[2], [10]$	$[1], [5], [7], [11]$
Untergruppen	$\{[0]\}$	$\{[0], [6]\}$	$\{[0], [4], [8]\}$	$\langle 3 \rangle = \langle 9 \rangle$	$\langle 2 \rangle = \langle 10 \rangle$	$\langle 1 \rangle = \mathbb{Z}_{12}$

Tatsächlich sind in diesem Beispiel und allgemein in  $(\mathbb{Z}_n, +)$  mit  $n \in \mathbb{N}$  alle Untergruppen zyklisch und jede aufgrund des Satzes von Lagrange zulässige Ordnung wird in  $(\mathbb{Z}_n, +)$  durch genau eine Untergruppe realisiert.

(2) in der **symmetrischen Gruppe**  $(\mathbf{S}_3, \circ)$  mit  $|\mathbf{S}_3| = 6$  (Bezeichnungen aus Abschnitt 3.1):

Ordnung	1	2	3	6
Elemente	id	$\tau_1, \tau_2, \tau_3$	$\sigma_1, \sigma_2$	—
Untergruppen	{id}	$\langle \tau_1 \rangle = \{\text{id}, \tau_1\}, \langle \tau_2 \rangle, \langle \tau_3 \rangle$	$\langle \sigma_1 \rangle = \langle \sigma_2 \rangle = \{\text{id}, \sigma_1, \sigma_2\}$	$\mathbf{S}_3$

In diesem Beispiel sind alle echten Untergruppen (also alle außer  $\mathbf{S}_3$  selbst) zyklisch.

(3) in der **alternierenden Gruppe**  $(\mathbf{A}_4, \circ)$  mit  $|\mathbf{A}_4| = 12$  (Bezeichnungen aus Abschnitt 3.1):

Ordnung	1	2	3	4	6	12
Elemente	id	$\vartheta_1, \vartheta_2, \vartheta_3$	$\eta_1, \eta_2, \eta_3, \eta_4, \eta_5, \eta_6, \eta_7, \eta_8$	—————	—	—
Untergruppen	{id}	$\langle \vartheta_1 \rangle, \langle \vartheta_2 \rangle, \langle \vartheta_3 \rangle$	$\langle \eta_1 \rangle = \langle \eta_2 \rangle, \langle \eta_3 \rangle, \langle \eta_5 \rangle, \langle \eta_7 \rangle$	$\{\text{id}, \vartheta_1, \vartheta_2, \vartheta_3\}$	—	$\mathbf{A}_4$

In diesem Beispiel gibt es keine Untergruppe der aufgrund des Satzes von Lagrange zulässigen Ordnung 6, und neben  $\mathbf{A}_4$  ist auch die echte Untergruppe  $\{\text{id}, \vartheta_1, \vartheta_2, \vartheta_3\}$  nicht zyklisch.

Als interessante Folgerung ergibt sich ein berühmter Grundsatz der Zahlentheorie:

**Korollar (kleiner Satz von Fermat).** Sei  $p \in \mathbb{P}$  eine Primzahl. Dann gelten

$$x^p = x \pmod{p} \quad \text{für alle } x \in \mathbb{Z} \quad \text{und} \quad x^{p-1} = 1 \pmod{p} \quad \text{für alle } x \in \mathbb{Z} \setminus p\mathbb{Z}.$$

**Bemerkung.** Die Behauptung des Satzes kann ganz elementar ohne Modulo-Rechnen zum Beispiel so formuliert werden: Ist  $p \in \mathbb{P}$  eine Primzahl, so ist für jedes  $x \in \mathbb{Z}$  entweder  $x$  oder  $x^{p-1} - 1$  durch  $p$  teilbar.

Der Beweis lässt sich mit den inzwischen erarbeiteten Techniken kurz und sehr elegant führen:

*Beweis des kleinen Satzes von Fermat.* Für  $x \in \mathbb{Z} \setminus p\mathbb{Z}$  ist  $[x]_{\mathbb{Z}_p} \neq [0]_{\mathbb{Z}_p}$  in  $\mathbb{Z}_p$ , womit  $[x]_{\mathbb{Z}_p}$  ein Element der multiplikativen Gruppe  $(\mathbb{Z}_p^\times, \cdot)$  der Ordnung  $|\mathbb{Z}_p^\times| = p-1$  ist. (Dass dies tatsächlich eine Gruppe ist, wurde in Abschnitt 3.1 gezeigt und war nicht ganz einfach. Davon profitieren wir nun.) Nach dem Satz von Lagrange ist die Ordnung  $m \in \mathbb{N}$  von  $[x]_{\mathbb{Z}_p}$  in  $(\mathbb{Z}_p^\times, \cdot)$  ein Teiler von  $p-1$ , also  $p-1 = \ell m$  für ein  $\ell \in \mathbb{N}$ . Es folgt

$$[x^{p-1}]_{\mathbb{Z}_p} = [x]_{\mathbb{Z}_p}^{p-1} = ([x]_{\mathbb{Z}_p}^m)^\ell = [1]_{\mathbb{Z}_p}^\ell = [1]_{\mathbb{Z}_p},$$

was  $x^{p-1} = 1 \pmod{p}$  bedeutet. Dies zeigt die zweite Behauptung. Die erste Behauptung folgt für  $x \in \mathbb{Z} \setminus p\mathbb{Z}$  durch Multiplikation mit  $x$ , gilt für  $x \in p\mathbb{Z}$  mit  $x^p = 0 = x \pmod{p}$  aber ebenfalls.  $\square$

Schließlich möchten wir die Quotientenmenge  $G:U$  beziehungsweise  $R:U$  (die wir für jede (additive) Untergruppe  $U$  bilden können) wieder mit Verknüpfungen versehen und selbst zu einer Gruppe beziehungsweise einem Ring machen. Dafür benötigen wir für  $U$  tatsächlich noch eine etwas andere Struktur:

**Definitionen (Normalteiler und Ideale).**

- (I) Ein **Normalteiler**  $N$  einer Gruppe  $(G, *)$  ist eine Untergruppe  $N$  von  $(G, *)$  mit  $g * N = N * g$  für alle  $g \in G$ .
- (II) Ein **Ideal**  $I$  eines Rings  $(R, +, \cdot)$  ist eine Untergruppe  $U$  von  $(R, +)$  mit  $rI \subset I$  und  $Ir \subset I$  für alle  $r \in R$ .

**Bemerkungen und Beispiele (zu Normalteilern und Idealen).**

- (1) Ein Normalteiler ist also eine Untergruppe, für die die Links- und Rechts-Nebenklassen übereinstimmen, und kann alternativ als Untergruppe  $N$  mit  $g * N * g^{-1} \subset N$  für alle  $g \in G$  charakterisiert werden. **In einer abelschen Gruppe** — und vor an solche denken wir im Folgenden — ist dies immer der Fall, so dass dort die **Normalteiler nichts anderes als Untergruppen** sind.
- (2) Ein Ideal muss 1 nicht enthalten und daher kein Unterring sein, beispielsweise ist  $x\mathbb{Z}$  für jedes  $x \in \mathbb{Z}$  ein Ideal im Ring  $(\mathbb{Z}, +, \cdot)$ , aber nur in den trivialen Fällen  $x \in \{-1, 1\}$  mit  $x\mathbb{Z} = \mathbb{Z}$  ein Unterring in  $(\mathbb{Z}, +, \cdot)$ . Andererseits muss ein Unterring kein Ideal sein, beispielsweise ist  $\mathbb{Z}$  ein Unterring von  $(\mathbb{Q}, +, \cdot)$ , aber kein Ideal in  $(\mathbb{Q}, +, \cdot)$  (denn beispielsweise ist  $\frac{1}{2}\mathbb{Z} \not\subset \mathbb{Z}$ ).
- (3) Analog zu erzeugten Untergruppen/-ringen/-körpern lassen sich der von einer Teilmenge  $A$  **erzeugte Normalteiler** in einer Gruppe und das von einer Teilmenge  $A$  **erzeugte Ideal** in einem Ring definieren. Auch für diese schreibt man manchmal  $\langle A \rangle$ .
- (4) Der **Kern eines Gruppenhomomorphismus**  $\varphi: G \rightarrow H$  zwischen Gruppen  $(G, *)$  und  $(H, \otimes)$  ist **stets ein Normalteiler** in  $(G, *)$ . Der **Kern eines Ringhomomorphismus**  $\psi: R \rightarrow S$  zwischen Ringen  $(R, +, \cdot)$  und  $(S, \oplus, \odot)$  ist **stets ein Ideal** in  $(R, +, \cdot)$ .

(Beweis: Dass die Kerne (additive) Untergruppen sind, sieht man problemlos. Für  $g \in G, n \in \text{Kern}(\varphi)$  ist zudem  $\varphi(g * n * g^{-1}) = \varphi(g) \otimes e_H \otimes \varphi(g)^{-1} = e_H$  und damit  $g * \text{Kern}(\varphi) * g^{-1} \subset \text{Kern}(\varphi)$ . Nach Bemerkung (1) ist also  $\text{Kern}(\varphi)$  ein Normalteiler. Für  $r \in R$  und  $n \in \text{Kern}(\psi)$  ist  $\psi(rn) = \psi(r)0 = 0$  und analog  $\psi(nr) = 0$ . Dies bedeutet  $r \text{Kern}(\psi) \subset \text{Kern}(\psi)$  und  $\text{Kern}(\psi)r \subset \text{Kern}(\psi)$ , so dass  $\text{Kern}(\psi)$  ein Ideal ist.)

**Satz & Definitionen (Faktorgruppen, Faktorringe).**

- (I) Ist  $N$  ein Normalteiler in einer Gruppe  $(G, *)$ , so erhalten wir durch

$$[g]_{G:N} * [h]_{G:N} := [g * h]_{G:N} \quad \text{für } g, h \in G$$

beziehungsweise äquivalent durch

$$(g * N) * (h * N) := (g * h) * N \quad \text{für } g, h \in G$$

eine wohldefinierte Verknüpfung auf  $G : N$ , mit der  $G : N$  zu einer Gruppe wird (abelsch, falls  $(G, *)$  abelsch). Wir schreiben dann  $G/N$  für  $G : N$  und nennen  $(G/N, *)$  die **Faktorgruppe** oder **Quotientengruppe** von  $G$  nach  $N$ .

- (II) Ist  $I$  ein Ideal in einem Ring  $(R, +, \cdot)$ , so erhalten wir durch

$$[r]_{R:I} + [s]_{R:I} := [r + s]_{R:I} \quad \text{und} \quad [r]_{R:I} \cdot [s]_{R:I} := [rs]_{R:I} \quad \text{für } r, s \in R$$

beziehungsweise äquivalent durch

$$(r+I) + (s+I) := (r+s)+I \quad \text{und} \quad (r+I) \cdot (s+I) := (rs)+I \quad \text{für } r, s \in R$$

wohldefinierte Verknüpfungen auf  $R:I$ , mit denen  $R:I$  ein Ring wird (kommutativ, falls  $(R, +, \cdot)$  kommutativ). Wir schreiben dann  $R/I$  für  $R:I$  und nennen  $(R/I, +, \cdot)$  den **Faktorring** oder **Quotientenring** von  $R$  nach  $I$ .

**Beispiel.** Das **wichtigste Beispiel** von Faktorgruppen und Faktorringen sind die **Restklassengruppen/-ringe**  $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ , die wir bereits ausführlich kennengelernt haben. An dieser Stelle können wir sie aber als Spezialfälle einer übergeordneten Theorie verstehen.

**Bemerkung.** Für einen Körper  $(K, +, \cdot)$  kann man zwar  $K:U$  für einen Unterkörper  $U$  betrachten, aber keinen nicht-trivialen „Faktorkörper“ gewinnen. Tatsächlich kommt wie bei Ringen bestenfalls die Faktorisierung nach Idealen in Frage, aber  $\{0\}$  und ganz  $K$  sind die einzigen Ideale von  $(K, +, \cdot)$ , für das eine ist  $K:\{0\}$  nur eine neue Version von  $K$ , für das andere hat  $K:K$  nur ein Element und wird zum Nullring, aber nicht zu einem Körper.

*Zum Beweis des Satzes.* Entscheidend ist der Beweis der Wohldefiniertheit der Verknüpfungen:

Bezüglich Teil (I) verifizieren wir für alternative Repräsentanten  $g' \in [g]_{G:N} = g * N$ ,  $h' \in [h]_{G:N} = h * N$  der Nebenklassen dazu  $g' * h' \in [g * h]_{G:N} = (g * h) * N$  durch die Rechnung

$$g' * h' \in g * N * h * N = g * h * N * N = g * h * N,$$

bei der entscheidend eingeht, dass  $N$  Normalteiler ist.

Bezüglich Teil (II) bemerken wir zunächst, dass die Addition durch Teil (I) abgedeckt ist (da  $I$  als Untergruppe in der *abelschen* Gruppe  $(R, +)$  automatisch Normalteiler ist). Für die Multiplikation betrachten wir  $r' \in [r]_{R:I} = r + I$ ,  $s' \in [s]_{R:I} = s + I$  und bekommen durch die Rechnung

$$r's' \in (r+I) \cdot (s+I) \subset rs + rI + Is + I \cdot I \subset rs + I$$

unter Verwendung der Ideal-Eigenschaft, dass wie benötigt  $r's' \in [rs]_{R:I} = rs + I$  gilt.

Alles Weitere (Assoziativität, Kommutativität, neutrale und inverse Elemente) erhält man problemlos aus den entsprechenden Eigenschaften von  $G$  beziehungsweise  $R$ .  $\square$

Zum Abschluss des Kapitels erwähnen wir die Faktorisierungssätze für Gruppen und für Ringe, bei denen es sich um weitgehende Analoga des Faktorisierungssatzes für Äquivalenzrelationen handelt:

**Satz (Faktorisierungssätze für Gruppen und Ringe).**

(I) Seien  $(G, *)$  und  $(H, \otimes)$  Gruppen,  $N$  ein Normalteiler von  $(G, *)$  und  $\varphi: G \rightarrow H$  ein Gruppenhomomorphismus mit  $N \subset \text{Kern}(\varphi)$ . Dann gibt es genau einen Gruppenhomomorphismus  $\varphi_*: G/N \rightarrow H$ , der  $\varphi_* \circ p = \varphi$  (mit der Quotientenabbildung  $p: G \rightarrow G/N$ ) erfüllt, also nebenstehendes Diagramm kommutativ macht.

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ p \downarrow & \nearrow \varphi_* & \\ G/N & & \end{array}$$

(II) Seien  $(R, +, \cdot)$  und  $(S, \oplus, \odot)$  Ringe,  $I$  ein Ideal von  $(R, +, \cdot)$  und  $\varphi: R \rightarrow S$  ein Ringhomomorphismus mit  $I \subset \text{Kern}(\varphi)$ . Dann gibt es genau einen Ringhomomorphismus  $\varphi_*: R/I \rightarrow S$ , der  $\varphi_* \circ p = \varphi$  (mit der Quotientenabbildung  $p: R \rightarrow R/I$ ) erfüllt, also nebenstehendes Diagramm kommutativ macht.

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ p \downarrow & \nearrow \varphi_* & \\ R/I & & \end{array}$$

**Bemerkung** (zu den **Faktorisierungssätzen**). Gemäß Bemerkung (4) zu Normalteilern und Idealen ist der Satz stets mit  $N = \text{Kern}(\varphi)$  beziehungsweise  $I = \text{Kern}(\varphi)$  anwendbar, und genau in diesem Fall ist  $\varphi_*$  injektiv. Außerdem gilt stets  $\text{Bild}(\varphi_*) = \text{Bild}(\varphi)$ , und insbesondere ist  $\varphi_*$  genau dann surjektiv, wenn  $\varphi$  surjektiv ist.

*Zum Beweis der Faktorisierungssätze.* Die Existenz und Eindeutigkeit einer Abbildung  $\varphi_*$  mit  $\varphi_* \circ \mathfrak{p} = \varphi$  ergibt sich aus dem Satz des Abschnitts 2.3.2 über die Faktorisierung nach einer Äquivalenzrelation, wenn man bedenkt, dass im Gruppenfall (I)

$$x \stackrel{N}{\sim} y \iff y^{-1} * x \in N \implies y^{-1} * x \in \text{Kern}(\varphi) \iff \varphi(y^{-1} * x) = e_G \iff \varphi(x) = \varphi(y)$$

für  $x, y \in N$  und im Ringfall (II)

$$x \stackrel{I}{\sim} y \iff x - y \in I \implies x - y \in \text{Kern}(\varphi) \iff \varphi(x - y) = 0 \iff \varphi(x) = \varphi(y)$$

für  $x, y \in R$  gilt. Gemäß dem vorigen Satz kann zudem  $(G/N, *)$  als Gruppe beziehungsweise  $(R/I, +, \cdot)$  als Ring aufgefasst werden, und es bleibt nur die Homomorphismus-Eigenschaft von  $\varphi_*$  nachzurechnen. Im Gruppenfall (I) gelingt dies mit der Rechnung

$$\varphi_*([g_1]_{G/N} * [g_2]_{G/N}) = \varphi_*([g_1 * g_2]_{G/N}) = \varphi(g_1 * g_2) = \varphi(g_1) \otimes \varphi(g_2) = \varphi_*([g_1]_{G/N}) \otimes \varphi_*([g_2]_{G/N})$$

für  $[g_1]_{G/N}, [g_2]_{G/N} \in G/N$ . Im Ringfall (II) kann man analog vorgehen.  $\square$

# Kapitel 4

## Reelle und komplexe Zahlen

In diesem Kapitel schließen wir die Diskussion der Zahlbereiche ab, indem wir nach  $\mathbb{N}$ ,  $\mathbb{Z}$  und  $\mathbb{Q}$  in Kapitel 2 auch die für die Analysis grundlegenden Bereiche der **reellen Zahlen**  $\mathbb{R}$  und der **komplexen Zahlen**  $\mathbb{C}$  präzise einführen.

### 4.1 Reelle Zahlen

Die Menge  $\mathbb{R}$  der reellen Zahlen kann man sich als die Menge aller **Dezimalzahlen (mit endlich oder unendlich vielen Nachkomma-Stellen)** oder als die Menge aller **Punkte der Zahlengerade** vorstellen. Neben den rationalen Zahlen aus  $\mathbb{Q}$  gehören zu  $\mathbb{R}$  auch sogenannte **irrationale Zahlen** aus  $\mathbb{R} \setminus \mathbb{Q}$  wie zum Beispiel Wurzeln aus ganzen Zahlen, die keine Quadratzahlen sind, Dezimalzahlen mit unendlich vielen nicht-periodischen Nachkommastellen, die Eulersche Zahl  $e$ , die Kreiszahl  $\pi$ , viele aus solchen gebildete algebraische Ausdrücke und überabzählbar viele weitere Zahlen.

Zur präzisen Einführung der reellen Zahlen gibt es verschiedene Möglichkeiten. Hier geben wir zunächst ein Axiomensystem an:

**Axiom (Axiome der reellen Zahlen).** *Es gibt eine Menge  $\mathbb{R}$ , zwei Verknüpfungen  $+$  und  $\cdot$  auf  $\mathbb{R}$  sowie eine Relation  $<$  auf  $\mathbb{R}$  mit folgenden Eigenschaften:*

- **Körperaxiome:** *Mit den beiden Verknüpfungen wird  $(\mathbb{R}, +, \cdot)$  ein Körper.*
- **Anordnungsaxiome:** *Die Relation  $<$  ist eine strikte Totalordnung auf  $\mathbb{R}$  und ist kompatibel mit der Addition  $+$  und der Multiplikation  $\cdot$ , d.h. für alle  $r, x, y \in \mathbb{R}$  gelten*

$$x < y \implies r+x < r+y, \quad 0 < r, x < y \implies r \cdot x < r \cdot y.$$

- **(Metrische) Vollständigkeit:** *Jede Intervallschachtelung in  $\mathbb{R}$  besitzt einen Kern in  $\mathbb{R}$ .*
- **Archimedisches Axiom:** *Für jedes  $x \in \mathbb{R}$  gibt es ein  $n \in \mathbb{N}$  mit  $x < n$ .*

Zu den Axiomen sind noch einige Erläuterungen zu geben und insbesondere die Begriffe der Intervallschachtelung und des Kerns einer solchen überhaupt einmal zu definieren. Wir gehen dies teils direkt, teils aber auch erst weiter hinten in diesem Abschnitt an.

**Bemerkungen** (zu den **Axiomen von  $\mathbb{R}$** ).

- (1) Wie üblich bezeichnen 0 und 1 das Null- und das Einselement des Körpers  $\mathbb{R}$ , und wir verstehen  $n = \sum_{i=1}^n 1 \in \mathbb{R}$  für  $n \in \mathbb{N}$ . Außerdem finden in  $\mathbb{R}$  alle allgemein für Körper besprochenen Regeln, Definitionen und Konventionen Anwendung.

(2) In der Kurzzusammenfassung besagen die Axiome:

$\mathbb{R}$  ist ein **vollständiger, Archimedisch angeordneter Körper**.

(3) Für die **rationalen Zahlen**  $\mathbb{Q}$  sind **alle Axiome außer der Vollständigkeit** erfüllt. **In Vollständigkeit besteht also der entscheidende Unterschied zwischen  $\mathbb{Q}$  und  $\mathbb{R}$ .**

Die komplexen Zahlen  $\mathbb{C}$ , die wir zu Beginn der Mathematik 2 einführen, bilden einen (in geeignetem Sinn) vollständigen Körper, erlauben aber *keine* mit Addition und Multiplikation kompatible Anordnung.

**Definitionen & Folgerungen** (zu/aus den **Anordnungsaxiomen**).

(1) Wir nennen eine Zahl  $x \in \mathbb{R}$  **positiv**, wenn  $0 < x$  gilt, und andernfalls **nichtpositiv**. Analog nennen wir  $x \in \mathbb{R}$  **negativ**, wenn  $x < 0$  gilt, und andernfalls **nichtnegativ**.

(2) Ausgehend von  $<$  können wir wie üblich die nicht-strikte Totalordnung  $\leq$  durch

$$x \leq y \iff (x < y \vee x = y) \quad \text{für } x, y \in \mathbb{R}$$

einführen sowie  $>$  und  $\geq$  als die Umkehrrelationen zu  $<$  und  $\leq$  erklären.

(3) Aus den Anordnungsaxiomen folgen die Regeln (für  $n \in \mathbb{N}$ ,  $r, s, x, y, x_i, y_i \in \mathbb{R}$ )

$$n > 0,$$

$$x \text{ positiv} \iff -x \text{ negativ},$$

$$x^2 \geq 0 \text{ (mit „=“ nur falls } x = 0 \text{)},$$

$$\sum_{i=1}^n x_i^2 \geq 0 \text{ (mit „=“ nur falls alle } x_i = 0 \text{)},$$

$$x_i \leq y_i \text{ für } i \in \{1, 2, \dots, n\} \implies \sum_{i=1}^n x_i \leq \sum_{i=1}^n y_i \text{ (mit „=“ nur falls alle } x_i = y_i \text{)},$$

$$0 < x_i \leq y_i \text{ für } i \in \{1, 2, \dots, n\} \implies \prod_{i=1}^n x_i \leq \prod_{i=1}^n y_i \text{ (mit „=“ nur falls alle } x_i = y_i \text{)},$$

$$x < y, r < 0 \iff r \cdot x > r \cdot y,$$

$$0 < r < s \implies \frac{1}{r} > \frac{1}{s} > 0.$$

Insbesondere ist  $n \neq 0$  für alle  $n \in \mathbb{N}$ , weshalb der Körper  $(\mathbb{R}, +, \cdot)$  der reellen Zahlen Charakteristik 0 hat und sein Primkörper mit dem Körper  $(\mathbb{Q}, +, \cdot)$  der rationalen Zahlen identifiziert werden kann. Wir verstehen daher immer

$$\mathbb{Q} \subset \mathbb{R}.$$

Weiterhin muss man sich **unbedingt merken, dass die Multiplikation mit einem negativen Faktor und die Reziprokenbildung  $\frac{1}{(\cdot)}$  bei positiven Zahlen das Ungleichheitszeichen umkehren**. (Beispiel für letzteres:  $4 < 7$ , aber  $-4 > -7$  und  $\frac{1}{4} > \frac{1}{7}$ .)

(Wir beweisen nicht alle hier genannten Regeln, zeigen aber zwei ganz grundlegende Argumente:

Begründung  $n > 0$ : Wäre  $1 < 0$ , so folgte durch Addition von  $-1$  auch  $0 < -1$ , durch Multiplikation mit  $-1$  dagegen  $-1 < 0$ . Widerspruch! Da somit weder  $1 < 0$  noch  $1 = 0$  gilt, ist zwingend  $1 > 0$ . Durch Addition von  $n-1$  folgt  $n > n-1$  für  $n \in \mathbb{N}$  und mit Transitivität  $n > 0$  für  $n \in \mathbb{N}$ .

Begründung  $x^2 \geq 0$ : Für  $x > 0$  gilt  $x^2 = x \cdot x > 0 \cdot x = 0$  und daher insgesamt  $x^2 > 0$ . Für  $x < 0$  gilt  $x^2 = (-x) \cdot (-x) > 0 \cdot (-x) = 0$  und damit wieder  $x^2 > 0$ . Für  $x = 0$  ist natürlich  $x^2 = 0^2 = 0$ .

Bevor wir nun die restlichen Axiome von  $\mathbb{R}$  genauer besprechen, geben wir erst einige grundlegende Definitionen:

**Definition (erweitere reelle Zahlen).** Die *erweiterten reellen Zahlen* sind

$$\overline{\mathbb{R}} := \mathbb{R} \dot{\cup} \{-\infty, \infty\}$$

mit zusätzlichen Symbolen  $\infty$  (Unendlich) und  $-\infty$  (minus Unendlich). Wir setzen die Relation  $<$  durch die Festlegung  $-\infty < x < \infty$  für alle  $x \in \mathbb{R}$  zu einer strikten Totalordnung auf  $\overline{\mathbb{R}}$  fort.

**Bemerkung (zum Umgang mit  $\pm\infty$ ).** Wie wir in Mathematik 2 sehen, kann man mit  $\infty$  und  $-\infty$  zu einem gewissen Grad rechnen, aber z.B.  $\infty + (-\infty)$  nicht sinnvoll erklären. Daher wird  $\overline{\mathbb{R}}$  nicht zu einem Körper oder überhaupt einer algebraischen Struktur im Sinn des Kapitels 3.

**Definition (Dazwischenliegen und Intervalle).**

(I) Eine Zahl  $x \in \overline{\mathbb{R}}$  liegt zwischen  $r \in \overline{\mathbb{R}}$  und  $s \in \overline{\mathbb{R}}$ , wenn  $r \leq x \leq s$  oder  $s \leq x \leq r$  gilt, und sie **liegt echt zwischen**  $r$  und  $s$ , wenn  $r < x < s$  oder  $s < x < r$  gilt.

(II) Eine Teilmenge  $I \subset \overline{\mathbb{R}}$  heißt ein **Intervall**, wenn  $I$  mit zwei Zahlen stets auch alle zwischen diesen liegenden enthält.

(III) **Spezielle Intervalle** sind

$$\begin{aligned} (a, b) &:= ]a, b[ := \{x \in \overline{\mathbb{R}} \mid a < x < b\} && \text{(offen)}, \\ (a, b] &:= ]a, b] := \{x \in \overline{\mathbb{R}} \mid a < x \leq b\} && \text{(links halboffen)}, \\ [a, b) &:= [a, b[ := \{x \in \overline{\mathbb{R}} \mid a \leq x < b\} && \text{(rechts halboffen)}, \\ [a, b] &:= [a, b] := \{x \in \overline{\mathbb{R}} \mid a \leq x \leq b\} && \text{(abgeschlossen)} \end{aligned}$$

mit **Randpunkten**  $a, b \in \overline{\mathbb{R}}$  (wobei oft nur  $a < b$  bzw.  $a \leq b$  betrachtet wird, da man andernfalls  $\emptyset$  erhält). Intervalle des Typs  $[a, b]$  mit  $a, b \in \mathbb{R}$  nennt man **kompakt**. Wir vereinbaren als naheliegenden Abkürzungen  $\mathbb{R}_{>a} := (a, \infty)$ ,  $\mathbb{R}_{<b} := (-\infty, b)$ ,  $\mathbb{R}_{\geq a} := [a, \infty)$ ,  $\mathbb{R}_{\leq b} := (-\infty, b]$  (und bemerken  $\mathbb{R} = (-\infty, \infty)$ ,  $\overline{\mathbb{R}} = [-\infty, \infty]$ ).

**Bemerkung (zu Intervallen).** Dass die speziellen Intervalle aus Teil (III) der Definition tatsächlich Intervalle sind, verifiziert man problemlos. Demnächst begründen wir außerdem, dass **tatsächlich alle Intervalle** in  $\overline{\mathbb{R}}$  von dieser Form sind.

**Definitionen (Signum und Betrag).**

(I) Die (reelle) **Vorzeichenfunktion** oder (reelle) **Signumfunktion** ist

$$\operatorname{sgn}: \mathbb{R} \rightarrow \mathbb{R}, \quad \operatorname{sgn}(x) := \begin{cases} 1 & \text{falls } x > 0 \\ 0 & \text{falls } x = 0 \\ -1 & \text{falls } x < 0 \end{cases} \quad \text{für } x \in \mathbb{R}$$

mit  $\operatorname{Bild}(\operatorname{sgn}) = \{-1, 0, 1\}$ .

(II) Die (reelle) **Betragsfunktion** ist

$$|\cdot|: \mathbb{R} \rightarrow \mathbb{R}, \quad |x| := \begin{cases} x & \text{falls } x \geq 0 \\ -x & \text{falls } x \leq 0 \end{cases} \quad \text{für } x \in \mathbb{R}$$

mit  $\operatorname{Bild}(|\cdot|) = \mathbb{R}_{\geq 0}$ .

**Bemerkungen (zu Signum und Betrag).** Seien  $x, y \in \mathbb{R}$ .

(1) Man kann den **Betrag**  $|x|$  als den **Abstand** von  $x$  **von 0 auf der Zahlengerade** und  $|y-x|$  als den Abstand von  $y$  von  $x$  auf den Zahlengerade interpretieren.

(2) Aus den Definitionen ergeben sich die Rechenregeln

$$\begin{aligned} x &= \operatorname{sgn}(x)|x|, & \operatorname{sgn}(xy) &= \operatorname{sgn}(x)\operatorname{sgn}(y) \stackrel{y \neq 0}{=} \operatorname{sgn}\left(\frac{x}{y}\right), & x^2 &= |x|^2, \\ |x| &= |y| \iff (x = y \vee x = -y), & |x| &\leq y \iff x \in [-y, y]. \end{aligned}$$

**Beispiel (zum Auflösen von (Un-)Gleichungen mit Beträgen).** Das Auflösen von (Un-)Gleichungen mit Beträgen gelingt oft mit Fallunterscheidungen. Ein konkretes Beispiel ist die Ungleichung

$$\frac{1}{|x|} \geq \frac{1}{1-x} \quad \text{für } x \in \mathbb{R} \setminus \{0, 1\},$$

bei der die Unterscheidung folgender 3 Fälle sinnvoll ist:

- Fall  $x < 0$ : Wir multiplizieren mit  $-x = |x| > 0$  und  $1-x > 0$  und erhalten als äquivalente Ungleichung erst  $1-x \geq -x$ , dann  $1 \geq 0$ , was generell erfüllt ist.
- Fall  $0 < x < 1$ : Wir multiplizieren mit  $x = |x| > 0$  und  $1-x > 0$  und erhalten als äquivalente Ungleichung erst  $1-x \geq x$ , dann  $x \leq \frac{1}{2}$ .
- Fall  $x > 1$ : Wir multiplizieren mit  $x = |x| > 0$  und  $1-x < 0$  (Achtung, negativer Faktor!) und erhalten als äquivalente Ungleichung erst  $1-x \leq x$ , dann  $x \geq \frac{1}{2}$ .

Zusammenfassend ist damit  $(-\infty, 0) \dot{\cup} (0, \frac{1}{2}] \dot{\cup} (1, \infty)$  die Lösungsmenge der obigen Ungleichung.

Nun kommen wir zurück zu den noch nicht genauer diskutierten Axiomen von  $\mathbb{R}$ , dem Archimedischen Axiom und dem Vollständigkeitsaxiom:

**Bemerkungen** (zum **Archimedischen Axiom**).

- (1) Das Archimedische Axiom sichert unter anderem die Möglichkeit der **Division mit Rest**: Für  $x \in \mathbb{R}$ ,  $q \in \mathbb{R}_{>0}$  existiert stets eine eindeutige Darstellung  $x = sq+r$  mit  $s \in \mathbb{Z}$ ,  $r \in [0, q)$ . Speziell für  $q = 1$  ist  $s \in \mathbb{Z}$  mit  $x \in [s, s+1)$  der in Abschnitt 2.3 erwähnte ganzzahlige Anteil, der mit der Gauß-Klammer als  $\lfloor x \rfloor \in \mathbb{Z}$  notiert wird.

(Begründung für Existenz von  $r, s$ : Gemäß dem Archimedischen Axiom ist  $T_{x,q} := \{z \in \mathbb{Z} \mid z > q^{-1}x\}$  nicht leer und hat eine untere Schranke in  $\mathbb{Z}$ . Nach Abschnitt 2.3.1 enthält dann  $T_{x,q} \subset \mathbb{Z}$  eine kleinste Zahl  $t$ , für  $s := t-1 \in \mathbb{Z}$  gilt  $sq \leq x < (s+1)q$ , und für  $r := x-sq \in [0, q)$  erhalten wir  $x = sq+r$ .

Begründung für Eindeutigkeit von  $r, s$ : Sei  $\tilde{s}q+\tilde{r} = sq+r$  mit  $s, \tilde{s} \in \mathbb{Z}$ ,  $r, \tilde{r} \in [0, q)$ . Im Fall  $\tilde{s} > s$  ist  $\tilde{s} \geq s+1$ , und es ergibt sich mit  $q \leq (\tilde{s}-s)q = r-\tilde{r} \leq r < q$  ein Widerspruch. Im Fall  $\tilde{s} < s$  folgt dieser analog. Also muss  $\tilde{s} = s$  und dann auch  $\tilde{r} = r$  sein.)

- (2) Aus dem Archimedischen Axiom folgt, das **zu jedem**  $\varepsilon \in \mathbb{R}_{>0}$  („wie klein es auch immer sein mag, so lange es nur positiv ist“) **ein**  $n \in \mathbb{N}$  **mit**  $\frac{1}{n} < \varepsilon$  **existiert**.

(Begründung: Nach dem Axiom gibt es  $n \in \mathbb{N}$  mit  $n > \frac{1}{\varepsilon} > 0$ . Durch Reziprokenbildung folgt  $\frac{1}{n} < \varepsilon$ .)

- (3) Als weitere Folgerung ergibt sich, dass  $\mathbb{R}$  **dicht geordnet** ist, das heißt, echt **zwischen zwei verschiedenen reellen Zahlen** liegen unendlich viele weitere reelle Zahlen. Tatsächlich finden im Zwischenbereich **immer sowohl unendlich viele rationale Zahlen** aus  $\mathbb{Q}$  **als auch unendlich viele irrationale Zahlen** aus  $\mathbb{R} \setminus \mathbb{Q}$ , weshalb auch  $\mathbb{Q}$  und  $\mathbb{R} \setminus \mathbb{Q}$  dicht geordnet sind. Mit etwas anderen Worten enthalten für  $a, b \in \mathbb{R}$  mit  $a < b$  sowohl  $(a, b) \cap \mathbb{Q}$  als auch  $(a, b) \setminus \mathbb{Q}$  stets unendlich viele Elemente.

(Begründung: Für beliebiges  $k \in \mathbb{N}$  gibt es nach Bemerkung (2) stets ein  $n \in \mathbb{N}$  mit  $\frac{k}{n} < b-a$ . Nach Bemerkung (1) können wir  $a = \frac{s}{n}+r$  mit  $s \in \mathbb{Z}$  und  $r \in [0, \frac{1}{n})$  schreiben. Damit liegen die  $k$  rationalen Zahlen  $\frac{s+1}{n}, \frac{s+2}{n}, \dots, \frac{s+k}{n}$  alle in  $(a, b) \cap \mathbb{Q}$  (denn  $\frac{s+1}{n} = \frac{s}{n} + \frac{1}{n} > \frac{s}{n} + r = a$  und  $\frac{s+k}{n} = \frac{s}{n} + \frac{k}{n} < \frac{s}{n} + r + b - a = b$ ). Da  $k$  beliebig war, enthält  $(a, b) \cap \mathbb{Q}$  also unendlich viele Zahlen.

Um dasselbe für  $(a, b) \setminus \mathbb{Q}$  zu zeigen, setzen wir voraus, dass es überhaupt eine irrationale Zahl  $t \in \mathbb{R}$  gibt (Beispiele folgen in Mathematik 2), und können dann auch  $t > 0$  annehmen. Wir argumentieren nun wie zuvor, wählen zu  $k \in \mathbb{N}$  ein  $n \in \mathbb{N}$  mit  $\frac{k}{n}t < b-a$ , schreiben  $a = \frac{s}{n}t+r$  mit  $s \in \mathbb{Z}$ ,  $r \in [0, \frac{1}{n}t)$  und erhalten die  $k$  irrationalen Zahlen  $\frac{s+1}{n}t, \frac{s+2}{n}t, \dots, \frac{s+k}{n}t$  in  $(a, b) \setminus \mathbb{Q}$ .)

**Definition (Intervallschachtelungen).** Eine **Intervallschachtelung** in  $\mathbb{R}$  ist eine unendliche Folge nicht-leerer kompakter Intervalle

$$[a_1, b_1] \supset [a_2, b_2] \supset [a_3, b_3] \supset [a_4, b_4] \supset \dots$$

mit Randpunkten  $-\infty < a_1 \leq a_2 \leq a_3 \leq a_4 \leq \dots \leq b_4 \leq b_3 \leq b_2 \leq b_1 < \infty$ , so dass zu jedem  $\varepsilon \in \mathbb{R}_{>0}$  ein  $n \in \mathbb{N}$  mit  $b_n - a_n < \varepsilon$  existiert (wobei man die letzte Bedingung in Worten so ausdrücken kann, dass die Intervall-Längen  $b_n - a_n$  mit wachsendem  $n \in \mathbb{N}$  beliebig klein werden). Als **Kern einer solchen Intervallschachtelung** bezeichnet man die (stets eindeutige) Zahl  $c \in \mathbb{R}$  mit  $c \in [a_n, b_n]$  für alle  $n \in \mathbb{N}$ .

*Begründung zur Eindeutigkeit des Kerns.* Sind  $c, \tilde{c} \in \mathbb{R}$  zwei Kerne, so gilt mit  $c, \tilde{c} \in [a_n, b_n]$  auch  $|\tilde{c}-c| \leq b_n - a_n$  für alle  $n \in \mathbb{N}$ . Wäre  $|\tilde{c}-c| > 0$ , so gäbe es ein  $n \in \mathbb{N}$  mit  $b_n - a_n < |\tilde{c}-c|$ , und wir erhielten einen Widerspruch. Also muss  $|\tilde{c}-c| = 0$  gelten, was  $\tilde{c} = c$  bedeutet.  $\square$

**Bemerkungen** (zum Axiom der metrischen Vollständigkeit).

- (1) Erst mit der gerade gegebenen Definition wird das **Axiom der metrischen Vollständigkeit** „Jede Intervallschachtelung in  $\mathbb{R}$  besitzt einen Kern in  $\mathbb{R}$ .“ sinnvoll. Die **anschauliche Interpretation** des Axioms ist, **dass die reellen Zahlen  $\mathbb{R}$  anders als die rationalen Zahlen  $\mathbb{Q}$  die gesamte Zahlengerade füllen und keine „Lücken“ mehr lassen.**

Konkret ist zum Beispiel  $\sqrt{2} = 1,4142135623\dots$  in  $\mathbb{R}$  der Kern der Intervallschachtelung  $[\frac{14}{10}, \frac{15}{10}] \supset [\frac{141}{100}, \frac{142}{100}] \supset [\frac{1414}{1000}, \frac{1415}{1000}] \supset [\frac{14142}{10000}, \frac{14143}{10000}] \supset \dots$  (wobei die Randpunkte allgemein als  $a_n := 10^{-n} \lfloor 10^n \sqrt{2} \rfloor \in \mathbb{Q}$  und  $b_n := a_n + 10^{-n} \in \mathbb{Q}$  geschrieben werden können). Da aber  $\sqrt{2} \notin \mathbb{Q}$  irrational ist (dazu in Mathematik 2 nochmal genauer), kommt  $\sqrt{2}$  als Kern in  $\mathbb{Q}$  nicht in Frage, und in  $\mathbb{Q}$  besitzt diese Intervallschachtelung eben keinen Kern.

- (2) Mit einem erst später eingeführten Konzept lässt sich metrische Vollständigkeit von  $\mathbb{R}$  so charakterisieren: Jede Cauchy-Folge in  $\mathbb{R}$  konvergiert in  $\mathbb{R}$ . (Für  $\mathbb{C}$  geht dies auch.)

Weitere Begriffe, die mit der Anordnung von  $\mathbb{R}$  zusammenhängen, sind:

**Definitionen (Beschränktheit, Maximum/Minimum, Supremum/Infimum).** Sei  $A$  eine Teilmenge von  $\overline{\mathbb{R}}$ .

- (I) Wir nennen  $A$  **von oben beschränkt** beziehungsweise **von unten beschränkt**, wenn  $A$  eine obere Schranke beziehungsweise untere Schranke in  $\mathbb{R}$  besitzt. Ist  $A$  von oben und unten beschränkt, so heißt  $A$  **beschränkt**.
- (II) Ein größtes Element bzw. kleinstes Element<sup>1</sup> von  $A$  nennt man auch **Maximum** bzw. **Minimum** von  $A$  und schreibt für dieses  $\max A = \max_{x \in A} x$  bzw.  $\min A = \min_{x \in A} x$ .
- (III) Eine kleinste obere Schranke bzw. größte untere Schranke für  $A$  in  $\overline{\mathbb{R}}$  bezeichnet man als **Supremum** bzw. **Infimum** von  $A$  und notiert diese als  $\sup A = \sup_{x \in A} x$  bzw. als  $\inf A = \inf_{x \in A} x$ .

Damit können wir eine etwas andere Vollständigkeitseigenschaft von  $\mathbb{R}$  formulieren:

**Satz (Ordnungs-Vollständigkeit von  $\mathbb{R}$ ).** Jede nicht-leere, von oben beschränkte Teilmenge von  $\mathbb{R}$  besitzt ein Supremum in  $\mathbb{R}$ .

**Bemerkungen** (zur Ordnungs-Vollständigkeit).

- (1) Als Folgerung besitzt *sogar jede* Teilmenge  $A \subset \overline{\mathbb{R}}$  ein Supremum in  $\overline{\mathbb{R}}$ , wobei  $\sup A = \infty$  genau für von oben unbeschränktes  $A$  und  $\sup A = -\infty$  genau für  $A = \emptyset$  und für  $A = \{-\infty\}$  eintritt.
- (2) Für  $A \subset \overline{\mathbb{R}}$  und  $M \in \overline{\mathbb{R}}$  ergibt sich folgende **Charakterisierung des Supremums**:

$$M = \sup A \iff \underbrace{(\forall x \in A: x \leq M)}_{M \text{ obere Schranke für } A} \text{ und } \forall L \in (-\infty, M): \underbrace{\exists y \in A: y > L}_{L \text{ keine obere Schranke für } A}$$

Diese Charakterisierung wird in Anwendungen des Öfteren benutzt.

<sup>1</sup>Da  $\mathbb{R}$  total geordnet ist, fallen größte bzw. kleinste Elemente hier mit maximalen bzw. minimalen Elementen zusammen; vergleiche mit Abschnitt 2.3.2.

- (3) Für  $A \subset \overline{\mathbb{R}}$  existiert  $\max A$  genau dann, wenn  $\sup A \in A$  gilt, und in diesem Fall ist  $\sup A = \max A \in A$ . (Auch  $\sup A \notin A$  kommt aber natürlich vor.)
- (4) Analoges gilt/folgt selbstverständlich für das Infimum (und das Minimum).
- (5) Aus dem Axiom folgt die Behauptung, **dass die speziellen Intervalle** aus Teil (III) der Intervalldefinition **alle Intervalle**  $I$  in  $\overline{\mathbb{R}}$  sind. Um dies einzusehen, nimmt man  $I \neq \emptyset$  an, erklärt  $a := \inf I \in [-\infty, \infty)$ ,  $b := \sup I \in (-\infty, \infty]$  und überlegt sich dann, dass  $I \in \{(a, b), (a, b], [a, b), [a, b]\}$  gilt.
- (6) Mit erst später eingeführten Konzepten lässt sich Ordnungs-Vollständigkeit von  $\mathbb{R}$  so charakterisieren: Jede beschränkte, monotone Folge in  $\mathbb{R}$  konvergiert in  $\mathbb{R}$ .

*Beweis des Satzes.* Sei  $A$  nicht-leere, von oben beschränkte Teilmenge von  $\mathbb{R}$ . Für fixiertes  $n \in \mathbb{N}$  betrachten wir obere Schranken für  $A$  der Form<sup>2</sup>  $\frac{z}{2^n}$  mit  $z \in \mathbb{Z}$ . Wegen der Beschränktheitsvoraussetzung besitzt  $A$  eine obere Schranke, gemäß dem Archimedischen Axiom dann auch eine obere Schranke der gegebenen Form und wegen der (Wohl-)Ordnungseigenschaften von  $\mathbb{Z}$  schließlich eine kleinste Schranke  $b_n$  der gegebenen Form. Setzen wir  $a_n := b_n - \frac{1}{2^n}$ , so ist insgesamt durch die Intervalle  $[a_n, b_n]$  mit  $n \in \mathbb{N}$  eine Intervallschachtelung gegeben, wobei  $b_n - a_n = \frac{1}{2^n} \leq \frac{1}{n}$  auch wieder wegen des Archimedischen Axioms für ein  $n \in \mathbb{N}$  kleiner als jedes gegebene  $\varepsilon \in \mathbb{R}_{>0}$  wird. Nach dem Axiom der metrischen Vollständigkeit besitzt die Intervallschachtelung einen Kern  $M \in \mathbb{R}$ . Jedes  $x \in A$  erfüllt nun  $x \leq b_n \leq M + \frac{1}{n}$  für alle  $n \in \mathbb{N}$ , also gilt auch  $x \leq M$ , und  $M$  ist eine obere Schranke für  $A$ . Außerdem gibt es zu jedem  $n \in \mathbb{N}$  ein  $y \in A$  mit  $y > a_n$  und folglich  $y > M - \frac{1}{n}$ , so dass  $M$  das Supremum von  $A$  sein muss.  $\square$

**Bemerkung** (zur **Äquivalenz der Vollständigkeitsbegriffe**). Tatsächlich ist Ordnungs-Vollständigkeit von  $\mathbb{R}$  unter Voraussetzung der Körper- und Anordnungsaxiome sogar äquivalent zur metrischen Vollständigkeit von  $\mathbb{R}$  zusammen mit dem Archimedischen Axiom. Daher besteht ein äquivalentes Axiomensystem für  $\mathbb{R}$  aus den Körperaxiomen, den Anordnungsaxiomen und der Ordnungs-Vollständigkeit.

*Beweis dieser Äquivalenz.* Dass metrische Vollständigkeit und das Archimedische Axiome Ordnungs-Vollständigkeit implizieren, zeigt der vorausgehende Beweis.

Für den Umkehrschluss sei Ordnungs-Vollständigkeit von  $\mathbb{R}$  vorausgesetzt. Ist  $([a_n, b_n])_{n \in \mathbb{N}}$  eine Intervallschachtelung in  $\mathbb{R}$ , so existiert  $c := \sup\{a_n \mid n \in \mathbb{N}\} \in \mathbb{R}$ , und für alle  $n \in \mathbb{N}$  gelten  $a_n \leq c$  und  $c \leq b_n$  (da  $b_n$  eine obere Schranke und  $c$  die kleinste obere Schranke für  $\{a_n \mid n \in \mathbb{N}\}$  ist). Damit ist  $c$  der Kern der Intervallschachtelung, und metrische Vollständigkeit von  $\mathbb{R}$  ist nachgewiesen. Das Archimedische Axiome erhält man durch ein Widerspruchsargument. Wäre das Axiom nicht erfüllt, so gäbe es ein  $x \in \mathbb{R}$  mit  $n \leq x$  für alle  $n \in \mathbb{N}$ . Damit wäre  $\mathbb{N}$  von oben beschränkt,  $M := \sup \mathbb{N} \in \mathbb{R}$  wäre die kleinste obere Schranke und  $M-1$  keine obere Schranke für  $\mathbb{N}$ . Es gäbe ein  $n_0 \in \mathbb{N}$  mit  $n_0 > M-1$ , und  $\mathbb{N} \ni n_0+1 > M$  stünde im Widerspruch zur Wahl von  $M$  als obere Schranke für  $\mathbb{N}$ . Es folgt die Gültigkeit des Archimedischen Axioms.  $\square$

Um die Mathematik — wie in Abschnitt 1.4 angekündigt — einzig auf das Zermelo-Fraenkel-Axiomensystem der Mengenlehre zu gründen, bleibt aber dennoch eine **Konstruktion des Zahlbereichs**  $\mathbb{R}$  auf Grundlage bereits eingeführter Bildungen anzugeben. Hierzu gibt es mehrere Möglichkeiten. Eine recht elementare Vorgehensweise geht vom bereits eingeführten Zahlbereich  $\mathbb{Q}$  aus und basiert auf der Verwendung sogenannter **Dedekindscher Schnitte**. Die Grundidee ist dabei, eine reelle Zahl  $x \in \mathbb{R}$  mit der Teilmenge  $\mathbb{Q}_{<x} := \{a \in \mathbb{Q} \mid a < x\}$  von  $\mathbb{Q}$  zu identifizieren. Mit der Teilmenge verbindet man gedanklich die Zerlegung  $\mathbb{Q} = \mathbb{Q}_{<x} \cup \mathbb{Q}_{\geq x}$ ,

<sup>2</sup>Mit Schranken der einfacheren Form  $\frac{z}{n}$  können wir hier nicht (ohne Weiteres) arbeiten, da sich nicht immer eine Intervallschachtelung ergäbe. Zum Beispiel für  $A = \{\frac{2}{3}\}$  bekämen wir nämlich  $[a_2, b_2] = [0, \frac{1}{2}] \not\supseteq [a_3, b_3] = [\frac{1}{3}, \frac{2}{3}]$ .

an der man insbesondere die „Schnittstelle“  $x$  ablesen kann. Als formale Konstruktion führt man  $\mathbb{R}$  daher als Menge von Teilmengen von  $\mathbb{Q}$  ein, die die charakteristischen Eigenschaften der gerade besprochenen Mengen  $\mathbb{Q}_{<x}$  aufweisen: Tatsächlich setzt man

$$\mathbb{R} := \left\{ A \in \mathcal{P}(\mathbb{Q}) \left| \begin{array}{l} \emptyset \neq A \neq \mathbb{Q} \\ \forall a \in A: \forall b \in \mathbb{Q} \setminus A: a < b \\ \text{Es gibt keine größte Zahl in } A. \end{array} \right. \right\}$$

und versteht dann  $\mathbb{Q} \subset \mathbb{R}$ , indem man  $q \in \mathbb{Q}$  mit  $\mathbb{Q}_{<q} \in \mathbb{R}$  identifiziert. Auf dem so definierten Bereich der reellen Zahlen erhält man nun die Kleiner-Relation  $<$  als die strikte Mengen-Inklusion  $\subsetneq$  und die Addition  $+$  als die Minkowski-Addition  $+$ . Die Multiplikation  $\cdot$  von  $A, B \in \mathbb{R}$  kann man im Fall  $A, B \geq 0$  durch  $A \cdot B := (A_{>0} \cdot B_{>0}) \cup \mathbb{Q}_{\leq 0}$  erklären, wobei  $\cdot$  auf der rechten Seite für die auf Mengen erweiterte Multiplikation (vgl. Abschnitt 3.1) steht und wir  $A_{>0} := \{a \in A \mid a > 0\}$  abgekürzt haben. Die Multiplikation mit negativen reellen Zahlen lässt sich (im Fortgang der Argumentation mit Hilfe des additiv Inversen) darauf zurückführen. Ausgehend von diesen Definitionen gilt es nun, die zuvor angegebenen Axiome von  $\mathbb{R}$  zu verifizieren, was etwas Aufwand erfordert und hier nicht weiter besprochen wird. Neben der Zurückführung auf die Mengenlehre erreicht man mit dieser Konstruktion übrigens auch den Nachweis, dass das für  $\mathbb{R}$  angegebene Axiomensystem widerspruchsfrei ist — jedenfalls, sofern das Zermelo-Fraenkel-Axiomensystem dies ist.

Als weiterführende Zusatz-Information sei noch erwähnt, dass sich in Anlehnung an die Konstruktion mittels Dedekindscher Schnitte auch folgende Eindeigkeitseigenschaft der reellen Zahlen nachweisen lässt:

**Satz ((strukturelle) Eindeutigkeit von  $\mathbb{R}$ ).** *Erfüllen zwei Mengen  $\mathbb{R}$  (mit  $+, \cdot, <$ ) und  $\tilde{\mathbb{R}}$  (mit  $\tilde{+}, \tilde{\cdot}, \tilde{<}$ ) alle Axiome der reellen Zahlen, so gibt es einen Körperisomorphismus  $\psi: \mathbb{R} \rightarrow \tilde{\mathbb{R}}$ , der zudem im Sinn von  $x < y \implies \psi(x) \tilde{<} \psi(y)$  für alle  $x, y \in \mathbb{R}$  Ordnung-erhaltend ist.*

*Beweisskizze.* Man betrachtet zunächst die Primkörper  $\mathbb{Q}$  und  $\tilde{\mathbb{Q}}$  von  $\mathbb{R}$  und  $\tilde{\mathbb{R}}$ , die beide den rationalen Zahlen entsprechen und somit durch einen Körperisomorphismus  $\varphi: \mathbb{Q} \rightarrow \tilde{\mathbb{Q}}$  identifiziert werden können. Mit den Anordnungsaxiomen kann gezeigt werden, dass  $\varphi$  (wie auch  $\varphi^{-1}$ ) Ordnung-erhaltend ist. Insbesondere ist daher für jedes  $x \in \mathbb{R}$  das Bild  $\varphi(\mathbb{Q}_{<x}) \subset \tilde{\mathbb{R}}$  der nicht-leeren, von oben beschränkten Menge  $\mathbb{Q}_{<x} \subset \mathbb{R}$  ebenfalls nicht-leer und von oben beschränkt. Gemäß der Ordnungs-Vollständigkeit von  $\tilde{\mathbb{R}}$  (deren Äquivalenz zur metrischen Vollständigkeit und dem Archimedischen Axiom ja schon diskutiert wurde) existiert dann für alle  $x \in \mathbb{R}$  das Supremum  $\widetilde{\sup} \varphi(\mathbb{Q}_{<x})$  in  $\tilde{\mathbb{R}}$ , und es lässt sich eine Abbildung  $\psi: \mathbb{R} \rightarrow \tilde{\mathbb{R}}$  durch  $\psi(x) := \widetilde{\sup} \varphi(\mathbb{Q}_{<x})$  für  $x \in \mathbb{R}$  definieren.

Die benötigten Eigenschaften von  $\psi$  verifiziert man in mehreren Schritten.

Um zunächst einzusehen, dass  $\psi$  ein Körperhomomorphismus ist, kann man für  $x, y \in \mathbb{R}$  von  $\mathbb{Q}_{<x+y} = \mathbb{Q}_{<x} + \mathbb{Q}_{<y}$  ausgehen und erhält  $\psi(x+y) = \widetilde{\sup} \varphi(\mathbb{Q}_{<x} + \mathbb{Q}_{<y}) = \widetilde{\sup} [\varphi(\mathbb{Q}_{<x}) + \varphi(\mathbb{Q}_{<y})] = \widetilde{\sup} \varphi(\mathbb{Q}_{<x}) + \widetilde{\sup} \varphi(\mathbb{Q}_{<y}) = \psi(x) + \psi(y)$ . Für die Multiplikation lässt sich ähnlich (aber mit Fallunterscheidung nach den Vorzeichen von  $x$  und  $y$ ) argumentieren.

Dass  $\psi$  Ordnung-erhaltend und damit insbesondere injektiv ist, erhält man wie folgt: Für  $x, y \in \mathbb{R}$  mit  $x < y$  gibt es wegen der dichten Anordnung von  $\mathbb{Q}$  in  $\mathbb{R}$  rationale Zwischenstellen  $p, q \in \mathbb{Q}$  mit  $x < p < q < y$ . Aus der Definition des Supremums und der Ordnung-Erhaltung unter  $\varphi$  ergibt sich dann  $\widetilde{\sup} \varphi(\mathbb{Q}_{<x}) \leq \varphi(p) < \varphi(q) \leq \widetilde{\sup} \varphi(\mathbb{Q}_{<y})$ , also wie benötigt  $\psi(x) \tilde{<} \psi(y)$ .

Um den Beweis der Surjektivität von  $\psi$  vorzubereiten, weist man zunächst  $\psi(q) = \varphi(q)$  für  $q \in \mathbb{Q}$  nach, mit anderen Worten also  $\varphi(q) = \widetilde{\sup} \varphi(\mathbb{Q}_{<q})$ . Dass es sich bei  $\varphi(q)$  um eine obere Schranke für  $\varphi(\mathbb{Q}_{<q})$  handelt, folgt aus der Ordnung-Erhaltung. Gäbe es noch eine kleinere obere Schranke für  $\varphi(\mathbb{Q}_{<q})$ , so könnte diese wegen der dichten Anordnung als  $\eta \in \tilde{\mathbb{Q}}$  mit  $\eta \tilde{<} \varphi(q)$  gewählt werden. Es ergäbe sich der Widerspruch, dass  $\varphi^{-1}(\eta) < q$ , aber  $\varphi^{-1}(\eta)$  obere Schranke für  $\mathbb{Q}_{<q}$  wäre. Also ist  $\varphi(q) = \widetilde{\sup} \varphi(\mathbb{Q}_{<q})$ .

Als weitere Vorbereitung zeigt man mit ähnlicher Argumentation  $\psi(\sup A) = \widetilde{\sup} \varphi(A)$  für nicht-leere, von oben beschränkte  $A \subset \mathbb{Q}$ . Direkt sieht man wieder, dass  $\psi(\sup A)$  obere Schranke für  $\varphi(A) = \psi(A)$  ist. Gäbe es eine kleinere obere Schranke, so könnte diese als  $\eta \in \tilde{\mathbb{Q}}$  mit  $\eta \tilde{<} \psi(\sup A)$  gewählt werden. Nun wäre  $\varphi^{-1}(\eta) < \sup A$  (denn mit  $\varphi^{-1}(\eta) \geq \sup A$  müsste auch  $\eta = \varphi(\varphi^{-1}(\eta)) = \psi(\sup A)$  gelten) und  $\varphi^{-1}(\eta)$  wäre kleinere obere Schranke für  $A$  als  $\sup A$ . In Anbetracht dieses Widerspruchs gilt wie behauptet  $\psi(\sup A) = \widetilde{\sup} \varphi(A)$ .

Schließlich lässt sich die Surjektivität von  $\psi$  beweisen. Sei dazu  $\alpha \in \tilde{\mathbb{R}}$  beliebig. Die schon bei der Definition von  $\psi$  angestellten Überlegungen liefern dann die Existenz von  $x := \sup \varphi^{-1}(\tilde{\mathbb{Q}}_{<\alpha}) \in \mathbb{R}$ , und mit den zuletzt nachgewiesenen Eigenschaften folgt  $\psi(x) = \psi(\sup \varphi^{-1}(\tilde{\mathbb{Q}}_{<\alpha})) = \sup \psi(\varphi^{-1}(\tilde{\mathbb{Q}}_{<\alpha})) = \sup \varphi(\varphi^{-1}(\tilde{\mathbb{Q}}_{<\alpha})) = \sup \tilde{\mathbb{Q}}_{<\alpha} = \alpha$ .

Insgesamt ist  $\psi: \mathbb{R} \rightarrow \tilde{\mathbb{R}}$  Ordnung-erhaltender Körperisomorphismus.  $\square$

ENDE DER MATHEMATIK 1!

KAPITEL 4 ZU REELLEN UND KOMPLEXEN ZAHLEN WIRD IN MATHEMATIK 2 FORTGESETZT.

# Literaturverzeichnis

Die Themen der Vorlesung werden in einer Vielzahl von Büchern behandelt, von denen hier einige aufgelistet werden. Abgesehen von [2, 5, 11, 17] und den fachdidaktischen Büchern [9, 10] handelt es sich dabei um bekannte fachwissenschaftliche Standardwerke entweder zur Analysis oder zur linearen Algebra:

- [1] H. AMANN, J. ESCHER: *Analysis I*. Birkhäuser, 2006.
- [2] Zitat F. BERNSTEIN aus: *R. Dedekind, Gesammelte mathematische Werke, Dritter Band, herausgegeben von R. Fricke, E. Noether, Ö. Ore*. S. 449, Vieweg, 1932.
- [3] S. BOSCH: *Lineare Algebra*. Springer, 2014.
- [4] T. BRÖCKER: *Lineare Algebra und Analytische Geometrie*. Birkhäuser, 2004.
- [5] O. DEISER: *Einführung in die Mengenlehre*. Springer, 2010.
- [6] G. FISCHER: *Lernbuch Lineare Algebra und Analytische Geometrie*. Springer, 2019.
- [7] G. FISCHER, B. SPRINGBORN: *Lineare Algebra*. Springer, 2020.
- [8] O. FORSTER: *Analysis 1*. Springer, 2015.
- [9] G. GREEFRATH, R. OLDENBURG, H.-S. SILLER, V. ULM, H.-G. WEIGAND: *Didaktik der Analysis*. Springer, 2016.
- [10] H.-W. HENN, A. FILLER: *Didaktik der Analytischen Geometrie und Linearen Algebra*. Springer, 2015.
- [11] P.R. HALMOS: *Naive Set Theory*. Springer, 1974.
- [12] H. HEUSER: *Lehrbuch der Analysis. Teil 1*. Vieweg+Teubner, 2009.
- [13] S. HILDEBRANDT: *Analysis 1*. Springer, 2006.
- [14] K. JÄNICH: *Lineare Algebra*. Springer, 2008.
- [15] K. KÖNIGSBERGER: *Analysis 1*. Springer, 2004.
- [16] W. WALTER: *Analysis 1*. Springer, 2009.
- [17] H.-D. EBBINGHAUS, H. HERMES, F. HIRZEBRUCH, M. KOECHER, K. LAMOTKE, K. MAINZER, J. NEUKIRCH, A. PRESTEL, R. REMMERT: *Zahlen*. Springer, 1992.