Vorlesungsnotizen

Mathematik 1 und 2

(für den Lehramtsstudiengang Sekundarstufe)

Wintersemester 2020/21

und

Sommersemester 2021

Thomas Schmidt

Stand: 24. September 2021

Mathematik 1 & 2: Inhaltsverzeichnis

Warnung: Diese Notizen sind nicht völlig identisch mit dem 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 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 Wahrheitstafeln

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	$A \Longrightarrow B$	Aus A folgt B. B folgt aus A.
Implikation	$B \Longleftarrow A$	A impliziert B. B wird von A impliziert.
Konditional	$A \to B$	Sei A (gegeben). Dann (gilt) B.
Subjunktion	$B \leftarrow A$	A (ist) hinreichend für B. B (ist) notwendig für A.
Äquivalenz Bikonditional	$A \Longleftrightarrow B$ $A \leftrightarrow B$	A (ist) äquivalent (zu) B A gleichbedeutend mit 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) **Wahrheitstafeln** festgelegt:

$\boldsymbol{A}$	$\boldsymbol{\neg A}$
w	f
f	w

$\boldsymbol{A}$	$\boldsymbol{B}$	$\boldsymbol{A \wedge B}$	$\boldsymbol{A \vee B}$	$\boldsymbol{A \Longrightarrow B}$	$\boldsymbol{A \Longleftrightarrow B}$
w	w	w	w	w	w
w	f	f	w	f	f
f	w	f	w	w	f
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 $A \Longrightarrow B$ bei falscher Prämisse A (dritte/vierte Zeile Tabellenkörper) als wahr festgelegt wird, also „aus Falschem alles folgt“. Beispiele sind etwa „3 ist ungerade $\Longrightarrow 2 \cdot 4 = 8$“ (wahr), „3 ist ungerade $\Longrightarrow 2 \cdot 4 = 7$“ (falsch), „3 ist gerade $\Longrightarrow 2 \cdot 4 = 8$“ (wahr) und „3 ist gerade $\Longrightarrow 2 \cdot 4 = 7$“ (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 Wahrheitstafeln 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):

$$A \wedge B \quad \text{gb. mit} \quad B \wedge A\,, \qquad\qquad A \vee B \quad \text{gb. mit} \quad B \vee A\,,$$
$$(A \wedge B) \wedge C \quad \text{gb. mit} \quad A \wedge (B \wedge C)\,, \qquad (A \vee B) \vee C \quad \text{gb. mit} \quad A \vee (B \vee C)\,.$$

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

$$(A \vee B) \wedge C \quad \text{gb. mit} \quad (A \wedge C) \vee (B \wedge C)\,, \qquad (A \wedge B) \vee C \quad \text{gb. mit} \quad (A \vee C) \wedge (B \vee C)\,,$$
$$A \Longrightarrow B \quad \text{gb. mit} \quad (\neg A) \vee B\,, \qquad\qquad A \Longleftrightarrow B \quad \text{gb. mit} \quad (A \wedge B) \vee (\neg(A \vee B))\,.$$

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 $\Longrightarrow$ und $\Longleftrightarrow$ 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:

$(\neg(\neg A)) \Longleftrightarrow A$	(Gesetz der doppelten Negation),
$A \vee (\neg A)$	(Satz vom ausgeschlossenen Dritten),
$(A \wedge B) \Longrightarrow (A \vee C)\,,$	
$(\neg(A \wedge B)) \Longleftrightarrow ((\neg A) \vee (\neg B))$	(**De Morgansche Gesetze** zur Negation der Konjunktion und Disjunktion),
$(\neg(A \vee B)) \Longleftrightarrow ((\neg A) \wedge (\neg B))$	
$(\neg(A \Longrightarrow B)) \Longleftrightarrow (A \wedge (\neg B))$	(Negation der Implikation).

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

$(A \wedge (A \Longrightarrow B)) \Longrightarrow B$	(Modus ponens),
$((A \Longrightarrow B) \wedge (B \Longrightarrow C)) \Longrightarrow (A \Longrightarrow C)$	(Transitivität der Implikation),
$(A \Longrightarrow B) \Longleftrightarrow ((\neg B) \Longrightarrow (\neg A))$	(**Kontrapositions-Prinzip**),
$(A \Longleftrightarrow B) \Longleftrightarrow ((A \Longrightarrow B) \wedge (B \Longrightarrow A))$	(Charakterisierung der Äquivalenz durch „Hin“- und „Rück“-Implikation).

Die Tautologien der Form $(\ldots) \Longleftrightarrow (\ldots)$ 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 $\Longleftrightarrow$ 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 solang diese nicht bestimmt sind, man etwa im Beispiel den Wert von x nicht kennt, solang 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[1] 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	$\forall x{\in}M\colon P(x)$	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	$\exists x{\in}M\colon P(x)$	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 $\forall x{\in}M\colon P(x)$ als wahr betrachtet, wenn $P(x)$ für jede Zahl/jedes Objekt aus der Grundmenge M, die/das an Stelle von x eingesetzt wird, wahr

[1] 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 „Mengen-freien" Aussagen $\forall x\colon P(x)$ und $\exists x\colon P(x)$ 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 $\forall x \in M\colon P(x)$ und $\exists x \in M\colon P(x)$ als abkürzende Schreibweisen für $\forall x\colon (x \in M \Longrightarrow P(x))$ und $\exists x\colon (x \in M \Longrightarrow P(x))$ 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 $\forall x{\in}M\colon P(x)$ als falsch. Analog betrachtet man $\exists x{\in}M\colon P(x)$ 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 $\exists x{\in}M\colon P(x)$ 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 $\bigwedge$ und $\bigvee$, 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 $\exists!x{\in}M\colon P(x)$ 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)

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

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 $\forall x{\in}M\colon \forall y{\in}N\colon P(x,y)$ und $\exists y{\in}N\colon \forall x{\in}M\colon P(x,y)$ 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 $\forall x{\in}M\colon \forall y{\in}N\colon P(x,y)$ äquivalent zu $\forall y{\in}N\colon \forall x{\in}M\colon P(x,y)$ und — in Vorgriff auf Notation des Abschnitts 1.4 — übrigens auch äquivalent zu $\forall (x,y){\in}M{\times}N\colon P(x,y)$. Die Vertauschung eines All-Quantors mit einem Existenz-Quantor ist dagegen nicht (ohne Unterschied in der Bedeutung) möglich: Tatsächlich bedeutet $\forall x{\in}M\colon \exists y{\in}N\colon P(x,y)$, dass zu jedem $x{\in}M$ ein von x abhängiges $y{\in}N$ existiert, so dass $P(x,y)$ gilt. Dagegen symbolisiert $\exists y{\in}N\colon \forall x{\in}M\colon P(x,y)$ 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 $\forall x{\in}M\colon \exists y{\in}N\colon P(x,y)$ 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 $\exists y{\in}N\colon \forall x{\in}M\colon P(x,y)$ 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)

$$(\neg(\forall x{\in}M\colon \exists y{\in}N\colon P(x,y))) \iff (\exists x{\in}M\colon \forall y{\in}N\colon (\neg P(x,y)))$$

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

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

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) $\Longleftrightarrow$ (3 teilt 873)“ gilt. Somit sind die Implikationen „(3 teilt 18) $\Longrightarrow$ (3 teilt 873)“ und „(3 teilt 18 nicht) $\Longrightarrow$ (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.*

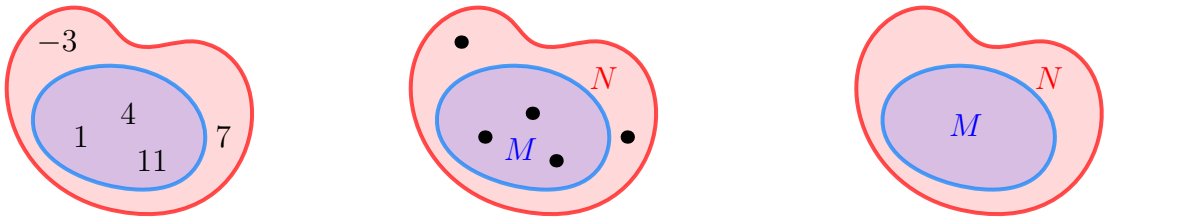
Für die logischen Negationen von $x \in M$, $M \subset N$, $N \supset M$, $M = N$ schreibt man naheliegenderweise $x \notin M$, $M \not\subset N$, $N \not\supset M$, $M \neq N$.

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 $\subseteq$, $\supseteq$, $\subseteqq$, $\supseteqq$ 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.

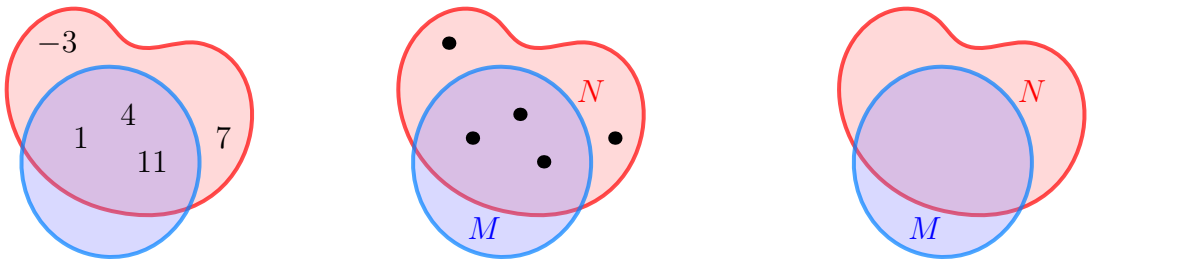
Die **Veranschaulichung von Mengen** und Mengen-Inklusionen kann man ***in geeigneten Fällen*** mit Bereichen oder Umrissen in der Zeichenebene angehen: Besonders in Fällen mit endlich vielen Elementen ist es üblich, die **Elemente in einem Bereich/Umriss von schematischer Bedeutung** einzutragen oder zumindest anzudeuten. Eine ***zweite Darstellungsweise***, die besonders im geometrischem 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 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.



$\{4,1,11\} \subset \{-3,4,1,7,11\}$ | $M \subset N$ für Mengen M und N mit angedeuteten Elementen | $M \subset N$ für Mengen M und N von Koordinatenpunkten in der Ebene

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.



$\{4,1,11\} \subset \{-3,4,1,7,11\}$ | $M \subset N$ für Mengen M und N mit angedeuteten Elementen | $M \not\subset N$ und $M \not\supset N$ für Mengen M und N von Koordinatenpunkten

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* $\{x_1, x_2, x_3, \ldots, x_{n-1}, x_n\}$ *mit irgendeiner natürlichen Zahl* n *für die Menge, die genau die* n *Objekte* x_1*,* x_2*,* x_3*,* $\ldots$*,* x_{n-1}*,* x_n *als Elemente enthält,*
- $\{x_1, x_2, x_3, \ldots,\}$ *für die Menge, die genau die unendlich vielen Objekte* x_1*,* x_2*,* x_3*,* $\ldots$ *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),
- $\{\text{rot}, \text{grün}, \text{blau}\}$ (Menge der RGB-Grundfarben; 3 Elemente),
- $\{+, -, \cdot, :\}$ (Menge der Grundrechenarten; 4 Elemente),
- $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, \text{A}, \text{B}, \text{C}, \text{D}, \text{E}, \text{F}\}$ (Menge der Hexadezimal-Ziffern; 16 Elemente),
- $\{-7, -6, -5, \ldots, 17, 18\}$ (Menge der ganzen Zahlen von -7 bis 18; 26 Elemente),
- $\{1, 2, 3, 4, \ldots\}$ (Menge der natürlichen Zahlen; unendlich viele Elemente),
- $\{\{1, 2, 3, 4, \ldots\}, \{+, -, \cdot, :\}, \{5, 13\}, \{2, 5, -\}\}$
  (Mengensystem mit 4 Mengen als Elementen; dargestellt in Abbildung 3),

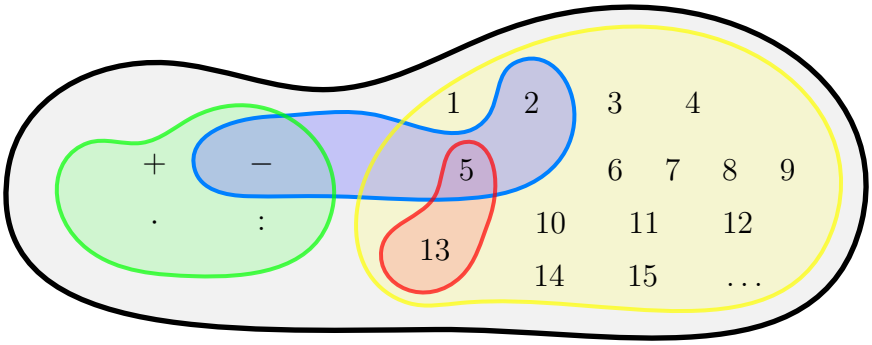


Abb. 3: Darstellung des Mengensystems $\{\{1, 2, 3, 4, \ldots\}, \{+, -, \cdot, :\}, \{5, 13\}, \{2, 5, -\}\}$

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

Geht man nur vom Bild aus, so könnte es sich in Abbildung 3 aber genausogut um das Mengensystem $\{\{\{5, 13\}, 1, 2, 3, 4, \ldots\}, \{+, -, \cdot, :\}, \{2, 5, -\}\}$ 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.*

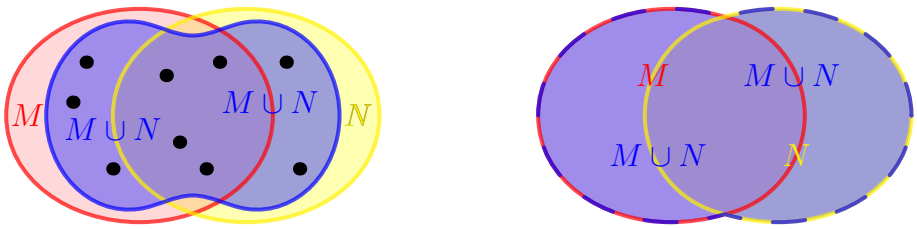


Abb. 4: Graphische Darstellungen der Vereinigungsmenge $M \cup N$

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 $\exists M \in \mathcal{S}\colon x \in M$.

(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 $(x \in M) \wedge (x \in N)$.*

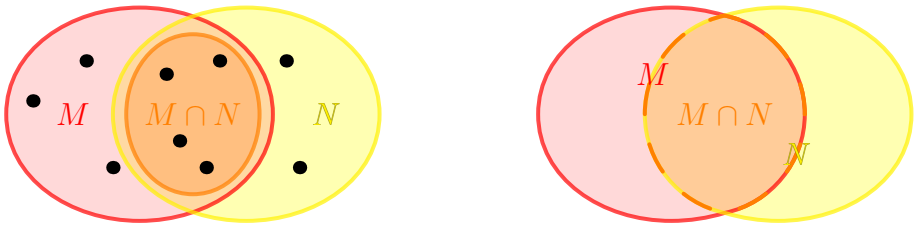


Abb. 5: Graphische Darstellungen der Schnittmenge $M \cap N$

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* $\forall M \in \mathcal{S}\colon x \in M$*.*

(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.*

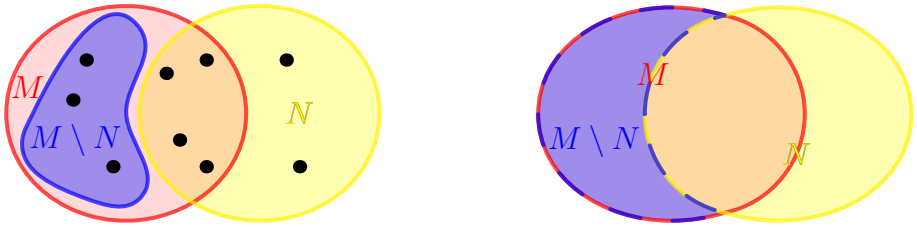


Abb. 6: Graphische Darstellungen der Differenzmenge $M \setminus N$

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

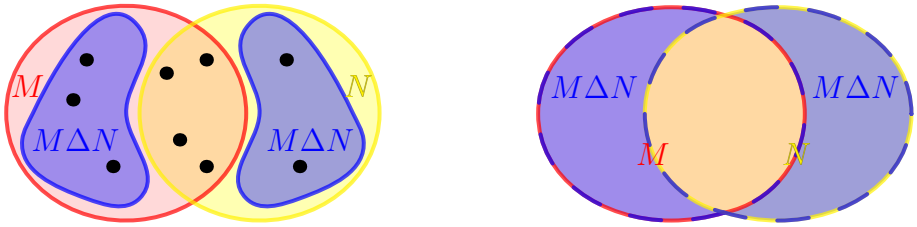


Abb. 7: Graphische Darstellungen der symmetrischen Differenzmenge $M\Delta N$

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 Assoziativgesetzte

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

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

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

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

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

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

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[2] und ist $\mathcal{S}$ ein/das Mengensystem, das als Elemente genau all diese M_i enthält, so verwenden wir

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

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 $M_1, M_2, \ldots, M_n$ (mit natürlicher Zahl n) bzw. unendliche viele Mengen $M_1, M_2, M_3, \ldots$ **(paarweise) disjunkt**, wenn $M_i \cap M_j = \emptyset$ für alle $i, j \in \{1, 2, \ldots, n\}$ mit $i \neq j$ bzw. alle $i, j \in \{1, 2, 3, \ldots\}$ 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 $M_1, M_2, \ldots, M_n$ nur der Schnitt $M_i \cap M_j$ von je zweien leer sein muss und eben *nicht* der Gesamt-Schnitt $M_1 \cap M_2 \cap \ldots \cap M_n$. 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 $M^{\mathrm{c}} := \mathcal{X} \setminus M$ das **Komplement** von M (in $\mathcal{X}$).*

[2] Später werden wir in dieser Situation von einer Familie $(M_i)_{i \in I}$ von Mengen oder äquivalent von einer Abbildung $I \to \mathcal{S}$, $i \mapsto M_i$ 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

$$(M^{\mathrm{c}})^{\mathrm{c}} = M$$

und die mengentheoretischen **de Morganschen Gesetze**

$$(M \cup N)^{\mathrm{c}} = M^{\mathrm{c}} \cap N^{\mathrm{c}}\,, \qquad (M \cap N)^{\mathrm{c}} = M^{\mathrm{c}} \cup N^{\mathrm{c}}\,,$$
$$\Big(\bigcup_{i\in I} M_i\Big)^{\mathrm{c}} = \bigcap_{i\in I} M_i^{\mathrm{c}}\,, \qquad \Big(\bigcap_{i\in I} M_i\Big)^{\mathrm{c}} = \bigcup_{i\in I} M_i^{\mathrm{c}}$$

(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 $(x, y) = (\widetilde{x}, \widetilde{y})$ von Paaren als gleichbedeutend mit $(x = \widetilde{x}) \wedge (y = \widetilde{y})$ 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* Paars 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.

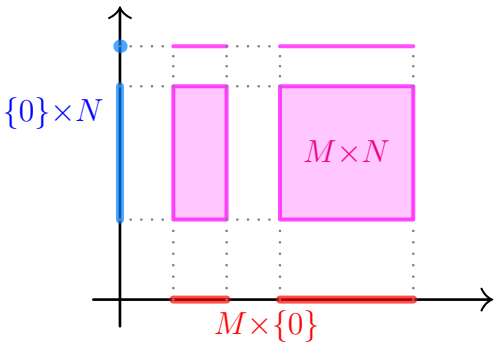


Abb. 8: Kartesisches Produkt $M\times N$ von Mengen M, N der Zahlengeraden

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** $(x_1, x_2, \ldots, x_n)$. Diese betrachtet man als Elemte des kartesischen Produkts mehrerer Mengen:

Definitionen (**mehrfache kartesische Produkte**). *Seien n eine natürliche Zahl*[3] *und M_1,*

[3] 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.

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

$$M_1 \times M_2 \times \ldots \times M_n$$

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

Besonders häufig braucht man tatsächlich das n-fache kartesische Produkt

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

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.

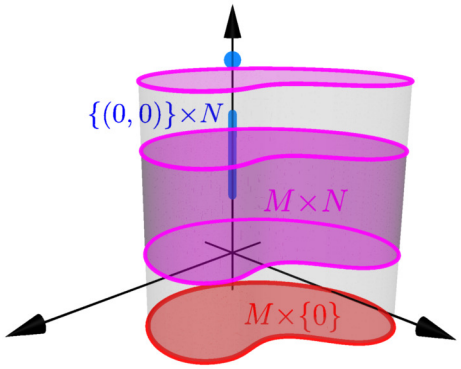


Abb. 9: Kartesisches Produkt $M \times N$ einer Menge M der Ebene mit einer Menge N der Zahlengeraden

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 auch später noch ein Exkurs): Hat M genau n verschiedene Elemente (für eine nichtnegative 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 Zusatzerläuterungen 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 $\forall x\colon (x \in M \iff x \in N)$.

  (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 $\forall x\colon x \notin \emptyset$ 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 $\forall x\colon (x \in \{a, b\} \iff x = a \vee x = b)$ 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 $\forall x\colon (x \in \bigcup \mathcal{S} \iff \exists M \in \mathcal{S}\colon x \in M)$ 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 $\forall T\colon (T \subset M \iff T \in \mathcal{P}(M))$ 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 $\forall x\colon (x \notin M \vee x \notin N)$ schreiben muss).

  (Dieses Axiom sichert, dass keine unendliche Kette von ineinander enthalten Mengen des Typs $M_1 \ni M_2 \ni M_3 \ni \ldots$ existieren kann (denn dann würde die unendliche Menge $M = \{M_1, M_2, M_3, \ldots\}$ 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).)

- **Aussonderungsaxiom:** 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 $\forall x\colon (x \in \{y \in M \mid P(y)\} \iff x \in M \wedge P(x)$ ist wahr).

  (Insbesondere können als Konsequenz des Axioms auch Schnittmengen und — wie vorne schon gesehen — Mengen-Differenzen definiert werden.)

- **Ersetzungsaxiom:** 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. $\forall M \in \mathcal{S}\colon M \neq \emptyset$ und $\forall M, N \in \mathcal{S}\colon M \neq N \Longrightarrow M \cap N = \emptyset$) 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)

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

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 im späteren Abschnitt 4.2 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*[1]*, die jedem Element x von*

[1] Den Begriff „(Zuordnungs-)Vorschrift“ können und werden wir in Abschnitt 2.3 noch präzisieren.

$\mathcal{X}$ ein eindeutiges Element y von $\mathcal{Y}$ zuordnet. Man sagt, f bilde das Element x auf das zugehörige 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 $f\colon \mathcal{X} \to \mathcal{Y}$ 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 $x \overset{f}{\mapsto} y$ beziehungsweise kurz $x \mapsto y$.*

(*Dabei ist es Konvention, den Pfeil $\to$ 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
$$f\colon \{1,2,4,5\} \to \{-3,-2,0,4,10\}$$
ist durch die Zuordnungen
$$1 \mapsto -2\,, \qquad 2 \mapsto -2\,, \qquad 4 \mapsto 4\,, \qquad 5 \mapsto 10$$
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
$$f\colon \{\emptyset, 5, \mathbb{N}\} \to \mathbb{Q}$$
erhält man durch die Festlegungen
$$f(\emptyset) := \frac{3}{2}\,, \qquad f(5) := 4\,, \qquad f(\mathbb{N}) := -\frac{1}{12}\,.$$

(3) Eine weitere Abbildung
$$f\colon \mathbb{N} \to \mathbb{N}$$
wird durch
$$f(n) := n^2 \qquad \text{für alle } n \in \mathbb{N}$$

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 $g\colon \mathbb{N} \to \{0,1,4,9,16\}$ 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 $h\colon \mathbb{N} \to \mathbb{N}$ 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

$$f\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$

auffassen, die durch

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

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

$$f\colon \mathbb{R} \to \mathbb{R}$$

erhält man durch die Festlegung

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

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

(6) Eine weitere Funktion

$$f\colon \mathcal{X} \to \mathcal{Y} \qquad \text{von } \mathcal{X} := \left\{x \in \mathbb{R} \,\middle|\, 1 \leq x < \tfrac{11}{2}\right\} \text{ nach } \mathcal{Y} := \left\{y \in \mathbb{R} \,\middle|\, -\tfrac{1}{2} < y < \tfrac{13}{2}\right\}$$

wird durch

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

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 $g\colon \mathcal{X} \to \mathcal{Z}$ in den kleineren Zielbereich $\mathcal{Z} := \left\{z \in \mathbb{R} \,\middle|\, -\frac{1}{4} < z \leq 6\right\} \subsetneq \mathcal{Y}$ ergibt.

(7) **„Gegenbeispiele“:** Die Versuche, $f\colon \mathbb{N} \to \mathbb{N}$ durch $f(n) := n^2{-}n$ für alle $n \in \mathbb{N}$ oder $g\colon \mathbb{N}_0 \to \mathbb{N}_0$ 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 $h\colon \mathbb{R} \to \mathbb{R}\,,\ x \mapsto \frac{1}{x}$ *keine* wohldefinierte Funktion, da $\frac{1}{0}$ nicht erklärt

und deshalb der Funktionswert $h(0)$ nicht definiert ist. (Die Variante $\widetilde{h}\colon \mathbb{R}\setminus\{0\} \to \mathbb{R}\,,\ x \mapsto \frac{1}{x}$ 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).

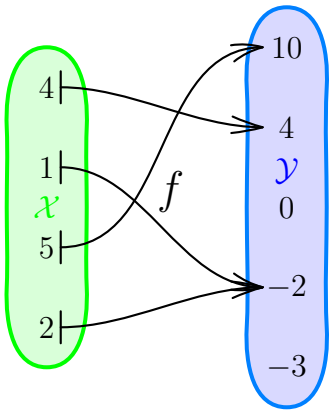


Abb. 10: Die Abbildung f aus Beispiel (1) von $\mathcal{X} = \{1, 2, 4, 5\}$ nach $\mathcal{Y} = \{-3, -2, 0, 4, 10\}$

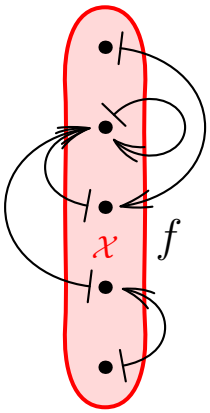


Abb. 11: Eine Selbstabbildung $f\colon \mathcal{X} \to \mathcal{X}$ einer 5-elementigen Menge $\mathcal{X}$

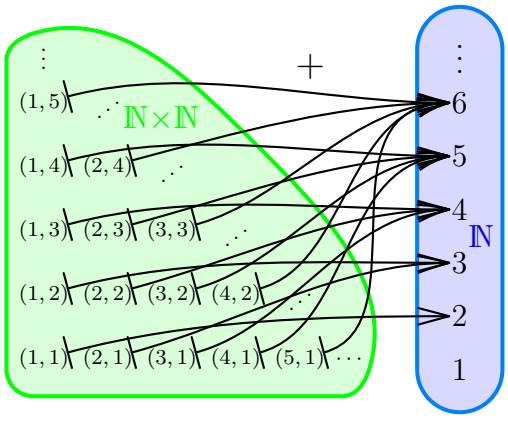


Abb. 12: Die Addition + als Abbildung des Beispiels (4) von $\mathbb{N}\times\mathbb{N}$ nach $\mathbb{N}$

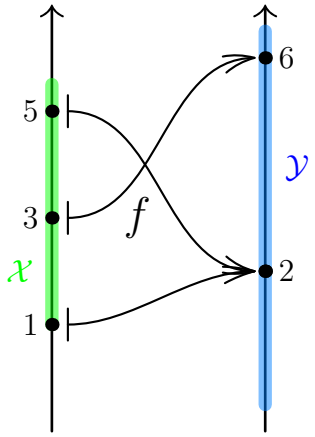


Abb. 13: Die Funktion f aus Beispiel (6) bildet 3 Punkte von $\mathcal{X} \subset \mathbb{R}$ nach $\mathcal{Y} \subset \mathbb{R}$ ab.

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 einzuzeichnen. Gelegentlich weicht man hiervon aber auch ab und verwendet alternative Darstellungen wie die der Abbildung 11.

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

$$\mathrm{G}_f := \{(x,y) \in \mathcal{X}\times\mathcal{Y} \,|\, f(x) = y\} \subset \mathbb{R}^2$$

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

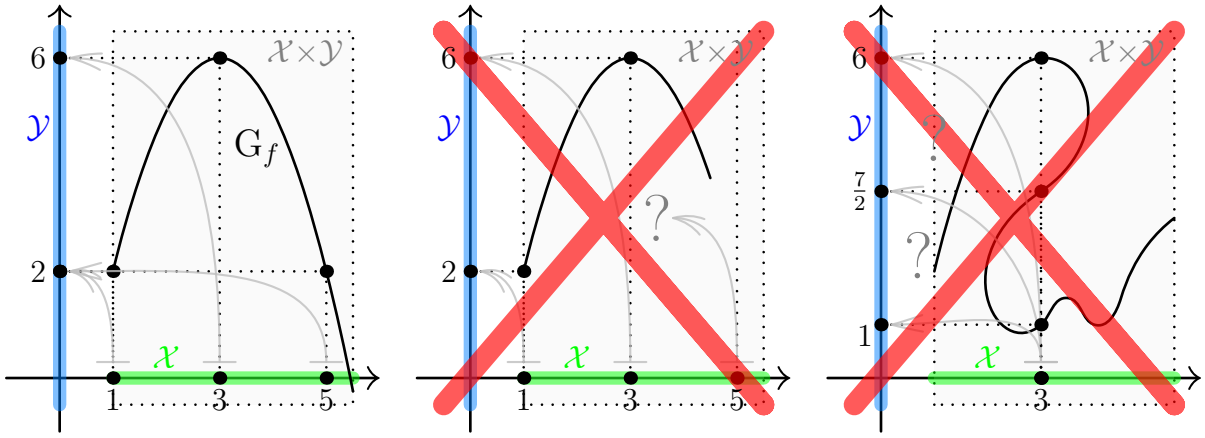


Abb. 14: Der Graph G_f der Funktion f aus Beispiel (6) von $\mathcal{X} = \{x \in \mathbb{R} \,|\, 1 \leq x < \frac{11}{2}\}$ nach $\mathcal{Y} = \{y \in \mathbb{R} \,|\, -\frac{1}{2} < y < \frac{13}{2}\}$ und zwei Kurven, die *nicht* Graph einer Funktion von $\mathcal{X}$ nach $\mathcal{Y}$ sind

$\mathcal{X}$ 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 $f\colon \mathcal{X} \to \mathcal{Z}$ 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

$$\mathrm{G}_f := \{(x,y,z) \in \mathcal{X}\times\mathcal{Z} \,|\, f(x,y) = z\} \subset \mathbb{R}^3$$

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[2] 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.

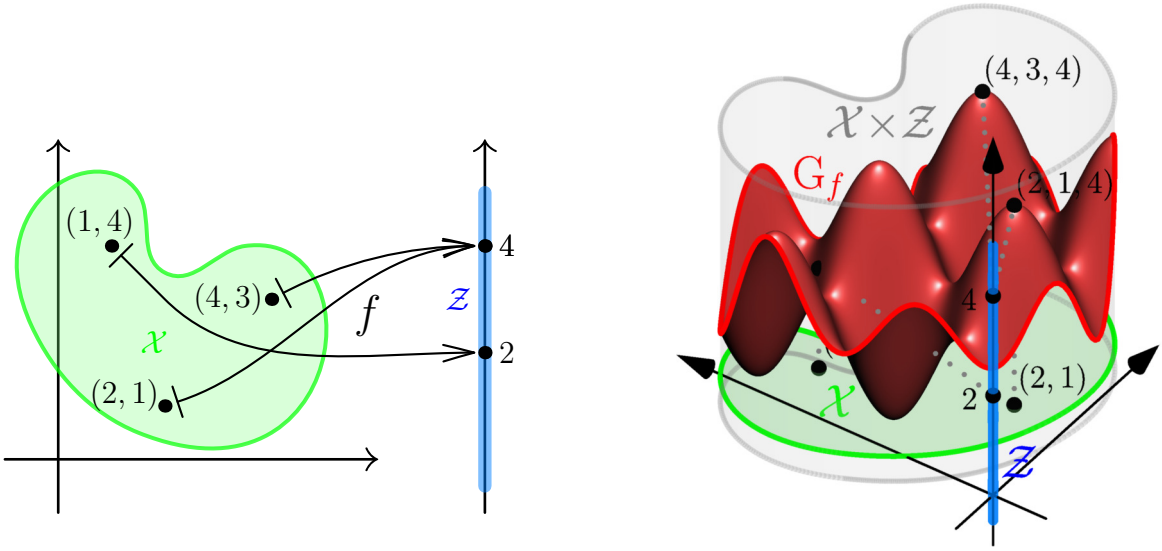


Abb. 15: Abbildung einiger Beispiel-Punkte und Graph G_f bei einer Funktion $f\colon \mathcal{X} \to \mathcal{Z}$ von einem 2-*dimensionalen Definitionsbereich* $\mathcal{X} \subset \mathbb{R}^2$ nach $\mathcal{Z} = \{z \in \mathbb{R} \,|\, -\frac{1}{2}<z<5\} \subset \mathbb{R}$

Als letzten Fall betrachten wir Darstellungen einer Funktion $f\colon \mathcal{X} \to \mathcal{Y}$ 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

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

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

$$\mathrm{G}_f := \{(x,y,z) \in \mathcal{X}\times\mathcal{Y} \,|\, f(x) = (y,z)\} \subset \mathbb{R}^3\,,$$

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.

[2] 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 π werden in der Vorlesung aber erst deutlich später eingeführt.

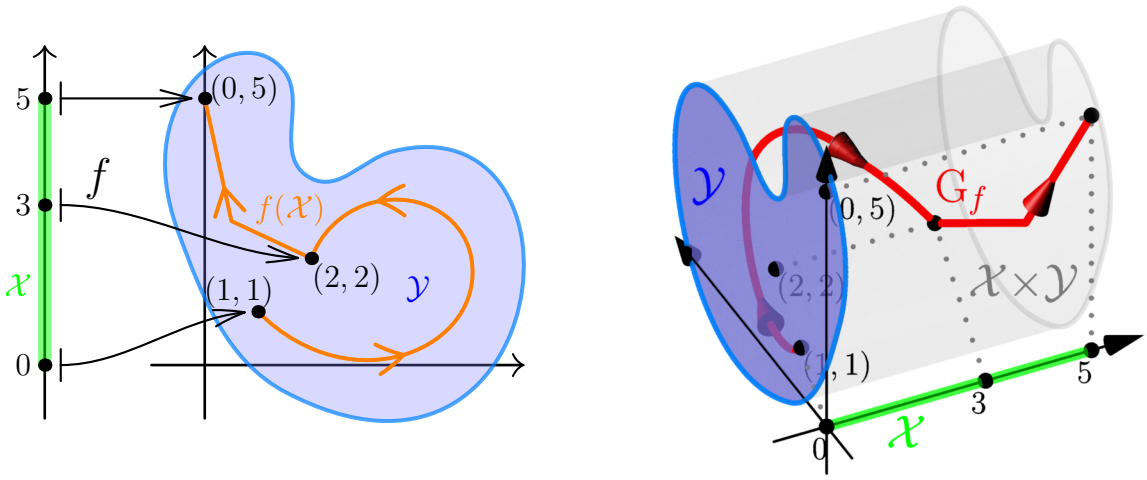


Abb. 16: Abbildung einiger Beispiel-Punkte, das Bild $f(\mathcal{X})$ und der Graph G_f bei einer Funktion $f\colon \mathcal{X} \to \mathcal{Y}$ von $\mathcal{X} = \{x \in \mathbb{R} \,|\, 0{\leq}x{\leq}5\} \subset \mathbb{R}$ in einen 2-*dimensionalen Zielbereich* $\mathcal{Y} \subset \mathbb{R}^2$

Übrigens ist der Graph G_f einer Funktion $f\colon \mathcal{X} \to \mathcal{Y}$ immer auch das Bild der Graphenabbildung $\mathcal{X} \to \mathcal{X}{\times}\mathcal{Y}$, $x \mapsto (x, f(x))$. 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 $f\colon \mathcal{X} \to \mathcal{Y}$ 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*

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

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

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

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

Für einzelne $y \in \mathcal{Y}$ gilt damit[3] $f^{-1}(\{y\}) = \{x \in \mathcal{X} \,|\, f(x) = y\}$. Die definierende Eigenschaft der Abbildung erzwingt generell $f^{-1}(\mathcal{Y}) = \mathcal{X}$ und auch $f^{-1}(\mathrm{Bild}(f)) = \mathcal{X}$.

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

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

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

[3] 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.

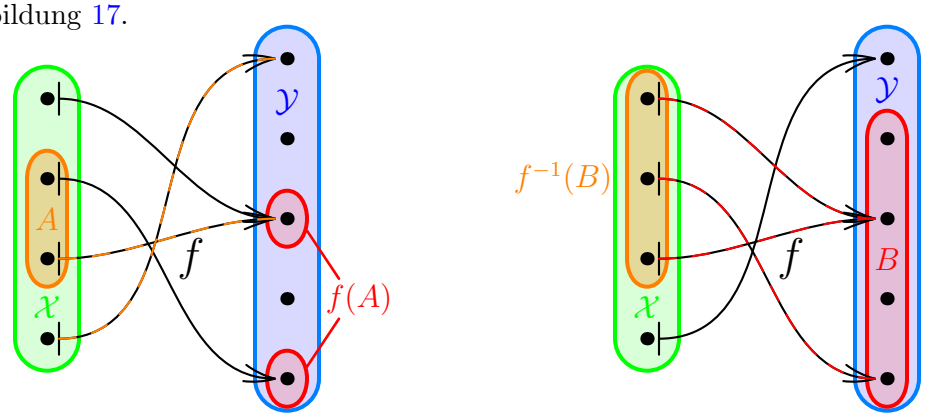


Abb. 17: Bild $f(A)$ von $A \subset \mathcal{X}$ und Urbild $f^{-1}(B)$ von $B \subset \mathcal{Y}$ unter einer Abbildung $f\colon \mathcal{X} \to \mathcal{Y}$

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

(1) Das Bild einer Abbildung $f\colon \mathcal{X} \to \mathcal{Y}$ ist die Menge B mit den wenigsten möglichen Elementen, so dass noch $\mathrm{G}_f \subset \mathcal{X}\times B$ gilt. Das Bild *kann* eine *echte* Teilmenge des Ziels sein.

(2) Für eine Abbildung $f\colon \mathcal{X} \to \mathcal{Y}$ 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* $f(\mathcal{X}) = \mathrm{Bild}(f)$ 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 $f^{-1}(\ldots)$ 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 $f\colon \mathcal{X} \to \mathcal{Y}$ 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*:

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

Dass beim Bild des Schnitts tatsächlich nur „$\subset$“ und nicht „$=$“ gelten kann, sieht man schon an einer Abbildung $f\colon \{a_1, a_2\} \to \{y\}$ 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 Mengen-Gleichheiten 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[4] mit der Definition von Urbild und Vereinigung durch

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

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

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

Definitionen (Abbildungseigenschaften). *Sei $f\colon \mathcal{X} \to \mathcal{Y}$ 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 $x, \widetilde{x} \in \mathcal{X}$ die Implikation*

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

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

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

(III) *Man nennt f **bijektiv** oder eine **Bijektion**, wenn zu jedem $y \in \mathcal{X}$ 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 $f\colon \mathcal{X} \to \mathcal{Y}$ 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.

[4] Aneinandergereihte Äquivalenzen $S_1 \iff S_2 \iff S_3 \iff \ldots \iff S_{n-1} \iff S_n$ für Aussagen $S_1, S_2, \ldots, S_n$ 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 $(S_1 \iff S_2) \wedge (S_2 \iff S_3) \wedge \ldots \wedge (S_{n-1} \iff S_n)$ schreiben.

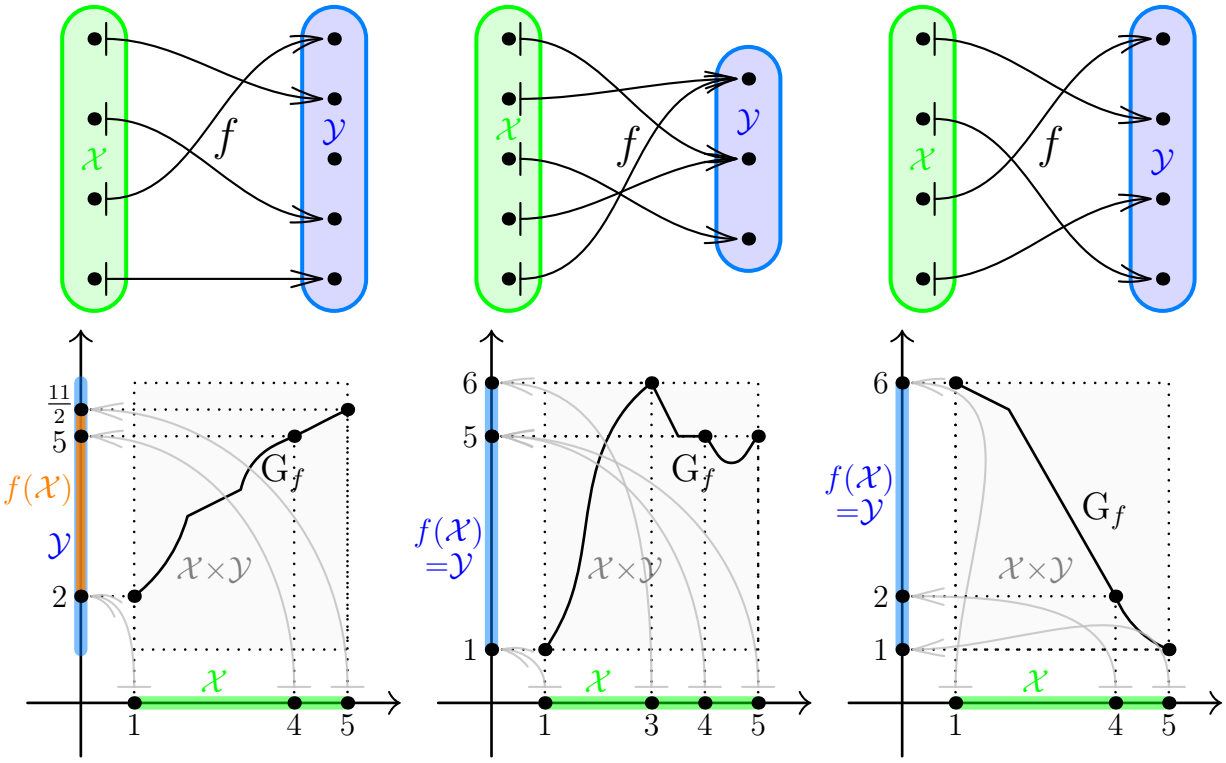


Abb. 18: Injektionen (links), Surjektionen (mittig) und Bijektionen (rechts) $f\colon \mathcal{X} \to \mathcal{Y}$ für endliche Mengen $\mathcal{X}$ und $\mathcal{Y}$ (oben) und in Graphendarstellung für $\mathcal{X} = \{x \in \mathbb{R} \,|\, 1{\leq}x{\leq}5\}$ und $\mathcal{Y} = \{y \in \mathbb{R}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

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** $\mathcal{X} \to \mathcal{Y}$ 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 Elemente 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 $f\colon \mathcal{X} \to \mathcal{Y}$ kann man durch Verkleinerung des Ziels stets die Surjektion $\widetilde{f}\colon \mathcal{X} \to \mathrm{Bild}(f)$ mit $\widetilde{f}(x) := f(x)$ für alle $x \in \mathcal{X}$ gewinnen. Ist f surjektiv, so ist dabei $\widetilde{f} = f$. Ist f injektiv, so ist $\widetilde{f}$ sogar bijektiv.

(4) Bei einer **Bijektion** $f\colon \mathcal{X} \to \mathcal{Y}$ 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 $\mathrm{Bild}(f)$. 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 $f\colon \mathcal{X} \to \mathcal{Y}$ eine Abbildung. Eine Abbildung $g\colon \mathcal{Y} \to \mathcal{X}$ heißt* ***Umkehrfunktion*** *oder* ***Umkehrabbildung*** *von/zu f, wenn folgende Äquivalenz für alle $x \in \mathcal{X}$ und $y \in \mathcal{Y}$ gilt*:

$$f(x) = y \quad \Longleftrightarrow \quad g(y) = x\,.$$

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 $f\colon \mathcal{X} \to \mathcal{Y}$ von $\mathcal{X} \subset \mathbb{R}$ nach $\mathcal{Y} \subset \mathbb{R}$ geht der Graph $\mathrm{G}_g = \{(y, x) \in \mathbb{R}^2 \,|\, (x, y) \in \mathrm{G}_f\}$ der Umkehrfunktion $g\colon \mathcal{Y} \to \mathcal{X}$ wie in Abbildung 20 aus dem Graph G_f von f durch Spiegelung an der ersten Winkelhalbierenden des Koordinatensystems hervor.

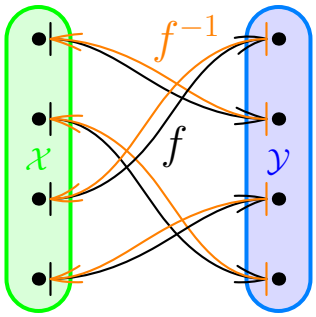


Abb. 19: Die Umkehrabbildung $f^{-1}\colon \mathcal{Y} \to \mathcal{X}$ einer Bijektion $f\colon \mathcal{X} \to \mathcal{Y}$

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

Beweis der Eindeutigkeit. Für zwei Umkehrfunktionen $g\colon \mathcal{Y} \to \mathcal{X}$ und $\widetilde{g}\colon \mathcal{Y} \to \mathcal{X}$ zu f ergibt die Definition $g(y) = x \iff \widetilde{g}(y) = x$ 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 $g(y) = g(y) \iff \widetilde{g}(y) = g(y)$. Da die linke Seite trivial gilt, gilt auch $\widetilde{g}(y) = g(y)$ für alle $y \in \mathcal{Y}$, und damit ist $\widetilde{g} = g$. □

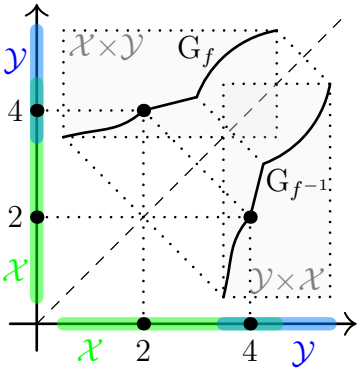


Abb. 20: Graphen G_f und $\mathrm{G}_{f^{-1}}$ von $f\colon \mathcal{X} \to \mathcal{Y}$ und $f^{-1}\colon \mathcal{Y} \to \mathcal{X}$ für $\mathcal{X}, \mathcal{Y} \subset \mathbb{R}$

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.

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

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

Beweis. „$\Longrightarrow$“: 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 $g\colon \mathcal{Y} \to \mathcal{X}$ 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.

„$\Longleftarrow$“: Sei $g\colon \mathcal{Y} \to \mathcal{X}$ 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. □

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

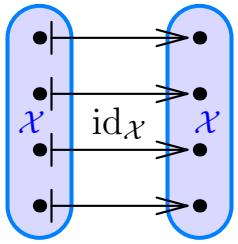


Abb. 21: Die Identität einer Menge $\mathcal{X}$ mit 4 Elementen

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

(1) *Für jede Menge $\mathcal{X}$ ist die* ***Identität*** *oder* ***identische Abbildung*** $\mathrm{id}_{\mathcal{X}}\colon \mathcal{X} \to \mathcal{X}$ *von $\mathcal{X}$ durch $\mathrm{id}_{\mathcal{X}}(x) := x$ 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.*

(2) *Für Mengen $\mathcal{X}$, $\mathcal{Y}$ und ein* **fixiertes** *Element $\boldsymbol{y} \in \mathcal{Y}$ heißt $\mathcal{X} \to \mathcal{Y}$, $x \mapsto y$ die* ***konstante Abbildung*** *von $\mathcal{X}$ nach $\mathcal{Y}$ mit (konstantem Funktions-)Wert y. Ist $f\colon \mathcal{X} \to \mathcal{Y}$ die konstante Abbildung mit Wert y, so notiert man*[5] $\boldsymbol{f \equiv y}$ *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*** $\mathbb{1}_A\colon \mathcal{X} \to \{0,1\}$ *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 $\delta_x\colon \mathcal{P}(\mathcal{X}) \to \{0,1\}$ 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 $f\colon \mathcal{X} \to \mathcal{Y}$ und $g\colon \mathcal{Y} \to \mathcal{Z}$ Abbildungen. Dann ist die* ***Komposition****, auch* ***Verkettung*** *oder* ***Hintereinanderausführung*** *genannt, von f und g die Abbildung*

$$g \circ f\colon \mathcal{X} \to \mathcal{Z}$$

mit

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

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

[5] 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.

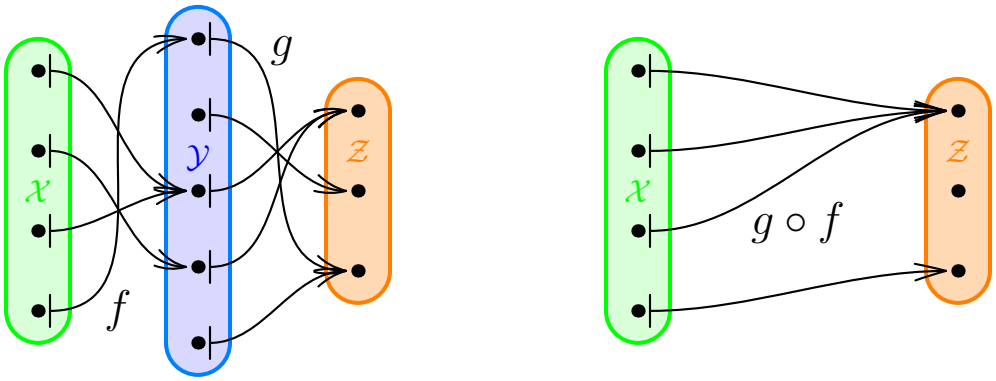


Abb. 22: Die Komposition $g \circ f \colon \mathcal{X} \to \mathcal{Z}$ von $f \colon \mathcal{X} \to \mathcal{Y}$ und $g \colon \mathcal{Y} \to \mathcal{Z}$

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 $f \colon \mathcal{W} \to \mathcal{X}$, $g \colon \mathcal{X} \to \mathcal{Y}$ und $h \colon \mathcal{Y} \to \mathcal{Z}$ gilt*

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

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

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

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 $f \colon \{0,1\} \to \{0,1\}$ mit $f \equiv 0$ und $g \colon \{0,1\} \to \{0,1\}$ mit $g \equiv 1$ offensichtlich $0 \equiv f \circ g \neq g \circ f \equiv 1$.

Übrigens liegt selbst für bijektive $f, g \colon \mathcal{X} \to \mathcal{X}$ im Allgemeinen keine Kommutativität vor: Zum Beispiel bei $f, g \colon \{1,2,3\} \to \{1,2,3\}$ 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 $f \colon \mathcal{X} \to \mathcal{Y}$ und $g \colon \mathcal{Y} \to \mathcal{Z}$ Abbildungen. Dann gelten:*

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

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 $f \colon \mathcal{X} \to \mathcal{Y}$ und $g \colon \mathcal{Y} \to \mathcal{X}$ Abbildungen. Dann heißen f und g **zueinander invers** und g heißt **inverse Abbildung**, **inverse Funktion** oder kurz **Inverse** von/zu f, wenn gelten:*

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

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

Beweis der Eindeutigkeit. Sind $g\colon \mathcal{Y} \to \mathcal{X}$ und $\widetilde{g}\colon \mathcal{Y} \to \mathcal{X}$ zwei Inverse zu f, so folgt

$$g = g \circ \mathrm{id}_{\mathcal{Y}} = g \circ (f \circ \widetilde{g}) = (g \circ f) \circ \widetilde{g} = \mathrm{id}_{\mathcal{X}} \circ \widetilde{g} = \widetilde{g}\,. \qquad \square$$

Tatsächlich ist die Inverse nichts anderes als die Umkehrfunktion:

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

Beweis. „$\Longrightarrow$“: 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.

„$\Longleftarrow$“: Ist g die Inverse zu f, so sind $g \circ f = \mathrm{id}_{\mathcal{X}}$ und $f \circ g = \mathrm{id}_{Y}$ beide bijektiv. Nach dem vorigen Satz ist dann f injektiv und surjektiv, also auch bijektiv. Damit existiert die Umkehrfunktion f^{-1} von f. Nach „$\Longrightarrow$“ 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 $f\colon \mathcal{X} \to \mathcal{Y}$ auf eine Teilmenge A des Definitionsbereichs $\mathcal{X}$ ist die Abbildung*

$$f|_A\colon A \to \mathcal{Y}$$

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 $\mathcal{X}, \mathcal{Y}, \mathcal{X}_1, \mathcal{Y}_1, \mathcal{X}_2, \mathcal{Y}_2, \ldots, \mathcal{X}_n, \mathcal{Y}_n$ Mengen.*

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

$$\mathrm{p}_i\colon \mathcal{X}_1 \times \mathcal{X}_2 \times \ldots \times \mathcal{X}_n \to \mathcal{X}_i$$

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

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

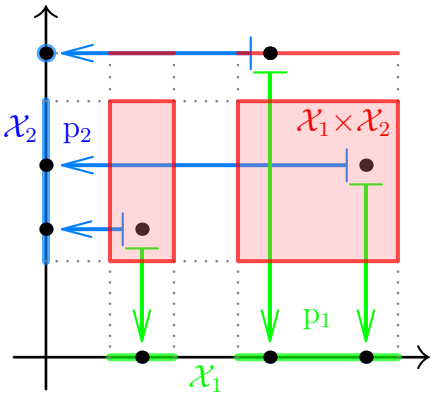


Abb. 23: Das Produkt $\mathcal{X}_1 \times \mathcal{X}_2$ und die Projektionen $\mathrm{p}_1\colon \mathcal{X}_1 \times \mathcal{X}_2 \to \mathcal{X}_1$ und $\mathrm{p}_2\colon \mathcal{X}_1 \times \mathcal{X}_2 \to \mathcal{X}_2$ für $\mathcal{X}_1, \mathcal{X}_2 \subset \mathbb{R}$

(2) *Eine Funktion*

$$f\colon \mathcal{X} \to \mathcal{Y}_1 \times \mathcal{Y}_2 \times \ldots \times \mathcal{Y}_n$$

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

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

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

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

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

$$f\colon \mathcal{X} \to \mathcal{Y}^n\,,$$

mit den n Komponentenfunktionen $f_1, f_2, \ldots, f_n\colon \mathcal{X} \to \mathcal{Y}$ der Funktion f.

(3) *Die **Diagonalabbildung** $\mathcal{X} \to \mathcal{X}^n$, $x \mapsto (x, x, \ldots, x)$ kann auch als die Abbildung $(\mathrm{id}_\mathcal{X}, \mathrm{id}_\mathcal{X}, \ldots, \mathrm{id}_\mathcal{X})\colon \mathcal{X} \to \mathcal{X}^n$, deren Komponenten alle $\mathrm{id}_\mathcal{X}$ sind, geschrieben werden. Sie ist stets injektiv.*

(4) *Das **kartesische Produkt von Abbildungen** $f_1\colon \mathcal{X}_1 \to \mathcal{Y}_1$, $f_2\colon \mathcal{X}_2 \to \mathcal{Y}_2$ ist die Abbildung $f_1 \times f_2\colon \mathcal{X}_1 \times \mathcal{X}_2 \to \mathcal{Y}_1 \times \mathcal{Y}_2$, 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 $\mathrm{p}_{\mathcal{Y}_1} \circ (f_1 \times f_2) = f_1 \circ \mathrm{p}_{\mathcal{X}_1}\colon \mathcal{X}_1 \times \mathcal{X}_2 \to \mathcal{Y}_1$ und $\mathrm{p}_{\mathcal{Y}_2} \circ (f_1 \times f_2) = f_2 \circ \mathrm{p}_{\mathcal{X}_2}\colon \mathcal{X}_1 \times \mathcal{X}_2 \to \mathcal{Y}_2$ mit den Projektionen $\mathrm{p}_{\mathcal{X}_1}, \mathrm{p}_{\mathcal{X}_2}$ und $\mathrm{p}_{\mathcal{Y}_1}, \mathrm{p}_{\mathcal{Y}_2}$ 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 $\mathrm{Abb}(\mathcal{X}, \mathcal{Y})$ 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 $\mathrm{Abb}(\mathcal{X}) := \mathrm{Abb}(\mathcal{X}, \mathcal{X})$ ab.*

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

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

$$\mathrm{Abb}(\mathcal{X}, \mathcal{Y}) \to \mathcal{Y}^n\,,\ f \mapsto (f(x_1), f(x_2), \ldots, f(x_n))$$

eine Bijektion. Daher kann man eine Abbildung $f \in \mathrm{Abb}(\mathcal{X}, \mathcal{Y})$ auf dem n-elementigen Definitionsbereich $\mathcal{X}$ auch als n-Tupel $(f(x_1), f(x_2), \ldots, f(x_n)) \in \mathcal{Y}^n$ ihrer Werte betrachten und bekommt in diesem Fall eine naheliegende **Identifikation von $\mathrm{Abb}(\mathcal{X}, \mathcal{Y})$ mit $\mathcal{Y}^n$**. In Anlehnung hieran kann man sich eine Abbildung $f \in \mathrm{Abb}(\mathbb{N}, \mathcal{Y})$ mit Definitionsbereich $\mathbb{N}$ als „unendliches Tupel“ $(f(x_1), f(x_2), f(x_3), \ldots)$ ihrer Werte vorstellen — ein Objekt, das wir so nicht definiert haben, das aber für $\mathrm{Abb}(\mathbb{N}, \mathcal{Y})$ die Schreibweise $\mathcal{Y}^\mathbb{N}$ nahelegt. Hierdurch wird für $\mathrm{Abb}(\mathcal{X}, \mathcal{Y})$ 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 $\mathcal{Y}_1 \times \mathcal{Y}_2 \times \ldots \times \mathcal{Y}_n$ und dem Tupel ihrer Komponentenfunktionen liegt tatsächlich eine Bijektion

$$\mathrm{Abb}(\mathcal{X}, \mathcal{Y}_1 \times \mathcal{Y}_2 \times \ldots \times \mathcal{Y}_n) \to \mathrm{Abb}(\mathcal{X}, \mathcal{Y}_1) \times \mathrm{Abb}(\mathcal{X}, \mathcal{Y}_2) \times \ldots \times \mathrm{Abb}(\mathcal{X}, \mathcal{Y}_n)$$

oder mit anderen Worten (und vielleicht intuitiver)

$$(\mathcal{Y}_1 \times \mathcal{Y}_2 \times \ldots \times \mathcal{Y}_n)^{\mathcal{X}} \to \mathcal{Y}_1^{\mathcal{X}} \times \mathcal{Y}_2^{\mathcal{X}} \times \ldots \times \mathcal{Y}_n^{\mathcal{X}}$$

zugrunde, die die Zuordnung $f \mapsto (f_1, f_2, \ldots, f_n)$ 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 $(f_1, f_2, \ldots, f_n) \mapsto (f_1, f_2, \ldots, f_n)$ zuordnet, wobei das Tupel der Einzelfunktionen $f_1, f_2, \ldots, f_n$ (links) und die Funktion mit Komponenten $f_1, f_2, \ldots, f_n$ (rechts) in unserer Notation nicht mehr unterscheidbar sind.

2.2 Natürliche und ganze Zahlen, Induktion und Rekursion

Natürlich wurde die Menge $\mathbb{N} = \{1, 2, 3, \ldots\}$ 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* $S\colon \mathbb{N} \to \mathbb{N}$ *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 $S\colon \mathbb{N} \to \mathbb{N}$ 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 $S(m) = S(n) \Longrightarrow m = n$ 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 $n \in M \Longrightarrow S(n) \in M$ 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.

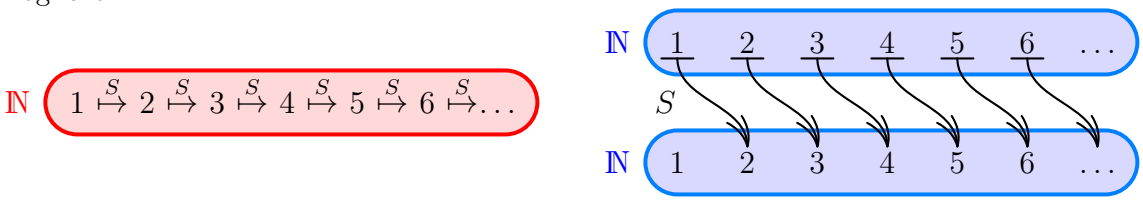


Abb. 24: $\mathbb{N}$ und die Nachfolge-Abbildung $S\colon \mathbb{N} \to \mathbb{N}$ (zwei Möglichkeiten der Veranschaulichung)

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 $S\colon \mathbb{N} \to \mathbb{N}$ zum einen die Bijektion $\widetilde{S}\colon \mathbb{N} \to S(\mathbb{N})$, durch die man die Elemente von $\mathbb{N}$ und $S(\mathbb{N})$ eins-zu-eins identifizieren kann. Zum anderen ist aber doch $S(\mathbb{N}) \subsetneqq \mathbb{N}$, 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 derzeitigem 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 $\{n \in \mathbb{N} \,|\, S(n) \neq n\}$ 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 $\mathrm{S}(\mathbb{N}) \cup \{1\}$ **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[6] 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*

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

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

[6] 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 $\mathbb{R}_{>0} := \{x \in \mathbb{R} \,|\, x > 0\}$ anstelle von $\mathbb{N}$ mit $S(x) := x{+}1$ für alle $x \in \mathbb{R}_{>0}$ 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“[7] $-\mathbb{N}$ *von* $\mathbb{N}$*, so dass die Abbildung* $\mathbb{N} \to -\mathbb{N}$*, 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* $S\colon \mathbb{Z} \to \mathbb{Z}$ *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 $S^{-1}\colon \mathbb{Z} \to \mathbb{Z}$ der Bijektion $S\colon \mathbb{Z} \to \mathbb{Z}$) 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 $S\colon \mathbb{N}_0 \to \mathbb{N}_0$ 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**[8] $A(n)$ für alle $n \in \mathbb{N}$, bei dem man wie folgt vorgeht:

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

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

[7] 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.

[8] 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 $\forall n \in \mathbb{N}\colon A(n)$.

$1 \in M$ und andererseits $n \in M \Longrightarrow S(n) \in M$. 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 $A(1), A(2), \ldots, A(n-1)$ 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:

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

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. □

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

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

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 $1{+}3{+}5{+}\ldots{+}(2n{-}3)+(2n{-}1) = n^2$ auf die Induktionsbehauptung $1{+}3{+}5{+}\ldots{+}(2n{-}1)+(2n{+}1) = (n{+}1)^2$ schließen. Dazu rechnen wir unter Verwendung der Induktionsannahme im zweiten Schritt

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

und erhalten die Induktionsbehauptung. □

In der praktischen Anwendung treten auch etliche **Varianten des Induktionsprinzips** auf: Zum Beispiel kann man eine Aussage $A(z)$ für alle $z \in \{z_0, z_0{+}1, z_0{+}2, \ldots\}$ 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 $z \in \{z_0, z_0{+}1, z_0{+}2, \ldots\}$ 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 $z \in \{z_0{+}1, z_0{+}2, z_0{+}3, \ldots\}$ durchführen. Man kann mehrere Einzelfälle als Induktionsanfang behandeln oder beim Induktionsschritt in Zweierschritten 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:

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

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

Entscheidend ist **bei allen Varianten** des Induktionsprinzip 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 $A(z_0{+}3)$, … *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 $p_1, p_2, \ldots, p_k \in \mathbb{N}$ mit $n = p_1 p_2 \cdot \ldots \cdot p_k$.

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 $2, 3, \ldots, n{-}1$ *auf* n *für* $n \in \mathbb{N}\setminus\{1,2\}$: Wir haben als Induktionsannahme, dass die behauptete Darstellung für $1, 2, \ldots, n{-}1$ 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 $a, b \in \{2, 3, \ldots, n{-}1\}$ schreiben. Gemäß Induktionsannahme gibt es daher einerseits $k \in \mathbb{N}$ und Primzahlen $p_1, p_2, \ldots, p_k \in \mathbb{N}$ mit $a = p_1 p_2 \cdot \ldots \cdot p_k$, andererseits $\ell \in \mathbb{N}$ und Primzahlen $q_1, q_2, \ldots, q_\ell \in \mathbb{N}$ mit $b = q_1 q_2 \cdot \ldots \cdot q_\ell$. Setzen wir $p_{k+i} := q_i$ für alle $i \in \{1, 2, \ldots, \ell\}$, so ergibt sich mit

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

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

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:

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

Hierbei ist (nur jetzt einmal, 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 $S\colon \mathbb{Z} \to \mathbb{Z}$ 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

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

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

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

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

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

und mit Rekursion als

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

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

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

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

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

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

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

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

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

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

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

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

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

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**

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

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

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

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

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

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

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

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

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

darauf aufbauend dann

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

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 $k \le \ell$ in $\mathbb{Z}$ das Produkt von $a_k, a_{k+1}, \ldots, a_{\ell-1}, a_\ell \in \mathbb{Z}$ mit dem **Produktzeichen** $\prod$ (nach dem Pi genannten griechischen Buchstaben Π) als

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

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 $I = \{i_1, i_2, \ldots, i_n\}$ 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 $j = i+v$)

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

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

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

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

$$\sum_{i\in I}(a_i+b_i) = \left(\sum_{i\in I} a_i\right) + \left(\sum_{i\in I} b_i\right), \qquad \prod_{i\in I}(a_i+b_i) = \left(\prod_{i\in I} a_i\right)\left(\prod_{i\in I} b_i\right),$$
$$\sum_{i\in I}(za_i) = z\sum_{i\in I} a_i\,, \qquad \prod_{i\in I}(a_i^n) = \left(\prod_{i\in I} a_i\right)^n.$$

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

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

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 $zm := z{\cdot}10^n{+}m$ 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 $0, 1, 2, \ldots, b-2, b-1 \in \mathbb{Z}$ des Dezimalsystems in üblicher Bedeutung und muss für $b > 10$ Ziffersymbole für die Dezimalzahlen $10, 11, 12, \ldots, b-2, b-1 \in \mathbb{Z}$ 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

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

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 $\forall x \in U\colon x \cup \{x\} \in U$. Wir erklären $\mathbb{N}$ als Durchschnitt aller Teilmengen von U, die diese Eigenschaften von U teilen, definieren $S\colon \mathbb{N} \to \mathbb{N}$ 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 $1 \notin \mathrm{S}(\mathbb{N})$.

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 $\forall x \in M\colon x \cup \{x\} \in M$. 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

$$1 := \emptyset\,, \qquad 2 := 1 \cup \{1\}\,, \qquad 3 := 2 \cup \{2\}\,, \qquad 4 := 3 \cup \{3\}\,, \qquad 5 := 4 \cup \{4\}\,, \qquad \ldots$$

und konkreter als

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

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 $(\widetilde{\mathbb{N}}, \widetilde{S}, \widetilde{1})$ erfüllt, so können $\mathbb{N}$ und $\widetilde{\mathbb{N}}$ durch eine Bijektion $f\colon \mathbb{N} \to \widetilde{\mathbb{N}}$ identifiziert werden, die $f(1) = \widetilde{1}$ und $f \circ S = \widetilde{S} \circ f$ erfüllt.*

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

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

Um Surjektivität von f nachzuweisen, beobachten wir einerseits $\widetilde{1} \in f(\mathbb{N})$ und andererseits $\widetilde{n} \in f(\mathbb{N}) \Longrightarrow \widetilde{S}(\widetilde{n}) \in f(\mathbb{N})$ (wobei letzteres gilt, weil $\widetilde{n} \in f(\mathbb{N})$ ja $\widetilde{n} = f(n)$ für ein $n \in \mathbb{N}$ und damit auch $\widetilde{S}(\widetilde{n}) = \widetilde{S}(f(n)) = f(S(n))$ bedeutet). Aufgrund dieser Beobachtungen gibt das Induktionsaxiom von $(\widetilde{\mathbb{N}}, \widetilde{S}, \widetilde{1})$ schon $f(\mathbb{N}) = \widetilde{\mathbb{N}}$, 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 $\widetilde{\mathbb{N}}$ die gleichen Axiome wie für $\mathbb{N}$ haben, können wir auch auf $\widetilde{\mathbb{N}}$ eine Addition $\widetilde{+}$ rekursiv einführen und erhalten analoge Eigenschaften. Jetzt ergibt sich aus der Vertauschbarkeit $f \circ S = \widetilde{S} \circ f$ von f mit $S, \widetilde{S}$ die Vertauschbarkeit von f mit $+, \widetilde{+}$ in der Form $f(m+n) = f(m)\widetilde{+}f(n)$ 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 $+, \widetilde{+}$ 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 $\widetilde{1} = f(1) = f(n) = f(n-1)\widetilde{+}\widetilde{1}$ (Rechenregeln und Vertauschbarkeit von f mit Addition verwendet) erhalten wir den Widerspruch, dass $\widetilde{1}$ ein Nachfolger ist. Im Subfall $m \neq 1$ bekommen wir auf ähnliche Weise $\widetilde{1}\widetilde{+}f(m-1) = f(m) = f(n) = f(n-m)\widetilde{+}\widetilde{1}\widetilde{+}f(m-1)$. Elimination des letzten Summanden $f(m-1)$ auf beiden Seiten der resultierenden Gleichung führt erneut auf den Widerspruch, dass $\widetilde{1}$ 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. □

Exkurs: 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 $A \Longrightarrow B$:** 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 $(\neg B) \Longrightarrow (\neg A)$, 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 $A \Longrightarrow B$ 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) $A \iff H_1$, $H_1 \iff H_2$, $H_2 \iff H_3$, …, $H_{n-1} \iff H_n$, $H_n \iff B$ (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 $\exists x \in \mathcal{X}\colon \forall y \in \mathcal{Y}\colon P(x,y)$ 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** $f, g\colon \mathcal{X} \to \mathcal{Y}$:

- **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 $f(x) = f(\widetilde{x}) \Longrightarrow x = \widetilde{x}$ für alle $x, \widetilde{x} \in \mathcal{X}$. Dies kann direkt, per Kontraposition ($x \neq \widetilde{x} \Longrightarrow f(x) \neq f(\widetilde{x})$) oder indirekt ($f(x) = f(\widetilde{x})$ für $x \neq \widetilde{x}$ 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* $x, \widetilde{x} \in \mathcal{X}$ mit $x \neq \widetilde{x}$, $f(x) = f(\widetilde{x})$, 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 $z \in \{z_0, z_0{+}1, z_0{+}2, \ldots\}$):

- 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 $A(1)$, $A(2)$, $\ldots$ $A(n)$ 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: $\ldots$“ oder „Behauptung: $\ldots$“! 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 $A \Longrightarrow B$ **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 $\mathrm{Rel}(\mathcal{X}, \mathcal{Y})$. Wir kürzen $\mathrm{Rel}(\mathcal{X}) := \mathrm{Rel}(\mathcal{X}, \mathcal{X})$ ab.*

Bemerkung. Für beliebige $n \in \mathbb{N}$ kann man eine ***n*-stellige Relation** zwischen Mengen $\mathcal{X}_1, \mathcal{X}_2, \ldots, \mathcal{X}_n$ als Tupel $(\mathcal{X}_1, \mathcal{X}_2, \ldots, \mathcal{X}_n, T)$ mit einer Teilmenge T des n-fachen kartesischen Produkts $\mathcal{X}_1\times\mathcal{X}_2\times\ldots\times\mathcal{X}_n$ 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 $R \in \mathrm{Rel}(\mathcal{X}, \mathcal{Y})$ der in Abbildung 25 gezeigte Graph $\mathrm{G}_R \subset \mathcal{X}\times\mathcal{Y}$. Die wahre Bedeutung von Relationen erschließt sich aber tatsächlich weniger aus der Definition und mehr aus folgenden Sprech-, Schreib- und Betrachtungsweisen:

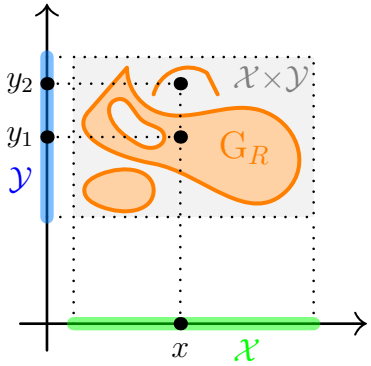


Abb. 25: Der Graph G_R eines $R \in \mathrm{Rel}(\mathcal{X}, \mathcal{Y})$ mit $\mathcal{X}, \mathcal{Y} \subset \mathbb{R}$ sowie $x \in \mathcal{X}$ und $y_1, y_2 \in \mathcal{Y}$ mit $x\,R\,y_1$, aber $\neg(x\,R\,y_2)$.

Notation & Betrachtungsweise (für/bei Relationen). *Seien $\mathcal{X}$, $\mathcal{Y}$ Mengen, $x \in \mathcal{X}$, $y \in \mathcal{Y}$ und $R \in \mathrm{Rel}(\mathcal{X}, \mathcal{Y})$. Wir sagen und schreiben im Fall $(x, y) \in \mathrm{G}_R$, 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.*

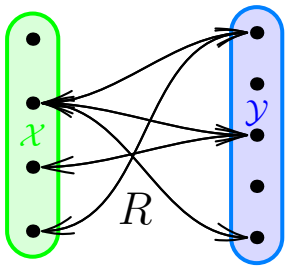


Abb. 26: Darstellung einer Relation R zwischen Mengen $\mathcal{X}$ und $\mathcal{Y}$ mit endlich vielen Elementen

Beispiele (von Relationen)**.**

(0) Für beliebige Mengen $\mathcal{X}, \mathcal{Y}$ enthält $\mathrm{Rel}(\mathcal{X}, \mathcal{Y})$ 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
$$y \overset{\mathrm{g}}{\sim} z :\Longleftrightarrow z-y \text{ ist gerade}, \qquad y \overset{\mathrm{u}}{\sim} z :\Longleftrightarrow z-y \text{ ist ungerade}$$
für $y, z \in \mathbb{Z}$ werden zwei Relationen $\overset{\mathrm{g}}{\sim}, \overset{\mathrm{u}}{\sim} \in \mathrm{Rel}(\mathbb{Z})$ erklärt, von denen für jedes $(y, z) \in \mathbb{Z}^2$ eine gilt und eine nicht. Zum Beispiel gelten $2 \overset{\mathrm{g}}{\sim} 4$, $(-2) \overset{\mathrm{u}}{\sim} 5$, $(-7) \overset{\mathrm{g}}{\sim} (-7)$ und $9 \overset{\mathrm{u}}{\sim} 0$. Die Graphen dieser beiden Relationen sind die Mengen $\mathrm{G}_{\overset{\mathrm{g}}{\sim}} = \{(y, z) \in \mathbb{Z}^2 \mid z-y \text{ ist gerade}\}$ und $\mathrm{G}_{\overset{\mathrm{u}}{\sim}} = \{(y, z) \in \mathbb{Z}^2 \mid z-y \text{ ist ungerade}\}$.

(2) Für jede Menge M ist die **Gleichheit „=“ von Elementen** eine Relation $(M, M, \mathrm{G}_=)$ auf M mit Graph $\mathrm{G}_= = \Delta_M := \{(x, y) \in M^2 \mid x = y\}$.

(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 $\mathrm{G}_\in = \{(x, M) \in \mathcal{X}\times\mathcal{S} \mid x \in M\}$. 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
$$z > y :\Longleftrightarrow y < z :\Longleftrightarrow z-y \in \mathbb{N} \qquad \text{für } y, z \in \mathbb{Z}$$
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 $\mathrm{Abb}(\mathcal{X}, \mathbb{B})$ 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 $f, g \in \mathrm{Abb}(\mathcal{X}, \mathbb{B})$ die meisten genannten Symbole $\square$ standardmäßig im punktweisen Sinn
$$f \,\square\, g :\Longleftrightarrow f \,\square\, g \text{ auf } \mathcal{X} :\Longleftrightarrow \forall x \in \mathcal{X}\colon f(x) \,\square\, g(x)$$
versteht. Lediglich bei der Ungleichheit $f \neq g$ hängt es tatsächlich vom Kontext ab, ob sie wie gerade beschrieben als $\forall x \in \mathcal{X}\colon f(x) \neq g(x)$ oder als logisches Gegenteil $\exists x \in \mathcal{X}\colon f(x) \neq g(x)$ der Gleichheit $f = g$ zu verstehen ist. Speziell für konstante $g \equiv y$ unterscheidet man hierfür manchmal die Notationen $f \neq y$ für $\forall x \in \mathcal{X}\colon f(x) \neq y$ und $f \not\equiv y$ für $\exists x \in \mathcal{X}\colon f(x) \neq y$. 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** „$|$“ ist auf jedem ganzzahligen Zahlbereich $\mathbb{B} \in \{\mathbb{N}_0, \mathbb{N}, \mathbb{Z}\}$ sinnvoll. Dabei bedeutet $t|z$ mit $t, z \in \mathbb{B}$, dass t ein Teiler von z ist, oder als Formel
$$t|z :\Longleftrightarrow \exists d \in \mathbb{B}\colon td = z \qquad \text{für } t, z, \in \mathbb{B}\,.$$

(8) Für jede feste Grundmenge $\mathcal{X}$ ist **Disjunktheit von Teilmengen** eine Relation auf $\mathcal{P}(\mathcal{X})$.

(9) Jede Funktion $f\colon \mathcal{X} \to \mathcal{Y}$ zwischen Mengen $\mathcal{X}, \mathcal{Y}$ induziert eine Relation $R \in \mathrm{Rel}(\mathcal{X}, \mathcal{Y})$ mit gleichem Graph $\mathrm{G}_R = \mathrm{G}_f$ (wobei $\mathrm{G}_f = \{(x, y) \in \mathcal{X}\times\mathcal{Y} \mid f(x) = y\}$ definiert war) oder äquivalent mit

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

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 $R \in \mathrm{Rel}(\mathcal{X}, \mathcal{Y})$ mit der „Genau-ein-y-Eigenschaft“ des Beispiels (9) durch eine eindeutig bestimmte Abbildung $f\colon \mathcal{X} \to \mathcal{Y}$ 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 $\mathcal{X} \to \mathcal{Y}$ und Relationen in $\mathrm{Rel}(\mathcal{X}, \mathcal{Y})$ 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 $f\colon \mathcal{X} \to \mathcal{Y}$ von $\mathcal{X}$ nach $\mathcal{Y}$ ist eine Relation $R \in \mathrm{Rel}(\mathcal{X}, \mathcal{Y})$, 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[9] 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 $\emptyset \to \mathcal{Y}$, 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 $f_1 \in \mathbf{Abb}(\mathcal{X}_1, \mathcal{Y}_1)$ und $f_2 \in \mathbf{Abb}(\mathcal{X}_2, \mathcal{Y}_2)$** 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 $R \in \mathrm{Rel}(\mathcal{X}, \mathcal{Y})$ 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

[9] 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 $\mathcal{X} \to \mathcal{Y}$ 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 $f\colon \mathcal{X} \to \mathcal{Y}$ mit $\mathrm{G}_f \subset \mathrm{G}_R$.

Dies ergibt sich durch Anwendung des Auswahlaxioms aus Abschnitt 1.4 auf das System der disjunkten nicht-leeren Mengen $\mathrm{G}_R \cap (\{x\}\times\mathcal{Y})$ mit $x \in \mathcal{X}$ und Festlegung von $f(x)$ mit $x \in \mathcal{X}$ als y-Eintrag des ausgewählten Paars (x,y) aus $\mathrm{G}_R \cap (\{x\}\times\mathcal{Y})$. 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 $R \in \mathrm{Rel}(\mathcal{S}, \bigcup_{M\in\mathcal{S}} M)$ mit $\mathrm{G}_R := \bigcup_{M\in\mathcal{S}} (\{M\}\times M)$ anwenden und erhält erst eine Abbildung $f\colon \mathcal{S} \to \bigcup_{M\in\mathcal{S}} M$ mit $\mathrm{G}_f \subset \mathrm{G}_R$ und daraus dann die Auswahlmenge $A := \mathrm{Bild}(f) \subset \bigcup_{M\in\mathcal{S}} M$ mit $A \cap M = \{f(M)\}$ für jedes $M \in \mathcal{S}$. □

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** $R \in \mathrm{Rel}(\mathcal{X},\mathcal{Y})$ und $S \in \mathrm{Rel}(\mathcal{Y},\mathcal{Z})$ ist die Relation $S \circ R := RS \in \mathrm{Rel}(\mathcal{X},\mathcal{Z})$ mit*

$$x\,(RS)\,z :\Longleftrightarrow \exists y \in \mathcal{Y}\colon (x\,R\,y \wedge y\,S\,z) \qquad \text{für alle } x \in \mathcal{X}\,,\ z \in \mathcal{Z}\,.$$

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

$$y\,R^{-1}\,x :\Longleftrightarrow x\,R\,y \qquad \text{für alle } x \in \mathcal{X}\,,\ y \in \mathcal{Y}\,.$$

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

$$x\,R^{\mathrm{c}}\,y :\Longleftrightarrow \neg(x\,R\,y) \qquad \text{für alle } x \in \mathcal{X}\,,\ y \in \mathcal{Y}\,.$$

Dies bedeutet, dass $\mathrm{G}_{R^{\mathrm{c}}}$ das Komplement von G_R in $\mathcal{X}\times\mathcal{Y}$ ist, also $\mathrm{G}_{R^{\mathrm{c}}} = (\mathrm{G}_R)^{\mathrm{c}}$ 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 $R \in \mathrm{Rel}(\mathcal{W},\mathcal{X})$, $S \in \mathrm{Rel}(\mathcal{X},\mathcal{Y})$, $T \in \mathrm{Rel}(\mathcal{Y},\mathcal{Z})$ gilt

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

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

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

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

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

(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 $\lfloor x \rfloor \in \mathbb{Z}$. Die **Abrunden-Funktion** $A\colon \mathbb{R} \to \mathbb{Z}$, $x \mapsto \lfloor x \rfloor$ ist surjektiv, aber nicht injektiv und nicht bijektiv und als Funktion nicht umkehrbar. Die Umkehr*relation* existiert aber immer und ist in diesem Fall die Relation $A^{-1} \in \mathrm{Rel}(\mathbb{Z}, \mathbb{R})$ mit $\mathrm{G}_{A^{-1}} = \{(z, r) \in \mathbb{Z}{\times}\mathbb{R} \,|\, z \leq r < z{+}1\}$. Die Graphen von A und A^{-1} werden in Abbildung 27 gezeigt.

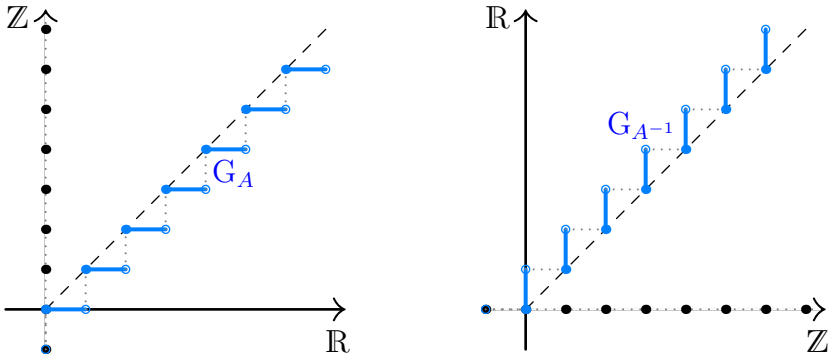


Abb. 27: Der Graph G_A der Abrunden-Funktion $A \in \mathrm{Abb}(\mathbb{R}, \mathbb{Z})$ und der Graph $\mathrm{G}_{A^{-1}}$ ihrer Umkehr*relation* $A^{-1} \in \mathrm{Rel}(\mathbb{Z}, \mathbb{R})$

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 $R \in \mathrm{Rel}(\mathcal{X})$ 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 $\left(R^{-1}\right)^{-1} = R$ 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 $R \in \mathrm{Rel}(\mathcal{X})$ 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 $\trianglelefteq$ auf $\mathcal{X}$ gehört eine strikte Ordnungsrelation $\triangleleft$ auf $\mathcal{X}$ mit „weggelassenen Gleichheitsfällen“, also mit $x \triangleleft y :\Longleftrightarrow (x \trianglelefteq y \wedge x \neq y)$ für $x, y \in \mathcal{X}$. Umgekehrt gehört zu jeder strikten Ordnungsrelation $\triangleleft$ auf $\mathcal{X}$ eine Ordnungsrelation $\trianglelefteq$ auf $\mathcal{X}$ mit „hinzugefügten Gleichheitsfällen“, also mit $x \trianglelefteq y :\Longleftrightarrow (x \triangleleft y \vee x = y)$ 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 $\leq^\delta \in \mathrm{Rel}(\mathbb{R})$ und die Ordnungsrelation $\underline{\leq}^\delta \in \mathrm{Rel}(\mathbb{R})$, die durch $x \leq^\delta y :\Longleftrightarrow x+\delta \leq y$ und $x \,\underline{\leq}^\delta\, y :\Longleftrightarrow (x+\delta < y \vee x = y)$ für $x, y \in \mathbb{R}$ definiert sind. Anschaulich spielt δ hier die Rolle eines Mindestabstands: Auf der Zahlengeraden bedeutet $x \leq^\delta y$, dass y um mindestens δ rechts von x liegen muss, und $x \,\underline{\leq}^\delta\, y$, dass y um mehr als δ 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 $\trianglelefteq$ auf $\mathcal{X}$ heißt eine **Totalordnung**, **totale Ordnung** oder **lineare Ordnung** auf einer Teilmenge T von $\mathcal{X}$, wenn $(x \trianglelefteq y) \vee (y \trianglelefteq x)$ 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 $\trianglelefteq$ auf $\mathcal{X}$ mit $x \trianglelefteq y :\Longleftrightarrow ((x \triangleleft y) \vee (x = y))$ 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 $\trianglelefteq$ auf $\mathcal{X}$ können zwei Elemente $x, y \in \mathcal{X}$ stets auf irgendeine Weise verglichen werden: Es gilt stets $x \trianglelefteq y$ oder $y \trianglelefteq x$. Bei einer allgemeinen Ordnungsrelation dagegen kann es passieren (vergleiche die folgenden Beispiele), dass für zwei Elemente $x, y \in \mathcal{X}$ weder $x \trianglelefteq y$ noch $y \trianglelefteq x$ 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 *Halb*ordnungen 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: $\trianglelefteq \in \mathrm{Rel}(\mathcal{X})$ ist genau dann eine Totalordnung auf $\mathcal{X}$, wenn $\trianglelefteq^{\mathrm{c}}$ eine strikte Totalordnung auf $\mathcal{X}$ ist. Umgekehrt damit auch: $\triangleleft \in \mathrm{Rel}(\mathcal{X})$ ist genau dann eine strikte Totalordnung auf $\mathcal{X}$, wenn $\triangleleft^{\mathrm{c}}$ 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 $\leq_{\mathrm{komp}}$ und $\leqq_{\mathrm{komp}}$ auf $\mathbb{B}^2$ **komponentenweise** durch

$$x \leq_{\mathrm{komp}} y :\Longleftrightarrow (x_1 \leq y_1\,,\, x_2 \leq y_2) \qquad \text{für } x, y \in \mathbb{B}^2\,,$$
$$x \leqq_{\mathrm{komp}} y :\Longleftrightarrow ((x_1 < y_1\,,\, x_2 < y_2) \vee (x_1 = y_1\,,\, x_2 = y_2) \qquad \text{für } x, y \in \mathbb{B}^2$$

erklären, aber $\leq_{\mathrm{komp}}$ und $\leqq_{\mathrm{komp}}$ 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 $\leq_{\mathrm{komp}}$) und $\{x \in \mathbb{B}^2 \,|\, x_1 = x_2\}$ (für $\leq_{\mathrm{komp}}$ und $\leqq_{\mathrm{komp}}$), 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)

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

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 $n \in \mathbb{N}\backslash\{1\}$ 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 $g(\widetilde{x}) < f(\widetilde{x})$ für ein anderes $\widetilde{x} \in \mathcal{X}$, 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 $\mathcal{X} \to T$.

(4) Die Relationen $\subset$, $\supset$, $\subsetneq$, $\supsetneq$ **sind *keine* (strikten) Totalordnungen** auf $\mathcal{P}(\mathcal{X})$, sofern die Grundmenge $\mathcal{X}$ zwei verschiedene Elemente $x \neq \widetilde{x}$ enthält, denn für $\{x\}, \{\widetilde{x}\} \in \mathcal{P}(\mathcal{X})$ gilt dann weder $\{x\} \subset \{\widetilde{x}\}$ noch $\{\widetilde{x}\} \subset \{x\}$ (bzw. weder $\{x\} \subsetneq \{\widetilde{x}\}$ noch $\{\widetilde{x}\} \subsetneq \{x\}$ noch $\{x\} = \{\widetilde{x}\}$). 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 $\widetilde{g} \in T$ ein größtes Element von T, so gilt sowohl $g \trianglelefteq \widetilde{g}$ als auch $\widetilde{g} \trianglelefteq g$, und die Antisymmetrie von $\trianglelefteq$ gibt $\widetilde{g} = g$.

- g die kleinste obere Schranke für T ist: Per Definition ist g obere Schranke für T und $g \trianglelefteq s$ 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 $g \trianglelefteq x$ zusätzlich $x \trianglelefteq g$ 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 $m \trianglelefteq g$ 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 $\trianglelefteq^{-1}$ auf das Vorige reduzieren. □

(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 $x \trianglelefteq m$ oder $m \trianglelefteq x$. Im zweiten Fall folgt $x = m$ per Maximalität von m und damit $x \trianglelefteq m$ gemäß der Reflexivität von $\trianglelefteq$. Also gilt tatsächlich $x \trianglelefteq m$ für jedes $x \in T$, und m ist ein größtes Element von T.

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

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 $\{x \in \mathbb{R} \mid x<0\} \dot\cup \{5\} \dot\cup \{2\}$. 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) Eine 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 $\leq_{\text{komp}}$, $\leqq_{\text{komp}}$, $\leq_{\text{lex}}$ 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 $\leqq_{\text{komp}}$ 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 $\leq^{\delta} \in \mathrm{Rel}(\mathbb{R})$ 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 $\trianglelefteq$ 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 $s \trianglelefteq x$. Dann ist auch $M \cup \{x\}$ eine Kette in $\mathcal{X}$ (denn Reflexivität gibt $x \trianglelefteq x$, die Schrankeneigenschaft von s gibt $m \trianglelefteq s$ für alle $m \in M$ und mit Transitivität folgt $m \trianglelefteq x$ 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 $x \trianglelefteq s$ und wegen Antisymmetrie von $\trianglelefteq$ 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 $f\colon \mathcal{P}(\mathcal{X}) \setminus \{\emptyset\} \to \mathcal{X}$ 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 $\widehat{T} := \{x \in \mathcal{X} \mid T \cup \{x\} \in \mathcal{K}\}$ und definieren dann eine Abbildung $g\colon \mathcal{K} \to \mathcal{K}$, die eine Kette wenn möglich um ein mit Hilfe von f ausgewähltes Element erweitert, durch

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

für alle $T \in \mathcal{K}$. Formal ist die Abbildung g wohldefiniert, weil es für nicht-maximales T eine Kette $\widetilde{T} \in \mathcal{K}$ mit $T \subsetneqq \widetilde{T}$ gibt und mit $T \subsetneqq \widetilde{T} \subset \widehat{T}$ dann $\widehat{T} \setminus T \neq \emptyset$, Wohldefiniertheit von $f\left(\widehat{T} \setminus T\right) \in \widehat{T} \setminus T$ und $T \dot\cup \left\{ f\left(\widehat{T} \setminus T\right) \right\} \in \mathcal{K}$ 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 $x, \widetilde{x} \in \bigcup \mathcal{S}$. Es gibt dann $T, \widetilde{T} \in \mathcal{S}$ mit $x \in T$ und $\widetilde{x} \in \widetilde{T}$, und wegen der Ketteneigenschaft von $\mathcal{S}$ gilt $T \subset \widetilde{T}$ oder $\widetilde{T} \subset T$. Somit gilt $x, \widetilde{x} \in \widetilde{T}$ oder $x, \widetilde{x} \in T$. Als Elemente *einer* Kette ($\widetilde{T}$ oder T) erfüllen $x, \widetilde{x}$ dann $x \trianglelefteq \widetilde{x}$ oder $\widetilde{x} \trianglelefteq x$. 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

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

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 $\exists T \in \mathcal{S}\colon g(V) \subset T$, somit $g(V) \subset \bigcup \mathcal{S}$ und $\bigcup \mathcal{S} \in \mathcal{T}_V$, oder es gilt $\forall T \in \mathcal{S}\colon T \subset V$, 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 $V \subsetneqq T$. Im ersten Fall folgt trivial $T \subset g(V)$. Im zweiten Fall benutzen wir $T \in \mathcal{T}_0 \overset{5)}{=} \mathcal{T}_V$ 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 $\exists V \in \mathcal{S}\colon T \subset V$ und somit $T \subset \bigcup \mathcal{S}$, oder es gilt $\forall V \in \mathcal{S}\colon V \subset T$ und somit $\bigcup \mathcal{S} \subset T$. Insgesamt gilt $\forall T \in \mathcal{T}_0\colon ((T \subset \bigcup \mathcal{S}) \vee (\bigcup \mathcal{S} \subset T))$, 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 $T, V \in \mathcal{T}_0 \overset{7)}{=} \mathcal{V}$ 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. □

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 $\forall n \in \mathbb{N}\colon 1 \leq n$ und $\forall n \in \mathbb{N}\colon n-1 \in \mathbb{N}_0$. 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

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

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 $z \in \{z_0, z_0+1, z_0+2, \ldots\}$ 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 $T \subset \{y \in \mathbb{N} \,|\, z \leq y\}$. Zudem ist aber $z \notin T$ (denn sonst wäre z kleinste Zahl in T) und damit sogar $T \subset \{y \in \mathbb{N} \,|\, z < y\} = \{y \in \mathbb{N} \,|\, z+1 \leq y\}$, 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 $z_0, z_0+1, z_0+2, \ldots \notin T$, 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 $\{-z \,|\, z \in \mathbb{Z}\}$.

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. □

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 $\trianglelefteq \in \mathrm{Rel}(\mathcal{W})$ durch

$$(D,G) \trianglelefteq (\widetilde{D},\widetilde{G}) :\Longleftrightarrow ((D \subset \widetilde{D}) \wedge (G \subset \widetilde{G}) \wedge (\forall x \in D\colon \forall y \in \widetilde{D} \setminus D\colon (x,y) \in \widetilde{G}))$$

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

Wir zeigen nun, dass die Voraussetzung des Zornschen Lemmas für $\mathcal{W}$ mit der Relation $\trianglelefteq$ 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 $R_{\mathcal{K}} \in \mathrm{Rel}(D_{\mathcal{K}})$, 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 $y \in \widetilde{D}$ für ein $(\widetilde{D},\widetilde{G}) \in \mathcal{K}$. 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 $y \in \widetilde{D} \setminus D$ ja $\widetilde{D} \subset D$ und damit $(\widetilde{D},\widetilde{G}) \trianglelefteq (D,G)$ ausschließt, muss $(D,G) \trianglelefteq (\widetilde{D},\widetilde{G})$ gelten. Die letzte Bedingung aus der Definition von $\trianglelefteq$ liefert für $x \in D$ und $y \in \widetilde{D} \setminus D$ dann $(x,y) \in \widetilde{G} \subset G_{\mathcal{K}}$. 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 $(D,G) \trianglelefteq (D_{\mathcal{K}},G_{\mathcal{K}})$ 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 $D \subsetneqq \mathcal{X}$. Dann könnten wir ein $x_0 \in \mathcal{X} \setminus D$ wählen, dieses x_0 durch die Festlegungen $D_0 := D \dot\cup \{x_0\}$, $G_0 := G \dot\cup (D_0 \times \{x\})$ als neues größtes Element hinzufügen und erhielten $(D_0,G_0) \in \mathcal{W}$ mit $(D,G) \trianglelefteq (D_0,G_0)$, 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. □

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 Zornsche Lemma den 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 $\{x_M | M \in \mathcal{S}\}$ gebildet werden. Diese hat dann die Auswahleigenschaft, 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*

$$\mathrm{p}_\sim \colon \mathcal{X} \to \mathcal{X}/\!\sim\,,\ x \mapsto [x]_\sim\,.$$

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

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 $\not\sim\ := \sim^{\mathrm{c}}$ 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

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

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 $y \sim x$. □

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

$$x \overset{\mathcal{S}}{\in\ni} y :\Longleftrightarrow \exists M \in \mathcal{S}\colon (x \in M \wedge y \in M) \qquad \text{für } x, y \in \mathcal{X}$$

eine Äquivalenzrelation $\overset{\mathcal{S}}{\in\ni} \in \mathrm{Rel}(\mathcal{X})$.

Dabei ergeben sich als Äquivalenzklassen von $\overset{\mathcal{S}}{\in\ni}$ gerade die in $\mathcal{S}$ enthaltenen Mengen, und aus einer Partition in Äquivalenzklassen erhält man die Äquivalenzrelation zurück, es gelten also stets $\mathcal{X}/\overset{\mathcal{S}}{\in\ni} = \mathcal{S}$ und $\overset{\mathcal{X}/\sim}{\in\ni} = \sim$. 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 $M \to M/\!=$ 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

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

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 $\overset{\mathrm{g}}{\sim}$ des früheren Beispiels (1) (wohingegen die Relation $\overset{\mathrm{u}}{\sim}$ von früher *keine* Äquivalenzrelation und hier irrelevant ist). Man verwendet bei den Modulo-Relationen die **allgemeinen Schreibweisen**

$$y = x \mod n \qquad \text{für} \qquad y \overset{n}{\sim} x$$

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

$$\mathbb{Z}/n\mathbb{Z} \qquad \text{für} \qquad \mathbb{Z}/\overset{n}{\sim}\,.$$

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

Die **Äquivalenzklassen modulo 2** sind

$$[0]_{\mathbb{Z}/2\mathbb{Z}} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\} = [2]_{\mathbb{Z}/2\mathbb{Z}} = [-2]_{\mathbb{Z}/2\mathbb{Z}}\,,$$
$$[1]_{\mathbb{Z}/2\mathbb{Z}} = \{\ldots, -5, -3, -1, 1, 3, 5, 7, \ldots\} = [3]_{\mathbb{Z}/2\mathbb{Z}} = [-1]_{\mathbb{Z}/2\mathbb{Z}}$$

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**.

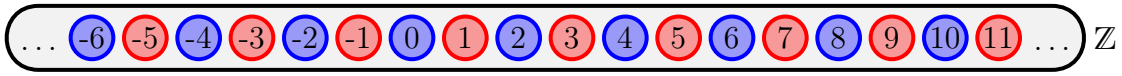


Abb. 28: Die Zerlegung $\mathbb{Z} = [0]_{\mathbb{Z}/2\mathbb{Z}} \dot\cup [1]_{\mathbb{Z}/2\mathbb{Z}}$ der ganzen Zahlen modulo 2

Die **Äquivalenzklassen modulo 3** sind

$$[0]_{\mathbb{Z}/3\mathbb{Z}} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\} \quad = [3]_{\mathbb{Z}/3\mathbb{Z}} = [-3]_{\mathbb{Z}/3\mathbb{Z}}\,,$$
$$[1]_{\mathbb{Z}/3\mathbb{Z}} = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\} = [4]_{\mathbb{Z}/3\mathbb{Z}} = [-2]_{\mathbb{Z}/3\mathbb{Z}}\,,$$
$$[2]_{\mathbb{Z}/3\mathbb{Z}} = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\} = [5]_{\mathbb{Z}/3\mathbb{Z}} = [-1]_{\mathbb{Z}/3\mathbb{Z}}$$

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 $4, 5, 6, 7, 8, 9, \ldots$ zerlegt. Ein Beispiel für eine **Äquivalenzklasse modulo 9** ist

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

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

$$m \overset{\sharp\mathrm{T}}{\sim} n :\Longleftrightarrow m \text{ und } n \text{ besitzen gleich viele Teiler in } \mathbb{N} \qquad \text{für } m, n \in \mathbb{N}\,.$$

Beispiele von Äquivalenzklassen bezüglich $\overset{\sharp\mathrm{T}}{\sim}$ sind

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

Insgesamt zerlegt die Äquivalenzrelation $\overset{\sharp T}{\sim}$ 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.

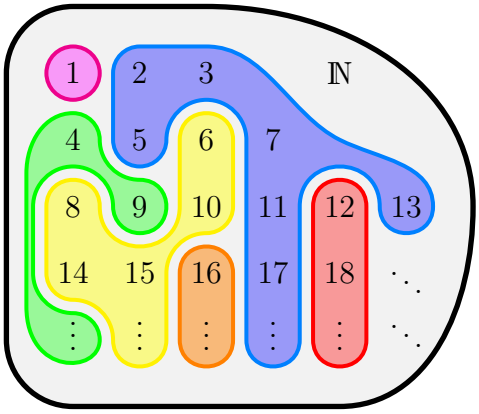


Abb. 30: Die Zerlegung von $\mathbb{N}$ in die Äquivalenzklassen der Relation $\overset{\sharp T}{\sim}$

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

$$f \propto g \mathrel{:\Longleftrightarrow} \exists \gamma \in \mathbb{R}\backslash\{0\} \colon \forall x \in \mathcal{X} \colon g(x) = \gamma f(x) \qquad \text{für } f, g \in \mathrm{Abb}(\mathcal{X}, \mathbb{R})$$

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

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

$$M \overset{123}{=} N \mathrel{:\Longleftrightarrow} M \cap \{1,2,3\} = N \cap \{1,2,3\} \qquad \text{für } M, N \subset \mathbb{N}$$

enthält die Äquivalenzklasse der Menge der ungeraden Zahlen

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

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 $\mathbb{N}\backslash\{2\}$, $\mathbb{P}\Delta\{1,2\}$ und $\{1,3,5,7,9,\ldots\}$ selbst. Insgesamt besteht $\mathcal{P}(\mathbb{N})/\overset{123}{=}$ aus 8 Äquivalenzklassen mit jeweils unendlich vielen Elementen.

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

$$M \overset{\infty}{=} N \mathrel{:\Longleftrightarrow} M\Delta N \text{ hat nur endlich viele Elemente} \qquad \text{für } M, N \subset \mathbb{N}$$

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

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

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

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

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

(Reflexivität, Symmetrie, Transitivität besagen hier $f(x)=f(x)$, $f(x)=f(y) \Longrightarrow f(y)=f(x)$ und $(f(x)=f(y) \wedge f(y)=f(z)) \Longrightarrow f(x)=f(z)$ 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 $\overset{\sharp\mathrm{T}}{=}$ ergibt sich für die Funktion $f\colon \mathbb{N} \to \mathbb{N}$, die $n \in \mathbb{N}$ auf die Anzahl der Teiler von n abbildet. Die Relation $\overset{123}{=}$ ergibt sich für $f\colon \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\{1,2,3\})\,,\ M \mapsto M \cap \{1,2,3\}$.

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

$$x \overset{f}{\cong} y :\Longleftrightarrow f(x) \cong f(y) \qquad \text{für alle } x, y \in \mathcal{X}$$

eine Äquivalenzrelation $\overset{f}{\lesssim}$ 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 $f\colon \mathcal{X} \to \mathcal{Y}$ 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 $f\colon \mathcal{X} \to \mathcal{Y}$ eine Abbildung mit der Eigenschaft*

$$y \sim x \Longrightarrow f(y) = f(x) \qquad \textit{für alle } x, y \in \mathcal{X}\,.$$

Dann gibt es genau eine Abbildung $f_*\colon \mathcal{X}/\!\sim \to \mathcal{Y}$ mit

$$f_*([x]) = f(x) \qquad \textit{für alle } x \in \mathcal{X}\,.$$

Beweis. Wir zeigen, dass $f_*\colon \mathcal{X}/\!\sim \to \mathcal{Y}$ 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. □

Beispiel (zum Satz über die Faktorisierung)**.** Wir betrachten die Abbildung $r\colon \mathbb{Z} \to \{0,1,2\}$, 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 $x = 3\lfloor x/3 \rfloor + r(x)$ für alle $x \in \mathbb{Z}$ erfüllt. Die zugehörige Relation $\overset{r}{\sim}$ im Sinn von Beispiel (7) ist die Modulo-3-Relation.

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

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

(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 $(y = x \bmod 6) \Longrightarrow (y = x \bmod 3) \Longrightarrow r(y) = r(x)$ sichergestellt — und genauso im allgemeinen Fall durch die Voraussetzung $y \sim x \Longrightarrow f(y) = f(x)$.

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 $y \sim x \Longrightarrow f(y) = f(x)$ 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 $x \sim y \Longrightarrow x \overset{f}{\sim} y$ für alle $x, y \in \mathcal{X}$ oder auch als $\mathrm{G}_\sim \subset \mathrm{G}_{\overset{f}{\sim}}$ 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 $y \sim x \Longleftrightarrow f(y) = f(x)$ für alle $x, y \in \mathcal{X}$) gilt,
- $\mathrm{Bild}(f_*) = \mathrm{Bild}(f)$ und insbesondere f_* genau dann surjektiv, wenn f surjektiv ist.

Beweis. Ist f_* injektiv, so erhalten wir $f(y) = f(x) \Longrightarrow y \sim x$ 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 $y \sim x \Longleftrightarrow f(y) = f(x)$ für alle $x, y \in \mathcal{X}$ gezeigt.

Gilt $y \sim x \Longleftrightarrow f(y) = f(x)$ für alle $x, y \in \mathcal{X}$, so erhalten wir $f_*([y]) = f_*([x]) \Longrightarrow [y] = [x]$ 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.

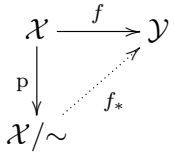
Die Gleichheit $\mathrm{Bild}(f_*) = \mathrm{Bild}(f)$ liest man aus $f_*([x]) = f(x)$ für alle $x \in \mathcal{X}$ ab und erhält dann auch die Aussage zur Surjektivität. □

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

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

(für die Quotientenabbildung $\mathrm{p}\colon \mathcal{X} \to \mathcal{X}/\!\sim$) 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 $f = f_* \circ \mathrm{p}$ 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_*.



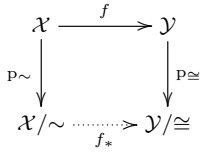
(4) Wie in Beispiel (7) kann man auch im Satz eine beliebige Äquivalenzrelation $\cong$ auf dem Ziel $\mathcal{Y}$ zulassen und erhält dann folgende **leicht allgemeinere Version**: Seien $\mathcal{X}$ und $\mathcal{Y}$ Mengen, $\sim$ eine Äquivalenzrelation auf $\mathcal{X}$ und $\cong$ eine Äquivalenzrelation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

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

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

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

oder mit anderen Worten $f_* \circ \mathrm{p}_\sim = \mathrm{p}_\cong \circ f$ 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*

$$(z,n) \overset{\mathbb{Q}}{\sim} (y,m) :\Longleftrightarrow mz = ny \qquad \textit{für alle } (z,n),(y,m) \in \mathbb{Z}\times(\mathbb{Z}\backslash\{0\})$$

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

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

- Reflexivität: $(z,n) \overset{\mathbb{Q}}{\sim} (z,n)$ bedeutet $nz = nz$ und gilt für alle $(z,n) \in \mathbb{Z}\times(\mathbb{Z}\backslash\{0\})$.
- Symmetrie: Es gilt sogar $(z,n) \overset{\mathbb{Q}}{\sim} (y,m) \Longleftrightarrow (y,m) \overset{\mathbb{Q}}{\sim} (z,n)$, denn die ausgeschriebene linke Seite $mz = ny$ und die ausgeschriebene rechte Seite $ny = mz$ besagen dasselbe.
- Transitivität: Wir zeigen $((z,n) \overset{\mathbb{Q}}{\sim} (y,m) \wedge (y,m) \overset{\mathbb{Q}}{\sim} (\ell,x)) \Longrightarrow (z,n) \overset{\mathbb{Q}}{\sim} (\ell,x)$: Die Prämisse bedeutet $mz = ny$ und $\ell y = mx$, und daraus folgt $m\ell z = \ell mz = \ell ny = n\ell y = nmx = mnx$. Wegen $m \neq 0$ erhalten wir $\ell z = nx$, also wie erforderlich $(z,n) \overset{\mathbb{Q}}{\sim} (x,\ell)$. □

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

$$\mathbb{Q} := (\mathbb{Z}\times(\mathbb{Z}\backslash\{0\}))/\!\overset{\mathbb{Q}}{\sim}$$

als die Quotientenmenge der Äquivalenzrelation $\overset{\mathbb{Q}}{\sim}$ *aus der vorausgehenden Proposition und vereinbaren die Schreibweisen*

$$z : n := z/n := \frac{z}{n} := [(z,n)] \qquad \textit{mit } z \in \mathbb{Z}\,,\ n \in \mathbb{Z}\backslash\{0\}$$

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

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

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*

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

für $y, z \in \mathbb{Z}$, $m, n \in \mathbb{Z}\backslash\{0\}$ (bei der Division auch $y \in \mathbb{Z}\backslash\{0\}$) 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 $\overset{\mathbb{Q}}{\sim}$ um in $n'z = nz'$ und $m'y = my'$ und bekommen dann $n'm'(mz\pm ny) = m'mn'z \pm n'nm'y = mnm'z' \pm nmn'y' = mn(m'z'\pm n'y')$, 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. □

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

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

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 $n \in \mathbb{Z}\backslash\{0\}$ 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 $\frac{z}{1}/\frac{n}{1} = \frac{q}{1}$ 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

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

(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 $q \geq p :\Longleftrightarrow p \leq q :\Longleftrightarrow (p < q \vee p = q)$ 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 $\frac{y}{1} < \frac{z}{1} \Longleftrightarrow y < z$ 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 *Gleich*mächtigkeit $|M| = |N|$).

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

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

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

$$|M|\le|M|\,,\qquad \big(|M| \le |N| \wedge |N| \le |M|\big) \implies |M| = |N|\,,\qquad \neg(|M|<|N| \wedge |N|<|M|)\,,$$
$$\big(|L|\le|M| \wedge |M|\le|N|\big) \implies |L|\le|N|\,,\qquad \big(|L|<|M| \wedge |M|<|N|\big) \implies |L|<|N|\,.$$

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 $M \to N$ aus einer Injektion $M \to N$ und einer Injektion $N \to M$ erfordert. Die rechten Regeln in beiden Zeilen ergeben sich dann aus diesem Satz (übrigens auch in schärferen Versionen, bei denen eines der „$<$“-Zeichen durch „$\le$“ 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 $|\mathcal{X}| \le |\mathcal{Y}|$, $|\mathcal{Y}| \le |\mathcal{X}|$, $|\mathcal{X}| = |\mathcal{Y}|$ 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 $=$, $\le$, $\ge$, $<$, $>$ sich als sehr sinnvoll und suggestiv erweist.

Als Nächstes geben wir wie angekündigt:

Beweis der Regel $(|M| \le |N| \wedge |N| \le |M|) \implies |M| = |N|$*, also des Satzes von Cantor-Schröder-Bernstein.* Es sei sowohl $|M| \le |N|$ als auch $|N| \le |M|$. Per Definition gibt es dann Injektionen $f\colon M \to N$ und $g\colon N \to M$, und aus letzterer erhalten wir durch Verkleinerung des Zielbereichs eine Bijektion $\widetilde{g}\colon N \to \mathrm{Bild}(g)$ mit Umkehrbijektion $\widetilde{g}^{-1}\colon \mathrm{Bild}(g) \to N$. Wir definieren $A_n \subset M$ für alle $n \in \mathbb{N}_0$ durch den Rekursionsanfang $A_0 := M \setminus \mathrm{Bild}(g)$ 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 $h\colon M \to N$ durch

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

(also ein gewisses „Zusammenstückeln“ von f und $\widetilde{g}^{-1}$) für alle $x \in M$ definieren, denn im Fall $x \notin A_*$ liegt x insbesondere in $M \setminus A_0 = \mathrm{Bild}(g)$, wo $\widetilde{g}^{-1}$ 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 $\widetilde{g}^{-1}(y) = \widetilde{g}^{-1}(x)$, und $y = x$ folgt aus der Bijektivität von $\widetilde{g}^{-1}$. Im Fall $x \in A_*$, $y \notin A_*$ gilt $\widetilde{g}^{-1}(y) = f(x)$. Es gibt dann ein $n \in \mathbb{N}_0$ mit $x \in A_n$ und folglich $y = \widetilde{g}(f(x)) = g(f(x)) \in A_{n+1} \subset A_*$. 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 $\widetilde{g}^{-1}$ bijektiv ist, können wir $y = \widetilde{g}^{-1}(x)$ mit $x \in \mathrm{Bild}(g) = M \setminus A_0$ schreiben. Wir unterscheiden wieder Fälle: Im Fall $x \notin A_*$ erhalten wir direkt $y = h(x) \in \mathrm{Bild}(h)$. 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 $y = \widetilde{g}^{-1}(x) = \widetilde{g}^{-1}(g(f(x'))) = \widetilde{g}^{-1}(\widetilde{g}(f(x'))) = f(x')$ mit $x' \in A_*$. Dies bedeutet auch in diesem Fall $y = h(x') \in \mathrm{Bild}(h)$. Damit ist, wie für Surjektivität benötigt, $y \in \mathrm{Bild}(h)$ in allen Fällen gezeigt.

Insgesamt ist $h\colon M \to N$ injektiv und surjektiv, also auch bijektiv, und es gilt $|M| = |N|$. □

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 ...*

- *genau $n \in \mathbb{N}_0$ Elemente hat, notiert $|M| = n$, wenn $|M| = |\{1, 2, 3, \dots, n-1, n\}|$ gilt*[10],
- ***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 $x_1 \in M$, $x_2 \in M \setminus \{x_1\}$, $x_3 \in M \setminus \{x_1, x_2\}$, $x_4 \in M \setminus \{x_1, x_2, x_3\}$, ... wählen, daraus eine Injektion $\mathbb{N} \to M$, $n \mapsto x_n$ 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-)Äbzählbarkeit**).

(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 $\mathbb{N} \to \mathbb{Z}$ 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 $\mathbb{N} \to \mathbb{N}^2$, 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:

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

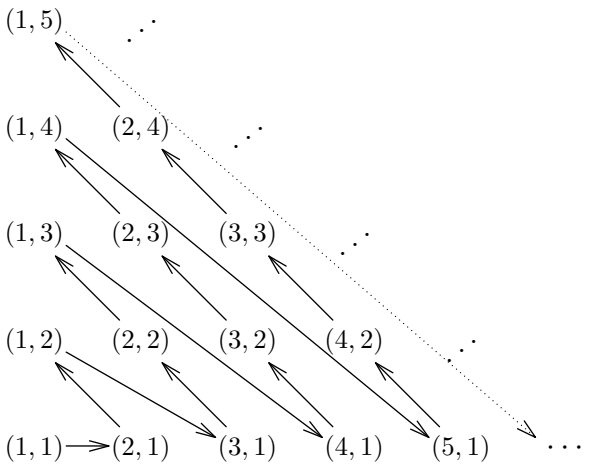


Abb. 31: Die Nummerierung von $\mathbb{N}^2$ durch das erste Cantorsche Diagonalverfahren (wobei die Pfeile keine Abbildungspfeile sind, sondern nur die Reihenfolge andeuten)

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 $\mathbb{Q} = (\mathbb{Z}\times(\mathbb{Z}\setminus\{0\}))/\mathrel{\mathop{\approx}^{\mathbb{Q}}}$ 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 Widerspruchsargument zum Nachweis, dass die **Menge $\mathbb{R}$ der reellen Zahlen** und ihre Teilmenge $\mathbb{I} := \{x \in \mathbb{R} \,|\, 0 \leq x \leq 1\}$ tatsächlich ***über*abzählbar** sind. Man verwendet dazu (worauf wir in Abschnitt 5.5 noch genauer eingehen), dass jedes $x \in \mathbb{I}$ eine Darstellung $0, z_1 z_2 z_3 \ldots$ mit unendlich vielen Nachkomma-Ziffern $z_1, z_2, z_3, \ldots \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ hat. *Angenommen*, man könnte in dieser Darstellung nun alle $x \in \mathbb{I}$ in einer Reihenfolge

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

auflisten. 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 $x^* := 0, z_1^* z_2^* z_3^* z_4^* \ldots \in \mathbb{I}$. 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[11] 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.

[11] An dieser Stelle ist etwas Vorsicht geboten, da bei der unendlichen Darstellung von Zahlen mit eigentlich nur endlich vielen Nachkomma-Stellen die Doppeldeutigkeit $0, z_1 z_2 \ldots z_{k-1} z_k 0000 \ldots = 0, z_1 z_2 \ldots z_{k-1}(z_k - 1)9999 \ldots$ 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[12] 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[13] 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 Zusatz-Annahmen 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 $|M| = n \Longrightarrow |\mathcal{P}(M)| = 2^n$ 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 $2^{|\mathbb{N}|} = \aleph_1$.

[12] 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.

[13] 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 $M \to \mathcal{P}(M)\,,\ x \mapsto \{x\}$ 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 $f\colon M \to \mathcal{P}(M)$ auszuschließen. *Angenommen*, es gäbe solch eine Bijektion f. Dann ließe sich die Teilmenge $T := \{x \in M \,|\, x \notin f(x)\} \in \mathcal{P}(M)$ 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 $f\colon M \to \mathcal{P}(M)$, womit $|M| < |\mathcal{P}(M)|$ gezeigt ist. □

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 $\mathcal{P}^k(\mathbb{N}) := \mathcal{P}(\mathcal{P}(\ldots\mathcal{P}(\mathbb{N})\ldots))$ ergibt. Man erhält dieses G einfach als $G := \mathcal{P}\big(\bigcup_{k\in\mathbb{N}_0} \mathcal{P}^k(\mathbb{N})\big)$.

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) darauf sehr weitgehend verallgemeinern**. Dies ist nützlich, um gemeinsame Eigenschaften der Zahlbereiche und der Rechenarten sowie weiterer, ähnlich gearteter Operationen einordnen, beschreiben 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 $*\colon G \times G \to G$. 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*

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

gilt.

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

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

gilt.

Beispiele (von **Verknüpfungen**)**.**

(1) **Verknüpfungen auf endlichen Mengen** können durch **Verknüpfungstafeln** 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 τ auf $\{2,3,5,7\}$ und eine Verknüpfung $\rtimes$ auf einer beliebigen 3-elementigen Menge $\{e,\alpha,\beta\}$ wie folgt gegeben:

τ	2	3	5	7
2	5	2	7	3
3	2	3	5	7
5	7	5	7	2
7	3	7	2	5

$\rtimes$	e	α	β
e	e	α	β
α	α	α	α
β	β	β	β

Dabei ist τ 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 $\rtimes$ 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 ($\alpha \rtimes \beta = \alpha \neq \beta \rtimes \alpha = \beta$).

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 $\mathbb{Z}\backslash\{0\}$ (z.B. $\frac{1}{2} \notin \mathbb{Z}$). Sie ist eine Verknüpfung auf $\mathbb{Q}\backslash\{0\}$ und $\mathbb{R}\backslash\{0\}$, 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 $\circ$ von Selbstabbildungen** eine Verknüpfung auf $\mathrm{Abb}(\mathcal{X})$. 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 $\mathrm{Abb}(\mathcal{X})$, z.B. auf der Menge der Injektionen $\mathcal{X} \to \mathcal{X}$, der Menge der Surjektionen $\mathcal{X} \to \mathcal{X}$ und der Menge der Bijektionen $\mathcal{X} \to \mathcal{X}$.

(7) Für jede Menge $\mathcal{X}$ sind die **Mengen-Operationen** Vereinigung ($\cup$), Durchschnitt ($\cap$), Differenz ($\backslash$) und symmetrische Differenz (Δ) Verknüpfungen auf der Potenzmenge $\mathcal{P}(\mathcal{X})$. Dabei sind $\cup$, $\cap$ und Δ kommutativ und assoziativ (vergleiche mit Abschnitt 1.4), während $\backslash$ für $|\mathcal{X}| \geq 1$ weder assoziativ (z.B. $(\{x\}\backslash\{x\})\backslash\emptyset \neq \{x\}\backslash(\emptyset\backslash\{x\})$) noch kommutativ (z.B. $\{x\}\backslash\emptyset \neq \emptyset\backslash\{x\}$) 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*

$$g * A := \{g * a \,|\, a \in A\}\,, \qquad A * g := \{a * g \,|\, a \in A\}\,, \qquad A * B := \{a * b \,|\, (a,b) \in A \times B\}$$

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 $A+B = \{a+b \,|\, (a,b) \in A\times B\}$ 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*

$$x * y := (x_1 * y_1, x_2 * y_2, \ldots, x_n * y_n) \in G^n \qquad \text{für } x, y \in G^n\,.$$

(2) *Für jede Menge $\mathcal{X}$ definieren wir die **punktweise** Anwendung der Verknüpfung $*$ **auf Abbildungen** $f_1, f_2 \colon \mathcal{X} \to G$ durch*

$$(f_1 * f_2)(x) := f_1(x) * f_2(x) \in G \qquad \text{für alle } x \in \mathcal{X}$$

und legen damit eine Abbildung $f_1 * f_2 \colon \mathcal{X} \to G$ 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 $\mathrm{Abb}(\mathcal{X}, G)$ der Abbildungen $\mathcal{X} \to G$. 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 $\boldsymbol{x \pm y}$**, das **komponentenweise Produkt $\boldsymbol{x \cdot y}$**, der **komponentenweise Quotient $\boldsymbol{\frac{x}{y}}$ von Tupeln** $x, y \in \mathbb{B}^n$ und die **komponentenweise Summe/Differenz $\boldsymbol{f_1 \pm f_2}$**, das **komponentenweise Produkt $\boldsymbol{f_1 \cdot f_2}$**, der **komponentenweise Quotient $\boldsymbol{\frac{f_1}{f_2}}$ von Abbildungen** $f_1, f_2 \colon \mathcal{X} \to \mathbb{B}$ **erklärt**, jedenfalls soweit die Rechenoperationen Verknüpfungen auf den Zahlbereichen $\mathbb{B} \in \{\mathbb{N}, \mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}\backslash\{0\}, \mathbb{Q}\backslash\{0\}, \mathbb{R}\backslash\{0\}\}$ 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:*

$$\begin{aligned} e^{-1} &= e && \text{für das neutrale Element } e \in G\,, \\ \left(g^{-1}\right)^{-1} &= g && \text{für invertierbares } g \in G\,, \\ \left(g * h\right)^{-1} &= h^{-1} * g^{-1} && \text{für invertierbare } g, h \in G\,. \end{aligned}$$

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 $g = g * r$ für alle $g \in G$ betrachtet. Solche Elemente sind im Allgemeinen nicht eindeutig bestimmt. Sobald aber ein linksneutrales Element ℓ* 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 τ im früheren Beispiel (1) nur bei der Verknüpfung von 5 mit sich modifiziert, die zweite unverändert)

$\circledast$	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

$\rtimes$	e	α	β
e	e	α	β
α	α	α	α
β	β	β	β

wird $(\{2,3,5,7\}, \circledast)$ zu einer abelschen Gruppe mit neutralem Element 3 und den Inversen 2^{-1}=7, 7^{-1}=2, 5^{-1}=5 sowie $(\{e, \alpha, \beta\}, \rtimes)$ zu einer nicht-kommutativen Halbgruppe mit neutralem Element e und nicht-invertierbaren Elementen α, β. 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[1]), 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):

	$\mathbb{N}$	$\mathbb{N}_0$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{Z}\backslash\{0\}$	$\mathbb{Q}\backslash\{0\}$	$\mathbb{R}\backslash\{0\}$
$+$	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 $\boldsymbol{-x}$, das **multiplikativ Inverse** zu $x \in \mathbb{B}\backslash\{0\}$ ist $\frac{\mathbf{1}}{\boldsymbol{x}}$.

[1] 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:

$\star$	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 $(G_1, *)$, $(G_2, *)$, …, $(G_n, *)$ eine (Halb-)Gruppe $(G_1 \times G_2 \times \ldots \times G_n, *)$, deren Verknüpfung durch $(g_1, g_2, \ldots, g_n) * (g'_1, g'_2, \ldots, g'_n) := (g_1 * g'_1, g_2 * g'_2, \ldots, g_n * g'_n)$ für $(g_1, g_2, \ldots, g_n), (g'_1, g'_2, \ldots, g'_n) \in G_1 \times G_2 \times \ldots \times G_n$ 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 $(\mathrm{Abb}(\mathcal{X}, G), *)$ mit der punktweisen Verknüpfung $*$ eine (Halb-)Gruppe, auf die sich auch Kommutativität und/oder Existenz des neutralen Elements überträgt. Speziell sind $(\mathrm{Abb}(\mathcal{X}, \mathbb{B}), +)$ und $(\mathrm{Abb}(\mathcal{X}, \mathbb{B}), \cdot)$ insoweit (Halb-)gruppen wie $(\mathbb{B}, +)$ und $(\mathbb{B}, \cdot)$.

(Halb-)Gruppen von Selbstabbildungen: Auch ist für jede Menge $\mathcal{X}$ auch $(\mathrm{Abb}(\mathcal{X}), \circ)$, die Menge der **Selbstabbildungen** von $\mathcal{X}$ **mit** der **Komposition** $\circ$, eine (für $|\mathcal{X}| \geq 2$ nicht kommutative) Halbgruppe mit neutralem Element $\mathrm{id}_{\mathcal{X}}$. Die Menge der Bijektionen $\mathcal{X} \to \mathcal{X}$ 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 $\mathcal{X} \to \mathcal{X}$ und die Menge der Surjektionen $\mathcal{X} \to \mathcal{X}$ stimmen übrigens für endliches $\mathcal{X}$ mit der Menge der Bijektionen $\mathcal{X} \to \mathcal{X}$ 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 Kapitel 6 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***

$$\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\overset{n}{\sim}.$$

*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*

$$[x]_{\mathbb{Z}_n} + [y]_{\mathbb{Z}_n} := [x+y]_{\mathbb{Z}_n} \qquad \textit{und} \qquad [x]_{\mathbb{Z}_n} \cdot [y]_{\mathbb{Z}_n} := [xy]_{\mathbb{Z}_n} \qquad \textit{für } x, y \in \mathbb{Z}$$

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 Inversem* $[-x]_{\mathbb{Z}_n}$ *zu* $[x]_{\mathbb{Z}_n}$ *sowie* $(\mathbb{Z}_n, \cdot\,)$ *eine kommutative Halbgruppe mit neutralem Element* $[1]_{\mathbb{Z}_n}$. *Kürzen wir* $\mathbb{Z}_p^\times := \mathbb{Z}_p \backslash \{[0]_{\mathbb{Z}_p}\}$ *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 $[x]_{\mathbb{Z}_n} = \{y \in \mathbb{Z} \,|\, y \overset{n}{\sim} x\} = \{y \in \mathbb{Z} \,|\, y{-}x = nz \text{ für ein } z \in \mathbb{Z}\} = \{x{+}nz \,|\, z \in \mathbb{Z}\} = x{+}n\mathbb{Z}$. □

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. □

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

$$[3] + [-5] = [-2] \quad \text{in } \mathbb{Z}_2\,, \qquad [1] + [1] = [0] \quad \text{in } \mathbb{Z}_2\,, \qquad [3] \cdot [5] = [1] \quad \text{in } \mathbb{Z}_7\,.$$

Dies bedeutet letztlich dasselbe wie

$$3 - 5 = -2 \mod 2\,, \qquad 1 + 1 = 0 \mod 2\,, \qquad 3 \cdot 5 = 1 \mod 7\,,$$

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 $[0] = n\mathbb{Z}$, $[1] = 1{+}n\mathbb{Z}$, $[2] = 2{+}n\mathbb{Z}$, …, $[n{-}2] = (n{-}2){+}n\mathbb{Z}$, $[n{-}1] = (n{-}1){+}n\mathbb{Z}$ 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 Verknüpfungstafeln vollständig angegeben. Wir zeigen hier die Verknüpfungstafeln

- für $\mathbb{Z}_2$:

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

$\cdot$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$

- für $\mathbb{Z}_3$:

$+$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

$\cdot$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$
$[2]$	$[0]$	$[2]$	$[1]$

- für $\mathbb{Z}_4$:

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

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 $x, y \in \{2, 3, \ldots, p{-}1\}$ 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 $x \in \{1, 2, 3, \ldots, p{-}2, p{-}1\}$, 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 $[0]$, $[x]$, $[2x]$, $[3x]$, …, $[(p{-}2)x]$, $[(p{-}1)x]$, also mit anderen Worten die Restklassen $[nx]$ mit $n \in \{0, 1, 2, \ldots, p{-}2, p{-}1\}$, in $\mathbb{Z}_p$ alle verschieden sind. Andernfalls müsste nämlich $[kx] = [\ell x]$ für $k, \ell \in \{0, 1, 2, \ldots, p{-}2, p{-}1\}$ mit $k < \ell$ gelten, und für $m := \ell{-}k \in \{1, 2, 3, \ldots, p{-}2, p{-}1\}$ bekämen wir $[mx] = [0]$, mit anderen Worten also $p|(mx)$. Mit der Eindeutigkeit der Primfaktorzerlegung (deren Beweis in Fussnote 2 des Abschnitts 5.2 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 $\{0, 1, 2, \ldots, p{-}2, p{-}1\}$ sind. Damit sind $[nx]$ mit $n \in \{0, 1, 2, \ldots, p{-}2, p{-}1\}$ in der Tat p verschiedene Elemente von $\mathbb{Z}_p$. Da $\mathbb{Z}_p$ genau die p Elemente $[0]$, $[1]$, $[2]$, …, $[p{-}2]$, $[p{-}1]$ enthält, muss somit $[nx] = [1]$ für ein $n \in \{1, 2, \ldots, p{-}2, p{-}1\}$ 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 $(\mathbb{Z}_p, \cdot\,)$). □

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 $G = \{e, g, g^2, g^3, \ldots, g^{n-1}\}$ für ein $g \in G$ mit $g^n = e \neq g^k$ für alle $k \in \{1, 2, \ldots, n-1\}$ 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, …, 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 $k, \ell \in \{0, 1, 2, \ldots, n-1\}$.

(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 $k \in \{0, 1, 2, \ldots, n-1\}$ 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 $[5] = [3]^{-1}$ als Erzeugern, denn $[3]^1 = [3]$, $[3]^2 = [2]$, $[3]^3 = [6]$, $[3]^4 = [4]$, $[3]^5 = [5]$, $[3]^6 = [1]$ und $[5]^1 = [5]$, $[5]^2 = [4]$, $[5]^3 = [6]$, $[5]^4 = [2]$, $[5]^5 = [3]$, $[5]^6 = [1]$ geben jeweils alle Elemente von $\mathbb{Z}_7^\times$, während für die anderen vier Elemente $[1]^1 = [2]^3 = [4]^3 = [6]^2 = [1]$ eintritt.

(2) Die Gruppe $(\mathbb{Z}_4,+)$ ist zyklisch von Ordnung 4 mit genau [1] und [3] als Erzeugern, denn $[1\cdot1] = [1]$, $[2\cdot1] = [2]$, $[3\cdot1] = [3]$, $[4\cdot1] = [0]$ und $[1\cdot3] = [3]$, $[2\cdot3] = [2]$, $[3\cdot3] = [1]$, $[4\cdot3] = [0]$ sind jeweils alle Elemente von $\mathbb{Z}_4$, während für die anderen beiden Elemente $[1\cdot0] = [2\cdot2] = [0]$ 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 $[1\cdot1] = [1]$, $[2\cdot1] = [2]$, …, $[(n-1)\cdot1] = [n-1]$, $[n\cdot1] = [0]$ 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 $x \in \mathbb{Z}_p^\times = \mathbb{Z}_p\backslash\{[0]\}$ die p Restklassen $[x]$, $[2x]$, $[3x]\ldots$, $[(p-1)x]$, $[px] = [0]$ 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 $\{1, 2, \ldots, n\}$ und nennen $(\mathrm{S}_n, \circ\,)$ die **symmetrische Gruppe** vom Grad n.*

(III) *Permutationen $\pi \in \mathrm{S}_n$ mit $n \in \mathbb{N}$ notieren wir manchmal in der Form*

$$\begin{aligned}\pi &= \begin{pmatrix} 1 & 2 & 3 & \ldots & n{-}1 & n \\ \pi(1) & \pi(2) & \pi(3) & \ldots & \pi(n{-}1) & \pi(n) \end{pmatrix} \\ &= \begin{pmatrix} \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n{-}1) & \sigma(n) \\ \pi(\sigma(1)) & \pi(\sigma(2)) & \pi(\sigma(3)) & \ldots & \pi(\sigma(n{-}1)) & \pi(\sigma(n)) \end{pmatrix}\end{aligned}$$

(mit einer weiteren Permutation $\sigma \in \mathrm{S}_n$).

Bemerkungen (zu Permutationen und symmetrischen Gruppen)**.**

(1) Man kann die Betrachtung von Permutationen **eigentlich immer auf den Modellfall** von S_n **über der Grundmenge $\{1, 2, \ldots, n\}$ reduzieren**, da jede endliche Menge $\mathcal{X}$ durch eine Bijektion mit $\{1, 2, \ldots, n\}$ für $n := |\mathcal{X}|$ identifiziert werden kann.

(2) Dass $(\mathrm{S}_n, \circ\,)$ (und allgemein die Menge der Bijektionen $\mathcal{X} \to \mathcal{X}$ 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 einem späteren Exkurs noch begründen, genau $n!$ Permutationen einer n-elementigen Menge, es gilt also $|\mathrm{S}_n| = n!$.

Beispiel (einer Permutation von 5 Elementen)**.** Die Permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix} = \begin{pmatrix} 4 & 2 & 5 & 1 & 3 \\ 1 & 4 & 5 & 2 & 3 \end{pmatrix} \in \mathrm{S}_5$$

ist die Bijektion $\pi\colon \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\}$ mit $1 \overset{\pi}{\mapsto} 2$, $2 \overset{\pi}{\mapsto} 4$, $3 \overset{\pi}{\mapsto} 3$, $4 \overset{\pi}{\mapsto} 1$, $5 \overset{\pi}{\mapsto} 5$.

Definitionen (**Transpositionen, Zykel**)**.** *Sei π eine Permutation einer endlichen Menge $\mathcal{X}$.*

(I) *Wir nennen π 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 π einen **Zykel** der Länge $\ell \in \mathbb{N}$ oder einen ℓ-Zykel (in $\mathcal{X}$), wenn es ein $a \in \mathcal{X}$ mit $\pi^\ell(a) = a \neq \pi^k(a)$ für alle $k \in \{1, 2, \ldots, \ell-1\}$ und $\pi(x) = x$ für alle $x \in \mathcal{X} \setminus \{a, \pi(a), \pi^2(a), \ldots, \pi^{\ell-1}(a)\}$ gibt. Für solche Zykel wird manchmal in Zykelschreibweise $\pi = (a\ \pi(a)\ \pi^2(a)\ \ldots\ \pi^{\ell-1}(a))$ 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 π ist selbstinvers. Für einen Zykel π der Länge ℓ in $\mathcal{X}$ gilt $\pi^\ell = \mathrm{id}_\mathcal{X}$.

Beispiele (der **symmetrischen Gruppen vom Grad 2 und 3**)**.** Wir betrachten folgende noch gut überschaubare Beispiele zwischen $\mathrm{S}_1 = \{\mathrm{id}\}$ und S_4 mit $|\mathrm{S}_4| = 4! = 24$:

(1) Die $2! = 2$ Elemente der **symmetrischen Gruppe $(\mathbf{S_2}, \circ)$** sind die Identität id und eine Transposition τ mit den Darstellungen

$$\mathrm{id} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \qquad \text{und} \qquad \tau = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

Offensichtlich ist τ selbstinvers und $(\mathrm{S}_2, \circ)$ zyklisch von Ordnung 2. In Zykelschreibweise kann man $\tau = (1\ 2) = (2\ 1)$ schreiben.

(2) Die $3! = 6$ Elemente der **symmetrischen Gruppe $(\mathbf{S_3}, \circ)$** sind die Identität id, drei Transpositionen τ_1, τ_2, τ_3 und zwei 3-Zykel σ_1, σ_2 mit den Darstellungen

$$\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$
$$\tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

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 Abschnitt 6.3 brauchen wir:

Satz (zur Darstellbarkeit von Permutationen durch Transpositionen)**.** *Sei π eine Permutation einer endlichen Menge $\mathcal{X}$.*

(I) *Dann kann π als Komposition $\pi = \tau_1 \circ \tau_2 \circ \ldots \circ \tau_{m-1} \circ \tau_m$ einer endlichen Zahl $m \in \mathbb{N}_0$ von Transpositionen $\tau_1, \tau_2, \ldots, \tau_{m-1}, \tau_m$ 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 π eindeutig bestimmt.*

Definitionen (**Parität/Vorzeichen von Permutationen, alternierende Gruppen**)**.**

(I) *Wir nennen eine Permutation π 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** $\mathrm{sgn}(\pi) \in \{-1, 1\}$ einer Permutation π erklären wir für gerade Permutationen π zu 1, für ungerade Permutationen π zu -1.*

(II) *Für $n \in \mathbb{N}$ setzen wir*

$$\mathrm{A}_n := \{\pi \in \mathrm{S}_n \,|\, \pi \textit{ ist gerade}\} = \{\pi \in \mathrm{S}_n \,|\, \mathrm{sgn}(\pi) = 1\}\,,$$

*und nennen $(\mathrm{A}_n, \circ)$ die **alternierende Gruppe** vom Grad n.*

Bemerkungen (zum Vorzeichen von Permutationen und der alternierenden Gruppe)**.**

(1) Für Permutationen π und σ von $\mathcal{X}$ gelten $\mathrm{sgn}(\pi^{-1}) = \mathrm{sgn}(\pi)$ und $\mathrm{sgn}(\sigma\circ\pi) = \mathrm{sgn}(\sigma)\,\mathrm{sgn}(\pi)$.

(Begründung für letzteres: Sind σ bzw. π Kompositionen von ℓ bzw. m Transpositionen, so ist $\sigma\circ\pi$ Komposition von $\ell+m$ Transpositionen. Im Fall $\mathrm{sgn}(\sigma) = \mathrm{sgn}(\pi)$ haben ℓ, m gleiche Parität, $\ell+m$ ist gerade, und es gilt $\mathrm{sgn}(\sigma\circ\pi) = 1 = \mathrm{sgn}(\sigma)\,\mathrm{sgn}(\pi)$. Im Fall $\mathrm{sgn}(\sigma) = -\mathrm{sgn}(\pi)$ dagegen haben ℓ, m verschiedene Parität, $\ell+m$ ist ungerade, und es gilt $\mathrm{sgn}(\sigma\circ\pi) = -1 = \mathrm{sgn}(\sigma)\,\mathrm{sgn}(\pi)$.)

(2) Insbesondere folgt aus Bemerkung (1), dass für $\pi, \sigma \in \mathrm{A}_n$ auch $\pi^{-1} \in \mathrm{A}_n$ und $\sigma\circ\pi \in \mathrm{A}_n$ gelten. Erst dies (zusammen mit früheren Beobachtungen) stellt sicher, dass $(\mathrm{A}_n, \circ)$ in der Tat eine Gruppe ist. Die Gruppe $(\mathrm{A}_n, \circ)$ ist *nur* für $n \in \{1, 2, 3\}$ abelsch.

(3) Für $n \in \mathbb{N}\backslash\{1\}$ enthält die Teilmenge A_n von S_n die Hälfte der Permutationen aus S_n, es gilt also $|\mathrm{A}_n| = \frac{1}{2}|\mathrm{S}_n| = \frac{n!}{2}$.

(Begründung: Sei $\tau \in \mathrm{S}_n$ eine beliebige Transposition, die als solche insbesondere selbstinvers mit $\mathrm{sgn}(\tau) = -1$ ist. Mit der vorausgehenden Bemerkung (1) und den Gruppeneigenschaften von $(\mathrm{S}_n, \circ)$ folgt, dass $\mathrm{A}_n \to \mathrm{S}_n\backslash\mathrm{A}_n$, $\pi \mapsto \tau\circ\pi$ eine wohldefinierte Bijektion von A_n nach $\mathrm{S}_n\backslash\mathrm{A}_n$ ist. Damit gilt $|\mathrm{A}_n| = |\mathrm{S}_n\backslash\mathrm{A}_n| = |\mathrm{S}_n| - |\mathrm{A}_n|$, und durch Auflösen ergibt sich $|\mathrm{A}_n| = \frac{1}{2}|\mathrm{S}_n|$.)

Beispiele (der **alternierenden Gruppen vom Grad 3 und 4**)**.** Wir betrachten folgende noch überschaubare Beispiele zwischen $\mathrm{A}_1 = \{\mathrm{id}\}$, $\mathrm{A}_2 = \{\mathrm{id}\}$ und A_5 mit $|\mathrm{A}_5| = \frac{5!}{2} = 60$:

(1) Die $\frac{3!}{2} = 3$ Elemente der **alternierenden Gruppe $(\mathbf{A_3}, \circ)$** sind die Identität id und die beiden als Elemente von $(\mathrm{S}_3, \circ)$ schon betrachteten 3-Zykel σ_1 und σ_2. Es gelten $\sigma_1^2 = \sigma_2$, $\sigma_2^2 = \sigma_1$ und $\sigma_1 \circ \sigma_2 = \mathrm{id} = \sigma_2 \circ \sigma_1$. Insbesondere ist $(\mathrm{A}_3, \circ)$ zyklisch von Ordnung 3.

(2) Die $\frac{4!}{2} = 12$ Elemente der **alternierenden Gruppe $(\mathbf{A_4}, \circ)$** sind die Identität 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

$$\mathrm{id} = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, \quad \eta_1 = \begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}, \quad \eta_2 = \begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}, \quad \eta_3 = \begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix},$$
$$\eta_4 = \begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}, \quad \eta_5 = \begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix}, \quad \eta_6 = \begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}, \quad \eta_7 = \begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix},$$
$$\eta_8 = \begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}, \quad \vartheta_1 = \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}, \quad \vartheta_2 = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}, \quad \vartheta_3 = \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}.$$

Dass $(\mathrm{A}_4, \circ)$ 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 $\emptyset \to \emptyset$ 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 π Permutation von $\mathcal{X}$. Wir wählen $x_1 \in \mathcal{X}$. Im Fall $\pi(x_1) = x_1$ sei $\tau_1 := \mathrm{id}_{\mathcal{X}}$, 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 $\widetilde{\pi}$ von $\mathcal{X} \setminus \{x_1\}$ mit $\widetilde{\pi}(x) = (\tau_1 \circ \pi)(x)$ für alle $x \in \mathcal{X} \setminus \{x_1\}$ bilden und $\widetilde{\pi}$ nach Induktionsannahme für ein $m \in \mathbb{N}$ als Komposition von $m-1$ Transpositionen schreiben. Wir erweitern diese zu $m-1$ Transpositionen $\tau_2, \tau_3, \ldots, \tau_m$ auf $\mathcal{X}$ mit $\tau_2(x_1) = \tau_3(x_1) = \ldots \tau_m(x_1) = x_1$ und bekommen $\tau_1 \circ \pi = \tau_2 \circ \tau_3 \circ \ldots \circ \tau_{m-1} \circ \tau_m$. Da τ_1 selbstinvers ist (Eigenschaft von id_X und jeder Transposition), erhalten wir $\pi = \tau_1^{-1} \circ \tau_2 \circ \tau_3 \circ \ldots \circ \tau_{m-1} \circ \tau_m = \tau_1 \circ \tau_2 \circ \tau_3 \circ \ldots \circ \tau_{m-1} \circ \tau_m$. Damit ist π die Komposition der Transpositionen $\tau_1, \tau_2, \ldots, \tau_{m-1}, \tau_m$ (im Fall $\pi(x_1) = x_1$ nach Weglassen von $\tau_1 = \mathrm{id}_{\mathcal{X}}$), und die Induktionsbehauptung ist gezeigt. □

Beweis von Teil (II) des Satzes. Wir nehmen der Einfachheit halber $\mathcal{X} = \{1, 2, \ldots, n\}$ an (könnten aber für allgemeines $\mathcal{X}$ eine beliebige Totalordnung auf $\mathcal{X}$ einführen und damit analog argumentieren). Wir betrachten die Menge

$$\mathrm{FS}(\pi) := \{(i,j) \in \{1,2,\ldots,n\}^2 \mid i < j\,,\ \pi(i) > \pi(j)\}$$

der sogenannten Fehlstände oder Inversionen eine Permutation $\pi \in \mathrm{S}_n$ und argumentieren mit der **Zahl der Fehlstände/Inversionen** $|\mathrm{FS}(\pi)| \in \mathbb{N}_0$. Für diesen Beweis entscheidend ist nun:

> **Behauptung:** Für eine beliebige Permutation $\pi \in \mathrm{S}_n$ und eine Transposition $\tau \in \mathrm{S}_n$ haben die Zahlen der Fehlstände $|\mathrm{FS}(\tau\circ\pi)|$ und $|\mathrm{FS}(\pi)|$ unterschiedliche Parität.

Zum Nachweis dieser Behauptung benutzen wir zunächst, dass die Transposition τ per Definition die Form $\tau = (k\ \ell)$ mit $k, \ell \in \{1, 2, \ldots, n\}$, $k \neq \ell$, hat. Da k und ℓ vertauscht werden können, behandeln wir *ohne Einschränkung* (typische Formulierung an solch einer Stelle!) nur den Fall $k < \ell$. Für ein Paar $(i,j) \in \{1,2,\ldots,n\}^2$ 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 $(i,j) \in \mathrm{FS}(\tau\circ\pi) \iff (i,j) \in \mathrm{FS}(\pi)$.

(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 $(i,j) \in \mathrm{FS}(\tau\circ\pi) \iff (i,j) \in \mathrm{FS}(\pi)$.

(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 $(i,j) \in \mathrm{FS}(\tau\circ\pi) \iff (i,j) \notin \mathrm{FS}(\pi)$.

(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 $(i,j) \in \mathrm{FS}(\tau\circ\pi) \iff (i,j) \notin \mathrm{FS}(\pi)$.

In den Fällen (a), (b) entnehmen wir, dass Fehlstände (i,j) von π bei $\tau\circ\pi$ weiterbestehen. In den Fällen (c), (d) treten bei $\tau\circ\pi$ gegenüber π Fehlstände hinzu oder fallen weg. Die Situation (c) tritt dabei (da es $\ell-k-1$ natürliche Zahlen zwischen k und ℓ gibt) für genau $2(\ell-k-1)$ Paare $(x,y) \in \{1,2,\ldots,n\}^2$ mit $x < y$ und dementsprechend auch für $2(\ell-k-1)$ Paare $(i,j) \in \{1,2,\ldots,n\}^2$ 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 $|\mathrm{FS}(\tau\circ\pi)\,\Delta\,\mathrm{FS}(\pi)| = 2(\ell-k-1)+1$ ungerade, wegen $|A|+|B| = |A\Delta B|+2|A\cap B|$ ist auch $|\mathrm{FS}(\tau\circ\pi)| + |\mathrm{FS}(\pi)|$ ungerade, also muss von $|\mathrm{FS}(\tau\circ\pi)|$ und $|\mathrm{FS}(\pi)|$ eins gerade, eins ungerade sein. Dies zeigt die obige Behauptung.

Da $|\mathrm{FS}(\mathrm{id})| = 0$ für die Identität $\mathrm{id} \in \mathrm{S}_n$ gerade ist, folgt für Transpositionen $\tau_1, \tau_2, \tau_3 \in \mathrm{S}_n$ iterativ, dass $|\mathrm{FS}(\tau_1)|$ ungerade ist, $|\mathrm{FS}(\tau_2 \circ \tau_1)|$ gerade ist, $|\mathrm{FS}(\tau_3 \circ \tau_2 \circ \tau_1)|$ 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 $\pi \in \mathrm{S}_n$ also $|\mathrm{FS}(\pi)|$ gerade, so kann $\pi = \tau_1 \circ \tau_2 \circ \ldots \circ \tau_{m-1} \circ \tau_m$ nur für gerades $m \in \mathbb{N}_0$ gelten. Ist $|\mathrm{FS}(\pi)|$ ungerade, so kann selbiges nur für ungerades $m \in \mathbb{N}_0$ gelten. Dies zeigt die behauptete Eindeutigkeit der Parität von m. □

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:*

$$x{\cdot}(y{+}z) = (x{\cdot}y) + (x{\cdot}z)\,, \qquad (x{+}y){\cdot}z = (x{\cdot}z) + (y{\cdot}z) \qquad \text{für alle } x, y, z \in R\,.$$

(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 **Einselement** 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*

$$0{+}x=x=x{+}0\,,\qquad 1x=x=x1\,,\qquad 0x=0=x0\,,\qquad (-x)y=-(xy)=x(-y)\,.$$

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 · ein (kommutativer) Ring mit Nullelement $0_{R^n}=(0_R,0_R,\ldots,0_R)$ und Einselement $1_{R^n}=(1_R,1_R,\ldots,1_R)$.

Allgemeiner ist für jedes $n\in\mathbb{N}$ und (kommutative) Ringe $(R_1,+,\cdot)$, $(R_2,+,\cdot)$, …, $(R_n,+,\cdot)$ auch $(R_1{\times}R_2{\times}\ldots{\times}R_n,+,\cdot)$ mit den komponentenweisen Verknüpfungen ein (kommutativer) Ring.

(3) **Abbildungs-Ringe**: Für jede Menge $\mathcal{X}$ und jeden (kommutativen) Ring $(R,+,\cdot)$ ist auch $(\mathrm{Abb}(\mathcal{X},R),+,\cdot)$ mit den punktweisen Verknüpfungen + und · ein (kommutativer) Ring.

Dagegen ergibt $(\mathrm{Abb}(R),+,\circ)$ mit der Komposition ∘ für $R\neq\{0_R\}$ *keinen* Ring: Zwar ist $(\mathrm{Abb}(R),+)$ abelsche Gruppe, $(\mathrm{Abb}(R),\circ)$ ist Halbgruppe mit neutralem Element, und das „rechte“ Distributivgesetz $(f{+}g)\circ h=f\circ h+g\circ h$ gilt für alle $f,g,h\in\mathrm{Abb}(R)$. 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 Abschnitt 6.3 **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** $\boldsymbol{R}$ auffassen. Man spricht in diesem Fall[2] von einem **Ring der Charakteristik 0**. Zum Beispiel haben $(\mathbb{B},+,\cdot)$, $(\mathbb{B}^n,+,\cdot)$, $(\mathrm{Abb}(\mathcal{X},\mathbb{B}),+,\cdot)$ 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 $\mathbb{Z}_{\boldsymbol{n}}$ **als Teilmenge von** $\boldsymbol{R}$ auffassen. In diesem Fall spricht man von einem **Ring der (endlichen) Charakteristik** $\boldsymbol{n} \in \mathbb{N}$. Zum Beispiel haben $(\mathbb{Z}_n,+,\cdot)$, $(\mathbb{Z}_n^k,+,\cdot)$, $(\mathrm{Abb}(\mathcal{X},\mathbb{Z}_n),+,\cdot)$ 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 $(\mathrm{Abb}(\mathcal{X},\mathbb{B}),+,\cdot)$ 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 $a,b \in \{2,3,\ldots,n-1\}$, 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.

[2] Gleichbedeutend mit „Charakteristik 0“ wird in der Literatur gelegentlich auch „Charakteristik ∞“ benutzt. Unter „endlicher Charakteristik“ versteht man aber so oder so nur Charakteristiken aus $\mathbb{N}$, also *nicht* 0 beziehungsweise ∞.

Bemerkungen (zu **Nullteilerfreiheit/Integritätsringen**).

(1) Dass ein kommutativer Ring $(R, +, \cdot)$ nullteilerfrei ist, bedeutet, dass die Implikation

$$xy = 0 \implies x = 0 \vee y = 0 \qquad \text{bzw. äquivalent} \qquad x \neq 0 \wedge y \neq 0 \implies xy \neq 0$$

für alle $x, y \in R$ gilt.

(2) Als vielleicht wichtigste Konsequenz gilt in nullteilerfreien Ringen und Integritätsringen $(R, +, \cdot)$ die **Kürzungsregel**

$$xz = yz \implies x = y \qquad \text{für alle } x, y \in R\,,\ z \in R \setminus \{0\}$$

(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 $(\mathrm{Abb}(\mathcal{X}, \mathbb{Q}), +, \cdot)$, $(\mathrm{Abb}(\mathcal{X}, \mathbb{R}), +, \cdot)$ 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[3], 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 $x=xyy^{-1}=0y^{-1}=0$, so dass y kein Nullteiler sein kann).

(4) Die **Charakteristik eines Körpers** oder auch eines Schiefkörpes 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

$$\begin{aligned} p &:= 2\mathrm{X}^2-3\mathrm{X}+4 \quad &&= 0\mathrm{X}^3+2\mathrm{X}^2+(-3)\mathrm{X}+4\,,\\ q &:= 3\mathrm{X}^3+6\mathrm{X}^2+\mathrm{X} &&= 3\mathrm{X}^3+6\mathrm{X}^2+1\mathrm{X}\quad +0 \end{aligned}$$

als symbolische Ausdrücke addieren wie in

$$p+q=(0{+}3)\mathrm{X}^3+(2{+}6)\mathrm{X}^2+(-3{+}1)\mathrm{X}+(4{+}0)=3\mathrm{X}^3+8\mathrm{X}^2-2\mathrm{X}+4$$

und multiplizieren wie in

$$\begin{aligned} pq &= (0{\cdot}3)\mathrm{X}^6+(2{\cdot}3{+}0{\cdot}6)\mathrm{X}^5+(-3{\cdot}3{+}2{\cdot}6{+}0{\cdot}1)\mathrm{X}^4+(4{\cdot}3{-}3{\cdot}6{+}2{\cdot}1{+}0{\cdot}0)\mathrm{X}^3\\ &\qquad +(4{\cdot}6{-}3{\cdot}1{+}2{\cdot}0)\mathrm{X}^2+(4{\cdot}1{-}3{\cdot}0)\mathrm{X}+(4{\cdot}0)\\ &= 6\mathrm{X}^5+3\mathrm{X}^4-4\mathrm{X}^3+21\mathrm{X}^2+4\mathrm{X}\,. \end{aligned}$$

Um diese Rechenoperationen allgemein und formal einführen zu können, identifizieren wir p und q mit ihren jeweiligen **Koeffizientenfolgen** $a\colon \mathbb{N}_0\to\mathbb{Z}$, $i\mapsto a_i$ und $b\colon \mathbb{N}_0\to\mathbb{Z}$, $i\mapsto b_i$, die wir uns als unendliche Tupel $(a_0,a_1,a_2,a_3,a_4,a_5,a_6,\ldots)=(4,-3,2,0,0,0,0,\ldots)\in\mathbb{Z}^{(\mathbb{N}_0)}$ und $(b_0,b_1,b_2,b_3,b_4,b_5,b_6,\ldots)=(0,1,6,3,0,0,0,\ldots)\in\mathbb{Z}^{(\mathbb{N}_0)}$ mit nur endlich vielen Nicht-Null-Einträgen vorstellen. (Zur Notation $\mathbb{Z}^{(\mathbb{N}_0)}$ siehe dabei die folgende Definition.)

[3] 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, Polynomringe**). *Sei* $(R,+,\cdot)$ *ein Ring.*

(I) *Wir setzen*

$$R[\mathrm{X}] := R^{(\mathbb{N}_0)} := \{a \in \mathrm{Abb}(\mathbb{N}_0, R) \,|\, a_i \neq 0 \text{ nur für endliche viele } i \in \mathbb{N}_0\}\,,$$

wobei wir $a_i \in R$ *für den Funktionswert von* $i \in \mathbb{N}_0$ *unter* a *schreiben und* $a \in R[\mathrm{X}]$ *auch durch Aufzählung der Funktionswerte in der Form* $a = (a_0, a_1, a_2, a_3, \ldots)$ *angeben.*

(II) *Wir nennen* $a = (a_0, a_1, a_2, a_3, \ldots) \in R[\mathrm{X}]$ *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* $(a_0, a_1, a_2, a_3, \ldots) \in R^{(\mathbb{N}_0)}$ *(genau genommen nichts anderes als* a *selbst) die* ***Koeffizientenfolge*** *von* a*.*

(III) *Wir erklären die* ***Summe*** $a{+}b \in R[\mathrm{X}]$ *und das* ***Produkt*** $ab \in R[\mathrm{X}]$ ***von Polynomen*** $a, b \in R[\mathrm{X}]$ *durch*

$$(a{+}b)_k := a_k{+}b_k\,, \qquad (ab)_k := \sum_{i=0}^{k} a_i b_{k-i} \qquad \text{für } k \in \mathbb{N}_0$$

(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* $(R[\mathrm{X}],+,\cdot)$ *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* $(R[\mathrm{X}],+,\cdot)$ *über* $(R,+,\cdot)$ *ein (kommutativer) Ring mit* $0_{R[\mathrm{X}]} = (0_R, 0_R, 0_R, 0_R, \ldots)$*,* $1_{R[\mathrm{X}]} = (1_R, 0_R, 0_R, 0_R, \ldots)$ *und additiv Inversen* $-(a_0, a_1, a_2, a_3, \ldots) = (-a_0, -a_1, -a_2, -a_3, \ldots)$ *zu* $(a_0, a_1, a_2, \ldots) \in R[\mathrm{X}]$*.*

Beweis. Dass $(R[\mathrm{X}],+)$ (mit $0_{R[\mathrm{X}]}$ und Inversen wie angegeben) eine abelsche Gruppe ist, folgt problemlos daraus, dass $(\mathrm{Abb}(\mathbb{N}_0, R),+)$ diese Eigenschaft hat, die Null in $R[\mathrm{X}]$ liegt und Inverse zu Elementen von $R[\mathrm{X}]$ in $R[\mathrm{X}]$ bleiben. Es gilt daher nur, die multiplikativen Eigenschaften und Distributivgesetze des Polynomrings zu verifizieren: Die benötigte Eigenschaft von $1_{R[\mathrm{X}]}$ entnehmen wir aus der Definition der Multiplikation (wo bei Multiplikation mit $1_{R[\mathrm{X}]}$ 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 $a, b, c \in R[\mathrm{X}]$, $k \in \mathbb{N}_0$)

$$\begin{aligned}((ab)c)_k &= \sum_{j=0}^{k}\sum_{i=0}^{j} a_i b_{j-i} c_{k-j} = \sum_{0\leq i\leq j\leq k} a_i b_{j-i} c_{k-j} = \sum_{i=0}^{k}\sum_{j=i}^{k} a_i b_{j-i} c_{k-j} \\ &= \sum_{i=0}^{k}\sum_{j=0}^{k-i} a_i b_j c_{k-i-j} = (a(bc))_k\end{aligned}$$

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 $I_k := \{(\overline{i},\overline{j}) \in \mathbb{N}_0^2 \,|\, \overline{i} \leq \overline{j} \leq k\}$ steht. Die Distributivgesetze des Polynomrings ergeben sich auf naheliegendere Weise durch Ausmultiplizieren von Summen in $(R,+,\cdot)$.

Ist schließlich $(R,+,\cdot)$ kommutativ, so bekommen wir multiplikative Kommutativität im Polynomring durch die Rechnung (für $a,b\in R[\mathrm{X}]$, $k\in\mathbb{N}_0$)

$$(ab)_k=\sum_{i=0}^{k}a_ib_{k-i}=\sum_{i=0}^{k}b_{k-i}a_i=\sum_{i=0}^{k}b_ia_{k-i}=(ba)_k$$

mit Indexlaufumkehr. Damit sind alle benötigten Eigenschaften gezeigt. □

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 $(r,0,0,0,\ldots)\in R[\mathrm{X}]$ verstehen wir*

$$R\subset R[\mathrm{X}]\,.$$

*Wir bezeichnen die Elemente von R in diesem Zusammenhang als **Konstanten** oder **konstante Polynome** und bekommen $r(a_0,a_1,a_2,a_3,\ldots)=(ra_0,ra_1,ra_2,ra_3,\ldots)$ sowie $(a_0,a_1,a_2,a_3,\ldots)r=(a_0r,a_1r,a_2r,a_3r,\ldots)$ für $r\in R$ und $(a_0,a_1,a_2,a_3,\ldots)\in R[\mathrm{X}]$.*

(II) *Wir verstehen die **Unbestimmte selbst als Polynom***

$$\mathrm{X}:=(0,1,0,0,0,\ldots)\in R[\mathrm{X}]$$

*mit $p\mathrm{X}=\mathrm{X}p$ für alle $p\in R[\mathrm{X}]$ und erhalten induktiv, dass das **Monom** $r\mathrm{X}^k$ der Ordnung $k\in\mathbb{N}_0$ mit Koeffizient $r\in R$ die Koeffizientenfolge $(0,0,\ldots,0,0,r,0,0,0,\ldots)\in R[\mathrm{X}]$ mit genau k Nullen vor einem r als dem einzigen Nicht-Null-Koeffizienten besitzt.*

(III) *Damit können wir jedes **Polynom** $p=(a_0,a_1,a_2,a_3,\ldots)\in R[\mathrm{X}]\setminus\{0\}$ **in Standard-Form**[4]*

$$\boxed{p=a_\ell\mathrm{X}^\ell+a_{\ell-1}\mathrm{X}^{\ell-1}+\ldots+a_2\mathrm{X}^2+a_1\mathrm{X}+a_0=\sum_{i=0}^{\ell}a_i\mathrm{X}^i}$$

*schreiben, wobei ℓ 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_ℓ den **Leitkoeffizient** oder führenden Koeffizient und $\operatorname{grad}(p):=\ell\in\mathbb{N}_0$ den **Grad** des Polynoms p. Für das Nullpolynom $0_{R[\mathrm{X}]}$ 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 $\sum_{i=0}^{\ell}a_i\mathrm{X}^i=\sum_{i=0}^{m}b_i\mathrm{X}^i$ von Polynomen in $R[\mathrm{X}]$ 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 $i\in\{1,2,\ldots,\ell\}$.*

(V) *An dieser Stelle erhalten wir für*

$$p=\sum_{i=0}^{\ell}a_i\mathrm{X}^i\in R[\mathrm{X}]\qquad\text{und}\qquad q=\sum_{i=0}^{m}b_i\mathrm{X}^i\in R[\mathrm{X}]$$

[4] Die Potenzen von X^i sind wie in einem allgemeinen Ring zu verstehen. Insbesondere ist $\mathrm{X}^0=1\in R\subset R[\mathrm{X}]$.

ganz allgemein die durch die anfängliche Motivation nahegelegten ***Rechenregeln für Summe und Produkt von Polynomen***

$$p+q=\sum_{k=0}^{\max\{\ell,m\}}(a_k{+}b_k)\mathrm{X}^k,\qquad pq=\sum_{k=0}^{\ell+m}\left(\sum_{i=0}^{k}a_ib_{k-i}\right)\mathrm{X}^k=\sum_{k=0}^{\ell+m}\left(\sum_{i=\max\{0,k-m\}}^{\min\{k,\ell\}}a_ib_{k-i}\right)\mathrm{X}^k,$$

wobei $\max\{x,y\}$ *bzw.* $\min\{x,y\}$ *die größere bzw. kleinere von zwei Zahlen* $x,y\in\mathbb{R}$ *bezeichnet und wir natürlich* $a_{\ell+1}=a_{\ell+2}=a_{\ell+3}=\ldots=0$ *sowie* $b_{m+1}=b_{m+2}=b_{m+3}=\ldots=0$ *verstehen.*

Wir halten noch fest:

Bemerkungen (zu **Polynomringen**).

(1) Für einen Integritätsring $(R,+,\cdot\,)$ ist auch der Polynomring $(R[\mathrm{X}],+,\cdot\,)$ ein Integritätsring.

(Begründung: Für Polynome $p=\sum_{i=0}^{\ell}a_i\mathrm{X}^i\in R[\mathrm{X}]\setminus\{0\}$ und $q=\sum_{i=0}^{m}b_i\mathrm{X}^i\in R[\mathrm{X}]\setminus\{0\}$ mit Leitkoeffizienten $a_\ell\neq 0\neq b_m$ ergibt sich als Leitkoeffizient $(\ell{+}m)$-ter Ordnung von $p{+}q$ gemäß Obigem $\sum_{i=\max\{0,\ell\}}^{\min\{\ell+m,\ell\}}a_ib_{\ell+m-i}=a_\ell b_m\neq 0$. Damit ist $pq\neq 0$ in $R[\mathrm{X}]$.)

(2) Selbst für einen Körper K ist der Polynomring $K[\mathrm{X}]$ *nie* ein Körper, denn das Polynom X ist (wie auch jedes andere Polynom vom Grad ≥ 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* $p=\sum_{i=0}^{\ell}a_i\mathrm{X}^i\in R[\mathrm{X}]$ *gehörige* ***Polynomfunktion*** $\widehat{p}\colon R\to R$ *ist durch*

$$\widehat{p}\,(r):=\sum_{i=0}^{\ell}a_ir^i\in R\qquad\qquad\text{für alle } r\in R$$

gegeben. Wir nennen $r\in R$ *eine* ***Nullstelle*** *von* $p\in R[\mathrm{X}]$ *(und auch von* $\widehat{p}\in\mathrm{Abb}(R)$*), wenn* $\widehat{p}\,(r)=0_R$ *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** $p=\sum_{i=0}^{\ell}a_i\mathrm{X}^i\in R[\mathrm{X}]$ ist formal als Koeffizientenfolge definiert und **als Objekt symbolischen Rechnens mit einer Unbestimmten X** zu verstehen. Die **Polynomfunktion** $\widehat{p}\in\mathrm{Abb}(R)$ ist **als Abbildung** $R\to R$ definiert (die übrigens ganz anders abbildet als die Koeffizientenfolge $\mathbb{N}_0\to R$ von p und mit dieser nicht unmittelbar zusammenhängt).

Noch etwas anderes ist der **Funktions*term*** $\widehat{p}\,(r)=\sum_{i=0}^{\ell}a_ir^i$ **der Polynomfunktion** $\widehat{p}$, der für jedes einzelne $r\in R$ selbst Element von R ist. Zwar besteht die Funktion $\widehat{p}$ im Wesentlichen in der Zuordnungsregel $r\mapsto\sum_{i=0}^{\ell}a_ir^i$ oder mit anderen Worten $\widehat{p}\,(r)=\sum_{i=0}^{\ell}a_ir^i$ für alle $r\in R$, die Gleichsetzung $\widehat{p}=\sum_{i=0}^{\ell}a_ir^i$ ohne „(r)“ links ist aber formal *nicht* korrekt.

(2) Die **Addition und Multiplikation im Polynomring $R[\mathrm{X}]$ entsprechen der punktweisen Addition und Multiplikation von Polynomfunktionen** in dem Sinn, dass

$$\widehat{p+q} = \widehat{p} + \widehat{q} \qquad \text{und} \qquad \widehat{p\,q} = \widehat{p}\,\widehat{q} \qquad \text{in } \mathrm{Abb}(R)$$

für alle $p, q \in R[\mathrm{X}]$ 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 $\widehat{p\,q} = \widehat{p}\,\widehat{q}$ zeigen wir, indem wir $p = \sum_{i=0}^{\ell} a_i \mathrm{X}^i$, $q = \sum_{j=0}^{m} b_j \mathrm{X}^j$ schreiben und mit der Kommutativität von $(R, +, \cdot\,)$ nachrechnen, dass

$$(\widehat{p}\,\widehat{q})(x) = \widehat{p}\,(x)\,\widehat{q}\,(x) = \left(\sum_{i=0}^{\ell} a_i x^i\right)\left(\sum_{j=0}^{m} b_j x^j\right) = \sum_{i=0}^{\ell}\sum_{j=0}^{m} a_i b_j x^{i+j}$$
$$= \sum_{i=0}^{\ell}\sum_{k=i}^{i+m} a_i b_{k-i} x^k = \sum_{0\le i\le k\le i+m\le \ell+m} a_i b_{k-i} x^k = \sum_{k=0}^{\ell+m}\sum_{i=\max\{0,k-m\}}^{\min\{k,\ell\}} a_i b_{k-i} x^k = \widehat{p\,q}\,(x)$$

für alle $x \in R$ gilt.)

(3) Als Konsequenz der vorigen Bemerkung bildet die Menge der Polynomfunktionen $R \to R$ 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 $p, q \in K[\mathrm{X}]$ mit $q \neq 0$ gibt es eindeutig bestimmte Polynome $r, s \in K[\mathrm{X}]$ mit*[5] $\mathrm{grad}(r) < \mathrm{grad}(q)$*, so dass $p = s \cdot q + r$ gilt.*

(II) ***Abspalten von Linearfaktoren*:** *Ist $x_0 \in K$ eine Nullstelle von $p \in K[\mathrm{X}]$, so kann p als $p = s \cdot (\mathrm{X} - x_0)$ mit $s \in K[\mathrm{X}]$ 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 $\mathrm{grad}(q) > \mathrm{grad}(p)$ können wir $r := p$ und $s := 0$ wählen und erhalten trivial $p = s \cdot q + r$ mit $\mathrm{grad}(r) = \mathrm{grad}(p) < \mathrm{grad}(q)$. Für $\mathrm{grad}(q) \le \mathrm{grad}(p)$ zeigen wir die Existenz durch Induktion nach $\mathrm{grad}(p) \in \mathbb{N}_0$. Beim Induktionsanfang für $\mathrm{grad}(p) = 0$ ist auch $\mathrm{grad}(q) = 0$ 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 $p \in K[\mathrm{X}]$ Grad $\ell \in \mathbb{N}$ und Leitkoeffizient a_ℓ sowie $q \in K[\mathrm{X}]$ Grad $m \in \mathbb{N}_0$ und Leitkoeffizient b_m, insbesondere $b_m \neq 0$, und es sei $m \le \ell$. Dann verschwindet bei $\widetilde{p} := p - a_\ell b_m^{-1} \mathrm{X}^{\ell-m} q \in K[\mathrm{X}]$ der Koeffizient ℓ-ter Ordnung, es gilt also $\mathrm{grad}(\widetilde{p}) < \ell$. Per Induktionsannahme gibt es daher $r, \widetilde{s} \in K[\mathrm{X}]$ mit $\mathrm{grad}(r) < \mathrm{grad}(q)$, so dass $\widetilde{p} = \widetilde{s} \cdot q + r$ gilt. Durch Umformen erhalten wir

[5] Wir erlauben $r = 0$ mit $\mathrm{grad}(r) = -\infty < \mathrm{grad}(q) \in \mathbb{N}_0$.

daraus $p = (\widetilde{s}+a_\ell b_m^{-1}\mathrm{X}^{\ell-m})\cdot q + r$, also die Induktionsbehauptung für das bereits eingeführte r und $s := \widetilde{s}+a_\ell b_m^{-1}\mathrm{X}^{\ell-m} \in K[\mathrm{X}]$.

Um Eindeutigkeit von r und s nachzuweisen, ist für $r, \widetilde{r}, s, \widetilde{s} \in K[\mathrm{X}]$ mit $\operatorname{grad}(r) < \operatorname{grad}(q)$, $\operatorname{grad}(\widetilde{r}) < \operatorname{grad}(q)$ und $\widetilde{s}\cdot q + \widetilde{r} = s\cdot q + r$ zu zeigen, dass $\widetilde{r} = r$, $\widetilde{s} = s$ sein muss. Dazu schreiben wir die Gleichung als $(\widetilde{s}-s)\cdot q = r-\widetilde{r}$ und bemerken im Fall $\widetilde{s} \neq s$, dass $\operatorname{grad}((\widetilde{s}-s)\cdot q) \geq \operatorname{grad}(q)$ gilt (Grad des Produkts ist Summe der Grade; benutzt Nullteilerfreiheit). Andererseits gilt aber $\operatorname{grad}(r-\widetilde{r}) < \operatorname{grad}(q)$, und wir erreichen einen Widerspruch. Also muss $\widetilde{s} = s$ sein, und dann folgt sofort auch $\widetilde{r} = r$. □

Beweis von Teil (II) des Satzes. Aus Teil (I) mit $q := \mathrm{X}-x_0 \in K[\mathrm{X}]$ lesen wir $p = s\cdot(\mathrm{X}-x_0)+r$ für $r, s \in K[\mathrm{X}]$ mit $\operatorname{grad}(r) < \operatorname{grad}(q) = 1$, also $r \in K$ ab. Durch Einsetzen von x_0 erhalten wir $0 = \widehat{p}\,(x_0) = \widehat{s}\,(x_0)\cdot 0 + r = r$, also gilt wie behauptet $p = s\cdot(\mathrm{X}-x_0)$. □

Beweis von Teil (III) des Satzes. Wir argumentieren indirekt: Sei $p \in K[\mathrm{X}]$ ein Polynom mit $\operatorname{grad}(p) = n \in \mathbb{N}_0$ und $(n+1)$ verschiedenen Nullstellen $x_1, x_2, \ldots, x_n, x_{n+1} \in K$. Dann erreichen wir durch $(n+1)$-malige Anwendung von Teil (II) des Satzes die Form $p = s\prod_{i=1}^{n+1}(\mathrm{X}-x_i)$ mit $s \in K[\mathrm{X}]$. Im Fall $s \neq 0$ folgt $\operatorname{grad}(p) \geq n+1$, im Fall $s = 0$ folgt $\operatorname{grad}(p) = -\infty$. Wir erhalten also in jedem Fall einen Widerspruch zu $\operatorname{grad}(p) = n \in \mathbb{N}_0$, und die Behauptung ist bewiesen. □

Beweis von Teil (IV) des Satzes. Wären $p, q \in K[\mathrm{X}]$ *verschiedene* Polynome mit $p(x) = q(x)$ für alle $x \in K$, so hätte $p-q \in K[\mathrm{X}] \setminus \{0\}$ mit $\operatorname{grad}(p-q) \in \mathbb{N}_0$ unendlich viele Nullstellen in K und stünde im Widerspruch zu Teil (III) des Satzes. □

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 $p \in R[\mathrm{X}]$ mit $\operatorname{grad}(p) = n$ 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 $\widehat{p} \equiv r \neq 0$). Für den Induktionsschritt betrachten wir $p = \sum_{i=0}^{n} a_i\mathrm{X}^i \in R[\mathrm{X}]$ mit $\operatorname{grad}(p) = n \in \mathbb{N}$. 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)

$$\widehat{p}\,(x) = \widehat{p}\,(x) - \widehat{p}\,(x_0) = \sum_{i=1}^{n} a_i(x^i - x_0^i) = (x-x_0)\sum_{i=1}^{n}\sum_{j=0}^{i-1} a_i x_0^{i-1-j}x^j = (x-x_0)\sum_{j=0}^{n-1} b_j x^j$$

für $b_j := \sum_{i=j+1}^{n} a_i x_0^{i-1-j} \in R$. Da R nullteilerfrei ist, hat das Polynom $\sum_{j=0}^{n-1} b_j\mathrm{X}^j \in R[\mathrm{X}]$ 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. □

Verfahren (Polynomdivision). Mit Teil (I) des Satzes geht das **Rechenverfahren der Polynomdivision** einher, mit dem man für gegebene Polynome $p, q \in K[\mathrm{X}]$, $q \neq 0$, über einem Körper K den Multiplikator s und den Rest r mit $p = s\cdot q + r$ und $\operatorname{grad}(r) < \operatorname{grad}(q)$ bestimmt. Man baut dabei exakt auf der Idee des vorgestellten Induktionsbeweises auf und bestimmt durch Division des Leitmonoms $a_\ell\mathrm{X}^\ell$ von p durch das Leitmonom $b_m\mathrm{X}^m$ von q zunächst das Leitmonom $a_\ell b_m^{-1}\mathrm{X}^{\ell-m}$ von s. Nun betrachtet man die „Korrektur“ $\widetilde{p} = p - a_\ell b_m^{-1}\mathcal{X}^{\ell-m}\cdot q$ und dividiert im nächsten Schritt das Leitmonom von $\widetilde{p}$ durch $b_m\mathrm{X}^m$, 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 $p := \mathrm{X}^4-4\mathrm{X}^3+4\mathrm{X}^2-2$ und $q := 2\mathrm{X}^2-4\mathrm{X}-6$ in $\mathbb{Q}[\mathrm{X}]$ wie folgt durch:

$$\begin{array}{l}
(\mathrm{X}^4-4\mathrm{X}^3 \qquad\quad +4\mathrm{X}-2) : (2\mathrm{X}^2-4\mathrm{X}-6) = \frac{1}{2}\mathrm{X}^2-\mathrm{X}-\frac{1}{2} + \dfrac{-4\mathrm{X}-5}{2\mathrm{X}^2-4\mathrm{X}-6}\,. \\
\underline{-(\mathrm{X}^4-2\mathrm{X}^3-3\mathrm{X}^2)} \\
\qquad -2\mathrm{X}^3+3\mathrm{X}^2 \\
\quad \underline{-(-2\mathrm{X}^3+4\mathrm{X}^2+6\mathrm{X})} \\
\qquad\quad -\ \mathrm{X}^2-2\mathrm{X} \\
\qquad \underline{-(-\ \mathrm{X}^2+2\mathrm{X}+3)} \\
\qquad\quad -4\mathrm{X}-5
\end{array}$$

Dabei wird im jedem Schritt ein farbiges Leitmonom der linken Seite durch das Leitmonom $2\mathrm{X}^2$ 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 $q = 2\mathrm{X}^2-4\mathrm{X}-6$ 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 $< \mathrm{grad}(q)$, womit das Verfahren endet und das verbleibende, hier violett gefärbte Polynom den Rest r bildet. Insgesamt haben wir im Beispielfall $s = \frac{1}{2}\mathrm{X}^2-\mathrm{X}-\frac{1}{2}$ und $r = -4\mathrm{X}-5$ gefunden und mit anderen Worten

$$\mathrm{X}^4-4\mathrm{X}^3+4\mathrm{X}^2-2 = \left(\tfrac{1}{2}\mathrm{X}^2-\mathrm{X}-\tfrac{1}{2}\right)\cdot(2\mathrm{X}^2-4\mathrm{X}-6)+(-4\mathrm{X}-5)$$

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

$$\sum_{\substack{i\in\{0,1,2,\ldots,\ell\}\\ j\in\{0,1,2,\ldots,m\}}} a_{ij}\mathrm{X}^i\mathrm{Y}^j := \sum_{j=0}^{m}\left(\sum_{i=0}^{\ell} a_{ij}\mathrm{X}^i\right)\mathrm{Y}^j \in \big(R[\mathrm{X}]\big)[\mathrm{Y}]$$

mit Koeffizienten $a_{ij} \in R$. Man schreibt daher

$$R[\mathrm{X},\mathrm{Y}] := (R[\mathrm{X}])[\mathrm{Y}]$$

und nennt $R[\mathrm{X},\mathrm{Y}]$ den Polynomring über R in zwei Unbestimmten X und Y (für die übrigens auch bei nicht-kommutativem Grundring stets $\mathrm{XY} = \mathrm{YX}$ und allgemeiner $p\mathrm{X} = \mathrm{X}p$, $p\mathrm{Y} = \mathrm{Y}p$ für alle $p \in R[\mathrm{X},\mathrm{Y}]$ gelten). Iteration dieser Vorgehensweise ergibt den Polynomring $R[\mathrm{X}_1,\mathrm{X}_2,\ldots,\mathrm{X}_n] := \big(\ldots\big(\big(R[\mathrm{X}_1]\big)[\mathrm{X}_2]\big)\ldots\big)[\mathrm{X}_n]$ über R in $n \in \mathbb{N}$ Unbestimmten X_1, X_2, …, 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* $(H,\circledast)$ *ist eine Abbildung* $\varphi\colon G\to H$ *mit* $\varphi(g_1{*}g_2)=\varphi(g_1)\circledast\varphi(g_2)$ *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* $\varphi\colon R\to S$ *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*[6] *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* $\mathcal{X}\to\mathcal{Y}$ *notieren wir als* $\mathrm{Hom}(\mathcal{X},\mathcal{Y})$ *und* $\mathrm{Iso}(\mathcal{X},\mathcal{Y})$, *für Endo- und Automorphismen vereinbaren wir* $\mathrm{End}(\mathcal{X}):=\mathrm{Hom}(\mathcal{X},\mathcal{X})$ *und* $\mathrm{Aut}(\mathcal{X}):=\mathrm{Iso}(\mathcal{X},\mathcal{X})$.

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 $\varphi\colon G\to H$ 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 $\varphi(e_G)=\varphi(e_G)\circledast\varphi(e_G)\circledast\varphi(e_G)^{-1}=\varphi(e_G{*}e_G)\circledast\varphi(e_G)^{-1}=\varphi(e_G)\circledast\varphi(e_G)^{-1}=e_H$ erhalten wie die Behauptung über die neutralen Elemente. Für die Regel zu den Inversen rechnen wir dann $\varphi(g)\circledast\varphi(g^{-1})=\varphi(g{*}g^{-1})=\varphi(e_G)=e_H$ und $\varphi(g^{-1})\circledast\varphi(g)=\varphi(g^{-1}{*}g)=\varphi(e_G)=e_H$.)

(3) Ein Ring- beziehungsweise Körperhomomorphismus $\varphi\colon R\to S$ 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 φ 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 $\varphi\colon R\to S\,,\ x\mapsto 0_S$.)

Beispiele (von **Homomorphismen**).

(0) Die identische Abbildung ist für jede Gruppe/jeden Ring/jeden Körper ein Automorphismus.

[6] In der fortgeschrittenen Algebra (Kategorientheorie) sind auch alternative Definitionen der verschiedenen Typen von Morphismen gebäuchlich, 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 $\mathbb{B} \to \mathbb{B}\,,\ x \mapsto -3x$ 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 $\mathbb{B}\backslash\{0\} \to \mathbb{B}\backslash\{0\}\,,\ x \mapsto x^2$ ein Gruppenendomorphismus von $(\mathbb{B}\backslash\{0\}, \cdot\,)$, denn es gilt $(xy)^2 = x^2y^2$ für $x, y \in \mathbb{B}\backslash\{0\}$.

(3) Die Abbildung $\mathbb{Z} \to \mathbb{Q} \setminus \{0\}\,,\ x \mapsto 2^x$ ist ein Gruppenmonomorphismus von der additiven Gruppe $(\mathbb{Z}, +)$ in die multiplikative Gruppe $(\mathbb{Q}\backslash\{0\}, \cdot\,)$, 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 $\mathbb{Z} \to \mathbb{Z}_n\,,\ x \mapsto [x]_{\mathbb{Z}_n}$ 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 $\mathbb{Q} \to \mathbb{R}\,,\ x \mapsto x$ von $\mathbb{Q}$ in $\mathbb{R}$ ist ein Körpermonomorphismus.

(6) Für jeden Ring $(R, +, \cdot\,)$ ist die Vertauschung der Einträge $\varphi\colon R^2 \to R^2\,,\ (x_1, x_2) \mapsto (x_2, x_1)$ ein Ringautomorphismus. Allgemeiner ist für $n \in \mathbb{N}$ und $\pi \in \mathrm{S}_n$ die **Koordinatenpermutation** $\varphi_\pi\colon R^n \to R^n\,,\ (x_1, x_2, \ldots, x_n) \mapsto (x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)})$ ein Ringautomorphismus.

(7) Für jeden kommutativen Ring $(R, +, \cdot\,)$ ist die Abbildung $R[\mathrm{X}] \to \mathrm{Abb}(R)\,,\ p \mapsto \widehat{p}$ ein Ringhomomorphismus und ebenso für jedes feste $r \in R$ die Abbildung $R[\mathrm{X}] \to R\,,\ p \mapsto \widehat{p}\,(r)$. Bei beiden Bildungen spricht man auch vom Einsetzungshomomorphismus.

(Für einen Integritätsring R mit unendlich vielen Elementen ist die erste Variante sogar Ring*mono*morphismus. Das folgt aus dem letzten Satz in Abschnitt 3.2 und der darauf folgenden Bemerkung.)

Bemerkungen (zu **Homomorphismengruppen**).

(1) Für eine Gruppe $(G, *)$ wird $\mathrm{Aut}(G)$ **mit Komposition** zu einer Gruppe, der **Automorphismengruppe** von $(G, *)$.

(Nachweis: Für $\varphi, \psi \in \mathrm{Aut}(G)$ rechnen wir $\psi\circ\varphi \in \mathrm{Aut}(G)$ 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 $\varphi^{-1} \in \mathrm{Aut}(G)$ für die Umkehrfunktion φ^{-1} aus $\varphi^{-1}(g_1{*}g_2) = \varphi^{-1}(\varphi(\varphi^{-1}(g_1)){*}\varphi(\varphi^{-1}(g_1))) = \varphi^{-1}(\varphi(\varphi^{-1}(g_1){*}\varphi^{-1}(g_2))) = \varphi^{-1}(g_1){*}\varphi^{-1}(g_2)$ für alle $g_1, g_2 \in G$.)

(2) Für eine Gruppe $(G, *)$ und eine abelsche Gruppe $(H, \circledast)$ werden $\mathrm{Hom}(G, H)$ und $\mathrm{End}(H)$ **mit punktweiser Verknüpfung** $\circledast$ auch abelsche Gruppen. Man spricht von **Homo- bzw. Endomorphismengruppen**.

(Nachweis: Für $\varphi, \psi \in \mathrm{Hom}(G, H)$ zeigen wir $\varphi\circledast\psi \in \mathrm{Hom}(G, H)$ durch die auf Kommutativität von $\circledast$ gegründete Rechnung $(\varphi\circledast\psi)(g_1{*}g_2) = \varphi(g_1{*}g_2)\circledast\psi(g_1{*}g_2) = \varphi(g_1)\circledast\varphi(g_2)\circledast\psi(g_1)\circledast\psi(g_2) = \varphi(g_1)\circledast\psi(g_1)\circledast\varphi(g_2)\circledast\psi(g_2) = (\varphi\circledast\psi)(g_1)\circledast(\varphi\circledast\psi)(g_2)$ für $g_1, g_2 \in G$. Dass die konstante Abbildung $G \to H$ auf das neutrale Element in H das neutrale Element in $\mathrm{Hom}(G, H)$ ist, ist klar. Schließlich können wir Inverse zu $\varphi \in \mathrm{Hom}(G, H)$ als punktweise Inverse φ^{-1} erhalten, denn die Rechnung $\varphi^{-1}(g_1{*}g_2) = \varphi(g_1{*}g_2)^{-1} = (\varphi(g_1)\circledast\varphi(g_2))^{-1} = \varphi(g_2)^{-1}\circledast\varphi(g_1)^{-1} = \varphi(g_1)^{-1}\circledast\varphi(g_2)^{-1}$ unter erneuter Verwendung der Kommutativität von $\circledast$ ergibt $\varphi^{-1} \in \mathrm{Hom}(G, H)$.)

(3) Für eine (meist additiv notierte) abelsche Gruppe $(G, +)$ wird $(\mathrm{End}(G), +, \circ)$ mit punktweiser Addition und Komposition sogar ein Ring, der **Endomorphismenring** von $(G, +)$. Anders als bei $(\mathrm{Abb}(G), +, \circ)$ (was gemäß Abschnitt 3.2 *kein* Ring ist) ergibt sich für Endomorphismen $\varphi, \psi, \chi \in \mathrm{End}(G)$ 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 φ. Die anderen benötigten Eigenschaften folgen aus Bemerkung (2) oder sind leicht zu prüfen.

Definitionen (Kern eines Homomorphismus).

(I) *Der **Kern eines Gruppenhomomorphismus** $\varphi\colon G \to H$ zwischen Gruppen $(G, *)$ und $(H, \circledast)$ ist*

$$\boxed{\operatorname{Kern}(\varphi) := \varphi^{-1}(\{e_H\}) = \{g \in G \mid \varphi(g) = e_H\} \subset G}$$

mit dem neutralen Element e_H von $(H, \circledast)$.

(II) *Der **Kern eines Ringhomomorphismus** $\varphi\colon R \to S$ zwischen Ringen $(R, +, \cdot)$ und $(S, \oplus, \odot)$ ist*

$$\boxed{\operatorname{Kern}(\varphi) := \varphi^{-1}(\{0_S\}) = \{x \in R \mid \varphi(x) = 0_S\} \subset R}.$$

*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 $e_G \in \operatorname{Kern}(\varphi)$ und wegen $\varphi(0_R) = 0_S$ in (II) stets $0_R \in \operatorname{Kern}(\varphi)$.

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 $\varphi\colon G \to H$ von Gruppen $(G, *)$ und $(H, \circledast)$ gilt:*

$$\boxed{\varphi \text{ injektiv} \iff \operatorname{Kern}\varphi = \{e_G\}}.$$

(II) *Für einen Homomorphismus $\varphi\colon R \to S$ von Ringen $(R, +, \cdot)$ und $(S, \oplus, \odot)$ gilt:*

$$\boxed{\varphi \text{ injektiv} \iff \operatorname{Kern}\varphi = \{0_R\}}.$$

(III) *Ein Homomorphismus $\varphi\colon K \to L$ 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, $\operatorname{Kern}(\varphi) \subset \{0_K\}$ für jeden Körperhomomorphismus $\varphi\colon K \to L$ zu zeigen (denn nach der Bemerkung ist dies gleichbedeutend mit $\operatorname{Kern}(\varphi) = \{0_K\}$ und gibt gemäß Teil (II) Injektivität). Dazu sei $x \in \operatorname{Kern}(\varphi)$, 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 $\operatorname{Kern}(\varphi) \subset \{0_K\}$ ist gezeigt. □

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* $x \in U\backslash\{0\}$*.*

Beispiele (für algebraische **Unterstrukturen**)**.**

(1) Für jedes $n \in \mathbb{N}$ ist $n\mathbb{Z}$ Untergruppe von $(\mathbb{Z},+)$, aber für $n \in \mathbb{N}\backslash\{1\}$ 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 $(\mathrm{S}_n,\circ)$.

(4) Für eine Gruppe $(G,*)$ und eine abelsche Gruppe $(H,\circledast)$ sind $\mathrm{Aut}(G)$ Untergruppe von $(\{f \in \mathrm{Abb}(G) \mid f \text{ bijektiv}\},\circ)$ und $(\mathrm{Hom}(G,H),*)$ Untergruppe von $(\mathrm{Abb}(G,H),*)$.

(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 $U\backslash\{0\} \neq \emptyset$ und $x - y \in U$ für alle $x, y \in U$ sowie $x^{-1}y \in U$ für alle $x, y \in U\backslash\{0\}$.

(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 $g_1, g_2, \ldots, g_n \in G$ wird $\langle g_1, g_2, \ldots, g_n \rangle := \langle \{g_1, g_2, \ldots, g_n\} \rangle$ 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 $\mathcal{S}_A := \{V \subset G \,|\, V \text{ Untergruppe von } (G, *),\ A \subset V\}$ 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. □

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 $(\mathbb{Z}[\mathrm{X}], +, \cdot\,)$ wird der von $\mathrm{X}^3 \in \mathbb{Z}[\mathrm{X}]$ erzeugte Unterring

$$\left\langle \mathrm{X}^3 \right\rangle = \left\{ a_\ell \mathrm{X}^{3\ell} + a_{\ell-1}\mathrm{X}^{3(\ell-1)} + \ldots + a_1 \mathrm{X}^3 + a_0 \,|\, \ell \in \mathbb{N}_0\,,\ a_i \in \mathbb{Z} \right\}$$

gelegentlich als $\mathbb{Z}[\mathrm{X}^3]$ aufgefasst — wobei, wenn man die Definition über Koeffizientenfolgen genau nimmt, $\left\langle \mathrm{X}^3 \right\rangle$ *nur isomorph* zu $\mathbb{Z}[\mathrm{X}^3] = \mathbb{Z}[\mathrm{X}]$ 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*

$$x \overset{U}{\sim} y :\Longleftrightarrow x^{-1} * y \in U \qquad \text{für } x, y \in G$$

eine Äquivalenzrelation $\overset{U}{\sim}$ auf G definiert, bei der $\left|[y]_{\overset{U}{\sim}}\right| = \left|[x]_{\overset{U}{\sim}}\right|$ 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*

$$G : U := G/\overset{U}{\sim} = \{[x]_{G:U} \,|\, x \in G\}$$

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 $\overset{U}{\sim}$: 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 $[x]_{\underset{\sim}{U}} = x * U$ ergibt sich aus $x \overset{U}{\sim} y \iff x^{-1} * y \in U \iff y \in x * U$ 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 $\lambda\colon [x]_{\underset{\sim}{U}} \to [y]_{\underset{\sim}{U}}$ (denn $z \in [x]_{\underset{\sim}{U}} = x * U$ impliziert $y * x^{-1} * z \in y * x^{-1} * x * U = y * U = [y]_{\underset{\sim}{U}}$). Analog gibt $\mu(z) := x * y^{-1} * z$ eine Abbildung $\mu\colon [y]_{\underset{\sim}{U}} \to [x]_{\underset{\sim}{U}}$, die die Umkehrabbildung zu λ ist. Somit ist λ eine Bijektion $[x]_{\underset{\sim}{U}} \to [y]_{\underset{\sim}{U}}$, und es gilt $\big|[y]_{\underset{\sim}{U}}\big| = \big|[x]_{\underset{\sim}{U}}\big|$. □

Bemerkung. Sei U eine Untergruppe einer Gruppe $(G, *)$. Eine sehr ähnliche Äquivalenzrelation auf G erhält man durch die Festlegung $x \overset{U}{\sim}_{\circ} y \mathrel{:\Longleftrightarrow} y * x^{-1}$ für $x, y \in G$. Die Äquivalenzklassen $[x]_{\underset{\sim}{U}_{\circ}} = U * x$ von $\overset{U}{\sim}_{\circ}$ 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 $k \in \{1, 2, \ldots, m-1\}$ (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, … unendliche viele verschiedene Elemente von G). Nun muss die von g erzeugte Untergruppe $\langle g \rangle$ gleich $\{e_G, g, g^2, g^3, \ldots, g^{m-1}\}$ 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. □

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 $|\mathrm{S}_3| = 6$ (Bezeichnungen aus Abschnitt 3.1):

Ordnung	1	2	3	6
Elemente	id	τ_1, τ_2, τ_3	σ_1, σ_2	—
Untergruppen	$\{\mathrm{id}\}$	$\langle\tau_1\rangle = \{\mathrm{id}, \tau_1\}, \langle\tau_2\rangle, \langle\tau_3\rangle$	$\langle\sigma_1\rangle = \langle\sigma_2\rangle = \{\mathrm{id}, \sigma_1, \sigma_2\}$	S_3

In diesem Beispiel sind alle echten Untergruppen (also alle außer S_3 selbst) zyklisch.

(3) in der **alternierenden Gruppe $(\mathbf{A_4}, \circ)$** mit $|\mathrm{A}_4| = 12$ (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	$\{\mathrm{id}\}$	$\langle\vartheta_1\rangle,\langle\vartheta_2\rangle,\langle\vartheta_3\rangle$	$\langle\eta_1\rangle{=}\langle\eta_2\rangle,\langle\eta_3\rangle,\langle\eta_5\rangle,\langle\eta_7\rangle$	$\{\mathrm{id}, \vartheta_1, \vartheta_2, \vartheta_3\}$	–	A_4

In diesem Beispiel gibt es keine Untergruppe der aufgrund des Satzes von Lagrange zulässigen Ordnung 6, und neben A_4 ist auch die echte Untergruppe $\{\mathrm{id}, \vartheta_1, \vartheta_2, \vartheta_3\}$ 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*

$$x^p = x \mod p \quad \textit{für alle } x \in \mathbb{Z} \qquad \textit{und} \qquad x^{p-1} = 1 \mod p \quad \textit{für alle } x \in \mathbb{Z} \setminus p\mathbb{Z}\,.$$

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

$$\left[x^{p-1}\right]_{\mathbb{Z}_p} = [x]_{\mathbb{Z}_p}^{p-1} = \left([x]_{\mathbb{Z}_p}^{m}\right)^{\ell} = [1]_{\mathbb{Z}_p}^{\ell} = [1]_{\mathbb{Z}_p}\,,$$

was $x^{p-1} = 1 \bmod p$ 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 $x^p = 0 = x \bmod p$ aber ebenfalls. □

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** $\varphi\colon G \to H$ zwischen Gruppen $(G,*)$ und $(H,\circledast)$ ist **stets ein Normalteiler** in $(G,*)$. Der **Kern eines Ringhomomorphismus** $\psi\colon R \to S$ 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 $g \in G, n \in \mathrm{Kern}(\varphi)$ ist zudem $\varphi(g*n*g^{-1}) = \varphi(g)\circledast e_H \circledast \varphi(g)^{-1} = e_H$ und damit $g*\mathrm{Kern}(\varphi)*g^{-1} \subset \mathrm{Kern}(\varphi)$. Nach Bemerkung (1) ist also $\mathrm{Kern}(\varphi)$ ein Normalteiler. Für $r \in R$ und $n \in \mathrm{Kern}(\psi)$ ist $\psi(rn) = \psi(r)0 = 0$ und analog $\psi(nr) = 0$. Dies bedeutet $r\,\mathrm{Kern}(\psi) \subset \mathrm{Kern}(\psi)$ und $\mathrm{Kern}(\psi)r \subset \mathrm{Kern}(\psi)$, so dass $\mathrm{Kern}(\psi)$ ein Ideal ist.)

Satz & Definitionen (**Faktorgruppen, Faktorringe**)**.**

(I) *Ist* N *ein Normalteiler in einer Gruppe* $(G,*)$*, so erhalten wir durch*

$$[g]_{G:N} * [h]_{G:N} := [g*h]_{G:N} \qquad \textit{für } g,h \in G$$

beziehungsweise äquivalent durch

$$(g*N) * (h*N) := (g*h)*N \qquad \textit{für } g,h \in G$$

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*

$$[r]_{R:I} + [s]_{R:I} := [r+s]_{R:I} \qquad \textit{und} \qquad [r]_{R:I} \cdot [s]_{R:I} := [rs]_{R:I} \qquad \textit{für } r,s \in R$$

beziehungsweise äquivalent durch

$$(r+I)+(s+I) := (r+s)+I \qquad \textit{und} \qquad (r+I)\cdot(s+I) := (rs)+I \qquad \textit{für } r,s \in R$$

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

$$r's' \in (r+I)\cdot(s+I) \subset rs + rI + Is + I\cdot I \subset rs + I$$

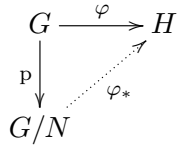
unter Verwendung der Ideal-Eigenschaft, dass wie benötigt $r's' \in [rs]_{R:I} = rs+I$ gilt.

Alles Weitere (Assoziativität, Kommutativität, neutrale und inverse Elemente) erhält man problemlos aus den entsprechenden Eigenschaften von G beziehungsweise R. □

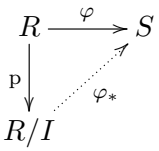
Zum Abschluss des Kapitels erwähnen wir die Faktorisierungssätze für Gruppen und für Ringe, bei denen es sich um weitgehende Analoga des Faktorisierungssatzes für Äquivalenzrelationen handelt:

Satz (Faktorisierungssätze für Gruppen und Ringe).

(I) *Seien $(G,*)$ und $(H,\circledast)$ Gruppen, N ein Normalteiler von $(G,*)$ und $\varphi\colon G \to H$ ein Gruppenhomomorphismus mit $N \subset \mathrm{Kern}(\varphi)$. Dann gibt es genau einen Gruppenhomomorphismus $\varphi_*\colon G/N \to H$, der $\varphi_* \circ \mathrm{p} = \varphi$ (mit der Quotientenabbildung $\mathrm{p}\colon G \to G/N$) erfüllt, also nebenstehendes Diagramm kommutativ macht.*



(II) *Seien $(R,+,\cdot)$ und $(S,\oplus,\odot)$ Ringe, I ein Ideal von $(R,+,\cdot)$ und $\varphi\colon R \to S$ ein Ringhomomorphismus mit $I \subset \mathrm{Kern}(\varphi)$. Dann gibt es genau einen Ringhomomorphismus $\varphi_*\colon R/I \to S$, der $\varphi_* \circ \mathrm{p} = \varphi$ (mit der Quotientenabbildung $\mathrm{p}\colon R \to R/I$) erfüllt, also nebenstehendes Diagramm kommutativ macht.*



Bemerkung (zu den **Faktorisierungssätzen**)**.** Gemäß Bemerkung (4) zu Normalteilern und Idealen ist der Satz stets mit $N = \mathrm{Kern}(\varphi)$ beziehungsweise $I = \mathrm{Kern}(\varphi)$ anwendbar, und genau in diesem Fall ist φ_* injektiv. Außerdem gilt stets $\mathrm{Bild}(\varphi_*) = \mathrm{Bild}(\varphi)$, und insbesondere ist φ_* genau dann surjektiv, wenn φ surjektiv ist.

Zum Beweis der Faktorisierungssätze. Die Existenz und Eindeutigkeit einer Abbildung φ_* mit $\varphi_* \circ \mathrm{p} = \varphi$ ergibt sich aus dem Satz des Abschnitts 2.3.2 über die Faktorisierung nach einer Äquivalenzrelation, wenn man bedenkt, dass im Gruppenfall (I)

$$x \overset{N}{\sim} y \iff y^{-1} * x \in N \implies y^{-1} * x \in \mathrm{Kern}(\varphi) \iff \varphi(y^{-1} * x) = e_G \iff \varphi(x) = \varphi(y)$$

für $x, y \in N$ und im Ringfall (II)

$$x \overset{I}{\sim} y \iff x - y \in I \implies x - y \in \mathrm{Kern}(\varphi) \iff \varphi(x - y) = 0 \iff \varphi(x) = \varphi(y)$$

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 φ_* nachzurechnen. Im Gruppenfall (I) gelingt dies mit der Rechnung

$$\varphi_*([g_1]_{G/N} * [g_2]_{G/N}) = \varphi_*([g_1 * g_2]_{G/N}) = \varphi(g_1 * g_2) = \varphi(g_1) \circledast \varphi(g_2) = \varphi_*([g_1]_{G/N}) \circledast \varphi_*([g_2]_{G/N})$$

für $[g_1]_{G/N}, [g_2]_{G/N} \in G/N$. Im Ringfall (II) kann man analog vorgehen. □

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 π, 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*

$$x < y \implies r+x < r+y\,, \qquad\qquad 0 < r\,,\, x < y \implies r \cdot x < r \cdot y\,.$$

- **(*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:

$$\mathbb{R} \text{ ist ein } \textbf{vollständiger, Archimedisch angeordneter Körper}.$$

(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 in Abschnitt 4.2 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

$$x \leq y :\Longleftrightarrow (x < y \vee x = y) \qquad \text{für } x, y \in \mathbb{R}$$

einführen sowie $>$ und $\geq$ als die Umkehrrelationen zu $<$ und $\leq$ erklären.

(3) Aus den Anordnungsaxiomen folgen die Regeln (für $n \in \mathbb{N}$, $r, s, x, y, x_i, y_i \in \mathbb{R}$)

$$n > 0\,,$$
$$x \text{ positiv} \iff -x \text{ negativ}\,,$$
$$x^2 \geq 0 \text{ (mit „=“ nur falls } x = 0)\,,$$
$$\sum_{i=1}^{n} x_i^2 \geq 0 \text{ (mit „=“ nur falls alle } x_i = 0)\,,$$
$$x_i \leq y_i \text{ für } i \in \{1, 2, \ldots, n\} \implies \sum_{i=1}^{n} x_i \leq \sum_{i=1}^{n} y_i \text{ (mit „=“ nur falls alle } x_i = y_i)\,,$$
$$0 < x_i \leq y_i \text{ für } i \in \{1, 2, \ldots, n\} \implies \prod_{i=1}^{n} x_i \leq \prod_{i=1}^{n} y_i \text{ (mit „=“ nur falls alle } x_i = y_i)\,,$$
$$x < y\,,\ r < 0 \iff r{\cdot}x > r{\cdot}y\,,$$
$$0 < r < s \implies \tfrac{1}{r} > \tfrac{1}{s} > 0\,.$$

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 ∞ (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 Kapitel 5 sehen werden, kann man mit ∞ und $-\infty$ bis 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*

$$\begin{aligned}
(a,b) :=]a,b[&:= \{x \in \overline{\mathbb{R}} \mid a < x < b\} && (\textbf{\textit{offen}}),\\
(a,b] :=]a,b] &:= \{x \in \overline{\mathbb{R}} \mid a < x \leq b\} && (\textit{links } \textbf{\textit{halboffen}}),\\
[a,b) := [a,b[&:= \{x \in \overline{\mathbb{R}} \mid a \leq x < b\} && (\textit{rechts } \textbf{\textit{halboffen}}),\\
[a,b] &:= \{x \in \overline{\mathbb{R}} \mid a \leq x \leq b\} && (\textbf{\textit{abgeschlossen}})
\end{aligned}$$

*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*

$$\operatorname{sgn}\colon \mathbb{R} \to \mathbb{R}\,, \qquad \operatorname{sgn}(x) := \begin{cases} 1 & \textit{falls } x > 0 \\ 0 & \textit{falls } x = 0 \\ -1 & \textit{falls } x < 0 \end{cases} \qquad \textit{für } x \in \mathbb{R}$$

mit $\operatorname{Bild}(\operatorname{sgn}) = \{-1, 0, 1\}$.

(II) *Die* (*reelle*) ***Betragsfunktion*** *ist*

$$|\cdot|\colon \mathbb{R} \to \mathbb{R}\,, \qquad |x| := \begin{cases} x & \textit{falls } x \geq 0 \\ -x & \textit{falls } x \leq 0 \end{cases} \qquad \textit{für } x \in \mathbb{R}$$

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

$$x = \operatorname{sgn}(x)|x|\,, \qquad \operatorname{sgn}(xy) = \operatorname{sgn}(x)\operatorname{sgn}(y) \overset{y\neq 0}{=} \operatorname{sgn}\Big(\frac{x}{y}\Big)\,, \qquad x^2 = |x|^2\,,$$
$$|x| = |y| \iff (x = y \vee x = -y)\,, \qquad |x| \leq y \iff x \in [-y, y]\,.$$

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

$$\frac{1}{|x|} \geq \frac{1}{1-x} \qquad \text{für } x \in \mathbb{R} \setminus \{0, 1\}\,,$$

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 $T_{x,q} := \{z \in \mathbb{Z} \,|\, z > q^{-1}x\}$ 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 $\widetilde{s}q{+}\widetilde{r} = sq{+}r$ mit $s, \widetilde{s} \in \mathbb{Z}$, $r, \widetilde{r} \in [0, q)$. Im Fall $\widetilde{s} > s$ ist $\widetilde{s} \geq s{+}1$, und es ergibt sich mit $q \leq (\widetilde{s}{-}s)q = r{-}\widetilde{r} \leq r < q$ ein Widerspruch. Im Fall $\widetilde{s} < s$ folgt dieser analog. Also muss $\widetilde{s} = s$ und dann auch $\widetilde{r} = r$ 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 sich 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 $r \in \left[0, \frac{1}{n}\right)$ schreiben. Damit liegen die k rationalen Zahlen $\frac{s+1}{n}$, $\frac{s+2}{n}$, …, $\frac{s+k}{n}$ 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 Abschnitt 5.2), 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 $s \in \mathbb{Z}$, $r \in \left[0, \frac{1}{n}t\right)$ und erhalten die k irrationalen Zahlen $\frac{s+1}{n}t$, $\frac{s+2}{n}t$, …, $\frac{s+k}{n}t$ in $(a, b) \setminus \mathbb{Q}$.)

Definition (**Intervallschachtelungen**). *Eine **Intervallschachtelung** in $\mathbb{R}$ ist eine unendliche Folge nicht-leerer kompakter Intervalle*

$$[a_1, b_1] \supset [a_2, b_2] \supset [a_3, b_3] \supset [a_4, b_4] \supset \ldots$$

*mit Randpunkten $-\infty < a_1 \leq a_2 \leq a_3 \leq a_4 \leq \ldots \leq b_4 \leq b_3 \leq b_2 \leq b_1 < \infty$, 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 $c, \widetilde{c} \in \mathbb{R}$ zwei Kerne, so gilt mit $c, \widetilde{c} \in [a_n, b_n]$ auch $|\widetilde{c}{-}c| \leq b_n{-}a_n$ für alle $n \in \mathbb{N}$. Wäre $|\widetilde{c}{-}c| > 0$, so gäbe es ein $n \in \mathbb{N}$ mit $b_n{-}a_n < |\widetilde{c}{-}c|$, und wir erhielten einen Widerspruch. Also muss $|\widetilde{c}{-}c| = 0$ gelten, was $\widetilde{c} = c$ bedeutet. □

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 $\sqrt{2} = 1,4142135623\ldots$ in $\mathbb{R}$ der Kern der Intervallschachtelung $\left[\frac{14}{10}, \frac{15}{10}\right] \supset \left[\frac{141}{100}, \frac{142}{100}\right] \supset \left[\frac{1414}{1000}, \frac{1415}{1000}\right] \supset \left[\frac{14142}{10000}, \frac{14143}{10000}\right] \supset \ldots$ (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 Abschnitt 5.2 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*[1] *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**:

$$M = \sup A \iff \big(\underbrace{\forall x \in A\colon x \le M}_{M \text{ obere Schranke für } A} \text{ und } \forall L \in (-\infty, M)\colon \underbrace{\exists y \in A\colon y > L}_{L \textit{ keine} \text{ obere Schranke für } A}\big)$$

Diese Charakterisierung wird in Anwendungen des Öfteren benutzt.

[1] 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[2] $\frac{z}{2^n}$ 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. □

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. □

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 $\mathbb{Q} = \mathbb{Q}_{<x} \dot\cup \mathbb{Q}_{\geq x}$,

[2] 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 $A = \left\{\frac{2}{5}\right\}$ bekämen wir nämlich $[a_2, b_2] = \left[0, \frac{1}{2}\right] \not\supset [a_3, b_3] = \left[\frac{1}{3}, \frac{2}{3}\right]$.

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

$$\mathbb{R} := \left\{ A \in \mathcal{P}(\mathbb{Q}) \;\middle|\; \begin{array}{c} \emptyset \neq A \neq \mathbb{Q} \\ \forall a \in A\colon \forall b \in \mathbb{Q} \setminus A\colon a < b \\ \text{Es gibt keine größte Zahl in } A\,. \end{array} \right\}$$

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 $A \cdot B := (A_{>0} \cdot B_{>0}) \dot\cup \mathbb{Q}_{\leq 0}$ 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 Eindeutigkeitseigenschaft der reellen Zahlen nachweisen lässt:

Satz (((strukturelle) Eindeutigkeit von $\mathbb{R}$**).** *Erfüllen zwei Mengen* $\mathbb{R}$ *(mit* $+$*,* $\cdot$*,* $<$*) und* $\widetilde{\mathbb{R}}$ *(mit* $\widetilde{+}$*,* $\widetilde{\cdot}$*,* $\widetilde{<}$*) alle Axiome der reellen Zahlen, so gibt es einen Körperisomorphismus* $\psi\colon \mathbb{R} \to \widetilde{\mathbb{R}}$*, der zudem im Sinn von* $x < y \implies \psi(x) \mathrel{\widetilde{<}} \psi(y)$ *für alle* $x, y \in \mathbb{R}$ *Ordnung-erhaltend ist.*

Beweisskizze. Man betrachtet zunächst die Primkörper $\mathbb{Q}$ und $\widetilde{\mathbb{Q}}$ von $\mathbb{R}$ und $\widetilde{\mathbb{R}}$, die beide den rationalen Zahlen entsprechen und somit durch einen Körperisomorphismus $\varphi\colon \mathbb{Q} \to \widetilde{\mathbb{Q}}$ identifiziert werden können. Mit den Anordnungsaxiomen kann gezeigt werden, dass φ (wie auch φ^{-1}) Ordnung-erhaltend ist. Insbesondere ist daher für jedes $x \in \mathbb{R}$ das Bild $\varphi(\mathbb{Q}_{<x}) \subset \widetilde{\mathbb{R}}$ 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 $\widetilde{\mathbb{R}}$ (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 $\widetilde{\mathbb{R}}$, und es lässt sich eine Abbildung $\psi\colon \mathbb{R} \to \widetilde{\mathbb{R}}$ durch $\psi(x) := \widetilde{\sup}\,\varphi(\mathbb{Q}_{<x})$ für $x \in \mathbb{R}$ definieren.

Die benötigten Eigenschaften von ψ verifiziert man in mehreren Schritten.

Um zunächst einzusehen, dass ψ 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 $\psi(x+y) = \widetilde{\sup}\,\varphi(\mathbb{Q}_{<x}+\mathbb{Q}_{<y}) = \widetilde{\sup}\,[\varphi(\mathbb{Q}_{<x}) \mathbin{\widetilde{+}} \varphi(\mathbb{Q}_{<y})] = \widetilde{\sup}\,\varphi(\mathbb{Q}_{<x}) \mathbin{\widetilde{+}} \widetilde{\sup}\,\varphi(\mathbb{Q}_{<y}) = \psi(x) \mathbin{\widetilde{+}} \psi(y)$. Für die Multiplikation lässt sich ähnlich (aber mit Fallunterscheidung nach den Vorzeichen von x und y) argumentieren.

Dass ψ Ordnung-erhaltend und damit insbesondere injektiv ist, erhält man wie folgt: Für $x, y \in \mathbb{R}$ mit $x < y$ gibt es gemäß der dichten Anordnung von $\mathbb{Q}$ in $\mathbb{R}$ rationale Zwischenstellen $p, q \in \mathbb{Q}$ mit $x \leq p < q < y$. Wegen der Definition des Supremums und der Erhaltung der Ordnung unter φ ergibt sich dann $\widetilde{\sup}\,\varphi(\mathbb{Q}_{<x}) \mathrel{\widetilde{\leq}} \varphi(p) \mathrel{\widetilde{<}} \varphi(q) \mathrel{\widetilde{\leq}} \widetilde{\sup}\,\varphi(\mathbb{Q}_{<y})$, also wie benötigt $\psi(y) \mathrel{\widetilde{<}} \psi(y)$.

Um den Beweis der Surjektivität von ψ 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, weil φ Ordnung-erhaltend ist. Gäbe es noch eine kleinere obere Schranke für $\varphi(\mathbb{Q}_{<q})$, so könnte diese wegen der dichten Anordnung als $\eta \in \widetilde{\mathbb{Q}}$ mit $\eta \mathrel{\widetilde{<}} \varphi(q)$ 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 $\eta \in \widetilde{\mathbb{Q}}$ mit $\eta \mathrel{\widetilde{<}} \psi(\sup A)$ gewählt werden. Nun wäre $\varphi^{-1}(\eta) < \sup A$ (denn mit $\varphi^{-1}(\eta) \geq \sup A$ müsste auch $\eta = \varphi(\varphi^{-1}(\eta)) = \psi(\varphi^{-1}(\eta)) \geq \psi(\sup A)$ gelten) und $\varphi^{-1}(\eta)$ wäre eine 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 ψ beweisen. Sei dazu $\alpha \in \widetilde{\mathbb{R}}$ beliebig. Die schon bei der Definition von ψ angestellten Überlegungen liefern dann die Existenz von $x := \sup \varphi^{-1}(\widetilde{\mathbb{Q}}_{<\alpha}) \in \mathbb{R}$, und mit den zuletzt nachgewiesenen Eigenschaften folgt $\psi(x) = \psi(\sup \varphi^{-1}(\widetilde{\mathbb{Q}}_{<\alpha})) = \sup \psi(\varphi^{-1}(\widetilde{\mathbb{Q}}_{<\alpha})) = \sup \varphi(\varphi^{-1}(\widetilde{\mathbb{Q}}_{<\alpha})) = \sup \widetilde{\mathbb{Q}}_{<\alpha} = \alpha$.

Insgesamt ist $\psi\colon \mathbb{R} \to \widetilde{\mathbb{R}}$ Ordnung-erhaltender Körperisomorphismus. □

4.2 Komplexe Zahlen

In diesem Abschnitt führen wir den (in der Mathematik 1 schon verschiedentlich angekündigten) **Zahlbereich $\mathbb{C}$ der komplexen Zahlen** ein.

Motivation (ausgehend von der Lösbarkeit polynomialer Gleichungen)**.** Im Bereich der reellen Zahlen besitzen relativ einfache (polynomiale) Gleichungen wie $x^2 = -1$ keine Lösung $x \in \mathbb{R}$, denn gemäß Abschnitt 4.1 ist $x^2 \geq 0$ und damit $x \neq -1$ für alle $x \in \mathbb{R}$. Um dies zu beheben, werden wir die Existenz einer in $\mathbb{R}$ nicht vorhandenen Zahl $\mathbf{i}$ mit

$$\mathbf{i}^2 = -1$$

im Wesentlichen einfach postulieren. Um mit $\mathbf{i}$ und den reellen Zahlen sinnvoll rechnen zu können, muss man auch Zahlen der Form $x+\mathbf{i}y$ mit $x, y \in \mathbb{R}$ zulassen, was auf folgendes Konzept führt:

Definitionen (**komplexe Zahlen**)**.**

(I) *Der **Zahlbereich der komplexen Zahlen** ist die Menge*

$$\mathbb{C} := \mathbb{R}^2$$

*der geordneten Paare reeller Zahlen. Eine komplexe Zahl $z = (x, y) \in \mathbb{R}^2$ wird in der **Normalform***

$$z = x + \mathbf{i}y$$

*notiert, wobei x als ihr **Realteil** $\mathcal{Re}(z)$ und y als ihr **Imaginärteil** $\mathcal{Im}(z)$ bezeichnet wird. Man identifiziert $x \in \mathbb{R}$ mit der komplexen Zahl $x+\mathbf{i}0$ mit Imaginärteil 0 und fasst so*

$$\mathbb{R} \subset \mathbb{C}$$

*auf. Schließlich bezeichnet man $\mathbf{i} := 0+\mathbf{i}1$ als die **imaginäre Einheit** und komplexe Zahlen $\mathbf{i}y := 0+\mathbf{i}y$ mit Realteil 0 als **rein imaginär**.*

(II) *Für komplexe Zahlen $z = x+\mathbf{i}y \in \mathbb{C}$ und $w = u+\mathbf{i}v \in \mathbb{C}$ (mit $x, y, u, v \in \mathbb{R}$) erklärt man die **Addition** durch*

$$z + w := (x+u) + \mathbf{i}(y+v) \in \mathbb{C}$$

*(also einfach komponentenweise) und die **Multiplikation** durch*

$$zw := (xu-yv) + \mathbf{i}(xv+yu) \in \mathbb{C}\,.$$

Satz (**über den Körper $\mathbb{C}$**)**.**

(I) *Mit den vorausgehenden Definition und Konventionen ist $(\mathbb{C}, +, \cdot)$ ein Körper, dessen Addition und Multiplikation auf dem Teilkörper $\mathbb{R}$ mit der reellen Addition und Multiplikation übereinstimmen.*

(II) *Die Gleichung $z^2 = -1$ hat in $\mathbb{C}$ genau die Lösungen $z = \mathbf{i}$ und $z = -\mathbf{i}$.*

Mit anderen Worten besagt Teil (I) des Satzes, dass das Rechnen in $\mathbb{C}$ das Rechnen in $\mathbb{R}$ verallgemeinert und alle in Körpern gültigen Rechenregeln auch allgemein bei komplexen Zahlen greifen (mit der „normalen“, in $\mathbb{R}$ enthaltenen Null und Eins). Ein Preis, den man für die Einführung der imaginären Einheit $\mathbf{i}$ mit $\mathbf{i}^2 \in \mathbb{R}_{<0}$ bezahlt, ist allerdings, dass **sich komplexe Zahlen nicht so gut wie reelle Zahlen anordnen lassen**, dass es also auf $\mathbb{C}$ keine gut mit den Rechenoperationen verträgliche (strikte) Ordnungsrelation (also keine Standard-Versionen von $<$, $>$, $\leq$, $\geq$) gibt.

Beweis des Satzes. Wir behandeln zunächst Teil (I). Ausgehend von den Körperaxiomen für $\mathbb{R}$ prüft man beispielsweise die Kommutativität der komplexen Addition durch die Rechnung

$$z+w = (x{+}u)+\mathbf{i}(y{+}v) = (u{+}x)+\mathbf{i}(v{+}y) = w+z$$

und die Assoziativität der komplexen Multiplikation durch die Rechnung

$$\begin{aligned}(zw)t &= ((xu{-}yv){+}\mathbf{i}(xv{+}yu))(r{+}\mathbf{i}s) = (xur{-}yvr{-}xvs{-}yus)+\mathbf{i}(xus{-}yvs{+}xvr{+}yur)\\ &= (x{+}\mathbf{i}y)((ur{-}vs){+}\mathbf{i}(us{+}vr)) = z(wt)\end{aligned}$$

für $z = x{+}\mathbf{i}y \in \mathbb{C}$, $w = u{+}\mathbf{i}v \in \mathbb{C}$, $t = r{+}\mathbf{i}s \in \mathbb{C}$. Weitere für Teil (I) benötigte Rechnungen verlaufen ähnlich. Erwähnenswert ist noch der Existenznachweis für das multiplikativ Inverse zu $z = x{+}\mathbf{i}y \in \mathbb{C}\setminus\{0\}$. Hierzu benutzt man, dass gemäß Abschnitt 4.1 für die *reellen* Zahlen x und y, die *nicht beide* Null sind, $x^2{+}y^2 > 0$ gilt und prüft, dass das Inverse durch die Reziprokenformel $\frac{x}{x^2+y^2}+\mathbf{i}\frac{-y}{x^2+y^2} \in \mathbb{C}$ (die wegen $x^2{+}y^2 \neq 0$ hingeschrieben werden darf) gegeben ist. Eine konstruktive Herleitung dieser Formel folgt unten (und in den Übungen). Für diesen Beweis reicht es aber, die Inversen-Eigenschaft mit

$$(x{+}\mathbf{i}y)\Big(\frac{x}{x^2{+}y^2}+\mathbf{i}\frac{-y}{x^2{+}y^2}\Big) = \frac{x^2}{x^2{+}y^2}+\frac{y^2}{x^2{+}y^2}+\mathbf{i}\Big(\frac{-xy}{x^2{+}y^2}+\frac{yx}{x^2{+}y^2}\Big) = 1\,.$$

nachzurechnen.

Zum Beweis von Teil (II) bemerken wir $z^2{+}1 = z^2{-}\mathbf{i}^2 = (z{-}\mathbf{i})(z{+}\mathbf{i})$ für $z \in \mathbb{C}$ und erhalten damit für $z \in \mathbb{C}$ die Äquivalenzen

$$z^2 = -1 \iff z^2{+}1 = 0 \iff (z{-}\mathbf{i} = 0 \vee z{+}\mathbf{i} = 0) \iff (z = \mathbf{i} \vee z = -\mathbf{i})\,.$$

Aus diesen liest man die Behauptung ab. □

Bemerkungen (zum **Rechnen mit komplexen Zahlen**).

(1) Die Formeln für die komplexe Addition und Multiplikation muss man sich nicht unbedingt merken, denn sie ergeben sich automatisch aus den Rechengesetzen in Körpern und $\mathbf{i}^2 = -1$.

(2) Anders als natürliche, ganze, rationale und reelle Zahlen lassen sich **komplexe Zahlen *nicht* mehr auf der Zahlengerade** veranschaulichen, sondern entsprechen definitionsgemäß Koordinatenpunkten in der Ebene $\mathbb{R}^2$. Man spricht in diesem Zusammenhang von der **Gaußschen Zahlenebene** und trägt üblicherweise die reellen Zahlen aus $\mathbb{R}$ auf der horizontalen Achse, die rein imaginären Zahlen aus $\mathbf{i}\mathbb{R}$ auf der vertikalen Achse auf.

(3) Das **Rechnen mit komplexen Zahlen** lässt sich in der Gaußschen Zahlenebene wie folgt **veranschaulichen**: Das Negative (d.h. das additiv Inverse) $-z \in \mathbb{C}$ einer komplexen Zahl

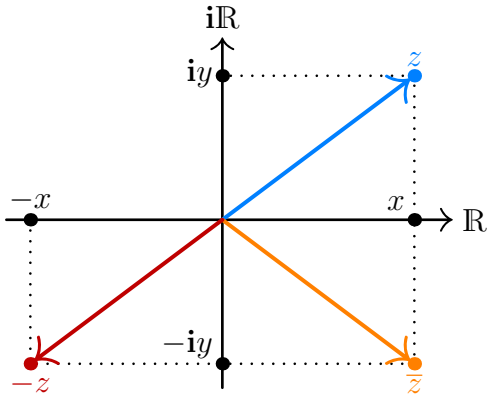


Abb. 32: Das Negative $-z = -x{-}\mathbf{i}y$ und die komplex konjugierte Zahl $\overline{z} = x{-}\mathbf{i}y$ zu einer komplexen Zahl $z = x{+}\mathbf{i}y$

$z \in \mathbb{C}$ ergibt sich durch Punktspiegelung am Ursprung und die (in der übernächsten Definition eingeführte) komplex konjugierte Zahl $\overline{z} \in \mathbb{C}$ zu z durch Spiegelung an der reellen Achse; vergleiche Abbildung 32. In Abbildung 33 wird zudem die komplexe Addition und Multiplikation von $z = x+\mathbf{i}y \in \mathbb{C}$ und $w = u+\mathbf{i}v \in \mathbb{C}$ graphisch dargestellt: Die Summe $z+w = (x+u)+\mathbf{i}(y+v) \in \mathbb{C}$ erhält man durch Vektoraddition der Ortsvektoren, d.h. durch Aneinanderlegen der vom Ursprung 0 zu z und w zeigenden Vektorpfeile. Das Produkt $zw = (xu-yv)+\mathbf{i}(xv+yu) \in \mathbb{C}$ lässt sich in der sogenannten Polardarstellung, bei der eine komplexe Zahl durch ihren Abstand vom Ursprung und durch den Polarwinkel zwischen ihrem Ortsvektor und dem positiven Teil der reellen Achse beschrieben wird, veranschaulichen und kommt dann durch Multiplikation der Abstände und Addition der Polarwinkel zustande. Die an dieser Stelle nur ganz kurz angerissene Thematik der Polardarstellung werden wir dabei in den Abschnitt 5.3 noch genauer beleuchten und in Abschnitt 5.6 weiter unterfüttern.

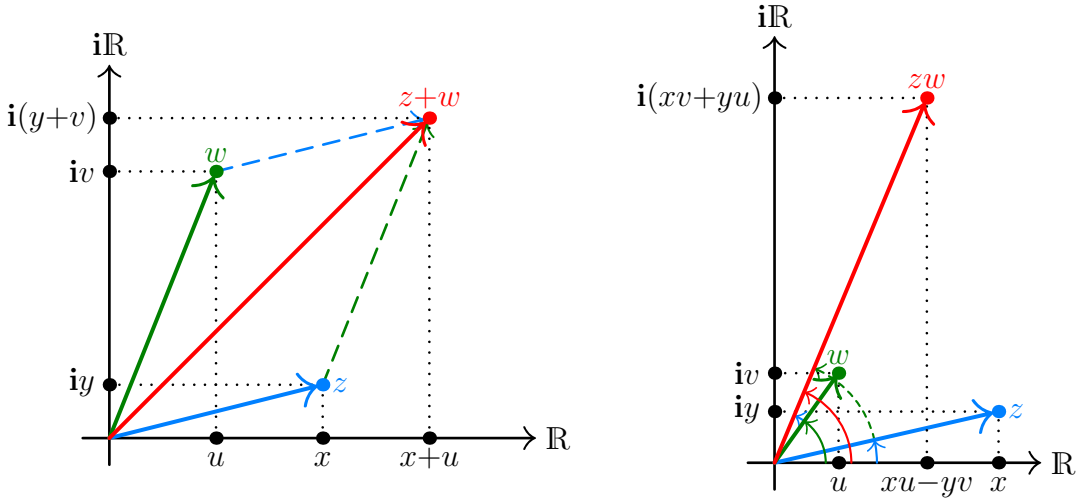


Abb. 33: Summe $z+w = (x+u)+\mathbf{i}(y+v)$ (links) und Produkt $zw = (xu-yv)+\mathbf{i}(xv+yu)$ (rechts) komplexer Zahlen $z = x+\mathbf{i}y$ und $w = u+\mathbf{i}v$

Als grundlegende Bildungen mit komplexen Zahlen führen wir nun den Betrag komplexer Zahlen und die komplexe Konjugation ein:

Definition (Betrag). *Die (komplexe)* ***Betragsfunktion*** *ist definiert als*

$$|\cdot|\colon \mathbb{C} \to \mathbb{R}\,, \qquad |z| := \sqrt{\mathcal{R}e(z)^2 + \mathit{Im}(z)^2} \quad \textit{für } z \in \mathbb{C}$$

und hat das Bild $\mathrm{Bild}(|\cdot|) = \mathbb{R}_{\geq 0}$.

Bemerkungen (zum Betrag).

(1) Die in der Definition auftretende Quadratwurzel wird erst in Abschnitt 5.2 präzise eingeführt, hier im Vorgriff[3] darauf aber schon benutzt. Da $\mathcal{R}e(z)^2 + \mathit{Im}(z)^2 \in \mathbb{R}_{\geq 0}$ gilt, kann diese Wurzel stets in $\mathbb{R}_{\geq 0}$ gezogen werden.

(2) Für $x \in \mathbb{R}$ ergibt $\sqrt{\mathcal{R}e(x)^2+\mathit{Im}(x)^2} = \sqrt{x^2} = \sqrt{|x|^2} = |x|$ den in Abschnitt 4.1 eingeführten reellen Betrag. Daher sind die Definitionen und Notationen mit Abschnitt 4.1 konsistent.

[3] Um den Vorgriff zu vermeiden, könnte man in diesem Abschnitt nur das Quadrat $|z|^2 := \mathcal{R}e(z)^2+\mathit{Im}(z)^2$ des Betrags einführen, was aber eher umständlich wäre.

(3) Ähnlich wie bei reellen Zahlen kann man auch für $z, w \in \mathbb{C}$ den **Betrag** $|z|$ als den **Abstand** von z **von 0 in der Gaußschen Zahlenebene** und $|z-w|$ als den Abstand von z und w in der Gaußschen Zahlenebene interpretieren. Dies ergibt sich aus dem elementargeometrischen Satz des Pythagoras (angewandt auf das Dreieck mit Ecken 0, $\mathcal{Re}(z)$, z oder alternativ das Dreieck mit Ecken 0, $\mathbf{i}\,\mathit{Im}(z)$, z).

(4) Für beliebige komplexe Zahlen $z, w, \zeta, z_j \in \mathbb{C}$ gelten die Positivität des Betrags

$$|z| \geq 0 \quad (\text{mit „=“ nur für } z = 0)\,,$$

die **Multiplikativität des Betrags**

$$|zw| = |z|\,|w|\,,$$

(insbesondere $|-z| = |z|$ und für $z \neq 0$ auch $|1/z| = 1/|z|$), die **Dreiecksungleichungen** (mit beliebiger endlicher Indexmenge J)

$$|z\pm w| \leq |z|+|w|\,, \qquad |z-w| \leq |z-\zeta| + |\zeta-w|\,, \qquad \left|\sum_{j\in J} z_j\right| \leq \sum_{j\in J} |z_j|$$

und die **umgekehrte Dreiecksungleichung**

$$\big||z| - |w|\big| \leq |z \pm w|\,.$$

Die Multiplikativität erhält man dabei durch direktes Nachrechnen oder als Folgerung aus der Multiplikativität der komplexen Konjugation; vergleiche mit den folgenden Bemerkungen (1) und (3). Beweise der Ungleichungen werden in den Übungen behandelt.

Definition (**komplexe Konjugation**). *Die zu* $z = \mathcal{Re}(z)+\mathbf{i}\,\mathit{Im}(z) \in \mathbb{C}$ ***(komplex) konjugierte Zahl*** *ist definiert als*

$$\overline{z} := \mathcal{Re}(z) - \mathbf{i}\,\mathit{Im}(z) \in \mathbb{C}\,.$$

Bemerkungen (zur **komplexen Konjugation**). Seien $z, w \in \mathbb{C}$.

(1) Die komplexe Konjugation ist ein involutorischer, Betrag-erhaltender Körperautomorphismus, d.h. es gelten

$$\overline{\overline{z}} = z\,, \qquad |\overline{z}| = |z|\,, \qquad \overline{z\pm w} = \overline{z}\pm\overline{w}\,, \qquad \overline{zw} = \overline{z}\,\overline{w}\,, \qquad \overline{1/z} = 1/\overline{z}\,.$$

Dies rechnet man problemlos mit den Definitionen nach.

(2) Mit der komplexen Konjugation ergibt sich eine Charakterisierung reeller und rein imaginärer Zahlen sowie von Real- und Imaginärteil durch

$$z \in \mathbb{R} \iff \overline{z} = z\,, \qquad z \in \mathbf{i}\mathbb{R} \iff \overline{z} = -z\,, \qquad \mathcal{Re}(z) = \frac{z+\overline{z}}{2}\,, \qquad \mathit{Im}(z) = \frac{z-\overline{z}}{2\mathbf{i}}\,.$$

Auch dies rechnet man mit den Definitionen nach.

(3) Die komplexe Konjugation hängt mit der komplexen Betragsfunktion durch

$$z\overline{z} = (\mathcal{R}e(z)+\mathbf{i}\,Im(z))(\mathcal{R}e(z)-\mathbf{i}\,Im(z)) = \mathcal{R}e(z)^2-\mathbf{i}^2\,Im(z)^2 = \mathcal{R}e(z)^2+Im(z)^2 = |z|^2$$

zusammen. Hieraus folgt die nützliche **Reziprokenformel** (wobei wir $z = x+\mathbf{i}y$ mit $x, y \in \mathbb{R}$ schreiben)

$$\frac{1}{z} = \frac{\overline{z}}{z\overline{z}} = \frac{\overline{z}}{|z|^2} = \frac{x}{x^2+y^2} - \mathbf{i}\frac{y}{x^2+y^2}\,,$$

die den Ansatz für das multiplikativ Inverse im vorigen Beweis erklärt und die **Berechnung der Normalform von Reziproken und Quotienten** erlaubt. Weiterhin entnimmt man aus der Reziprokenformel, dass das Reziproke $\frac{1}{z}$ einer komplexen Zahl z sich, wie in Abbildung 34 dargestellt, durch Spiegelung an der reellen Achse und anschließende „Inversion“ gemäß $|\frac{1}{z}| = \frac{1}{|\overline{z}|}$ an der Einheitskreislinie $\{q \in \mathbb{C}\,|\,|q| = 1\}$ ergibt.

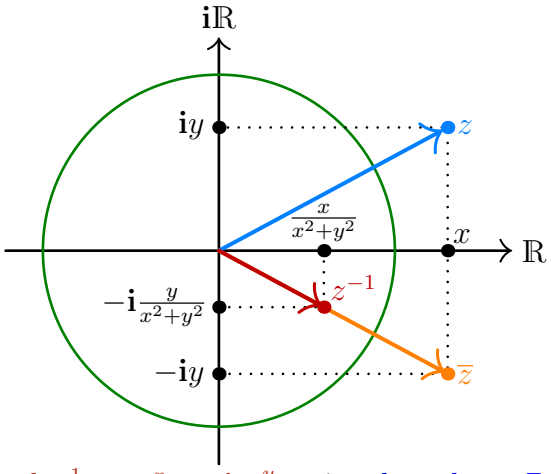


Abb. 34: Das Reziproke $\frac{1}{z} = \frac{x}{x^2+y^2} - \mathbf{i}\frac{y}{x^2+y^2}$ einer komplexen Zahl $z = x+\mathbf{i}y$ mit der konjugierten Zahl $\overline{z} = x-\mathbf{i}y$ und der Einheitskreislinie $\{q \in \mathbb{C}\,|\,|q| = 1\}$

Zum Abschluss dieses Abschnitts sei hervorgehoben, dass der **entscheidende Gewinn beim Übergang von $\mathbb{R}$ zu $\mathbb{C}$** in der **allgemeinen Lösbarkeit polynomialer Gleichungen über $\mathbb{C}$** besteht. Genauer besagt der sogenannte **Fundamentalsatz der Algebra**, dass *jedes* Polynom vom Grad ≥ 1 in $\mathbb{C}$ mindestens eine Nullstelle besitzt, oder mit anderen Worten, dass *jede* Gleichung

$$c_n z^n + c_{n-1} z^{n-1} + \ldots + c_2 z^2 + c_1 z + c_0 = 0$$

mit $n \in \mathbb{N}$, $c_0, c_1, c_2, \ldots, c_n \in \mathbb{C}$, $c_n \neq 0$ mindestens eine Lösung $z \in \mathbb{C}$ hat. Eng damit verbunden ist, dass für *jedes* $z \in \mathbb{C} \setminus \{0\}$ in $\mathbb{C}$ genau n verschiedene n-te Wurzeln (also Zahlen $w \in \mathbb{C}$ mit $w^n = z$) existieren. Beweisen können wir diese Sachverhalte allerdings noch nicht und werden darauf erst bei der Behandlung von Stetigkeit an späterer Stelle zurückkommen.

4.3 Endliche Summen und Produkte

Auch in den Zahlbereichen $\mathbb{R}$ und $\mathbb{C}$ können endliche Summen und Produkte mit Hilfe des Summenzeichens $\sum$ beziehungsweise des Produktzeichens $\prod$ notiert werden, und es kann mit diesen Zeichen weiterhin wie in Abschnitt 2.2 gerechnet werden. Tatsächlich hatten wir ja in

Abschnitt 3.2 schon bemerkt, dass Summen- und Produktzeichen sogar in jedem kommutativen Ring sinnvoll sind.

Beispiele (wichtiger endlicher Summen und Produkte). Seien $k, \ell \in \mathbb{Z}$ mit $k \leq \ell$, sei $n \in \mathbb{N}_0$, und $\mathbb{K}$ sei ein Körper, beispielsweise $\mathbb{R}$ oder $\mathbb{C}$.

(1) **Teleskopsummen** sind Summen des Typs

$$\sum_{i=k}^{\ell}(a_{i+1}-a_i) = a_{\ell+1}-a_k \qquad \text{für } a_k, a_{k+1}, \ldots, a_\ell, a_{\ell+1} \in \mathbb{K}\,,$$

und **Teleskopprodukte** sind Produkte des Typs

$$\prod_{i=k}^{\ell}\frac{a_{i+1}}{a_i} = \frac{a_{\ell+1}}{a_k} \qquad \text{für } a_k, a_{k+1}, \ldots, a_\ell, a_{\ell+1} \in \mathbb{K}\setminus\{0\}\,.$$

Die Gültigkeit der Summenformel (und den Grund für die Benennung) erkennt man durch Ausschreiben $\sum_{i=k}^{\ell}(a_{i+1}-a_i) = a_{k+1}-a_k+a_{k+2}-a_{k+1}+a_{k+3}-a_{k+2}+\ldots+a_\ell-a_{\ell-1}+a_{\ell+1}-a_\ell$ und Wegstreichen der sich aufhebenden Summanden. Ohne Pünktchen, aber mit einer Indexverschiebung lässt sich diese Rechnung in der Form $\sum_{i=k}^{\ell}(a_{i+1}-a_i) = \sum_{i=k+1}^{\ell+1} a_i - \sum_{i=k}^{\ell} a_i = \sum_{i=k+1}^{\ell} a_i + a_{\ell+1} - a_k - \sum_{i=k+1}^{\ell} a_i = a_{\ell+1} - a_k$ schreiben. Die Produktformel folgt analog.

(2) Gelegentlich können Summen oder Produkte erst nach Umformung mit Hilfe eines Teleskop-Tricks berechnet werden. Ein typisches einfaches Beispiel hierfür ist

$$\sum_{i=1}^{n}\frac{1}{i(i+1)} = \sum_{i=1}^{n}\left(\frac{i+1}{i(i+1)} - \frac{i}{i(i+1)}\right) = \sum_{i=1}^{n}\left(\frac{1}{i} - \frac{1}{i+1}\right) = 1 - \frac{1}{n+1} = \frac{n}{n+1}$$

(3) Die **arithmetische Summenformel** und die als Spezialfall enthaltene **Gaußsche Summenformel**

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

kamen schon in der Übungen zur Mathematik 1 vor. Wir können die Gaußsche Summenformel als Alternative zu früheren Beweisen per Teleskop-Summation durch

$$\sum_{i=1}^{n} i = \frac{1}{2}\left[\sum_{i=1}^{n}\left((i+1)^2-i^2\right) - \sum_{i=1}^{n} i\right] = \frac{1}{2}\left[(n+1)^2-1-n\right] = \frac{n(n+1)}{2}$$

neu herleiten. Mit analogem, in den Übungen genauer besprochenem Vorgehen gewinnt man die **Formeln für sie Summe der ersten n Quadrat- beziehungsweise Kubikzahlen**

$$\sum_{i=1}^{n} i^2 = \frac{(2n+1)(n+1)n}{6} \qquad \text{und} \qquad \sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}\,.$$

Eine Verallgemeinerung auf beliebige Ordnung ist möglich und wird in Kürze angerissen.

(4) Die **geometrische Summenformel** kam ebenfalls bereits in den Übungen zur Mathematik 1 vor und enthält als wichtigsten Fall die Formel

$$\sum_{i=0}^{n} q^i = \frac{q^{n+1}-1}{q-1} \qquad \text{für } q \in \mathbb{K} \setminus \{1\} \quad (\text{mit Konvention } q^0 := 1)\,.$$

Es folgt eine wichtige Definition mit einem endlichen Produkt (die prinzipiell über jedem Körper der Charakteristik 0 getroffen werden kann, aber meist für Zahlbereiche gebraucht wird):

Definition (**Binomialkoeffizienten**). *Sei* $\mathbb{K}$ *ein Körper der Charakteristik* 0*, beispielsweise* $\mathbb{R}$ *oder* $\mathbb{C}$*. Für* $z \in \mathbb{K}$ *und* $k \in \mathbb{N}_0$ *wird der Binomialkoeffizient* $\binom{z}{k}$ (*lies*: z *über* k) *als*

$$\binom{z}{k} := \prod_{i=0}^{k-1} \frac{z-i}{k-i} = \frac{z(z-1)(z-2)\cdot\ldots\cdot(z-k+2)\cdot(z-k+1)}{k(k-1)(k-2)\cdot\ldots\cdot 2\cdot 1} \in \mathbb{K}$$

definiert. Für $z \in \mathbb{K}$ *und* $k \in -\mathbb{N}$ *vereinbart man* $\binom{z}{k} := 0$.

Bemerkungen (zu **Binomialkoeffizienten**). Im Fall $z = n \in \mathbb{N}_0$ können Binomialkoeffizienten durch die Formel

$$\binom{n}{k} = \binom{n}{n-k} = \begin{cases} \frac{n!}{k!(n-k)!} & \text{für } k \in \{0,1,2,\ldots,n-1,n\} \\ 0 & \text{für } k \in \mathbb{Z} \setminus \{0,1,2,\ldots,n-1,n\} \end{cases}$$

auf Fakultäten zurückgeführt werden. Außerdem lassen sich diese natürlichen Binomialkoeffizienten $\binom{n}{k}$ im sogenannten **Pascalschen Dreieck** anordnen:

$n=0$:					1					
$n=1$:				1		1				
$n=2$:			1		2		1			
$n=3$:		1		3		3		1		
$n=4$:	1		4		6		4		1	
$n=5$:	1		5		10		10		5	1

Dabei stehen die Koeffizienten zu gleichem n in der gleichen Zeile, die zu gleichem k auf der gleichen von rechts oben nach links unten verlaufenden Diagonale, und alle freien Plätze links und rechts entsprechen Nullen. In diesem Dreieck erweist sich jeder Koeffizient als Summe der beiden schräg über ihm stehenden. Dies ist Ausdruck der tatsächlich für alle $z \in \mathbb{K}$ und $k \in \mathbb{Z}$ gültigen und leicht nachzurechnenden Summationsregel

$$\binom{z}{k} + \binom{z}{k+1} = \binom{z+1}{k+1}\,.$$

Insbesondere ergibt sich mit der Anordnung im Pascalschen Dreieck beziehungsweise der Summationsregel auch, dass für $n \in \mathbb{N}_0$ und $k \in \mathbb{Z}$ stets $\binom{n}{k} \in \mathbb{N}_0$ gilt.

Eine **allgemeine Version des Distributivgesetzes** für Produkte von $n \in \mathbb{N}$ Summen über Indexmengen I_1, I_2, …, I_n lautet

$$\prod_{k=1}^{n} \left(\sum_{i \in I_k} a_{k,i} \right) = \sum_{i_1 \in I_1, i_2 \in I_2, \ldots, i_n \in I_n} a_{1,i_1} a_{2,i_2} \ldots a_{n,i_n}$$

und gilt für Elemente eines Körpers (etwa reelle/komplexe Zahlen) $a_{k,i}$ mit $k \in \{1, 2, \ldots, n\}$, $i \in I_k$. Diese kompliziert erscheinende Regel lässt sich problemlos mit Induktion nachweisen und **besagt tatsächlich nur, dass man die n Klammern auf der linken Seite in der gewohnten Weise ausmultiplizieren darf**.

Handelt es sich links immer um dieselbe Summe mit zwei Summanden, so ergibt sich daraus durch Nachverfolgung, welcher Summand rechts wie oft auftritt:

Satz (**Binomialsatz, binomischer Lehrsatz, allgemeine binomische Formel**). *Sei* $\mathbb{K}$ *ein Körper, beispielsweise* $\mathbb{R}$ *oder* $\mathbb{C}$. *Für* $n \in \mathbb{N}_0$ *und* $a, b \in \mathbb{K}$ *gilt*[4] (*mit der Konvention* $0^0 := 1$)

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} = \sum_{\substack{k,\ell \in \mathbb{N}_0 \\ k+\ell=n}} \frac{n!}{k!\ell!} a^k b^\ell \,.$$

Bemerkung und Beispiel (zum **Binomialsatz**)**.** Konkret kann man die in der binomischen Formel für festes n auftretenden **Binomialkoeffizienten in einer Zeile des Pascalschen Dreiecks ablesen**. Beispielsweise ergibt sich aus der $n = 4$ entsprechenden Zeile die Formel

$$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4 \,.$$

Der Satz kann problemlos mit vollständiger Induktion nach $n \in \mathbb{N}_0$ bewiesen werden. Ein besseres Hintergrund-Verständnis vermittelt aber:

Beweisidee zum Binomialsatz. Für $a_1 := a$, $a_2 := b$ besagt das allgemeine Distributivgesetz

$$(a+b)^n = \sum_{i_1, i_2, \ldots, i_n \in \{1,2\}} a_{i_1} a_{i_2} \cdot \ldots \cdot a_{i_n} \,,$$

wobei alle Terme rechts die Form $a^k b^{n-k}$ mit $k \in \{0, 1, 2, \ldots, n\}$ haben. In der Summe ergibt sich $a^k b^{n-k}$ genau dann, wenn genau k Indizes i_j gleich 1 und folglich die anderen $n-k$ gleich 2 sind, oder mit anderen Worten erhalten wir beim Ausmultiplizieren genau dann einen Term $a^k b^{n-k}$, wenn wir in k der zu multiplizierenden n Klammern $(a+b)$ den Summand a, in den anderen $n-k$ den Summand b wählen und die gewählten Summanden multiplizieren. Da es (vergleiche den bald folgenden Exkurs zur Kombinatorik) genau $\binom{n}{k}$ Möglichkeiten gibt, k aus den insgesamt n Indizes beziehungsweise k aus den insgesamt n Klammern auszuwählen, kommt $a^k b^{n-k}$ in der Summe rechts genau $\binom{n}{k}$ mal vor, und die Summe vereinfacht sich wie behauptet zu

$$\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \,.$$

Die Summe mit Koeffizienten $\frac{n!}{k!\ell!}$ ergibt sich daraus, indem man zu $k \in \{0, 1, 2, \ldots, n\}$ das eindeutige $\ell \in \mathbb{N}_0$ mit $k+\ell = n$ einführt (während für $k > n$ kein solches ℓ existiert). □

[4] Im Allgemeinen ist hier der Binomialkoeffizient $\binom{n}{k}$ bzw. $\frac{n!}{k!\ell!}$ in $\mathbb{N}_0$ zu bilden und dann mittels der in Abschnitt 3.2 besprochenen Zuordnung $n \mapsto n_{\mathbb{K}}$ als Element von $\mathbb{K}$ aufzufassen. Hat $\mathbb{K}$ Charakteristik 0, so liegt $\mathbb{Q}$ als Primkörper in $\mathbb{K}$ und dies ist nichts anders als die direkte Bildung des Binomialkoeffizienten in $\mathbb{K}$. Hat $\mathbb{K}$ aber Charakteristik $p \in \mathbb{P}$, so scheitert eine direkte Bildung in $\mathbb{K}$ eventuell an Null-Faktoren im Nenner.

Betrachtet man auf der linken Seite des allgemeinen Distributivgesetzes immer dieselbe Summe, aber nun mit einer beliebigen Zahl $m \in \mathbb{N}$ von Summanden, so führt dies auf folgende Verallgemeinerung des Binomialsatzes (der für $m = 2$ enthalten ist):

Satz (**Multinomialsatz**). *Sei $\mathbb{K}$ ein Körper, beispielsweise $\mathbb{R}$ oder $\mathbb{C}$. Für $n \in \mathbb{N}_0$, $m \in \mathbb{N}$ und $a_1, a_2, \ldots, a_m \in \mathbb{K}$ gilt (mit der Konvention $0^0 := 1$)*

$$(a_1+a_2+\ldots+a_m)^n = \sum_{\substack{k_1,k_2,\ldots,k_m\in\mathbb{N}_0\\ k_1+k_2+\ldots+k_m=n}} \frac{n!}{k_1!\,k_2!\cdot\ldots\cdot k_m!} a_1^{k_1} a_2^{k_2}\ldots a_m^{k_m}\,.$$

Auch der Multinomialsatz lässt sich entweder per Induktion oder analog zur beschriebenen Idee für den Binomialsatz beweisen, was wir hier jedoch nicht detailliert ausführen. Erwähnt sei nur, dass der **Multinomialkoeffizient** $\frac{n!}{k_1!\,k_2!\cdot\ldots\cdot k_m!} \in \mathbb{N}$ die Zahl der Möglichkeiten angibt, die Menge der insgesamt n Indizes auf der rechten Seite des allgemeinen Distributivgesetzes in m *disjunkte* Sets von Indizes zu zerlegen, wobei das erste Set aus k_1 Indizes besteht, das zweite aus k_2 Indizes, das dritte aus k_3 Indizes und schließlich das m-te und letzte Set aus k_m Indizes.

Eine gelegentlich nützliche Konsequenz der Sätze ist:

Korollar (**Summenformeln für Binomialkoeffizienten und Multinomialkoeffizienten**). *Für die Binomialkoeffizienten in der zu $n \in \mathbb{N}_0$ zugehörigen Zeile des Pascalschen Dreiecks gilt*

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

und für die Multinomialkoeffizienten zu $n \in \mathbb{N}_0$, $m \in \mathbb{N}$ gilt

$$\sum_{\substack{k_1,k_2,\ldots,k_m\in\mathbb{N}_0\\ k_1+k_2+\ldots+k_m=n}} \frac{n!}{k_1!\,k_2!\cdot\ldots\cdot k_m!} = m^n\,.$$

Beweis. Dies ergibt sich unmittelbar durch Anwendung des Binomialsatz mit $a = b = 1$ und des Multinomialsatzes mit $a_1 = a_2 = \ldots = a_m = 1$. □

Abschließend kommen wir auf die schon erwähnte Problematik allgemeiner Potenzsummen zurück und halten (ohne Ausführung aller Details) fest:

Bemerkung (zur **allgemeinen Potenzsummen-Formel**). Die **Bernoulli-Zahlen**[5] $b_k \in \mathbb{Q}$ zu $k \in \mathbb{N}_0$, sind rekursiv durch $b_0 := 1$ und $\sum_{j=0}^{k-1} \binom{k}{j} b_j = 0$ für $k \in \mathbb{N}_{\geq 2}$ definiert. Die Folge dieser Zahlen beginnt mit $b_0 = 1$, $b_1 = -\frac{1}{2}$, $b_2 = \frac{1}{6}$, $b_3 = 0$, $b_4 = -\frac{1}{30}$, $b_5 = 0$, $b_6 = \frac{1}{42}$, $b_7 = 0$, $b_8 = -\frac{1}{30}$, $b_9 = 0$, $b_{10} = \frac{5}{66}$ und ist so gewählt, dass sich für die durch $B_k(x) := (b_\bullet + x)^k := \sum_{j=0}^{k} \binom{k}{j} b_j x^{k-j}$ definierten Bernoulli-Polynome B_k gerade $B_k(x+1) - B_k(x) = kx^{k-1}$ nachrechnen lässt. Dies kann man nutzen und erhält analog zu den zuvor diskutieren Fällen bis Ordnung 3 durch Teleskop-Summation auch die **Potenzsummen-Formel beliebiger Ordnung**

$$\sum_{i=1}^{n-1} i^{k-1} = \frac{1}{k}\big[B_k(n) - b_k\big] = \frac{1}{k}\sum_{j=0}^{k-1} \binom{k}{j} b_j n^{k-j} \qquad \text{für alle } n \in \mathbb{N} \text{ und } k \in \mathbb{N}_{\geq 2}\,.$$

[5] Tatsächlich unterscheidet man die obigen Bernoulli-Zahlen *erster Art* b_k und die Bernoulli-Zahlen *zweiter Art* $b_k^* := (-1)^k b_k$. Man kann allerdings $b_k = 0$ für alle ungeraden $k \geq 3$ beweisen, so dass tatsächlich $b_k^* = b_k$ für alle $k \in \mathbb{N}_0 \setminus \{1\}$ gilt und einzig bei $b_1 = -\frac{1}{2}$ und $b_1^* = \frac{1}{2}$ ein Unterschied beim Vorzeichen besteht.

Exkurs: Grundlegende Kombinatorik

In der (abzählenden) Kombinatorik geht es darum, die **Anzahl der möglichen Konfigurationen/Anordnungen/Auswahlen** zu einer gegebenen Problemstellung zu bestimmen. Es geht dabei normalerweise um **endlich viele Möglichkeiten**, also letztlich um die Bestimmung von (eventuell sehr großen) natürlichen Zahlen.

Kombinatorik kann dabei als Grundlage für die **Bestimmung von Wahrscheinlichkeiten** dienen, und tatsächlich geht die Kombinatorik teils fließend in den Beginn der Wahrscheinlichkeitstheorie (die wiederum in das größere mathematische Gebiet der Stochastik fällt) über. Genauer ergibt sich, ***falls*** eine sogenannte Gleichverteilung vorliegt, bei der **alle Möglichkeiten gleich wahrscheinlich** sind, die Wahrscheinlichkeit (als Zahl aus $[0,1]$) für ein Ereignis als der Quotient

$$\frac{\text{„Zahl der günstigen Möglichkeiten“}}{\text{„Zahl aller Möglichkeiten“}},$$

wobei die günstigen Möglichkeiten eben die sind, für die das Ereignis eintritt. Ist das Ereignis zum Beispiel, mit einem handelsüblichen sechsseitigen Würfel bei zwei aufeinander folgenden Würfen mindestens einmal (eventuell auch zweimal) Vier zu würfeln, so ist die Wahrscheinlichkeit dafür $\frac{11}{36} \approx 30,56\%$, denn die 11 Würfelergebnisse Eins-Vier, Vier-Eins, Zwei-Vier, Vier-Zwei, Drei-Vier, Vier-Drei, Vier-Vier, Fünf-Vier, Vier-Fünf, Sechs-Vier, Vier-Sechs sind 11 günstige unter insgesamt 36 Möglichkeiten.

Trifft man auf Problemstellungen, bei denen nicht mehr alle Möglichkeiten als gleich wahrscheinlich angesehen werden können, so stößt dieses Vorgehen allerdings an seine Grenzen. Tendenziell nützen rein kombinatorische Überlegungen zur Berechnung von Wahrscheinlichkeiten daher häufig nur bei grundlegenden und seltener bei fortgeschrittenen Fragestellungen. In diesem Exkurs beschränken wir uns nun tatsächlich auf das reine Abzählen und haben höchstens den obigen Quotienten und Anwendungen im Stil des vorausgehenden Beispiels im Auge, während Sie Weitergehendes zu Wahrscheinlichkeiten in Ihrem Studium erst nach Abschluss der Grundvorlesungszyklusses Mathematik 1 bis 4 lernen.

Zuerst beschäftigen wir uns hier mit der kombinatorischen Zählung sogenannter Variationen:

Definition (**Variationen**)**.** *Für $k \in \mathbb{N}$ erklären wir eine **k-gliedrige Variation** aus einer (Grund-)Menge $\mathcal{X}$ als ein k-Tupel $(x_1, x_2, \ldots, x_k) \in \mathcal{X}^k$. Sind $x_1, x_2, \ldots, x_k$ alle verschieden, gilt also für $i \neq j$ in $\{1, 2, \ldots, k\}$ stets $x_i \neq x_j$, so sprechen wir von einer Variation **ohne Wiederholung**. Im Fall $\mathcal{X} = \{x_1, x_2, \ldots, x_k\}$ heißt die Variation **vollständig**.*

Bemerkungen (zu **Variationen**)**.** Seien $k \in \mathbb{N}$ und $\mathcal{X}$ eine Menge.

(1) **Entscheidend** ist bei Variationen die (in der Definition von Tupeln begründete) **Berücksichtigung der Reihenfolge der Einträge**, dass also etwa die beiden 4-gliedrigen Tupel $(2,5,5,7)$ und $(5,5,2,7)$ aus $\{2,3,5,7,11\}^4$ tatsächlich verschieden sind.

(2) Eine Variation $(x_1, x_2, \ldots, x_k) \in \mathcal{X}^k$ kann **auch als Abbildung** $\{1, 2, \ldots, k\} \to \mathcal{X}$, $i \mapsto x_i$ betrachtet werden. Eine Variation ohne Wiederholung entspricht dabei einer injektiven, eine vollständige Variation einer surjektiven Abbildung.

(3) Offensichtlich gibt es[6] k-gliedrige Variationen ohne Wiederholung aus $\mathcal{X}$ nur im Fall $|\mathcal{X}| \geq k$

[6] Das ziemlich offensichtliche Prinzip, dass es k-gliedrige Variationen ohne Wiederholung aus $\mathcal{X}$ nur im Fall $|\mathcal{X}| \geq k$ geben kann, ist auch als Schubfach-Prinzip bekannt: Um k Gegenstände ohne Doppelbelegung auf n Schubfächer verteilen zu können, muss $n \geq k$ sein.

und vollständige k-gliedrige Variationen aus $\mathcal{X}$ nur im Fall $|\mathcal{X}| \leq k$.

(4) Ein sinnvolles kombinatorisches Zählen ist (normalerweise) nur für eine **endliche Zahl** $n = |\mathcal{X}|$ **von Elementen** möglich. Es werden also meist nur endliche Grundmengen $\mathcal{X}$ betrachtet. Da es nur um die Anzahl der Elemente und Möglichkeiten geht, kann man sich tatsächlich auf $\mathcal{X} = \{1, 2, \ldots, n\}$ zurückziehen, wenn man das möchte.

(5) Anstelle der Indizes $1, 2, \ldots, k$ in der Definition ließe sich auch eine beliebige Indexmenge I mit $|I| = k$ Elementen verwenden. Variationen entsprächen dann Abbildungen $I \to \mathcal{X}$.

Interpretation (von **Variationen**)**.** Zwei typische anschauliche Modelle für Variationen folgen:

(1) Beim **Urnenmodell** entspricht $\mathcal{X}$ einer Menge von unterscheidbaren Kugeln, die aus einer Urne (so hier die traditionelle Benennung) gezogen werden. Zieht man k-mal nacheinander und notiert die gezogenen Kugeln in Reihenfolge der Ziehungen, so erhält man eine k-gliedrige Variation von $\mathcal{X}$. Allgemeine Variationen entsprechen hierbei einem **Ziehen mit Zurücklegen** der gezogenen Kugeln. Variationen ohne Wiederholung entsprechen einem **Ziehen ohne Zurücklegen**.

(2) Beim **Würfelmodell** wirft man einen Würfel mit einer Menge $\mathcal{X}$ von unterscheidbaren Seiten k-mal nacheinander. Notiert man die gefallenen Seiten (oder deren Augenzahlen) in Reihenfolge der Würfe, so erhält man eine k-gliedrige Variation von $\mathcal{X}$. (Speziell Variationen ohne Wiederholung kann man mit Würfeln weniger natürlich veranschaulichen. Dafür müsste man die Wiederholung der gleichen Seite vermeiden oder verwerfen.)

Als Hauptergebnis zu Variationen, das wir im Folgenden erklären, aber nicht völlig formal mit Mengen und Mächtigkeiten beweisen werden, halten wir fest:

Kombinatorische Prinzipien (**Zahl der Variationen**)**.** *Seien* $k, n \in \mathbb{N}$.

(I) *Die Zahl der k-gliedrigen* ***Variationen*** *aus einer n-elementigen Menge (und damit die Zahl der Abbildungen von einer k-elementigen in eine n-elementige Menge) ist*

$$\boxed{n^k}.$$

(II) *Die Zahl der k-gliedrigen* ***Variationen*** **ohne Wiederholung** *aus einer n-elementigen Menge (und damit die Zahl der* injektiven *Abbildungen von einer k-elementigen in eine n-elementige Menge) ist*

$$\boxed{n(n-1)(n-2)(n-3)\cdot\ldots\cdot(n-k+2)\cdot(n-k+1) = k!\binom{n}{k}},$$

was für $k > n$ gleich Null ist.

Begründung der Prinzipien. Betrachtet man allgemeine k-gliedrige Variationen einer n-elementigen Menge, so gibt es für jeden der k Einträge des Tupels, jeden der k Züge aus der Urne bzw. jeden der k Würfelwürfe jeweils n Möglichkeiten. Die einzelnen Möglichkeiten können über die k Einträge/Züge/Würfe beliebig kombiniert werden. Die Gesamtzahl aller möglichen Variationen ergibt sich daher als Produkt von k Faktoren n und ist n^k.

Betrachtet man nur k-gliedrige Variationen ohne Wiederholung einer n-elementigen Menge, so gibt es beim ersten Eintrag des Tupels, beim ersten Zug aus der Urne bzw. beim ersten Würfelwurf weiterhin n Möglichkeiten, beim zweiten aber nur $(n-1)$ Möglichkeiten, beim dritten nur noch $(n-2)$, da ein beziehungsweise zwei Ergebnisse durch das Vorgeschehen bereits ausgeschlossen sind. Dies setzt sich entsprechend bis zu $n-k+1$ Möglichkeiten beim k-ten Eintrag/Zug/Wurf fort. Die Gesamtzahl der möglichen Variationen ohne Wiederholung ergibt sich als das angegebene Produkt der k Faktoren. □

Folgerungen (aus dem **Zählen von Variationen**).

(1) Die **Zahl der Elemente der Potenzmenge** einer k-elementigen Menge I ist $\mathbf{2^k}$. Es gilt also, wie schon in Abschnitt 1.4 behauptet, $|\mathcal{P}(I)| = 2^{|I|}$. Dies folgt aus dem Prinzip (I) mit $n = 2$, indem wir jede Teilmenge A von $I = \{i_1, i_2, \ldots, i_k\}$ per Eins-zu-Eins-Korrespondenz mit der k-gliedrigen Variation $(x_{i_1}, x_{i_2}, \ldots, x_{i_k})$ aus der 2-elementigen Menge $\{0, 1\}$ identifizieren, bei der $x_{i_j} = 1$ für $i_j \in A$ und $x_{i_j} = 0$ für $i_j \notin A$ ist. (Mit anderen Worten entspricht A über seine Indikatorfunktion $\mathbb{1}_A \colon I \to \{0, 1\}$ einer k-gliedrigen Variation von $\{0, 1\}$.)

(2) Die **Zahl der Zerlegungen von $\ell \in \mathbb{N}$ in endlich viele Summanden $\in \mathbb{N}$** (unter Berücksichtigung der Reihenfolge der Summanden) ist $\mathbf{2^{\ell-1}}$. Dies ergibt sich, indem man eine Zerlegung in $m \in \mathbb{N}$ Summanden wie für $\ell = 8$ und $m = 4$ zum Beispiel $8 = 2+1+1+4$ durch eine Folge von ℓ Einsen, die durch $m-1$ Striche entsprechend gruppiert werden, im Beispiel $11|1|1|1111$, repräsentiert. Die Zerlegung entspricht dann für jede der $\ell-1$ Zwischenstellen zwischen benachbarten Einsen einer Wahl zwischen 2 Möglichkeiten, nämlich, ob dort ein Strich steht oder nicht. Gemäß dem Prinzip (I) mit $k = \ell-1$ und $n = 2$ bestehen somit insgesamt $2^{\ell-1}$ Auswahl-Möglichkeiten.

(3) Die **Zahl der Permutationen** einer n-elementigen Menge ist $\boldsymbol{n!}$. Es gilt also, wie schon in Abschnitt 3.1 behauptet, $|\mathrm{S}_n| = n!$. Dies ergibt sich als Spezialfall $k = n$ des Prinzips (II), denn Variationen ohne Wiederholung sind für $k = n$ automatisch vollständig (oder mit anderen Worten, injektive Abbildungen zwischen endlichen Mengen gleicher Elementzahl automatisch bijektiv).

Ergänzung (zu **Variationen mit gegebenen Vielfachheiten**). Von Interesse sind auch Variationen aus $\mathcal{X} = \{1, 2, \ldots, n\}$ mit gegebenen Vielfachheiten $k_1, k_2, \ldots, k_n \in \mathbb{N}_0$, bei denen $i \in \{1, 2, \ldots, n\}$ als Eintrag der Variation bzw. Zug-/Würfelergebnis jeweils genau k_i-mal vorkommen soll. Offensichtlich ist dies für eine k-gliedrige Variation genau im Fall $k_1+k_2+\ldots+k_n = k$ möglich.

Um solche Variationen zu zählen, kann man sich im Urnenmodell *zunächst* vorstellen, dass für jedes $i \in \{1, 2, \ldots, n\}$ genau k_i unterscheidbare Kugeln in die Urne gegeben und dann k Ziehungen ohne Zurücklegen aus den insgesamt k Kugeln erfolgen, bis die Urne am Ende leer ist. Hierbei gibt es nach dem Prinzip (II) $k!$ mögliche Ergebnisse. Tatsächlich ändert sich die Variation aber nicht, wenn zwei *gleiche* Einträge i vertauscht werden, wir müssen uns also *tatsächlich* vorstellen, dass für jedes $i \in \{1, 2, \ldots, n\}$ eine Gruppe von k_i *un*unterscheidbaren Kugeln in die Urne gegeben und nach den Ziehungen nur die Gruppennummer i notiert wird. Dies reduziert die Zahl der Ergebnisse, die notiert werden können, weil Vertauschungen der Reihenfolge *innerhalb der Gruppen* nun nichts mehr ändern. Genauer sind ausgehend von jedem möglichen Ergebnis innerhalb der Gruppe mit Nummer i stets $k_i!$ Permutationen[7] der Reihenfolge möglich

[7] Dabei zählt die Identität, die nichts ändert, natürlich als eine Permutation. Insbesondere erhält man also auch für $k_i \in \{0, 1\}$ mit $k_i! = 1$ das richtige Ergebnis.

und insgesamt dann $k_1!\,k_2!\cdot\ldots\cdot k_n!$ Permutationen, bei denen jede Kugel in ihrer Gruppe bleibt und sich die Variation nicht ändert. Wir haben somit beim vorläufigen Ergebnis $k!$ jede Variation $k_1!\,k_2!\cdot\ldots\cdot k_n!$-mal gezählt. Die tatsächliche **Zahl der k-gliedrigen Variationen von $\{1,2,\ldots,n\}$ mit gegebenen Vielfachheiten $k_1,k_2,\ldots,k_n\in\mathbb{N}_0$, $k_1+k_2+\ldots+k_n=k$ gibt** daher **der Multinomialkoeffizient**

$$\frac{k!}{k_1!\,k_2!\cdot\ldots\cdot k_n!}$$

an. (Da die Zahl der betreffenden Variationen eine ganze Zahl ist, kommt bei diesem (zugegeben) nicht ganz formalen Argument übrigens mit heraus, dass die Multinomialkoeffizienten, wie in Abschnitt 4.3 behauptet, stets $\in\mathbb{N}$ sind.) Ein Anwendungsbeispiel hierzu folgt in den Übungen.

Da zu jeder Variation eindeutige Vielfachheiten gehören, muss die Summe über alle möglichen Vielfachheiten

$$\sum_{\substack{k_1,k_2,\ldots,k_n\in\mathbb{N}_0\\ k_1+k_2+\ldots+k_n=k}}\frac{k!}{k_1!\,k_2!\cdot\ldots\cdot k_n!}=n^k$$

die Gesamtzahl n^k des Prinzips (I) ergeben, was auch die Summenformel für die Multinomialkoeffizienten aus Abschnitt 4.3 bestätigt. Beschränkt man sich bei der Summation nur auf Vielfachheiten $k_i\in\{0,1\}$ beziehungsweise $k_i\in\mathbb{N}$, so erhält man die Zahl der Variationen ohne Wiederholung beziehungsweise der vollständigen Variationen. Im ersteren Fall verschwinden dabei wegen $0!=1!=1$ alle Nenner und die Summe erweist sich als Summe von $\binom{n}{k}$ gleichen Faktoren $k!$ (wobei die Zahl $\binom{n}{k}$ der Summanden mit dem Ergebnis des Prinzips (II) zusammenpasst und demnächst bei der Zählung von Kombinationen noch bestätigt wird). Für die Zahl der *vollständigen* k-gliedrigen Variationen aus einer n-elementigen Menge (und die entsprechende Zahl *surjektiver* Abbildungen) wünscht man sich ebenfalls eine besser handhabbare Formel als die über die Summation von Multinomialkoeffizienten. Die Herleitung einer solchen Formel ist deutlich schwieriger, gelingt aber mit dem Siebverfahren von Sylvester und Poincaré und gibt die Zahl der *vollständigen* k-gliedrigen Variationen aus einer n-elementigen Menge als $\sum_{\ell=0}^{n-1}(-1)^\ell\binom{n}{\ell}(n-\ell)^k$ an. Die wesentliche Idee der Herleitung ist, zunächst alle Variationen zu zählen und dies dann nach und nach um (Mehrfach-)Zählungen solcher Variationen zu korrigieren, bei denen zunächst ein, dann zwei, dann drei, usw. Elemente nicht auftreten. Weitere Details gehen deutlich über das Ziel dieses Exkurses hinaus und werden hier nicht besprochen.

Im zweiten Teil dieses Exkurses kommen wir zur Zählung sogenannter Kombinationen:

Definition (**Kombinationen**)**.** *Für $k\in\mathbb{N}$ und eine Menge $\mathcal{X}$ erklären wir eine Äquivalenzrelation $\sim$ auf $\mathcal{X}^k$ durch*

$$y\sim x:\Longleftrightarrow\exists\pi\in\mathrm{S}_k\colon y_1=x_{\pi(1)}\,,\ y_2=x_{\pi(2)}\,,\ \ldots\,,\ y_k=x_{\pi(k)}\qquad\text{für } x,y\in\mathcal{X}^k\,.$$

*Als eine k-**gliedrige Kombination** aus der Menge $\mathcal{X}$ bezeichnen wir eine Äquivalenzklasse $[(x_1,x_2,\ldots,x_k)]_\sim\in\mathcal{X}^k/\!\sim$ bezüglich dieser Relation. Sind $x_1,x_2,\ldots,x_k$ alle verschieden, gilt also für $i\neq j$ in $\{1,2,\ldots,k\}$ stets $x_i\neq x_j$, so sprechen wir von einer Kombination **ohne Wiederholung**. Im Fall $\mathcal{X}=\{x_1,x_2,\ldots,x_k\}$ heißt die Kombination **vollständig**.*

Bemerkungen (zu **Kombinationen**)**.** Seien $k\in\mathbb{N}$ und $\mathcal{X}$ eine Menge.

(1) In den Äquivalenzklassen bezüglich $\sim$ werden jeweils diejenigen Tupel zusammengefasst, die dieselben Einträge in unterschiedlicher Reihenfolge enthalten, in $\{2,3,5,7,11\}^4/\!\sim$ gilt zum Beispiel $[(2,5,5,7)]_\sim=[(5,5,2,7)]_\sim$. Die Definition von Kombinationen als solche Äquivalenzklassen bedeutet, dass die **Reihenfolge der Einträge** bei Kombinationen ***nicht* berücksichtigt** wird.

(2) Man kann sich auf **Standard-Repräsentanten** der Äquivalenzklassen einigen und für $\mathcal{X}=\{1,2,\ldots,n\}$ mit $n\in\mathbb{N}$ nutzen, dass jede Äquivalenzklasse in $\{1,2,\ldots,n\}^k/\!\sim$ einen eindeutigen Repräsentanten $(x_1,x_2,\ldots,x_k)\in\mathcal{X}^k$ mit $x_1\le x_2\le x_3\le\ldots\le x_{k-1}\le x_k$ besitzt (im Fall ohne Wiederholung sogar mit „$<$“). Tatsächlich wird eine Kombination in der

Literatur zu allermeist als ein Tupel mit dieser Zusatzeigenschaft definiert, da man so die Begriffe Äquivalenzrelation und -klasse umgehen kann. Sind einem diese Begriffe vertraut, so ist die obige Definition aber konzeptionell klarer (und macht auch direkt deutlich, dass der Begriff der Kombination keinesfalls von einer Ordnung auf $\mathcal{X}$ abhängt).

(3) Eine k-gliedrige Kombination $(x_1, x_2, \ldots, x_k) \in \mathcal{X}^k/\sim$ ohne Wiederholung kann **auch als k-elementige Teilmenge** $\{x_1, x_2, \ldots, x_k\}$ von $\mathcal{X}$ betrachtet werden. Eine allgemeine k-gliedrige Kombination wird **auch durch die Vielfachheiten** $k_x \in \mathbb{N}_0$, mit der die Einträge $x \in \mathcal{X}$ jeweils auftreten, beschrieben, wobei[8] $\sum_{x\in\mathcal{X}} k_x = k$ gilt.

(4) Genau wie bei Variationen gibt es k-gliedrige Kombinationen ohne Wiederholung aus $\mathcal{X}$ nur im Fall $|\mathcal{X}| \geq k$ und vollständige k-gliedrige Kombinationen aus $\mathcal{X}$ nur im Fall $|\mathcal{X}| \leq k$, von Interesse ist nur der Fall $n = |\mathcal{X}| < \infty$, und man könnte einerseits nur $\mathcal{X} = \{1, 2, \ldots, n\}$, andererseits statt $1, 2, \ldots, k$ Indizes aus einer beliebigen Menge I mit $|I| = k$ betrachten.

Interpretation (von **Kombinationen**)**.** Mit dem **Urnenmodell** (mit/ohne Zurücklegen) und dem **Würfelmodell** lassen sich neben Variationen auch Kombinationen veranschaulichen, wenn bei den Ergebnissen die Reihenfolge der Ziehungen beziehungsweise Würfe *nicht* berücksichtigt wird. Somit sind im Hinblick auf Kombinationen $(2, 5, 5, 7)$ und $(5, 5, 2, 7)$ als gleiche Ergebnisse zu betrachten, oder es wird im Geist der Bemerkung (2) gleich in beiden Fällen $(2, 5, 5, 7)$ notiert. Eine konkrete Instanz des Urnenmodells ohne Zurücklegen ist die **Lotto-Ziehung** von 6 aus 49 nummerierten Kugeln, bei der es im Ergebnis auf die Reihenfolge der Ziehungen nicht ankommt. Somit geht es beim 6-aus-49-Lotto um 6-gliedrige Kombinationen aus $\{1, 2, 3, \ldots, 47, 48, 49\}$.

Tatsächlich kann man sich beim Urnenmodell ohne Zurücklegen (für Kombinationen ohne Wiederholung) und beim Würfelmodell (für alle Kombinationen) den Ablauf auch so vorstellen, dass eine Gesamt-Ziehung von k Kugeln aus einer Urne beziehungsweise ein simultaner Wurf mit k Würfeln erfolgt. Bei dieser Vorstellung ist die Vernachlässigung der Reihenfolge dann fest eingebaut, da gar nicht mehr einzeln und in Reihenfolge gezogen beziehungsweise gewürfelt wird.

Als Hauptergebnis zu Kombinationen bekommen wir:

Kombinatorische Prinzipien (**Zahl der Kombinationen**)**.** *Seien $k, n \in \mathbb{N}$.*

(I) *Die Zahl der k-gliedrigen **Kombinationen** aus einer n-elementigen Menge ist*

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

(II) *Die Zahl der k-gliedrigen **Kombinationen ohne Wiederholung** aus einer n-elementigen Menge (und damit die Zahl der **k-elementigen Teilmengen** einer n-elementigen Menge) ist*

$$\boxed{\binom{n}{k}},$$

was für $k > n$ gleich Null ist.

[8] Im Fall $|\mathcal{X}| = \infty$, der hier formal zugelassen, aber nicht von Interesse ist, lässt man $k_x \neq 0$ nur für endliche viele $x \in \mathcal{X}$ zu, so dass $\sum_{x\in\mathcal{X}} k_x := \sum_{\substack{x\in\mathcal{X}\\ k_x\neq 0}} k_x$ sinnvoll bleibt.

(III) *Die Zahl der k-gliedrigen* **vollständigen *Kombinationen*** *aus einer n-elementigen Menge ist*

$$\boxed{\binom{k-1}{n-1} = \binom{k-1}{k-n}},$$

was für $k < n$ gleich Null ist.

Bemerkung. Eine k-elementige Teilmenge von $\mathcal{X}$ mit $|\mathcal{X}| = n$ lässt sich beschreiben, indem man entweder ihre k Elemente aus $\mathcal{X}$ auswählt oder für jedes der n in Frage kommenden Elemente eine $\{0,1\}$-Auswahl trifft, ob es zur Teilmenge gehört (dies k-mal) oder nicht (dies $(n-k)$-mal). Daher entsprechen die k-elementigen Teilmengen von $\mathcal{X}$ sowohl k-gliedrigen Kombinationen aus $\mathcal{X}$, wie wir sie hier im Prinzip (II) betrachten, als auch n-gliedrigen *Variationen* aus $\{0,1\}$ mit gegebenen Vielfachheiten $n_1 = k$ und $n_0 = n-k$, was sich als der Spezialfall einer 2-elementigen Grundmenge in der Ergänzung zu Variationen mit gegebenen Vielfachheiten erweist. Wir können das Ergebnis des Prinzips (II) also aus dem Vorausgehenden schon ablesen, geben jetzt aber trotzdem ein separates und leichter zugängliches Argument an.

Begründung der Prinzipien. Wir behandeln ohne Einschränkung die Grundmenge $\{1,2,\ldots,n\}$.

Einfacher gestaltet sich zunächst die Begründung für das Prinzip (II) zur Zahl der k-gliedrigen Kombinationen ohne Wiederholung aus $\{1,2,\ldots,n\}$: Sind nämlich $x_1,x_2,\ldots,x_k \in \{1,2,\ldots,n\}$ alle verschieden, so ergibt sich für jede der $k!$ Permutationen $\pi \in \mathrm{S}_k$ ein anderes Tupel $(x_{\pi(1)},x_{\pi(2)},\ldots,x_{\pi(k)})$, und die Äquivalenzklasse $[(x_1,x_2,\ldots,x_k)]_\sim$ besteht aus genau $k!$ so entstehenden *Variationen* ohne Wiederholung. Es werden also bei der Bildung von $\{1,2,\ldots,n\}^k/\!\sim$ jeweils $k!$ Variationen ohne Wiederholung zu einer Kombination ohne Wiederholung zusammengefasst, weshalb die Zahl $k!\binom{n}{k}$ der Variationen ohne Wiederholung lediglich durch $k!$ zu teilen ist, um die Zahl $\binom{n}{k}$ der Kombinationen ohne Wiederholung zu erhalten.

Zur Begründung des Prinzips (I) beschreiben wir eine allgemeine k-gliedrige Kombination aus $\{1,2,\ldots,n\}$ durch ihre Vielfachheiten $k_1,k_2,\ldots,k_n \in \mathbb{N}_0$ mit $k_1+k_2+\ldots+k_n = k$ und diese ähnlich wie schon früher durch Einfügen von $n-1$ Strichen zwischen k Einsen, wobei beispielsweise die 6-gliedrige Kombination $[(4,1,2,4,1,1)]_\sim$ aus $\{1,2,3,4\}$ mit Vielfachheiten $k_1 = 3, k_2 = 1, k_3 = 0, k_4 = 2$ der Folge $111|1||11$ entspricht. Hierbei sind allgemein aus insgesamt $k+n-1$ Positionen die der k Einsen beziehungsweise äquivalent der $n-1$ Striche auszuwählen. Eine allgemeine k-gliedrige Kombination aus $\{1,2,\ldots,n\}$ entspricht also der Auswahl einer k-elementigen beziehungsweise $(n-1)$-elementigen Teilmenge aus einer $(n+k-1)$-elementigen Menge. Hierfür gibt es nach dem schon begründeten Prinzip (II) genau $\binom{k+n-1}{k} = \binom{k+n-1}{n-1}$ Möglichkeiten.

Alternativ kann man das Prinzip (I) herleiten, indem man eine Bijektion zwischen den allgemeinen k-gliedrigen Kombinationen aus $\{1,2,\ldots,n\}$ und den k-gliedrigen Kombinationen ohne Wiederholung aus $\{1,2,\ldots,k+n-1\}$ herstellt. Dazu bildet man tatsächlich eine k-gliedrige Kombination $[(x_1,x_2,x_3,\ldots,x_{k-1},x_k)]_\sim$ aus $\{1,2,\ldots,n\}$, die mit dem Standard-Repräsentant angegeben wird, also $x_1 \le x_2 \le x_3 \le \ldots \le x_{k-1} \le x_k$ erfüllt, auf die k-gliedrige Kombination ohne Wiederholung $[(x_1,x_2+1,x_3+2,\ldots,x_{k-1}+k-2,x_k+k-1)]_\sim$ aus $\{1,2,\ldots,k+n-1\}$ ab (die dann $x_1 < x_2+1 < x_3+2 < \ldots < x_{k-1}+k-2 \le x_k+k-1$ erfüllt).

Zur Herleitung des Prinzips (III) beschreiben wir eine vollständige k-gliedrige Kombination aus $\{1,2,\ldots,n\}$ wieder durch die Vielfachheiten $k_1,k_2,\ldots,k_n \in \mathbb{N}$ (Null nun ausgeschlossen) mit $k_1+k_2+\ldots+k_n = k$ und diese wie zuvor durch das Einfügen von $n-1$ Strichen zwischen k Einsen. Dabei dürfen zwischen benachbarten Einsen aber nicht wie bei allgemeinen Kombinationen mehrere Striche auftreten, sondern es steht dort entweder ein Strich oder kein Strich. Es sind also

jetzt aus den $k-1$ Zwischenstellen zwischen benachbarten Einsen die $n-1$ mit Strich beziehungsweise äquivalent die $k-n$ ohne Strich auszuwählen. Eine vollständige k-gliedrige Kombination aus $\{1, 2, \ldots, n\}$ entspricht somit der Auswahl einer $(n-1)$-elementigen beziehungsweise $(k-n)$-elementigen Teilmenge aus einer $(k-1)$-elementigen Menge. Hierfür gibt es nach dem Prinzip (II) genau $\binom{k-1}{n-1} = \binom{k-1}{k-n}$ Möglichkeiten. □

Folgerungen (aus dem **Zählen von Kombinationen**).

(0) Die **Zahl der k-elementigen Teilmengen** einer n-elementigen Menge beträgt gemäß dem Prinzip (II) gerade $\binom{n}{k}$.

(1) Die Zahl der Tupel $(x_1, x_2, \ldots, x_k) \in \{1, 2, \ldots, n\}^k$ mit $x_1 \leq x_2 \leq x_3 \leq \ldots \leq x_{k-1} \leq x_k$ ist $\binom{k+n-1}{k} = \binom{k+n-<1}{n-1}$, und unter diesen sind $\binom{n}{k}$ mit $x_1 < x_2 < x_3 < \ldots < x_{k-1} < x_k$. Dies folgt direkt aus den Prinzipien (I) und (II), denn zur jeder Kombination gehört genau ein solches Tupel (das, wie schon erwähnt, als Standard-Repräsentant genutzt werden kann).

(2) Die **Zahl der Zerlegungen von $k \in \mathbb{N}$ in $n \in \mathbb{N}$ Summanden $\in \mathbb{N}_0$** (unter Berücksichtigung der Reihenfolge der Summanden) ist $\binom{k+n-1}{k} = \binom{k+n-1}{n-1}$, und die **Zahl der Zerlegungen von $k \in \mathbb{N}$ in $n \in \mathbb{N}$ Summanden $\in \mathbb{N}$** (ebenfalls unter Berücksichtigung der Reihenfolge) ist $\binom{k-1}{n-1} = \binom{k-1}{k-n}$. Dies ergibt sich mit den Begründungen der Prinzipien (I) und (III).

(3) Beim 6-aus-49-Lotto (ohne Berücksichtigung von Zusatz-/Superzahlen) gibt es nach dem Prinzip (II) genau $\binom{49}{6} = 13.983.816$ Kombinations-Möglichkeiten. Darunter sind für $r \in \{0, 1, 2, 3, 4, 5, 6\}$ jeweils $\binom{6}{r}\binom{43}{6-r}$ günstige Möglichkeiten, dass bei einer festen 6-aus-49-Ziehung von 6 abgegebenen Zahlentipps r richtige gezogen und $6-r$ falsche nicht gezogen werden. Die Wahrscheinlichkeit für „r Richtige“ ist somit $\binom{6}{r}\binom{43}{6-r}/\binom{49}{6} \in (0, 1)$ und beträgt für $r = 0, 1, 2, 3, 4, 5, 6$ circa $43,6\%$, $41,3\%$, $13,2\%$, $1,8\%$, $9,7{\cdot}10^{-4}$, $1,8{\cdot}10^{-5}$, $7,1{\cdot}10^{-8}$.

(4) Die Wahrscheinlichkeit, beim Ziehen ohne Zurücklegen aus einer Urne mit $s \in \mathbb{N}$ schwarzen Kugeln und $w \in \mathbb{N}$ weißen Kugeln in $i+j$ Zügen genau $i \in \{0, 1, 2 \ldots, s-1, s\}$ schwarze und $j \in \{0, 1, 2, \ldots, w-1, w\}$ weiße Kugeln zu ziehen, beträgt gemäß dem Prinzip (II) genau $\binom{s}{i}\binom{w}{j}/\binom{s+w}{i+j} \in (0, 1]$. Um dies detaillierter zu begründen, stellt man sich die $s+w$ schwarzen und weißen Kugeln zunächst einzeln unterscheidbar (z.B. zusätzlich durchnummeriert) vor und hat dann bei $i+j$ Zügen und ohne Berücksichtigung der Reihenfolge[9] insgesamt $\binom{s+w}{i+j}$ mögliche und gleich wahrscheinliche (!) Zugergebnisse. Nun gibt es $\binom{s}{i}$ Möglichkeiten, sich i aus den s schwarzen, und $\binom{w}{j}$ Möglichkeiten, sich j aus den w weißen Kugeln auszusuchen. Damit sind unter den Zugergebnissen als günstige Möglichkeiten $\binom{s}{i}\binom{w}{j}$ mit genau i schwarzen und j weißen Kugeln, und die gesuchte Wahrscheinlichkeit ergibt sich in der Tat als der behauptete Quotient mit Zähler $\binom{s}{i}\binom{w}{j}$ und Nenner $\binom{s+w}{i+j}$.

Zusammenfassend lassen sich die Hauptergebnisse dieses Exkurses wie folgt festhalten:

[9] Mit Berücksichtigung der Reihenfolge gibt es $(i+j)!\binom{s+w}{i+j}$ Ergebnisse, die ebenfalls alle gleich wahrscheinlich sind. Aber, wenn man es so anginge, dann ließen sich die günstigen Fälle nicht so einfach zählen.

Anzahl	k-gliedrige **Variationen** aus n-elementiger Menge	k-gliedrige **Kombinationen** aus n-elementiger Menge
alle	n^k	$\binom{k+n-1}{k} = \binom{k+n-1}{n-1}$
ohne Wiederholung	$n(n-1)(n-2)\cdot\ldots\cdot(n-k+1)$	$\binom{n}{k}$
vollständige	komplizierter	$\binom{k-1}{n-1} = \binom{k-1}{k-n}$
vollständige ohne Wiederholung	$\begin{cases} n! & \text{für } k = n \\ 0 & \text{sonst} \end{cases}$	$\begin{cases} 1 & \text{für } k = n \\ 0 & \text{sonst} \end{cases}$
mit geg. Vielfachheiten $k_1, k_2, \ldots, k_n \in \mathbb{N}_0$, $k_1+k_2+\ldots+k_n = k$	$\dfrac{k!}{k_1!\,k_2!\cdot\ldots\cdot k_n!}$	1

Kapitel 5

Grenzwerte und Konvergenz bei Folgen und Reihen, Grundfunktionen

Das **präzise Konzept des Grenzwerts** zählt zu den wichtigsten Grundlagen der Mathematik und kann als ***der* zentrale Grundpfeiler der Analysis** angesehen werden. Unter den verschiedenen Grenzwertbegriffen behandeln wir **zunächst Grenzwerte von Folgen** reeller oder komplexer Zahlen, wobei die meisten wichtigen Eigenschaften bereits auftreten werden.

5.1 Grenzwerte von Folgen

Wir präzisieren zunächst, dass eine Folge eine Abbildung mit Definitionsbereich $\mathbb{N}$ ist:

Definition (**Folgen**). *Eine* ***Folge*** *(von Elementen) in einer Menge $\mathcal{X}$ ist eine Abbildung $a \in \mathcal{X}^{\mathbb{N}} = \mathrm{Abb}(\mathbb{N}, \mathcal{X})$ von der Menge $\mathbb{N}$ der natürlichen Zahlen nach $\mathcal{X}$. Die einzelnen Funktionswerte $a(n) \in \mathcal{X}$ zu $n \in \mathbb{N}$ heißen die* ***Folgenglieder****. Meist notiert man a_n für einzelne Folgenglieder $a(n)$ sowie $(a_n)_{n\in\mathbb{N}}$ oder $(a_1, a_2, a_3, \ldots)$ für die ganze Folge a.*

Bemerkung. Auch bei „verwandten“ Definitionsbereichen wie $\mathbb{N}_0$, $\mathbb{N}_{\geq k}$, $\mathbb{Z}_{<0}$ oder $\mathbb{Z}$ spricht man manchmal von Folgen, im Fall des Definitionsbereichs $\mathbb{Z}$ gelegentlich auch von Bifolgen, und nutzt die Terminologie analog.

Für allgemeine Definitionsbereiche dagegen verwendet man dagegen eher den Begriff der Familie (den wir hier aber nur am Rande festhalten):

Definition (**Familien**). *Eine* ***Familie*** *(von Elementen) aus/über einer Menge $\mathcal{X}$ ist eine Abbildung $a \in \mathcal{X}^I = \mathrm{Abb}(I, \mathcal{X})$ von einer beliebigen (Index-)Menge I nach $\mathcal{X}$. Man notiert a_i für einzelne Elemente $a(i)$ der Familie und $(a_i)_{i\in I}$ für die ganze Familie a.*

Nach diesen ersten begrifflichen Klärungen kommen wir jetzt zum entscheidenden Punkt:

Motivation (des **Grenzwertbegriffs**). Uns interessieren Folgen $(a_n)_{n\in\mathbb{N}}$ reeller oder komplexer Zahlen, bei denen **die Glieder a_n für immer größere n einer festen Zahl beliebig nahe kommen**. Natürlich zeigt nicht jede Zahlenfolge ein solches Verhalten, aber, wenn dieses Phänomen auftritt, dann möchten wir es beschreiben.

Konkrete Beispiele, die abgedeckt werden sollen, sind etwa die Folgen mit den Gliedern $\frac{1}{n}$ und $\left(-\frac{1}{2}\right)^n$, die 0 beliebig nahe kommen, sowie die mit den Gliedern $\frac{n-1}{n}$ und $\frac{n}{n+1}$, die 1 beliebig nahe

kommen. Typische Darstellungen dieser Beispiele zeigt Abbildung 35. Ein weiterer Modellfall ist die Folge mit Gliedern $\left(1+\frac{1}{n}\right)^n$, die sich — wie wir noch sehen werden — einer als Eulersche Zahl e bekannten Zahl annähern.

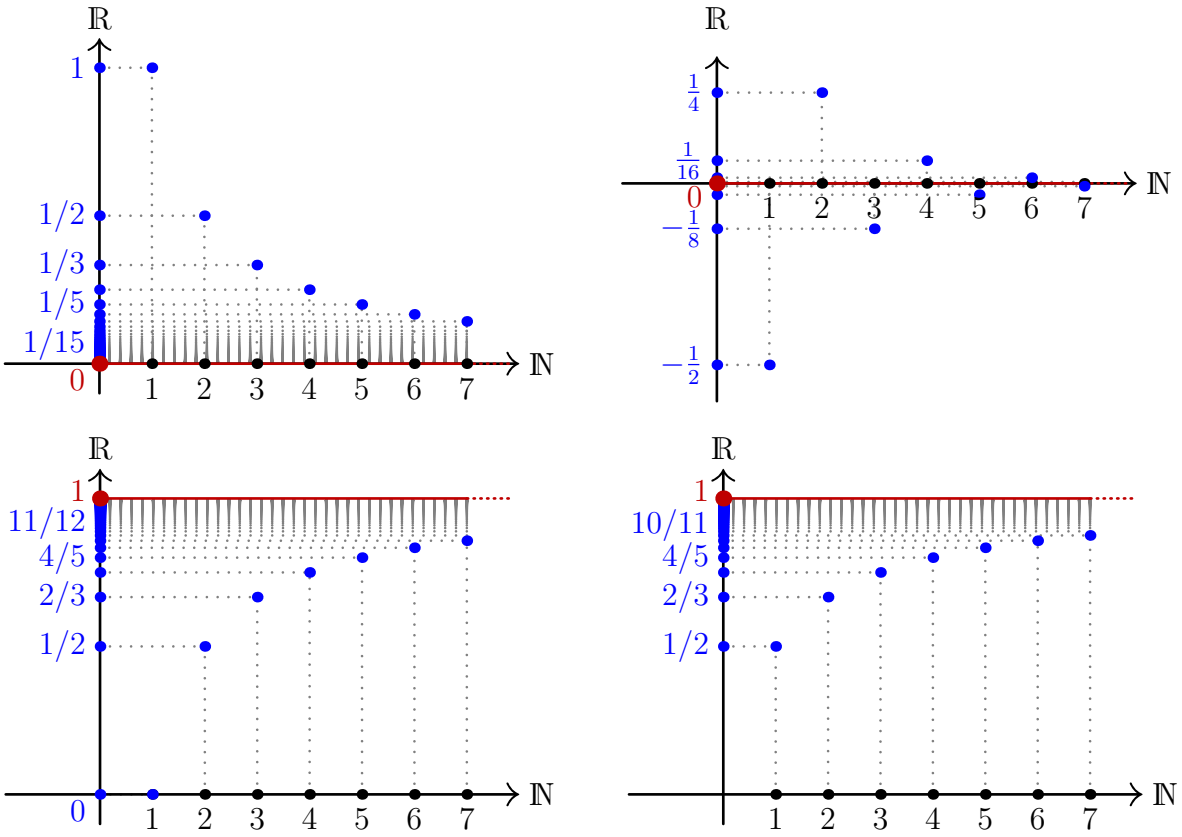


Abb. 35: Einige Folgenglieder $\frac{1}{n}$ (links oben), $(-\frac{1}{2})^n$ (rechts oben), $\frac{n-1}{n}$ (links unten), $\frac{n+1}{n}$ (rechts unten) mit dem jeweiligen Grenzwert 0 bzw. 1

Die präzise Beschreibung solcher Annäherungsprozesse erfordert ein ausgefeiltes Konzept, das sich tatsächlich erst im Zug einer langen historischen Entwicklung herauskristallisiert hat:

Definition (**Grenzwerte** und **Konvergenz** bei Folgen)**.** *Seien* $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$, $(a_n)_{n\in\mathbb{N}}$ *eine Folge in* $\mathbb{K}$ *und* $a \in \mathbb{K}$*. Dann heißt* a ***Grenzwert*** *oder* ***Limes*** *der Folge* $(a_n)_{n\in\mathbb{N}}$*, und* $(a_n)_{n\in\mathbb{N}}$ *heißt* ***(bei*** $n \to \infty$***) gegen*** a ***konvergent****, wenn es zu jedem* $\varepsilon \in \mathbb{R}_{>0}$ *ein* $n_0 \in \mathbb{N}$ *gibt, so dass für alle* $n \in \mathbb{N}$ *mit* $n \geq n_0$ *die Ungleichung* $|a_n - a| < \varepsilon$ *gilt. Man notiert hierfür*

$$\lim_{n\to\infty} a_n = a \qquad \text{oder gleichbedeutend} \qquad a_n \underset{n\to\infty}{\longrightarrow} a\,.$$

Besitzt $(a_n)_{n\in\mathbb{N}}$ *einen Grenzwert in (einer Teilmenge von)* $\mathbb{K}$*, so heißt die Folge* $(a_n)_{n\in\mathbb{N}}$ *in (dieser Teilmenge von)* $\mathbb{K}$ ***konvergent*** *und andernfalls* ***divergent****.*

Bemerkungen (zur **Definition des Grenzwerts**)**.**

(1) In einer **Formulierung mit Quantoren** liest sich die Definition wie folgt: Dass a Grenzwert von $(a_n)_{n\in\mathbb{N}}$ ist, bedeutet

$$\forall \varepsilon \in \mathbb{R}_{>0} \colon \exists n_0 \in \mathbb{N} \colon \forall n \in \mathbb{N}_{\geq n_0} \colon |a_n - a| < \varepsilon\,.$$

Dass $(a_n)_{n\in\mathbb{N}}$ in einer Teilmenge $\mathcal{X}$ von $\mathbb{K}$ konvergent ist, bedeutet

$$\exists a \in \mathcal{X}\colon \forall \varepsilon \in \mathbb{R}_{>0}\colon \exists n_0 \in \mathbb{N}\colon \forall n \in \mathbb{N}_{\geq n_0}\colon |a_n - a| < \varepsilon\,.$$

Der Typ und die genaue Reihenfolge der Quantoren sind hierbei essentiell.

(2) **Ein Grenzwert existiert nicht immer**. Die Folge $(0,1,0,1,0,1,0,1,0,1,0,\ldots)$ zum Beispiel besitzt keinen Grenzwert, ist also divergent. **Wenn ein Grenzwert existiert, so ist er** aber **stets eindeutig.** Zur Einführung in die Arbeit mit dem Grenzwertbegriff, wird der einfache Beweis der Eindeutigkeit nun (fast schon zu) detailliert erörtert:

Beweis für die Eindeutigkeit des Grenzwerts einer Folge. Seien $a, \widetilde{a} \in \mathbb{K}$ zwei Grenzwerte einer Folge $(a_n)_{n\in\mathbb{N}}$ in $\mathbb{K}$. Ist dann $\widetilde{a} \neq a$, so liefert die Definition, angewandt mit $\varepsilon = \frac{1}{2}|\widetilde{a}-a| > 0$, zwei Zahlen $n_0, \widetilde{n}_0 \in \mathbb{N}$, so dass

$$|a_n - a| < \tfrac{1}{2}|\widetilde{a}-a| \text{ für } n \in \mathbb{N}_{\geq n_0} \qquad \text{und} \qquad |a_n - \widetilde{a}| < \tfrac{1}{2}|\widetilde{a}-a| \text{ für } n \in \mathbb{N}_{\geq \widetilde{n}_0}$$

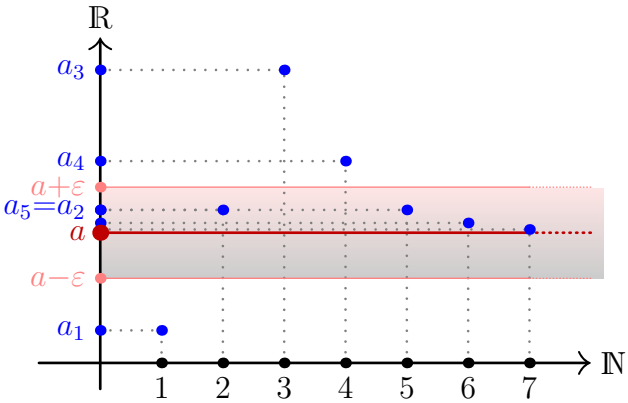
gelten. Für die Zahl $n_* := \max\{n_0, \widetilde{n}_0\} \in \mathbb{N}$ sind beide diese Ungleichungen anwendbar, und mit der Dreiecksungleichung aus Abschnitt 4.2 folgt

$$|\widetilde{a}-a| \leq |a_{n_*} - \widetilde{a}| + |a_{n_*} - a| < \tfrac{1}{2}|\widetilde{a}-a| + \tfrac{1}{2}|\widetilde{a}-a| = |\widetilde{a}-a|\,.$$

Als Resultat erhalten wir den Widerspruch $|\widetilde{a}-a| < |\widetilde{a}-a|$, also kann $\widetilde{a} \neq a$ nicht auftreten, und es muss $\widetilde{a} = a$ gelten. □

(3) Die in Bemerkung (1) auftretende Quantoren-Abfolge $\exists n_0 \in \mathbb{N}\colon \forall n \in \mathbb{N}_{\geq n_0}$ bedeutet, dass die folgende Aussage für **alle bis auf endlich viele $n \in \mathbb{N}$** gilt. Verbreitete Umschreibungen für genau diesen Sachverhalt sind, dass die Aussage **für fast alle $n \in \mathbb{N}$**, **für ausreichend große $n \in \mathbb{N}$** oder **für (alle) $n \gg 1$** (lies: n wesentlich größer als 1) gilt.

(4) Mit anderen Worten verlangt die Grenzwertdefinition, dass für alle (noch so kleinen) $\varepsilon > 0$ die Folgenglieder a_n mit ausreichend großem n für $\mathbb{K} = \mathbb{C}$ alle im Kreis in der Gaußschen Zahlenebene mit Radius ε und Mittelpunkt a liegen und für $\mathbb{K} = \mathbb{R}$ alle im Intervall $(a-\varepsilon, a+\varepsilon)$. Dabei ist entscheidend, dass der Kreis bzw. das Intervall wirklich *alle* Folgenglieder ab einem (tendenziell) großen Index n_0 beinhalten. Dass sie stattdessen „nur“ unendlich viele Folgenglieder enthalten, ist noch keine gleichermaßen starke Forderung; dies erkennt man wieder am Beispiel der divergenten Folge $(0,1,0,1,0,1,0,1,0,1,\ldots)$.



Eine Folge $(a_n)_{n\in\mathbb{N}}$ in $\mathbb{R}$ mit Grenzwert a und als „2ε-Schlauch“ dargestelltem Intervall $(a-\varepsilon, a+\varepsilon)$

(5) **Abänderung endlich vieler Folgenglieder ändert nichts am Grenzwert** (und auch nicht seine Existenz oder Nicht-Existenz), d.h. aus $a_n = b_n$ für *fast* alle $n \in \mathbb{N}$ folgt $\lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n$. Vor diesem Hintergrund betrachtet man Grenzwerte $\lim_{n\to\infty} a_n$ auch dann, wenn a_n nur für *fast* alle, aber eventuell nicht für alle $n \in \mathbb{N}$ definiert ist.

(6) **Konvergente Folgen sind stets beschränkt** (wobei Beschränktheit einer Folge $(a_n)_{n\in\mathbb{N}}$ bedeutet, dass die Menge $\{a_n \mid n \in \mathbb{N}\}$ beschränkt ist, also $\sup_{n\in\mathbb{N}} |a_n| < \infty$ gilt).

Beweis. Ist $(a_n)_{n\in\mathbb{N}}$ gegen $a \in \mathbb{K}$ konvergent, so liefert die Definition ein (zu $\varepsilon = 1$ gehöriges) $n_0 \in \mathbb{N}$ mit $|a_n| \leq |a_n - a| + |a| < 1 + |a|$ für alle $n \in \mathbb{N}_{\geq n_0}$. Damit ist

$$\sup_{n\in\mathbb{N}} |a_n| \leq \max\{|a_1|, |a_2|, |a_3|, \ldots, |a_{n_0-1}|, 1+|a|\} < \infty\,. \qquad \square$$

(7) Als **Nullfolge** bezeichnet man eine Folge $(a_n)_{n\in\mathbb{N}}$ mit $\lim_{n\to\infty} a_n = 0$. Aus der Definition folgt, dass $(a_n)_{n\in\mathbb{N}}$ genau dann eine Nullfolge ist, wenn die Folge $(|a_n|)_{n\in\mathbb{N}}$ der Beträge eine Nullfolge ist. Außerdem gilt $\lim_{n\to\infty} a_n = a$ genau dann, wenn $(a_n - a)_{n\in\mathbb{N}}$ eine Nullfolge ist.

Beispiele (für **Grenzwerte von Folgen**).

(0) Konstante Folgen $(a)_{n\in\mathbb{N}}$ mit Wert a konvergieren auch gegen a, es gilt also $\lim_{n\to\infty} a = a$.

(1) Es gilt $\lim_{n\to\infty} \frac{1}{n} = 0$, die Folge $\left(\frac{1}{n}\right)_{n\in\mathbb{N}}$ ist also eine Nullfolge. Um dies einzusehen, wählt man zu $\varepsilon > 0$ einfach $n_0 := \left\lfloor \frac{1}{\varepsilon} \right\rfloor + 1 > \frac{1}{\varepsilon}$ und bemerkt $\left|\frac{1}{n}\right| = \frac{1}{n} \leq \frac{1}{n_0} < \varepsilon$ für alle $n \in \mathbb{N}_{\geq n_0}$.

Hiermit lassen sich auch andere einfach Limites schon berechnen, mit Bemerkung (7) folgt beispielsweise $\lim_{n\to\infty} \frac{2n-1}{n} = \lim_{n\to\infty} \left(2 - \frac{1}{n}\right) = 2$.

(2) Für jede Intervallschachtelung $([a_n, b_n])_{n\in\mathbb{N}}$ in $\mathbb{R}$ mit Kern $c \in \mathbb{R}$ existieren die Limites $\lim_{n\to\infty} a_n = c = \lim_{n\to\infty} b_n$.

(Begründung: Nach Definition der Intervallschachteleung in Abschnitt 4.1 existiert zu jedem $\varepsilon \in \mathbb{R}_{>0}$ ein $n_0 \in \mathbb{N}$ mit $b_{n_0} - a_{n_0} < \varepsilon$. Wegen $c \in [a_n, b_n] \subset [a_{n_0}, b_{n_0}]$ für $n \in \mathbb{N}_{\geq n_0}$ erhalten wir für alle $n \in \mathbb{N}_{\geq n_0}$ auch $|a_n - c| = c - a_n \leq c - a_{n_0} \leq b_{n_0} - a_{n_0} < \varepsilon$ und $|b_n - c| = b_n - c \leq b_{n_0} - c \leq b_{n_0} - a_{n_0} < \varepsilon$. Dies bedeutet per Definition $\lim_{n\to\infty} a_n = c$ und $\lim_{n\to\infty} b_n = c$.)

Für Folgen von *reellen* Zahlen kann das Konzept des Grenzwerts auf die sogenannten uneigentlichen Grenzwerte ∞ und $-\infty$ erweitert werden:

Definition (**uneigentliche Grenzwerte, uneigentliche Konvergenz**). *Sei $(a_n)_{n\in\mathbb{N}}$ eine Folge in $\mathbb{R}$. Gilt $\forall \varepsilon \in \mathbb{R}_{>0} \colon \exists n_0 \in \mathbb{N} \colon \forall n \in \mathbb{N}_{\geq n_0} \colon a_n > \frac{1}{\varepsilon}$, so bezeichnet man $(a_n)_{n\in\mathbb{N}}$ als **gegen ∞ konvergent** und notiert*

$$\lim_{n\to\infty} a_n = \infty \qquad \textit{oder gleichbedeutend} \qquad a_n \underset{n\to\infty}{\longrightarrow} \infty\,.$$

*Analog heißt $(a_n)_{n\in\mathbb{N}}$ **gegen $-\infty$ konvergent**, so $\forall \varepsilon \in \mathbb{R}_{>0} \colon \exists n_0 \in \mathbb{N} \colon \forall n \in \mathbb{N}_{\geq n_0} \colon a_n < -\frac{1}{\varepsilon}$ gilt, und man notiert*

$$\lim_{n\to\infty} a_n = -\infty \qquad \textit{oder gleichbedeutend} \qquad a_n \underset{n\to\infty}{\longrightarrow} -\infty\,.$$

*Man nennt $\pm\infty$ in diesem Zusammenhang **uneigentliche Grenzwerte** und bezeichnet die gegen $\pm\infty$ konvergierenden Folgen $(a_n)_{n\in\mathbb{N}}$ als **uneigentlich konvergent** oder gleichbedeutend als **bestimmt divergent**.*

Bemerkung. Folgen $(a_n)_{n\in\mathbb{N}}$ in $\mathbb{R}$ mit $\lim_{n\to\infty} a_n = \infty$ heißen **Unendlichfolgen**. Unendlichfolgen in $\mathbb{R}$ entsprechen durch Negation genau den Folgen in $\mathbb{R}$ mit Grenzwert $-\infty$, und Unendlichfolgen in $\mathbb{R}_{>0}$ entsprechen durch Reziprokenbildung genau den Nullfolgen in $\mathbb{R}_{>0}$.

Als Nächstes beschäftigen wir uns kurz mit dem Vergleich verschiedener Null- und Unendlichfolgen und werden danach sehen, dass dies auch für die Berechnung allgemeiner Grenzwerte durchaus nützen kann.

Definition (**Wachstumsvergleich, Geschwindigkeitsvergleich bei Folgen**). *Für zwei Unendlichfolgen $(a_n)_{n\in\mathbb{N}}$ und $(b_n)_{n\in\mathbb{N}}$ sagt man, dass $(b_n)_{n\in\mathbb{N}}$* ***schneller*** *als $(a_n)_{n\in\mathbb{N}}$* ***gegen*** $\boldsymbol{\infty}$ ***geht/strebt/wächst***, *wenn $\left(\frac{b_n}{a_n}\right)_{n\in\mathbb{N}}$ ebenfalls Unendlichfolge ist. Für Nullfolgen $(a_n)_{n\in\mathbb{N}}$ und $(b_n)_{n\in\mathbb{N}}$ mit $a_n \neq 0$ für (fast) alle $n \in \mathbb{N}$ sagt man, dass $(b_n)_{n\in\mathbb{N}}$* ***schneller*** *als $(a_n)_{n\in\mathbb{N}}$* ***gegen*** **0** ***geht/strebt***, *wenn $\left(\frac{b_n}{a_n}\right)_{n\in\mathbb{N}}$ ebenfalls Nullfolge ist.*

Beispiele (für den **Vergleich von Unendlich-/Nullfolgen**).

(1) **Wichtige Unendlichfolgen** mit reellen Parametern $0 < r < s$ und $1 < p < q$ sind

$$\log(\log n)\,,\quad (\log n)^r\,,\quad (\log n)^s\,,\quad n^r\,,\quad n^r \log n\,,\quad n^s\,,\quad p^n\,,\quad q^n\,,\quad n!\,,\quad n^n$$

(wobei wir den natürlichen Logarithmus log und Potenzen mit reellen Exponenten erst demnächst präzise einführen, diese aber im Vorgriff darauf schon erwähnen). Die Folgen wurden dabei **so geordnet**, dass **weiter rechts** stehende Folgen stets **schneller** gegen ∞ gehen als weiter links stehende Folgen.

(2) **Wichtige Nullfolgen** sind die Reziproken der genannten Unendlichfolgen, mit reellen Parametern $0 < r < s$ (*unverändert*) und $0 < q < p < 1$ (*beachte Änderung*!) sind

$$\frac{1}{\log(\log n)}\,,\quad \frac{1}{(\log n)^r}\,,\quad \frac{1}{(\log n)^s}\,,\quad \frac{1}{n^r}\,,\quad \frac{1}{n^r \log n}\,,\quad \frac{1}{n^s}\,,\quad p^n\,,\quad q^n\,,\quad \frac{1}{n!}\,,\quad \frac{1}{n^n}\,.$$

Auch hierbei streben die **weiter rechts** stehende Folgen **schneller** gegen Null als die weiter links stehenden Folgen.

Bemerkung. Das Wachstum zweier Unendlich- oder Nullfolgen kann auch unvergleichbar sein. Zum Beispiel bei den Unendlichfolgen $1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, \ldots$ und $1, 2^3, 3, 4^3, 5, 6^3, 7, 8^3, \ldots$ wächst weder die eine schneller als die andere noch die andere schneller als die eine.

Manches über (eventuell uneigentliche) Grenzwerte lässt sich mit Abschätzungen herausfinden. Grundprinzipien für solche Betrachtungen sind:

Satz (**Vergleichsprinzipien**).

(I) ***Majorantenkriterium*** *für Nullfolgen: Ist $(a_n)_{n\in\mathbb{N}}$ eine Folge in $\mathbb{R}$ oder $\mathbb{C}$ mit $|a_n| \leq Cb_n$ für (fast) alle $n \in \mathbb{N}$ mit einer Konstante $C \in \mathbb{R}_{\geq 0}$ und einer Nullfolge $(b_n)_{n\in\mathbb{N}}$ in $\mathbb{R}_{\geq 0}$, so ist $(a_n)_{n\in\mathbb{N}}$ selbst eine Nullfolge.*

(II) ***Minorantenkriterium*** *für Unendlichfolgen: Ist $(a_n)_{n\in\mathbb{N}}$ eine Folge in $\mathbb{R}$ mit $a_n \geq cb_n$ für (fast) alle $n \in \mathbb{N}$ mit einer Konstante $c \in \mathbb{R}_{>0}$ und einer Unendlichfolge $(b_n)_{n\in\mathbb{N}}$, so ist $(a_n)_{n\in\mathbb{N}}$ selbst eine Unendlichfolge.*

(III) *Sind $(a_n)_{n\in\mathbb{N}}$, $(b_n)_{n\in\mathbb{N}}$ Folgen in $\mathbb{R}$ mit $a_n \leq b_n$ für (fast) alle $n \in \mathbb{N}$ und existieren $\lim_{n\to\infty} a_n$ und $\lim_{n\to\infty} b_n$, so gilt $\lim_{n\to\infty} a_n \leq \lim_{n\to\infty} b_n$.*

(IV) ***Einschachtelungsprinzip***: *Ist eine Folge $(x_n)_{n\in\mathbb{N}}$ in $\mathbb{R}$ durch $a_n \leq x_n \leq b_n$ für (fast) alle $n \in \mathbb{N}$ zwischen Folgen $(a_n)_{n\in\mathbb{N}}$ und $(b_n)_{n\in\mathbb{N}}$ in $\mathbb{R}$ eingeschachtelt und existieren $\lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n =: c$ mit gleichem Wert c, so existiert auch $\lim_{n\to\infty} x_n = c$.*

Bemerkungen (zu den **Vergleichsprinzipien**).

(1) Die Kriterien (I) und (II) werden **oft für Produkte** $a_n = c_n b_n$ angewandt und besagen dann: Ist $(b_n)_{n\in\mathbb{N}}$ Nullfolge und $(c_n)_{n\in\mathbb{N}}$ zumindest beschränkt, so ist auch $(a_n)_{n\in\mathbb{N}}$ Nullfolge. Ist $(b_n)_{n\in\mathbb{N}}$ Unendlichfolge und $(c_n)_{n\in\mathbb{N}}$ zumindest positiv und von Null weg beschränkt (d.h. $\inf_{n\in\mathbb{N}} c_n > 0$), so ist auch $(a_n)_{n\in\mathbb{N}}$ Unendlichfolge.

(2) Das in Teil (III) des Satzes formulierte Prinzip der Erhaltung *schwacher* Ungleichungen bei Grenzübergängen überträgt sich übrigens nicht auf *strikte* Ungleichungen: Mit anderen Worten **folgt aus einer strikten Ungleichung $a_n < b_n$ für die Folgenglieder *keinesfalls* die strikte Ungleichung $\lim_{n\to\infty} a_n < \lim_{n\to\infty} b_n$ für die Limites**. Dies erkennt man an einfachen Beispielen wie $a_n = 0$ und $b_n = \frac{1}{n}$.

Beweis des Satzes. Alle vier Teile des Satzes lassen sich problemlos mit Grenzwertdefinition beweisen. Wir führen dies nur für die Teile (I) und (IV) exemplarisch aus:

Seien a_n, b_n wie in (I) mit $|a_n| \le C b_n$ für $n \gg 1$. Im Fall $C = 0$ folgt direkt $a_n = 0$ für $n \gg 1$, also $\lim_{n\to\infty} a_n = 0$. Im Fall $C > 0$ gibt für jedes $\varepsilon \in \mathbb{R}_{>0}$ die Definition von $\lim_{n\to\infty} b_n = 0$ (angewandt auf $\frac{\varepsilon}{C}$ statt ε), dass $b_n = |b_n| < \frac{\varepsilon}{C}$ für $n \gg 1$ gilt. Es folgt $|a_n| \le C b_n < C\frac{\varepsilon}{C} = \varepsilon$ für $n \gg 1$, also ist $\lim_{n\to\infty} a_n = 0$ anhand der Grenzwertdefinition gezeigt.

Seien a_n, b_n wie in (IV) mit $a_n \le x_n \le b_n$ für $n \gg 1$. Für jedes $\varepsilon \in \mathbb{R}_{>0}$ bedeutet die Existenz von $\lim_{n\to\infty} a_n = c$ und $\lim_{n\to\infty} b_n = c$, dass $|a_n - c| < \varepsilon$ und $|b_n - c| < \varepsilon$ für $n \gg 1$ gelten. Daraus folgt einerseits $x_n - c \le b_n - c \le |b_n - c| < \varepsilon$, andererseits $c - x_n \le c - a_n \le |a_n - c| < \varepsilon$ für $n \gg 1$, zusammengenommen also $|x_n - c| = \max\{x_n - c, c - x_n\} < \varepsilon$ für $n \gg 1$. Wir erhalten wie behauptet $\lim_{n\to\infty} x_n = c$. □

Berechnungen konkreter Grenzwerte gelingen manchmal mit dem Einschachtelungsprinzip (IV). *Viel* häufiger und schematischer werden aber die folgenden Rechenregeln eingesetzt.

Satz (**Rechenregeln der Grenzwertrechnung**). *Seien $(a_n)_{n\in\mathbb{N}}$ und $(b_n)_{n\in\mathbb{N}}$ Folgen in $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$, für die $a := \lim_{n\to\infty} a_n \in \mathbb{K}$ und $b := \lim_{n\to\infty} b_n \in \mathbb{K}$ existieren. Dann existieren auch*

$$\lim_{n\to\infty} (a_n + b_n) = a + b\,, \qquad \lim_{n\to\infty} (a_n - b_n) = a - b\,, \qquad \lim_{n\to\infty} (a_n b_n) = ab\,.$$

Ist $b \neq 0$, so folgt $b_n \neq 0$ für $n \gg 1$, und es existiert auch

$$\lim_{n\to\infty} \frac{a_n}{b_n} = \frac{a}{b}\,.$$

Beweis. Wir beweisen die Regeln für Summe und Differenz: Ist ein beliebiges $\varepsilon \in \mathbb{R}_{>0}$ gegeben, so erhalten wir erst $|a_n - a| < \frac{\varepsilon}{2}$ und $|b_n - b| < \frac{\varepsilon}{2}$ für $n \gg 1$. Mit der Dreiecksungleichung folgt

$$\big|(a_n \pm b_n) - (a \pm b)\big| = \big|(a_n - a) \pm (b_n - b)\big| \le |a_n - a| + |b_n - b| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon\,.$$

Die zeigt $\lim_{n\to\infty}(a_n \pm b_n) = a \pm b$.

Die Regeln für Produkt und Quotient werden in den Übungen behandelt. □

Bei Folgen *reeller* Zahlen gelten weitere Regeln, die sich erst in Abschnitt 5.2 nach Einführung allgemeiner Potenzen und Logarithmen herleiten lassen, die wir aber schon einmal festhalten:

Zusatz (weitere **Rechenregeln der Grenzwertrechnung**). *Seien $(b_n)_{n\in\mathbb{N}}$ und $(r_n)_{n\in\mathbb{N}}$ Folgen in $\mathbb{R}$, für die $b := \lim_{n\to\infty} b_n \in \mathbb{R}$ und $r := \lim_{n\to\infty} r_n \in \mathbb{R}$ existieren. Ist $b > 0$, so folgt $b_n > 0$ für $n \gg 1$, und es existiert*

$$\lim_{n\to\infty} (b_n)^{r_n} = b^r \,.$$

Weiterhin bleibt diese Regel auch für $b = 0 < r$ richtig, sofern $b_n \geq 0$ für $n \gg 1$ gilt. Gelten schließlich $1 \neq b > 0$ und $r > 0$, so folgen $1 \neq b_n > 0$ und $r_n > 0$ für $n \gg 1$, und es existiert

$$\lim_{n\to\infty} \log_{b_n} r_n = \log_b r \,.$$

Ganz entscheidend für die Berechnung konkreter Grenzwerte ist weiterhin auch der richtige Umgang mit Situationen, in denen diese Regeln nicht (ohne Weiteres) greifen:

Bemerkungen (zu **symbolischen Rechenregeln für Grenzwerte**).

(1) Auch für das Rechnen mit uneigentlichen Grenzwerten und manchen in $\mathbb{R}$ oder $\mathbb{C}$ nicht sinnvollen Ausdrücken gibt es Regeln. Man drückt diese manchmal durch **symbolische Regeln** wie

$$\frac{1}{\infty} = 0\,, \quad -3{+}\infty = \infty\,, \quad -\infty{-}\infty = -\infty\,, \quad \frac{1}{0+} = \infty\,, \quad \frac{1}{0-} = -\infty\,, \quad 2^\infty = \infty\,, \quad \infty^1 = \infty$$

aus, ohne dass man mit solchen Termen allerdings vollständig wie mit Zahlen rechnen darf. Tatsächlich soll die erste Regel nur besagen, dass aus $\lim_{n\to\infty} a_n = \infty$ stets $\lim_{n\to\infty} \frac{1}{a_n} = 0$ folgt, die zweite, dass sich aus $\lim_{n\to\infty} a_n = -3$ und $\lim_{n\to\infty} b_n = \infty$ stets $\lim_{n\to\infty}(a_n{+}b_n) = \infty$ ergibt. Ähnlich sind die anderen Regeln zu verstehen, wobei $0+$ und $0-$ als Platzhalter für Nullfolgen mit (fast) nur positiven und (fast) nur negativen Gliedern dienen.

(2) Es lässt sich aber keineswegs für alle auftretenden Situationen eine solche Regel aufstellen. Vielmehr gibt es auch **unbestimmte Ausdrücke** wie

$$\infty{-}\infty\,, \qquad \frac{\infty}{\infty}\,, \qquad \infty{\cdot}0{+}\,, \qquad \infty^{0+}\,, \qquad 1^\infty\,, \qquad 0^0\,.$$

Die Unbestimmtheit von $\infty{-}\infty$ bedeutet dabei, dass man aus $\lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n = \infty$ nichts über $\lim_{n\to\infty}(a_n{-}b_n)$ schließen kann, denn tatsächlich kann $\lim_{n\to\infty}(a_n{-}b_n)$ in dieser Situation jeden beliebigen Wert in $\mathbb{R}\cup\{-\infty,\infty\}$ annehmen oder auch gar nicht existieren. Ähnlich verhält sich dies bei den anderen unbestimmten Ausdrücken.

Zum Abschluss dieses Abschnitts geben wir Beispiele für die Berechnung von Grenzwerten:

Beispiele (für **konkrete Grenzwertberechnungen**).

(1) Beim Grenzwert $\lim_{n\to\infty} \frac{7n^3+4n-2}{-2n^3+n^2+1}$ lassen sich die Rechenregeln zunächst nicht anwenden (denn man käme auf den unbestimmten Typ $\frac{\infty}{\infty}$). Nach „Kürzen“ von n^3 geht dies aber doch, und man kann

$$\lim_{n\to\infty} \frac{7n^3+4n-2}{-2n^3+n^2+1} = \lim_{n\to\infty} \frac{7+\frac{4}{n^2}-\frac{2}{n^3}}{-2+\frac{1}{n}+\frac{1}{n^3}} = \frac{7+0-0}{-2+0+0} = -\frac{7}{2}$$

bestimmen. Auf ähnliche Weise lassen sich tatsächlich Grenzwerte beliebiger gebrochenrationaler Terme (also von Quotienten zweier Polynomen) bestimmen.

(2) Bei $\lim_{n\to\infty} \sqrt{n}(\sqrt{n+1}-\sqrt{n})$ führt schon der Teilausdruck $(\sqrt{n+1}-\sqrt{n})$ auf $\infty-\infty$, und, auch wenn man diesen als Nullfolge erkennt, kommt man immer noch auf $\infty\cdot 0+$. Nach geschicktem Erweitern mit $(\sqrt{n+1}+\sqrt{n})$ und Ausnutzung der dritten binomischen Formel erhält man jedoch

$$\begin{aligned}\lim_{n\to\infty} \sqrt{n}\big(\sqrt{n+1}-\sqrt{n}\big) &= \lim_{n\to\infty} \frac{\sqrt{n}\big(\sqrt{n+1}^2-\sqrt{n}^2\big)}{\sqrt{n+1}+\sqrt{n}} \\ &= \lim_{n\to\infty} \frac{\sqrt{n}}{\sqrt{n+1}+\sqrt{n}} = \lim_{n\to\infty} \frac{1}{\sqrt{1+\frac{1}{n}}+1} = \frac{1}{\sqrt{1+0}+1} = \frac{1}{2}\end{aligned}$$

(wobei sich die benötigte Grenzwertregel für Quadratwurzeln aus dem Zusatz mit $b_n = b = \frac{1}{2}$ oder auch elementarer ergibt).

(3) Bei $\lim_{n\to\infty} \sqrt[n]{n}$ führt die naheliegende Umformung $\sqrt[n]{n} = n^{\frac{1}{n}}$ auf den unbestimmten Typ ∞^{0+}. Formt man weiter um und nutzt aus, dass $(n)_{n\in\mathbb{N}}$ schneller wachsende Unendlichefolge ist als $(\log_2 n)_{n\in\mathbb{N}}$, so erhält man mit den Grenzwertregeln für Potenzen und Logarithmen aber tatsächlich

$$\lim_{n\to\infty} \sqrt[n]{n} = \lim_{n\to\infty} n^{\frac{1}{n}} = \lim_{n\to\infty} 2^{\frac{1}{n}\log_2 n} = 2^0 = 1\,.$$

(Sobald wir etwas später die Eulersche Zahl e und den natürlichen Logarithmus $\log = \log_{\mathrm{e}}$ eingeführt haben, machen wir derartige Rechnungen übrigens bevorzugt bezüglich der Basis e, schreiben also dann $\sqrt[n]{n} = \mathrm{e}^{\frac{1}{n}\log n}$ um.)

Für weitere Beispiele zur Grenzwertberechnung sei auf die Übungen verwiesen.

Als Nächstes beschäftigen wir uns mit zwei grundlegenden **Kriterien für Konvergenz**, dem Monotonie-Kriterium für Folgenkonvergenz in $\mathbb{R}$ und dem Cauchy-Kriterium für Folgenkonvergenz in $\mathbb{R}$ und $\mathbb{C}$. Wie in Abschnitt 4.1 bereits angedeutet **charakterisieren** diese Kriterien **die Vollständigkeit** von $\mathbb{R}$ (und $\mathbb{C}$).

Das Monotonie-Kriterium können wir nach Einführung geeigneter Begriffe wie folgt angeben:

Definition (**Monotonie von Folgen**)**.** *Eine Folge $(a_n)_{n\in\mathbb{N}}$ in $\mathbb{R}$ heißt **monoton wachsend**, wenn $a_{n+1} \geq a_n$ für alle $n \in \mathbb{N}$ gilt, und **streng monoton wachsend**, wenn sogar $a_{n+1} > a_n$ für alle $n \in \mathbb{N}$ gilt. Analog heißt die Folge **monoton fallend** beziehungsweise **streng monoton fallend**, wenn $a_{n+1} \leq a_n$ beziehungsweise $a_{n+1} < a_n$ für alle $n \in \mathbb{N}$ gilt.*

Satz (**Monotonie-Kriterium** für Folgenkonvergenz)**.** ***Jede beschränkte monotone Folge $(a_n)_{n\in\mathbb{N}}$ in $\mathbb{R}$ konvergiert in $\mathbb{R}$.** Falls $(a_n)_{n\in\mathbb{N}}$ monoton wächst, ist dabei der Grenzwert $\lim_{n\to\infty} a_n = \sup_{n\in\mathbb{N}} a_n$. Falls $(a_n)_{n\in\mathbb{N}}$ monoton fällt, ist er $\lim_{n\to\infty} a_n = \inf_{n\in\mathbb{N}} a_n$.*

Beweis. Wir behandeln ohne Einschränkung nur eine beschränkte wachsende Folge $(a_n)_{n\in\mathbb{N}}$ und bilden auf Grundlage der Ordnungs-Vollständigkeit $a := \sup_{n\in\mathbb{N}} a_n \in \mathbb{R}$. Sei nun $\varepsilon > 0$. Da $a-\varepsilon$ *keine* obere Schranke für $\{a_n \mid n \in \mathbb{N}\}$ ist, gibt es ein $n_0 \in \mathbb{N}$ mit $a-\varepsilon < a_{n_0}$. Mit der Monotonie und der Schranken-Eigenschaft von a erhalten wir für $n \geq n_0$ dann $a-\varepsilon < a_n \leq a$ und somit $|a_n-a| < \varepsilon$. Dies zeigt die Konvergenz $\lim_{n\to\infty} a_n = a$. □

Bemerkung (zum **Monotonie-Kriterium ohne Beschränktheit**)**.** Ähnlich begründet man: Unbeschränkte monotone Folgen in $\mathbb{R}$ konvergieren uneigentlich gegen ∞ (falls wachsend) oder $-\infty$ (falls fallend). Insgesamt kann man daher sagen: **Jede monotone Folge in $\mathbb{R}$ konvergiert eigentlich oder uneigentlich.**

Auch für das Cauchy-Kriterium brauchen wir zunächst noch einen Begriff:

Definition (**Cauchy-Folgen**). *Sei* $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$. *Eine Folge* $(a_n)_{n\in\mathbb{N}}$ *in* $\mathbb{K}$ *besitzt die* ***Cauchy-Eigenschaft****, wenn es zu jedem* $\varepsilon \in \mathbb{R}_{>0}$ *ein* $n_0 \in \mathbb{N}$ *mit* $|a_n - a_m| < \varepsilon$ *für alle* $m, n \in \mathbb{N}_{\geq n_0}$ *gibt. Man bezeichnet Folgen mit dieser Eigenschaft kurz als* ***Cauchy-Folgen****.*

Bemerkungen (zur **Cauchy-Eigenschaft**). Sei $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$.

(1) Die Gültigkeit der Cauchy-Eigenschaft wird manchmal durch eine Notation wie

$$\lim_{n\geq m\to\infty} |a_n - a_m| = 0 \qquad \text{oder} \qquad |a_n - a_m| \underset{n\geq m\to\infty}{\longrightarrow} 0$$

zum Ausdruck gebracht.

(2) In Quantoren-Schreibweise verlangt die Definition der Cauchy-Folge

$$\forall \varepsilon \in \mathbb{R}_{>0} \colon \exists n_0 \in \mathbb{N} \colon \forall m, n \in \mathbb{N}_{\geq n_0} \colon |a_n - a_m| < \varepsilon \,.$$

(3) Die Cauchy-Eigenschaft ist stärker als nur die Forderung $\lim_{n\to\infty}(a_{n+1} - a_n) = 0$, denn zum Beispiel die Folge $(\sqrt{n})_{n\in\mathbb{N}}$ erfüllt $\lim_{n\to\infty}(\sqrt{n+1} - \sqrt{n}) = 0$, ist aber *keine* Cauchy-Folge.

(4) **Jede in** $\mathbb{K}$ **konvergente Folge ist eine Cauchy-Folge.**

(Begründung: Sei $(a_n)_{n\in\mathbb{N}}$ in $\mathbb{K}$ gegen den Grenzwert a konvergent, und sei $\varepsilon > 0$. Dann gibt es nach Definition der Konvergenz ein $n_0 \in \mathbb{N}$ mit $|a_n - a| < \frac{\varepsilon}{2}$ für alle $n \in \mathbb{N}_{\geq n_0}$. Per Dreiecksungleichung folgt $|a_n - a_m| \leq |a_n - a| + |a_m - a| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$ für alle $m, n \in \mathbb{N}_{\geq n_0}$. Also ist $(a_n)_{n\in\mathbb{N}}$ Cauchy-Folge.)

(5) Cauchy-Folgen sind stets beschränkt.

(Begründung: Sei $(a_n)_{n\in\mathbb{N}}$ Cauchy-Folge in $\mathbb{K}$. Ähnlich wie beim entsprechenden Beweis für konvergente Folgen existiert dann ein (zu $\varepsilon = 1$ gehöriges) $n_0 \in \mathbb{N}$ mit $|a_n| \leq |a_n - a_{n_0}| + |a_{n_0}| < 1 + |a_{n_0}|$ für alle $n \in \mathbb{N}_{\geq n_0}$, und damit ist

$$\sup_{n\in\mathbb{N}} |a_n| \leq \max\{|a_1|, |a_2|, |a_3|, \ldots, |a_{n_0-1}|, 1 + |a_{n_0}|\} < \infty \,.$$

Das Cauchy-Kriterium besagt nun, dass tatsächlich auch die Umkehrung zu Bemerkung (4) gilt, dass also die Cauchy-Folgen in $\mathbb{K}$ genau die in $\mathbb{K}$ konvergenten Folgen sind:

Satz (**Cauchy-Kriterium** für Folgenkonvergenz). *Sei* $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$. ***Jede Cauchy-Folge in*** $\mathbb{K}$ ***konvergiert in*** $\mathbb{K}$***.***

Beweis. Wir betrachten zunächst im Fall $\mathbb{K} = \mathbb{R}$ eine Cauchy-Folge $(x_n)_{n\in\mathbb{N}}$ in $\mathbb{R}$. Für alle $k \in \mathbb{N}$ gilt dann

$$a_m := \inf_{n\in\mathbb{N}_{\geq m}} x_n \leq x_m \leq \sup_{n\in\mathbb{N}_{\geq m}} x_n =: b_m \,,$$

wobei $(a_m)_{m\in\mathbb{N}}$ wachsend und $(b_m)_{m\in\mathbb{N}}$ fallend ist, so dass $a := \lim_{m\to\infty} a_m$ und $b := \lim_{m\to\infty} b_m$ nach dem letzten Satz in $\mathbb{R}$ existieren. Für jedes $\varepsilon \in \mathbb{R}_{>0}$ gibt es wegen der Cauchy-Eigenschaft von $(x_n)_{n\in\mathbb{N}}$ ein $n_0 \in \mathbb{N}$, so dass zunächst $|x_n - x_m| < \varepsilon$ für alle $m, n \in \mathbb{N}_{\geq n_0}$ und dann auch $0 \leq b_m - a_m \leq \varepsilon$ für alle $m \in \mathbb{N}_{\geq n_0}$ gilt. Dies bedeutet für die Grenzwerte $b = a$, und nach dem Einschachtelungsprinzip konvergiert dann auch $(x_m)_{m\in\mathbb{N}}$ gegen $a = b$.

Der Fall $\mathbb{K} = \mathbb{C}$ lässt sich mit der einfachen Abschätzung

$$\max\{|\mathcal{Re}(z)|, |\mathcal{Im}(z)|\} \leq |z| \leq |\mathcal{Re}(z)| + |\mathcal{Im}(z)| \qquad \text{für alle } z \in \mathbb{C}$$

darauf zurückführen: Ist $(z_n)_{n\in\mathbb{N}}$ eine Cauchy-Folge in $\mathbb{C}$, so sind zunächst wegen der linken Ungleichung $(\mathcal{Re}(z_n))_{n\in\mathbb{N}}$ und $(\mathcal{Im}(z_n))_{n\in\mathbb{N}}$ Cauchy-Folgen in $\mathbb{R}$. Nach dem für den Fall $\mathbb{K}=\mathbb{R}$ Bewiesenen existieren dann $x := \lim_{n\to\infty} \mathcal{Re}(z_n) \in \mathbb{R}$ und $y := \lim_{n\to\infty} \mathcal{Im}(z_n) \in \mathbb{R}$, und mit der rechten Ungleichung folgt $\lim_{n\to\infty} z_n = x+\mathbf{i}y \in \mathbb{C}$. □

Bemerkung (zur **Konstruktion „Cauchy-Folgen modulo Nullfolgen“**). Auf Cauchy-Folgen basiert eine **elegante Konstruktion von $\mathbb{R}$ aus $\mathbb{Q}$**, die eine Alternative zu den am Ende von Abschnitt 4.1 erwähnten Dedekindschen Schnitten darstellt. Man führt $\mathbb{R}$ dabei als Faktorring des Rings der Cauchy-Folgen in $\mathbb{Q}$ modulo des Ideals der Nullfolgen in $\mathbb{Q}$ ein (oder, so dieses Konzept bekannt, direkt als Faktoralgebra). Dann identifiziert man $q \in \mathbb{Q}$ mit der Restklasse, die die konstante Folge $(q)_{n\in\mathbb{N}}$ enthält, und erhält so $\mathbb{Q} \subset \mathbb{R}$. Auch bei dieser Konstruktion sind etliche Details zu prüfen, auf die hier nicht eingegangen wird. Als wesentlicher Vorteil sei aber hervorgehoben, dass die Vorgehensweise auch in viel allgemeinerem Kontext, nämlich für sogenannte metrische Räume, einsetzbar ist.

Anwendung (**Konvergenz von Iterationsfolgen, Lösung von Fixpunktgleichungen**). Seien $\mathbb{K} \in \{\mathbb{R},\mathbb{C}\}$, $\mathcal{X} \subset \mathbb{K}$ und $f\colon \mathcal{X} \to \mathcal{X}$ eine Selbstabbildung von $\mathcal{X}$. Für jeden Startwert $x_0 \in \mathcal{X}$ definiert dann die Rekursionsvorschrift

$$x_{n+1} := f(x_n) \qquad \text{für } n \in \mathbb{N}_0$$

eine **Iterationsfolge** $(x_n)_{n\in\mathbb{N}_0}$ in $\mathcal{X}$. ***Falls*** Konvergenz von $(x_n)_{n\in\mathbb{N}_0}$ gegen einen Limes $x_* \in \mathcal{X}$ sichergestellt werden kann, so ergibt sich

$$f(x_*) = f\Big(\lim_{n\to\infty} x_n\Big) = \lim_{n\to\infty} f(x_n) = \lim_{n\to\infty} x_{n+1} = x_*$$

(wobei die zweite Gleichheit allgemein eine schwache Eigenschaft von f, bekannt als Stetigkeit, erfordert, in konkreten Fällen aber oft durch die Grenzwertrechenregeln gerechtfertigt ist). Damit löst x_* die **Fixpunktgleichung** $f(x) = x$ und ist ein sogenannter **Fixpunkt** von f.

Das Vorausgehende kann auf zwei Arten nützen: Kann man die Fixpunktgleichung für f leicht (explizit und vielleicht sogar eindeutig) lösen, so lassen sich auf diese Weise der Grenzwert oder mögliche Grenzwerte der Iterationsfolge $(x_n)_{n\in\mathbb{N}_0}$ bestimmen. Ist die Lösung der Fixpunktgleichung dagegen schwierig, so kann mit Hilfe der konvergenten Iterationsfolge eventuell die Existenz eines Fixpunkts beweisen und/oder Näherungswerte für diesen ausrechnen.

In jedem Fall muss man die oben angenommene **Konvergenz** von $(x_n)_{n\in\mathbb{N}_0}$ tatsächlich **sicherstellen** und kann hierfür oft die zuvor behandelten **Konvergenzkriterien einsetzen**: Für $\mathbb{K}=\mathbb{R}$, beschränktes $\mathcal{X}$ und monoton wachsendes f (im Sinn, dass $x \le y \implies f(x) \le f(y)$ für alle $x,y \in \mathcal{X}$ gilt) erweist sich $(x_n)_{n\in\mathbb{N}_0}$ als beschränkt und monoton, und man kann das Monotonie-Kriterium nutzen. Für abgeschlossenes $\mathcal{X}$ und eine strikte Kontraktion f — dies wird im Folgenden noch genauer erklärt — kann man die Cauchy-Eigenschaft für $(x_n)_{n\in\mathbb{N}_0}$ nachweisen und das Cauchy-Kriterium einsetzen.

Beispiele (für **Auftreten und Konvergenz von Iterationsfolgen**).

(1) Im Fall der monoton wachsenden Funktion $f\colon \mathbb{R}_{\ge -1} \to \mathbb{R}_{\ge -1}$ mit $f(x) := \sqrt{1+x}$ für $x \in \mathbb{R}_{\ge -1}$ konvergiert für jeden Startwert $x_0 \in \mathbb{R}_{\ge -1}$ die Iterationsfolge $(x_n)_{n\in\mathbb{N}_0}$ gegen den eindeutigen Fixpunkt $\frac{1+\sqrt{5}}{2}$ von f. Dies kann man als Präzisierung der unendlichen **Wurzelkette** $\cdots \sqrt{1+\sqrt{1+\sqrt{1+\sqrt{1+x_0}}}} = \frac{1+\sqrt{5}}{2}$ auffassen.

(2) Im Fall der strikten Kontraktion $f\colon \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ mit $f(x) := \frac{1}{2+x}$ für $x \in \mathbb{R}_{\geq 0}$ konvergiert für jeden Startwert $x_0 \in \mathbb{R}_{\geq 0}$ die Iterationsfolge $(x_n)_{n\in\mathbb{N}_0}$ gegen den einzigen Fixpunkt $\sqrt{2}{-}1$ von f. Die kann als Präzisierung des unendlichen **Kettenbruchs** $\cfrac{\ddots\ 1}{2+\cfrac{1}{2+\cfrac{1}{2+x_0}}} = \sqrt{2}{-}1$ verstanden werden.

Als Nächstes wenden wir uns kurz dem oben erwähnten Begriff der Kontraktion zu und zeigen, wie durch diesen die Cauchy-Eigenschaft der Iterationsfolge gesichert wird:

Definition (**(strikte) Kontraktionen**). *Eine Abbildung $f\colon \mathcal{X} \to \mathcal{Y}$ zwischen Teilmengen $\mathcal{X}$ und $\mathcal{Y}$ von $\mathbb{R}$ oder $\mathbb{C}$ heißt* ***Kontraktion****, wenn $|f(\widetilde{x}){-}f(x)| \leq |\widetilde{x}{-}x|$ für alle $x, \widetilde{x} \in \mathcal{X}$ gilt. Sie heißt* ***strikte Kontraktion****, wenn sogar $|f(\widetilde{x}){-}f(x)| \leq \kappa|\widetilde{x}{-}x|$ für alle $x, \widetilde{x} \in \mathcal{X}$ mit einer festen Konstante $\kappa \in [0,1)$ gilt.*

Bemerkung. Entscheidend für eine ***strikte*** **Kontraktion** ist, dass ***κ echt* kleiner als 1** ist.

Eine der wichtigsten Eigenschaften von Kontraktionen beschreibt der nächste Satz.

Satz (**Kontraktionssatz**). *Sei $\mathcal{X}$ nicht-leeres abgeschlossenes Intervall in $\mathbb{R}$ (d.h. vom Typ $[a,b]$, $[a,\infty)$ oder $(-\infty,b]$ mit $a \leq b$ in $\mathbb{R}$) oder $\mathcal{X} = \mathcal{X}_\mathrm{r}{+}\mathbf{i}\mathcal{X}_\mathrm{i} \subset \mathbb{C}$ mit nicht-leeren abgeschlossenen Intervallen $\mathcal{X}_\mathrm{r}, \mathcal{X}_\mathrm{i} \subset \mathbb{R}$. Dann* ***besitzt jede strikte Kontraktion $f\colon \mathcal{X} \to \mathcal{X}$ genau einen Fixpunkt*** *$x_* \in \mathcal{X}$, und für beliebiges $x_0 \in \mathcal{X}$ konvergiert die durch $x_{n+1} := f(x_n)$ für $n \in \mathbb{N}_0$ rekursiv definierte Iterationsfolge $(x_n)_{n\in\mathbb{N}_0}$ gegen x_*.*

Beweis. Es bezeichne $\kappa \in [0,1)$ die Kontraktionskonstante von f (wie in der Definition).

Die Eindeutigkeit des Fixpunkts sieht man schnell: Gäbe es zwei Fixpunkte $x, \widetilde{x} \in \mathcal{X}$ von f mit $\widetilde{x} \neq x$, so bekäme man mit $|\widetilde{x}{-}x| = |f(\widetilde{x}){-}f(x)| \leq \kappa|\widetilde{x}{-}x| < |\widetilde{x}{-}x|$ einen Widerspruch.

Im Hauptteil des Beweises zeigen wir nun die Existenz eines Fixpunkts und die Konvergenz der Iterationsfolge. Zunächst folgt aus der rekursiven Definition von $(x_n)_{n\in\mathbb{N}_0}$ und der Kontraktionseigenschaft

$$|x_{i+1}{-}x_i| = |f(x_i) - f(x_{i-1})| \leq \kappa|x_i{-}x_{i-1}| \qquad \text{für alle } i \in \mathbb{N}\,.$$

Mit Induktion erhalten wir daraus

$$|x_{i+1}{-}x_i| \leq \kappa^i|x_1{-}x_0| \qquad \text{für alle } i \in \mathbb{N}_0\,.$$

Für $n \geq m$ in $\mathbb{N}_0$ schreiben wir nun per Teleskopsumme $x_n{-}x_m = \sum_{i=m}^{n-1}(x_{i+1}{-}x_i)$ und rechnen mit der Dreiecksungleichung, der vorigen Abschätzung und der geometrischen Summenformel

$$|x_n{-}x_m| \leq \sum_{i=m}^{n-1}|x_{i+1}{-}x_i| \leq \sum_{i=m}^{n-1}\kappa^i|x_1{-}x_0| = \frac{\kappa^m{-}\kappa^n}{1{-}\kappa}|x_1{-}x_0| \leq \frac{\kappa^m}{1{-}\kappa}|x_1{-}x_0|\,.$$

Wegen $\kappa < 1$ wird die rechte Seite der Ungleichungskette für $n \geq m \gg 1$ kleiner als jedes vorgegebene $\varepsilon \in \mathbb{R}_{>0}$. Also hat $(x_n)_{n\in\mathbb{N}_0}$ die Cauchy-Eigenschaft, und gemäß dem Cauchy-Kriterium existiert $x_* := \lim_{n\to\infty} x_n$ in $\mathbb{R}$ bzw. $\mathbb{C}$. Da im Fall $\mathcal{X} \subset \mathbb{R}$ aus $a \leq x_n \leq b$ schon $a \leq x \leq b$ folgt (und im Fall $\mathcal{X} \subset \mathbb{C}$ Entsprechendes für Real- und Imaginärteile gilt), liegt auch x_* im *abgeschlossenen* Intervall/Bereich $\mathcal{X}$. Wegen $|f(x_n){-}f(x_*)| \leq \kappa|x_n{-}x_*|$ sichert das Majorantenkriterium, dass $(f(x_n){-}f(x_*))_{n\in\mathbb{N}}$ Nullfolge ist, und mit $f(x_*) = \lim_{n\to\infty} f(x_n) = \lim_{n\to\infty} x_{n+1} = x_*$ folgt, dass x_* ein Fixpunkt von f ist. Damit sind alle Behauptungen verifiziert. □

Bemerkung. In der Situation des Kontraktionssatzes lassen sich **Iterationsfolgen** $(x_n)_{n\in\mathbb{N}_0}$ mit beliebigen Startwert $x_0 \in \mathcal{X}$ **gut zur näherungsweisen Berechnung des Fixpunktes** x_* einsetzen. Ähnliche Rechnungen wie im Beweis geben dabei **Abschätzungen für den Näherungsfehler** $|x_n - x_*|$, der nach Berechnung von x_n mit $n \in \mathbb{N}$ verbleibt:

$$|x_n - x_*| \leq \frac{\kappa}{1-\kappa}|x_n - x_{n-1}| \leq \frac{\kappa^n}{1-\kappa}|f(x_0) - x_0|\,.$$

Bei der Abschätzung durch $\frac{\kappa^n}{1-\kappa}|f(x_0)-x_0|$ handelt es sich um eine A-priori-Fehlerabschätzung, bei der die Schranke bestimmt werden kann, bevor man mehrere x_n berechnet. Bei der schärferen Abschätzung durch $\frac{\kappa}{1-\kappa}|x_n-x_{n-1}|$ handelt es sich um eine A-posteriori-Fehlerabschätzung, die erst nach Berechnung der Folgenglieder bis hin zu x_{n-1} und x_n nützt.

5.2 Allgemeine Wurzeln, Potenzen und Logarithmen

In diesem Abschnitt werden wir den Grenzwertbegriff und die Vollständigkeit von $\mathbb{R}$ nutzen, um allgemeine Wurzeln, Potenzen und Logarithmen einzuführen. Wir beginnen mit Wurzeln.

Satz & Definition (**Wurzeln nichtnegativer reeller Zahlen**). *Zu $x \in \mathbb{R}_{\geq 0}$ und $k \in \mathbb{N}$ gibt es genau ein $b \in \mathbb{R}_{\geq 0}$ mit $b^k = x$. Diese Zahl b bezeichnet man als die **k-te Wurzel** aus x und notiert für sie $\sqrt[k]{x}$. Für $k = 2$ spricht man von Quadratwurzeln und setzt $\sqrt{x} := \sqrt[2]{x}$*

Beweis. Die Eindeutigkeit von b ist klar, weil für $a < b$ in $\mathbb{R}_{\geq 0}$ stets $a^k < b^k$ gilt.

Wir zeigen nun die Existenz von b mit Hilfe der Menge $A_x := \{a \in \mathbb{R}_{\geq 0} \,|\, a^k \leq x\}$. Diese ist nicht-leer und von oben beschränkt (denn es ist $0 \in A_x$ und wegen $a \leq a^k \leq x$ für $1 \leq a \in A_x$ ist $\max\{1, x\}$ eine obere Schranke für A_x). Gemäß der Ordnungs-Vollständigkeit existiert also $b := \sup A_x \in \mathbb{R}_{\geq 0}$. Einerseits ist nun $b + \frac{1}{n} \notin A_x$, also $\left(b+\frac{1}{n}\right)^k > x$ für alle $n \in \mathbb{N}$. Mit Produktregel[1] und Vergleichsprinzip für Grenzwerte folgt $b^k = \lim_{n\to\infty}(b+\frac{1}{n})^k \geq x$. Andererseits gibt es Zahlen $a_n \in A_x$ mit dementsprechend $a_n^k \leq x$ für $n \in \mathbb{N}$ und $\lim_{n\to\infty} a_n = b$. Erneut mit der Produktregel und Vergleichsprinzip folgt $b^k = \lim_{n\to\infty} a_n^k \leq x$. □

Bemerkung (zu **negativen Wurzeln**). Sei $x \in \mathbb{R}_{>0}$. Für *gerades* $k \in 2\mathbb{N}$ ist neben $\sqrt[k]{x}$ auch $-\sqrt[k]{x} \in \mathbb{R}_{\leq 0}$ eine k-te Wurzel aus x, erfüllt also auch $\left(-\sqrt[k]{x}\right)^k = x$. Für *ungerades* $k \in 2\mathbb{N}-1$ ist $-\sqrt[k]{x}$ eine k-te Wurzel aus der negativen Zahl $-x$, erfüllt also $\left(-\sqrt[k]{x}\right)^k = -x$. Wir erlauben in unserer Notation dennoch *keine negativen Zahlen unter dem Wurzelzeichen* (da für solche Wurzeln nicht alle üblichen Rechenregeln gelten und es beim Umgang damit leicht zu Fehlern und absurden Ergebnissen wie $-1 = \sqrt[3]{-1} = \sqrt[6]{(-1)^2} = \sqrt[6]{1} = 1$ kommen kann).

Rechenregeln für Wurzeln werden sich als Spezialfälle allgemeinerer Regeln für Potenzen ergeben und werden daher nicht separat behandelt. Zu Wurzeln aus komplexen Zahlen kommen wir in Abschnitt 5.3 noch einmal. Wir halten hier aber noch fest, dass wir mit Wurzeln auch grundlegende Beispiele irrationaler Zahlen erhalten:

Satz (über **Irrationalität von Wurzeln**). *Sei $k \in \mathbb{N}$. Ist $m \in \mathbb{N}$ **keine k-te Potenz** einer natürlichen Zahl, also $\sqrt[k]{m} \notin \mathbb{N}$, **dann** ist $\sqrt[k]{m}$ stets **irrational**, d.h. $\sqrt[k]{m} \notin \mathbb{Q}$. Speziell sind Quadratwurzeln aus Nicht-Quadrat-Zahlen wie $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, $\sqrt{6}$, $\sqrt{7}$, $\sqrt{8}$, $\sqrt{10}$ und Kubikwurzeln aus Nicht-Kubik-Zahlen wie $\sqrt[3]{2}$, $\sqrt[3]{3}$, $\sqrt[3]{4}$, $\sqrt[3]{5}$, $\sqrt[3]{6}$, $\sqrt[3]{7}$, $\sqrt[3]{9}$, $\sqrt[3]{10}$ stets irrational.*

[1] Entscheidend ist, dass an dieser Stelle, dass die Grenzwertregel $\lim_{n\to\infty} a_n^k = a^k$ für *natürliche* Exponenten $k \in \mathbb{N}$ und $a := \lim_{n\to\infty} a_n$ sich tatsächlich durch Induktion nach k aus der in den Übungen bewiesenen Produktregel ergibt. Man braucht an dieser Stelle also nicht etwa die in Abschnitt 5.1 im Vorgriff angegebene Regel für allgemeine Potenzen, die wir noch nicht sauber behandelt haben.

Beweis. Wir nutzen die Primfaktorzerlegung[2] $m = p_1^{\ell_1} p_2^{\ell_2} \cdot \ldots \cdot p_q^{\ell_q}$ von m (und gleich auch analog von anderen natürlichen Zahlen) mit eindeutigem $q \in \mathbb{N}_0$, eindeutigen Primfaktoren $p_i \in \mathbb{P}$ und eindeutigen Vielfachheiten $\ell_i \in \mathbb{N}$. Es gibt einen Primfaktor $p_{i_0} \in \mathbb{P}$ von m, dessen Vielfachheit ℓ_{i_0} nicht durch k teilbar ist (denn ansonsten wären die p_i alle k-te Potenzen und auch m selbst eine k-te Potenz). *Angenommen*, es ist $\sqrt[k]{m} \in \mathbb{Q}$, also $\sqrt[k]{m} = \frac{z}{n}$ mit $z, n \in \mathbb{N}$. Dann tritt p_{i_0} als Primfaktor von z^k und n^k entweder gar nicht oder mit einer durch k teilbaren Vielfachheit auf (denn die Primfaktoren von z^k und n^k sind genau die k-ten Potenzen derer von z und n). Bei mn^k hat der Primfaktor p_{i_0} aber eine um ℓ_{i_0} höhere Vielfachheit als bei n^k, die daher nicht durch k teilbar ist. Wegen $mn^k = z^k$ kommt der Primfaktor p_{i_0} aber bei mn^k und z^k mit der gleichen Vielfachheit vor. Dass diese einerseits durch k teilbar, andererseits nicht durch k teilbar ist, liefert uns einen *Widerspruch*. Folglich ist $\sqrt[k]{m} \notin \mathbb{Q}$. □

Potenzen b^z einer Basis $b \in \mathbb{R}_{\neq 0}$ mit ***ganzzahligen* Exponenten** $z \in \mathbb{Z}$ sind (wie früher schon allgemein in Gruppen und Ringen) durch die Festlegungen $b^0 := 1$, $b^n := \prod_{i=1}^{n} b$ (Produkt n gleicher Faktoren b) und $b^{-n} := (b^n)^{-1} = (b^{-1})^n$ für $n \in \mathbb{N}$ erklärt.

Potenzen b^q einer *positiven* Basis $b \in \mathbb{R}_{>0}$ mit ***rationalen* Exponenten** $q \in \mathbb{Q}$ erklären wir darauf aufbauend durch

$$b^{z/n} := \sqrt[n]{b^z} = \left(\sqrt[n]{b}\right)^z \qquad \text{für } z \in \mathbb{Z}\,,\ n \in \mathbb{N}\,,$$

wobei die Wohldefiniertheit dieser Bildung und die Gleichheit der letzten beiden Terme aus der Eindeutigkeit von Wurzeln folgen. Insbesondere können wir somit Wurzeln gemäß $\sqrt[k]{x} = x^{1/k}$ in Potenzen umschreiben.

Im Folgenden lassen wir sogar *reelle* Exponenten zu:

Satz & Definition (Potenzen mit *reellen* Exponenten). *Für jede* positive *Zahl $b \in \mathbb{R}_{>0}$ und jedes $r \in \mathbb{R}$ gibt es eine eindeutige positive Zahl $b^r \in \mathbb{R}_{>0}$, genannt die **Potenz der Basis b zum Exponent r**, so dass insgesamt für $a, b, b_n \in \mathbb{R}_{>0}$ und $r, r_n, s \in \mathbb{R}$ folgende Gesetzmäßigkeiten gelten*:

- ***Monotonie-Eigenschaften***[3]

$$r < s \implies a^r \lesseqgtr a^s \text{ falls } a \gtreqless 1\,,$$
$$a < b \implies a^r \lesseqgtr b^r \text{ falls } r \gtreqless 0\,,$$

[2] Tatsächlich wurde die Existenz der Primfaktorzerlegung in Abschnitt 2.2 mit Induktion gezeigt. Ein **Beweis für die Eindeutigkeit der Primfaktorzerlegung**, die wir hier auch benutzen, wurde bisher nicht gegeben, kann aber gemäß einer Idee von E. Zermelo so erfolgen: *Angenommen*, es gibt ein $n \in \mathbb{N}$ mit nicht eindeutiger Primfaktorzerlegung. Dann gibt es auch ein kleinstes solches $n \in \mathbb{N}$ mit $n = p_1 p_2 \cdot \ldots \cdot p_\ell = q_1 q_2 \cdot \ldots \cdot q_m$ für $\ell, m \in \mathbb{N}$ und Primzahlen $p_i, q_j \in \mathbb{P}$, wobei sich die q_j nicht durch Umnummerierung der p_i ergeben. Es folgt $p_i \neq q_j$ für alle $(i,j) \in \{1,2,\ldots,\ell\} \times \{1,2,\ldots,m\}$, denn sonst gäbe Division von n durch $p_i = q_j$ eine kleinere Zahl mit nicht eindeutiger Primfaktorzerlegung. Wir betrachten nun den Fall $p_1 < q_1$. Dann ist p_1 als Teiler von n und von $p_1 q_2 q_3 \cdot \ldots \cdot q_m$ auch Teiler von $\lambda := n - p_1 q_2 q_3 \cdot \ldots \cdot q_m = (q_1 - p_1) q_2 q_3 \cdot \ldots \cdot q_m \in \mathbb{N}$. Wir erhalten eine Primfaktorzerlegung von λ einerseits durch Primfaktorzerlegung von λ/p_1 und Multiplikation mit p_1, andererseits durch Primfaktorzerlegung von $q_1 - p_1$ und Multiplikation mit $q_2 q_3 \cdot \ldots \cdot q_m$. Da p_1 bei der ersteren Zerlegung vorkommt und die Primfaktorzerlegung von $\lambda < n$ eindeutig ist, muss bei p_1 auch bei der zweiten Zerlegung vorkommen. Da p_1 mit keiner der Primzahlen $q_2, q_3, \ldots, q_m$ übereinstimmt, erzwingt dies, dass p_1 in der zweiten Zerlegung aus der Primfaktorzerlegung von $q_1 - p_1$ stammt, also Teiler von $q_1 - p_1$ ist. Damit ist p_1 auch ein von 1 und q_1 verschiedener Teiler von q_1, was im *Widerspruch* zur Primzahleigenschaft von q_1 steht. Im Fall $p_1 > q_1$ ergibt sich dieser *Widerspruch* analog. Damit ist die Primfaktorzerlegung aller natürlichen Zahlen eindeutig.

[3] Die Formeln mit $\lesseqgtr$ und $\gtreqless$ sind so zu verstehen, dass die Ungleichung vor dem ‚falls' mit der oberen Relation $<$ gilt, wenn bei der Bedingung nach dem ‚falls' die obere Relation $>$ eintritt. Entsprechend gilt die Ungleichung mit der unteren Relation $>$, wenn bei der Bedingung die untere Relation $<$ eintritt.

- ***Rechenregeln***

$$b^0 = 1\,, \qquad b^1 = b\,, \qquad 1^r = 1\,,$$
$$b^{r+s} = b^r b^s\,, \qquad b^{rs} = (b^r)^s\,, \qquad (ab)^r = a^r b^r\,,$$

- ***Bernoulli-Ungleichungen***

$$(1{+}x)^r \geq 1{+}rx \qquad \textit{für } x \in \mathbb{R}_{>-1}\,,\ \textit{falls } r \in \mathbb{R} \setminus (0,1)\,,$$
$$(1{+}x)^r \leq 1{+}rx \qquad \textit{für } x \in \mathbb{R}_{>-1}\,,\ \textit{falls } r \in [0,1]$$

mit Gleichheit einzig für $x = 0$ oder $r \in \{0,1\}$,

- ***Grenzwertregeln***

$$\lim_{n\to\infty} b_n = b > 0\,,\ \lim_{n\to\infty} r_n = r \implies \lim_{n\to\infty} (b_n)^{r_n} = b^r\,,$$
$$\lim_{n\to\infty} b_n = 0\,,\ \lim_{n\to\infty} r_n = r > 0 \implies \lim_{n\to\infty} (b_n)^{r_n} = 0\,.$$

Ergänzend vereinbart man die Konvention $0^r := 0$ für $r > 0$ (mit der die letzte Grenzwertregel sogar dann Sinn macht und gültig bleibt, wenn unendlich viele b_n gleich 0 sind).

Zum Beweis. Als Vorüberlegung verifiziert man ohne besondere Probleme, dass die Monotonie-Eigenschaften erst für ganzzahlige Exponenten, dann für Stammbrüche $\frac{1}{n}$ als Exponenten (die n-ten Wurzeln entsprechen) und dann für rationale Exponenten gelten. Es folgt, dass die durch

$$b^r := \sup\{b^q \,|\, q \in \mathbb{Q}_{\leq r}\} \qquad \text{für } b \in [1,\infty)\,,$$
$$b^r := \inf\{b^q \,|\, q \in \mathbb{Q}_{\leq r}\} \qquad \text{für } b \in (0,1]\,.$$

definierten Potenzen mit reellen Exponenten $r \in \mathbb{R}$ die Potenzen mit rationalen Exponenten konsistent erweitern und auch selbst die Monotonie-Eigenschaften haben. Mit gleichem Vorgehen (erst ganzzahlige Exponenten, dann Wurzeln und rationale Exponenten, schließlich reelle Exponenten) erfolgen auch die Nachweise der Rechenregeln ohne besondere Kniffe.

Die Bernoulli-Ungleichung wurde für *natürliche Exponenten* $r \in \mathbb{N}$ auf Übungsblatt 3 behandelt. Um die Ungleichung für *reelle* Exponenten aus $[1,\infty)$ zu zeigen, betrachtet man für $y \in \mathbb{R}$ die Folge $(a_n(y))_{n\in\mathbb{N}_{-y}}$ mit Gliedern $a_n(y) := \left(1{+}\frac{y}{n}\right)^n$ (für $y > -1$ für alle $n \in \mathbb{N}$ definiert; sonst nur für $n \in \mathbb{N}$ mit $n > -y$). Man erhält aus der bereits bewiesenen Bernoulli-Ungleichung mit der Rechnung

$$\frac{a_{n+1}(y)}{a_n(y)} = \left(\frac{n{+}1{+}y}{n{+}1} \Big/ \frac{n{+}y}{n}\right)^{n+1} \frac{n{+}y}{n} = \left(1 - \frac{y}{(n{+}1)(n{+}y)}\right)^{n+1} \frac{n{+}y}{n} \geq \left(1 - \frac{y}{n{+}y}\right)\frac{n{+}y}{n} = 1\,,$$

dass $(a_n(y))_{n\in\mathbb{N}_{>-y}}$ für $y \in \mathbb{R}$ monoton wächst. Für $x \in \mathbb{R}_{>-1}$ und $m, n \in \mathbb{N}$ mit $n \geq m > -nx$ erhalten wir daraus

$$(1{+}x)^{\frac{n}{m}} = a_n(nx)^{\frac{1}{m}} \geq a_m(nx)^{\frac{1}{m}} = 1{+}\tfrac{n}{m}x\,,$$

wobei die resultierende Ungleichung sogar allgemein für $x \in \mathbb{R}_{>-1}$ und $m, n \in \mathbb{N}$ mit $n \geq m$ gilt (denn für $m \leq -nx$ ist die linke Seite positiv und die rechte Seite nichtpositiv). Damit gilt $(1{+}x)^q > 1{+}qx$ für $x \in \mathbb{R}_{>-1}$ und *rationale* $q = \frac{n}{m} \in \mathbb{Q} \cap [1,\infty)$. Für *reelle* $r \in [1,\infty)$ gibt Monotonie $(1{+}x)^r \geq (1{+}x)^q \geq 1{+}qx$ für $x \in [0,\infty)$, $q \in \mathbb{Q}\cap[1,r]$ sowie $(1{+}x)^r \geq (1{+}x)^q \geq 1{+}qx$

für $x \in (-1,0]$, $q \in \mathbb{Q} \cap [r,\infty)$, und insgesamt folgt durch Supremumbildung $(1{+}x)^r \geq 1{+}rx$ für alle $x \in \mathbb{R}_{>-1}$. Um für $x \in \mathbb{R}_{>-1}\backslash\{0\}$, $r \in (1,\infty)$ sogar die strikte Ungleichung nachzuweisen, führen wir $\xi := \sqrt{1{+}x}{-}1 \in \mathbb{R}_{>-1}\backslash\{0\}$ mit $1{+}x = (1{+}\xi)^2$ und $2\xi = x{-}\xi^2$ ein und erhalten $(1{+}x)^r = \big((1{+}\xi)^r\big)^2 \geq (1{+}r\xi)^2 = 1{+}r2\xi{+}r^2\xi^2 = 1{+}rx + (r{-}1)r\xi^2 > 1{+}rx$.

Für reelle Exponenten aus $(0,1]$ zeigen wir die Bernoulli-Ungleichung weitgehend analog. Aus der Monotonie von $(a_n(x))_{n\in\mathbb{N}_{>-x}}$ erhalten wir zunächst

$$(1{+}x)^{\frac{m}{n}} = a_m(mx)^{\frac{1}{n}} \leq a_n(mx)^{\frac{1}{n}} = 1{+}\tfrac{m}{n}x$$

für $x \in \mathbb{R}_{>-1}$ und $m,n \in \mathbb{N}$ mit $n \geq m$ (wobei $m > -mx$ trivial gilt). Daraus ergibt sich erst $(1{+}x)^q \leq 1{+}qx$ für $x \in \mathbb{R}_{>-1}$ und rationale $q = \frac{m}{n} \in \mathbb{Q} \cap (0,1]$ und dann $(1{+}x)^r \leq 1{+}rx$ für $x \in \mathbb{R}_{>-1}$ und reelle $r \in (0,1]$. Für $x \in \mathbb{R}_{>-1}\backslash\{0\}$ und $r \in (0,1)$ erhalten wir die schließlich die strikte Ungleichung durch neuerliche Rechnung mit $\xi := \sqrt{1{+}x}{-}1 \in \mathbb{R}_{>-1}\backslash\{0\}$.

Im Fall reeller Exponenten aus $(-\infty,0)$ gewinnen wir die Bernoulli-Ungleichung, direkt in der strikten Version, durch Zurückführung auf das Vorige: Für $x \in \mathbb{R}_{>-1}\backslash\{0\}$, $r \in [1,\infty)$ schätzen wir gemäß $(1{+}x)^{-r} = \big(\frac{1}{1+x}\big)^r = \big(1{-}\frac{x}{1+x}\big)^r \geq 1{-}r\frac{x}{1+x} > 1{-}r\frac{x+x^2}{1+x} = 1{-}rx$ ab und für $x \in \mathbb{R}_{>-1}\backslash\{0\}$, $r \in (0,1]$ gemäß $(1{+}x)^{-r} = \frac{1}{(1+x)^r} \geq \frac{1}{1+rx} > \frac{1-r^2x^2}{1+rx} = 1{-}rx$. Für $x = 0$ schließlich gilt die schwache Ungleichung „$\geq$“ natürlich sowieso.

Im letzten verbleibenden Fall $r = 0$ gilt die Bernoulli-Ungleichung trivial (beide Seiten 1).

Schließlich kommen wir zu den behaupteten Grenzwertregeln. Für beliebige $b_n \in \mathbb{R}_{>0}$ und $r_n \in \mathbb{R}$ erhalten wir aus der Bernoulli-Ungleichung die Abschätzungen

$$1{+}r_n(b_n{-}1) \leq (b_n)^{r_n} = \frac{1}{(1/b_n)^{r_n}} \leq \frac{1}{1{+}r_n(1/b_n{-}1)} \qquad \text{im Fall } r_n \in \mathbb{R}\backslash(0,1)$$

und dieselben Abschätzungen mit „$\geq$“ statt „$\leq$“ im Fall $r_n \in [0,1]$. Ist nun $\lim_{n\to\infty} b_n = b \in \mathbb{R}_{>0}$ und $\lim_{n\to\infty} r_n = r \in \mathbb{R}$ mit entweder $b = 1$ oder $r = 0$, so konvergieren gemäß den früher bewiesenen Grenzwertregeln für die Grundrechenarten die linken und rechten Seiten der Abschätzungen bei $n \to \infty$ gegen 1, und per Einschachtelungsprinzip erhalten wir $\lim_{n\to\infty}(b_n)^{r_n} = 1$. Im allgemeinen Fall mit beliebigen $b \in \mathbb{R}_{>0}$, $r \in \mathbb{R}$ beobachten wir zunächst $\lim_{n\to\infty}(b_n/b) = 1$, $\lim_{n\to\infty}(r_n{-}r) = 0$ nach Differenzen- und Quotientenregel und können dann mit Produktregel und vorausgehendem Spezialfall auf $\lim_{n\to\infty}(b_n)^{r_n} = \lim_{n\to\infty}\big[(b_n/b)^{r_n}b^{r_n-r}b^r\big] = 1{\cdot}1{\cdot}b^r = b^r$ schließen. Im Fall mit $b = 0$, $r \in \mathbb{R}_{>0}$ betrachten wir ein beliebiges $\varepsilon \in \mathbb{R}_{>0}$ und erhalten für $n \gg 1$ sowohl $0 \leq b_n < 1$ und $b_n < \varepsilon^{2/r}$ als auch $r_n > r/2$. Mit Monotonie schließen wir für $n \gg 1$ auf $0 \leq (b_n)^{r_n} < (b_n)^{r/2} < \big(\varepsilon^{2/r}\big)^{r/2} = \varepsilon$, erhalten also wie behauptet $\lim_{n\to\infty}(b_n)^{r_n} = 0$. □

Als Nächstes kommen wir zu einer weiteren zentralen Grundfunktion der Analysis, die eng mit Potenzen verbunden ist.

Satz & Definition (**natürliche Exponentialfunktion** und **Eulersche Zahl e**).

(I) *Für jedes $x \in \mathbb{R}$ bilden die Intervalle*

$$\left[\Big(1{+}\frac{x}{n}\Big)^n, \Big(1{-}\frac{x}{n}\Big)^{-n}\right] \qquad \textit{mit } n \in \mathbb{N}_{>|x|}$$

eine Intervallschachtelung in $\mathbb{R}_{>0}$. Der Kern dieser Intervallschachtelung bezeichnen wir mit $\exp(x) \in \mathbb{R}_{>0}$ und nennen die zugehörige Funktion $\exp\colon \mathbb{R} \to \mathbb{R}_{>0}$ die ***(natürliche) Exponentialfunktion****. Insbesondere hat die natürliche Exponentialfunktion* exp

die ***Grenzwertdarstellungen***

$$\exp(x) = \lim_{n\to\infty} \left(1+\frac{x}{n}\right)^n = \lim_{n\to\infty} \left(1-\frac{x}{n}\right)^{-n} \qquad \textit{für alle } x \in \mathbb{R}\,.$$

(II) *Die natürliche Exponentialfunktion* exp *ist auch durch die* ***Potenzen der Eulerschen Zahl*** $\mathrm{e} := \exp(1) \in \mathbb{R}_{>0}$ *gegeben, d.h. es gilt*

$$\boxed{\exp(x) = \mathrm{e}^x \qquad \textit{für alle } x \in \mathbb{R}}\,.$$

Man bezeichnet e *auch als die natürliche Basis der Exponentialfunktion.*

(III) *Für die natürliche Exponentialfunktion gelten die* ***fundamentalen Ungleichungen***

$$\mathrm{e}^x \geq 1+x \qquad \textit{für alle } x \in \mathbb{R} \qquad \textit{und} \qquad \mathrm{e}^x \leq \frac{1}{1-x} \qquad \textit{für alle } x \in \mathbb{R}_{<1}$$

mit Gleichheit in jeder der Ungleichungen einzig für $x = 0$.

Bemerkungen (zur **Eulerschen Zahl** und zur **natürlichen Exponentialfunktion**).

(1) Die **Eulersche Zahl e** ist **irrational**[4]. Ihre näherungsweise Berechnung ergibt

$$\mathrm{e} = 2,71828\ldots\,.$$

Tatsächlich ist e gemäß einem Satz von C. Hermite (1822–1901) aus dem Jahr 1873 sogar transzendent, das heißt, e ist nicht Nullstelle irgendeines Polynoms aus $\mathbb{Q}[\mathrm{X}]$.

(2) Als entscheidende Konsequenz von Teil (II) des Satzes gilt für die Exponentialfunktion exp das Exponentialgesetz

$$\exp(x+y) = \exp(x)\exp(y) \qquad \text{für alle } x, y \in \mathbb{R}\,.$$

Beweis des Satzes. Wir beginnen mit dem Beweis von Teil (I). Dazu fixieren wir $x \in \mathbb{R}$ und schreiben

$$a_n(x) := \left(1+\frac{x}{n}\right)^n \qquad \text{und} \qquad b_n(x) := \left(1-\frac{x}{n}\right)^{-n}$$

für die Randpunkte der betrachteten Intervalle. Im vorigen Beweis wurde bereits gezeigt, dass $(a_n(x))_{n\in\mathbb{N}_{>-x}}$ monoton wächst, und wegen $b_n(x) = \frac{1}{a_n(-x)}$ folgt, dass $(b_n(x))_{n\in\mathbb{N}_{>x}}$ monoton fällt. Zudem entnehmen wir für $n \in \mathbb{N}$ mit $n > |x|$ aus $\frac{a_n(x)}{b_n(x)} = \left(1+\frac{x}{n}\right)^n\left(1-\frac{x}{n}\right)^n = \left(1-\frac{x^2}{n^2}\right)^n \leq 1$, dass $a_n(x) \leq b_n(x)$ gilt. Somit sind die betrachteten Intervalle nicht-leer und liegen für $n > |x|$ gemäß $[a_n(x), b_n(x)] \supset [a_{n+1}(x), b_{n+1}(x)]$ ineinander. Damit tatsächlich eine Intervallschachtelung vorliegt, ist noch zu zeigen, dass die Intervalllänge $b_n(x)-a_n(x)$ für $n \to \infty$ gegen 0 strebt. Hierfür schätzen wir für $n \in \mathbb{N}$ mit $n > |x|$ erst $\frac{a_n(x)}{b_n(x)} = \left(1-\frac{x^2}{n^2}\right)^n \geq 1-\frac{x^2}{n}$ per Bernoulli-Ungleichung ab und erhalten mit $0 \leq b_n(x)-a_n(x) \leq \frac{x^2}{n} b_n(x) \leq \frac{x^2}{n} b_{n_0}(x) \underset{n\to\infty}{\longrightarrow} 0$ die benötigte

[4] Ein einfacher Beweis für die Irrationalität von e basiert auf der Fehlerabschätzung für Näherungssummen $0 < \mathrm{e} - \sum_{k=0}^n \frac{1}{k!} \leq \frac{\mathrm{e}-1}{(n+1)!} \leq \frac{1}{n!}$ für alle $n \in \mathbb{N}$, die wir in Abschnitt 5.6 noch allgemeiner kennenlernen werden. Könnte man nämlich e als Bruch mit Nenner $q \in \mathbb{N}$ darstellen, so ließe sich die positive Zahl $\mathrm{e} - \sum_{k=0}^n \frac{1}{k!}$ für jedes $n \in \mathbb{N}_{\geq q}$ als Bruch mit dem Hauptnenner $n!$ schreiben (den ja $q, 1!, 2!, 3!, \ldots, n!$ alle teilten). Damit wäre aber $\mathrm{e} - \sum_{k=0}^n \frac{1}{k!} \geq \frac{1}{n!}$ für jedes $n \in \mathbb{N}_{\geq q}$, was der Fehlerabschätzung widerspräche.

Konvergenz (wobei $n_0 \in \mathbb{N}_{>x}$ beliebig und die letzte Abschätzung durch $b_{n_0}(x)$ für $n \in \mathbb{N}_{\geq n_0}$ gültig ist). Die Grenzwertdarstellungen ergeben sich dann aus der in Abschnitt 5.1 beobachten Konvergenz der Randpunkte einer Intervallschachtelung.

Zum Beweis von Teil (II) rechnen wir für $x \in \mathbb{R}$ und $k \in \mathbb{N}$ zunächst mit den Grenzwertdarstellungen gemäß Teil (I) und den Grenzwertrechenregeln:

$$\exp(kx) = \lim_{n\to\infty} \left(1+\frac{kx}{n}\right)^n = \lim_{n\to\infty} \left(1+\frac{kx}{kn}\right)^{kn} = \lim_{n\to\infty} \left[\left(1+\frac{x}{n}\right)^n\right]^k = \exp(x)^k\,,$$

$$\exp(-x) = \lim_{n\to\infty} \left(1-\frac{x}{n}\right)^n = \lim_{n\to\infty} \left[\left(1-\frac{x}{n}\right)^{-n}\right]^{-1} = \exp(x)^{-1}\,.$$

Durch mehrfache Anwendung dieser Regeln erhalten wir

$$\exp(\pm\ell/m) = \exp(\ell/m)^{\pm 1} = \exp(1/m)^{\pm\ell} = \big(\exp(1/m)^m\big)^{\pm\ell/m} = \exp(1)^{\pm\ell/m} = \mathrm{e}^{\pm\ell/m}$$

für beliebige $\ell, m \in \mathbb{N}$, zusammen mit der trivialen Beobachtung $\exp(0) = 1$ also tatsächlich $\exp(q) = \mathrm{e}^q$ für alle $q \in \mathbb{Q}$. Um diese Gleichheit auf ein beliebiges $x \in \mathbb{R}$ zu übertragen, betrachten wir eine Folge $(q_k)_{k\in\mathbb{N}}$ in $\mathbb{Q}_{<x}$ mit $\lim_{n\to\infty} q_k = x$. Nun gilt $a_n(x) \geq a_n(q_k)$ für[5] $n \gg 1$ und im Limes $n \to \infty$ dann auch $\exp(x) \geq \exp(q_k)$. Insgesamt erhalten wir dann $\exp(x) \geq \lim_{k\to\infty} \exp(q_k) = \lim_{k\to\infty} \mathrm{e}^{q_k} = \mathrm{e}^x$ mit der Grenzwertregel für Potenzen. Eine analoge Approximation von x aus $\mathbb{Q}_{>x}$ gibt $\exp(x) \leq \mathrm{e}^x$. Damit ist $\exp(x) = \mathrm{e}^x$ gezeigt.

Zum Beweis von Teil (III) schätzen wir einerseits über die linken Randpunkte der Intervallschachtelung aus Teil (I) und die Bernoulli-Ungleichung

$$\mathrm{e}^x = \exp(x) \geq \left(1+\frac{x}{n}\right)^n > 1+x \qquad \text{für alle } x \in \mathbb{R}\backslash\{0\}$$

ab, wofür $n \in \mathbb{N}$ nur $n > \max\{-x, 1\}$ erfüllen muss. Indem wir dies mit $-x$ anstelle x anwenden, ergibt sich dann auch

$$\mathrm{e}^x = \frac{1}{\mathrm{e}^{-x}} < \frac{1}{1-x} \qquad \text{für alle } x \in \mathbb{R}_{<1}\backslash\{0\}\,.$$

Für $x = 0$ gelten die zugehörigen schwachen Ungleichungen trivialerweise. □

Korollar (Abschätzung für das Wachstum der Fakultäten). *Für alle $n \in \mathbb{N}$ gilt*

$$\mathrm{e}\left(\frac{n}{\mathrm{e}}\right)^n \leq n! \leq n\mathrm{e}\left(\frac{n}{\mathrm{e}}\right)^n.$$

Beweis. Wir argumentieren per Induktion nach $n \in \mathbb{N}$. Beim Induktionsanfang für $n = 1$ sind alle drei Terme gleich 1. Für den Schritt von $n \in \mathbb{N}$ zu $n+1$ nehmen wir $\mathrm{e}\left(\frac{n}{\mathrm{e}}\right)^n \leq n! \leq n\mathrm{e}\left(\frac{n}{\mathrm{e}}\right)^n$ an. Mit der Induktionsannahme und der Abschätzung $\mathrm{e} \geq (1+\frac{1}{n})^n = \left(\frac{n+1}{n}\right)^n$ von e durch einen linken Randpunkt der Intervallschachtelung im vorigen Satz erhalten wir dann

$$(n+1)! = (n+1)n! \geq (n+1)\mathrm{e}\left(\frac{n}{\mathrm{e}}\right)^n \geq (n+1)\left(\frac{n+1}{n}\right)^n \left(\frac{n}{\mathrm{e}}\right)^n = \mathrm{e}\left(\frac{n+1}{\mathrm{e}}\right)^{n+1}.$$

Analog ergibt sich mit Induktionsannahme und Abschätzung $\mathrm{e} \leq (1-\frac{1}{n+1})^{-(n+1)} = \left(\frac{n+1}{n}\right)^{n+1}$ durch einen rechten Randpunkt

$$(n+1)! = (n+1)n! \leq (n+1)n\mathrm{e}\left(\frac{n}{\mathrm{e}}\right)^n \leq (n+1)n\left(\frac{n+1}{n}\right)^{n+1}\left(\frac{n}{\mathrm{e}}\right)^n = (n+1)\mathrm{e}\left(\frac{n+1}{\mathrm{e}}\right)^{n+1}.$$

Mit den beiden erhaltenen Abschätzungen ist der Induktionsschritt komplett. □

[5] Tatsächlich reicht $n > -q_k$, womit die Basis in der Definition von $a_n(q_k)$ und $a_n(x)$ positiv ist.

In engem Zusammenhang mit Potenzen und Exponentialfunktionen steht folgendes Konzept:

Satz & Definition (**Logarithmen**). *Für jedes $b \in \mathbb{R}_{>0}\backslash\{1\}$ und jedes $x \in \mathbb{R}_{>0}$ gibt es genau eine Zahl $\log_b x \in \mathbb{R}$, genannt den* ***Logarithmus von x (zur Basis b)****, mit*

$$b^{\log_b x} = x\,.$$

Den Logarithmus zur Basis e *bezeichnet man als* ***natürlichen Logarithmus*** *und schreibt kurz* log *oder* ln *für* $\log_{\mathrm{e}}$. *Für $b, b_n \in \mathbb{R}_{>0}\backslash\{1\}$, $x, x_n, y \in \mathbb{R}_{>0}$ und $r \in \mathbb{R}$ gelten dann:*

- ***Monotonie-Eigenschaft***

$$x < y \implies \log_b x \lesseqgtr \log_b y \text{ falls } b \gtrless 1\,,$$

- ***Rechenregeln*** (*unter anderem*)

$$\log_b 1 = 0\,, \qquad \log_b(xy) = \log_b x + \log_b y\,,$$
$$\log_b(x^r) = r \log_b x\,, \qquad \log_b x = \frac{\log x}{\log b}\,, \qquad x^r = \mathrm{e}^{r \log x}\,,$$

- ***fundamentale Ungleichungen*** (*für den natürlichen Logarithmus*)

$$\frac{x}{1+x} \le \log(1+x) \le x \qquad \text{für alle } x \in \mathbb{R}_{>-1}$$

  mit Gleichheit in jeder der Ungleichungen einzig für $x = 0$,

- ***Grenzwertregel***

$$\lim_{n\to\infty} x_n = x\,,\ \lim_{n\to\infty} b_n = b \implies \lim_{n\to\infty} \log_{b_n} x_n = \log_b x\,.$$

Bemerkung (zu **Logarithmen**). Mit anderen Worten bedeutet die definierende Eigenschaft des Logarithmus, dass die **Logarithmusfunktion** $\log_b\colon \mathbb{R}_{>0} \to \mathbb{R}$ zur Basis b die **Umkehrfunktion der Exponentialfunktion** $\mathbb{R} \to \mathbb{R}_{>0}\,,\ r \mapsto b^r$ zur Basis b ist.

Beweis. Wir zeigen zuerst die Existenz von $\log_b x$ für $b \in (1,\infty)$, $x \in \mathbb{R}_{>0}$. Dazu benutzen wir, dass $R_x := \{r \in \mathbb{R} \,|\, b^r \le x\}$ wegen $\lim_{n\to\infty} b^{-n} = 0$, $\lim_{n\to\infty} b^n = \infty$ und $b^n \le b^r$ für $n \le r$ nicht-leer und von oben beschränkt ist. Somit können wir $\log_b x := \sup R_x \in \mathbb{R}$ wählen und dafür $b^{\log_b x} = x$ wie folgt nachweisen. Einerseits ist $\frac{1}{n} + \log_b x \notin R_x$, also $b^{\frac{1}{n}+\log_b x} > x$ und nach Grenzwertregeln und Vergleichsprinzip dann $b^{\log_b x} = \lim_{n\to\infty} b^{\frac{1}{n}+\log_b x} \ge x$. Andererseits ist $\log_b x = \lim_{n\to\infty} r_n$ für gewisse $r_n \in R_x$, für die $b^{r_n} \le x$ gilt. Es folgt $b^{\log_b x} = \lim_{n\to\infty} b^{r_n} \le x$. Insgesamt gilt wie behauptet $b^{\log_b x} = x$. Für $b \in (0,1)$, $x \in \mathbb{R}_{>0}$ ist R_x nicht-leer und von unten beschränkt, man kann $\log_b x := \inf R_x \in \mathbb{R}$ wählen und analog $b^{\log_b x} = x$ zeigen.

Die Monotonie-Eigenschaft, die Rechenregeln und die Grenzwertregel für den Logarithmus ergeben sich problemlos aus denen für Potenzen.

Die fundamentalen Ungleichungen für log geht man an, indem man die fundamentalen Ungleichungen der natürlichen Exponentialfunktion in folgender Form schreibt:

$$\mathrm{e}^{\frac{x}{1+x}} \le \frac{1}{1-\frac{x}{1+x}} = 1+x \le \mathrm{e}^x \qquad \text{für alle } x \in \mathbb{R}_{>-1}$$

(wobei dann ja $\frac{x}{1+x} \in \mathbb{R}_{<1}$ ist). Da alle Terme positiv sind, kann man log auf diese Ungleichungen anwenden und erhält in Anbetracht der Monotonie die letzten Behauptungen. □

Zum Abschluss dieses Abschnitts erwähnen wir kurz, dass mit allgemeinen Potenzen auch allgemeine Mittelwerte gebildet werden können:

Bemerkung (zu **Mittelwerten positiver Zahlen**). Für $n \in \mathbb{N}$, ein Tupel $x = (x_1, x_2 \ldots, x_n)$ positiver Zahlen $x_i \in \mathbb{R}_{>0}$ und ein Tupel $t = (t_1, t_2, \ldots, t_n)$ von Gewichten $t_i \in [0,1]$ mit $\sum_{i=1}^n t_i = 1$, im Basis-Fall gleicher Gewichtung einfach $t_1 = t_2 = \ldots = t_n = \frac{1}{n}$, erklärt man den (gewichteten) **Potenz-Mittelwert** von x_1, x_2, …, x_n zum Exponent $s \in \mathbb{R} \setminus \{0\}$ als

$$\mathrm{PM}_s(x\,;t) := \left(\sum_{i=1}^n t_i x_i^s\right)^{\frac{1}{s}} \in \mathbb{R}_{>0}\,.$$

Spezialfälle dieser Bildung sind das (gewichtete) **arithmetische Mittel** und das (gewichtete) **harmonische Mittel**

$$\mathrm{AM}(x\,;t) := \mathrm{PM}_1(x) = \sum_{i=1}^n t_i x_i \qquad \text{und} \qquad \mathrm{HM}(x\,;t) := \mathrm{PM}_{-1}(x) = \left(\sum_{i=1}^n t_i x_i^{-1}\right)^{-1}.$$

Als sinnvoller Ersatz für den Potenz-Mittelwert zum bisher ausgeschlossenen Exponenten $s = 0$ erweist sich das (gewichtete) **geometrische Mittel**

$$\mathrm{GM}(x) := \mathrm{PM}_0(x) := \prod_{i=1}^n (x_i)^{t_i} \in \mathbb{R}_{>0}\,.$$

Mit diesen Festlegungen gilt für $x \in (\mathbb{R}_{>0})^n$, $t \in [0,1]^n$ mit $\sum_{i=1}^n t_i = 1$ ganz allgemein die Ungleichung zwischen Potenzmittelwerten

$$\min\{x_1, x_2, \ldots, x_n\} \le \mathrm{PM}_r(x\,;t) \le \mathrm{PM}_s(x\,;t) \le \max\{x_1, x_2, \ldots, x_n\}\,, \qquad \text{falls } r \le s \text{ in } \mathbb{R}\,.$$

Zumindest für den grundlegenden Spezialfall der **AM-GM-Ungleichung**

$$\mathrm{GM}(x\,;t) \le \mathrm{AM}(x\,;t)$$

wird ein Beweis in den Übungen behandelt.

5.3 Kreiszahl und Kreisfunktionen

Motivation. Die **Kreiszahl** π gibt die ***halbe*** **Länge einer Kreislinie mit Radius 1** an, wobei man als Modellfall einer solchen Kreislinie meist die **Einheitskreislinie**

$$\mathrm{S}^1 := \{z \in \mathbb{C} \,|\, |z| = 1\}$$

in der Gaußschen Zahlenebene $\mathbb{C}$ heranzieht. Die anschauliche Vorstellung von π anhand der Kreislinie ist wichtig und entscheidend, muss für eine formale Definition aber dennoch präzisiert werden. Unter vielen Möglichkeiten zur präzisen Definition wählen wir hier eine geometrisch naheliegende und relativ elementare Variante:

Definition (der **Kreiszahl $\boldsymbol{\pi}$**). *Wir setzen*

$$\zeta_1 := -1 \in \mathrm{S}^1\,, \qquad \zeta_2 := \mathbf{i} \in \mathrm{S}^1 \qquad \textit{und rekursiv } \zeta_{n+1} := \frac{\zeta_n + 1}{|\zeta_n + 1|} \in \mathrm{S}^1 \textit{ für } n \in \mathbb{N}_{\ge 2}\,.$$

Die Kreiszahl π definieren wir dann als

$$\pi := \lim_{n\to\infty} 2^{n-1}|\zeta_n - 1| \in \mathbb{R}_{>0}$$

Die Verbindung zum Kreis und auch die Wohldefiniertheit erfordern hierbei aber weitere Erklärungen:

Bemerkungen und Erläuterungen (zur **Definition der Kreiszahl π**).

(1) Der **geometrischen Hintergrund** der Definition klärt sich mit folgenden Beobachtungen auf:

- Für alle $n \in \mathbb{N}$ gilt $(\zeta_{n+1})^2 = \zeta_n$, und **$\zeta_n$ ist eine primitive 2^n-te Einheitswurzel**. (Begründung: Für $n \in \mathbb{N}_{\geq 2}$ rechnet man mit Hilfe der komplexen Konjugation

$$(\zeta_{n+1})^2 = \frac{(\zeta_n+1)^2}{(\zeta_n+1)(\overline{\zeta_n+1})} = \frac{\zeta_n^2+2\zeta_n+1}{|\zeta_n|^2+\zeta_n+\overline{\zeta_n}+1} = \frac{\zeta_n^2+2\zeta_n+\zeta_n\overline{\zeta_n}}{1+\zeta_n+\overline{\zeta_n}+1} = \frac{\zeta_n(\zeta_n+2+\overline{\zeta_n})}{2+\zeta_n+\overline{\zeta_n}} = \zeta_n\,.$$

  Daneben ist $(\zeta_2)^2 = \zeta_1$ klar, und die Einheitswurzel-Eigenschaft folgt per Induktion.)
- Die 2^n Zahlen $1, \zeta_n, (\zeta_n)^2, (\zeta_n)^3, \ldots, (\zeta_n)^{2^n-1}$ sind die **Ecken eines in die Kreislinie S^1 einbeschriebenen regulären 2^n-Ecks** mit 2^n Seiten der gleichen Länge $|\zeta_n-1|$ und dementsprechend **mit halbem Umfang $2^{n-1}|\zeta_n-1|$**.
  (Begründung: Für alle $n \in \mathbb{N}$ und $k \in \{0, 1, 2, \ldots, 2^n-1\}$ gilt einerseits $|(\zeta_n)^k| = |\zeta_n|^k = 1$ und andererseits $|(\zeta_n)^{k+1}-(\zeta_n)^k| = |\zeta_n^k(\zeta-1)| = |(\zeta_n)^k|\,|\zeta_n-1| = |\zeta_n-1|$. Deshalb liegen die $(\zeta_n)^k$ auf S^1, und je zwei benachbarte (mit gleichem festem n) haben den festen Abstand $|\zeta_n-1|$.)
- Die halben Umfänge $2^{n-1}|\zeta_n-1|$ der einbeschriebenen 2^n-Ecke geben **für $n \gg 1$ Näherungen an die Länge der halben Kreislinie** (und übrigens sind diese Näherungen auch in dem Sinn gut, dass $2^{n-1}|\zeta_n-1|$ ziemlich schnell gegen π konvergiert).

(2) Die **Kreiszahl π** ist **irrational** und gemäß einem Satz von F. von Lindemann (1852–1939) aus dem Jahr 1882 sogar transzendent. Ihre näherungsweise Berechnung ergibt

$$\pi = 3,14159\ldots\,.$$

(3) Die **Existenz des Limes** in der Definition ist nicht selbstverständlich, und wir müssen diese tatsächlich noch **sicherstellen**:

Beweis für die Existenz der Limes in der Definition. Wir verifizieren, dass $(2^{n-1}|\zeta_n-1|)_{n\in\mathbb{N}}$ wachsende, beschränkte Folge ist, woraus die Existenz mit dem Monotonie-Kriterium folgt.

Um zunächst einzusehen, dass $(2^{n-1}|\zeta_n-1|)_{n\in\mathbb{N}}$ wachsend ist, schätzen wir mit der Dreiecksungleichung $|\zeta_n-1| \leq |\zeta_n-\zeta_{n+1}| + |\zeta_{n+1}-1| = |(\zeta_{n+1})^2-\zeta_{n+1}| + |\zeta_{n+1}-1| = 2|\zeta_{n+1}-1|$ ab und erhalten wie benötigt $2^{n-1}|\zeta_n-1| \leq 2^n|\zeta_{n+1}-1|$.

Für die Beschränktheit (und Nutzung in einem späteren Beweis) überlegen wir uns für $n \in \mathbb{N}_{\geq 2}$ und $k \in \{0, 1, 2, \ldots, 2^{n-2}\}$, dass $\mathcal{Re}((\zeta_n)^k) \in [0,1]$ fallend und $\mathcal{Im}((\zeta_n)^k) \in [0,1]$ wachsend von k abhängt. Wegen $|(\zeta_n)^k| = 1$ ist hierbei klar, dass die Real- und Imaginärteile ≤ 1 sind. Dass diese auch ≥ 0 sind, kann man durch Induktion nach $n \in \mathbb{N}_{\geq 2}$ zeigen: Dabei erhält man im Induktionsschritt $\mathcal{Re}(\zeta_{n+1}) \geq 0$ und $\mathcal{Im}(\zeta_{n+1}) \geq 0$ direkt aus der rekursiven Definition von ζ_{n+1}, beobachtet $(\zeta_{n+1})^k = (\zeta_n)^{k/2} \geq 0$ für gerade $k \in \{0, 2, 4, \ldots, 2^{n-1}\}$ und rechnet für ungerade $k \in \{1, 3, \ldots, 2^{n-1}-1\}$ die Behauptung mit $(\zeta_{n+1})^k = 2\,\mathcal{Re}(\zeta_{n+1})(\zeta_n^{(k+1)/2}+\zeta_n^{(k-1)/2}) \geq 0$ nach. Die Monotonie-Behauptungen erhält man dann mit dem Wissen $\mathcal{Re}((\zeta_n)^k)$, $\mathcal{Im}((\zeta_n)^k) \in [0,1]$ und $|(\zeta_n)^k| = 1$ aus den Definition der Multiplikation und des Betrags in $\mathbb{C}$. Genauer schätzt man für $n \in \mathbb{N}_{\geq 2}$, $k \in \{1, 2, \ldots, 2^{n-2}\}$ gemäß $\mathcal{Re}((\zeta_n)^k) = \mathcal{Re}(\zeta_n)\,\mathcal{Re}((\zeta_n)^{k-1}) - \mathcal{Im}(\zeta_n)\,\mathcal{Im}((\zeta_n)^{k-1}) \leq \mathcal{Re}(\zeta_n)\,\mathcal{Re}((\zeta_n)^{k-1}) \leq \mathcal{Re}((\zeta_n)^{k-1})$ ab und nutzt dann $\mathcal{Im}((\zeta_n)^k) = \sqrt{1-\mathcal{Re}((\zeta_n)^k)^2}$.

Zum eigentlichen Nachweis der Beschränktheit schätzen wir nun für $n \in \mathbb{N}_{\geq 2}$ folgendermaßen ab, wobei wir nacheinander die Gleichheit der Seitenlängen, die Ungleichung

$|z| \le |\mathcal{Re}(z)| + |\mathit{Im}(z)|$ für $z \in \mathbb{C}$, die gerade gezeigte Monotonie (ganz entscheidend!) und Teleskop-Summation samt den Identitäten $(\zeta_n)^0 = 1$, $(\zeta_n)^{2^{n-2}} = \zeta_2 = \mathbf{i}$ verwenden:

$$\begin{aligned}
2^{n-1}|\zeta_n - 1| &= 2\sum_{k=1}^{2^{n-2}} \big|(\zeta_n)^k - (\zeta_n)^{k-1}\big| \\
&\le 2\sum_{k=1}^{2^{n-2}} \big|\mathcal{Re}((\zeta_n)^k - (\zeta_n)^{k-1})\big| + 2\sum_{k=1}^{2^{n-2}} \big|\mathit{Im}((\zeta_n)^k - (\zeta_n)^{k-1})\big| \\
&= 2\sum_{k=1}^{2^{n-2}} \big(\mathcal{Re}((\zeta_n)^{k-1}) - \mathcal{Re}((\zeta_n)^k)\big) + 2\sum_{k=1}^{2^{n-2}} \big(\mathit{Im}((\zeta_n)^k) - \mathit{Im}((\zeta_n)^{k-1})\big) \\
&= 2\big(\mathcal{Re}(1) - \mathcal{Re}(\mathbf{i})\big) + 2\big(\mathit{Im}(\mathbf{i}) - \mathit{Im}(1)\big) = 4
\end{aligned}$$

Wir erhalten $2^{n-1}|\zeta_n - 1| \le 4$ für alle $n \in \mathbb{N}$, womit der Beweis komplett ist. □

Nach der Kreiszahl führen wir nun die Kreisfunktionen ein.

Motivation. Zunächst geht es uns um eine Abbildung[6]

$$\operatorname{cis}\colon \mathbb{R} \to \mathrm{S}^1$$

mit folgender **anschaulicher Bedeutung**: Jedes $\vartheta \in \mathbb{R}$ wird auf den Endpunkt $\operatorname{cis}\vartheta$ des vom Anfangspunkt 1 ausgehenden Kreisbogens in S^1 mit Länge $|\vartheta|$ abgebildet, wobei der Kreisbogen für $\vartheta \ge 0$ von 1 an gegen den Uhrzeigersinn aufgetragen, für $\vartheta \le 0$ im Uhrzeigersinn. Mit anderen Worten bildet der Ortsvektor von $\operatorname{cis}\vartheta \in \mathrm{S}^1$ mit der positiven x-Achse gerade den im Bogenmaß bemessenen Winkel $|\vartheta|$ (je nach Vorzeichen von ϑ gegen/im Uhrzeigersinn an die Achse angetragen). Für eine formale Definition gilt es diese Vorstellung aber wieder zu präzisieren, was wie bei der Kreiszahl π mit Hilfe der 2^n-ten Einheitswurzeln ζ_n erfolgen kann:

Definition (**Kreisfunktion cis**). *Es bezeichne ζ_n die primitive 2^n-te Einheitswurzel aus der vorausgehenden Definition der Kreiszahl π, und für $\vartheta \in \mathbb{R}$, $n \in \mathbb{N}$ sei $k_n(\vartheta) \in \mathbb{Z}$ die eindeutige ganze Zahl mit $\frac{2\pi k_n(\vartheta)}{2^n} \le \vartheta < \frac{2\pi(k_n(\vartheta)+1)}{2^n}$ (also $k_n(\vartheta) = \lfloor \frac{2^n\vartheta}{2\pi} \rfloor$). Dann definieren wir*

$$\operatorname{cis}\vartheta := \lim_{n\to\infty} (\zeta_n)^{k_n(\vartheta)} \in \mathrm{S}^1 .$$

Auch diese Definition bedarf der näheren Erläuterung:

Bemerkungen und Erläuterungen (zur **Definition des Kreisfunktion cis**).

(1) Insbesondere garantiert die Definition

$$\operatorname{cis}\frac{2\pi k}{2^m} = (\zeta_m)^k \qquad \text{für alle } k \in \mathbb{Z},\ m \in \mathbb{N},$$

denn es gilt $k_n(\frac{2\pi k}{2^m}) = 2^{n-m}k$ für $n \in \mathbb{N}_{\ge m}$, und somit ist $(\zeta_n)^{k_n(\frac{2\pi k}{2^m})} = (\zeta_n)^{2^{n-m}k} = (\zeta_m)^k$ für $n \in \mathbb{N}_{\ge m}$ konstant. Also **realisiert** die Definition von cis in diesen Fällen **die anschaulichen Bedeutung**, denn bei $(\zeta_m)^k$ handelt es sich um 2^m gleichmäßig auf der Kreislinie S^1 verteilte 2^m-te Einheitswurzeln, zwischen zwei benachbarten von diesen liegt ein Kreisbogen der Länge $\frac{2\pi}{2^m}$, und $(\zeta_m)^k$ liegt wie benötigt am Ende eines vom Anfangspunkt 1 ausgehenden Kreisbogens in S^1 der Länge $\frac{2\pi|k|}{2^m}$ (je nach Vorzeichen von k gegen/im Uhrzeigersinn).

[6] Dabei steht „cis“ für „Cosinus plus **i** Sinus“. Der Grund dieser Benennung wird demnächst klar.

(2) Die **Existenz des Limes** in der Definition müssen wir auch hier sicherstellen:

Beweis für die Existenz des Limes in der Definition. Wir beobachten zuerst, dass stets

$$k_{n+1}(\vartheta) \geq 2k_n(\vartheta)$$

gilt und tatsächlich $k_{n+1}(\vartheta)$ entweder gleich $2k_n(\vartheta)$ oder gleich $2k_n(\vartheta)+1$ ist. Dies folgt aus der Definition und der Zerlegung $\left[\frac{k_n(\vartheta)}{2^n}, \frac{k_n(\vartheta)+1}{2^n}\right) = \left[\frac{2k_n(\vartheta)}{2^{n+1}}, \frac{2k_n(\vartheta)+1}{2^{n+1}}\right) \dot\cup \left[\frac{2k_n(\vartheta)+1}{2^{n+1}}, \frac{2k_n(\vartheta)+2}{2^{n+1}}\right)$.

Im Fall $\vartheta \in \left[0, \frac{\pi}{2}\right]$ ist zudem $k_n(\vartheta) \in \{0, 1, 2, \ldots, 2^{n-2}\}$. Mit der bei der Definition von π gezeigten Monotonie von $\mathcal{Re}((\zeta_n)^k)$ und $\mathit{Im}((\zeta_n)^k)$ in k erhalten wir daher

$$\begin{aligned}\mathcal{Re}((\zeta_{n+1})^{k_{n+1}(\vartheta)}) &\leq \mathcal{Re}((\zeta_{n+1})^{2k_n(\vartheta)}) = \mathcal{Re}((\zeta_n)^{k_n(\vartheta)}),\\ \mathit{Im}((\zeta_{n+1})^{k_{n+1}(\vartheta)}) &\geq \mathit{Im}((\zeta_{n+1})^{2k_n(\vartheta)}) = \mathit{Im}((\zeta_n)^{k_n(\vartheta)}).\end{aligned}$$

Also verhalten sich die Real- und Imaginärteile von $(\zeta_n)^{k_n(\vartheta)}$ monoton und mit $|(\zeta_n)^{k_n(\vartheta)}| = 1$ auch beschränkt. Nach dem Monotonie-Kriterium konvergieren die Real- und Imaginärteile, womit dann auch $\lim_{n\to\infty}(\zeta_n)^{k_n(\vartheta)} \in \mathbb{C}$ existiert. Nach den Grenzwertregeln hat mit $(\zeta_n)^{k_n(\vartheta)}$ auch der Grenzwert Betrag 1, liegt also in S^1.

Der Fall $\vartheta \in \left[\frac{\pi}{2}, \pi\right]$ lässt sich darauf zurückführen, denn wir haben jetzt die Existenz von $\lim_{n\to\infty}(\zeta_n)^{k_n(\vartheta-\frac{\pi}{2})}$ mit $\vartheta-\frac{\pi}{2} \in \left[0, \frac{\pi}{2}\right]$ und können dann mittels $k_n(\vartheta) = k_n(\vartheta-\frac{\pi}{2})+2^{n-2}$ und $(\zeta_n)^{k_n(\vartheta)} = (\zeta_n)^{k_n(\vartheta-\frac{\pi}{2})}\mathbf{i}$ auf die Existenz von $\lim_{n\to\infty}(\zeta_n)^{k_n(\vartheta)}$ schließen können. Ähnlich lassen sich auch beliebige $\vartheta \in \mathbb{R}$ auf den behandelten Fall zurückführen. □

Tatsächlich erweist sich cis als surjektiv (auf die Einheitskreislinie), was durch den folgenden Satz verallgemeinert wird:

Satz (über die **Polardarstellung** komplexer Zahlen)**.** *Für jedes*[7] $z \in \mathbb{C}\backslash\{0\}$ *gibt es einen sogenannten* ***Polarwinkel*** $\vartheta \in \mathbb{R}$ *mit* $z = |z| \operatorname{cis}\vartheta$.

Beweis. Wir nehmen zunächst $z \in \mathrm{S}^1$, $\mathcal{Re}(z) \geq 0$, $\mathit{Im}(z) \geq 0$ an. Wegen der bei der Definition von π gezeigten fallenden Monotonie von $\mathcal{Re}((\zeta_n)^k)$ in $k \in \{0, 1, 2, \ldots, 2^{n-2}\}$ samt $\mathcal{Re}((\zeta_n)^0) = 1$, $\mathcal{Re}((\zeta_n)^{2^{n-2}}) = 0$ existiert für jedes $n \in \mathbb{N}_{\geq 2}$ ein eindeutiges $k_n \in \{0, 1, 2, \ldots, 2^{n-2}\}$ mit $\mathcal{Re}((\zeta_n)^{k_n}) \geq \mathcal{Re}(z) > \mathcal{Re}((\zeta_n)^{k_n+1})$. Wegen $|(\zeta_n)^{k_n+1}-(\zeta_n)^k| = |\zeta_n-1| \underset{n\to\infty}{\longrightarrow} 0$ (z.B. mit der früheren Abschätzung für $2^{n-1}|\zeta_n-1|$) bedeutet dies insbesondere $\lim_{n\to\infty}\mathcal{Re}((\zeta_n)^{k_n}) = \mathcal{Re}(z)$. Da die betrachteten Zahlen Betrag 1 und Imaginärteil ≥ 0 haben, folgt auch $\lim_{n\to\infty}(\zeta_n)^{k_n} = z$. Wegen $(\zeta_{n+1})^2 = \zeta_n$ lesen wir aus der Wahl von k_n außerdem ab, dass k_{n+1} gleich $2k_n$ oder gleich $2k_n+1$ ist, womit insbesondere $\left[\frac{k_{n+1}}{2^{n+1}}, \frac{k_{n+1}+1}{2^{n+1}}\right) \subset \left[\frac{k_n}{2^n}, \frac{k_n+1}{2^n}\right)$ gilt. Per Monotonie-Kriterium folgt die Existenz von $\vartheta := \lim_{n\to\infty}\frac{2\pi k_n}{2^n} \in \mathbb{R}$ mit $\frac{2\pi k_n}{2^n} \leq \vartheta \leq \frac{2\pi(k_n+1)}{2^n}$ für alle $n \in \mathbb{N}_{\geq 2}$. Hieraus erhalten wir $k_n(\vartheta) = k_n$ für alle $n \in \mathbb{N}_{\geq 2}$, sobald wir — eine kleine technische Feinheit — noch begründen, dass die rechte Ungleichung immer strikt ist. Dies könnte wegen der schon gezeigten Inklusion der Intervalle aber nur scheitern, wenn für $n \gg 1$ die rechten Randpunkte $\frac{2\pi(k_n+1)}{2^n}$ *alle* übereinstimmen, für $n \gg 1$ *stets* $k_{n+1} = 2k_n+1$ gilt und für $n \gg 1$ die Zahlen $(\zeta_n)^{k_n+1}$ *alle* übereinstimmen. Dann wäre aber schon $z = (\zeta_n)^{k_n+1}$ für $n \gg 1$, was im Widerspruch

[7] Formal betrachtet gilt der Satz mit $0 = |0| \operatorname{cis}\vartheta$ für jedes $\vartheta \in \mathbb{R}$ auch für $z = 0$. Wegen der völligen Beliebigkeit von ϑ spricht man dann aber nicht von Polardarstellung oder Polarwinkel und schließt diesen Fall oft aus.

zur strikten Ungleichung bei der Wahl von k_n stünde. Also ist tatsächlich $k_n(\vartheta) = k_n$ für alle $n \in \mathbb{N}_{\geq 2}$, und wir erhalten insgesamt

$$z = \lim_{n\to\infty} (\zeta_n)^{k_n} = \lim_{n\to\infty} (\zeta_n)^{k_n(\vartheta)} = \operatorname{cis}\vartheta\,.$$

Im Fall $z \in \mathrm{S}^1$, $\mathcal{Re}(z) \leq 0 \leq \mathit{Im}(z)$ können wir das Vorige auf $-\mathbf{i}z$ mit $|-\mathbf{i}z| = 1$, $\mathcal{Re}(-\mathbf{i}z) \geq 0$, $\mathit{Im}(-\mathbf{i}z) \geq 0$ anwenden. Aus $-\mathbf{i}z = \operatorname{cis}\vartheta$ für $\vartheta \in \mathbb{R}$ erhalten wir dann $z = \mathbf{i}\operatorname{cis}\vartheta = \operatorname{cis}(\frac{\pi}{2}+\vartheta)$. Ähnlich lassen sich die anderen Fälle mit $z \in \mathrm{S}^1$ behandeln.

Für allgemeines $z \in \mathbb{C}\setminus\{0\}$ schließlich wenden wir das Gezeigte auf $\frac{z}{|z|} \in \mathrm{S}^1$ und erhalten ein $\vartheta \in \mathbb{R}$ mit $\frac{z}{|z|} = \operatorname{cis}\vartheta$, also $z = |z|\operatorname{cis}\vartheta$. □

Als Nächstes führen wir weitere Kreisfunktionen ein und halten Grundeigenschaften fest.

Definition (der **Kreisfunktionen Kosinus** und **Sinus**)**.** *Die Kreisfunktionen* ***Kosinus*** *und* ***Sinus*** *sind definiert als*

$$\cos\colon \mathbb{R} \to [-1,1]\,,\ \vartheta \mapsto \mathcal{Re}(\operatorname{cis}\vartheta)\,, \qquad \sin\colon \mathbb{R} \to [-1,1]\,,\ \vartheta \mapsto \mathit{Im}(\operatorname{cis}\vartheta)$$

oder mit anderen Worten durch die Gleichung

$$\operatorname{cis}\vartheta = \cos\vartheta + \mathbf{i}\sin\vartheta \qquad \textit{für alle } \vartheta \in \mathbb{R}\,.$$

Bemerkung (zu **Kosinus** und **Sinus**)**.** Man kann die Definition von cos und sin am Einheitskreis S^1 veranschaulichen und dort auch folgende **elementargeometrische Interpretation an rechtwinkligen Dreiecken** ablesen: In einem Dreieck mit einem rechten Winkel und einem im Bogenmaß bemessenen Winkel $\vartheta \in (0, \frac{\pi}{2})$ gibt $\cos\vartheta$ das Längenverhältnis **„Ankathete durch Hypotenuse“** und $\sin\vartheta$ das Längenverhältnis **„Gegenkathete durch Hypotenuse“** an.

Eigenschaften (der **Kreisfunktionen cis, cos, sin**)**.**

(1) Für alle $\vartheta \in \mathbb{R}$ gelten per Definition

$$|\operatorname{cis}\vartheta| = 1 \qquad \text{und} \qquad \cos^2\vartheta + \sin^2\vartheta = 1$$

(wobei Abkürzungen wie $\cos^2\vartheta := (\cos\vartheta)^2$ und $\sin^2\vartheta := (\sin\vartheta)^2$ nun oft verwendet werden).

(2) **Spezielle Funktionswerte** sind $\operatorname{cis} 0 = 1$, $\operatorname{cis}\frac{\pi}{4} = \frac{1+\mathbf{i}}{\sqrt{2}}$, $\operatorname{cis}\frac{\pi}{2} = \mathbf{i}$, $\cos\frac{\pi}{2} = \sin 0 = \sin\pi = 0$, $\cos\frac{\pi}{6} = \sin\frac{\pi}{3} = \frac{1}{2}\sqrt{3}$, $\cos\frac{\pi}{4} = \sin\frac{\pi}{4} = \frac{1}{2}\sqrt{2}$ und $\cos\frac{\pi}{3} = \sin\frac{\pi}{6} = \frac{1}{2}$.

(3) Die Funktion cis ist **periodisch** mit **minimaler Periode 2π**, und für $\vartheta, \varphi \in \mathbb{R}$ gelten

$$\operatorname{cis}\vartheta = \operatorname{cis}\varphi \iff \vartheta - \varphi = 2k\pi \text{ für ein } k \in \mathbb{Z}\,,$$
$$\operatorname{cis}(\vartheta+2\pi) = \operatorname{cis}\vartheta\,, \qquad \operatorname{cis}(\vartheta+\pi) = -\operatorname{cis}\vartheta\,.$$

Insbesondere bedeutet dies, dass der **Polarwinkel** in der Polardarstellung in ganz $\mathbb{R}$ **(nur) bis auf Addition von Vielfachen von 2π eindeutig**, beispielsweise in $(-\pi, \pi]$ aber vollständig eindeutig ist. Hieraus folgt Eindeutigkeit der sogenannten **Argumentfunktion** $\operatorname{Arg}\colon \mathbb{C}\setminus\{0\} \to (-\pi,\pi]$ mit $|z|\operatorname{cis}(\operatorname{Arg} z) = z$ für alle $z \in \mathbb{C}\setminus\{0\}$.

Außerdem folgt aus den Eigenschaften von cis, dass auch cos und sin minimale Periode 2π haben und den Regeln $\cos(\vartheta+2\pi) = \cos\vartheta$, $\cos(\vartheta+\pi) = -\cos\vartheta$, $\sin(\vartheta+2\pi) = \sin\vartheta$, $\sin(\vartheta+\pi) = -\sin\vartheta$ sowie $\cos(\frac{\pi}{2}-\vartheta) = \sin\vartheta$, $\sin(\frac{\pi}{2}-\vartheta) = \cos\vartheta$ für $\vartheta \in \mathbb{R}$ genügen. (Von der gerade angegebenen Äquivalenz für cis überträgt sich auf cos und sin damit aber nur die Richtung ‚$\Longleftarrow$‘, während ‚$\Longrightarrow$‘ für cos oder sin kein direktes Analogon hat.)

(4) Für die Kreisfunktionen gelten die **Paritäts-Regeln**

$$\operatorname{cis}(-\vartheta) = \overline{\operatorname{cis}\vartheta} = \frac{1}{\operatorname{cis}\vartheta}\,, \qquad \cos(-\vartheta) = \cos\vartheta\,, \qquad \sin(-\vartheta) = -\sin\vartheta \qquad \text{für } \vartheta \in \mathbb{R}\,.$$

Damit ist **cos eine gerade Funktion** und **sin eine ungerade Funktion**.

(5) Die **Additionstheoreme** für die Kreisfunktionen besagen

$$\begin{aligned} \operatorname{cis}(\vartheta{+}\varphi) &= (\operatorname{cis}\vartheta)(\operatorname{cis}\varphi)\,, \\ \cos(\vartheta{\pm}\varphi) &= (\cos\vartheta)(\cos\varphi) \mp (\sin\vartheta)(\sin\varphi)\,, \\ \sin(\vartheta{\pm}\varphi) &= (\sin\vartheta)(\cos\varphi) \pm (\cos\vartheta)(\sin\varphi) \end{aligned}$$

für alle $\vartheta, \varphi \in \mathbb{R}$. Iterative Anwendung des Additionstheorems für cis gibt die **Formel von De Moivre** für Winkel-Vervielfachung

$$\operatorname{cis}(k\vartheta) = (\operatorname{cis}\vartheta)^k = (\cos\vartheta{+}\mathbf{i}\sin\vartheta)^k$$

für $\vartheta \in \mathbb{R}$, $k \in \mathbb{Z}$. Durch Ausmultiplizieren der rechten Seite mit dem Binomialsatz und Bildung des Realteils erhält man die Vervielfachungs-Formel für den Kosinus

$$\cos(k\vartheta) = \sum_{j=0}^{\lfloor k/2 \rfloor} (-1)^j \binom{k}{2j} (\sin\vartheta)^{2j} (\cos\vartheta)^{k-2j}$$

für $\vartheta \in \mathbb{R}$, $k \in \mathbb{Z}$. Analog führt Bildung des Imaginärteils zu einer Formel für den Sinus.

(6) **Fundamentale Ungleichungen** für die Kreisfunktion cis sind

$$\begin{aligned} |\operatorname{cis}\vartheta - \operatorname{cis}\varphi| &\le |\vartheta{-}\varphi| && \text{für } \vartheta, \varphi \in \mathbb{R}\,, \\ |\operatorname{cis}\vartheta - \operatorname{cis}\varphi| \ge |\vartheta{-}\varphi| \frac{|\operatorname{cis}\vartheta + \operatorname{cis}\varphi|}{2} &= |\vartheta{-}\varphi| \sqrt{1 - \tfrac{1}{4}|\operatorname{cis}\vartheta - \operatorname{cis}\varphi|^2} && \text{für } \vartheta, \varphi \in \mathbb{R}\,,\ |\vartheta{-}\varphi| \le \pi \end{aligned}$$

mit Gleichheit jeweils nur für $\vartheta = \varphi$. Für den Sinus ergeben sich daraus

$$\begin{aligned} |\sin\vartheta - \sin\varphi| &\le |\vartheta{-}\varphi| && \text{für } \vartheta, \varphi \in \mathbb{R}\,, \\ \sin\vartheta &\le \vartheta && \text{für } \vartheta \in \mathbb{R}_{\ge 0}\,, \\ \sin\vartheta &\ge \vartheta\cos\vartheta && \text{für } \vartheta \in [0, \pi] \end{aligned}$$

mit Gleichheit jeweils nur für $\vartheta = \varphi$ bzw. für $\vartheta = 0$. Für den Kosinus folgt

$$\begin{aligned} |\cos\vartheta - \cos\varphi| &\le |\vartheta{-}\varphi| && \text{für } \vartheta, \varphi \in \mathbb{R}\,, \\ \cos\vartheta &\le \frac{1}{\sqrt{1{+}\vartheta^2}} && \text{für } \vartheta \in \left[-\tfrac{3\pi}{2}, \tfrac{3\pi}{2}\right]\,, \\ \cos\vartheta &\ge \sqrt{1{-}\vartheta^2} && \text{für } \vartheta \in [-1, 1] \end{aligned}$$

mit Gleichheit jeweils nur für $\vartheta = \varphi$ bzw. für $\vartheta = 0$.

Beweise der Eigenschaften (1)–(5) *von* cis, cos, sin. Wir beschränken uns größtenteils auf Nachweise der Eigenschaften von cis, da die Eigenschaften von cos und sin oft durch Real- und Imaginärteil-Bildung folgen.

Zunächst ist (1) nach der Definition von cis als S^1-wertige Abbildung klar.

Die speziellen Werte in (2) an den Stellen 0, $\frac{\pi}{4}$, $\frac{\pi}{2}$, π und zudem $\operatorname{cis}(2\pi) = 1$ ergeben sich aus Bemerkung (1) direkt nach der Definition von cis. Zudem erhalten wir $\cos\vartheta, \sin\vartheta \in (0,1)$ für alle $\vartheta \in (0, \frac{\pi}{2})$ aus der früher schon gezeigten Monotonie der Real- und Imaginärteile von $(\zeta_n)^k$ in $k \in \{0, 1, 2, \dots, 2^{n-2}\}$.

Das Additionstheorem für cis in (5) ist die Grundlage der weiteren Eigenschaften und lässt sich wie folgt zeigen: Nach Addition der Ungleichungen für $k_n(\vartheta)$, $k_n(\varphi)$ lesen wir aus $\frac{2\pi(k_n(\vartheta)+k_n(\varphi)}{2^n} \leq \vartheta+\varphi < \frac{2\pi(k_n(\vartheta)+k_n(\varphi)+2)}{2^n}$ ab, dass $k_n(\vartheta+\varphi)$ gleich $k_n(\vartheta)+k_n(\varphi)$ oder gleich $k_n(\vartheta)+k_n(\varphi)+1$ ist. Wegen $\lim_{n\to\infty}\zeta_n = 1$ erhalten wir daraus $\lim_{n\to\infty}(\zeta_n)^{k_n(\vartheta+\varphi)} = \lim_{n\to\infty}(\zeta_n)^{k_n(\vartheta)+k_n(\varphi)} = \lim_{n\to\infty}(\zeta_n)^{k_n(\vartheta)}(\zeta_n)^{k_n(\varphi)}$, und insgesamt folgt $\operatorname{cis}(\vartheta+\varphi) = (\operatorname{cis}\vartheta)(\operatorname{cis}\varphi)$.

Die Werte an den Stellen $\frac{\pi}{3}$ und $\frac{\pi}{6}$ in (2) ergeben sich durch Lösen quadratischer Gleichungen. Zum Beispiel kann man für $\cos\frac{\pi}{6} \in (0,1)$ von $0 = \cos\frac{\pi}{2} = (\cos^2\frac{\pi}{6} - 3\sin^2\frac{\pi}{6})\cos\frac{\pi}{6}$ gemäß (5) und $\cos^2\frac{\pi}{6} + \sin^2\frac{\pi}{6} = 1$ gemäß (1) ausgehen.

Zum Nachweis von (4) bemerken wir $(\operatorname{cis}\vartheta)(\operatorname{cis}(-\vartheta)) = \operatorname{cis}(t-t) = \operatorname{cis}0 = 1$ gemäß (5) und damit $\operatorname{cis}(-\vartheta) = \frac{1}{\operatorname{cis}\vartheta}$. Wegen (1) ist zudem $\frac{1}{\operatorname{cis}\vartheta} = \overline{\operatorname{cis}\vartheta}$.

Für die 2π-Periodizität in (3) reicht in Anbetracht von (4) und (5) der Nachweis von $\operatorname{cis}\vartheta = 1 \iff \vartheta \in 2\mathbb{Z}\pi$ für $\vartheta \in \mathbb{R}$. Bei letzterer Äquivalenz ist „$\Longleftarrow$“ mit $\operatorname{cis}(2\pi) = 1$ und (5) klar, und für „$\Longrightarrow$“ brauchen wir nur noch $\operatorname{cis}\vartheta \neq 1$ für $\vartheta \in (0, 2\pi)$ nachzuweisen. Dabei kennen wir die Werte $\operatorname{cis}\frac{\pi}{2} = \mathbf{i}$, $\operatorname{cis}\pi = -1$ und $\operatorname{cis}\frac{3\pi}{2} = -\mathbf{i}$ bereits. Zudem hat $\operatorname{cis}\vartheta$ für $\vartheta \in (0, \frac{\pi}{2})$ Real- und Imaginärteil $\neq 0$, und mit (5) folgt, dass auch $\operatorname{cis}(\vartheta+\frac{\pi}{2}) = \mathbf{i}\operatorname{cis}\vartheta$, $\operatorname{cis}(\vartheta+\pi) = -\operatorname{cis}\vartheta$ und $\operatorname{cis}(\vartheta+\frac{3\pi}{2}) = -\mathbf{i}\operatorname{cis}\vartheta$ mit $\vartheta \in (0, \frac{\pi}{2})$ alle Real- und Imaginärteil $\neq 0$ haben. Somit sind all diese Werte wie benötigt $\neq 1$. □

Etwas aufwändiger gestalten sich die Nachweise der Ungleichungen in (6).

Beweis der Ungleichung $|\operatorname{cis}\vartheta - \operatorname{cis}\varphi| \leq |\vartheta-\varphi|$. Wir zeigen $|\operatorname{cis}\vartheta - 1| \leq |\vartheta|$ für $\vartheta \in \mathbb{R}_{\geq 0}$. Ist dies erledigt, so folgt mit (4), (5) dasselbe für $\vartheta \in \mathbb{R}_{<0}$ und allgemein $|\operatorname{cis}\vartheta - \operatorname{cis}\varphi| = \left|\frac{\operatorname{cis}\vartheta}{\operatorname{cis}\varphi} - 1\right| |\operatorname{cis}\varphi| = |\operatorname{cis}(\vartheta-\varphi) - 1| \leq |\vartheta-\varphi|$. Zum Beweis von $|\operatorname{cis}\vartheta - 1| \leq \vartheta$ für $\vartheta \geq 0$ kombinieren wir die (ähnlich schon früher benutzte) Abschätzung $|(\zeta_n)^k - 1| \leq \sum_{j=1}^{k} |(\zeta_n)^j - (\zeta_n)^{j-1}| = k|\zeta_n - 1|$ für $k \in \mathbb{N}_0$ und die von der Definition von π herrührende Ungleichung $2^n|\zeta_n - 1| \leq 2\pi$ zu

$$|(\zeta_n)^{k_n(\vartheta)} - 1| \leq k_n(\vartheta)|\zeta_n - 1| \leq \frac{2\pi k_n(\vartheta)}{2^n}$$

für alle $n \in \mathbb{N}$. Wir machen bei dieser Ungleichung den Grenzübergang $n \to \infty$ und erhalten wegen $\lim_{n\to\infty}(\zeta_n)^{k_n(\vartheta)} = \operatorname{cis}\vartheta$ und $\lim_{n\to\infty}\frac{2\pi k_n(\vartheta)}{2^n} = \vartheta$ die Behauptung $|\operatorname{cis}\vartheta - 1| \leq \vartheta$ für $\vartheta \in \mathbb{R}_{\geq 0}$.

Die Gleichheitsdiskussion lässt sich nun wie folgt erledigen. Im Fall $0 < |\vartheta-\varphi| < \pi$ erhalten wir mit $|\operatorname{cis}\vartheta - \operatorname{cis}\varphi| = |\operatorname{cis}[(\vartheta-\varphi)/2] - \operatorname{cis}[(\varphi-\vartheta)/2]| = 2|\sin[(\vartheta-\varphi)/2]| < 2\sqrt{(\cos[(\vartheta-\varphi)/2]-1)^2 + (\sin[(\vartheta-\varphi)/2])^2} = 2|\operatorname{cis}[(\vartheta-\varphi)/2] - 1| \leq 2\left|\frac{\vartheta-\varphi}{2}\right| = |\vartheta-\varphi|$ die strikte Ungleichung. Im Fall $|\vartheta-\varphi| \geq \pi$ gilt trivialerweise $|\operatorname{cis}\vartheta - \operatorname{cis}\varphi| \leq 2 < \pi \leq |\vartheta-\varphi|$. Insgesamt ist daher $\vartheta = \varphi$ der einzige Gleichheitsfall. □

Beweis der Ungleichung $|\operatorname{cis}\vartheta - \operatorname{cis}\varphi| \geq |\vartheta-\varphi|\frac{|\operatorname{cis}\vartheta + \operatorname{cis}\varphi|}{2}$. Wir zeigen $|\operatorname{cis}\vartheta - \operatorname{cis}(-\vartheta)| \geq |\vartheta|\,|\operatorname{cis}\vartheta + \operatorname{cis}(-\vartheta)|$ für $\vartheta \in [0, \frac{\pi}{2})$. Ist dies erledigt, so können wir auch $\vartheta \in [-\frac{\pi}{2}, \frac{\pi}{2}]$ zulassen, und über $|\operatorname{cis}\vartheta - \operatorname{cis}\varphi| = |\operatorname{cis}\frac{\vartheta-\varphi}{2} - \operatorname{cis}\frac{\varphi-\vartheta}{2}|$ folgt wie im vorigen Beweis die allgemeine Ungleichung $|\operatorname{cis}\vartheta - \operatorname{cis}\varphi| \geq |\vartheta-\varphi|\,|\operatorname{cis}\vartheta + \operatorname{cis}\varphi|/2$ für $|\vartheta-\varphi| \leq \pi$. Wir beginnen die Argumentation mit der Betrachtung von $z = x+\mathbf{i}y$ und $w = u+\mathbf{i}v$ mit $|z| = |w| = 1$, $0 < u \leq x$, $0 \leq y \leq v$. Gemäß der Youngschen Ungleichung aus den Übungen oder direkter Rechnung gilt $xu+yv \leq \frac{1}{2}(x^2+y^2+u^2+v^2) = 1 = u^2+v^2$, und durch Umformung erhält man $u(x-u) \leq v(v-y)$. Als Nächstes ergibt sich $|z-w| = \frac{1}{u}\sqrt{u^2(x-u)^2+u^2(v-y)^2} \leq \frac{1}{u}\sqrt{v^2+u^2}(v-y) = \frac{1}{u}(v-y)$. Wegen der früher gezeigten Montonie von $(\zeta_n)^j$ in j darf die resultierende Ungleichung für $n \in \mathbb{N}_{\geq 2}$ und $j \leq k$ in $\{1, 2, \dots, 2^{n-2}-1\}$ auf $z = (\zeta_n)^{j-1}$ und $w = (\zeta_n)^j$ angewandt werden und gibt $|(\zeta_n)^j - (\zeta_n)^{j-1}| \leq \frac{\mathit{Im}(\zeta_n^j) - \mathit{Im}(\zeta_n^{j-1})}{\mathit{Re}(\zeta_n^j)} \leq \frac{\mathit{Im}(\zeta_n^j) - \mathit{Im}(\zeta_n^{j-1})}{\mathit{Re}(\zeta_n^k)}$. Insgesamt erhalten wir daraus mit der Dreiecksungleichung und Teleskop-Summation die Hilfsabschätzung

$$k|\zeta_n - 1| = \sum_{j=1}^{k} |(\zeta_n)^j - (\zeta_n)^{j-1}| \leq \frac{\mathit{Im}(\zeta_n^k)}{\mathit{Re}(\zeta_n^k)} \qquad \text{für alle } n \in \mathbb{N}_{\geq 2} \text{ und } k \in \{0, 1, 2, \dots, 2^{n-2}-1\}\,.$$

Für die Hauptabschätzung wenden wir dies mit $k = k_n(\vartheta)$ an (wobei $k_n(\vartheta) < 2^{n-2}$ aus $\vartheta < \frac{\pi}{2}$ folgt) und bekommen

$$\frac{\left|(\zeta_n)^{k_n(\vartheta)} - (\zeta_n)^{-k_n(\vartheta)}\right|}{\left|(\zeta_n)^{k_n(\vartheta)} + (\zeta_n)^{-k_n(\vartheta)}\right|} = \frac{\mathit{Im}\left(\zeta_n^{k_n(\vartheta)}\right)}{\mathit{Re}\left(\zeta_n^{k_n(\vartheta)}\right)} \geq k_n(\vartheta)|\zeta_n - 1| = \frac{2\pi k_n(\vartheta)}{2^n} \cdot \frac{2^{n-1}|\zeta_n - 1|}{\pi}\,.$$

für $n \gg 1$. Durch Grenzübergang $n \to \infty$ erhalten wir wegen $\lim_{n\to\infty}(\zeta_n)^{\pm k_n(\vartheta)} = \operatorname{cis}(\pm\vartheta)$, $\lim_{n\to\infty}\frac{2\pi k_n(\vartheta)}{2^n} = \vartheta$ und $\lim_{n\to\infty} 2^{n-1}|\zeta_n - 1| = \pi$ die Behauptung $\frac{|\operatorname{cis}\vartheta - \operatorname{cis}(-\vartheta)|}{|\operatorname{cis}\vartheta + \operatorname{cis}(-\vartheta)|} \geq \vartheta$.

Auch bei der hier bewiesenen Ungleichung lässt sich die Gleichheitsdiskussion im Nachhinein durchführen. Ähnlich wie oben überlegen wir uns im Fall $0 < |\vartheta-\varphi| < \pi$ dazu $\frac{|\operatorname{cis}\vartheta - \operatorname{cis}\varphi|}{|\operatorname{cis}\vartheta + \operatorname{cis}\varphi|} = \frac{|\sin[(\vartheta-\varphi)/2]|}{|\cos[(\vartheta-\varphi)/2]|} = 2\frac{|\sin[(\vartheta-\varphi)/4]||\cos[(\vartheta-\varphi)/4]|}{\cos^2[(\vartheta-\varphi)/4] - \sin^2[(\vartheta-\varphi)/4]} > 2\frac{|\sin[(\vartheta-\varphi)/4]||\cos[(\vartheta-\varphi)/4]|}{\cos^2[(\vartheta-\varphi)/4]} = 2\frac{|\sin[(\vartheta-\varphi)/4]|}{|\cos[(\vartheta-\varphi)/4]|} = 2\frac{|\operatorname{cis}(\vartheta/2) - \operatorname{cis}(\varphi/2)|}{|\operatorname{cis}(\vartheta/2) + \operatorname{cis}(\varphi/2)|} \geq \left|\frac{\vartheta}{2} - \frac{\varphi}{2}\right| = |\vartheta-\varphi|/2$. Im Fall $|\vartheta-\varphi| = \pi$ gilt die strikte Ungleichung trivialerweise, und als Gleichheitsfall verbleibt nur $\vartheta = \varphi$. □

Beweise der Ungleichungen für sin *und* cos. Die Ungleichungen $|\sin\vartheta-\sin\varphi| \leq |\vartheta-\varphi|$ und $|\cos\vartheta-\cos\varphi| \leq |\vartheta-\varphi|$ samt Gleichheitsdiskussionen folgen direkt aus der ersten Ungleichung für cis, die Ungleichung $\sin\vartheta \leq \vartheta$ für $\vartheta \in \mathbb{R}_{\geq 0}$ ist ein Spezialfall. Durch Anwendung der zweiten Ungleichung für cis mit $\varphi = -\vartheta$ erhält man außerdem $\sin\vartheta \geq \vartheta\cos\vartheta$ für $\vartheta \in [0, \frac{\pi}{2}]$ samt Gleichheitsdiskussion (und für $\vartheta \in (\frac{\pi}{2}, \pi]$ gilt diese Ungleichung sowieso). Damit folgt auch

$$(1+\vartheta^2)(\cos\vartheta)^2 = (\cos\vartheta)^2 + (\vartheta\cos\vartheta)^2 \leq (\cos\vartheta)^2 + (\sin\vartheta)^2 = 1 \qquad \text{für } \vartheta \in \left[-\tfrac{\pi}{2}, \tfrac{\pi}{2}\right]$$

und somit die Abschätzung $\cos\vartheta \leq \frac{1}{\sqrt{1+\vartheta^2}}$ für $\vartheta \in [-\frac{\pi}{2}, \frac{\pi}{2}]$ (und für $|\vartheta| \in (\frac{\pi}{2}, \frac{3\pi}{2}]$ gilt diese Ungleichung sowieso). Mit

$$\cos\vartheta = \sqrt{1-(\sin\vartheta)^2} \geq \sqrt{1-\vartheta^2} \qquad \text{für } \vartheta \in [-1, 1]$$

ist auch die letzte Abschätzung für den Kosinus erledigt. Die verbleibenden Aussagen über Gleichheitsfälle kommen bei diesen Argumenten gleich mit heraus. □

Für die Kreisfunktionen gelten neben den oben genannten noch viele weitere Formeln und Eigenschaften. An dieser Stelle soll aber nur noch eine weitere Definition getroffen werden.

Definition (**Tangens und Kotangens**). *Die Kreisfunktionen Tangens und Kotangens sind definiert als*

$$\tan\colon \mathbb{R}\backslash\{\pm\tfrac{\pi}{2}, \pm 3\tfrac{\pi}{2}, \pm 5\tfrac{\pi}{2}, \ldots\} \to \mathbb{R}\,,\ \vartheta \mapsto \frac{\sin\vartheta}{\cos\vartheta}\,,$$
$$\cot\colon \mathbb{R}\backslash\{0, \pm\pi, \pm 2\pi, \pm 3\pi, \ldots\} \to \mathbb{R}\,,\ \vartheta \mapsto \frac{\cos\vartheta}{\sin\vartheta}\,.$$

Eigenschaften dieser Funktionen wie beispielsweise $\tan 0 = 0$, $\tan\frac{\pi}{4} = 1$, $1+\tan^2\vartheta = \frac{1}{\cos^2}\vartheta$ für $\tan(\vartheta+\pi) = \tan\vartheta$, $\tan(-\vartheta) = -\tan\vartheta$ für $\vartheta \in \mathbb{R}\backslash\{\pm\frac{\pi}{2}, \pm 3\frac{\pi}{2}, \pm 5\frac{\pi}{2}, \ldots\}$ und $\tan\vartheta > \vartheta$ für $\vartheta \in \left[0, \frac{\pi}{2}\right]$ lassen sich aus den Eigenschaften des Kosinus und des Sinus ableiten.

Als abschließende Anwendung nutzen wir die Kreisfunktionen, um komplexe Wurzeln in Polardarstellung allgemein angeben zu können:

Satz (**Wurzeln komplexer Zahlen**). *Für $k \in \mathbb{N}$ besitzt jedes $z \in \mathbb{C}\backslash\{0\}$ genau k verschiedene k-te Wurzeln in $\mathbb{C}$. Bei Polardarstellung $z = |z|\operatorname{cis}\vartheta$ mit $\vartheta \in \mathbb{R}$ sind diese Wurzeln gerade*

$$\sqrt[k]{|z|}\operatorname{cis}\frac{\vartheta}{k}\,, \qquad \sqrt[k]{|z|}\operatorname{cis}\frac{\vartheta+2\pi}{k}\,, \qquad \sqrt[k]{|z|}\operatorname{cis}\frac{\vartheta+4\pi}{k}\,, \qquad \ldots\,, \qquad \sqrt[k]{|z|}\operatorname{cis}\frac{\vartheta+2(k-1)\pi}{k}\,.$$

Beweis. Die k-ten Wurzeln aus z sind genau die Lösungen $w \in \mathbb{C}$ der polynomialen Gleichung $w^k - z = 0$, und gemäß Abschnitt 3.2 gibt es höchstens k solche Lösungen. Es bleibt somit nur nachzurechnen, dass die angegebenen Zahlen in der Tat k verschiedene Wurzeln sind. Dies gelingt mit den Eigenschaften von cis und wird in den Übungen genauer erörtert. □

Zumindest für Zweierpotenzen k kann man die k-ten Wurzeln aber als iterierte Quadratwurzeln auch ohne Kreisfunktionen erhalten, denn:

Bemerkung (zu **komplexen *Quadrat*wurzeln**). Die beiden komplexen *Quadrat*wurzeln aus $z \in \mathbb{C}\backslash\mathbb{R}_{\leq 0}$ kann man als

$$\pm\sqrt{|z|}\,\frac{z+|z|}{\left|z+|z|\right|}$$

angeben und berechnen. Diese Formel bestätigt man mit der schon für die Einheitswurzeln ζ_n gemachten Rechnung. Im verbleibenden Fall $z = x \in \mathbb{R}_{<0}$, in dem der Nenner in der Formel Null ist, erhält man die beiden komplexen Quadratwurzeln natürlich einfach als $\pm\mathbf{i}\sqrt{|x|}$.

5.4 Häufungswerte und Teilfolgen

In diesem Abschnitt wenden wir uns zwei Begriffen zu, mit denen auch das Grenzverhalten divergenter Folgen bei $n \to \infty$ beschrieben werden kann:

Definition (**Häufungswerte**). *Sei $(x_n)_{n\in\mathbb{N}}$ eine Folge in $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$. Dann heißt $x \in \mathbb{K}$ ein **Häufungswert** (manchmal auch: Häufungspunkt) der Folge $(x_n)_{n\in\mathbb{N}}$, wenn es für jedes $\varepsilon \in \mathbb{R}_{>0}$ unendliche viele $n \in \mathbb{N}$ mit $|x_n - x| < \varepsilon$ gibt. Im Fall $\mathbb{K} = \mathbb{R}$ bezeichnen wir zudem $\pm\infty$ als **(uneigentlichen) Häufungswert** der Folge $(x_n)_{n\in\mathbb{N}}$, wenn es für jedes $\varepsilon \in \mathbb{R}_{>0}$ unendliche viele $n \in \mathbb{N}$ mit $\pm x_n > \frac{1}{\varepsilon}$ gibt.*

Bemerkung (zur **Definition des Häufungswerts**). In Quantoren-Schreibweise verlangt die Definition des Häufungswerts

$$\forall \varepsilon \in \mathbb{R}_{>0} \colon \forall n_0 \in \mathbb{N} \colon \exists n \in \mathbb{N}_{\geq n_0} \colon |x_n - x| < \varepsilon$$

(und bei uneigentlich Häufungswerten analog $\forall \varepsilon \in \mathbb{R}_{>0} \colon \forall n_0 \in \mathbb{N} \colon \exists n \in \mathbb{N}_{\geq n_0} \colon \pm x_n > \frac{1}{\varepsilon}$).

Beispiel (für **Häufungswerte**). Die Folge $(1-\frac{1}{1}, 3+\frac{1}{2}, 1-\frac{1}{3}, 3+\frac{1}{4}, 1-\frac{1}{5}, 3+\frac{1}{6}, 1-\frac{1}{7}, 3+\frac{1}{8}, \ldots)$, die wir konzis als $\big(2+(-1)^n\big(1+\frac{1}{n}\big)\big)_{n\in\mathbb{N}}$ schreiben können, hat genau 1 und 3 als Häufungswerte.

Definition (**Teilfolgen**). *Sei $(x_n)_{n\in\mathbb{N}}$ eine Folge in einer Menge $\mathcal{X}$. Ist $n_1 < n_2 < n_3 < \ldots$ in $\mathbb{N}$ (also $(n_k)_{k\in\mathbb{N}}$ eine streng monoton wachsende Folge in $\mathbb{N}$), so heißt $\big(x_{n_k}\big)_{k\in\mathbb{N}}$ eine Teilfolge von $(x_n)_{n\in\mathbb{N}}$.*

Bemerkung (zu **Teilfolgen**). Manchmal verwendet man die etwas andere Konvention, dass statt $\big(x_{n_k}\big)_{k\in\mathbb{N}}$ die Indexfolge $(n_k)_{k\in\mathbb{N}}$ als Teilfolge bezeichnet wird. Die Grundidee ist und bleibt aber, dass $(n_k)_{k\in\mathbb{N}}$ das Aussondern von $\big(x_{n_k}\big)_{k\in\mathbb{N}}$ aus einer (beliebigen) Folge $(x_n)_{n\in\mathbb{N}}$ erlaubt.

Es besteht ein **grundlegender Zusammenhang von Häufungswerten und Teilfolgen**:

Proposition. *Für eine Folge $(x_n)_{n\in\mathbb{N}}$ in $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$ und $x \in \mathbb{K}$ (und im Fall $\mathbb{K} = \mathbb{R}$ sogar für $x \in \overline{\mathbb{R}}$) gilt:*

$$\boxed{x \text{ ist Häufungswert von } (x_n)_{n\in\mathbb{N}} \iff x \text{ ist Grenzwert einer Teilfolge von } (x_n)_{n\in\mathbb{N}}}.$$

Beweis. Dies folgt aus den Definitionen und wird auch in den Übungen noch besprochen. □

Von entscheidender Bedeutung in vielen verschiedenen Zusammenhängen ist nun der folgende Satz über die Existenz von Häufungswerten, der auch als **allgemeiner Existenzsatz für Grenzwerte (von Teilfolgen)** verstanden werden kann:

Hauptsatz (**Satz von Bolzano-Weierstraß**). *Sei $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$. **Jede beschränkte Folge in $\mathbb{K}$ besitzt einen Häufungswert in $\mathbb{K}$ und, äquivalent, eine in $\mathbb{K}$ konvergente Teilfolge.***

Beweis. Im Fall $\mathbb{K} = \mathbb{R}$ sei $(x_n)_{n\in\mathbb{N}}$ eine beschränkte Folge in $\mathbb{R}$. Es gibt dann eine Schranke $M \in \mathbb{R}_{\geq 0}$, so dass $I_0 := [-M, M]$ alle x_n mit $n \in \mathbb{N}$ enthält. Durch iterative Intervallhalbierung findet man für jedes $k \in \mathbb{N}$ ein Intervall $I_k = [a_k, b_k] \subset I_{k-1}$ mit Länge $b_k - a_k = 2^{1-k}M$, das jedenfalls *unendlich viele* x_n mit $n \in \mathbb{N}$ enthält. Genauer zeigt man die Existenz von I_k mit Induktion und nutzt dabei im Induktionsschritt, dass mit I_{k-1} mindestens eines der halbierten

Intervalle $\left[a_{k-1}, \frac{a_{k-1}+b_{k-1}}{2}\right]$ und $\left[\frac{a_{k-1}+b_{k-1}}{2}, b_{k-1}\right]$ unendlich viele x_n enthält und als I_k gewählt werden kann. Wegen der Vollständigkeit von $\mathbb{R}$ besitzt die durch die Intervalle I_k gebildete Intervallschachtelung einen Kern $x \in \mathbb{R}$ mit $x \in I_k$ für alle $k \in \mathbb{N}$. Für jedes $\varepsilon \in \mathbb{R}_{>0}$ betrachte nun ein $k \in \mathbb{N}$ mit $2^{1-k}M < \varepsilon$ und erhalte, dass unendlich viele x_n mit $n \in \mathbb{N}$ in $I_k \subset (x-\varepsilon, x+\varepsilon)$ liegen. Also ist x ein Häufungspunkt von $(x_n)_{n\in\mathbb{N}}$.

Den Fall $\mathbb{K} = \mathbb{C}$ kann man durch ein analoges Argument mit Rechteckschachtelungen erledigen oder wie folgt auf den Fall $\mathbb{K} = \mathbb{R}$ zurückführen: Ist $(x_n)_{n\in\mathbb{N}}$ eine beschränkte Folge in $\mathbb{C}$, so erhält man erst die Konvergenz einer Teilfolge $\left(\mathcal{Re}\left(x_{n_k}\right)\right)_{k\in\mathbb{N}}$ der Realteile gegen ein $x \in \mathbb{R}$, dann die Konvergenz einer (weiteren) Teilfolge $\left(\mathcal{Im}\left(x_{n_{k_\ell}}\right)\right)_{\ell\in\mathbb{N}}$ der Imaginärteile gegen ein $y \in \mathbb{R}$. Hieraus folgt die Konvergenz der Teilfolge $\left(x_{n_{k_\ell}}\right)_{\ell\in\mathbb{N}}$ von $(x_n)_{n\in\mathbb{N}}$ gegen $x+\mathbf{i}y \in \mathbb{C}$. □

Bemerkungen (zum **Satz von Bolzano-Weierstraß**).

(1) Ein alternativer Beweis des Satzes von Bolzano-Weierstraß gelingt mit der (etwas Überlegung erfordernden) Beobachtung, dass jede Folge in $\mathbb{R}$ eine monotone Teilfolge besitzt, und dem Monotonie-Kriterium.

(2) Unbeschränkte Folgen in $\mathbb{R}$ besitzen einen uneigentlichen Häufungswert und, äquivalent, eine uneigentlich konvergente Teilfolge. Insgesamt kann man daher sagen: **Jede Folge in $\mathbb{R}$ besitzt, im eigentlichen oder im uneigentlichen Sinne, einen Häufungswert und eine konvergente Teilfolge.**

(3) Als Korollar zum Satz von Bolzano-Weierstraß ergeben sich folgende Äquivalenzen: Für eine Folge $(x_n)_{n\in\mathbb{N}}$ in $\mathbb{K}$ und $x \in \mathbb{K}$ gilt

$$\boxed{\lim_{n\to\infty} x_n = x \iff (x_n)_{n\in\mathbb{N}} \text{ beschränkt}, x \textit{ einziger} \text{ Häufungswert von } (x_n)_{n\in\mathbb{N}} \text{ in } \mathbb{K}},$$

und für eine Folge $(x_n)_{n\in\mathbb{N}}$ in $\mathbb{R}$ und $x \in \overline{\mathbb{R}}$ gilt

$$\boxed{\lim_{n\to\infty} x_n = x \iff x \textit{ einziger} \text{ Häufungswert von } (x_n)_{n\in\mathbb{N}} \text{ in } \overline{\mathbb{R}}}.$$

In beiden Fällen ist dabei der Beweis von „$\Longrightarrow$“ elementar, während der Beweis von „$\Longleftarrow$“ mit dem Hauptsatz und einem sogenannten Teilfolgenargument erfolgt; vergleiche mit den Übungen.

Abschließend beschäftigen wir uns kurz mit der Menge aller Häufungswerte einer Folge:

Satz & Definition (**Grenzwerte von Häufungswerten, Limes superior und inferior**).

(I) *Ist $(x_n)_{n\in\mathbb{N}}$ eine Folge in $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$ und existiert für eine Folge $(a_k)_{k\in\mathbb{N}}$ von Häufungswerten von $(x_n)_{n\in\mathbb{N}}$ der (für $\mathbb{K} = \mathbb{R}$ eventuell uneigentliche) Grenzwert*[8] *$a := \lim_{k\to\infty} a_k$, so ist a wieder ein Häufungswert von $(x_n)_{n\in\mathbb{N}}$. Man drückt diese Eigenschaft auch so aus, dass die Menge der Häufungswerte von $(x_n)_{n\in\mathbb{N}}$ (unter Grenzwerten) abgeschlossen ist.*

(II) *Bei einer Folge $(x_n)_{n\in\mathbb{N}}$ in $\mathbb{R}$ gibt es stets einen **größten Häufungswert** und einen **kleinsten Häufungswert** in $\mathbb{R} \cup \{-\infty, \infty\}$. Wir bezeichnen diese als den **Limes superior** $\limsup_{n\to\infty} x_n$ und den **Limes inferior** $\liminf_{n\to\infty} x_n$ von $(x_n)_{n\in\mathbb{N}}$.*

[8] Man beachte, dass für $\mathbb{K} = \mathbb{R}$ uneigentliche Häufungswerte $a_k = \pm\infty$ möglich sind und hier behandelt werden können, wenn die (uneigentliche) Grenzwertdefinition auf naheliegende Weise auf Folgen in $\overline{\mathbb{R}}$ erweitert wird.

Beweis. Sei $\mathcal{H}$ die Menge der Häufungswerte von $(x_n)_{n\in\mathbb{N}}$ in $\overline{\mathbb{R}}$ beziehungsweise $\mathbb{C}$.

Wir beginnen mit Teil (I) und betrachten eine gegen a konvergente Folge $(a_k)_{k\in\mathbb{N}}$ in $\mathcal{H}$. Wir können $a_k \in \mathbb{K}$ annehmen (denn, ist $a_k = \pm\infty$ für unendliche viele $k \in \mathbb{N}$, so muss $a = \pm\infty \in \mathcal{H}$ sein). Wir erhalten eine Teilfolge $\big(x_{n_k}\big)_{k\in\mathbb{N}}$ von $(x_n)_{n\in\mathbb{N}}$ mit $|x_{n_k} - a_k| < \frac{1}{k}$ für alle $k \in \mathbb{N}$, indem wir erst $n_1 \in \mathbb{N}$ mit $|x_{n_1} - a_1| < 1$ und dann rekursiv $n_{k+1} \in \mathbb{N}_{>n_k}$ mit $|x_{n_{k+1}} - a_{k+1}| < \frac{1}{k+1}$ wählen. Es folgt $\lim_{k\to\infty} x_{n_k} = \lim_{k\to\infty} a_k = a$, also ist a ein Häufungswert von $(x_n)_{n\in\mathbb{N}}$.

Um die in Teil (II) behauptete Existenz eines größten und kleinsten Elements von $\mathcal{H}$ nachzuweisen, bemerken wir zuerst, dass der Satz von Bolzano-Weierstraß $\mathcal{H} \neq \emptyset$ sichert. Somit existieren $\sup\mathcal{H}, \inf\mathcal{H} \in \overline{\mathbb{R}}$. Da $\sup\mathcal{H}$ und $\inf\mathcal{H}$ als Grenzwerte von Folgen in $\mathcal{H}$ geschrieben werden können, erhalten wir mit Teil (I), dass $\sup\mathcal{H}, \inf\mathcal{H} \in \mathcal{H}$ das größte und das kleinste Element von $\mathcal{H}$ sind. □

Bemerkungen (zu **(größten/kleinsten) Häufungswerten**).

(1) Nach Definition gilt für eine Folge $(x_n)_{n\in\mathbb{N}}$ in $\overline{\mathbb{R}}$ stets $\liminf_{n\to\infty} x_n \leq \limsup_{n\to\infty} x_n$. Der (eventuell uneigentliche) Limes $\lim_{n\to\infty} x_n$ existiert genau in dem Fall, dass Gleichheit $\liminf_{n\to\infty} x_n = \limsup_{n\to\infty} x_n$ eintritt.

(2) Eine Folge kann sehr viele Häufungswerte besitzen. Wird etwa durch eine Folge $(x_n)_{n\in\mathbb{N}}$ ganz $\mathbb{Q} = \{x_n \,|\, n \in \mathbb{N}\}$ abgezählt (was nach dem ersten Cantorschen Diagonalverfahren ja möglich ist), so sind *alle* Elemente von $\overline{\mathbb{R}}$ Häufungswerte von $(x_n)_{n\in\mathbb{N}}$.

5.5 Konvergenz von Reihen

Reihen sind unendliche Summen und können als (spezielle) Grenzwerte von Folgen aufgefasst werden. Die Theorie der Reihen erweist sich aber als erstaunlich vielseitig und reichhaltig und verdient eine separate Behandlung:

Definition (**Reihen**). *Sei* $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$.

(I) *Eine* ***Reihe*** *ist eine* ***formale unendliche Summe***

$$\sum_{k=k_0}^{\infty} a_k = a_{k_0} + a_{k_0+1} + a_{k_0+2} + a_{k_0+3} + \dots$$

mit $k_0 \in \mathbb{Z}$ *und einer Folge* $(a_k)_{k\in\mathbb{Z}_{\geq k_0}}$ *von* ***Reihengliedern*** $a_k \in \mathbb{K}$. *Wir bezeichnen die endlichen Summen* $\sum_{k=k_0}^{n} a_k$ *mit* $n \in \mathbb{Z}_{\geq k_0}$ *als* ***Partialsummen*** *der Reihe.*

(II) *Wir nennen eine Reihe* $\sum_{k=k_0}^{\infty} a_k$ ***konvergent****, wenn die zugehörige Partialsummenfolge* $\big(\sum_{k=k_0}^{n} a_k\big)_{n\in\mathbb{Z}_{\geq k_0}}$ *in* $\mathbb{K}$ *konvergiert, und andernfalls* ***divergent****. Für* $\mathbb{K} = \mathbb{R}$ *nennen wir* $\sum_{k=k_0}^{\infty} a_k$ ***bestimmt divergent****, wenn* $\big(\sum_{k=k_0}^{n} a_k\big)_{n\in\mathbb{Z}_{\geq k_0}}$ *bestimmt gegen* ∞ *oder* $-\infty$ *divergiert, und in anderen Divergenzfällen* ***unbestimmt divergent****.*

(III) *Für konvergente oder bestimmt divergente Reihen erklären wir den* ***Wert der Reihe***

$$\sum_{k=k_0}^{\infty} a_k := \lim_{n\to\infty} \sum_{k=k_0}^{n} a_k$$

als den (bei bestimmter Divergenz uneigentlichen) ***Grenzwert der Partialsummen****.*

Die erwähnte Schreibweise $a_{k_0}+a_{k_0+1}+a_{k_0+2}+a_{k_0+3}+\ldots$ mit De-Facto-Angabe nur endlich vieler Reihenglieder ist dabei im Gegensatz zur Schreibweise $\sum_{k=k_0}^{\infty} a_k$ mit dem Summenzeichen nicht völlig präzise. Führt man ausreichend viele Reihenglieder an, um ein klares Bildungsgesetz zu suggerieren, so erweist sich die Pünktchen-Notation in der Rechenpraxis aber dennoch als unproblematisch und sinnvoll.

Wir geben nun **vier fundamentale** (Typen von) **Reihen** als Beispiele an:

Beispiele (von **Reihen**)**.**

(1) Aus der geometrischen Summenformel $\sum_{k=0}^{n} q^k = \frac{q^{n+1}-1}{q-1}$ für $q \in \mathbb{C}\backslash\{1\}$ und $n \in \mathbb{N}_0$ folgt durch Grenzübergang $n \to \infty$ die **Konvergenz der geometrischen Reihe**

$$\sum_{k=0}^{\infty} q^k = \frac{1}{1-q} \qquad \text{für } q \in \mathbb{C} \text{ mit } \boldsymbol{|q| < 1}\,.$$

Für $q \in \mathbb{C}$ mit $|q| \geq 1$ dagegen divergiert $\sum_{k=0}^{\infty} q^k$ (wobei für $q \in \mathbb{R}_{\geq 1}$ bestimmte Divergenz gegen ∞, für $q \in \mathbb{R}_{\leq -1}$ unbestimmte Divergenz vorliegt).

(2) Die **harmonischen Reihe**

$$\sum_{k=1}^{\infty} \frac{1}{k} = \infty$$

ist bestimmt divergent. Dies kann man mit der Abschätzung $\sum_{k=2}^{2^n} \frac{1}{k} = \sum_{\ell=0}^{n-1} \sum_{k=2^\ell+1}^{2^{\ell+1}} \frac{1}{k} \geq \sum_{\ell=0}^{n-1} \sum_{k=2^\ell+1}^{2^{\ell+1}} \frac{1}{2^{\ell+1}} = \sum_{\ell=0}^{n-1} 2^\ell \frac{1}{2^{\ell+1}} = \sum_{\ell=0}^{n-1} \frac{1}{2} = \frac{n}{2} \underset{n\to\infty}{\longrightarrow} \infty$ einsehen, die einem Spezialfall des demnächst folgenden Verdichtungskriteriums entspricht. Alternativ werden wir die bestimmte Divergenz der harmonischen Reihe gegen Ende dieses Abschnitts noch mit Hilfe eines unendlichen Produkts zeigen.

(3) Die Konvergenz der **reellen Exponentialreihe**

$$\sum_{k=0}^{\infty} \frac{1}{k!} x^k = \exp(x) = \mathrm{e}^x \qquad \text{für } x \in \mathbb{R}$$

wurde für $x \in \mathbb{R}_{\geq 0}$ in den Übungen gezeigt und wird für $x \in \mathbb{R}_{<0}$ in Abschnitt 5.6 im allgemeineren Kontext der komplexen Exponentialreihe nachgetragen. Insbesondere ist

$$\sum_{k=0}^{\infty} \frac{1}{k!} = 1+1+\frac{1}{2}+\frac{1}{3!}+\frac{1}{4!}+\frac{1}{5!}+\ldots = \mathrm{e} \quad \text{und} \quad \sum_{k=0}^{\infty} \frac{(-1)^k}{k!} = 1-1+\frac{1}{2}-\frac{1}{3!}+\frac{1}{4!}-\frac{1}{5!}\pm\ldots = \frac{1}{\mathrm{e}}\,.$$

(4) Für $k_0 \in \mathbb{Z}$ und jede in $\mathbb{C}$ konvergente[9] Folge $(b_k)_{k\in\mathbb{Z}_{\geq k_0}}$ konvergiert die **Teleskopreihe**

$$\sum_{k=k_0}^{\infty} (b_{k+1}-b_k) = \Big(\lim_{k\to\infty} b_k\Big) - b_{k_0}\,.$$

Ein konkretes Beispiel dieses Typs ist

$$\sum_{k=2}^{\infty} \frac{1}{k(k+1)} = \sum_{k=2}^{\infty} \left(\frac{1}{k} - \frac{1}{k+1}\right) = \frac{1}{2}\,.$$

[9] Man kann sich hier tatsächlich auf gegen 0 konvergente Folgen $(b_k)_{k\in\mathbb{Z}_{\geq k_0}}$ zurückziehen, da man für beliebiges $b := \lim_{k\to\infty} b_k \in \mathbb{C}$ durch $\widetilde{b}_k := b_k - b$ eine Nullfolge $\big(\widetilde{b}_k\big)_{k\in\mathbb{N}}$ mit $\widetilde{b}_{k+1}-\widetilde{b}_k = b_{k+1}-b_k$ für $k \in \mathbb{Z}_{\geq k_0}$ erhält.

Als grundlegende Eigenschaften bei Reihen halten wir fest:

Grundeigenschaften (von **Reihen**). Für $k_0 \leq m$ in $\mathbb{Z}$, $s \in \mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$ und Folgen $(a_k)_{k\in\mathbb{Z}_{\geq k_0}}$ und $(b_k)_{k\in\mathbb{Z}_{\geq k_0}}$ in $\mathbb{K}$ gelten:

(1) Sind die Reihen $\sum_{k=k_0}^{\infty} a_k$ und $\sum_{k=k_0}^{\infty} b_k$ konvergent oder bestimmt divergent, so ist auch $\sum_{k=k_0}^{\infty}(a_k \pm b_k)$ konvergent oder bestimmt divergent mit Wert

$$\sum_{k=k_0}^{\infty}(a_k \pm b_k) = \sum_{k=k_0}^{\infty} a_k \pm \sum_{k=k_0}^{\infty} b_k\,,$$

vorausgesetzt rechts tritt **nicht** der unbestimmte Ausdruck $\boldsymbol{\infty-\infty}$ oder $\boldsymbol{-\infty+\infty}$ auf.

Falls eine der Reihen $\sum_{k=k_0}^{\infty} a_k$, $\sum_{k=k_0}^{\infty}(sa_k)$ mit $s \neq 0$ konvergiert oder bestimmt divergiert, so ist dies auch für die andere der Fall, und es gilt

$$\sum_{k=k_0}^{\infty}(sa_k) = s\sum_{k=k_0}^{\infty} a_k\,.$$

(2) Falls eine der Reihen $\sum_{k=k_0}^{\infty} a_k$, $\sum_{k=m}^{\infty} a_k$ konvergiert oder bestimmt divergiert, so ist dies auch für die andere der Fall, und es gilt

$$\sum_{k=k_0}^{\infty} a_k = \sum_{k=k_0}^{m-1} a_k + \sum_{k=m}^{\infty} a_k\,.$$

(3) **Abänderung endlich vieler Glieder ändert nichts an Konvergenz oder Divergenz** einer Reihe, ändert aber (normalerweise) ihren Wert. **Vertauschung endlicher vieler Glieder beeinflusst weder** die **Konvergenz** einer Reihe **noch** den **Reihenwert**.

(4) Liegt eine disjunkte Zerlegung $\mathbb{Z}_{\geq k_0} = \{\ell_i \,|\, i \in \mathbb{N}\} \dot\cup \{m_j \,|\, j \in \mathbb{N}\}$ mit *streng monoton wachsenden Indexfolgen* $(\ell_i)_{i\in\mathbb{N}}$ und $(m_j)_{j\in\mathbb{N}}$ vor und sind $\sum_{i=1}^{\infty} a_{\ell_i}$ und $\sum_{j=1}^{\infty} a_{m_j}$ konvergent oder bestimmt divergent, so ist auch $\sum_{k=k_0}^{\infty} a_k$ konvergent oder bestimmt divergent mit Wert

$$\sum_{k=k_0}^{\infty} a_k = \sum_{i=1}^{\infty} a_{\ell_i} + \sum_{j=1}^{\infty} a_{m_j}\,,$$

vorausgesetzt rechts tritt **nicht** der unbestimmte Ausdruck $\boldsymbol{\infty-\infty}$ oder $\boldsymbol{-\infty+\infty}$ auf. Ein typischer Spezialfall dieser Regel (mit $k_0 = 1$) ist die Zerlegung

$$\sum_{k=1}^{\infty} a_k = \sum_{i=1}^{\infty} a_{2i} + \sum_{j=1}^{\infty} a_{2j-1}$$

in Teilreihen mit nur geraden und nur ungeraden Indizes (falls die rechte Seite sinnvoll ist).

(5) Gilt im Fall $\mathbb{K} = \mathbb{R}$ die Ungleichung

$$a_k \leq b_k \qquad \text{für } \textit{alle } k \in \mathbb{Z}_{\geq k_0}$$

und sind $\sum_{k=k_0}^{\infty} a_k$ und $\sum_{k=k_0}^{\infty} b_k$ konvergent oder bestimmt divergent, so folgt

$$\sum_{k=k_0}^{\infty} a_k \leq \sum_{k=k_0}^{\infty} b_k\,.$$

Zu den Beweisen der Grundeigenschaften. Die Eigenschaften (1) und (2) erhält man problemlos, indem man bei den Grenzwerten der Partialsummen die Grenzwertregeln für Summen und Produkte anwendet (inklusive symbolischer Regeln bei Fällen mit bestimmter Divergenz).

Die Eigenschaft (3) ergibt sich nach Umschreiben mit (2) aus dem entsprechenden Verhalten bei endlichen Summen.

Zum Nachweis der Eigenschaft (4) beobachten wir

$$\sum_{k=k_0}^{n} a_k = \sum_{i=1}^{i_n} a_{\ell_i} + \sum_{j=1}^{j_n} a_{m_j} \qquad \text{für } n \in \mathbb{Z}_{\geq k_0}$$

mit $i_n := \max\{i \in \mathbb{N} \,|\, \ell_i \leq n\}$ und $j_n := \max\{j \in \mathbb{N} \,|\, m_j \leq n\}$. Wegen $\lim_{n\to\infty} i_n = \infty$ konvergiert dabei der erste Term auf der rechten Seite für $n \to \infty$ gegen $\sum_{i=1}^{\infty} a_{\ell_i}$, und analog konvergiert der zweite Term gegen $\sum_{j=1}^{\infty} a_{m_j}$. Die Grenzwertregeln für Folgen implizieren dann die Konvergenz von $\sum_{k=k_0}^{n} a_k$ und die behauptete Summenformel.

Die Eigenschaft (5) schließlich folgt aus dem entsprechenden Vergleichsprinzip für Grenzwerte. □

Wir kommen nun zu **Konvergenzkriterien** für Reihen und halten dazu erste Beobachtungen fest, wobei das Nullfolgenkriterium für Theorie *und* Rechenpraxis nützt, während die andere Kriterien von überwiegend theoretischer Bedeutung sind. Im nächsten Satz folgen dann weitere Kriterien, mit denen die Konvergenz konkret gegebener Reihen besser untersucht werden kann.

Satz (über **Grundkriterien für Konvergenz von Reihen**). *Sei $k_0 \in \mathbb{Z}$, und sei $(a_k)_{k\in\mathbb{Z}_{\geq k_0}}$ eine Folge in $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$.*

(I) ***Beschränktheitskriterium*:** *Sei $\mathbb{K} = \mathbb{R}$.* **Falls** *$a_k \geq 0$ für $k \gg 1$ gilt, so konvergiert $\sum_{k=k_0}^{\infty} a_k$ genau dann, wenn die Folge $\big(\sum_{k=k_0}^{n} a_k\big)_{n\in\mathbb{Z}_{\geq k_0}}$ der Partialsummen beschränkt bleibt, und andernfalls liegt bestimmte Divergenz $\sum_{k=k_0}^{\infty} a_k = \infty$ vor.*

(II) ***Cauchy-Kriterium*:** *Genau dann konvergiert $\sum_{k=k_0}^{\infty} a_k$, wenn $\lim_{n\geq m\to\infty} \sum_{k=m}^{n} a_k = 0$ gilt (wobei letzteres gemäß der für die Cauchy-Eigenschaft eingeführten Notation präzise $\forall \varepsilon \in \mathbb{R}_{>0} \colon \exists n_0 \in \mathbb{N} \colon \forall m \in \mathbb{N}_{\geq n_0} \colon \forall n \in \mathbb{N}_{\geq m} \colon \big|\sum_{k=m}^{n} a_k\big| < \varepsilon$ bedeutet).*

(III) ***Nullfolgenkriterium*:** *Wenn $\sum_{k=k_0}^{\infty} a_k$ konvergiert, dann gilt $\lim_{n\to\infty} a_n = 0$. Mit anderen Worten* ***ist für Konvergenz einer Reihe* notwendig, *dass ihre Glieder eine Nullfolge bilden*.**

(IV) *Wenn $\sum_{k=k_0}^{\infty} a_k$ konvergiert, so bilden die* ***Reihenreste*** *$\sum_{k=m}^{\infty} a_k$ eine Nullfolge, genauer gilt $\lim_{m\to\infty} \sum_{k=m}^{\infty} a_k = 0$ (was Konvergenz von $\sum_{k=m}^{\infty} a_k$ mit $m \gg 1$ einschließt).*

In Anbetracht des Beschränktheitskriteriums (I) wird die Konvergenz einer Reihe $\sum_{k=k_0}^{\infty} a_k$ mit (fast nur) nichtnegativen Gliedern $a_k \geq 0$ auch einfach durch $\sum_{k=k_0}^{\infty} a_k < \infty$ ausgedrückt.

Beweis. Die Kriterien (I) und (II) folgen durch Anwendung des Monotonie- beziehungsweise Cauchy-Kriteriums aus Abschnitt 5.1 auf die Partialsummen $s_n := \sum_{k=k_0}^{n} a_k$ (denn $s_n - s_{m-1} = \sum_{k=m}^{n} a_k$ für $n \geq m$). Das Kriterium (III) ergibt sich für $m = n$ aus (II) oder alternativ, weil mit $\lim_{n\to\infty} s_{n-1} = \lim_{n\to\infty} s_n$ schon $\lim_{n\to\infty} a_n = \lim_{n\to\infty}(s_n - s_{n-1}) = 0$ folgt. Das Kriterium (IV) erhält man entweder durch Grenzübergang $n \to \infty$ in der Cauchy-Bedingung von (II) oder durch Grenzübergang $m \to \infty$ in der Formel der vorausgehenden Grundeigenschaft (2). □

Bemerkung (zum **Nullfolgenkriterium**)**.** Das **Nullfolgenkriterium** sollte man bei der Untersuchung der Konvergenz einer gegebenen Reihe (wenn es sich nicht gerade um einen schon bekannten Standard-Typ handelt) **unbedingt zuallererst prüfen (!!!)**. Stellt man fest, dass die Glieder **keine Nullfolge** bilden, so kann man die Reihe sofort **als divergent abhaken** und kann im Fall $\mathbb{K} = \mathbb{R}$ normalerweise auch leicht ablesen, ob bestimmte Divergenz gegen $\pm\infty$ oder unbestimmte Divergenz vorliegt. Wenn dagegen **eine Nullfolge** vorliegt, so kann man — das ist das Wesen eines notwendigen Kriteriums — noch nicht entscheiden, ob Konvergenz vorliegt, und muss die Reihe mit anderen Kriterien **genauer untersuchen**.

Weitere, nützliche Kriterien, mit denen man über Konvergenz oder Divergenz vieler konkret gegebener Reihen entscheiden kann, gibt der folgende Satz.

Satz (über **Konvergenzkriterien für Reihen**)**.** *Seien $k_0 \in \mathbb{Z}$, sei $(a_k)_{k\in\mathbb{Z}_{\geq k_0}}$ eine Folge in $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$, und sei $(b_k)_{k\in\mathbb{Z}_{\geq k_0}}$ eine Folge in $\mathbb{R}$.*

(I) ***Majorantenkriterium*:** *Gilt $|a_k| \leq Cb_k$ für $k \gg 1$ mit festem $C \in \mathbb{R}_{\geq 0}$ und konvergiert die Majorantenreihe $\sum_{k=k_0}^{\infty} b_k$, so konvergiert auch $\sum_{k=k_0}^{\infty} a_k$.*

(II) ***Minorantenkriterium*:** *Sei $\mathbb{K} = \mathbb{R}$. Gilt $a_k \geq cb_k$ für $k \gg 1$ mit festem $c \in \mathbb{R}_{>0}$ und divergiert die Minorantenreihe $\sum_{k=k_0}^{\infty} b_k = \infty$, so divergiert auch $\sum_{k=k_0}^{\infty} a_k = \infty$.*

(III) ***Quotientenkriterium*:** *Ist $a_k \neq 0$ für $k \gg 1$ und gilt $\limsup_{k\to\infty} \frac{|a_{k+1}|}{|a_k|} < 1$, so konvergiert $\sum_{k=k_0}^{\infty} a_k$.*

(IV) ***Wurzelkriterium*:** *Gilt $\limsup_{k\to\infty} \sqrt[k]{|a_k|} < 1$, so konvergiert $\sum_{k=k_0}^{\infty} a_k$.*

(V) ***Verdichtungskriterium*:** *Sei $\mathbb{K} = \mathbb{R}$. Ist (ein Endstück von) $(a_k)_{k\in\mathbb{Z}_{\geq k_0}}$* monotone Nullfolge *und ist $\ell_0 \in \mathbb{N}_0$ mit $2^{\ell_0} \geq k_0$, so konvergiert $\sum_{k=k_0}^{\infty} a_k$ genau dann, wenn auch die verdichtete Reihe $\sum_{\ell=\ell_0}^{\infty} 2^{\ell} a_{2^\ell}$ konvergiert.*

(VI) ***Leibniz-Kriterium*:** *Sei $\mathbb{K} = \mathbb{R}$. Ist (ein Endstück von) $(a_k)_{k\in\mathbb{Z}_{\geq k_0}}$* monotone Nullfolge*, so konvergiert die **alternierende Reihe** $\sum_{k=k_0}^{\infty} (-1)^k a_k$.*

Beweise. Für das Majorantenkriterium (I) argumentieren wir so: Da $\sum_{k=k_0}^{\infty} b_k$ konvergiert, gibt das Cauchy-Kriterium $\lim_{n\geq m\to\infty} \sum_{k=m}^{n} b_k = 0$. Wegen $|\sum_{k=m}^{n} a_k| \leq \sum_{k=m}^{n} |a_k| \leq C \sum_{k=m}^{n} b_k$ für $n \geq m \gg 1$ folgt daraus $\lim_{n\geq m\to\infty} \sum_{k=m}^{n} a_k = 0$, und eine erneute Anwendung des Cauchy-Kriteriums gibt Konvergenz von $\sum_{k=k_0}^{\infty} a_k$.

Zur Herleitung des Minorantenkriterium (II) fixieren wir $m \in \mathbb{Z}_{\geq k_0}$ mit $a_k \geq cb_k$ für *alle* $k \in \mathbb{N}_{\geq m}$ und folglich $\sum_{k=m}^{n} a_k \geq c \sum_{k=m}^{n} b_k$ für $n \in \mathbb{N}_{\geq m}$. Die bestimmte Divergenz $\sum_{k=k_0}^{\infty} b_k = \infty$, die gemäß Grundeigenschaft (2) gleichbedeutend mit $\lim_{n\to\infty} \sum_{k=m}^{n} b_k = \infty$ ist, impliziert dann gemäß dem Minorantenkriterium des Abschnitts 5.1 für Unendlichfolgen auch $\lim_{n\to\infty} \sum_{k=m}^{n} a_k = \infty$ und $\sum_{k=k_0}^{\infty} a_k = \infty$.

In der Situation des Quotientenkriteriums (III) gibt es $q \in [0, 1)$ und $m \in \mathbb{N}$ mit $\frac{|a_{k+1}|}{|a_k|} \leq q$, also $|a_{k+1}| \leq q|a_k|$, für alle $k \in \mathbb{N}_{\geq m}$. Induktiv folgt $|a_k| \leq q^{k-m}|a_m| = Cq^k$ für $k \in \mathbb{N}_{\geq m}$, wobei $C := q^{-m}|a_m| \in \mathbb{R}_{\geq 0}$ fest ist. Somit lässt sich das Majorantenkriterium (I) mit der konvergenten geometrischen Reihe $\sum_{k=k_0}^{\infty} q^k$ als Majorantenreihe anwenden und gibt Konvergenz von $\sum_{k=k_0}^{\infty} a_k$.

Unter der Voraussetzung der Wurzelkriteriums gibt es $q \in [0,1)$ und $m \in \mathbb{N}$ mit $\sqrt[k]{|a_k|} \leq q$, also $|a_k| \leq q^k$, für alle $k \in \mathbb{N}_{\geq m}$. Daher greift erneut (I) mit Majorantenreihe $\sum_{k=k_0}^{\infty} q^k$.

Beim Beweis des Verdichtungskriteriums (V) behandeln wir in Anbetracht von Grundeigenschaft (2) nur $k_0 = 1$, $\ell_0 = 0$ und sowie eine fallende Nullfolge $(a_k)_{k\in\mathbb{N}_0}$ in $\mathbb{R}_{\geq 0}$. Nach dem Beschränktheitskriterium kann nun sowohl $\sum_{k=1}^{\infty} a_k$ als auch $\sum_{\ell=0}^{\infty} 2^\ell a_{2^\ell}$ nur gegen einen endlichen Wert konvergieren oder bestimmt gegen ∞ divergieren. Zudem lassen sich die zugehörigen Partialsummen mit $p \in \mathbb{N}$ durch Zusammenfassen von Reihengliedern in Gruppen gemäß

$$\begin{aligned}\sum_{k=1}^{2^p-1} a_k &= a_1 + (a_2{+}a_3) + (a_4{+}a_5{+}a_6{+}a_7) + \ldots + (a_{2^{p-1}}{+}a_{2^{p-1}+1}{+}\ldots{+}a_{2^p-2}{+}a_{2^p-1}) \\ &\leq a_1 + 2a_2 + 4a_4 + \ldots + 2^{p-1}a_{2^{p-1}} = \sum_{\ell=0}^{p-1} 2^\ell a_{2^\ell}\end{aligned}$$

und

$$\begin{aligned}\sum_{k=1}^{2^p} a_k &= a_1 + a_2 + (a_3{+}a_4) + (a_5{+}a_6{+}a_7{+}a_8) + \ldots + (a_{2^{p-1}+1}{+}a_{2^{p-1}+2}{+}\ldots{+}a_{2^p-1}{+}a_{2^p}) \\ &\geq \tfrac{1}{2}a_1 + a_2 + 2a_4 + 4a_8 \ldots + 2^{p-1}a_{2^p} = \frac{1}{2}\sum_{\ell=0}^{p} 2^\ell a_{2^\ell}\end{aligned}$$

von oben und unten durch einander abschätzen. Daher müssen $\sum_{k=1}^{\infty} a_k$ und $\sum_{\ell=0}^{\infty} 2^\ell a_{2^\ell}$ tatsächlich *beide* gegen einen endlichen Wert konvergieren oder *beide* bestimmt gegen ∞ divergieren.

Auch beim Leibniz-Kriterium (VI) behandeln wir ohne Einschränkung nur $k_0 = 0$ und eine fallende Nullfolge $(a_k)_{k\in\mathbb{N}}$ in $\mathbb{R}_{\geq 0}$. Mit den Partialsummen $s_n := \sum_{k=0}^{n}(-1)^k a_k$ bilden wir für $n \in \mathbb{N}_0$ Intervalle $I_n := [s_{2n+1}, s_{2n}]$, die wegen $s_{2n+1} = s_{2n}{-}a_{2n+1} \leq s_{2n}$ nicht-leer sind und wegen $s_{2(n+1)} = s_{2n}{-}a_{2n+1}{+}a_{2n+2} \leq s_{2n}$ und $s_{2(n+1)+1} = s_{2n+1}{+}a_{2n+2}{-}a_{2n+3} \geq s_{2n+1}$ zudem $I_{n+1} \subset I_n$ erfüllen. Aufgrund von $s_{2n} - s_{2n+1} = -a_{2n+1} \underset{n\to\infty}{\longrightarrow} 0$ bilden die Intervalle I_n sogar eine Intervallschachtelung. Mit deren Kern $s \in \mathbb{R}$ folgt $\lim_{n\to\infty} s_{2n+1} = s = \lim_{n\to\infty} s_{2n}$. Also konvergiert auch $\sum_{k=0}^{\infty}(-1)^k a_k = \lim_{n\to\infty} s_n$ mit Wert s. □

Bemerkungen und Beispiele (zu den **Konvergenzkriterien für Reihen**).

(1) Das Majorantenkriterium (I) und das Minorantenkriterium (II) sind oft nützlich, um über die Konvergenz oder Divergenz einer gegebenen Reihe durch Vergleich mit einfacheren und schon behandelten Reihen zu entscheiden. Beispiele hierzu sind Thema der Übungen.

(2) **Zahlen mit unendlich vielen Nachkommastellen** im (schon in Abschnitt 2.2 angesprochenen) Stellenwertsystem zu einer Basis $b \in \mathbb{N}\backslash\{1\}$ lassen sich **als Reihen**

$$(z_n z_{n-1} \ldots z_2 z_1 z_0, z_{-1} z_{-2} z_{-3} \ldots)_b := \sum_{i=-n}^{\infty} z_{-i} b^{-i}$$

mit $n \in \mathbb{N}_0$ und b-adischen Ziffern $z_i \in \{0, 1, 2, \ldots, b{-}2, b{-}1\}$ **präzise erklären**. Wegen $|z_{-i}b^{-i}| \leq b^{1-i}$ wird dabei die Konvergenz der auftretenden Reihe allgemein durch die Konvergenz der geometrischen Majorantenreihe $\sum_{i=-n}^{\infty} b^{-i}$ gesichert, und es ist nicht schwer zu zeigen, dass jede nichtnegative reelle Zahl eine Zifferndarstellung der obigen Form besitzt.

Ist $z_{-i} = 0$ für $i \gg 1$, so verzichtet man in der Notation auf das Endstück aus Nullen und schreibt die Zahl in üblicher Notation mit endlich vielen Nachkommastellen. Verschwinden mit $z_{-i} = 0$ für alle $i \in \mathbb{N}$ gar alle Nachkommaziffern, so liefert dies natürlich die aus Abschnitt 2.2 bekannte b-adische Darstellung natürlicher Zahlen zurück. Als Spezialfall sei noch erwähnt, dass wir im Dezimalsystem die bekannte **„Null-Komma-Periode-Neun-Problematik“** per geometrischer Reihe **präzise auflösen** können: Tatsächlich ist

$$0,99999999\ldots = \sum_{i=1}^{\infty} 9{\cdot}10^{-i} = 9\Big(\frac{1}{1-10^{-1}}-1\Big) = 1\,.$$

(3) Mit dem Quotientenkriterium (III) und dem Wurzelkriterium (IV) lassen sich — wie man aus dem Beweis abliest — gewisse Reihen behandeln, die eine geometrische Majorantenreihe besitzen. Der Hauptvorteil dieser beiden Kriterien besteht dabei in der Möglichkeit, sie recht schematisch einzusetzen. In interessanten Grenzfällen versagen sie aber oft und liefern dann auch kaum Ansatzpunkte für weitere Untersuchungen.

(4) Das Verdichtungskriterium (V) ergibt, dass die (speziellen) **Dirichlet-Reihen**

$$\sum_{k=1}^{\infty} \frac{1}{k^s} \qquad \text{mit } s \in \mathbb{R}$$

genau für $s > 1$ konvergent sind. Genauer ergibt das Kriterium erst, dass die geometrische Reihe $\sum_{\ell=0}^{\infty}(2^{1-s})^{\ell}$ dasselbe Konvergenzverhalten aufweist, und letztere konvergiert dann genau für $2^{1-s} < 1$, also mit anderen Worten genau für $s > 1$.

Durch $\zeta(s) := \sum_{k=1}^{\infty} \frac{1}{k^s} \in \mathbb{R}_{>0}$ sind übrigens auch die Werte der **Riemannschen Zeta-Funktion** ζ auf $\mathbb{R}_{>1}$ gegeben. Es handelt sich dabei um eine berühmte komplexe Funktion, die in der Zahlentheorie große Bedeutung besitzt und später in natürlicher Weise auf ganz $\mathbb{C}\backslash\{1\}$ fortgesetzt und weiter untersucht werden kann. Die Werte von ζ auf geraden natürlichen Zahlen gibt Eulers erstaunliche Formel $\zeta(2k) = \frac{(-1)^{k-1}2^{2k-1}b_{2k}}{(2k)!}\pi^{2k}$ für $k \in \mathbb{N}$ mit den Bernoulli-Zahlen b_k (während über die Werte auf ungeraden natürlichen Zahlen wenig bekannt ist). Speziell gelten

$$\sum_{k=1}^{\infty} \frac{1}{k^2} = 1+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}+\ldots = \zeta(2) = \frac{\pi^2}{6} \qquad \text{und} \qquad \sum_{k=1}^{\infty} \frac{1}{k^4} = 1+\frac{1}{16}+\frac{1}{81}+\frac{1}{256}+\ldots = \zeta(4) = \frac{\pi^4}{90}\,.$$

(5) Das Leibniz-Kriterium (VI) zeigt (zusammen mit dem Nullfolgenkriterium), dass die alternierenden Reihen

$$\sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k^s} \qquad \text{und} \qquad \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k+1)^s} \qquad \text{mit } s \in \mathbb{R}$$

genau für $s > 0$ konvergent sind. Speziell konvergieren die **alternierende harmonische Reihe**

$$\sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} \pm \ldots\,,$$

deren Wert in den Übungen zu $\log 2$ bestimmt wird, und die **Leibnizsche Reihe**

$$\sum_{k=0}^{\infty} \frac{(-1)^k}{2k+1} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} \pm \ldots\,,$$

auf deren Wert $\frac{\pi}{4}$ am Ende von Abschnitt 5.6 zumindest ansatzweise eingegangen wird.

Als Nächstes erklären wir ein Konzept besonders gutartiger Konvergenz.

Definition (absolute Konvergenz). *Sei $k_0 \in \mathbb{Z}$, und sei $(a_k)_{k\in\mathbb{Z}_{\geq k_0}}$ eine Folge in $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$. Dann heißt $\sum_{k=k_0}^{\infty} a_k$ **absolut konvergent**, wenn die Reihe der Beträge $\sum_{k=k_0}^{\infty} |a_k|$ konvergiert.*

Bemerkungen und Beispiele (zu **absoluter Konvergenz**).

(1) Aus dem Majorantenkriterium (I) (mit $b_k = |a_k|$) folgt, dass eine **absolute konvergente Reihe** $\sum_{k=k_0}^{\infty} a_k$ **stets konvergent** ist. Durch Grenzübergang in der Dreiecksungleichung für endliche (Partial-)Summen ergibt sich für solche Reihen zudem die **Dreiecksungleichung**

$$\left| \sum_{k=k_0}^{\infty} a_k \right| \leq \sum_{k=k_0}^{\infty} |a_k| \,.$$

(2) Die Kriterien (I), (III), (IV), (V) des letzten Satzes (also Majoranten-, Quotienten-, Wurzel-, und Verdichtungskriterium) erfassen mit einer Reihe stets auch die zugehörige Reihe der Beträge und geben daher stets absolute Konvergenz. (Bei den ersten drei Kriterien liegt dies daran, dass überhaupt nur die Beträge der Glieder auftreten. Beim Verdichtungskriterium folgt es, weil fast alle Glieder a_k der monotonen Nullfolge gleiches Vorzeichen haben müssen).

(3) Das Leibniz-Kriterium erfasst auch einige **konvergente, aber nicht absolut konvergente Reihen** wie beispielsweise die Reihen $\sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k^s}$ und $\sum_{k=0}^{\infty} \frac{(-1)^k}{(2k+1)^s}$ mit $s \in (0, 1]$ (für die sich dieses Verhalten aus den vorausgehenden Punkten (4) und (5) ergibt).

Für einige weitere Sachverhalte bei Reihen ist eine allgemeine Definition nützlich, die wir an dieser Stelle kurz einschieben:

Definition (Positiv- und Negativteil). *Für $x \in \mathbb{R}$ erklären wir den **Positivteil** x_+ von x und den **Negativteil** x_- von x durch*

$$x_+ := \max\{x, 0\} \in \mathbb{R}_{\geq 0} \qquad \text{und} \qquad x_- := \max\{-x, 0\} \in \mathbb{R}_{\geq 0} \,.$$

Damit bekommen wir die Zerlegungen

$$x = x_+ - x_- \qquad \text{und} \qquad |x| = x_+ + x_- \qquad \text{für jedes } x \in \mathbb{R} \,.$$

Als Nächstes beschäftigen wir uns mit der Frage, ob Konvergenz und Wert einer Reihe von der Reihenfolge abhängen, in der die Summanden addiert werden. Wie wir sehen werden, lässt sich dies nicht allgemein bejahen oder verneinen, sondern die Antwort hängt ganz wesentlich davon ab, wie gutartig die Konvergenz der betreffenden Reihe ist. Wir machen dies im nächsten Satz präzise, prägen dafür aber zunächst noch ein zugehöriges Konzept.

Definition (Umordnungen von Reihen). *Für $k_0, \ell_0 \in \mathbb{Z}$ seien $(a_k)_{k\in\mathbb{Z}_{\geq k_0}}$ und $(b_\ell)_{\ell\in\mathbb{Z}_{\geq \ell_0}}$ Folgen in $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$. Dann heißt $\sum_{\ell=\ell_0}^{\infty} b_\ell$ eine **Umordnung** von $\sum_{k=k_0}^{\infty} a_k$, wenn es eine Bijektion $\pi\colon \mathbb{Z}_{\geq \ell_0} \to \mathbb{Z}_{\geq k_0}$ mit $b_\ell = a_{\pi(\ell)}$ für alle $\ell \in \mathbb{Z}_{\geq \ell_0}$ gibt.*

Satz (über **Umordnungen von Reihen**). *Sei $k_0 \in \mathbb{Z}$, und sei $(a_k)_{k\in\mathbb{Z}_{\geq k_0}}$ eine Folge in $\mathbb{R}$.*

(I) *Gilt entweder $\sum_{k=k_0}^{\infty}(a_k)_+ < \infty$ oder $\sum_{k=k_0}^{\infty}(a_k)_- < \infty$, so haben alle Umordnungen von $\sum_{k=k_0}^{\infty} a_k$ das gleiche Konvergenzverhalten und den gleichen Wert wie $\sum_{k=k_0}^{\infty} a_k$ selbst. Insbesondere greift dies in den Fällen, dass entweder $a_k \geq 0$ für $k \gg 1$ gilt, $a_k \leq 0$ für $k \gg 1$ gilt oder $\sum_{k=k_0}^{\infty} a_k$ **absolut** konvergiert.*

(II) ***Riemannscher Umordnungssatz:** Ist $\sum_{k=k_0}^{\infty} a_k$ konvergent, aber **nicht absolut** konvergent, so gibt es für **jedes** $s \in \overline{\mathbb{R}}$ Umordnungen von $\sum_{k=k_0}^{\infty} a_k$ mit Wert s und auch unbestimmt divergente Umordnungen von $\sum_{k=k_0}^{\infty} a_k$.*

Hier sagt Teil (I), dass in den dort erfassten Fällen die Reihenfolge der Summation irrelevant ist und durch Umordnungen keine Probleme entstehen. Insbesondere erweisen sich die absolut konvergenten Reihen als **unbedingt konvergente Reihen**, bei denen jede Umordnung gegen den gleichen endlichen Wert konvergiert. Dagegen kann **bei *nicht-absoluter* Konvergenz** gemäß Teil (II) **durch Umordnung „alles maximal schiefgehen“**, und die nicht-absolut konvergenten Reihen sind **bedingt konvergente Reihen**, die zwar konvergieren, aber Umordnungen mit unterschiedlichem Verhalten und unterschiedlichen Werten besitzen.

Beweis von Teil (I) des Satzes. Wir behandeln erst den Fall, dass $a_k \geq 0$ für alle $k \in \mathbb{Z}_{\geq k_0}$ gilt. Da dann nur Konvergenz oder unbestimmte Divergenz gegen ∞ in Frage kommen, können wir das Konvergenzverhalten am Wert festmachen und müssen nur die Übereinstimmung der Werte zeigen. Der Schlüssel hierzu ist die Darstellung

$$\sum_{k=k_0}^{\infty} a_k = \lim_{n\to\infty} \sum_{k=k_0}^{n} a_k = \sup\left\{ \sum_{k=k_0}^{n} a_k \,\middle|\, n \in \mathbb{N} \right\} = \sup\left\{ \sum_{k\in E} a_k \,\middle|\, E \subset \mathbb{Z}_{\geq k_0}\,,\ |E| < \infty \right\}.$$

der Reihe $\sum_{k=k_0}^{\infty} a_k$ als Supremum endlicher Summen über beliebige endliche Teilmengen E der Indexmenge $\mathbb{Z}_{\geq k_0}$. Beim letzten „=“ gilt hier „$\leq$“, weil jede Partialsummen $\sum_{k=k_0}^{n} a_k$ der Reihe gleich einer endlichen Summe $\sum_{k\in E} a_k$ mit $E = \{k_0, k_0{+}1, \ldots, n\}$ ist, und „$\geq$“ gilt, weil jede endliche Summe $\sum_{k\in E} a_k$ kleiner oder gleich einer Partialsumme $\sum_{k=k_0}^{n} a_k$ mit $n = \max E$ ist. Ist $\ell_0 \in \mathbb{Z}$ und $\pi\colon \mathbb{Z}_{\geq \ell_0} \to \mathbb{Z}_{\geq k_0}$ eine Bijektion, so können wir obige Darstellung auch auf die Umordnung $\sum_{\ell=\ell_0} a_{\pi(\ell)}$ anwenden. Mit der Bijektivität von π ergibt sich dann

$$\begin{aligned}\sum_{\ell=\ell_0}^{\infty} a_{\pi(\ell)} &= \sup\left\{ \sum_{\ell\in F} a_{\pi(\ell)} \,\middle|\, F \subset \mathbb{Z}_{\geq \ell_0}\,,\ |F| < \infty \right\} = \sup\left\{ \sum_{k\in\pi(F)} a_k \,\middle|\, F \subset \mathbb{Z}_{\geq \ell_0}\,,\ |F| < \infty \right\} \\ &= \sup\left\{ \sum_{k\in E} a_k \,\middle|\, E \subset \mathbb{Z}_{\geq k_0}\,,\ |E| < \infty \right\} = \sum_{k=k_0}^{\infty} a_k\,,\end{aligned}$$

also die behauptete Übereinstimmung der Werte.

Die allgemeine Aussage führen wir durch Zerlegung in Positiv- und Negativteil auf das Vorige zurück. Zunächst ist bei $\sum_{k=k_0}^{\infty} a_k = \sum_{k=k_0}(a_k)_+ - \sum_{k=k_0}(a_k)_-$ wegen der gemachten Voraussetzung das Auftreten von $\infty{-}\infty$ ausgeschlossen, und die Reihe ist konvergent oder bestimmt divergent mit definiertem Wert in $\overline{\mathbb{R}}$. Da wir die Reihen mit Gliedern $(a_k)_\pm \geq 0$ nach dem schon Gezeigten ohne Änderung des Wertes umordnen dürfen, folgt dasselbe für jede Umordnung $\sum_{\ell=\ell_0}^{\infty} a_{\pi(\ell)}$ (mit $\ell_0 \in \mathbb{Z}$ und Bijektion $\pi\colon \mathbb{Z}_{\geq \ell_0} \to \mathbb{Z}_{\geq k_0}$) samt der behaupteten Übereinstimmung

$$\sum_{\ell=\ell_0}^{\infty} a_{\pi(\ell)} = \sum_{\ell=\ell_0}^{\infty} \big(a_{\pi(\ell)}\big)_+ - \sum_{\ell=\ell_0}^{\infty} \big(a_{\pi(\ell)}\big)_- = \sum_{k=k_0}^{\infty} (a_k)_+ - \sum_{k=k_0}^{\infty} (a_k)_- = \sum_{k=k_0}^{\infty} a_k\,. \qquad \square$$

Beweisskizze zu Teil (II) des Satzes. Wir beobachten zunächst: Die nicht-absolute Konvergenz von $\sum_{k=k_0}^{\infty} a_k$ erzwingt, dass $\sum_{k=k_0}^{\infty} (a_k)_+ = \infty$ *und* $\sum_{k=k_0}^{\infty} (a_k)_- = \infty$ gelten, denn in allen anderen Fällen ergäbe die frühere Grundeigenschaft (1) entweder $\sum_{k=k_0}^{\infty} |a_k| < \infty$ oder $\sum_{k=k_0}^{\infty} a_k = \pm\infty$.

Wir konstruieren nun eine Umordnung mit beliebig gegebenem Wert $s \in \mathbb{R}$. Die Grundidee hierzu ist, eine Indexfolge $n_1 < n_2 < n_3 < n_4 \ldots$ in $\mathbb{Z}_{\geq k_0}$ und zugehörige umgeordnete Partialsummen $s_{n_i} := \sum_{\ell=1}^{n_i} a_{\pi(\ell)}$ zu wählen, für die $s_{n_1}, s_{n_3}, s_{n_5}, \ldots > s$ und $s_{n_2}, s_{n_4}, s_{n_6}, \ldots < s$ gelten, also s_{n_i} abwechselnd größer und kleiner als s ist. Hierzu sollen abwechselnd nur Summanden ≥ 0 und nur Summanden < 0 zusätzlich addiert werden (wobei unwichtige Null-Summanden per Konvention dem ersten Fall zugeschlagen wurden), es sollen also etwa $a_{\pi(1)}, a_{\pi(2)}, \ldots, a_{\pi(n_1)}, a_{\pi(n_2+1)}, a_{\pi(n_2+2)}, \ldots, a_{\pi(n_3)} \geq 0$ und $a_{\pi(n_1+1)}, a_{\pi(n_1+2)}, \ldots, a_{\pi(n_2)}, a_{\pi(n_3+1)}, a_{\pi(n_3+2)}, \ldots, a_{\pi(n_4)} \leq 0$ gelten. Um dies zu erreichen, gehen wir im i-ten Schritt tatsächlich von s_{i-1} aus und bilden s_i durch Hinzunahme von noch nicht verwendeten Summanden a_k passenden

Vorzeichens, die dann umnummeriert und als $a_{\pi(\ell)}$ in die Umordnung eingefügt werden. Wegen $\sum_{k=m}^{\infty}(a_k)_+ = \infty$ und $\sum_{k=m}^{\infty}(a_k)_- = \infty$ für jedes $m \in \mathbb{N}$ können wir dabei mit dem verbleibenden Vorrat an Summanden immer wieder eine Summe $> s$ bzw. $< s$ erreichen. Um die Wahl der Summanden $a_{\pi(\ell)}$ eindeutig festzulegen, vereinbaren wir tatsächlich, unter den Summanden a_k, die das richtige Vorzeichen haben und noch nicht verwendet wurden, die mit den kleinsten Indizes k zu verwenden und das im jeweiligen Schritt nur, bis die Summe *erstmals* $> s$ bzw. *erstmals* $< s$ ist. Damit erreichen wir auch, dass alle Summanden a_k irgendwann vorkommen, so dass die Umnummerierung π bijektiv und $\sum_{\ell=1}^{\infty} a_{\pi(\ell)}$ tatsächlich eine Umordnung von $\sum_{k=k_0}^{\infty} a_k$ wird. Nun bringen wir noch ein, dass gemäß Nullfolgenkriterium $\lim_{k\to\infty} a_k = 0$ und für beliebiges $\varepsilon \in \mathbb{R}_{>0}$ folglich $|a_{\pi(\ell)}| < \varepsilon$ für $\ell \gg 1$ gilt. Da die s_{n_i} den Wert s erst durch Addition des letzten Summanden über- oder unterschreiten, erhalten $|s_{n_i} - s| < \varepsilon$ für $i \gg 1$ und wegen Monotonie der Partialsummen zwischen benachbarten s_{n_i} dann auch $\left|\sum_{\ell=1}^{n} a_{\pi(\ell)} - s\right| < \varepsilon$ für $n \gg 1$. Dies zeigt die behauptete Konvergenz $\sum_{\ell=1}^{\infty} a_{\pi(\ell)} = s$.

Eine Umordnung mit Wert ∞ lässt sich ganz ähnlich konstruieren. Wir fügen dazu wie zuvor abwechselnd *nicht*negative und negative Summanden hinzu, erzeugen jetzt mit entsprechender Abbruchbedingung aber Partialsummen $s_{n_1} > 2$, $s_{n_2} < 1$, $s_{n_3} > 4$, $s_{n_4} < 3$, $s_{n_5} > 6$, $s_{n_6} < 5$, $s_{n_7} > 8$, $s_{n_8} < 7$, und so weiter. Analog erhalten wir eine Umordnung mit Wert $-\infty$. Für eine bestimmt divergente Umordnung schließlich erzeugen wir mit demselben Verfahren Partialsummen $s_{n_1} > 1$, $s_{n_2} < 0$, $s_{n_3} > 1$, $s_{n_4} < 0$, $s_{n_5} > 1$, $s_{n_6} < 0$, $s_{n_7} > 1$, $s_{n_8} < 0$, und so weiter. □

Bemerkung (zur **Umordnung von Reihen mit komplexen Gliedern**). Durch Zerlegung in Real- und Imaginärteil kann Teil (I) des vorigen Satzes auf Reihen $\sum_{k=k_0}^{\infty} a_k$ mit komplexen Gliedern $a_k \in \mathbb{C}$ verallgemeinert werden. Dafür müssen natürlich die Voraussetzungen des Teils (I) für die Reihen $\sum_{k=k_0}^{\infty} \mathcal{R}e(a_k)$ und $\sum_{k=k_0}^{\infty} \mathit{Im}(a_k)$ der Real- und Imaginärteile vorliegen, was wegen $|\mathcal{R}e(z)| \le |z|$ und $|\mathit{Im}(z)| \le |z|$ für $z \in \mathbb{C}$ insbesondere dann der Fall ist, wenn $\sum_{k=k_0}^{\infty} a_k$ *absolut* konvergiert.

Tatsächlich können wir die Sachlage bei Umordnungen besser verstehen (und in Folge auch weitere Resultate zu Reihen herleiten), wenn wir unendliche Summen noch einmal neu auf etwas andere Art und Weise einführen:

Definition (**Summation über allgemeine Indexmengen**). *Summen $\sum_{k\in I} a_k$ mit einer beliebigen[10] Menge I als Indexmenge können wir in Anlehnung an (den Beweis von) Teil (I) des vorigen Satzes mit folgendem mehrschrittigen Vorgehen erklären*:

- *Bei **nichtnegativen Gliedern** $a_k \in \mathbb{R}_{\ge 0}$ für $k \in I$ setzen wir*

$$\sum_{k\in I} a_k := \sup\left\{ \sum_{k\in E} a_k \,\middle|\, E \subset I\,,\ |E| < \infty \right\} \in [0,\infty]\,.$$

- *Bei **allgemeinen reellen Gliedern** $a_k \in \mathbb{R}$ für $k \in I$ definieren wir darauf aufbauend*

$$\sum_{k\in I} a_k := \sum_{k\in I} (a_k)_+ - \sum_{k\in I} (a_k)_- \in \overline{\mathbb{R}}\,,$$

  sofern *entweder $\sum_{k\in I}(a_k)_+ < \infty$ oder $\sum_{k\in I}(a_k)_- < \infty$ gilt. Im komplementären Fall mit $\sum_{k\in I}(a_k)_+ = \sum_{k\in I}(a_k)_- = \infty$ bleibt $\sum_{k\in I}(a_k)$ undefiniert (vom Typ $\infty-\infty$).*

- *Bei **komplexen Gliedern** $a_k \in \mathbb{C}$ für $k \in I$ definieren wir in weiterer Verallgemeinerung*

$$\sum_{k\in I} a_k := \sum_{k\in I} \mathcal{R}e(a_k) + \mathbf{i}\sum_{k\in I} \mathit{Im}(a_k) \in \mathbb{C}\,,$$

  sofern *$\sum_{k\in I} \mathcal{R}e(a_k)$ und $\sum_{k\in I} \mathit{Im}(a_k)$ von definiertem Typ mit endlichem Wert in $\mathbb{R}$ sind.*

[10] Von Interesse sind vor allem Summen über *abzählbare* Indexmengen. Dies erklärt sich daraus, dass $\sum_{k\in I} a_k$ — wie ein kurzer Widerspruchsbeweis auf Basis der Definition zeigt — nur dann einen definierten *endlichen* Wert in $\mathbb{R}$ oder $\mathbb{C}$ haben kann, wenn die „wirklich relevante“ Indexmenge $\{k \in I \,|\, a_k \neq 0\}$ abzählbar ist.

Bemerkungen (zur **Summation über allgemeine Indexmengen**)**.** Direkt aus der Definition allgemeiner Summen ergeben sich einige Folgerungen:

(1) Für Indexmengen $I = \mathbb{Z}_{\geq k_0}$ mit $k_0 \in \mathbb{Z}$ ergibt sich aus dem vorigen Beweis (erst für nichtnegative Glieder und dann allgemein), dass die allgemeine Summation mit der Summation im Sinn einer Reihe übereinstimmt. Der einzige Unterschied besteht bei Gliedern $a_k \in \mathbb{R}$ im Fall $\sum_{k=k_0}^{\infty} (a_k)_+ = \sum_{k=k_0}^{\infty} (a_k)_- = \infty$: Die allgemeine Summe $\sum_{k \in \mathbb{Z}_{\geq k_0}} a_k$ ist dann undefiniert „$\infty - \infty$“, während bei der Reihe $\sum_{k=k_0}^{\infty} a_k$ die drei Möglichkeiten[11] unbestimmte Divergenz, bestimmte Divergenz gegen ∞ oder $-\infty$ und nicht-absolute Konvergenz gegen einen Wert in $\mathbb{R}$ verbleiben.

(2) Allgemeine Summen können beliebig in Teilsummen aufgeteilt uns zusammengefasst werden, genauer gilt für eine Familie $(I_\ell)_{\ell \in J}$ disjunkter Indexmengen I_ℓ stets

$$\sum_{k \in \dot{\bigcup}_{\ell \in J} I_\ell} a_k = \sum_{\ell \in J} \left(\sum_{k \in I_\ell} a_k \right),$$

sofern eine Seite der Gleichung definiert ist.

(3) Im Fall der Indexmenge $I = \mathbb{N}_0 \times \mathbb{N}_0$ erhalten wir den **Doppelreihensatz**: Für eine Familie $(a_{k,\ell})_{(k,\ell) \in \mathbb{N}_0 \times \mathbb{N}_0}$ reeller oder komplexer Zahlen gilt

$$\sum_{k,\ell=0}^{\infty} a_{k,\ell} = \sum_{k=0}^{\infty} \left(\sum_{\ell=0}^{\infty} a_{k,\ell} \right) = \sum_{\ell=0}^{\infty} \left(\sum_{k=0}^{\infty} a_{k,\ell} \right) = \sum_{m=0}^{\infty} \left(\sum_{k=0}^{m} a_{k,m-k} \right),$$

sobald nur bei einer dieser Summationsweisen die Summe entweder der Positivteile $(a_{k,\ell})_+$ oder der Negativteile $(a_{k,\ell})_-$ endlich ist. Dabei soll die Summe ganz links nur als andere Schreibweise für die allgemeine Summation über $\mathbb{N}_0 \times \mathbb{N}_0$ verstanden werden. Die anderen Terme sind über Reihen (und eine endliche Summe) erklärt und entsprechenden der **zeilenweisen Summation**, der **spaltenweisen Summation** und einer **diagonalen Summation** in folgendem Schema:

$$\begin{array}{cccccccc} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} & a_{0,4} & a_{0,5} & \dots \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} & a_{1,5} & \dots \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} & a_{2,5} & \dots \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} & a_{3,5} & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{array}.$$

Speziell kann der Doppelreihensatz auf Reihenglieder der Produkt-Form $a_{k,\ell} = a_k b_\ell$ angewandt werden und gibt dann zusammen mit Umformungen durch das Herausziehen konstanter Faktoren den folgenden Sachverhalt: Für zwei *absolut* konvergente Reihen $\sum_{k=0}^{\infty} a_k$ und $\sum_{\ell=0}^{\infty} b_\ell$ reeller oder komplexer Zahlen a_k und b_ℓ ist auch die Reihe $\sum_{m=0}^{\infty} \left(\sum_{k=0}^{m} a_k b_{m-k} \right)$ mit Gliedern $\sum_{k=0}^{m} a_k b_{m-k}$ absolut konvergent und erfüllt

$$\sum_{m=0}^{\infty} \left(\sum_{k=0}^{m} a_k b_{m-k} \right) = \left(\sum_{k=0}^{\infty} a_k \right) \left(\sum_{\ell=0}^{\infty} b_\ell \right).$$

Man nennt $\sum_{m=0}^{\infty} \left(\sum_{k=0}^{m} a_k b_{m-k} \right)$ das **Cauchy-Produkt** von $\sum_{k=0}^{\infty} a_k$ und $\sum_{\ell=0}^{\infty} b_\ell$.

[11] Ist die Reihe $\sum_{k=k_0}^{\infty} a_k$ in diesem Fall bestimmt divergent oder nicht-absolut konvergent, so kann man sich vorstellen, dass eine gewisse „Verrechnung“ $\infty - \infty$ durch starke Kürzungseffekte bei den Partialsummen zustande kommt. Gemäß Teil (II) des vorigen Satzes hängt dabei das Ergebnis sehr stark an der Reihenfolge der Glieder.

Am Ende dieses Abschnitts gehen wir ganz kurz auf multiplikative Analoga zu Reihen ein:

Bemerkungen (zu **unendlichen Produkten**).

(1) Ein **unendliches Produkt** $\prod_{k=k_0}^{\infty} a_k$ mit Startindex $k_0 \in \mathbb{Z}$ und reellen oder komplexen Faktoren a_k erklären wir als

$$\prod_{k=k_0}^{\infty} a_k := \lim_{n\to\infty} \prod_{k=k_0}^{n} a_k \,,$$

falls der Limes der Partialprodukte auf der rechten Seite existiert. Im Fall positiver reeller Faktoren $a_k \in \mathbb{R}_{>0}$ können unendliche Produkte **auf Reihen zurückgeführt** werden, denn per Logarithmus-Rechenregel folgt

$$\log \prod_{k=k_0}^{\infty} a_k = \sum_{k=k_0}^{\infty} \log a_k$$

(sofern eine Seite existiert und eventuell mit Verständnis $\log 0 = -\infty$ sowie $\log \infty = \infty$).

(2) Als konkretes Beispiel (aus dem wir gleich noch eine interessante Folgerung ziehen) betrachten wir das Teleskopprodukt

$$\prod_{k=1}^{\infty} \left(1+\frac{1}{k}\right) = \prod_{k=1}^{\infty} \frac{k+1}{k} = \lim_{n\to\infty} \frac{n+1}{1} = \infty$$

und erhalten durch Logarithmieren gemäß Bemerkung (1) dann $\sum_{k=1}^{\infty} \log(1+\frac{1}{k}) = \infty$. Damit ergibt sich ein eleganter **neuer Beweis für die Divergenz der harmonischen Reihe** $\sum_{k=1}^{\infty} \frac{1}{k} = \infty$, denn gemäß der fundamentalen Logarithmus-Ungleichung gilt $\frac{1}{k} \geq \log(1+\frac{1}{k})$ für alle $k \in \mathbb{N}$, womit sich $\sum_{k=1}^{\infty} \log(1+\frac{1}{k})$ als divergente Minorante für $\sum_{k=1}^{\infty} \frac{1}{k}$ erweist.

5.6 Funktionenfolgen und Potenzreihen

Das Konzept der Konvergenz kann von Folgen und Reihen in $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$ auf Folgen und Reihen $\mathbb{K}$-wertiger Funktionen ausgedehnt werden und wird sich auch in dieser größeren Allgemeinheit noch verschiedentlich als sehr wichtig erweisen.

Definitionen (**Konvergenz von Funktionenfolgen und Funktionenreihen**). *Seien $\mathcal{X}$ eine Menge, $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$ und $(f_n)_{n\in\mathbb{N}}$ eine (Funktionen-)Folge in* $\mathrm{Abb}(\mathcal{X}, \mathbb{K})$.

(I) *Dass die Folge $(f_n)_{n\in\mathbb{N}}$* ***punktweise*** *auf $\mathcal{X}$ gegen eine Grenzfunktion $f \in \mathrm{Abb}(\mathcal{X}, \mathbb{K})$* ***konvergiert****, bedeutet*

$$\lim_{n\to\infty} f_n(x) = f(x) \qquad \textit{für alle } x \in \mathcal{X} \,.$$

(II) *Dass die Folge $(f_n)_{n\in\mathbb{N}}$* ***gleichmäßig*** *auf $\mathcal{X}$ gegen eine Grenzfunktion $f \in \mathrm{Abb}(\mathcal{X}, \mathbb{K})$* ***konvergiert****, bedeutet*

$$\lim_{n\to\infty} \left(\sup_{x\in\mathcal{X}} |f_n(x) - f(x)| \right) = 0 \,.$$

In beiden Fällen notieren wir $\lim_{n\to\infty} f_n = f$ oder gleichbedeutend $f_n \underset{n\to\infty}{\longrightarrow} f$ und kennzeichnen die Art der Konvergenz durch Hinzusetzen von „punktweise auf $\mathcal{X}$“ oder „gleichmäßig auf $\mathcal{X}$“.

Für $k_0 \in \mathbb{Z}$ und eine Folge $(g_k)_{k\in\mathbb{Z}_{\geq k_0}}$ in $\mathrm{Abb}(\mathcal{X},\mathbb{K})$ erklären wir die punktweise bzw. gleichmäßige Konvergenz der (Funktionen-)Reihe $\sum_{k=k_0}^{\infty} g_k$ als die punktweise bzw. gleichmäßige Konvergenz der Partialsummenfolge $(\sum_{k=k_0}^{n} g_k)_{n\in\mathbb{Z}_{\geq k_0}}$. Wir notieren bei derart konvergenten Reihen auch $\sum_{k=k_0}^{\infty} g_k := \lim_{n\to\infty} \sum_{k=k_0}^{n} g_k$ für die Grenzfunktion.

Bemerkungen (zur **Konvergenz von Funktionenfolgen**)**.**

(1) Die **Grenzfunktion** einer Funktionenfolge oder Funktionenreihe ist, wenn sie existiert, **stets eindeutig bestimmt**.

(Für punktweise Konvergenz folgt dies direkt aus der Eindeutigkeit des Grenzwerts von Zahlenfolgen. Für gleichmäßige Konvergenz gilt es nach der folgenden Bemerkung (3) erst recht.)

(2) **Punktweise Konvergenz** $\lim_{n\to\infty} f_n = f$ auf $\mathcal{X}$ lässt sich mit Quantoren als

$$\forall x \in \mathcal{X}\colon \forall \varepsilon \in \mathbb{R}_{>0}\colon \exists n_0 \in \mathbb{N}\colon \forall n \in \mathbb{N}_{\geq n_0}\colon |f_n(x)-f(x)| < \varepsilon$$

ausschreiben, **gleichmäßige Konvergenz** $\lim_{n\to\infty} f_n = f$ auf $\mathcal{X}$ als

$$\forall \varepsilon \in \mathbb{R}_{>0}\colon \exists n_0 \in \mathbb{N}\colon \forall n \in \mathbb{N}_{\geq n_0}\colon \forall x \in \mathcal{X}\colon |f_n(x)-f(x)| < \varepsilon$$

(wobei man mit der Definition des Supremums zunächst nur $\leq \varepsilon$ bekäme, wegen der Beliebigkeit von ε aber tatsächlich auch $< \varepsilon$ schreiben kann).

Der Unterschied zwischen diesen Bedingungen besteht darin, dass der All-Quantor $\forall x \in \mathcal{X}$ einmal am Anfang, einmal am Ende der Quantoren-Abfolge steht, wobei die Vertauschung von $\forall x \in \mathcal{X}$ mit den anderen All-Quantoren $\forall \varepsilon \in \mathbb{R}_{>0}$ und $\forall n \in \mathbb{N}_{\geq n_0}$ tatsächlich nichts ändert, die Vertauschung von $\forall x \in \mathcal{X}$ mit dem Existenz-Quantor $\exists n_0 \in \mathbb{N}$ aber ganz entscheidend ist. Letztere führt zum wesentlichen Unterschied, dass **n_0 bei punktweiser Konvergenz** von ε und **von der betrachteten Stelle x abhängen darf**, während **n_0 bei gleichmäßiger Konvergenz** nur von ε, aber eben **nicht von x abhängen darf**. Dies erklärt auch die Benennung als punktweise und gleichmäßige Konvergenz: Bei punktweiser Konvergenz fordert man die Existenz eines n_0 (und auch überhaupt die Konvergenz) für jeden Punkt $x \in \mathcal{X}$ einzeln, bei gleichmäßiger Konvergenz fordert man die Existenz eines (bei gegebenem ε) universellen n_0, das dann für alle $x \in \mathcal{X}$ gleichermaßen funktioniert.

(3) Nach Bemerkung (2) ist klar: **Aus gleichmäßiger Konvergenz folgt punktweise Konvergenz.**

(4) Zur **Veranschaulichung gleichmäßiger Konvergenz** $\lim_{n\to\infty} f_n = f$ für Funktionen $f_n, f \in \mathrm{Abb}(\mathcal{X},\mathbb{R})$ auf $\mathcal{X} \subset \mathbb{R}$ halten wir fest, dass für jedes $\varepsilon \in \mathbb{R}_{>0}$ die Graphen von f_n mit $n \gg 1$ in einem **„2ε-Schlauch“** der Höhe 2ε **um den Graph von f als Mittellinie** bleiben. Dieses Verhalten wird in Abbildung 36 angedeutet.

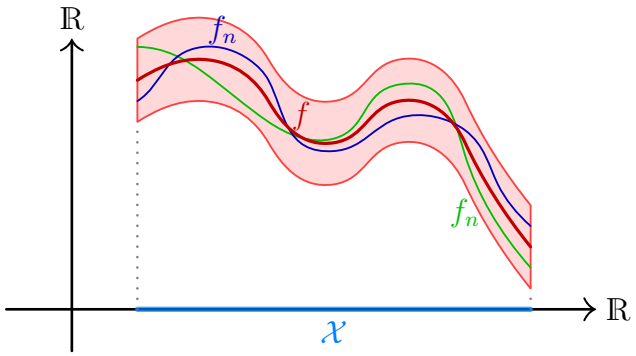


Abb. 36: Darstellung gleichmäßiger Konvergenz $\lim_{n\to\infty} f_n = f$ auf $\mathcal{X} \subset \mathbb{R}$ mit „2ε-Schlauch“ um den Graph der Grenzfunktion $f\colon \mathcal{X} \to \mathbb{R}$ und Graphen zweier Funktionen $f_n\colon \mathcal{X} \to \mathbb{R}$ mit $n \gg 1$

(5) Man bezeichnet eine Folge $(f_n)_{n\in\mathbb{N}}$ in $\mathrm{Abb}(\mathcal{X},\mathbb{K})$ (mit Menge $\mathcal{X}$ und $\mathbb{K}\in\{\mathbb{R},\mathbb{C}\}$) als **gleichmäßige Cauchy-Folge** auf $\mathcal{X}$, wenn

$$\forall\varepsilon\in\mathbb{R}_{>0}\colon\exists n_0\in\mathbb{N}\colon\forall m,n\in\mathbb{N}_{\geq n_0}\colon\forall x\in\mathcal{X}\colon|f_n(x)-f_m(x)|<\varepsilon$$

gilt. Damit gilt das folgende **gleichmäßige Cauchy-Kriterium**: Eine Folge in $\mathrm{Abb}(\mathcal{X},\mathbb{K})$ konvergiert genau dann gleichmäßig auf $\mathcal{X}$ gegen eine Grenzfunktion in $\mathrm{Abb}(\mathcal{X},\mathbb{K})$, wenn sie eine gleichmäßige Cauchy-Folge auf $\mathcal{X}$ ist.

Beweis des gleichmäßigen Cauchy-Kriteriums. Bei gleichmäßiger Konvergenz $\lim_{n\to\infty} f_n = f$ auf $\mathcal{X}$ gibt es zu jedem $\varepsilon\in\mathbb{R}_{>0}$ ein $n_0\in\mathbb{N}$ mit $|f_n(x)-f(x)|<\frac{\varepsilon}{2}$ für alle $n\in\mathbb{N}_{\geq n_0}$ und alle $x\in\mathcal{X}$. Hieraus folgt per Dreiecksungleichung $|f_n(x)-f_m(x)|\leq|f_n(x)-f(x)|+|f_m(x)-f(x)|<\frac{\varepsilon}{2}+\frac{\varepsilon}{2}=\varepsilon$ alle $m,n\in\mathbb{N}_{\geq n_0}$ und alle $x\in\mathcal{X}$. Also ist $(f_n)_{n\in\mathbb{N}}$ gleichmäßige Cauchy-Folge auf $\mathcal{X}$.

Ist $(f_n)_{n\in\mathbb{N}}$ gleichmäßige Cauchy-Folge auf $\mathcal{X}$, so gibt es zu jedem $\varepsilon\in\mathbb{R}_{>0}$ ein $n_0\in\mathbb{N}$ mit $|f_n(x)-f_m(x)|<\frac{\varepsilon}{2}$ für alle $m,n\in\mathbb{N}_{\geq n_0}$ und alle $x\in\mathcal{X}$. Insbesondere ist $(f_n(x))_{n\in\mathbb{N}}$ für jedes feste $x\in\mathcal{X}$ eine Cauchy-Folge in $\mathbb{K}$. Nach dem Cauchy-Kriterium aus Abschnitt 5.1 existiert daher $f(x):=\lim_{m\to\infty} f_m(x)$ für jedes $x\in\mathcal{X}$ und definiert eine Funktion $f\in\mathrm{Abb}(\mathcal{X},\mathbb{K})$. Durch Grenzübergang $m\to\infty$ in der Ungleichung $|f_n(x)-f_m(x)|<\frac{\varepsilon}{2}$ erhalten wir $|f_n(x)-f(x)|\leq\frac{\varepsilon}{2}<\varepsilon$ für alle $n\in\mathbb{N}_{\geq n_0}$ und alle $x\in\mathcal{X}$. Also liegt gleichmäßige Konvergenz $\lim_{n\to\infty} f_n = f$ vor. (Wir haben in diesem zweiten Beweisteil nur deshalb mit $\frac{\varepsilon}{2}$ statt direkt mit ε begonnen, weil „$<$“ im Grenzwert zu „$\leq$“ wird und wir am Ende trotzdem mit einem „$<$“ herauskommen möchten. Man kann dies auch anders lösen.) □

Es gibt noch einige weitere Kriterien für die Konvergenz von Funktionenfolgen und Funktionenreihen. Auf solche soll hier aber nicht weiter eingegangen werden.

(6) **Gleichmäßige Konvergenz erlaubt oft die Vertauschung von Grenzwerten** (wofür auch implizit in Bildungen wie Supremum, Ableitung oder Integral enthaltene Grenzwerte in Frage kommen). Diese Rolle der gleichmäßigen Konvergenz wird sich erst im Verlauf der Nachfolge-Vorlesungen klarer herauskristallisieren.

Beispiel (für eine **punktweise, aber nicht gleichmäßig konvergente Folge**)**.** Für die durch

$$f_n(x) := \frac{1}{1+n^3\left(x-\frac{1}{n}\right)^2} = \frac{1}{n^3x^2-2n^2x+n+1} \qquad \text{für } x\in\mathbb{R}\,,\ n\in\mathbb{N}$$

gegebene Folge $(f_n)_{n\in\mathbb{N}}$ in $\mathrm{Abb}(\mathbb{R},\mathbb{R})$ gilt

$$\lim_{n\to\infty} f_n = 0$$

punktweise auf $\mathbb{R}$ (gemäß Grenzwertberechnung bei festem $x\in\mathbb{R}$), aber nicht gleichmäßig auf $\mathbb{R}$ (wegen $\sup_{x\in\mathbb{R}}|f_n(x)| = f_n\left(\frac{1}{n}\right) = 1$ für jedes $n\in\mathbb{N}$). Diese Konvergenz wird in Abbildung 37 illustriert.

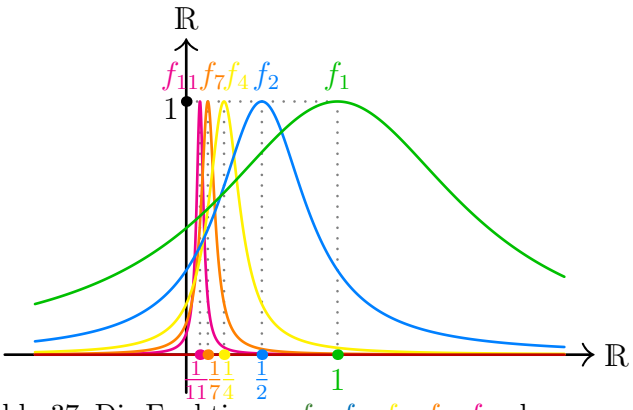


Abb. 37: Die Funktionen f_1, f_2, f_4, f_7, f_{11} der gegen die Nullfunktion konvergenten Beispielfolge $(f_n)_{n\in\mathbb{N}}$

Im Rest dieses Abschnitts beschäftigen wir uns hauptsächlich mit folgendem speziellen Typ von Funktionenreihen.

Definition (**Potenzreihen**)**.** *Eine* ***Potenzreihe*** *(in einer Variablen) ist formal durch einen* ***Entwicklungspunkt*** $a\in\mathbb{C}$ *und eine Folge* $(c_k)_{k\in\mathbb{N}_0}$ *von* ***Koeffizienten*** $c_0,c_1,c_2,c_3,\ldots\in\mathbb{C}$ *gegeben, mit denen für beliebiges* $z\in\mathbb{C}$ *die Reihe*

$$\sum_{k=0}^{\infty} c_k(z-a)^k = c_0 + c_1(z-a) + c_2(z-a)^2 + c_3(z-a)^3 + \ldots$$

(*speziell im Fall $z = a$ mit $0^0 := 1$ und daher Wert gleich c_0*) *gebildet wird. Der* ***Konvergenzbereich*** *der Potenzreihe $\sum_{k=0}^{\infty} c_k(z-a)^k$ ist die Teilmenge $\{z \in \mathbb{C} \mid \sum_{k=0}^{\infty} c_k(z-a)^k$ konvergiert$\}$ von $\mathbb{C}$.*

Man kann Potenzreihen als „nächst allgemeinere“ Bildung nach Polynomen auffassen, denn während für ein Polynom nur endlich viele monomiale Terme $c_k(z-a)^k$ aufsummiert werden, sind es bei einer Potenzreihe (normalerweise) *un*endlich viele solche Terme. Die große Bedeutung solcher Reihen liegt zum einen darin, dass sich mit Ihnen viele Funktionen als Funktionenreihen mit Monomfunktionen (das sind im Wesentlichen Potenzen mit natürlichen Exponenten, also relativ einfache Funktionen) als Gliedern ausdrücken lassen, zum anderen darin, dass ihr Konvergenzbereich gemäß dem nächsten Satz eine prinzipiell einfache Struktur hat.

Satz (zum **Konvergenzverhalten von Potenzreihen**). *Seien $a \in \mathbb{C}$, $(c_k)_{k\in\mathbb{N}_0}$ eine Folge in $\mathbb{C}$. Dann existiert genau ein $R \in [0,\infty]$, der* ***Konvergenzradius*** *der Potenzreihe $\sum_{k=0}^{\infty} c_k(z-a)^k$, so dass sich die Fälle $|z-a| < R$ und $|z-a| > R$ wie folgt wesentlich unterscheiden*:

- *Für alle $z \in \mathbb{C}$ mit $|z-a| < R$ konvergiert $\sum_{k=0}^{\infty} c_k(z-a)^k$ absolut, und für jedes $r \in [0,R)$ konvergiert $\sum_{k=0}^{\infty} c_k p_a^k$ mit $p_a^k(z) := (z-a)^k$ auf $\{z \in \mathbb{C} \mid |z-a| < r\}$ sogar gleichmäßig.*
- *Für alle $z \in \mathbb{C}$ mit $|z-a| > R$ divergiert $\sum_{k=0}^{\infty} c_k(z-a)^k$ bestimmt oder unbestimmt.*

Bemerkungen (zu **Potenzreihen**).

(1) Der Satz besagt, dass der **Konvergenzbereich einer Potenzreihe** $\sum_{k=0}^{\infty} c_k(z-a)^k$ die **Kreisscheibe um den Entwicklungspunkt** $a \in \mathbb{C}$ als Mittelpunkt **mit dem Konvergenzradius** $R \in [0,\infty]$ als Radius ist. Genauer liegt jedenfalls für z innerhalb der Kreisscheibe (Fall $|z-a| < R$) Konvergenz und für z außerhalb der Kreisscheibe (Fall $|z-a| > R$) Divergenz vor, während für Randpunkte z der Kreisscheibe (Fall $|z-a| = R$) offen bleibt, ob Konvergenz oder Divergenz besteht. Damit ist der genaue Konvergenzbereich gemäß

$$\{z \in \mathbb{C} \mid |z-a| < R\} \subset \left\{ z \in \mathbb{C} \;\middle|\; \sum_{k=0}^{\infty} c_k(z-a)^k \text{ konvergent} \right\} \subset \{z \in \mathbb{C} \mid |z-a| \le R\}$$

zwischen der Kreisscheibe ohne Randpunkte und der Kreisscheibe mit Randpunkten eingeschachtelt. Für das Randverhalten, auf das wir hier nicht genauer eingehen, bestehen tatsächlich die Möglichkeiten, dass für $z \in \mathbb{C}$ mit $|z-a| = R$ entweder stets absolute Konvergenz oder stets nicht-absolute Konvergenz oder stets Divergenz oder in ziemlich beliebiger Mischung für manche z nicht-absolute Konvergenz, für andere Divergenz vorliegt.

(2) Speziell ist der *reelle* Konvergenzbereich $\{x \in \mathbb{R} \mid \sum_{k=0}^{\infty} c_k(x-a)^k$ konvergent$\}$ einer Potenzreihe $\sum_{k=0}^{\infty} c_k(z-a)^k$ stets ein Intervall. Im Fall $a \in \mathbb{R}$ handelt es sich um eines der Intervalle $(a-R, a+R)$, $[a-R, a+R)$, $(a-R, a+R]$, $[a-R, a+R]$ mit dem Konvergenzradius R.

(3) **Der Konvergenzradius R kann auch 0 oder ∞ sein.** Im Fall $R = 0$ besteht der genaue Konvergenzbereich $\{a\}$ nur aus dem Entwicklungspunkt a. Im Fall $R = \infty$ liegt für alle $z \in \mathbb{C}$ Konvergenz vor, und der genau Konvergenzbereich ist ganz $\mathbb{C}$.

Der **Beweis** für das gerade beschriebene Konvergenz- und Divergenzverhalten **basiert entscheidend auf dem Vergleich mit geometrischen Reihen** und verläuft genauer wie folgt.

Beweis des Satzes. Die Eindeutigkeit von R ist klar (denn wären $R_1 < R_2$ zwei Radien mit den genannten Eigenschaften, so müsste für $z \in \mathbb{C}$ mit $R_1 < |z-a| < R_2$ sowohl Divergenz als auch Konvergenz vorliegen). Die Existenz von R beweisen wir, indem wir für die Wahl

$$R := \sup\left\{ s \in \mathbb{R}_{\geq 0} \,\middle|\, (|c_k| s^k)_{k\in\mathbb{N}_0} \text{ Nullfolge} \right\}$$

das behauptete Konvergenz- und Divergenzverhalten nachweisen. Dazu bemerken wir, dass $(|c_k|s^k)_{k\in\mathbb{N}_0}$ für *alle* $s \in [0, R)$ Nullfolge ist (denn $0 \leq s < S$ und $\lim_{k\to\infty} |c_k| S^k = 0$ implizieren $\lim_{k\to\infty} |c_k| s^k = \lim_{k\to\infty} |c_k| S^k (s/S)^k = 0 \cdot 0 = 0$) und für alle $s \in (R, \infty)$ *keine* Nullfolge ist (klar). Dann argumentieren wir einmal für (gutartige) Konvergenz und einmal für Divergenz:

- Wir betrachten $z \in \mathbb{C}$ mit $|z-a| \leq r < R$ und fixieren ein beliebiges $s \in (r, R)$, zum Beispiel $s := \begin{cases} (R+r)/2 & \text{für } R < \infty \\ r+1 & \text{für } R = \infty \end{cases}$. Damit schätzen wir $|c_k(z-a)^k| \leq |c_k| r^k = |c_k| s^k (r/s)^k \leq (r/s)^k$ für alle $k \in \mathbb{N}_{\geq k_0}$ ab, wobei die letzte Abschätzung wegen $s < R$ und $\lim_{k\to\infty} |c_k| s^k = 0$ ab einem gewissen z-unabhängigen (!) Index $k_0 \in \mathbb{N}$ möglich ist. Also ist die geometrische Reihe $\sum_{k=0}^{\infty} (r/s)^k$ zur Basis $r/s \in [0, 1)$ eine konvergente Majorantenreihe für $\sum_{k=0}^{\infty} c_k (z-a)^k$, und nach dem Majorantenkriterium konvergiert $\sum_{k=0}^{\infty} c_k (z-a)^k$ absolut. Dass die Konvergenz in der behaupteten Weise gleichmäßig ist, folgt durch z-unabhängige Abschätzung der Reihenreste von $\sum_{k=0}^{\infty} c_k (z-a)^k$ durch die von $\sum_{k=0}^{\infty} (r/s)^k$, genauer ab $m \in \mathbb{N}_{\geq k_0}$ durch die Abschätzung $\left| \sum_{k=m}^{\infty} c_k (z-a)^k \right| \leq \sum_{k=m}^{\infty} |c_k (z-a)^k| \leq \sum_{k=m}^{\infty} (r/s)^k \underset{m\to\infty}{\longrightarrow} 0$.
- Für $z \in \mathbb{C}$ mit $|z-a| > R$ ist nach Obigem $(|c_k|\,|z-a|^k)_{k\in\mathbb{N}_0}$ und damit auch $(c_k(z-a)^k)_{k\in\mathbb{N}_0}$ *keine* Nullfolge. Nach dem Nullfolgenkriterium divergiert $\sum_{k=0}^{\infty} c_k (z-a)^k$ in diesem Fall.

Insgesamt ist die Existenz von R mit beiden behaupteten Eigenschaften gezeigt. □

Weitere Bemerkungen (zu **Potenzreihen**)**.**

(1) Zur **Bestimmung des Konvergenzradius** einer Potenzreihe $\sum_{k=0}^{\infty} c_k (z-a)^k$ gibt es verschiedene Möglichkeiten. Oft lässt sich **direkt** durch Vergleich mit bekannten Reihen oder mit Kriterien aus Abschnitt 5.5 **entscheiden**, für welche $z \in \mathbb{C}$ Konvergenz beziehungsweise Divergenz besteht, und der Konvergenzradius kann abgelesen werden. Alternativ kann man sich an den vorausgehenden Beweis anlehnen und $\boldsymbol{\lim_{k\to\infty} |c_k| s^k}$ mit Parameter $s \in \mathbb{R}_{\geq 0}$ **untersuchen**. Findet man das $R \in [0, \infty]$ (das es gemäß dem Beweis stets gibt), so dass der Limes für $s \in [0, R)$ Null und für $s \in (R, \infty)$ nicht Null (tatsächlich sogar immer ∞) ist, so ist der Konvergenzradius R bestimmt. Weitere Möglichkeiten zur Berechnung des Konvergenzradius R bieten die **Formel von Euler**

$$R = \lim_{k\to\infty} \left| \frac{c_k}{c_{k+1}} \right|$$

(gültig, falls dieser Limes in $[0, \infty]$ existiert; Konvergenzradius existiert aber auch bei Nicht-Existenz des Limes) oder die **Formel von Cauchy-Hadamard**

$$R = \frac{1}{\limsup_{k\to\infty} \sqrt[k]{|c_k|}}$$

(allgemein gültig; *auch*, wenn der Limes superior 0 oder ∞ ist; in letzteren Fällen mit Verständnis $\frac{1}{0} := \infty$ bzw. $\frac{1}{\infty} := 0$). Die beiden Formeln lehnen sich dabei an das Quotientenkriterium und das Wurzelkriterium aus Abschnitt 5.5 an. Genauer stellen die Kriterien für

das durch die Formeln gegebene R und $z \in \mathbb{C}$ mit $|z-a| < R$ Konvergenz von $\sum_{k=0}^{\infty} c_k(z-a)^k$ sicher. Für $|z-a| > R$ Divergenz einzusehen und damit den Beweis der beiden Formeln zu vervollständigen, ist dann auch nicht mehr schwer.

(2) Unter der **Entwicklung einer Potenzreihe** $\sum_{k=0}^{\infty} c_k(z-a)^k$ mit Konvergenzradius R **um einen anderen Punkt** b im Innern des Konvergenzbereichs (d.h. um $b \in \mathbb{C}$ mit $|b-a| < R$) versteht man den Übergang zur Potenzreihe $\sum_{\ell=0}^{\infty} d_\ell(z-b)^\ell$ mit Entwicklungspunkt b und neuen Koeffizienten $d_\ell = \sum_{k=\ell}^{\infty} c_k \binom{k}{\ell}(b-a)^{k-\ell}$. Diese neue Reihe mit Entwicklungspunkt b ergibt sich, indem man bei der ursprünglichen Reihe mit Entwicklungspunkt a per Binomialsatz $(z-a)^k = \sum_{\ell=0}^{k} \binom{k}{\ell}(z-b)^\ell(b-a)^{k-\ell}$ ausmultipliziert und dann umsummiert. Man kann zeigen, dass der Konvergenzradius der neuen Reihe mindestens $R-|b-a|$ ist und dass zumindest für $z \in \mathbb{C}$ mit $|z-b| < R-|b-a|$ (woraus dann $|z-a| < R$ folgt) die Werte der beiden Reihen übereinstimmen. Anschaulich umfasst der Konvergenzbereich der neuen Reihe mindestens die größte Kreisscheibe mit Mittelpunkt b, die noch ganz im Innern des Konvergenzbereichs der ursprünglichen Reihe liegt.

Auch wenn wir Potenzreihen hier ganz allgemein eingeführt haben, werden wir uns im Folgenden vor allem für Varianten der geometrischen Reihe, bei denen der Konvergenzradius endlich ist, sowie für die Exponentialreihe und daraus abgeleitete Reihen mit Konvergenzradius ∞ interessieren. Wir geben zunächst zwei Beispiele vom einfachen geometrischen Typ.

Beispiele (für einfache **Potenzreihen** vom Typ der geometrischen Reihe)**.**

(1) Die Potenzreihe $\sum_{k=0}^{\infty} 2^k(z-1)^k$ in der Variablen $z \in \mathbb{C}$ hat Entwicklungspunkt 1 und kann als geometrische Reihe zur Basis $2(z-1)$ aufgefasst werden. Damit ist klar, dass Konvergenz genau für $|2(z-1)| < 1$ oder mit anderen Worten genau für $|z-1| < \frac{1}{2}$ besteht. Der Konvergenzradius der Reihe ist $\frac{1}{2}$.

(2) Die Potenzreihe $\sum_{k=4}^{\infty} \frac{z^{2k}}{2^k}$ in der Variablen $z \in \mathbb{C}$ hat Entwicklungspunkt 0 und kann als geometrische Reihe zur Basis $\frac{z^2}{2}$ aufgefasst werden (wobei der Startindex 4 sich auf das Konvergenzverhalten natürlich nicht auswirkt). Konvergenz besteht genau für $\left|\frac{z^2}{2}\right| < 1$ oder äquivalent genau für $|z| < \sqrt{2}$. Der Konvergenzradius der Reihe ist $\sqrt{2}$.

Als Nächstes betrachten wir die **vielleicht wichtigste Potenzreihe überhaupt**, die komplexe Exponentialreihe, und nutzen diese zur Einführung der komplexen Exponentialfunktion:

Definition (**komplexe Exponentialfunktion**)**.** *Wir erklären die* ***komplexe Exponentialfunktion*** $\exp\colon \mathbb{C} \to \mathbb{C}$ *über die* (*gemäß dem folgenden Satz konvergente*) ***komplexe Exponentialreihe***

$$\exp(z) := \mathrm{e}^z := \sum_{k=0}^{\infty} \frac{1}{k!} z^k \qquad \textit{für alle } z \in \mathbb{C}\,.$$

Hauptsatz (**Eigenschaften der komplexen Exponentialfunktion**)**.** *Die Exponentialreihe der vorausgehenden Definition ist eine Potenzreihe mit Entwicklungspunkt* 0 *und Konvergenzradius* ∞ *und konvergiert insbesondere für alle* $z \in \mathbb{C}$ *absolut. Weiterhin hat die komplexe Exponentialfunktion folgende Eigenschaften*:

(I) *Für die Approximation der komplexen Exponentialfunktion durch die Partialsummen der Exponentialreihe gilt die* ***Fehlerabschätzung***

$$\left|\mathrm{e}^z - \sum_{k=0}^{n} \frac{1}{k!} z^k\right| \leq \sum_{k=n+1}^{\infty} \frac{1}{k!}|z|^k \leq \frac{|z|^n}{(n+1)!}\left(\mathrm{e}^{|z|}-1\right) \leq \frac{|z|^{n+1}}{(n+1)!}\mathrm{e}^{|z|} \qquad \text{für alle } z \in \mathbb{C}\,,\ n \in \mathbb{N}_0\,.$$

(II) *Die komplexe Exponentialfunktion hat die* ***Grenzwertdarstellung***

$$\mathrm{e}^z = \lim_{n\to\infty}\left(1+\frac{z_n}{n}\right)^n \qquad \text{für jede Folge } (z_n)_{n\in\mathbb{N}} \text{ in } \mathbb{C} \text{ mit } \lim_{n\to\infty} z_n = z$$

(*insbesondere natürlich* $\mathrm{e}^z = \lim_{n\to\infty}\left(1+\frac{z}{n}\right)^n$ *für jedes* $z \in \mathbb{C}$) *und erweist sich damit als* ***konsistente Erweiterung der reellen Exponentialfunktion*** *aus Abschnitt 5.2.*

(III) *Es gilt das allgemeine* ***Exponentialgesetz***

$$\boxed{\mathrm{e}^{z+w} = \mathrm{e}^z\mathrm{e}^w \qquad \text{für alle } w, z \in \mathbb{C}}\,.$$

(IV) *Es gilt die* ***Eulersche Formel***

$$\boxed{\mathrm{e}^{\mathbf{i}\vartheta} = \operatorname{cis}\vartheta = \cos\vartheta + \mathbf{i}\sin\vartheta \qquad \text{für alle } \vartheta \in \mathbb{R}}\,.$$

(V) *Bei beliebigem* $M \in \mathbb{R}$ *gilt die Lipschitz-Abschätzung*

$$|\mathrm{e}^w - \mathrm{e}^z| \leq \mathrm{e}^M |w-z| \qquad \text{für alle } z, w \in \mathbb{C} \text{ mit } \max\{\mathcal{Re}(z), \mathcal{Re}(w)\} \leq M\,.$$

Ausgehend von Exponentialgesetz und Eulerscher Formel kann man sich vom Abbildungsverhalten der komplexen Exponentialfunktion die in Abbildung 38 gezeigt Vorstellung machen.

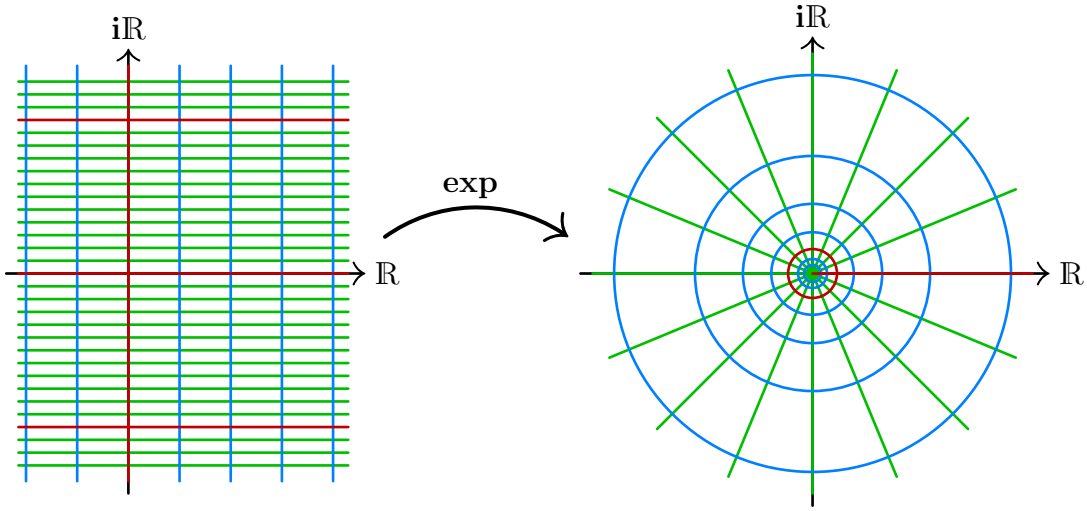


Abb. 38: Die komplexe Exponentialfunktion exp bildet ℝ und ℝ±2πiℝ auf $\mathbb{R}_{>0}$ ab, zu ℝ parallele Geraden auf Ursprungstrahlen, iℝ auf S^1 und zu iℝ parallele Geraden auf (immer wieder durchlaufene) Kreise um den Ursprung.

Zudem ergeben sich verschiedene Folgerungen: Für jedes $z \in \mathbb{C}$ erhält man die **Polardarstellung**

$$\mathrm{e}^z = \mathrm{e}^{\mathcal{R}e(z)} \operatorname{cis}(\mathit{Im}(z))$$

von e^z mit $|\mathrm{e}^z| = \mathrm{e}^{\mathcal{R}e(z)}$ und Polarwinkel $\mathit{Im}(z)$. Da das Bild der *reellen* Exponentialfunktion ganz $\mathbb{R}_{>0}$ ist, folgt

$$\operatorname{Bild}(\exp) = \mathbb{C}\backslash\{0\}\,,$$

und die gerade erwähnte Polardarstellung ist letztlich nichts anderes als die aus Abschnitt 5.3, die jede komplexe Zahl in $\mathbb{C}\backslash\{0\}$ erfasst. Weiterhin folgt auch $\overline{\mathrm{e}^z} = \mathrm{e}^{\overline{z}}$ für alle $z \in \mathbb{C}$, und mit der 2π-Periodizität von cis ergibt sich für $z, w \in \mathbb{C}$ die **2πi-Periodizität** der komplexen Exponentialfunktion

$$\mathrm{e}^w = \mathrm{e}^z \iff w \in z + 2\pi\mathbf{i}\mathbb{Z}\,.$$

Nach diesen Ergänzungen kommen wir zum Nachweis der Gesetzmäßigkeiten im Hauptsatz.

Beweis des Hauptsatzes. Wegen $\lim_{k\to\infty} \frac{1}{k!} s^k = 0$ für alle $s \in \mathbb{R}_{\geq 0}$ hat die Exponentialreihe Konvergenzradius ∞ und ist für alle $z \in \mathbb{C}$ absolut konvergent.

Wir beweisen nun die einzelnen Ungleichungen des Teils (I). Die linke Ungleichung folgt durch Abschätzung des Reihenrests $\left|\mathrm{e}^z - \sum_{k=0}^n \frac{1}{k!} z^k\right| = \left|\sum_{k=n+1}^\infty \frac{1}{k!} z^k\right| \leq \sum_{k=n+1}^\infty \frac{1}{k!} |z|^k$ mit der Dreiecksungleichung. Die mittlere Ungleichung ergibt sich mit der Exponentialreihe, einer Indexverschiebung und der Beobachtung $(n+k)! = (n+1)! \prod_{i=2}^k (n+i) \geq (n+1)! \prod_{i=2}^k i = (n+1)!\, k!$ durch Rechnung $\sum_{k=n+1}^\infty \frac{1}{k!} |z|^k = |z|^n \sum_{k=1}^\infty \frac{1}{(n+k)!} |z|^k \leq \frac{|z|^n}{(n+1)!} \sum_{k=1}^\infty \frac{1}{k!} |z|^k = \frac{|z|^n}{(n+1)!} (\mathrm{e}^{|z|} - 1)$. Die rechte Ungleichung folgt mit $\mathrm{e}^{|z|} - 1 = \sum_{k=1}^\infty \frac{1}{k!} |z|^k = |z| \sum_{k=0}^\infty \frac{1}{(k+1)!} |z|^k \leq |z| \sum_{k=0}^\infty \frac{1}{k!} |z|^k = |z| \mathrm{e}^{|z|}$.

Den Beweis des Teils (II) gehen wir durch Ausmultiplizieren mittels Binomialsatz

$$\left(1 + \frac{z_n}{n}\right)^n = \sum_{k=0}^n \binom{n}{k} \frac{z_n^k}{n^k} = \sum_{k=0}^n t_{k,n} z_n^k \qquad \text{mit der Abkürzung } t_{k,n} := \frac{1}{k!} \prod_{i=0}^{k-1} \frac{n-i}{n}$$

an. Dabei gilt offensichtlich $\lim_{n\to\infty} t_{k,n} = \frac{1}{k!}$ für alle $k \in \mathbb{N}_0$, woraus sich für die Summe mit n-abhängiger Zahl von Summanden aber nicht direkt eine Folgerung ziehen lässt. Wir führen deshalb eine beliebige Obergrenze $m \in \mathbb{N}$ ein, und schätzen für $n \geq m$ mit der Dreiecksungleichung und der Abschätzung $0 < t_{k,n} \leq \frac{1}{k!}$ für $k \in \{1, 2, \ldots, n\}$ wie folgt ab:

$$\begin{aligned}\left|\left(1 + \frac{z_n}{n}\right)^n - \sum_{k=0}^n \frac{1}{k!} z^k\right| &\leq \left|\sum_{k=0}^m \left(t_{k,n} z_n^k - \frac{1}{k!} z^k\right)\right| + \left|\sum_{k=m+1}^n t_{k,n} z_n^k\right| + \left|\sum_{k=m+1}^n \frac{1}{k!} z^k\right| \\ &\leq \sum_{k=0}^m \left|t_{k,n} z_n^k - \frac{1}{k!} z^k\right| + \sum_{k=m+1}^n \frac{1}{k!} |z_n|^k + \sum_{k=m+1}^n \frac{1}{k!} |z|^k\,.\end{aligned}$$

Wegen $\lim_{n\to\infty} t_{k,n} = \frac{1}{k!}$ und $\lim_{n\to\infty} z_n^k = z^k$ für alle $k \in \mathbb{N}_0$ geht nun der erste Term auf der rechten Seite (mit der festen Zahl $m+1$ von Summanden) für $n \to \infty$ gegen Null, während der zweite Term für $n \gg 1$ durch $\sum_{k=m+1}^\infty \frac{1}{k!} (2|z|)^k$ nach oben abgeschätzt ist. Insgesamt erhalten wir daher

$$\limsup_{n\to\infty} \left|\left(1 + \frac{z_n}{n}\right)^n - \sum_{k=0}^n \frac{1}{k!} z^k\right| \leq \sum_{k=m+1}^\infty \frac{1}{k!} (2|z|)^k + \sum_{k=m+1}^\infty \frac{1}{k!} |z|^k \qquad \text{für beliebiges } m \in \mathbb{N}\,.$$

Wir können nun auch den Grenzübergang $m \to \infty$ durchführen. Da es sich um Reihenreste der Exponentialreihe an den Stellen $2|z|$ und $|z|$ handelt, gehen dann die Terme rechts gegen Null, und der Limes Superior auf der linken Seite ist tatsächlich ein Limes mit Wert Null. Wir erhalten also erst $\lim_{n\to\infty} \left|\left(1+\frac{z_n}{n}\right)^n - \sum_{k=0}^n \frac{1}{k!} z^k\right| = 0$ und daraus dann mit

$$\lim_{n\to\infty} \left(1+\frac{z_n}{n}\right)^n = \lim_{n\to\infty} \sum_{k=0}^{n} \frac{1}{k!} z^k = \sum_{k=0}^{\infty} \frac{1}{k!} z^k = \mathrm{e}^z$$

die behauptete Grenzwertdarstellung der Exponentialfunktion.

Teil (III) des Satzes wird in den Übungen durch Berechnung des Cauchy-Produkts zweier Exponentialreihen bewiesen.

Zum Beweis von Teil (IV) gehen wir von den aus Abschnitt 5.3 bekannten Ungleichungen $1 \geq \cos\vartheta \geq \sqrt{1-\vartheta^2}$ für $\vartheta \in [-1,1]$ aus. Für beliebiges $\vartheta \in \mathbb{R}$ lassen sich diese auf $\frac{\vartheta}{n}$ mit $n \gg 1$ anstelle von ϑ anwenden und zeigen

$$0 \geq n\big(\cos\tfrac{\vartheta}{n} - 1\big) \geq n\left(\sqrt{1-\tfrac{\vartheta^2}{n^2}} - 1\right) = \frac{-\vartheta^2}{\sqrt{n^2-\vartheta^2}+n} \underset{n\to\infty}{\longrightarrow} 0\,.$$

Per Einschachtelungsprinzip folgt $\lim_{n\to\infty} n\big(\cos\frac{\vartheta}{n}-1\big) = 0$. Ähnlich nutzen wir nun die Ungleichungen $\vartheta \geq \sin\vartheta \geq \vartheta\cos\vartheta$ für $\vartheta \in [0,\pi]$ aus Abschnitt 5.3. Für $\vartheta \in \mathbb{R}_{\geq 0}$ und $n \gg 1$ bekommen wir daraus

$$\vartheta \geq n\sin\tfrac{\vartheta}{n} \geq \vartheta\cos\tfrac{\vartheta}{n} \underset{n\to\infty}{\longrightarrow} \vartheta$$

und somit $\lim_{n\to\infty} n\sin\frac{\vartheta}{n} = \vartheta$, wobei letzteres wegen der ungeraden Parität von sin sogar für alle $\vartheta \in \mathbb{R}$ richtig bleibt. Für $\mathrm{cis} = \cos + \mathbf{i}\sin$ haben wir in Zusammenfassung der gerade betrachteten Grenzwerte

$$\lim_{n\to\infty} n\big(\mathrm{cis}\,\tfrac{\vartheta}{n} - 1\big) = \mathbf{i}\vartheta \qquad\qquad \text{für alle } \vartheta \in \mathbb{R}$$

gezeigt. Für gegebenes $\vartheta \in \mathbb{R}$ kombinieren wir dies nun mit Teil (II) für $z_n := n\big(\mathrm{cis}\,\frac{\vartheta}{n}-1\big) \underset{n\to\infty}{\longrightarrow} \mathbf{i}\vartheta$ und der Formel von De Moivre aus Abschnitt 5.3 zu

$$\mathrm{e}^{\mathbf{i}\vartheta} = \lim_{n\to\infty} \left(1+\frac{z_n}{n}\right)^n = \lim_{n\to\infty} \left(\mathrm{cis}\,\frac{\vartheta}{n}\right)^n = \mathrm{cis}\,\vartheta\,.$$

Zum Beweis von Teil (V) benutzen wir $|a-b|^2 = (a-b)\big(\overline{a}-\overline{b}\big) = |a|^2+|b|^2-a\overline{b}-\overline{a}b$ für $a,b \in \mathbb{C}$. Zudem schreiben wir $w,z \in \mathbb{C}$ als $w = u+\mathbf{i}v$ und $z = x+\mathbf{i}y$ mit $u,v,x,y \in \mathbb{R}$. Mit zweimaliger Anwendung der gerade angegebenen Regel, dem Exponentialgesetz aus (III) und $|\mathrm{e}^{\mathbf{i}v}| = |\mathrm{e}^{\mathbf{i}y}| = 1$ erhalten wir dann

$$\begin{aligned}\big|\mathrm{e}^w-\mathrm{e}^z\big|^2 &= \big|\mathrm{e}^w\big|^2 + \big|\mathrm{e}^z\big|^2 - \mathrm{e}^w\overline{\mathrm{e}^z} - \overline{\mathrm{e}^w}\mathrm{e}^z = \big(\mathrm{e}^u\big)^2 + \big(\mathrm{e}^x\big)^2 + \mathrm{e}^u\mathrm{e}^x\big(-\mathrm{e}^{\mathbf{i}v}\overline{\mathrm{e}^{\mathbf{i}y}} - \overline{\mathrm{e}^{\mathbf{i}v}}\mathrm{e}^{\mathbf{i}y}\big)\\ &= \big(\mathrm{e}^u\big)^2 + \big(\mathrm{e}^x\big)^2 - 2\mathrm{e}^u\mathrm{e}^x + \mathrm{e}^u\mathrm{e}^x\big(2 - \mathrm{e}^{\mathbf{i}v}\overline{\mathrm{e}^{\mathbf{i}y}} - \overline{\mathrm{e}^{\mathbf{i}v}}\mathrm{e}^{\mathbf{i}y}\big) = \big(\mathrm{e}^u-\mathrm{e}^x\big)^2 + \mathrm{e}^u\mathrm{e}^x\big|\mathrm{e}^{\mathbf{i}v}-\mathrm{e}^{\mathbf{i}y}\big|^2\end{aligned}$$

Mit der fundamentalen Ungleichung $\mathrm{e}^t \geq 1+t$ für $t \in \mathbb{R}$ aus Abschnitt 5.2 können wir für $x \leq u \leq M$ nun $|\mathrm{e}^u-\mathrm{e}^x| = \mathrm{e}^u(1-\mathrm{e}^{x-u}) \leq \mathrm{e}^M(u-x) = \mathrm{e}^M|u-x|$ und für $u \leq x \leq M$ analog $|\mathrm{e}^u-\mathrm{e}^x| = \mathrm{e}^x(1-\mathrm{e}^{u-x}) \leq \mathrm{e}^M(x-u) = \mathrm{e}^M|u-x|$ abschätzen. Aus Teil (IV) und der fundamentalen Ungleichung für cis aus Abschnitt 5.3 bekommen wir zudem $|\mathrm{e}^{\mathbf{i}v}-\mathrm{e}^{\mathbf{i}y}| = |\mathrm{cis}\,v - \mathrm{cis}\,y| \leq |v-y|$. Wenden wir diese Beobachtungen auf der rechten Seite der vorausgehenden Abschätzung für $|\mathrm{e}^w-\mathrm{e}^z|^2$ an, so ergibt sich für $w = u+\mathbf{i}v$, $z = x+\mathbf{i}y$ mit $\max\{x,u\} \leq M$ insgesamt

$$\big|\mathrm{e}^w-\mathrm{e}^z\big|^2 \leq \big(\mathrm{e}^M|u-x|\big)^2 + \mathrm{e}^M\mathrm{e}^M|v-y|^2 = \big(\mathrm{e}^M\big)^2|w-z|^2\,.$$

Durch Ziehen der Quadratwurzel erhalten wir dann die letzte Behauptung. □

Aufbauend auf der komplexen Exponentialfunktionen lassen sich verschiedene **weitere Grundfunktionen im Komplexen** einführen.

Korollar & Definition (komplexer Logarithmus). *Zu jedem $z \in \mathbb{C}\backslash\{0\}$ existiert ein **komplexer Logarithmus** $w \in \mathbb{C}$ mit $\mathrm{e}^w = z$, der (nur) bis auf Addition von $2\pi\mathbf{i}k$ mit $k \in \mathbb{Z}$ eindeutig ist. Die Abbildung*

$$\operatorname{Log}\colon \mathbb{C} \setminus \{0\} \to \mathbb{R} + \mathbf{i}(-\pi, \pi]\,,$$

*die einer Zahl in $\mathbb{C}\backslash\{0\}$ den eindeutigen Logarithmus w mit $\mathrm{Im}(w) \in (-\pi, \pi]$ zuordnet, heißt der **Hauptzweig des komplexen Logarithmus** und ist bijektiv von $\mathbb{C}\backslash\{0\}$ auf $\mathbb{R}+\mathbf{i}(-\pi, \pi]$. Mit der in Abschnitt 5.3 eingeführten Argumentfunktion $\operatorname{Arg}\colon \mathbb{C}\backslash\{0\} \to (-\pi, \pi]$ gilt hierbei $\operatorname{Log}(z) = \log|z| + \mathbf{i}\operatorname{Arg}(z)$ für alle $z \in \mathbb{C}\backslash\{0\}$.* □

Korollar & Definition (Potenzen mit komplexen Exponenten). *Die Potenzen mit reellen Exponenten aus Abschnitt 5.2 werden durch*

$$b^s := \mathrm{e}^{s \log b} \qquad \text{für } b \in \mathbb{R}_{>0}\,,\ s \in \mathbb{C}$$

verallgemeinert. Neben den üblichen Potenzgesetzen gilt hierfür auch $|b^s| = b^{\mathcal{R}\mathrm{e}(s)}$. □

Bemerkung. Allgemeiner noch kann man $z^s := \exp(s \operatorname{Log} z)$ für $z \in \mathbb{C}\backslash\{0\}$, $s \in \mathbb{C}$ definieren, doch dies ist weniger üblich und natürlich. Schon für $s = \frac{1}{2}$ handelt es sich bei $z^{\frac{1}{2}} = \exp(\frac{1}{2}\operatorname{Log} z)$ um diejenige der beiden Quadratwurzeln aus z mit Polarwinkel in $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right]$, was relativ willkürlich scheint und wofür $(zw)^{\frac{1}{2}} = z^{\frac{1}{2}} w^{\frac{1}{2}}$ *nicht* allgemein gilt.

Korollar & Definition (Kreis- und Hyperbelfunktionen im Komplexen).

(I) *Die **Kreisfunktionen** Sinus, Kosinus, Tangens und Kotangens werden durch*

$$\cos z := \frac{\mathrm{e}^{\mathbf{i}z} + \mathrm{e}^{-\mathbf{i}z}}{2} \quad \text{für } z \in \mathbb{C}\,, \qquad \sin z := \frac{\mathrm{e}^{\mathbf{i}z} - \mathrm{e}^{-\mathbf{i}z}}{2\mathbf{i}} \quad \text{für } z \in \mathbb{C}\,,$$
$$\tan z := \frac{\sin z}{\cos z} \quad \text{für } z \in \mathbb{C} \setminus (2\mathbb{Z}+1)\tfrac{\pi}{2}\,, \qquad \cot z := \frac{\cos z}{\sin z} \quad \text{für } z \in \mathbb{C} \setminus \mathbb{Z}\pi\,,$$

konsistent auf komplexe Argumente erweitert. Der Sinus und der Kosinus besitzen die Potenzreihenentwicklungen

$$\cos z = \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k)!} z^{2k} \quad \text{für } z \in \mathbb{C}\,, \qquad \sin z = \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k+1)!} z^{2k+1} \quad \text{für } z \in \mathbb{C}$$

mit Entwicklungspunkt 0 und Konvergenzradius ∞, und es gilt

$$\cos^2 z + \sin^2 z = 1 \qquad \text{für alle } z \in \mathbb{C}\,.$$

(II) *Die **Hyperbelfunktionen** Sinus hyperbolicus, Kosinus hyperbolicus, Tangens hyperbolicus und Kotangens hyperbolicus werden durch*

$$\cosh z := \frac{\mathrm{e}^{z} + \mathrm{e}^{-z}}{2} \quad \text{für } z \in \mathbb{C}\,, \qquad \sinh z := \frac{\mathrm{e}^{z} - \mathrm{e}^{-z}}{2} \quad \text{für } z \in \mathbb{C}\,,$$
$$\tanh z := \frac{\sinh z}{\cosh z} \quad \text{für } z \in \mathbb{C} \setminus (2\mathbb{Z}+1)\mathbf{i}\tfrac{\pi}{2}\,, \qquad \coth z := \frac{\cosh z}{\sinh z} \quad \text{für } z \in \mathbb{C} \setminus \mathbb{Z}\mathbf{i}\pi\,,$$

konsistent auf komplexe Argumente erweitert. Der Sinus hyperbolicus und der Kosinus hyperbolicus besitzen die Potenzreihenentwicklungen

$$\cosh z = \sum_{k=0}^{\infty} \frac{1}{(2k)!} z^{2k} \quad \textit{für } z \in \mathbb{C}\,, \qquad \sinh z = \sum_{k=0}^{\infty} \frac{1}{(2k+1)!} z^{2k+1} \quad \textit{für } z \in \mathbb{C}$$

mit Entwicklungspunkt 0 *und Konvergenzradius* ∞*, und es gilt*

$$\cosh^2 z - \sinh^2 z = 1 \qquad \textit{für alle } z \in \mathbb{C}\,. \qquad \square$$

Wir schließen dieses Kapitel nun mit einem Ausblick zur tatsächlich noch viel weiter führenden Theorie von (Potenz-)Reihen ab:

Ausblick (zur **Potenzreihenentwicklung weiterer Grundfunktionen**)**.** Tatsächlich lassen sich für alle Grundfunktionen der Analysis Potenzreihenentwicklungen angeben, und mit Differential- und Integralrechnung wird später auch die systematische Bestimmung solcher Entwicklungen möglich. Wir erwähnen hier *ohne Beweis* zwei grundlegende und interessante Fälle:

(1) Die **Logarithmusreihe**

$$\sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k} z^k = \operatorname{Log}(1+z) \qquad \text{für } z \in \mathbb{C} \text{ mit } |z| < 1$$

mit Entwicklungspunkt 0 hat Konvergenzradius 1. Mit etwas Aufwand (Konvergenzkriterium von Dirichlet und Abelscher Grenzwertsatz) kann man tatsächlich zeigen, dass diese Reihe auch für Randpunkte $z \in \mathrm{S}^1 \backslash \{-1\}$ nicht-absolut konvergent mit Wert $\operatorname{Log}(1+z)$ ist. Als Spezialfälle gibt dies Konvergenz und Wert interessanter Reihen: Für $z = 1$ erhalten wir die **alternierende harmonische Reihe**

$$1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} \pm \ldots = \log 2\,.$$

Für $z = \mathbf{i}$ ergibt sich

$$\sum_{\ell=1}^{\infty} \frac{(-1)^{\ell-1}}{2\ell} + \mathbf{i} \sum_{\ell=0}^{\infty} \frac{(-1)^{\ell}}{2\ell+1} = \operatorname{Log}(1+\mathbf{i}) = \frac{1}{2}\log 2 + \mathbf{i}\frac{\pi}{4}\,,$$

wobei die Realteile wieder auf die alternierende harmonische Reihe, die Imaginärteile auf die **Leibnizsche Reihe**

$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} \pm \ldots = \frac{\pi}{4}$$

führen.

(2) Die **Binomialreihe**

$$\sum_{k=0}^{\infty} \binom{s}{k} z^k = (1+z)^s \qquad \text{für } z \in \mathbb{C} \text{ mit } |z| < 1$$

mit Parameter $\boldsymbol{s} \in \mathbb{C}$ und Entwicklungspunkt 0 hat für $s \in \mathbb{C} \backslash \mathbb{N}_0$ Konvergenzradius 1 und ergibt die mit dem Logarithmus-Hauptzweig definierte Potenz $(1+z)^s = \exp(s \operatorname{Log}(1+z))$ (wie etwas früher in einer Bemerkung erwähnt). Im Fall $s \in \mathbb{N}_0$ vereinfacht sich die Reihe wegen $\binom{s}{k} = 0$ für $k \in \mathbb{N}_{>s}$ zu einer endlichen Summe, deren Wert durch den Binomialsatz aus Abschnitt 4.3 gegeben ist. Formal hat die Reihe für $s \in \mathbb{N}_0$ daher Konvergenzradius ∞.

Kapitel 6

Vektorräume und lineare Abbildungen

In diesem Kapitel behandeln wir eine **systematische Theorie von Vektorräumen und linearen Abbildungen** zwischen Vektorräumen als abstrakte algebraische Bildungen ähnlich den früher in Kapitel 3 eingeführten. In engem Wechselspiel damit steht aber tatsächlich auch **konkreteres Rechnen mit Vektoren und Matrizen**.

6.1 Vektorräume und Untervektorräume

Wir beginnen mit der grundlegenden Definition der Theorie.

Definition (Vektorräume, Vektoren, Skalare). *Sei $(K,+,\cdot)$ ein Körper. Ein **K-Vektorraum** oder **Vektorraum über K** ist ein Tripel $(V,+,\cdot)$ aus einer Menge V und Abbildungen*

$$+\colon V\times V\to V \qquad \text{und} \qquad \cdot\colon K\times V\to V\,,$$

*genannt die **(Vektor-)Addition** und die **Skalarmultiplikation** des Vektorraums, so dass folgende **Vektorraumaxiome** erfüllt sind:*

- *Bei $(V,+)$ handelt es sich um eine abelsche Gruppe.*
- *Es gelten die **Distributivgesetze***

$$(s{+}t){\cdot}v = (s{\cdot}v)+(t{\cdot}v)\,, \qquad s{\cdot}(v{+}w) = (s{\cdot}v)+(s{\cdot}w) \qquad \text{für } s,t\in K\,,\ v,w\in V\,.$$

- *Es gelten das **Assoziativgesetz** und die **Neutralität der Eins***

$$(st){\cdot}v = s{\cdot}(t{\cdot}v)\,, \qquad 1_K{\cdot}v = v \qquad \text{für } s,t\in K\,,\ v\in V\,.$$

*Dabei haben wir die Symbole $+$ und $\cdot$ sowohl für die Vektoraddition und die Skalarmultiplikation als auch die Körperaddition und -multiplikation verwendet, obwohl es sich um unterschiedliche Operationen handelt und diese in den Vektorraumaxiomen vermischt auftreten. Da sich die zugehörigen Operationen oft aus dem Kontext ergeben, bezeichnen wir statt $(K,+,\cdot)$ und $(V,+,\cdot)$ oft auch nur K als Körper und V als K-Vektorraum. Die Elemente des Vektorraums V nennen wir **Vektoren**, die des Grundkörpers K dagegen **Skalare**. Dass neutrale Element der abelschen Gruppe $(V,+)$ bezeichnen wir als **Nullvektor** 0_V oder kurz 0.*

Notationen & Folgerungen (für **Vektorräume**).

(1) *Wir verwenden für Vektoren und Skalare dieselben* ***Konventionen zur Notationsvereinfachung wie für Zahlen oder Ring-/Körperelemente****, also das Einsparen des Malpunkts, die Notationen $-v$ für das additiv Inverse zu $v \in V$ und $v-w := v+(-w)$ für die Differenz von $v, w \in V$ und die üblichen Konventionen zur Klammereinsparung wie „Punkt- vor Strichrechnung“. Zudem erlauben wir auch, die Skalarmultiplikation in umgekehrter Reihenfolge zu Notieren, vereinbaren also*

$$v \cdot s := s \cdot v \qquad \text{für } s \in K\,,\ v \in V\,.$$

(2) *Für das Rechnen mit einem Vektor $v \in V$, einem Skalar $s \in K$ sowie den neutralen Elementen $0_V \in V$ und $0_K, 1_K \in K$ (die wir in Zukunft meist ohne die Indizes $_V$ und $_K$ notieren werden) gelten die Grundregeln*

$$0_K v = 0_V\,, \qquad s0_V = 0_V\,, \qquad sv = 0_V \implies (s = 0_K \vee v = 0_V)\,, \qquad (-1_K)v = -v\,.$$

(*Begründungen*: *Aus dem ersten Distributivgesetz erhalten wir $0v+0v = (0+0)v = 0v$ und kommen dann durch Subtraktion von $0v$ auf die erste Regel $0v = 0$. Analog gibt das zweite Distributivgesetz $s0+s0 = s(0+0) = s0$, woraus die zweite Regel folgt. Für die dritte Regel gehen wir von $sv = 0$ aus und nehmen ohne Einschränkung $s \neq 0$ an. Mit dem Reziproken s^{-1} zu s im Körper K, der Neutralität der Eins, dem Assoziativgesetz und der gerade bewiesenen zweiten Regel bekommen wir dann $v = 1v = (s^{-1}s)v = s^{-1}(sv) = s^{-1}0 = 0$, also die Behauptung. Für die letzte Regel rechnen wir in ähnlicher Weise $v+(-1)v = 1v + (-1)v = (1+(-1))v = 0v = 0$ und lesen ab, dass $(-1)v$ das additiv Inverse $-v$ zu v ist.*)

Bemerkung (zu **Verallgemeinerungen des Vektorraumkonzepts**). Allgemeiner als oben kann man das Konzept des Vektorraums auch über Schiefkörpern K (also bei nicht-kommutativer Körpermultiplikation) einführen. Es ist dann allerdings zwischen K-Linksvektorräumen und K-Rechtsvektorräumen zu unterscheiden, wobei erstere wie oben und zweitere mit Skalarmultiplikation „von rechts“ $\cdot\colon V \times K \to V$ und daran angepassten Axiomen wie dem Rechts-Distributivgesetz $v\cdot(st) = (v\cdot s)\cdot t$ definiert werden. Die oben getroffene Konvention $v\cdot s = s\cdot v$ würde über Schiefkörpern schnell zu Irritation führen und ist in dieser Allgemeinheit nicht sinnvoll. Abgesehen von etlichen Unterscheidungen zwischen „Links-Begriffen“ und „Rechts-Begriffen“ verläuft die Theorie über Schiefkörpern aber relativ weitgehend analog zu der über Körpern.

Noch allgemeiner gibt es auch über einem Ring R das zum K-Vektorraum analoge Konzept des R-Moduls. Auch hier ist bei nicht-kommutativen R zwischen R-Linksmoduln und R-Rechtsmoduln zu unterscheiden. Moduln verhalten sich im Allgemeinen deutlich weniger gutartig als Vektorräume, beginnend schon damit, dass die dritte Regel in (2) oben nicht übertragen werden kann. Daher unterscheidet sich diese Theorie wesentlich von der der Vektorräume.

Beispiele (für **Vektorräume**).

(0) Der **Nullvektorraum {0}**, der als einzigen Vektor den Nullvektor enthält, ist (mit der einzig möglichen Vektoraddition und Skalarmultiplikation) ein Vektorraum über jedem Körper.

(1) **Jeder Körper ist** (mit der Körperaddition als Vektoraddition und der Körpermultiplikation als Skalarmultiplikation) **ein Vektorraum über sich selbst.**

(2) Als **Hauptbeispiel** betrachten wir für einen Körper K und $n \in \mathbb{N}$ den

K-Vektorraum K^n

mit der komponentenweisen Addition

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1+y_1 \\ x_2+y_2 \\ \vdots \\ x_n+y_n \end{pmatrix} \qquad \text{für } x_1, y_1, x_2, y_2, \ldots, x_n, y_n \in K$$

als Vektoraddition und der durch

$$s\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} sx_1 \\ sx_2 \\ \vdots \\ sx_n \end{pmatrix} \qquad \text{für } s, x_1, x_2, \ldots, x_n \in K$$

definierten Skalarmultiplikation. Dabei haben wir, wie ab jetzt oft, **Tupel als Spaltenvektoren**

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} := (x_1, x_2, \ldots, x_n) \in K^n$$

notiert, wobei die Spaltenvektoren und Tupel (letztere mit Kommata!) aber von ab Abschnitt 6.3 verwendeten Zeilenvektoren $(x_1\ x_2\ \ldots\ x_n)$ (ohne Kommata!) zu unterscheiden sind. Besonders werden wir im Folgenden $K = \mathbb{R}$ im Auge haben und haben dann auch eine gewisse **Anschauung des $\mathbb{R}$-Vektorraums $\mathbb{R}^n$**: Wie früher schon oft bemerkt **entspricht** nämlich $\mathbb{R}$ **einer Gerade, $\mathbb{R}^2$ einer Ebene und $\mathbb{R}^3$ einem Raum**. Beim allgemeinen $\mathbb{R}^n$ mit $n \in \mathbb{N}$ kann man an eine Art „Raum mit n (beidseitig unendlichen) Richtungen“ denken. In ähnlicher Weise ist für $n \in \mathbb{N}$ und jeden K-Vektorraum V auch das n-fache Produkt V^n ein K-Vektorraum sowie allgemeiner für $n \in \mathbb{N}$ und K-Vektorräume $V_1, V_2, \ldots, V_n$ auch das Produkt $V_1 \times V_2 \times \ldots \times V_n$ ein K-Vektorraum (jeweils mit der komponentenweisen Addition und der zum Vorausgehenden analogen Skalarmultiplikation).

(3) Ist K ein Teilkörper eines Körpers L, so ist jeder L-Vektorraum, etwa L selbst oder L^n mit $n \in \mathbb{N}$, auch ein K-Vektorraum (mit entsprechend eingeschränkter Skalarmultiplikation). Hieraus ergibt sich zum Beispiel, dass der $\mathbb{C}$-Vektorraum $\mathbb{C}$ auch $\mathbb{R}$- und $\mathbb{Q}$-Vektorraum sowie der $\mathbb{R}$-Vektorraum $\mathbb{R}^3$ auch $\mathbb{Q}$-Vektorraum ist.

(4) Für jede Menge $\mathcal{X}$ und jeden Vektorraum V über einem Körper K ist auch $\mathbf{Abb}(\boldsymbol{\mathcal{X}}, \boldsymbol{V})$ mit der punktweisen Addition und der durch $(s{\cdot}f)(x) := s(f(x)) \in V$ für $s \in K$, $f \in \mathrm{Abb}(\mathcal{X}, V)$, $x \in \mathcal{X}$ definierten Skalarmultiplikation ein K-Vektorraum. Für konkrete $\mathcal{X}$ und V werden sich auch Teilmengen von $\mathrm{Abb}(\mathcal{X}, V)$ wie etwa die Mengen der stetigen, differenzierbaren oder integrierbaren Funktionen $\mathcal{X} \to V$ oder gewisser Homomorphismen $\mathcal{X} \to V$ oft als Vektorräume erweisen.

(5) Der **Polynomring** $K[\mathrm{X}]$ über einem Körper K ist mit der Polynomaddition und der durch

$$s(a_\ell \mathrm{X}^\ell + a_{\ell-1}\mathrm{X}^\ell + \ldots + a_2\mathrm{X}^2 + a_1\mathrm{X} + a_0) := sa_\ell \mathrm{X}^\ell + sa_{\ell-1}\mathrm{X}^\ell + \ldots + sa_2\mathrm{X}^2 + sa_1\mathrm{X} + sa_0$$

für $\ell \in \mathbb{N}_0$, $s, a_0, a_1, a_2, \ldots, a_{\ell-1}, a_\ell \in K$ definierten Skalarmultiplikation ein K-Vektorraum. Auch die Teilmenge $\{p \in K[\mathrm{X}] \mid \mathrm{grad}(p) \leq n\}$ der Polynome vom Grad $\leq n$ und die Teilmenge $\{a_\ell \mathrm{X}^{2\ell+1} + a_{\ell-1}\mathrm{X}^{2\ell-1} + \ldots + a_2\mathrm{X}^5 + a_1\mathrm{X}^3 + a_0\mathrm{X} \mid \ell \in \mathbb{N}_0\,,\ a_0, a_1, a_2, \ldots, a_{\ell-1}, a_\ell \in K\}$ der ungeraden Polynome sind mit derselben Addition und Skalarmultiplikation K-Vektorräume.

Wie für die algebraischen Strukturen des Kapitels 3 in Abschnitt 3.3 gesehen, lassen sich auch für Vektorräume Unterstrukturen erklären.

Definition (**Untervektorräume**). *Sei K ein Körper. Ein **K-Untervektorraum** eines K-Vektorraums V ist eine Teilmenge U von V mit folgenden Eigenschaften*:

- *$0_V \in U$ für den Nullvektor 0_V von V,*
- ***Abgeschlossenheit unter Vektoraddition**: $v{+}w \in U$ für alle $v, w \in U$,*

- ***Abgeschlossenheit unter Skalarmultiplikation*:** *$sv \in U$ für alle $s \in K$, $v \in U$.*

Gelegentlich bezeichnen wir einen Untervektorraum auch kurz als ***Unterraum****.*

Bemerkungen (zu **Untervektorräumen**)**.**

(0) Da ein Untervektorraum zumindest den Nullvektor enthält, ist er insbesondere $\neq \emptyset$.

(1) Aus der Abgeschlossenheit eines K-Untervektorraums U von V unter Skalarmultiplikation folgt wegen $-v = (-1)v$ seine **Abgeschlossenheit auch unter Negation** im Sinn von $-v \in U$ für alle $v \in U$. Die Abgeschlossenheit unter Addition und Negation bedeuten zusammen, dass U dann auch **stets auch additive Untergruppe** von V ist.

(2) Die Definition des Untervektorraums wurde (natürlich!) so getroffen, dass **jeder K-Untervektorraum** mit entsprechend eingeschränkter Addition und Skalarmultiplikation **selbst ein K-Vektorraum** ist.

Beispiele (für **Untervektorräume**)**.**

(0) Für jeden K-Vektorraum V sind der **Nullvektorraum** $\{0\}$ und der ganze Vektorraum V zwei K-Untervektorräume von V (und offensichtlich der kleinst- und größtmögliche solche).

(1) Erste Beispiele für Untervektorräume ergeben sich aus den Beispielen (3), (4) und (5) zu Vektorräumen: Konkret ist etwa $\mathbb{R}$ ein $\mathbb{R}$-Untervektorraum und $\mathbb{Q}$-Untervektorraum von $\mathbb{C}$, $\mathbb{Q}^3$ ist ein $\mathbb{Q}$-Untervektorraum von $\mathbb{R}^3$, und $\mathbb{R}\times\{(0,0)\}\times\mathbb{R}\times\{0\}$ ist ein $\mathbb{R}$-Untervektorraum und $\mathbb{Q}$-Untervektorraum von $\mathbb{R}^5$. Auch sind über einem beliebigen Körper K die im vorigen Beispiel (5) angegebenen Teilmengen von $K[\mathrm{X}]$ stets K-Untervektorräume von $K[\mathrm{X}]$.

(2) Absolute **Standard-Beispiele von K-Untervektorräumen** eines K-Vektorraums V sind

$$Kv = \{sv \,|\, s \in K\} \qquad \text{und} \qquad Kv+Kw = \{sv+tw \,|\, s,t \in K\}$$

mit dem Grundkörper K und festen Vektoren $v, w \in V$. Zwei konkrete Beispiele dieses Typs sind die $\mathbb{R}$-Untervektorräume

$$\mathbb{R}\begin{pmatrix}1\\-2\\\pi\end{pmatrix} = \left\{\begin{pmatrix}s\\-2s\\\pi s\end{pmatrix} \,\middle|\, s \in \mathbb{R}\right\} \qquad \text{und} \qquad \mathbb{R}\begin{pmatrix}1/2\\-1\end{pmatrix} + \mathbb{R}\begin{pmatrix}1\\4\end{pmatrix} = \left\{\begin{pmatrix}s/2+t\\-s+4t\end{pmatrix} \,\middle|\, s,t \in \mathbb{R}\right\}$$

von $\mathbb{R}^3$ und $\mathbb{R}^2$. Anschaulich entspricht dabei ersterer eine **Gerade in $\mathbb{R}^3$**, für zweiteren wird etwas später klar, dass er mit der ganzen **Ebene $\mathbb{R}^2$** übereinstimmt.

Weitere Bemerkung (zu **Untervektorräumen**)**.**

(2) Sei W ein Vektorraum über einem Körper K. Für K-Untervektorräume U und V von W geben der **Schnitt** $U \cap V$ und die **Summe** $U + V = \{u+v \,|\, u \in U, v \in V\}$ **wieder K-Untervektorräume** von W.

(Begründung: Offensichtlich ist $0 \in U\cap V$ und $0 \in U+V$. Daneben sind diese Eigenschaften zu zeigen:

Abgeschlossenheit von $U\cap V$ unter Addition: Für $w_1, w_2 \in U\cap V$ ist einerseits mit $w_1, w_2 \in U$ auch $w_1+w_2 \in U$, andererseits mit $w_1, w_2 \in V$ auch $w_1+w_2 \in V$, insgesamt also $w_1+w_2 \in U\cap V$.

Abgeschlossenheit von $U\cap V$ unter Skalarmultiplikation: Für $s \in K$, $w \in U\cap V$ ist einerseits mit $w \in U$ auch $sw \in U$, andererseits mit $w \in V$ auch $sw \in V$, insgesamt also $sw \in U\cap V$.

Abgeschlossenheit von $U+V$ unter Addition: Für $w_1, w_2 \in U+V$ ist $w_1 = u_1+v_1$, $w_2 = u_2+v_2$ mit $u_1, u_2 \in U$, $v_1, v_2 \in V$, und wir bekommen $w_1+w_2 = (u_1+u_2)+(v_1+v_2) \in U+V$.

Abgeschlossenheit von $U+V$ unter Skalarmultiplikation: Für $s \in K$, $w \in U+V$ ist $w = u+v$ mit $u \in U$, $v \in V$, und wir bekommen $sw = su+sv \in U+V$.)

Analog ergibt sich, dass sogar der Schnitt $\bigcap_{i\in I} U_i$ einer beliebigen Familie $(U_i)_{i\in I}$ von K-Untervektorräumen von W und die Summe $\sum_{i=1}^{n} U_i = \left\{ \sum_{i=1}^{n} u_i \,|\, u_i \in U_i \text{ für } i = 1, 2 \ldots, n \right\}$ einer endlichen Zahl $n \in \mathbb{N}$ von K-Untervektorräumen $U_1, U_2, \ldots, U_n$ von W wieder K-Untervektorräume von W sind.

Dagegen ist die **Vereinigung** $U \cup V$ von K-Untervektorräumen U und V von W **normalerweise *kein* K-Untervektorraum** von W, da für $u \in U$, $v \in V$ zwar $u, v \in U \cup V$, aber im Allgemeinen *nicht* $u+v \in U \cup V$ gilt. Tatsächlich ist $U \cup V$ ausschließlich in der trivialen Situation, dass $U \subset V$ oder $V \subset U$ gilt und somit $U \cup V$ mit U oder V selbst übereinstimmt, wieder ein K-Untervektorraum von W.

In erneuter Anlehnung an Abschnitt 3.3 betrachten wir als Nächstes erzeugte Unterstrukturen, die sich hier bei Vektorräumen schnell als eng verbunden mit sogenannten Linearkombinationen herausstellen werden:

Definitionen (**Linearkombinationen** und **aufgespannte/erzeugte Untervektorräume**)**.** *Seien K ein Körper, V ein K-Vektorraum und A eine beliebige Teilmenge von V.*

(1) *Eine **K-Linearkombination** von $n \in \mathbb{N}_0$ Vektoren $v_1, v_2, \ldots, v_n \in V$ ist ein Vektor*

$$\sum_{i=1}^{n} \lambda_i v_i = \lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_n v_n \in V$$

*mit beliebigen Koeffizienten $\lambda_1, \lambda_2, \ldots, \lambda_n \in K$. Sind alle Koeffizienten gleich Null, so heißt die Linearkombination **trivial**, ist mindestens einer ungleich Null, so heißt sie **nichttrivial**. Weiterhin bezeichnen wir einen Vektor in V als K-Linearkombination von Vektoren aus A, wenn er für irgendein* endliches[1] *$n \in \mathbb{N}_0$ eine K-Linearkombination von n Vektoren aus A ist.*

(2) *Der **von A aufgespannte** oder **von A erzeugte K-Untervektorraum** von V oder die **K-lineare Hülle** von A in V ist der (bezüglich „$\subset$“) kleinste K-Untervektorraum U von V mit $A \subset U$. Er wird als* $\mathrm{Span}(A)$, $\mathrm{Span}_K A$ *oder* $\langle A \rangle$ *notiert. Für als Liste angegebene, endliche oder abzählbare Mengen A verzichten wir bei dieser Notation gelegentlich auf Mengenklammern und schreiben beispielsweise $\langle v_1, v_2, \ldots \rangle$ für $\langle \{v_1, v_2, \ldots\} \rangle$ oder* $\mathrm{Span}(v_1, v_2, \ldots, v_n)$ *für* $\mathrm{Span}(\{v_1, v_2, \ldots, v_n\})$.

Satz (über die **lineare Hülle**)**.** *Seien K ein Körper, V ein K-Vektorraum und A eine beliebige Teilmenge von V. Dann existiert* $\mathrm{Span}_K A$ *und erfüllt*

$$\boxed{\mathrm{Span}_K A = \{w \in V \,|\, w \text{ ist } K\text{-Linearkombination von Vektoren aus } A\}}.$$

Die rechte Seite kann dabei auch als $\bigcup_{n=0}^{\infty} \bigcup_{v_1, v_2, \ldots, v_n \in V} \sum_{i=1}^{n} K v_i$ ausgedrückt werden.

[1] Beim Begriff der Linearkombination gehen also auch für *unendliche* Mengen A nur *endliche* Summen ein. Unendliche Summen haben wir in einem beliebigen Vektorraum tatsächlich auch gar nicht zur Verfügung.

Am Rande sei angemerkt, dass wir oben für $n = 0$ die leere Summe $\sum_{i=1}^{0} \lambda_i v_i$ als den Nullvektor verstehen. Mit dieser Konvention ist der Nullvektor formal K-Linearkombination von 0 Vektoren und auch K-Linearkombination von Vektoren aus $\emptyset$. Später erspart uns dies bisweilen, solche trivialen Situationen explizit ausschließen zu müssen.

Beweis. Sei $\mathrm{LK}_K(A)$ die im Satz auftretende Menge der Linearkombinationen. Es ist zu zeigen, dass $\mathrm{LK}_K(A)$ ein K-Untervektorraum von V mit $A \subset \mathrm{LK}_K(A)$ ist und zudem $\mathrm{LK}_K(A) \subset U$ für jeden anderen K-Untervektorraum U von V mit $A \subset U$ gilt.

Dabei ist $A \subset \mathrm{LK}_K(A)$ klar (weil jedes $w \in A$ mit $w = 1w$ Linearkombination von sich selbst ist), ebenso $0 \in \mathrm{LK}_K(A)$ und die Abgeschlossenheit von $\mathrm{LK}_K(A)$ unter Skalarmultiplikation. Dass $\mathrm{LK}_K(A)$ abgeschlossen unter Addition und damit K-Untervektorraum von V ist, kann man so begründen: Sind $v, w \in \mathrm{LK}_K(A)$, also $v = \sum_{i=1}^{m} \lambda_i v_i$ und $w = \sum_{j=1}^{n} \lambda_{m+j} v_{m+j}$ mit $m, n \in \mathbb{N}_0$, $v_i \in A$, $\lambda_i \in K$, so ist offensichtlich auch $v+w = \sum_{i=1}^{m+n} \lambda_i v_i \in \mathrm{LK}_K(A)$.

Ist U ein weiterer K-Untervektorraum von V mit $A \subset U$, so erhalten wir $\mathrm{LK}_K(A) \subset U$ wie folgt: Für $v \in \mathrm{LK}_K(A)$ ist $v = \sum_{i=1}^{m} \lambda_i v_i$ mit $m \in \mathbb{N}$, $v_i \in A$, $\lambda_i \in K$. Wegen $A \subset U$ sind dann $v_i \in U$ und wegen der Abgeschlossenheit des Untervektorraums U unter Skalarmultiplikation und Addition folgen $\lambda_i v_i \in U$ und $v = \sum_{i=1}^{m} \lambda_i v_i \in U$. □

Bemerkung (zur **Existenz des aufgespannten Untervektorraums**)**.** Die generelle Existenz von $\mathrm{Span}_K A$ ergibt sich mit dem vorausgehenden Beweis. *Alternativ* kann man die Existenz mit dem Standard-Ansatz zeigen, dass der *kleinste* K-Untervektorraum U von V mit $A \subset U$ sich als Durchschnitt *aller* K-Untervektorräume U von V mit $A \subset U$ ergibt.

Beispiele (für **aufgespannte Untervektorräume**)**.**

(0) Da der Nullvektorraum $\{0\}$ stets der kleinste Untervektorraum ist, gelten $\langle\emptyset\rangle = \{0\}$ und $\langle\{0\}\rangle = \{0\}$ in jedem Vektorraum.

(1) In jedem Vektorraum V über einem Körper K geben

$$\langle v\rangle = Kv \qquad \text{und} \qquad \langle v_1, v_2, \ldots, v_n\rangle = Kv_1 + Kv_2 + \ldots + Kv_n$$

mit $v \in V$ bzw. $n \in \mathbb{N}$ und $v_1, v_2, \ldots, v_n \in V$ im Wesentlichen schon betrachtete Standard-Beispiele von Untervektorräumen.

(2) Im $\mathbb{R}$-Vektorraum $\mathbb{R}$ ist $\mathrm{Span}_{\mathbb{R}} A = \mathbb{R}$ für *jede* Teilmenge $A \subset \mathbb{R}$ außer $A = \emptyset$ und $A = \{0\}$. Als für unsere Betrachtungen eher randständige Beispiele im $\mathbb{Q}$-Vektorraum $\mathbb{R}$ erwähnen wir aber noch $\mathrm{Span}_{\mathbb{Q}} \mathbb{Q} = \mathbb{Q}$ und $\mathrm{Span}_{\mathbb{Q}}(\mathbb{R}\backslash\mathbb{Q}) = \mathbb{R}$.

Zum Abschluss dieses Abschnitts beschreiben wir noch in Kürze, wie mit Untervektorräumen einerseits affine Unterräume, andererseits — ein weiteres Mal analog zu Abschnitt 3.3 — Faktorräume gebildet werden können.

Definition (**affine Unterräume**)**.** *Seien K ein Körper und V ein K-Vektorraum. Ein **affiner Unterraum** von V ist eine Teilmenge der Form $x+U$ von V mit beliebigem $x \in V$ und einem K-Untervektorraum U von V.*

Bemerkungen (zu **affinen Unterräumen**)**.** Seien K ein Körper und V ein K-Vektorraum.

(1) Ein affiner Unterraum A von V erfüllt $A = x+U$ für *jedes beliebige* $x \in A$ und *einen festen* K-Untervektorraum U von V. (Dies ergibt sich, weil für $\widetilde{x} \in x+U$ stets $\widetilde{x}+U = x+U$ gilt.) In Anlehnung an die folgenden Beispiele bezeichnet man dabei manchmal x als Aufpunkt und U als Raum der Richtungen von A.

(2) Ein affiner Unterraum A von V ist genau dann ein K-Untervektorraum von V, wenn $0 \in A$ gilt. (Dies folgt aus der vorigen Bemerkung (1) mit $x = 0$ oder auch direkter.)

(3) Auch der von einer nicht-leeren Teilmenge von V **aufgespannte *affine* Unterraum** von V kann als der kleinste affine Unterraum von V, der die Teilmenge enthält, sinnvoll erklärt werden. Da jeder nicht-leere Schnitt von affinen Unterräumen (wie man mit Bemerkung (1) sieht) wieder ein affiner Unterraum ist, ergibt sich auch die generelle Existenz aufgespannter affiner Unterräume mit der üblichen Durchschnitts-Konstruktion.

Beispiele (für **affine Unterräume**).

(1) Ein affiner Unterraum
$$x + \langle v \rangle = x + \mathbb{R}v$$
mit Aufpunkt $x \in \mathbb{R}^n$ und Richtungsvektor $v \in \mathbb{R}^n \backslash \{0\}$ entspricht einer **Gerade in $\mathbb{R}^n$**. Dabei sind weder x noch v, aber schon $\langle v \rangle = \mathbb{R}v$ eindeutig durch den affinen Unterraum bestimmt.

(2) Ein affiner Unterraum
$$x + \langle v_1, v_2 \rangle = x + \mathbb{R}v_1 + \mathbb{R}v_2$$
mit Aufpunkt $x \in \mathbb{R}^n$ und Richtungsvektoren $v_1, v_2 \in \mathbb{R}^n \backslash \{0\}$, so dass $\mathbb{R}v_1 \neq \mathbb{R}v_2$, entspricht einer **Ebene in $\mathbb{R}^n$**. Dabei sind weder x noch $\langle v_1 \rangle = \mathbb{R}v_1$ noch $\langle v_2 \rangle = \mathbb{R}v_2$, aber schon $\langle v_1, v_2 \rangle = \mathbb{R}v_1 + \mathbb{R}v_2$ eindeutig durch den affinen Unterraum bestimmt.

Zuletzt kommen wir in diesem Abschnitt zu Faktorräumen, die für Vektorräume ganz analog zu den schon in Abschnitt 3.3 behandelten Faktorgruppen und Faktorringen erklärt werden.

Definition (**Faktorräume**). *Seien K ein Körper, V ein K-Vektorraum und U ein Untervektorraum von V. Unter dem **Faktorraum** V/U (lies: V durch U oder V modulo U) versteht man die Quotientenmenge*
$$V/U := \{x+U \mid x \in V\}$$
(bezüglich der durch $x \overset{U}{\sim} y :\Longleftrightarrow y-x \in U$ gegebenen Äquivalenzrelation mit zugehörigen Äquivalenzklassen $[x]_{\overset{U}{\sim}} = x+U = \{x+u \mid u \in U\}$) zusammen mit der durch
$$\begin{aligned} (x+U) + (y+U) &:= (x+y)+U \in V/U && \text{für } x+U, y+U \in V/U\,, \\ s\cdot(x+U) &:= sx+U \in V/U && \text{für } s \in K\,,\ x+U \in V/U \end{aligned}$$
definierten Vektoraddition und Skalarmultiplikation.

Bei Vektorräumen verhält sich diese Bildung sogar besonders gutartig. Anders als etwa bei Gruppen oder Ringen erhält man nämlich ganz allgemein und ohne Zusatzbedingung an den Untervektorraum U als Quotient V/U stets wieder einen Vektorraum:

Satz (zu **Faktorräumen**). *Seien K ein Körper, V ein K-Vektorraum und U ein Untervektorraum von V. Dann sind die Addition und Skalarmultiplikation der vorigen Definition wohldefiniert, und der Faktorraum V/U ist mit diesen Operationen ein K-Vektorraum.*

Beweis. Dass die Vektoraddition wohldefiniert und V/U mit dieser eine abelsche Gruppe bildet, wissen wir aus Abschnitt 3.3 (denn in der *abelschen* Gruppe $(V,+)$ ist die Untergruppe U auch Normalteiler).

Für die Wohldefiniertheit der Skalarmultiplikation betrachten wir zwei Repräsentanten $x, x' \in V$ einer Äquivalenzklasse $x'+U = x+U \in V/U$. Aus $x'-u \in U$ folgt dann mit der Abgeschlossenheit von U unter Skalarmultiplikation $sx'-sx = s(x'-x) \in U$. Mit $sx'+U = sx+U$ sehen

wir dann, dass der $s\cdot(x+U)$ definierende Ausdruck $sx+U$ nicht von der Repräsentantenwahl abhängt.

Somit bleiben nur die Vektorraumaxiome für V/U aus den Definitionen und den Vektorraumaxiomen von V abzuleiten. Zum Beispiel rechnet man für das zweite Distributivgesetz

$$s((x+U)+(y+U)) = s((x+y)+U) = s(x+y)+U = (sx+sy)+U = (sx+U)+(sy+U)$$

für $s \in K$, $x, y \in V$. Die weiteren Axiome weist man ganz ähnlich nach. □

Bemerkung. Die Elemente von V/U sind die affinen Unterräume von V, die den festen Untervektorraum U als Raum von Richtungen haben. Speziell für eine Ursprungsgerade U bzw. eine Ebene U durch den Ursprung in $\mathbb{R}^n$, besteht $\mathbb{R}^n/U$ aus allen zu U parallelen Geraden bzw. Ebenen in $\mathbb{R}^n$. Das Rechnen in diesen Faktorräumen kann man daher als ein Rechnen mit parallelen affinen Unterräumen, parallelen Geraden bzw. parallelen Ebenen auffassen.

6.2 Basen von Vektorräumen und der Dimensionsbegriff

Als Nächstes wollen wir ausgehend von einem System nur einiger Vektoren eines Vektorraums alle anderen Vektoren auf eindeutige Weise als deren Linearkombinationen beschreiben. Die gutartigen Systeme, bezüglich denen dies möglich sein wird, heißen Basen. Bevor wir zu diesen kommen, führen wir aber zunächst ein vorbereitendes und ebenfalls wichtiges Konzept ein:

Definition (**lineare Unabhängigkeit, lineare Abhängigkeit**). *Seien K ein Körper und V ein K-Vektorraum.*

(I) *Wir nennen $m \in \mathbb{N}$ Vektoren $v_1, v_2, \ldots, v_m \in V$* ***linear unabhängig*** *(über K), wenn für alle $\lambda_1, \lambda_2, \ldots, \lambda_m \in K$ die Implikation*

$$\sum_{j=1}^{m} \lambda_j v_j = 0 \implies \lambda_1 = \lambda_2 = \ldots = \lambda_m = 0$$

gilt. Andernfalls heißen $v_1, v_2, \ldots, v_m$ ***linear abhängig*** *(über K).*

(II) *Wir nennen eine Teilmenge A von V* ***linear unabhängig*** *(über K), wenn jede* endliche *Zahl von Vektoren aus A (ohne Mehrfachnennung desselben Vektors) über K linear unabhängig ist, wenn also die Implikation $\sum_{v\in E} \lambda_v v = 0 \implies \forall v \in E\colon \lambda_v = 0$ für alle* endlichen *Teilmengen E von A und alle mit E indizierten Familien $(\lambda_v)_{v\in E}$ von Elementen von K gilt. Andernfalls heißt A* ***linear abhängig*** *(über K).*

In gleicher Bedeutung sprechen wir auch von ***K-linear unabhängigen*** *und von* ***K-linear abhängigen*** *Vektoren und Mengen.*

Bemerkungen (zu **linearer (Un-)Abhängigkeit**).

(0) Lineare (Un-)Abhängigkeit endlich vieler Vektoren und endlicher Teilmengen sind im Wesentlichen dieselben Konzepte. Genauer sind Vektoren $v_1, v_2, \ldots, v_m$ mit $m \in \mathbb{N}$ genau dann linear unabhängig, wenn sie alle verschieden sind und $\{v_1, v_2, \ldots, v_m\}$ linear unabhängig ist.

(1) Die **lineare Unabhängigkeit *eines*** einzelnen **Vektors** $v_1 \in V$ (Fall $m = 1$ in der Definition) bedeutet einfach $v_1 \neq 0$.

(2) Die **lineare Unabhängigkeit *zweier* Vektoren** $v_1, v_2 \in V$ (Fall $m = 2$ in der Definition) bedeutet $v_1 \neq 0$ und $v_2 \neq sv_1$ für alle $s \in K$. Für $K = \mathbb{R}$ bedeutet dies anschaulich, dass zwei linear unabhängige Vektoren nicht auf derselben Ursprungsgerade liegen, also beide von Null verschieden sind und nicht in dieselbe, aber auch nicht in exakt entgegengesetzte Richtungen zeigen.

(3) Im Fall $V = K^n$ mit $n \in \mathbb{N}$ (auf den wir demnächst andere Fälle werden reduzieren können) ist **zum Prüfen linearer Unabhängigkeit** ein **lineares Gleichungssystem** zu **lösen**. Sind genauer

$$v_1 = \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{n1} \end{pmatrix}, \; v_2 = \begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{n2} \end{pmatrix}, \; v_3 = \begin{pmatrix} a_{13} \\ a_{23} \\ \vdots \\ a_{n3} \end{pmatrix}, \; \ldots, \; v_m = \begin{pmatrix} a_{1m} \\ a_{2m} \\ \vdots \\ a_{nm} \end{pmatrix} \in K^n$$

gegeben, gilt also mit anderen Worten $v_j = \sum_{i=1}^{n} a_{ij} \mathrm{e}_i$ für $j = 1, 2, 3, \ldots, m$ mit Koeffizienten $a_{ij} \in K$ und den kanonischen Basisvektoren e_i des K^n, so bilden die n skalaren Komponenten-Gleichungen der Vektor-Gleichung $\sum_{j=1}^{m} \lambda_j v_j = 0$ das Gleichungssystem

$$\begin{aligned} a_{11}\lambda_1 + a_{12}\lambda_2 + \ldots + a_{1m}\lambda_m &= 0\,, \\ a_{21}\lambda_1 + a_{22}\lambda_2 + \ldots + a_{2m}\lambda_m &= 0\,, \\ \vdots \qquad\quad \vdots \qquad\qquad\quad \vdots \qquad\quad \vdots & \\ a_{n1}\lambda_1 + a_{n2}\lambda_2 + \ldots + a_{nm}\lambda_m &= 0 \end{aligned}$$

für die m Variablen $\lambda_1, \lambda_2, \ldots, \lambda_m \in K$. Ist die triviale Lösung $\lambda_1 = \lambda_2 = \ldots = \lambda_m = 0$ (die offensichtlich immer eine Lösung ist) die *einzige* Lösung des Gleichungssystems, so sind $v_1, v_2, \ldots, v_m$ über K linear unabhängig. Gibt es neben der trivialen Lösung weitere Lösungen, so sind $v_1, v_2, \ldots, v_m$ über K linear abhängig.

Beispiel (zum **Nachweis linearer Unabhängigkeit**)**.** Als vereinfachtes Beispiel untersuchen wir die Vektoren $\binom{4}{1}, \binom{3}{2} \in \mathbb{R}^2$ auf lineare Unabhängigkeit über $\mathbb{R}$, wozu das Gleichungssystem

$$\begin{aligned} 4\lambda_1 + 3\lambda_2 &= 0 \qquad \text{(I)}\,, \\ \lambda_1 + 2\lambda_2 &= 0 \qquad \text{(II)} \end{aligned}$$

in den zwei Variablen $\lambda_1, \lambda_2 \in \mathbb{R}$ zu lösen ist. Wir erhalten durch Kombination der Gleichungen gemäß (I)-4(II) die neue Gleichung $-5\lambda_2 = 0$ (die (I) oder (II) ersetzen kann) und lesen daraus $\lambda_2 = 0$ ab. Hierauf aufbauend liefert (II) dann auch $\lambda_1 = 0$. Also ist $\lambda_1 = \lambda_2 = 0$ tatsächlich die *einzige* Lösung des Gleichungssystems, und $\binom{4}{1}, \binom{3}{2} \in \mathbb{R}^2$ sind $\mathbb{R}$-linear unabhängig.

Definition (**Erzeugendensysteme** und **Basen**)**.** *Seien K ein Körper und V ein K-Vektorraum.*

(I) *Wir nennen $m \in \mathbb{N}$ Vektoren $b_1, b_2, \ldots, b_m \in V$ ein **Erzeugendensystem** von V (über K), wenn $\mathrm{Span}_K(b_1, b_2, \ldots, b_m) = V$ gilt. Sind die Vektoren $b_1, b_2, \ldots, b_m$ des Erzeugendensystems zusätzlich linear unabhängig, so heißen sie eine **Basis** von V (über K).*

(II) *Analog nennen wir eine Teilmenge B von V ein **Erzeugendensystem** von V (über K), wenn $\mathrm{Span}_K B = V$ gilt. Ist das Erzeugendensystem B zusätzlich linear unabhängig, so heißt es eine **Basis** von V (über K).*

*Ab und zu sprechen wir auch von einem **K-Erzeugendensystem** oder einer **K-Basis** von V.*

Die einzelnen Vektoren bzw. Elemente einer Basis bezeichnet man auch oft als **Basisvektoren**. Dieser Begriff ist aber ohne Benennung der gesamten Basis nicht wohldefiniert und normalerweise *nur im Kontext fester Basen* sinnvoll.

Bemerkungen (zu **Erzeugendensystemen** und **Basen**)**.** Seien K ein Körper, V ein K-Vektorraum und $m, n \in \mathbb{N}$.

(0) Die Konzepte für endlich viele Vektoren und endliche Teilmengen sind praktisch dieselben: Vektoren $b_1, b_2, \ldots, b_m \in V$ sind genau dann ein K-Erzeugendensystem von V, wenn $\{b_1, b_2, \ldots, b_m\}$ ein K-Erzeugendensystem von V ist. Und $b_1, b_2, \ldots, b_m \in V$ sind genau dann eine K-Basis von V, wenn sie alle verschieden sind und $\{b_1, b_2, \ldots, b_m\}$ eine K-Basis von V ist.

(1) Oft kann man einen Untervektorraum als **erzeugten Untervektorraum samt einer zugehörigen Basis** aus folgender einfachen Beobachtung **erhalten**: Sind $b_1, b_2, \ldots, b_m \in V$ linear unabhängig über K, so sind $b_1, b_2, \ldots, b_m$ immer eine K-Basis von $\mathrm{Span}_K(b_1, b_2, \ldots, b_m)$. Und ist B linear unabhängige Teilmenge von V über K, so ist B eine K-Basis von $\mathrm{Span}_K B$.

(2) Manchmal werden wir bei einer Basis $b_1, b_2, \ldots, b_m$ Wert auf die Reihenfolge der Vektoren legen. Wir fassen dann die Basisvektoren als Tupel $(b_1, b_2, \ldots, b_m)$ zusammen und sprechen manchmal auch von einer ***geordneten* Basis**.

(3) Die definierende Eigenschaft eines K-Erzeugendensystems $b_1, b_2, \ldots, b_m$ von V ist die, dass jeder Vektor $v \in V$ als K-Linearkombination $v = \sum_{j=1}^{m} \lambda_j b_j$ der Basisvektoren mit gewissen Koeffizienten $\lambda_1, \lambda_2, \ldots, \lambda_m \in K$ geschrieben werden kann. Bei einer K-Basis $b_1, b_2, \ldots, b_m$ von V sind zudem die Koeffizienten λ_j durch den Vektor v und die Basis eindeutig bestimmt, weil ansonsten die Differenz zweier Darstellungen eine nicht-triviale Darstellung des Nullvektors gäbe und dies durch lineare Unabhängigkeit ausgeschlossen ist. Man hat also für jedes $v \in V$ eine **Basisdarstellung**

$$\boxed{v = \sum_{j=1}^{m} \lambda_j b_j \qquad \textbf{mit } \textbf{\textit{eindeutigen}} \textbf{ Koeffizienten } \lambda_1, \lambda_2, \ldots, \lambda_m \in K}.$$

Zur konkreten Bestimmung der Koeffizienten ist erneut ein lineares Gleichungssystem für diese zu lösen. Auf der linken Seite des Systems stehen dabei exakt dieselben Terme wie beim Nachweis der linearen Unabhängigkeit von $b_1, b_2, \ldots, b_m$, nur auf der rechten Seite stehen statt der Nullen die Einträge des gegebenen Vektors v. Aufgrund der Übereinstimmung links kann man aber über dieselben Umformungen vorgehen und beide Aufgaben zu einem gewissen Grad simultan erledigen.

(4) Mit den n Vektoren

$$\mathrm{e}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \mathrm{e}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \mathrm{e}_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \ldots, \mathrm{e}_n = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \in K^n$$

gilt $x = \begin{pmatrix} x_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ x_2 \\ \vdots \\ 0 \end{pmatrix} + \ldots + \begin{pmatrix} 0 \\ 0 \\ \vdots \\ x_n \end{pmatrix} = \sum_{i=1}^{n} x_i \mathrm{e}_i$ für jeden Vektor $x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in K^n$. Da diese Darstellung offensichtlich eindeutig ist, bilden somit $\mathrm{e}_1, \mathrm{e}_2, \ldots, \mathrm{e}_n$ eine K-Basis von K^n, die als **kanonische Basis von K^n** oder **Standard-Basis von K^n** bezeichnet wird.

(5) Mit der vorigen Bemerkung wird klar, dass die Einträge eines Spaltenvektors aus K^n die Koeffizienten der Basisdarstellung bezüglich der kanonischen Basis sind. Aufbauend hierauf notiert man auch die **$\mathcal{B}$-Basisdarstellung** bezüglich einer beliebigen geordneten Basis $\mathcal{B} = (b_1, b_2, \ldots, b_m)$ von V manchmal in an die „normalen" Spaltenvektoren angelehnter Notation

$$\begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_m \end{bmatrix}_{\mathcal{B}} := \sum_{j=1}^{m} \lambda_j b_j \in V \qquad \text{für } \lambda_1, \lambda_2, \ldots, \lambda_m \in K\,.$$

Für die kanonische Basis $\mathcal{E} = (\mathrm{e}_1, \mathrm{e}_2, \ldots, \mathrm{e}_n)$ von K^n ist dabei natürlich $\begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_m \end{bmatrix}_{\mathcal{E}} = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_m \end{pmatrix}$.

Beispiel (zu **Basen** und **Basisdarstellungen**)**.** Bezüglich der geordneten Basis

$$\mathcal{B} := \left(\begin{pmatrix}1\\2\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}\right)$$

von $\mathbb{R}^2$ über $\mathbb{R}$ hat der Vektor $\left(\begin{smallmatrix}-3\\4\end{smallmatrix}\right) \in \mathbb{R}^2$ die Basisdarstellung

$$\begin{pmatrix}-3\\4\end{pmatrix} = 7\begin{pmatrix}1\\2\end{pmatrix} - 10\begin{pmatrix}1\\1\end{pmatrix} = \begin{bmatrix}7\\-10\end{bmatrix}_{\mathcal{B}}.$$

Die Berechnung dieser Darstellung gelingt dabei mit dem linearen Gleichungssystem

$$\begin{aligned} \lambda_1 + \lambda_2 &= -3\,, \\ 2\lambda_1 + \lambda_2 &= 4\,, \end{aligned}$$

für das man die eindeutige Lösung $\lambda_1 = 7$, $\lambda_2 = -10$ ermittelt.

Unsere nächsten Ziele sind drei **entscheidende Sätze über Basen**:

Hauptsatz (zur **Existenz von Basen**)**.** *Sei K ein Körper.* ***Jeder K-Vektorraum hat eine K-Basis.***

Satz (**Basisergänzungssatz**)**.** *Seien K ein Körper und V ein K-Vektorraum. Für jede K-linear unabhängige Teilmenge A von V gibt es eine K-Basis B von V mit $A \subset B$.*

Satz (**Basisauswahlsatz**)**.** *Seien K ein Körper und V ein K-Vektorraum. Für jedes K-Erzeugendensystem C von V gibt es eine K-Basis B von V mit $B \subset C$.*

Dabei ist der Existenzsatz für $A = \emptyset$ im Basisergänzungssatz enthalten. Tatsächlich formulieren wir als Nächstes aber sogar eine Aussage, die alle drei Sätze als Spezialfälle enthält (den Existenzsatz für $A = \emptyset$ und $C = V$, den Basisergänzungssatz für $C = V$ und den Basisauswahlsatz für $A = \emptyset$), und nur diese verallgemeinerte Aussage werden wir daher noch beweisen.

Satz. *Seien K ein Körper und V ein K-Vektorraum. Für eine K-linear unabhängige Teilmenge A von V und ein K-Erzeugendensystem C von V mit $A \subset C$ gibt es stets eine K-Basis B von V mit $A \subset B \subset C$.*

Bemerkung. Der Hauptsatz sichert zwar generell die Existenz mindestens einer Basis, bringt aber keine Möglichkeit, eine Basis explizit zu bestimmen. Tatsächlich stützt sich der noch folgende Beweis entscheidend auf das Zornsche Lemma aus Abschnitt 2.3.1 (welches wiederum auf dem Auswahlaxiom der Mengenlehre basiert) und ist überhaupt nicht konstruktiv. Konkret lässt sich etwa für den $\mathbb{Q}$-Vektorraum $\mathbb{R}$ eine Basis nicht explizit angeben. Es kann aber gezeigt werden, dass alle $\mathbb{Q}$-Basen von $\mathbb{R}$ überabzählbar sind, und daher kann man sich vorstellen, dass es eben wegen der großen Zahl der benötigten Basisvektoren keine Möglichkeit gibt, eine Basis schematisch anzugeben oder zu überblicken.

Beweis des letzten Satzes. Wir betrachten das Mengensystem

$$\mathcal{S} := \{M \in \mathcal{P}(V) \mid M \text{ linear unabhängig über } K \text{ mit } A \subset M \subset C\}$$

mit der Mengeninklusion „$\subset$“ als Ordnungsrelation auf $\mathcal{S}$ und halten $\mathcal{S} \neq \emptyset$ fest (denn wegen der K-linearen Unabhängigkeit von A gilt auf jeden Fall $A \in \mathcal{S}$). Wir zeigen nun folgende, als Voraussetzung für das Zornsche Lemma benötigte Aussage (alles bezüglich „$\subset$“):

$$\text{Jede Kette } \mathcal{K} \subset \mathcal{S} \text{ hat eine obere Schranke in } \mathcal{S}\,.$$

Für $\mathcal{K} = \emptyset$ ist jedes Element von $\mathcal{S}$ eine obere Schranke und dies klar (aber nur, weil $\mathcal{S} \neq \emptyset$). Für $\mathcal{K} \neq \emptyset$ ist $\bigcup \mathcal{K} = \bigcup_{M \in \mathcal{K}} M$ die benötigte Schranke, sofern $\bigcup \mathcal{K} \in \mathcal{S}$ gilt. Dafür weisen wir erst K-lineare Unabhängigkeit von $\bigcup \mathcal{K}$ nach: Für endlich viele Vektoren $v_1, v_2, \ldots, v_m \in \bigcup \mathcal{K}$ gibt es $M_1, M_2, \ldots, M_m \in \mathcal{K}$ mit $v_i \in M_i$ für alle $i \in \{1, 2, \ldots, m\}$. Da $\mathcal{K}$ eine Kette ist, ist unter $M_1, M_2, \ldots, M_m$ eine größte Menge M_{i_0} mit $i_0 \in \{1, 2, \ldots, m\}$, so dass $M_i \subset M_{i_0}$ für alle $i \in \{1, 2, \ldots, m\}$ gilt. Es sind also $v_1, v_2, \ldots, v_m \in M_{i_0}$, und M_{i_0} ist K-linear unabhängig (wegen $M_{i_0} \in \mathcal{K} \subset \mathcal{S}$ und der Wahl von $\mathcal{S}$). Also sind $v_1, v_2, \ldots, v_m$ ebenfalls K-linear unabhängig, und $\bigcup \mathcal{K}$ ist insgesamt K-linear unabhängig. Nach Wahl von $\mathcal{S}$ gilt zudem $A \subset M \subset C$ für alle $M \in \mathcal{K} \neq \emptyset$ und damit $A \subset \bigcup \mathcal{K} \subset C$. Insgesamt ist wie benötigt $\bigcup \mathcal{K} \in \mathcal{S}$ und die obige, benötigte Aussage gezeigt.

Damit können wir das Zornsche Lemma aus Abschnitt 2.3.1 auf $\mathcal{S}$ anwenden und erhalten die Existenz eines bezüglich Mengeninklusion maximalen Elements B von $\mathcal{S}$. Nach Wahl von $\mathcal{S}$ gilt $A \subset B \subset C$, und B ist K-linear unabhängig. Um die Behauptung des Satzes zu erhalten, müssen wir also nur noch aus der Maximalität von B folgern, dass B ein K-Erzeugendensystem (und damit eine K-Basis) von V ist. Sei hierzu $v \in C \setminus B$. Wegen der Maximalität von B kann dann $B \dot\cup \{v\}$ nicht in $\mathcal{S}$ sein. Da $A \subset B \dot\cup \{v\} \subset C$ erfüllt ist, erzwingt dies K-lineare Abhängigkeit von $B \dot\cup \{v\}$. Es gibt also $m \in \mathbb{N}$, $b_1, b_2, \ldots, b_m \in B$ und Koeffizienten $\lambda, \lambda_1, \lambda_2, \ldots, \lambda_m \in K$, die nicht alle Null sind, mit $\lambda v + \sum_{i=1}^m \lambda_i b_i = 0$. Ist $\lambda = 0$, so erhalten wir mit $\sum_{i=1}^m \lambda_i b_i = 0$, wobei nicht alle λ_i Null sind, einen Widerspruch zur K-linearen Unabhängigkeit von B. Also ist $\lambda \neq 0$, wir können zu $v = -\frac{1}{\lambda} \sum_{i=1}^m \lambda_i b_i$ auflösen und $v \in \operatorname{Span}_K B$ ablesen. Insgesamt haben wir damit $C \setminus B \subset \operatorname{Span}_K B$ gezeigt und bekommen wegen der trivialen Inklusion $B \subset \operatorname{Span}_K B$ sofort auch $C \subset \operatorname{Span}_K B$. Hieraus folgt mit der Eigenschaft des K-Erzeugendensystems C schließlich $V = \operatorname{Span}_K C \subset \operatorname{Span}_K(\operatorname{Span}_K B) = \operatorname{Span}_K B$. Also ist B ein K-Erzeugendensystem von V und der Beweis komplett. □

Aus dem Basisergänzungs- und dem Basisauswahlsatz ergeben sich zwei grundlegende Charakterisierungen von Basen, die beim vorigen Beweis teils schon mitschwangen.

Korollar. *Für einen Körper K, einen K-Vektorraum V und $B \subset V$ sind* ***äquivalent***:

(1) *B ist eine* ***K-Basis*** *von V.*

(2) *B ist eine bezüglich „$\subset$“* ***maximale K-linear unabhängige Teilmenge*** *von V.*

(3) *B ist ein bezüglich „$\subset$“* ***minimales K-Erzeugendensystem*** *von V.*

Beweis. Die Implikation (2) $\Longrightarrow$ (1) ergibt sich mit dem Basisergänzungssatz: Die maximale K-linear unabhängige Teilmenge B von V kann zu einer K-Basis von V ergänzt werden, die insbesondere K-linear unabhängig ist und wegen der Maximalität mit B übereinstimmt. Analog ergibt sich (3) $\Longrightarrow$ (1) mit dem Basisauswahlsatz. Die Implikationen (1) $\Longrightarrow$ (2) und (1) $\Longrightarrow$ (3) sind Thema der Übungen. □

Im Rest dieses Abschnitts geht es maßgeblich um den Begriff der Dimension. Um diese definieren zu können, benötigen wir aber zunächst noch ein etwas stärker technisch angehauchtes Resultat über Basen von Vektorräumen.

Satz (Basisaustauschsatz von Steinitz). *Seien K ein Körper, V ein K-Vektorraum und B eine K-Basis von V. Für $n \in \mathbb{N}$ und K-linear unabhängige Vektoren $v_1, v_2, \ldots, v_n \in V$ gibt es n verschiedene Vektoren $b_1, b_2, \ldots, b_n \in B$, so dass auch $(B \setminus \{b_1, b_2, \ldots, b_n\}) \dot\cup \{v_1, v_2, \ldots, v_n\}$ eine K-Basis von V ist.*

Grob gesprochen besagt der Satz, dass gegebene, untereinander linear unabhängige Vektoren $v_1, v_2, \ldots, v_n \in V$ in einer ebenfalls gegebenen Basis B gewisse Basisvektoren $b_1, b_2, \ldots, b_n \in B$ ersetzen können, ohne dass hierdurch die Basiseigenschaft zerstört wird. Man kann also „alte“ Basisvektoren $b_1, b_2, \ldots, b_n$ durch die „neuen“ Basisvektoren $v_1, v_2, \ldots, v_n$ austauschen.

Der Schlüssel zum Beweis des Austauschsatzes ist tatsächlich die Behandlung des Falls $n = 1$, für den wir noch eine minimal präzisere Aussage (nämlich inklusive Kriterium, *welcher* Basisvektor weggelassen werden kann) als Lemma formulieren und beweisen:

Lemma. *Seien K ein Körper, V ein K-Vektorraum und B eine K-Basis von V. Ist für $v \in V$ in der Basisdarstellung $v = \sum_{i=1}^{\ell} \lambda_i \beta_i$ mit $\ell \in \mathbb{N}$, $\beta_1, \beta_2, \ldots, \beta_\ell \in B$, $\lambda_1, \lambda_2, \ldots, \lambda_\ell \in K$ für ein $i_0 \in \{1, 2, \ldots, \ell\}$ der Koeffizient $\lambda_{i_0} \neq 0$, so ist auch $(B \setminus \{\beta_{i_0}\}) \dot\cup \{v\}$ eine K-Basis von V.*

Beweis des Lemmas. Zunächst ist $(B \setminus \{\beta_{i_0}\}) \cap \{v\} = \emptyset$ und „$\dot\cup$“ in der Aussage des Lemmas berechtigt, weil in der eindeutigen B-Basisdarstellung eines Basisvektors $v \in B \setminus \{\beta_{i_0}\}$ im Widerspruch zur Voraussetzung $\lambda_{i_0} = 0$ wäre.

Wir komplettieren den Beweis durch die Nachweise, dass $(B \setminus \{\beta_{i_0}\}) \dot\cup \{v\}$ einerseits ein K-Erzeugendensystem von V, andererseits K-linear unabhängig ist.

Für die Eigenschaft als Erzeugendensystem lösen wir die B-Basisdarstellung $v = \sum_{i=1}^{\ell} \lambda_i \beta_i$ zu $\beta_{i_0} = \lambda_{i_0}^{-1}\big(v - \sum_{i \in \{1,2,\ldots,\ell\} \setminus \{i_0\}} \lambda_i \beta_i\big)$ auf. Damit können wir das Auftreten von β_{i_0} in der B-Basisdarstellung eines Vektors $v \in V$ eliminieren und β_{i_0} durch v und die β_i mit $i \neq i_0$ ersetzen. Somit ist jedes $v \in V$ eine K-Linearkombination von Vektoren aus $(B \setminus \{\beta_{i_0}\}) \dot\cup \{v\}$, und $(B \setminus \{\beta_{i_0}\}) \dot\cup \{v\}$ ist ein K-Erzeugendensystem von V.

Zum Beweis der K-linearen Unabhängigkeit von $(B \setminus \{\beta_{i_0}\}) \dot\cup \{v\}$ schreiben wir 0 als Linearkombination von Vektoren aus $(B \setminus \{\beta_{i_0}\}) \dot\cup \{v\}$ und zeigen, dass diese Linearkombination trivial sein muss. Wir können ohne Einschränkung annehmen, dass die schon im Lemma auftretenden Basisvektoren $\beta_1, \beta_2, \ldots, \beta_{i_0-1}, \beta_{i_0+1}, \ldots, \beta_\ell$ bei der Linearkombination, eventuell mit Null-Koeffizienten, vorkommen, können also $\mu v + \sum_{i \in \{1,2,\ldots,m\} \setminus \{i_0\}} \mu_i \beta_i = 0$ mit beliebigen $m \in \mathbb{N}_{\geq \ell}$, $\beta_{\ell+1}, \beta_{\ell+2}, \ldots, \beta_m \in B$, $\mu, \mu_1, \mu_2, \ldots, \mu_{i_0-1}, \mu_{i_0+1}, \ldots, \mu_m \in K$ ansetzen. Vereinbaren

wir $\lambda_i := 0$ für $i \in \mathbb{N}_{>\ell}$, so können wir $v = \sum_{i=1}^{m} \lambda_i \beta_i$ in den Ansatz einsetzen und bekommen $\mu\lambda_{i_0}\beta_{i_0} + \sum_{i\in\{1,2,\ldots,m\}\setminus\{i_0\}} (\mu_i + \mu\lambda_i)\beta_i = 0$. Wegen der linearen Unabhängigkeit der β_i folgen $\mu\lambda_{i_0} = 0$ und $\mu_i + \mu\lambda_i = 0$ für $i \in \{1, 2, \ldots, m\} \setminus \{i_0\}$. Wegen $\lambda_{i_0} \neq 0$ bedeutet dies, dass mit $\mu = 0$ und $\mu_i = 0$ für $i \in \{1, 2, \ldots, m\} \setminus \{i_0\}$ alle Koeffizienten des Ansatzes Null sind. Also ist $(B \setminus \{\beta_{i_0}\}) \dot\cup \{v\}$ wie behauptet K-linear unabhängig. □

Beweis des Basisaustauschsatzes. Wir zeigen die Behauptung des Satzes durch vollständige Induktion nach $n \in \mathbb{N}$.

Beim Induktionsanfang für $n = 1$ ist $v_1 \in V$ nach Voraussetzung linear unabhängig, also $v_1 \neq 0$. In der Basisdarstellung $v = \sum_{i=1}^{\ell} \lambda_i \beta_i$ mit $\ell \in \mathbb{N}$, $\beta_1, \beta_2, \ldots, \beta_\ell \in B$, $\lambda_1, \lambda_2, \ldots, \lambda_\ell \in K$ ist daher $\lambda_{i_0} \neq 0$ für mindestens ein $i_0 \in \{1, 2, \ldots, \ell\}$. Nach dem Lemma ist $(B \setminus \{\beta_{i_0}\}) \dot\cup \{v_1\}$ eine Basis von V, und wir erhalten die Behauptung des Satzes für $n = 1$ mit $b_1 = \beta_{i_0}$.

Beim Induktionsschluss von $n \in \mathbb{N}$ zu $n+1$ sind linear unabhängige $v_1, v_2, \ldots, v_{n+1} \in V$ gegeben. Da insbesondere $v_1, v_2, \ldots, v_n$ linear unabhängig sind, ist nach Induktionsannahme $(B \setminus \{b_1, b_2, \ldots, b_n\}) \dot\cup \{v_1, v_2, \ldots, v_n\}$ eine Basis von V. Nun hat v_{n+1} eine Basisdarstellung $v_{n+1} = \sum_{i=1}^{\ell} \lambda_i \beta_i + \sum_{j=1}^{n} \mu_j v_j$ mit $\ell \in \mathbb{N}$, $\beta_1, \ldots, \beta_\ell \in B \in B \setminus \{b_1, b_2, \ldots, b_n\}$, $\lambda_1, \ldots, \lambda_\ell, \mu_1, \ldots, \mu_n \in K$. Im Fall $\lambda_1 = \lambda_2 = \ldots = \lambda_\ell = 0$ wäre der Nullvektor $0 = v_{n+1} - \sum_{j=1}^{n} \mu_j v_j$ nicht-triviale Linearkombination von $v_1, v_2, \ldots, v_n, v_{n+1}$, was im Widerspruch zur linearen Unabhängigkeit von $v_1, v_2, \ldots, v_n, v_{n+1}$ stünde. Also gibt es mindestens ein $i_0 \in \{1, 2, \ldots, \ell\}$ mit $\lambda_{i_0} \neq 0$. Das Lemma, angewandt auf die vorausgehende Basisdarstellung von v_{n+1}, erlaubt daher, in der Basis $(B \setminus \{b_1, b_2, \ldots, b_n\}) \dot\cup \{v_1, v_2, \ldots, v_n\}$ den Vektor $b_{n+1} := \beta_{i_0} \in B \setminus \{b_1, b_2, \ldots, b_n\}$ durch v_{n+1} auszutauschen. Wir erhalten, dass $(B \setminus \{b_1, b_2, \ldots, b_n, b_{n+1}\}) \dot\cup \{v_1, v_2, \ldots, v_n, v_{n+1}\}$ eine Basis von V ist, und der Induktionsschritt ist komplett. □

Als zentrale Anwendung des Basisaustauschsatzes können wir die Dimension eines Vektorraums als die eindeutig bestimmte (!) Länge seiner Basen einführen:

Hauptsatz (zur **Länge von Basen**). *Seien K ein Körper und V ein K-Vektorraum. Ist V über K endlich erzeugt (d.h. gibt es ein K-Erzeugendensystem von V aus endlich vielen Vektoren), so hat **jede K-Basis** B von V die **gleiche Länge** $|B| \in \mathbb{N}_0$, besteht also aus der gleichen endlichen Zahl $|B|$ von Vektoren.*

Definition (**Dimension**). *Sei K ein Körper. Einen über K endlich erzeugten K-Vektorraum V nennen wir **endlich-dimensional** (über K), und erklären die **Dimension** $\dim V = \dim_K V \in \mathbb{N}_0$ von V (über K) als die eindeutige Länge $|B|$ einer K-Basis B von V. Einen über K nicht endlich erzeugten K-Vektorraum V nennen wir **unendlich-dimensional** (über K), und setzen für einen solchen $\dim V := \dim_K V := \infty$.*

Beweis des Hauptsatzes. Da ein Erzeugendensystem nach dem Basisauswahlsatz immer eine Basis enthält, besitzt der endlich erzeugte Vektorraum V eine endliche Basis B mit $|B| \in \mathbb{N}_0$. Wir zeigen, dass für jede weitere Basis $\widetilde{B}$ von V notwendig $|\widetilde{B}| = |B|$ gilt. Wäre $|B| > |\widetilde{B}|$, so ergäbe sich durch Anwendung des Basisaustauschsatzes (oder trivial im Fall $n = 0$), dass $(B \setminus \{b_1, b_2, \ldots, b_n\}) \dot\cup \widetilde{B}$ mit $n := |\widetilde{B}| \in \mathbb{N}_0$ und gewissen $b_1, b_2, \ldots, b_n \in B$ eine Basis von V wäre. Wegen $|B| > |\widetilde{B}| = n$ wäre also $\widetilde{B}$ *nicht* maximale linear unabhängige Teilmenge von V, und wir erhielten einen Widerspruch zur Basiseigenschaft von $\widetilde{B}$. Wäre $|\widetilde{B}| > |B|$, so ergäbe sich durch völlig analoge Argumentation mit $n := |B| \in \mathbb{N}_0$ ein Widerspruch. Also ist $|\widetilde{B}| = |B|$. □

Bemerkungen (zur **Mächtigkeit von Basen und verwandten Systemen**)**.** Seien K ein Körper und V ein K-Vektorraum.

(1) Im unendlich-dimensionalen Fall $\dim_K V = \infty$ kann mit dem Auswahlaxiom die Variante des Hauptsatzes gezeigt werden, dass alle K-Basen von V zueinander gleichmächtig sind.

(Beweisskizze: Seien A und B Basen von V. Für jedes $a \in A$ gibt es dann $m(a) \in \mathbb{N}$ und $b_1(a), b_2(a), \ldots, b_{m(a)}(a) \in B$ mit $a \in \mathrm{Span}\{b_1(a), b_2(a), \ldots, b_{m(a)}(a)\}$. Mit A ist auch $\bigcup_{a\in A}\{b_1(a), b_2(a), \ldots, b_{m(a)}(a)\}$ ein Erzeugendensystem von V. Weil die Basis B ein *minimales* Erzeugendensystem von V ist, folgt daraus $\bigcup_{a\in A}\{b_1(a), b_2(a), \ldots, b_{m(a)}(a)\} = B$. Mit dem Auswahlaxiom ergibt sich aus dieser Gleichheit eine Injektion $B \to A\times\mathbb{N}$, die jedes $b \in B$ auf ein $(a, i) \in A\times\mathbb{N}$ mit $i \in \{1, 2, \ldots, m(a)\}$ und $b_i(a) = b$ abbildet. Gemäß einem weiteren Argument mit dem Auswahlaxiom, auf das wir hier nicht im Detail eingehen, ist $A\times\mathbb{N}$ für die unendliche Menge A gleichmächtig[2] zu A. Insgesamt erhalten wir eine Injektion $B \to A$. Dieselben Argumente mit vertauschten Rolle von A und B ergeben eine weitere Injektion $A \to B$, und mit dem in Abschnitt 2.5 erwähnten Satz von Cantor-Schröder-Bernstein folgt Gleichmächtigkeit von A und B.)

(2) Im **endlich-dimensionalen Fall mit $n := \dim_K V \in \mathbb{N}_0$** ...

- besteht eine **K-linear unabhängige Teilmenge** von V aus ***höchstens n* Vektoren**,
- besteht ein **K-Erzeugendensystem** von V aus ***mindestens n* Vektoren**.

Dies folgt aus dem Basisergänzungs- beziehungsweise dem Basisauswahlsatz.

Beispiele (zur **Dimension**)**.** Sei K ein Körper.

(0) Der Nullvektorraum $\{0\}$ ist der einzige Vektorraum der Dimension 0 über K.

(1) Das absolute **Standard-Beispiel eines *endlich-dimensionalen* K-Vektorraums** ist der Raum $\boldsymbol{K^n}$ der Vektoren mit $n \in \mathbb{N}$ Einträgen aus K. Da die kanonische Basis von K^n Länge n hat, ist

$$\boxed{\dim_K K^n = n}.$$

(2) Drei Beispiele für *unendlich-dimensionale* K-Vektorräume sind der Raum $K[\mathrm{X}]$ der Polynome über K, der Raum $K^{(\mathbb{N})} = \{(x_n)_{n\in\mathbb{N}} \mid x_n = 0 \text{ für } n \gg 1\}$ der abbrechenden Folgen über K und der Raum $K^{\mathbb{N}}$ aller Folgen über K. Eine Basis von $K[\mathrm{X}]$ ist $\{1, \mathrm{X}, \mathrm{X}^2, \mathrm{X}^3, \mathrm{X}^4, \ldots\}$, und eine Basis von $K^{(\mathbb{N})}$ ist $\{(1,0,0,0,0,\ldots), (0,1,0,0,0,\ldots), (0,0,1,0,0,\ldots), \ldots\}$. Eine Basis von $K^{\mathbb{N}}$ ist notwendig überabzählbar und lässt sich nicht explizit angeben.

Als **wichtige Folgerungen für den künftigen Umgang mit Unterräumen und Dimensionen** halten wir fest:

Korollar. *Seien K ein Körper, V, V_1, V_2 Vektorräume über K und U, U_1, U_2 Untervektorräume von V über K. Dann gelten (wobei insbesondere **immer $\boldsymbol{U \subset V}$ vorausgesetzt** ist):*

(I) $\dim_K(V_1\times V_2) = \dim_K V_1 + \dim_K V_2$,

(II) **$\dim_K U \leq \dim_K V$ *mit „=“ nur für $U = V$ oder* $\dim_K U = \dim_K V = \infty$**
(*wobei insbesondere die **Charakterisierung des Gleichheitsfalls oft nützlich** ist*),

(III) *die Existenz eines K-Untervektorraums U^{c} von V mit $U \oplus U^{\mathrm{c}} = V$ (genannt ein **komplementärer Untervektorraum** zu U in V)*,

[2] Speziell für abzählbar unendliches A folgt die Gleichmächtigkeit von $A\times\mathbb{N}$ und A aus dem in Abschnitt 2.5 beschriebenen ersten Cantorschen Diagonalverfahren. Allgemeine unendliche A können durch eine Argumentation mit dem Auswahlaxiom darauf zurückgeführt werden.

(IV) $\dim_K(V/U) + \dim_K U = \dim_K V$ *(für den Faktorraum V/U von V nach U),*

(V) *die* ***Dimensionsformel für Untervektorräume***

$$\boxed{\dim_K(U_1{+}U_2) + \dim_K(U_1 \cap U_2) = \dim_K U_1 + \dim_K U_2}$$

und speziell $\dim_K(U_1 \oplus U_2) = \dim_K U_1 + \dim_K U_2$ *im Fall* $U_1 \cap U_2 = \{0\}$.

Beweis des Korollars. Zum Beweis von Teil (I) seien B_1 eine Basis von V_1 und B_2 eine Basis von V_2. Dann ist $B := (B_1{\times}\{0\}) \dot\cup (\{0\}{\times}B_2)$ eine Basis von $V_1{\times}V_2$, und es folgt $\dim(V_1{\times}V_2) = |B| = |B_1|{+}|B_2| = \dim V_1 {+} \dim V_2$.

Für Teil (II) sei B eine Basis von U. Nach dem Basisergänzungssatz gibt es eine Basis B^* von V mit $B \subset B^*$. Es folgt $|B| \leq |B^*|$ mit „=“ nur für $B = B^*$ oder $|B| = |B^*| = \infty$. Wir erhalten also $\dim U = |B| \leq |B^*| = \dim V$ mit „=“ nur für $U = \operatorname{Span} B = \operatorname{Span} B^* = V$ oder $\dim U = \dim V = \infty$.

Für Teil (III) betrachten wir B und B^* wie gerade zuvor und setzen $U^{\mathrm{c}} := \operatorname{Span}(B^*\backslash B)$. Da B^* ein Erzeugendensystem von V ist, gilt dann $U{+}U^{\mathrm{c}} = \operatorname{Span} B {+} \operatorname{Span}(B^*\backslash B) = V$. Da B^* linear unabhängige Teilmenge von V ist, folgt zudem $U \cap U^{\mathrm{c}} = \operatorname{Span} B \cap \operatorname{Span}(B^*\backslash B) = \{0\}$ (denn für $v \in \operatorname{Span} B \cap \operatorname{Span}(B^*\backslash B)$ ist $v = \sum_{b\in E} \lambda_b b = \sum_{b\in E^*} \lambda_b b$ für endliche Teilmengen $E \subset B$ und $E^* \subset B^*\backslash B$ und gewisse $\lambda_b \in B$; aus $\sum_{b\in E} \lambda_b b - \sum_{b\in E^*} \lambda_b b = 0$ ergibt sich dann, dass alle λ_b Null sind, also auch $v = 0$).

Für Teil (IV) betrachten wir für B und B^* wie zuvor jetzt $B' := \{b{+}U \mid b \in B^*\backslash B\} \subset V/U$. Wir zeigen zunächst, dass B' ein Erzeugendensystem von V/U ist. Für $v{+}U \in V/U$ mit $v \in V$ nutzen wir dazu die B^*-Basisdarstellung $v = \sum_{b\in F^*} \lambda_b b$ mit endlichem $F^* \subset B^*$ und gewissen $\lambda_b \in K$. Es folgt $v{+}U = \sum_{b\in F^*} \lambda_b(b{+}U) = \sum_{b\in F^*\backslash B} = \lambda_b(b{+}U) \in \operatorname{Span}(B^*\backslash B)$ in V/U, weil $b{+}U = 0{+}U = 0$ in V/U für $b \in B \subset U$ gilt. Also ist B' ein Erzeugendensystem von V/U. Weiter zeigen wir, dass B' in V/U linear unabhängig ist. Sei dazu $\sum_{b\in E^*} \lambda_b(b{+}U) = 0$ in V/U für endliches $E^* \subset B^*\backslash B$ und gewisse $\lambda_b \in K$. Mit anderen Worten bedeutet dies $\sum_{b\in E^*} \lambda_b b \in U$ und $\sum_{b\in E^*} \lambda_b b = \sum_{b\in E} \lambda_b b$ für endliches $E \subset B$ (und weitere $\lambda_b \in K$). Mit der linearen Unabhängigkeit von $E \dot\cup E^* \subset B$ folgt $\lambda_b = 0$ für alle $b \in E \dot\cup E^*$, womit insbesondere gezeigt ist, dass alle $b{+}U$ mit $b \in B^*\backslash B$ in V/U verschieden sind und B' in V/U linear unabhängig ist. Damit ist B' eine Basis von V/U, und wir erhalten insgesamt $\dim(V/U){+}\dim U = |B'|{+}|B| = |B^*\backslash B|{+}|B| = |B^*| = \dim V$.

Bezüglich Teil (V) behandeln wir erst den Fall $U_1 \cap U_2 = \{0\}$ (in dem wir $U_1{\oplus}U_2$ schreiben dürfen). Seien B_1 eine Basis von U_1 und B_2 eine Basis von U_2. Mit ähnlichen Argumenten wie beim Nachweis von (III) folgt dann, dass $B_1 \dot\cup B_2$ eine Basis von $U_1{\oplus}U_2$ ist, und wir erhalten $\dim(U_1{\oplus}U_2) = |B_1 \dot\cup B_2| = |B_1|{+}|B_2| = \dim U_1 {+} \dim U_2$.

Für den allgemeinen Fall von Teil (V) benutzen wir, dass es gemäß (III) einen zu $U_1 \cap U_2$ in U_2 komplementären Unterraum $\widetilde{U}_2$ mit $U_2 = (U_1 \cap U_2) \oplus \widetilde{U}_2$ gibt. Es folgt dann leicht $U_1 + U_2 = U_1 \oplus \widetilde{U}_2$, so dass wir durch zweimalige Anwendung des schon behandelten Spezialfalls $\dim(U_1{+}U_2) + \dim(U_1 \cap U_2) = \dim U_1 + \dim \widetilde{U}_2 + \dim(U_1 \cap U_2) = \dim U_1 + \dim U_2$ erhalten. □

Im Folgenden reißen wir **affine Analoga der betrachteten Begriffe** lineare Unabhängigkeit, Erzeugen(densystem), Basis, Dimension und Dimensionsformel zumindest an.

Definitionen & Bemerkungen (zur **Dimension von *affinen* Unterräumen**). *Seien K ein Körper und V ein K-Vektorraum.*

(I) *Wir sagen für $\ell \in \mathbb{N}_0$, dass sich $(\ell{+}1)$ Punkte $x_0, x_1, x_2, x_3, \ldots, x_{\ell-1}, x_\ell \in V$* ***in allgemeiner Lage*** *befinden, wenn die ℓ Vektoren $x_1{-}x_0, x_2{-}x_0, x_3{-}x_0, \ldots, x_\ell{-}x_0$ (über K) linear unabhängig sind.*

Am besten versteht man dieses Konzept anhand der Spezialfälle $\ell = 0, 1, 2, 3$ in $V = \mathbb{R}^n$:

- $\ell = 0$: Ein Punkt x_0 ist immer in allgemeiner Lage.
- $\ell = 1$: Zwei Punkte x_0, x_1 sind in allgemeiner Lage, wenn $x_1 \neq x_0$ ist.
- $\ell = 2$: Drei Punkte x_0, x_1, x_2 sind in allgemeiner Lage, wenn es keine Gerade durch alle drei Punkte gibt.
- $\ell = 2$: Vier Punkte x_0, x_1, x_2, x_3 sind in allgemeiner Lage, wenn es keine Ebene durch alle vier Punkte gibt.

(Übrigens sieht es in der Definition so aus, als spiele der zuerst genannte Punkt x_0 beim Konzept der allgemeinen Lage eine andere Rolle als die anderen Punkte, an den Spezialfällen wird aber klar, dass dem wohl nicht so ist. Tatsächlich kann man dies auch formal einsehen, indem man sich mit der Definition der linearen Unabhängigkeit überlegt, dass lineare Unabhängigkeit von $x_1{-}x_0, x_2{-}x_0, x_3{-}x_0, \ldots, x_\ell{-}x_0$ äquivalent zu linearer Unabhängigkeit von etwa $x_0{-}x_1, x_2{-}x_1, x_3{-}x_1 \ldots, x_\ell{-}x_1$ ist.)

(II) *Die* ***Dimension eines affinen Unterraums*** *A von V erklärt man unter Rückgriff auf die Darstellung*

$$A = x + U_A$$

mit $x \in A$ und **eindeutigem** *Untervektorraum U_A von V als*

$$\dim_K A := \dim_K U_A \in \mathbb{N}_0 \cup \{\infty\}$$

In $V = \mathbb{R}^n$ entspricht ein affiner Unterraum ...

- der Dimension 0 einem einzelnen Punkt,
- der Dimension 1 einer Gerade,
- der Dimension 2 einer Ebene,
- der Dimension 3 einem Raum wie dem uns umgebenden

und muss dabei anders als ein Untervektorraum ***nicht*** **durch den Ursprung 0** gehen.

(III) *Ist A affiner Unterraum endlicher Dimension $n := \dim A \in \mathbb{N}_0$ von V, so gibt es $(n{+}1)$ Punkte $x_0, x_1, x_2, \ldots, x_n \in A$ in allgemeiner Lage mit $\mathrm{Af}(\{x_0, x_1, x_2, \ldots, x_n\}) = A$ in V, wobei $\mathrm{Af}(A)$ den von einer nicht-leeren Menge $A \subset V$ aufgespannten affinen Unterraum von V bezeichnet (vergleiche dazu Bemerkung (3) zu affinen Unterräumen in Abschnitt 6.1). Man kann und sollte sich solche Punkte $x_0, x_1, x_2, \ldots, x_n$ als eine Art affine Basis von A vorstellen, die nun bei Dimension n aber aus $n{+}1$ Punkten besteht. Die Analogie zur Dimension bei Untervektorräumen wird auch dadurch fortgeführt, dass in einem affinen Unterraum der Dimension $n \in \mathbb{N}_0$ höchstens $n{+}1$ Punkte in allgemeiner Lage sind und eine diesen affinen Unterraum aufspannende Menge aus mindestens $n{+}1$ Punkten besteht.*

(IV) *Da $A_1 \cap A_2 = \emptyset$ für affine Unterräume A_1 und A_2 von V möglich und $\emptyset$ (nach unserer Definition)* kein *affiner Unterraum ist, erhalten wir die* ***Dimensionsformel für affine Unterräume*** *A_1 und A_2 in der Form*

$$\begin{aligned} \dim(\mathrm{Af}(A_1 \cup A_2)) + \dim(A_1 \cap A_2) &= \dim A_1 + \dim A_2\,, && \text{falls } A_1 \cap A_2 \neq \emptyset\,, \\ \dim(\mathrm{Af}(A_1 \cup A_2)) + \dim(U_{A_1} \cap U_{A_2}) &= \dim A_1 + \dim A_2 + 1\,, && \text{falls } A_1 \cap A_2 = \emptyset\,. \end{aligned}$$

(*wieder mit dem von $A_1 \cup A_2$ aufgespannten affinen Unterraum $\mathrm{Af}(A_1 \cup A_2)$*).

Sind etwa A_1 und A_2 zwei Geraden in $V = \mathbb{R}^n$, so sind hier folgende Fälle möglich: Die obere Formel greift, falls die Geraden übereinstimmen und die immer noch gleiche Gerade aufspannen (dann 1+1 = 1+1) oder die Geraden sich in einem Punkt schneiden und eine Ebene aufspannen (dann 2+0 = 1+1). Die untere Formel greift, falls die Geraden parallel sind und eine Ebene aufspannen (dann 2+1 = 1+1+1) oder die Geraden windschief sind und einen Raum aufspannen (dann 3+0 = 1+1+1).

Die Beweise der Behauptungen in (III) und (IV) erfolgen durch Zurückführung auf den Fall von Untervektorräumen. Wir gehen diesbezüglich nicht in Details, erwähnen aber noch kurz, dass die zusätzliche 1 auf der rechten Seite der Dimensionsformel im Fall $A_1 \cap A_2 = \emptyset$ im Wesentlichen daher kommt, dass man in diesem Fall einen zusätzlichen Richtungsvektor und damit eine zusätzliche Dimension benötigt, um überhaupt von A_1 zu A_2 zu kommen.

6.3 Matrizen und lineare Abbildungen

Wie in Abschnitt 3.3 für Gruppen, Ringe und Körper führen wir wir jetzt auch für Vektorräume zugehörige Struktur-erhaltende Abbildungen, genannt Homomorphismen, ein. Wie wir etwas später in diesem Abschnitt sehen werden, kann man sich im (endlich-dimensionalen) Vektorraum-Fall aber einen besonders guten Überblick über solche Abbildungen verschaffen und ein schematisches Rechnen mit ihnen einführen. Die Definition und die ersten Bemerkungen dazu sind aber weitgehend analog zu Abschnitt 3.3, weshalb wir uns fürs Erste kurz fassen.

Definitionen (**lineare Abbildungen**). *Seien K ein Körper und V, W zwei K-Vektorräume.*

(I) *Eine Abbildung $\varphi\colon V \to W$ heißt ein **Homomorphismus** (von K-Vektorräumen) oder eine **(K-)lineare Abbildung**, wenn gelten:*

- ***Verträglichkeit mit Vektoraddition:*** *$\varphi(v+\widetilde{v}) = \varphi(v)+\varphi(\widetilde{v})$ für alle $v, \widetilde{v} \in V$,*
- ***Verträglichkeit mit Skalarmultiplikation:*** *$\varphi(sv) = s\varphi(v)$ für alle $s \in K$, $v \in V$.*

(II) *Ein Homomorphismus heißt **Monomorphismus**, **Epimorphismus** bzw. **Isomorphismus**, wenn er injektiv, surjektiv bzw. bijektiv ist. Gibt es zwischen V und W einen Isomorphismus, so heißen V und W (zueinander) **isomorph**. Ein Homomorphismus $V \to V$ mit gleichem Definitionsbereich und Ziel heißt **Endomorphismus**, einen bijektiven Endomorphismus nennen wir **Automorphismus**. Die Mengen aller Homo- und aller Isomorphismen $V \to W$ bezeichnen wir mit $\mathrm{Hom}_K(V,W) = \mathcal{L}_K(V,W)$ und $\mathrm{Iso}_K(V,W)$, für Endo- und Automorphismen vereinbaren wir $\mathrm{End}_K(V) := \mathcal{L}_K(V) := \mathrm{Hom}_K(V,V)$ und $\mathrm{Aut}_K(V) := \mathrm{Iso}_K(V,V)$ (wobei auf den Index $_K$ später auch öfter verzichtet wird).*

Bemerkungen (zu **linearen Abbildungen**). Seien K ein Körper, V, W, X drei K-Vektorräume.

(1) Eine K-lineare Abbildung $\varphi\colon V \to W$ ist insbesondere ein Gruppenhomomorphismus von $(V,+)$ nach $(W,+)$ und erfüllt als solcher, wie in Abschnitt 3.3 schon bemerkt, automatisch $\varphi(0_V) = 0_W$ sowie $\varphi(-v) = -\varphi(v)$ für alle $v \in V$

(2) Für K-lineare Abbildungen $\varphi\colon V \to W$ und $\psi\colon W \to X$ bleibt auch ihre Komposition $\psi \circ \varphi\colon V \to X$ stets K-linear. Dies folgt sofort aus der Definition.

Für eine bijektive K-lineare Abbildung (die wir ja Isomorphismus nennen) $\varphi\colon V \to W$ ist die Umkehrabbildung $\varphi^{-1}\colon W \to V$ ebenfalls K-linear. Der Nachweis erfolgt ebenfalls mit der Definition und ist Thema der Übungen.

(3) Die Mengen $\mathrm{Hom}_K(V,W)$ und $\mathrm{End}_K(V)$ der **Homo- und Endomorphismen** zwischen festen Vektorräumen sind **selbst K-Vektorräume**, genauer sind sie K-Untervektorräume von $\mathrm{Abb}(V,W)$ bzw. $\mathrm{Abb}(V)$ mit der punktweisen Addition und Skalarmultiplikation.

Die Endomorphismen $\mathrm{End}_K(V)$ bilden mit der punktweisen Addition und der Komposition zudem einen Ring $(\mathrm{End}_K(V), +, \circ)$, den **Endomorphismenring** von V.

Die Automorphismen $\mathrm{Aut}_K(V)$ werden mit der Komposition zu einer Gruppe $(\mathrm{Aut}_K(V), \circ)$, der **Automorphismengruppe** von V.

Als zweites zentrales Konzept dieses Abschnitts führen wir jetzt Matrizen ein.

Definitionen (Matrizen). *Seien K ein Körper und $m, n, p \in \mathbb{N}$.*

(I) *Eine Familie $(a_{ij})_{(i,j)\in\{1,2,\dots,m\}\times\{1,2,\dots,n\}}$ über K mit Indexmenge $\{1,2,\dots,m\}\times\{1,2,\dots,n\}$ notieren wir als Tabelle mit **m Zeilen** und **n Spalten***

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{mn} \end{pmatrix}$$

*und bezeichnen sie als **$(m\times n)$-Matrix** $(a_{ij})_{\substack{i=1,2,\dots,m \\ j=1,2,\dots,n}}$, deren Einträge $a_{ij} \in K$ in der Tabelle gemäß dem (zuerst genannten) Zeilenindex i und dem (danach genannten) Spaltenindex j eingeordnet sind. Naheliegenderweise identifizieren wir $(m\times 1)$-Matrizen mit Spaltenvektoren aus K^m und schreiben $K^{m\times n}$ für die **Menge aller $(m\times n)$-Matrizen** über K (speziell also $K^{m\times 1} = K^m$). Wir notieren eine $(m\times n)$-Matrix $(a_{ij})_{\substack{i=1,2,\dots,m \\ j=1,2,\dots,n}} \in K^{m\times n}$ gelegentlich als*

$$\left(\begin{array}{c|c|c|c|c} & & & & \\ v_1 & v_2 & v_3 & \cdots & v_n \\ & & & & \end{array}\right) \qquad \text{oder} \qquad \left(\begin{array}{c} w_1 \\ \hline w_2 \\ \hline w_3 \\ \hline \vdots \\ \hline w_m \end{array}\right)$$

*mit ihren **n Spaltenvektoren** $v_j = \begin{pmatrix} a_{1j} \\ a_{2j} \\ a_{3j} \\ \vdots \\ a_{mj} \end{pmatrix} \in K^{m\times 1} = K^m$ für $j = 1,2,\dots,n$ und ihren **m Zeilenvektoren** $w_i = (a_{i1}\ a_{i2}\ a_{i3}\ \cdots\ a_{in}) \in K^{1\times n}$ für $i = 1,2,\dots,m$.*

(II) *Die Summe von $A = (a_{ij})_{\substack{i=1,2,\dots,m \\ j=1,2,\dots,n}} \in K^{m\times n}$ und $B = (b_{ij})_{\substack{i=1,2,\dots,m \\ j=1,2,\dots,n}} \in K^{m\times n}$ ist definiert als $A+B := (a_{ij}+b_{ij})_{\substack{i=1,2,\dots,m \\ j=1,2,\dots,n}} \in K^{m\times n}$. Das Produkt von $s \in K$ und $A = (a_{ij})_{\substack{i=1,2,\dots,m \\ j=1,2,\dots,n}} \in K^{m\times n}$ ist $sA := (sa_{ij})_{\substack{i=1,2,\dots,m \\ j=1,2,\dots,n}} \in K^{m\times n}$.*

*Somit ergeben sich eine (eintragsweise) **Addition** $+\colon K^{m\times n} \times K^{m\times n} \to K^{m\times n}$ und eine (eintragsweise) **Skalarmultiplikation** $\cdot\colon K \times K^{m\times n} \to K^{m\times n}$.*

(III) *Das* ***Produkt*** *einer* $\boldsymbol{(m\times n)}$***-Matrix*** $A = (a_{ij})_{\substack{i=1,2,\dots,m\\ j=1,2,\dots,n}} \in K^{m\times n}$ *und einer* $\boldsymbol{(n\times p)}$***-Matrix*** $B = (b_{jk})_{\substack{j=1,2,\dots,n\\ k=1,2,\dots,p}} \in K^{n\times p}$ *ist die* $\boldsymbol{(m\times p)}$***-Matrix***

$$AB := \left(\sum_{j=1}^{n} a_{ij}b_{jk}\right)_{\substack{i=1,2,\dots,m\\ k=1,2,\dots,p}} \in K^{m\times p},$$

deren (i,k)*-Eintrag* $\sum_{j=1}^{n} a_{ij}b_{jk}$ *sich aus der* i*-ten Zeile* $(a_{i1}\ a_{i2}\ a_{i3}\ \cdots\ a_{in}) \in K^{1\times n}$ *von* A *und der* k*-ten Spalte* $\begin{pmatrix} b_{1k}\\ b_{2k}\\ b_{3k}\\ \vdots\\ b_{nk}\end{pmatrix} \in K^n$ *von* B *berechnet (****Merkregel „Zeile mal Spalte“****).*

Damit ergibt sich die ***Matrizenmultiplikation*** $\cdot\colon K^{m\times n}\times K^{n\times p}\to K^{m\times p}$ *und als Spezialfall* $p=1$ *die* ***Matrix-Vektor-Multiplikation*** $\cdot\colon K^{m\times n}\times K^n\to K^m$*.*

Beispiele (zur **Matrix-Vektor-Multiplikation** und **Matrizenmultiplikation**)**.** Ein Beispiel für die Matrix-Vektor-Multiplikation einer Matrix aus $\mathbb{R}^{2\times 4}$ mit einem Vektor aus $\mathbb{R}^4$ ist

$$\begin{pmatrix} 3 & 2 & 1 & 0\\ -1 & 0 & 0 & 5\end{pmatrix}\begin{pmatrix} -2\\ 0\\ 0\\ 1\end{pmatrix} = \begin{pmatrix} -6+0+0+0\\ 2+0+0+5\end{pmatrix} = \begin{pmatrix} -6\\ 7\end{pmatrix} \in \mathbb{R}^2.$$

Ein Beispiel für die Matrizenmultiplikation einer Matrix aus $\mathbb{R}^{2\times 4}$ und einer Matrix aus $\mathbb{R}^{4\times 3}$ ist

$$\begin{pmatrix} 3 & 2 & 1 & 0\\ -1 & 0 & 0 & 5\end{pmatrix}\begin{pmatrix} 0 & -2 & 0\\ 0 & 0 & 4\\ 1 & 0 & 0\\ 0 & 1 & 0\end{pmatrix} = \begin{pmatrix} 0+0+1+0 & -6+0+0+0 & 0+8+0+0\\ 0+0+0+0 & 2+0+0+5 & 0+0+0+0\end{pmatrix} = \begin{pmatrix} 1 & -6 & 8\\ 0 & 7 & 0\end{pmatrix} \in \mathbb{R}^{2\times 3}.$$

Bemerkungen (zum **Rechnen mit Matrizen**)**.** Seien K ein Körper und $m,n,p,q\in\mathbb{N}$.

(1) Die Matrizenmultiplikation ist assoziativ, erfüllt die Distributivgesetze und ist mit der Negation verträglich, das heißt für $A,A'\in K^{m\times n}$, $B,B'\in K^{n\times p}$, $C\in K^{p\times q}$ gelten die Regeln

$$(AB)C = A(BC), \qquad \big(A+A'\big)B = AB+A'B,$$
$$A\big(B+B'\big) = AB+AB', \qquad A(-B) = (-A)B = -(AB).$$

Die Nachweise sind mit den Definitionen problemlos. Für den darunter noch schwierigsten Nachweis der Assoziativität ist nur die Übereinstimmung der (i,ℓ)-Einträge von $(AB)C$ und $A(BC)$ gemäß $\sum_{k=1}^{p}\big(\sum_{j=1}^{n} a_{ij}b_{jk}\big)c_{k\ell} = \sum_{j=1}^{n} a_{ij}\big(\sum_{k=1}^{p} b_{jk}c_{k\ell}\big)$ zu prüfen (wobei $a_{ij},b_{jk},c_{k\ell}$ natürlich für die Einträge von A,B,C stehen).

(2) Die $\boldsymbol{(n\times p)}$**-Nullmatrix** $0_{K^{n\times p}}$, bei der alle np Einträge Null sind, erfüllt $A0_{K^{n\times p}} = 0_{K^{m\times p}}$ für alle $A\in K^{m\times n}$ und $0_{K^{n\times p}}A = 0_{K^{n\times q}}$ für alle $A\in K^{p\times q}$.

Möglichkeiten zur Angabe der $\boldsymbol{(n\times n)}$**-Einheitsmatrix** $\mathbb{I}_{\boldsymbol{n}}$ sind

$$\mathbb{I}_n := \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0\\ 0 & 1 & 0 & \cdots & 0 & 0\\ 0 & 0 & 1 & \cdots & 0 & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots\\ 0 & 0 & 0 & \cdots & 1 & 0\\ 0 & 0 & 0 & \cdots & 0 & 1\end{pmatrix} = \left(\begin{array}{c|c|c|c|c} & & & & \\ \mathrm{e}_1 & \mathrm{e}_2 & \mathrm{e}_3 & \cdots & \mathrm{e}_n\\ & & & & \end{array}\right) = \big(\delta_{ij}\big)_{i,j=1,2,\dots,n} \in K^{n\times n}$$

mit der kanonischen Basis $\mathrm{e}_1, \mathrm{e}_2, \mathrm{e}_3, \ldots, \mathrm{e}_n$ von K^n und dem **Kronecker-Symbol** oder **Kronecker-Delta**

$$\delta_{ij} := \begin{cases} 1 & \text{falls } i = j \\ 0 & \text{falls } i \neq j \end{cases} .$$

Es gelten $A\mathbb{I}_n = A$ für alle $A \in K^{m\times n}$ und $\mathbb{I}_n A = A$ für alle $A \in K^{n\times p}$, insbesondere $\mathbb{I}_n x = x$ für alle $x \in K^n$.

(3) Die Menge $\boldsymbol{K^{m\times n}}$ **ist** mit der oben in (II) definierten Addition und Skalarmultiplikation **ein $\boldsymbol{K}$-Vektorraum**. Man spricht vom **Raum der $\boldsymbol{(m\times n)}$-Matrizen** über K.

Die Menge $\boldsymbol{K^{n\times n}}$ bildet nur im Fall **quadratischer Matrizen** (!) mit der Addition aus (II) und der Matrizenmultiplikation aus (III) einen Ring mit der Nullmatrix $0_{K^{n\times n}}$ als neutralem Element der Addition und der Einheitsmatrix $\mathbb{I}_n$ als neutralem Element der Multiplikation. Man nennt $(K^{n\times n}, +, \cdot\,)$ den $(n\times n)$-**Matrizenring**.

(Dass wie bei Homomorphismen eine Vektorraumstruktur und wie bei Endomorphismen eine Ringstruktur vorliegt, kann man als ersten, vagen Hinweis auf eine Verwandtschaft von Matrizen und linearen Abbildungen sehen.)

(4) Nach den vorausgehenden Bemerkungen (1), (2), (3) ist klar, dass wir mit Matrizen sehr weitgehend mit den üblichen Regeln rechnen können. Etwas **Vorsicht** ist aber geboten, denn die **Matrizenmultiplikation ist** (auch dann, wenn es vom Format der Matrizen her möglich wäre) ***nicht* kommutativ**. Zum Beispiel ist

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} .$$

Insbesondere sind im Matrizenring $K^{n\times n}$ alle allgemein für Ringe eingeführten Begriffe sinnvoll. Wir halten dies speziell bei Invertierbarkeit noch explizit fest.

Definition (Invertierbarkeit, inverse Matrizen). *Sei K ein Körper. Eine quadratische (!) Matrix $A \in K^{n\times n}$ mit $n \in \mathbb{N}$ heißt **invertierbar** mit **inverser Matrix** $A^{-1} \in K^{n\times n}$, wenn A im Ring $K^{n\times n}$ invertierbar mit inversem Element A^{-1} ist (was $AA^{-1} = \mathbb{I}_n = A^{-1}A$ bedeutet).*

Bemerkung (zum **Produkt invertierbarer Matrizen**). Sei K ein Körper. Sind $A, B \in K^{n\times n}$ mit $n \in \mathbb{N}$ invertierbar, so ist auch AB invertierbar mit inverser Matrix

$$(AB)^{-1} = B^{-1}A^{-1} .$$

Dies rechnet man direkt nach (und es wurde auch in Abschnitt 3.1 für Gruppen schon bemerkt).

Eine manchmal nützliche Operation bei Matrizen ist das Vertauschen von Zeilen und Spalten:

Definition (Transponieren). *Seien K ein Körper, $m, n \in \mathbb{N}$ und $A = (a_{ij})_{\substack{i=1,2,\ldots,m \\ j=1,2,\ldots,n}} \in K^{m\times n}$.*

(I) *Die zur $(m\times n)$-Matrix A **transponierte Matrix** oder **Transponierte** der $(m\times n)$-Matrix A ist die $(n\times m)$-Matrix $A^{\mathrm{T}} := (a_{ji})_{\substack{i=1,2,\ldots,n \\ j=1,2,\ldots,m}} \in K^{n\times m}$.*

(II) *Im Fall $m = n$ heißt die quadratische (!) Matrix A **symmetrisch**, wenn $A^{\mathrm{T}} = A$ oder mit anderen Worten $a_{ji} = a_{ij}$ für alle $i, j \in \{1, 2, \ldots, n\}$ gilt, und **schiefsymmetrisch**, wenn $A^{\mathrm{T}} = -A$ oder mit anderen Worten $a_{ji} = -a_{ij}$ für alle $i, j \in \{1, 2, \ldots, n\}$ gilt.*

Die wahre Bedeutung dieser Definition erkennt man am besten an Beispielen:

Beispiele (für **transponierte** und **(schief)symmetrische Matrizen**)**.** Ein Beispiel für das Transponieren einer Matrix in $\mathbb{R}^{2\times 3}$ ist

$$\begin{pmatrix} 2 & 3 & -1 \\ \frac{1}{2} & 5 & 6 \end{pmatrix}^{\mathrm{T}} = \begin{pmatrix} 2 & \frac{1}{2} \\ 3 & 5 \\ -1 & 6 \end{pmatrix} \in \mathbb{R}^{3\times 2}\,.$$

Je ein Beispiel für eine symmetrische und eine schiefsymmetrische (3×3)-Matrix sind

$$\begin{pmatrix} 1 & 0 & 5 \\ 0 & 2 & 2 \\ 5 & 2 & 3 \end{pmatrix} \in \mathbb{R}^{3\times 3} \qquad \text{und} \qquad \begin{pmatrix} 0 & -1 & 2 \\ 1 & 0 & -4 \\ -2 & 4 & 0 \end{pmatrix} \in \mathbb{R}^{3\times 3}$$

(wobei hier wie generell für schiefsymmetrisches $(a_{ij})_{\substack{i=1,2,\dots,m\\ j=1,2,\dots,n}}$ die Diagonaleinträge a_{ii} Null sind).

Bemerkung (zu **transponierten Matrizen**)**.** Seien K ein Körper und $m, n, p \in \mathbb{N}$. Generell gilt für $A \in K^{m\times n}$ und $B \in K^{n\times p}$ dann

$$(AB)^{\mathrm{T}} = B^{\mathrm{T}} A^{\mathrm{T}}\,.$$

Für invertierbares $A \in K^{n\times n}$ folgt hieraus Invertierbarkeit von A^{T} mit inverser Matrix

$$\left(A^{\mathrm{T}}\right)^{-1} = \left(A^{-1}\right)^{\mathrm{T}}\,.$$

Die **vielleicht grundlegendste Beobachtung der gesamten linearen Algebra** ist der **enge Zusammenhang zwischen Matrizen und linearen Abbildungen**, die bei richtiger Betrachtungsweise sogar 1-zu-1 identifiziert werden können. Einführend bemerken wir dazu zunächst, dass man aus jeder Matrix $A = (a_{ij})_{\substack{i=1,2,\dots,m\\ j=1,2,\dots,n}} \in K^{m\times n}$ über einem Körper K eine K-lineare Abbildung

$$\mathrm{L}(A)\colon K^n \to K^m\,,\ v \mapsto Av$$

mit dem **Matrix-Vektor-Produkt** von A und v auf der rechten Seite erhält. (Die für die K-Linearität benötigten Eigenschaften $A(v+\widetilde{v}) = Av + A\widetilde{v}$ und $A(sv) = s(Av)$ für $v, \widetilde{v} \in K^n$, $s \in K$ sind dabei Spezialfälle schon bemerkter Regeln für das Rechnen mit Matrizen.) Als charakteristische Eigenschaft der Abbildung $\mathrm{L}(A)$, die wir verallgemeinern werden, halten wir fest, dass die kanonischen Basisvektoren $\mathrm{e}_j \in K^n$ mit $j \in \{1, 2, \dots, n\}$ durch $\mathrm{L}(A)$ auf

$$\mathrm{L}(A)(\mathrm{e}_j) = A\mathrm{e}_j = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix} \in K^m$$

abgebildet werden. Den Zusammenhang zwischen A und $\mathrm{L}(A)$ werden wir nun verallgemeinern und im folgenden Hauptsatz sehen, dass zwischen endlich-dimensionalen Vektorräumen jede lineare Abbildung auf analoge Weise erhalten werden kann. Vorbereitend halten wir aber zunächst noch fest, dass sich bei linearen Abbildungen alles auf den Vektoren einer Basis entscheidet.

Satz (über **Bestimmtheit linearer Abbildungen auf Basisvektoren**)**.** *Seien V und W Vektorräume über einem Körper K und B eine K-Basis von V. Dann gibt es für jede Abbildung $\eta\colon B \to W$ genau eine K-lineare Abbildung $\varphi\colon V \to W$ mit $\varphi(b) = \eta(b)$ für alle $b \in B$.*

Der Satz macht tatsächlich eine Existenz- und Eindeutigkeitsaussage für die K-lineare Fortsetzung φ von η. Die Eindeutigkeit kann dabei auch so ausgedrückt werden, dass **eine K-lineare Abbildung $\varphi\colon V \to W$ durch die Werte $\varphi(b)$ auf Basisvektoren $b \in B$** (die ja genau η entsprechen) **eindeutig bestimmt** ist.

Beweis des Satzes. Wir verwenden die entscheidende Basiseigenschaft, dass jeder Vektor $v \in V$ eine Basisdarstellung $v = \sum_{b\in E} \lambda_b b$ mit endlichem $E \subset B$ und durch v eindeutig bestimmten Koeffizienten $\lambda_b \in K$ besitzt.

Zum einen können wir damit $\varphi(v) := \sum_{b\in E} \lambda_b \eta(b)$ definieren und erhalten $\varphi\colon V \to W$. Um Verträglichkeit von φ mit Addition nachzuweisen, betrachten wir neben v einen Vektor $\widetilde{v} = \sum_{b\in \widetilde{E}} \widetilde{\lambda}_b b \in V$ mit endlichem $\widetilde{E} \subset B$ und $\widetilde{\lambda}_b \in K$. Wir erhalten $v+\widetilde{v} = \sum_{b\in E\cup\widetilde{E}} (\lambda_b+\widetilde{\lambda}_b) b$, (wobei wir $\lambda_b = 0$ für $b \in B \setminus E$ und $\widetilde{\lambda}_b = 0$ für $b \in B \setminus \widetilde{E}$ verstehen) und somit $\varphi(v+\widetilde{v}) = \sum_{b\in E\cup\widetilde{E}} (\lambda_b+\widetilde{\lambda}_b)\eta(b) = \sum_{b\in E} \lambda_b\eta(b) + \sum_{b\in\widetilde{E}} \widetilde{\lambda}_b\eta(b) = \varphi(v)+\varphi(\widetilde{v})$. Analog sieht man die Verträglichkeit von φ mit Skalarmultiplikation, also insgesamt die K-Linearität von φ und die behauptete Existenzaussage.

Zum anderen erhalten wir auch die Eindeutigkeit von φ, denn für jede K-lineare Abbildung mit $\varphi(b) = \eta(b)$ für $b \in E$ ist $\varphi(v) = \varphi\big(\sum_{b\in E} \lambda_b b\big) = \sum_{b\in E} \lambda_b \varphi(b) = \sum_{b\in E} \lambda_b \eta(b)$ für beliebiges $v \in V$ durch η und (die Basisdarstellung von) v eindeutig bestimmt. □

Hauptsatz (zur **Darstellung linearer Abbildungen durch Matrizen**). *Seien V und W endlich-dimensionale Vektorräume über einem Körper K mit $n := \dim_K V \in \mathbb{N}$ und K-Basis $\mathcal{B} = (\beta_1, \beta_2, \ldots, \beta_n)$ von V sowie $m := \dim_K W \in \mathbb{N}$ und K-Basis $\mathcal{C} = (\gamma_1, \gamma_2, \ldots, \gamma_m)$ von W. Dann gibt es zu jeder Matrix $A = (a_{ij})_{\substack{i=1,2,\ldots,m\\ j=1,2,\ldots,n}} \in K^{m\times n}$ eine eindeutige K-lineare Abbildung $\varphi\colon V \to W$ und umgekehrt zu jeder K-linearen Abbildung $\varphi\colon V \to W$ eine eindeutige Matrix $A = (a_{ij})_{\substack{i=1,2,\ldots,m\\ j=1,2,\ldots,n}} \in K^{m\times n}$ mit*

$$\varphi(\beta_j) = \sum_{i=1}^{m} a_{ij}\gamma_i \quad \textit{oder m.a.W.} \quad \varphi(\beta_j) = \begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{bmatrix}_{\mathcal{C}} \qquad \textit{für alle } j \in \{1, 2, \ldots, n\} \qquad (*)$$

Beweis. Ist die Matrix A gegeben, so definieren wir φ auf den Basisvektoren β_j durch $(*)$ (was der Abbildung η im vorigen Satz entspricht) und setzen φ dann mit dem vorigen Satz auf ganz V fort. Die Eindeutigkeit von φ folgt ebenfalls aus dem vorigen Satz.

Ist die Abbildung φ gegeben, so liefert die $\mathcal{C}$-Basisdarstellung von $\varphi(\beta_j) \in W$ eindeutige Koeffizienten $a_{1j}, a_{2j}, \ldots, a_{mj} \in K$ mit $(*)$. Diese Koeffizienten stellen wir in A zusammen. □

Bemerkung. Die Bedingung $(*)$ des Hauptsatzes ist äquivalent zu

$$\varphi(x_{\mathcal{B}}) = [Ax]_{\mathcal{C}} \qquad \text{für alle } x \in K^n\,,$$

wobei wir die aus den Koeffizientenvektoren $x = \sum_{j=1}^{n} x_j \mathrm{e}_j \in K^n$ bzw. $Ax = \sum_{i=1}^{m} (Ax)_i \mathrm{e}_i \in K^m$ erhaltenen Vektoren in $\mathcal{B}$- bzw. $\mathcal{C}$-Basisdarstellung wie in Abschnitt 6.2 als $x_{\mathcal{B}} = \sum_{j=1}^{n} x_j \beta_j \in V$ und $[Ax]_{\mathcal{C}} = \sum_{i=1}^{m} (Ax)_i \gamma_i \in W$ schreiben.

(Begründung: Gilt $(*)$, so folgt mit der K-Linearität von φ auch

$$\varphi(x_{\mathcal{B}}) = \varphi\Big(\sum_{j=1}^{n} x_j\beta_j\Big) = \sum_{j=1}^{n} x_j\varphi(\beta_j) = \sum_{j=1}^{n} x_j \sum_{i=1}^{m} a_{ij}\gamma_i = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}x_j\gamma_i = \sum_{i=1}^{m} (Ax)_i\gamma_i = [Ax]_{\mathcal{C}}\,.$$

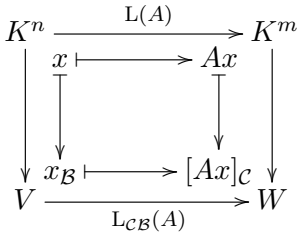
für alle $x \in K^n$. Umgekehrt ergibt Einsetzen von $(\mathrm{e}_j)_{\mathcal{B}} = \beta_j$ in dieser Bedingung wieder $(*)$.)

Definition (**darstellende Matrizen, dargestellte lineare Abbildungen**). *Hängen A und φ wie im Hauptsatz über (∗) zusammen, so nennen wir $\mathrm{M}_{\mathcal{CB}}(\varphi) := A$ die **darstellende Matrix** von φ und $\mathrm{L}_{\mathcal{CB}}(A) := \varphi$ die durch A **dargestellte lineare Abbildung**. Sind $\mathcal{B}$ und $\mathcal{C}$ die kanonischen Basen von $V = K^n$ und $W = K^m$, so verzichten wir bei dieser Notation auf die Indizes $_{\mathcal{CB}}$ (was mit der eingangs verwendeten Notation $\mathrm{L}(A)$ konsistent ist).*

Den entscheidenden Zusammenhang (∗) bei der Darstellung sollte man sich dabei so **merken, dass in den Spalten der Matrix A die φ-Bilder der Basisvektoren stehen** — einfach so im Fall der kanonischen Basis $\mathcal{C}$ von K^m und in Form ihrer $\mathcal{C}$-Koeffizienten im Fall einer allgemeinen Basis $\mathcal{C}$ von W.

Bemerkungen (zu **darstellenden Matrizen** und **dargestellten linearen Abbildungen**). Seien V, W, X endlich-dimensionale Vektorräume über einem Körper K mit $n := \dim_K V \in \mathbb{N}$, $m := \dim_K W \in \mathbb{N}$, $\ell := \dim_K X \in \mathbb{N}$ und mit K-Basen $\mathcal{B} = (\beta_1, \beta_2, \ldots, \beta_n)$ von V, $\mathcal{C} = (\gamma_1, \gamma_2, \ldots, \gamma_m)$ von W, $\mathcal{D} = (\delta_1, \delta_2, \ldots, \delta_\ell)$ von X.

(1) Die Umformulierung von (∗) aus der letzten Bemerkung bedeutet, dass die durch $A \in \mathbb{R}^{m\times n}$ dargestellte lineare Abbildung $\mathrm{L}_{\mathcal{CB}}(A)$ genau $\mathrm{L}_{\mathcal{CB}}(A)(x_{\mathcal{B}}) = [Ax]_{\mathcal{C}}$ für alle $x \in \mathbb{R}^n$ erfüllt. Mit anderen Worten entspricht dies der Kommutativität des nebenstehenden Diagramms, in dem die waagerechten Pfeile der Matrix-Vektor-Multiplikation $\mathrm{L}(A)$ bzw. $x \mapsto Ax$ und der von A dargestellten Abbildung $\mathrm{L}_{\mathcal{CB}}(A)$ entsprechen und die senkrechten Pfeile den Übergängen $x \mapsto x_{\mathcal{B}}$ und $y \mapsto y_{\mathcal{C}}$ von Koeffizienten zu Vektoren in $\mathcal{B}$- und $\mathcal{C}$-Basisdarstellung. Letztere sind auch selbst lineare Abbildungen und werden als **Basiswechsel** in Mathematik 3 noch häufiger vorkommen.



(2) **Matrizenmultiplikation und Komposition linearer Abbildungen entsprechen einander** durch

$$\begin{aligned} \mathrm{L}_{\mathcal{DB}}(BA) &= \mathrm{L}_{\mathcal{DC}}(B) \circ \mathrm{L}_{\mathcal{CB}}(A) && \text{für } A \in K^{m\times n},\ B \in K^{\ell\times m}, \\ \mathrm{M}_{\mathcal{DC}}(\psi)\mathrm{M}_{\mathcal{CB}}(\varphi) &= \mathrm{M}_{\mathcal{DB}}(\psi \circ \varphi) && \text{für } \varphi \in \mathrm{Hom}_K(V,W),\ \psi \in \mathrm{Hom}_K(W,X). \end{aligned}$$

Insbesondere überträgt sich Invertierbarkeit einer linearen Abbildung zwischen gleich-dimensionalen[3] Vektorräumen auf die darstellende Matrix und umgekehrt Invertierbarkeit eine Matrix auf die dargestellte lineare Abbildung. Für $A \in K^{m\times n}$ und $\varphi \in \mathrm{Hom}_K(V,W)$ mit $m = \dim_K W = \dim_K V = n$ gilt also

$$\begin{aligned} A \text{ invertierbare Matrix} &\iff \mathrm{L}_{\mathcal{CB}}(A) \text{ Isomorphismus}, \\ \varphi \text{ Isomorphismus} &\iff \mathrm{M}_{\mathcal{CB}}(\varphi) \text{ invertierbare Matrix}. \end{aligned}$$

(3) Die Korrespondenzen

$$\mathrm{L}_{\mathcal{CB}} \colon K^{m\times n} \to \mathrm{Hom}_K(V,W) \qquad \text{und} \qquad \mathrm{M}_{\mathcal{CB}} \colon \mathrm{Hom}_K(V,W) \to K^{m\times n}$$

sind selbst K-lineare Abbildungen und zueinander invers, ergeben also einen **Isomorphismus von K-Vektorräumen**

$$\boxed{\mathrm{Hom}_K(V,W) \cong K^{m\times n}}$$

(wobei $n = \dim_K V$, $m = \dim_K W$). Im Fall $W = V$ ist dieser auch Ringisomorphismus.

[3] Mit der etwa später in diesem Abschnitt folgenden Dimensionsformel wird klar, dass eine lineare Abbildung überhaupt nur dann invertierbar sein kann, wenn ihr Definitionsbereich und Ziel gleiche Dimension haben.

Die Korrespondenz zwischen Matrizen und linearen Abbildungen hat wichtige Folgerungen für die Isomorphie von Vektorräumen:

Korollar (**Isomorphiesatz für Vektorräume gleicher endlicher Dimension**). *Sei K ein Körper. Für* ***endlich-dimensionale*** *K-Vektorräume V und W gilt*

$$V \cong W \text{ als } K\text{-Vektorräume} \iff \dim_K V = \dim_K W\,.$$

Insbesondere ***ist jeder K-Vektorraum V mit $\dim_K V = n \in \mathbb{N}$ isomorph zu K^n.***

Mit anderen Worten bilden alle K-Vektorräume gleicher endlicher Dimension eine Isomorphieklasse, sie weisen alle die gleiche Struktur und die gleichen Eigenschaften auf. Schaut man nur auf die Struktur und nicht auf die genauen Elemente, so könnte man die Unterscheidung zwischen isomorphen Vektorräumen sogar aufgeben und damit den Standpunkt beziehen, dass es nur einen K-Vektorraum jeder festen Dimension $n \in \mathbb{N}_0$ gibt. In dieser Vorlesung gehen wir so weit aber nicht und unterscheiden verschiedene, isomorphe Vektorräume. Dennoch bedeutet die Isomorphie-Klassifikation, dass wir bei einem n-dimensionalen K-Vektorraum eigentlich immer an unser n-dimensionales Standard-Beispiel K^n mit $n \in \mathbb{N}$ denken können (und für $n = 0$ natürlich an den Nullvektorraum $\{0\}$). Praktisch alles, was in K^n funktioniert, kann dann per Isomorphie auf einen allgemeinen n-dimensionalen K-Vektorraum übertragen werden.

Beweis des Korollars. Wir zeigen die beiden Implikationen der Äquivalenz separat.

Sei $V \cong W$, es gebe also einen Isomorphismus $\varphi\colon V \to W$ von K-Vektorräumen. Sei weiter $\beta_1, \beta_2, \dots, \beta_n$ mit $n := \dim_K V \in \mathbb{N}_0$ eine K-Basis von V. Dann lässt sich nachrechnen, dass $\varphi(\beta_1), \varphi(\beta_2), \dots, \varphi(\beta_n)$ eine K-Basis von W ist. Also ist $\dim_K W = n = \dim_K V$.

Sei $n := \dim_K V = \dim_K W \in \mathbb{N}_0$. Seien $\beta_1, \beta_2, \dots, \beta_n$ eine K-Basis von V und $\gamma_1, \gamma_2, \dots, \gamma_n$ eine K-Basis von W. Nach dem Satz über die Bestimmtheit linearer Abbildungen auf Basisvektoren gibt es eindeutige K-lineare Abbildungen $\varphi\colon V \to W$ mit $\varphi(\beta_i) = \gamma_i$ für $i = 1, 2, \dots, n$ und $\psi\colon W \to V$ mit $\psi(\gamma_i) = \beta_i$ für $i = 1, 2, \dots, n$. Aus $(\psi \circ \varphi)(\beta_i) = \beta_i = \mathrm{id}_V(\beta_i)$ für $i = 1, 2, \dots, n$ folgt mit demselben Satz $\psi \circ \varphi = \mathrm{id}_V$, und analog ergibt sich $\varphi \circ \psi = \mathrm{id}_W$. Also sind φ und ψ Isomorphismen von K-Vektorräumen, und es ist $V \cong W$. □

Mit anderen Worten ergeben sich die Abbildungen im zweiten Teil des vorigen Beweises übrigens als $\varphi = \mathrm{L}_{\mathcal{CB}}(\mathbb{I}_n)$ und $\psi = \mathrm{L}_{\mathcal{BC}}(\mathbb{I}_n)$, und sie sind dann nach der vorausgehenden Bemerkung (2) Isomorphismen.

Nun beschäftigen wir uns kurz mit dem speziellen Fall K-wertiger K-linearer Abbildungen.

Definition (**Dualraum, Linearformen**). *Sei K ein Körper. Der* ***Dualraum*** *eines K-Vektorraums V ist der K-Vektorraum $V^* := \mathrm{Hom}_K(V, K)$. Die Elemente von V^*, also die K-linearen Abbildungen von V in den Grundkörper K, nennt man* ***(K-)Linearformen*** *auf V.*

Ist $n := \dim_K V \in \mathbb{N}$, so sind die darstellenden Matrizen der Linearformen in V^* Matrizen in $K^{1\times n}$, haben also nur eine Zeile und n Spalten. Solche Matrizen hatten wir schon einmal als Zeilenvektoren bezeichnet. Sie sind ein Gegenstück zu Spaltenvektoren, in gewisser Weise „dual“ zu diesen, was jedenfalls ein Stück weit die Benennung als Dualraum erklärt. Konkret stellt ein Zeilenvektor $w = (w_1\ w_2\ \dots\ w_n) \in K^{1\times n}$ bezüglich einer Basis $\mathcal{B} = (\beta_1, \beta_2, \dots, \beta_n)$ von V und der 1-elementigen Standard-Basis 1 von K tatsächlich die Linearform $\varphi = \mathrm{L}_{1\mathcal{B}}(w)$ mit $\varphi(x_{\mathcal{B}}) = wx = \sum_{j=1}^{n} w_j x_j$ für alle $x \in \mathbb{R}^n$ dar. Darüber hinaus halten wir für den Dualraum hier nur noch fest:

Korollar (**Isomorphiesatz für den Dualraum**). *Sei K ein Körper. Für jeden **endlichdimensionalen** K-Vektorraum V gilt die Isomorphie $V^* \cong V$ von K-Vektorräumen.*

Beweis. Ist $\dim_K V = 0$, so ist die Isomorphie der Nullvektorräume V^* und V klar. Wir können also $n := \dim_K V \in \mathbb{N}$ annehmen. Die gerade besprochene Korrespondenz zwischen Linearformen und Zeilenvektoren bedeutet dann $V^* \cong K^{1\times n}$ als K-Vektorräume. Da Transponieren der kanonischen Basis von K^n eine Basis von $K^{1\times n}$ gibt, folgt $\dim_K(V^*) = \dim_K(K^{1\times n}) = n$. Dies bedeutet $\dim_K(V^*) = \dim_K V$, und mit dem vorigen Korollar folgt die behauptete Isomorphie $V^* \cong V$ von K-Vektorräumen. □

Als Nächstes führen wir einige, teils schon aus den Abschnitten 2.1 und 3.3 bekannte Konzepte parallel für Matrizen und lineare Abbildungen ein:

Definitionen (**Kern**, **Bild** und **Rang** von Matrizen und linearen Abbildungen). *Seien K ein Körper, $A \in K^{m\times n}$ mit $m,n \in \mathbb{N}$ eine $(m\times n)$-Matrix über K und $\varphi \in \mathrm{Hom}_K(V,W)$ eine K-lineare Abbildung zwischen Vektorräumen V und W über K.*

(I) *Der **Kern** der Matrix A und der **Kern** der linearen Abbildung φ werden definiert als*

$$\mathrm{Kern}\, A := \{x \in K^n \mid Ax = 0\} = \left\{x \in K^n \;\middle|\; \sum_{j=1}^{n} x_j A\mathrm{e}_j = 0\right\} \subset K^n\,,$$
$$\mathrm{Kern}\,\varphi := \varphi^{-1}(\{0_W\}) = \{v \in V \mid \varphi(v) = 0_W\} \subset V\,.$$

(II) *Das **Bild** der Matrix A und das **Bild** der linearen Abbildung φ werden definiert als*

$$\mathrm{Bild}\, A := \{Ax \mid x \in K^n\} = \mathrm{Span}\{A\mathrm{e}_1, A\mathrm{e}_2, \ldots, A\mathrm{e}_n\} \subset K^m\,,$$
$$\mathrm{Bild}\,\varphi := \varphi(V) = \{\varphi(v) \mid v \in V\} \subset W\,.$$

(III) *Der (Spalten-)**Rang** der Matrix A und der **Rang** der linearen Abbildung φ werden definiert als*

$$\mathrm{Rang}\, A := \dim(\mathrm{Bild}\, A) \in \{0,1,2,\ldots,m\}\,,$$
$$\mathrm{Rang}\,\varphi := \dim(\mathrm{Bild}\,\varphi) \in \mathbb{N}_0 \dot\cup \{\infty\}\,.$$

Bemerkungen (zu **Kern**, **Bild** und **Rang**). Seien K ein Körper, $m,n \in \mathbb{N}$ und V, W Vektorräume über K.

(1) Der **Kern** von $A \in K^{m\times n}$ bzw. $\varphi \in \mathrm{Hom}_K(V,W)$ ist **stets** ein ***K*-Untervektorraum** von K^n bzw. V. Das **Bild** von $A \in K^{m\times n}$ bzw. $\varphi \in \mathrm{Hom}_K(V,W)$ ist **stets** ein ***K*-Untervektorraum** von K^m bzw. W, womit die Definition des Rangs als Dimension des Bilds überhaupt erst sinnvoll wird. Der Nachweis der Untervektorraum-Eigenschaften anhand der Definitionen ist dabei problemlos.

(2) Kern, Bild und Rang einer Matrix A hängen auf naheliegende Weise mit Kern, Bild und Rang einer durch A dargestellten linearen Abbildung zusammen. Genauer gelten für $A \in K^{m\times n}$, eine K-Basis $\mathcal{B}$ von V mit $\dim V = n$ und eine K-Basis $\mathcal{C}$ von W mit $\dim W = m$ die Zusammenhänge (die man aus der Definition und $\mathrm{L}_{\mathcal{CB}}(A)(x_{\mathcal{B}}) = [Ax]_{\mathcal{C}}$ abliest)

$$\mathrm{Kern}\,\mathrm{L}(A) = \mathrm{Kern}\, A\,, \qquad \mathrm{Bild}\,\mathrm{L}(A) = \mathrm{Bild}\, A\,, \qquad \mathrm{Rang}\,\mathrm{L}(A) = \mathrm{Rang}\, A\,,$$
$$\mathrm{Kern}\,\mathrm{L}_{\mathcal{CB}}(A) = \{x_{\mathcal{B}} \mid x \in \mathrm{Kern}\, A\}\,, \quad \mathrm{Bild}\,\mathrm{L}_{\mathcal{CB}}(A) = \{y_{\mathcal{C}} \mid y \in \mathrm{Bild}\, A\}\,, \quad \mathrm{Rang}\,\mathrm{L}_{\mathcal{CB}}(A) = \mathrm{Rang}\, A\,.$$

(3) Die Bedeutung des Kerns liegt zu einem großen Teil in folgendem, in ähnlicher Form schon aus Abschnitt 3.3 bekannten **Injektivitäts-Kriterium**: Für $\varphi \in \mathrm{Hom}_K(V,W)$ gilt

$$\boxed{\varphi \text{ injektiv} \iff \operatorname{Kern}\varphi = \{0_V\}}\,.$$

(4) Dass wir bei einer Matrix A auch vom ***Spalten*rang** sprechen, erklärt sich daraus, dass $\operatorname{Bild} A$ von den Spalten $Ae_1, Ae_2, \ldots, Ae_n \in K^m$ von A aufgespannt wird und daher $\operatorname{Rang} A$ die maximale Zahl linear unabhängiger Spalten von A angibt. Da $A \in K^{m\times n}$ aus n Spaltenvektoren $Ae_1, Ae_2, \ldots, Ae_n \in K^m$ besteht, ergibt sich hieraus als generelle Regel

$$\operatorname{Rang} A \leq \min\{m,n\} \qquad \text{für } A \in K^{m\times n}\,.$$

Neben dem *Spalten*rang lässt sich der ***Zeilen*rang** von $A \in K^{m\times n}$ als der Spaltenrang von A^{T} einführen und gibt die maximale Zahl linear unabhängiger Zeilen von A an. Bis auf Weiteres werden wir immer mit dem Spaltenrang arbeiten. In Abschnitt 6.4 werden wir dann tatsächlich zeigen, dass Spaltenrang und Zeilenrang einer Matrix stets übereinstimmen und daher die Behandlung nur des Spaltenrangs keine Einschränkung ist.

Beispiel (für **Kern, Bild und Rang einer Matrix**)**.** Für die Matrix

$$A := \begin{pmatrix} 1 & 2 & 3 \\ 4 & -1 & 0 \\ 3 & 6 & 9 \end{pmatrix} \in \mathbb{R}^{3\times 3}$$

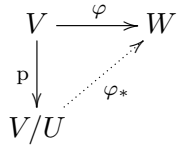
erhalten wir (mit den spitzen Klammern als Notation für den aufgespannten $\mathbb{R}$-Untervektorraum)

$$\operatorname{Kern} A = \left\langle \begin{pmatrix} 1 \\ 4 \\ -3 \end{pmatrix} \right\rangle, \qquad \operatorname{Bild} A = \left\langle \begin{pmatrix} 1 \\ 4 \\ 3 \end{pmatrix}, \begin{pmatrix} 2 \\ -1 \\ 6 \end{pmatrix}, \begin{pmatrix} 3 \\ 0 \\ 9 \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} 1 \\ 0 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\rangle, \qquad \operatorname{Rang} A = 2\,.$$

Die Bestimmung des Kerns erfolgt dabei durch Lösen des linearen Gleichungssystems $Ax = 0$. Das Bild ergibt sich in der ersten Form als Span der 3 Spaltenvektoren von A und kann dann, da diese 3 Vektoren nicht linear unabhängig sind, als Span von 2 linear unabhängigen Vektoren umgeschrieben werden. Damit ist $\operatorname{Rang} A = \dim(\operatorname{Bild} A) = 2$ klar.

Ein Zusammenhang zwischen den Dimensionen von Kern und Bild leiten wir nun mit Hilfe des aus Abschnitt 3.3 bekannten Konzepts der Faktorisierung auf elegante Weise her. Wir halten dazu zunächst fest, dass der Faktorisierungssatz auch für lineare Abbildungen wie folgt gilt.

Satz (**Faktorisierungssatz für lineare Abbildungen**)**.** *Seien V und W Vektorräume über einem Körper K und U ein K-Untervektorraum von V. Für jede K-lineare Abbildung $\varphi\colon V \to W$ mit $U \subset \operatorname{Kern}\varphi$ gibt es genau eine K-lineare Abbildung $\varphi_*\colon V/U \to W$, die $\varphi_* \circ \mathrm{p} = \varphi$ (mit der Quotientenabbildung $\mathrm{p}\colon V \to V/U$) erfüllt, also nebenstehendes Diagramm kommutativ macht.*



Wie bei den früheren Versionen des Satzes erfüllt φ_* mit anderen Worten einfach $\varphi_*(x+U) = \varphi(x)$ für $x \in V$, der Satz ist stets mit $U = \operatorname{Kern}\varphi$ anwendbar, und genau in diesem Fall ist φ_* injektiv. Außerdem gilt stets $\operatorname{Bild}\varphi_* = \operatorname{Bild}\varphi$, und φ_* ist genau dann surjektiv, wenn φ dies ist.

Beweis des Faktorisierungssatzes. Die Existenz und Eindeutigkeit von φ_* als additiver Gruppenhomomorphismus folgen aus dem entsprechenden Sachverhalt des Abschnitt 3.3 für Gruppen. Dass φ_* sogar K-linear ist, folgt dann aus der Rechnung $\varphi_*(s(x+U)) = \varphi_*(sx+U) = \varphi(sx) = s\varphi(x) = s\varphi_*(x+U)$ für $s \in K$ und $x \in V$. □

Hier geht es uns aber vor allem um die Anwendung des Faktorisierungssatzes zum Beweis des schon angekündigten Zusammenhangs zwischen Kern und Bild:

Satz (**Dimensionsformel für lineare Abbildungen**). *Seien V und W Vektorräume über einem Körper K. Für jede K-lineare Abbildung $\varphi\colon V \to W$ gilt*

$$\boxed{\dim V = \dim(\operatorname{Kern}\varphi) + \operatorname{Rang}\varphi}\,.$$

Bemerkung (**Dimensionsformel für Matrizen**). Insbesondere gilt auch für eine $(m\times n)$-Matrix $A \in K^{m\times n}$ mit $m, n \in \mathbb{N}$ über einem Körper K stets

$$\boxed{n = \dim(\operatorname{Kern} A) + \operatorname{Rang} A}\,.$$

Beweis der Dimensionsformel. Die Formel des Abschnitts 6.2 für die Dimension des Faktorraums liefert

$$\dim V = \dim(\operatorname{Kern}\varphi) + \dim(V/\operatorname{Kern}\varphi)\,.$$

Durch Faktorisierung nach $\operatorname{Kern}\varphi$ erhalten wir aus φ nun ein injektives φ_*, das in seinen Bildbereich $\operatorname{Bild}\varphi_* = \operatorname{Bild}\varphi$ auch surjektiv ist und daher als Isomorphismus $\varphi_*\colon V/\operatorname{Kern}\varphi \to \operatorname{Bild}\varphi$ aufgefasst werden kann. Insbesondere ist $\dim(V/\operatorname{Kern}\varphi) = \dim(\operatorname{Bild}\varphi) = \operatorname{Rang}\varphi$, und wir erhalten mit

$$\dim V = \dim(\operatorname{Kern}\varphi) + \operatorname{Rang}\varphi$$

die Dimensionsformel für die lineare Abbildung $\varphi\colon V \to W$. Die Dimensionsformel für die Matrix $A \in K^{m\times n}$ kann man daraus durch Anwendung auf $\mathrm{L}(A)\colon K^n \to K^m$ erhalten. □

Als erste Folgerung aus der Dimensionsformel halten wir fest:

Korollar (zur **Invertierbarkeit von Matrizen**). *Für $n \in \mathbb{N}$, einen Körper K und eine quadratische* (!) *Matrix $A \in K^{n\times n}$ gilt*

$$A \text{ invertierbar} \iff \operatorname{Kern} A = \{0\} \iff \operatorname{Bild} A = K^n \iff Ae_1, Ae_2, \ldots, Ae_n \text{ Basis von } K^n\,.$$

Da Invertierbarkeit von A und A^{T} äquivalent sind, ist neben der Basiseigenschaft der *Spalten* $Ae_1, Ae_2, \ldots, Ae_n$ von A übrigens genauso die Basiseigenschaft der (transponierten) *Zeilen* $A^{\mathrm{T}}e_1, A^{\mathrm{T}}e_2, \ldots, A^{\mathrm{T}}e_n$ von A notwendig und hinreichend für Invertierbarkeit von A.

Beweis des Korollars. Invertierbarkeit von A ist äquivalent zu Invertierbarkeit und damit letztlich zu Injektivität und Surjektivität von $\mathrm{L}(A)\colon K^n \to K^n$. Die Injektivität kann dabei äquivalent durch $\operatorname{Kern}\mathrm{L}(A) = \{0\}$ oder durch $\operatorname{Kern} A = \{0\}$ oder durch $\forall x \in K^n\colon (Ax = 0 \Longrightarrow x = 0)$ oder durch lineare Unabhängigkeit der Spalten $Ae_1, Ae_2, \ldots, Ae_n$ ausgedrückt werden (letzteres, weil $Ax = \sum_{j=1}^n x_j Ae_j$). Die Surjektivität kann äquivalent durch $\operatorname{Bild}\mathrm{L}(A) = K^n$ oder durch $\operatorname{Bild} A = K^n$ oder durch $\operatorname{Span}\{Ae_1, Ae_2, \ldots, Ae_n\} = K^n$ oder dadurch, dass die Spalten $Ae_1, Ae_2, \ldots, Ae_n$ Erzeugendensystem von K^n sind, ausgedrückt werden. Aus diesen Äquivalenzen entnehmen wir insgesamt

$$A \text{ invertierbar} \iff \operatorname{Kern} A = \{0\}\,,\ \operatorname{Bild} A = K^n \iff Ae_1, Ae_2, \ldots, Ae_n \text{ Basis von } K^n\,.$$

Wegen der Dimensionsformel $n = \dim(\operatorname{Kern} A) + \dim(\operatorname{Bild} A)$ (die wir tatsächlich nur für diesen letzten Schluss benötigen) sind hierbei die beiden Bedingungen $\operatorname{Kern} A = \{0\}$ und $\operatorname{Bild} A = K^n$ sowieso gleichbedeutend, weshalb auch jede der beiden einzeln als Kriterium ausreicht. □

Die Beobachtungen des gerade geführten Beweises erklären übrigens auch, warum es sinnvoll war, Invertierbarkeit von vorne herein nur für *quadratische* Matrizen $A \in K^{n\times n}$ zu definieren: Tatsächlich könnte man ja zunächst hoffen, dass auch für $A \in K^{m\times n}$ mit $m, n \in \mathbb{N}$ eine allgemeinere Inverse $B \in K^{n\times m}$ über die Bedingungen $AB = \mathbb{I}_m$ und $BA = \mathbb{I}_n$ definiert werden kann. Damit diese Bedingungen gelten können, muss aber weiterhin $\mathrm{L}(A)$ injektiv und surjektiv sein, es muss also $\operatorname{Kern} A = \{0\}$ und $\operatorname{Bild} A = K^m$ gelten und dann folgt nach Dimensionsformel eben $n = \dim \operatorname{Kern} A + \dim(\operatorname{Bild} A) = 0+m = m$. Auch mit der allgemeineren Definition kann Invertierbarkeit also letztlich doch nur für quadratische Matrizen vorliegen.

Im Rest dieses Abschnitts beschäftigen wir uns hauptsächlich mit der jetzt eingeführten Determinante als einer sehr wichtigen Kennzahl quadratischer Matrizen.

Definition (**Determinanten** von Matrizen)**.** *Seien K ein Körper und $n \in \mathbb{N}$. Die **Determinante** einer quadratischen (!) Matrix $A = (a_{i,j})_{i,j=1,2,\dots,n} \in K^{n\times n}$ erklären wir über die sogenannte **Leibniz-Formel** als*

$$\det A := \sum_{\pi\in \mathrm{S}_n} \operatorname{sgn}(\pi) \prod_{i=1}^{n} a_{i,\pi(i)} = \sum_{\pi\in \mathrm{S}_n} \operatorname{sgn}(\pi) a_{1,\pi(1)} a_{2,\pi(2)} \cdot \ldots \cdot a_{n,\pi(n)} \in K$$

(wobei S_n die in Abschnitt 3.1 eingeführte symmetrische Gruppe vom Grad n, also die Menge aller $n!$ Permutationen von $\{1, 2, \dots, n\}$, bezeichnet). Gelegentlich notieren wir die Determinante auch mit senkrechten Strichen in der Form[4]

$$\begin{vmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{vmatrix} := \det \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix} .$$

Bemerkungen und Beispiele (zur **Berechnung von Determinanten**)**.** Sei K ein Körper.

(1) Für **(1×1)-Matrizen** gilt trivial $\det(s) = s$ mit $s \in K$.

(2) Für **(2×2)-Matrizen** besagt die Leibniz-Formel

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc \qquad \text{mit } a, b, c, d \in K$$

(wobei in $\mathrm{S}_2 = \{\mathrm{id}, \tau\}$ die Identität id den Term ad, die Transposition τ den Term $-bc$ gibt).

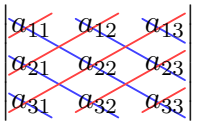
(3) Im Spezialfall von **(3×3)-Matrizen** ist die Leibniz-Formel als **Regel von Sarrus** bekannt und besagt

$$\det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$$
$$= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33}$$

für $(a_{ij})_{i,j=1,2,3} \in K^{3\times 3}$ (wobei in $\mathrm{S}_3 = \{\mathrm{id}, \tau_1, \tau_2, \tau_3, \sigma_1, \sigma_2\}$ die Identität id und die 3-Zykel σ_1, σ_2 die drei blauen Terme sowie die Transpositionen τ_2, τ_3, τ_1 die drei roten Terme geben). Um sich die Regel zu merken, kann man sich wie folgt diagonale Linien in der Matrix

[4] Für $n = 1$ sollte man diese Notation allerdings vermeiden, um Verwechslungen mit dem Betrag auszuschließen.

vorstellen:



Die drei Terme mit positivem Vorzeichen ergeben sich dann jeweils durch Multiplikation der drei Zahlen entlang blauer Linien (wobei die Linien, die die Matrix links oder rechts verlassen, als auf der jeweils anderen Seite fortgesetzt zu betrachten sind). Die drei Terme mit negativem Vorzeichen erhält man analog durch Multiplikation entlang roter Linien.

(4) Für obere **Dreiecksmatrizen** beliebiger Zeilen- und Spaltenzahl $n \in \mathbb{N}$ (mit beliebigen, nicht unbedingt gleichen Einträgen aus K an den mit $*$ markierten Stellen) erhält man die Determinante

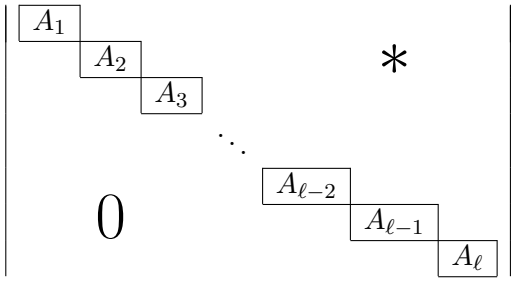
$$\begin{vmatrix} \lambda_1 & * & * & \cdots & * & * & * \\ 0 & \lambda_2 & * & \cdots & * & * & * \\ 0 & 0 & \lambda_3 & \cdots & * & * & * \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_{n-2} & * & * \\ 0 & 0 & 0 & \cdots & 0 & \lambda_{n-1} & * \\ 0 & 0 & 0 & \cdots & 0 & 0 & \lambda_n \end{vmatrix} = \lambda_1\lambda_2\lambda_3 \cdot \ldots \cdot \lambda_{n-2}\lambda_{n-1}\lambda_n$$

als Produkt der Einträge $\lambda_1, \lambda_2, \ldots, \lambda_n \in K$ auf der **Hauptdiagonale** von der linken, oberen Ecke zur rechten, unteren Ecke. Der Grund für diese Regel ist, dass für eine Matrix $(a_{i,j})_{i,j=1,2,\ldots,n}$ dieser Struktur und $\pi \in \mathrm{S}_n$ nur dann $\prod_{i=1}^{n} a_{i,\pi(i)} \neq 0$ sein kann, wenn $\pi(i) \geq i$ für alle $i \in \{1, 2, \ldots, n\}$ eintritt, was wiederum $\pi = \mathrm{id}$ erzwingt und die Leibniz-Formel auf einen einzigen Summanden reduziert. Eine analoge Regel gilt für *untere* Dreiecksmatrizen (und ergibt sich mit derselben Begründung oder gemäß Teil (I) des nächsten Satzes). Insbesondere gilt im Spezialfall von **Diagonalmatrizen**

$$\begin{vmatrix} \lambda_1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & \lambda_2 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & \lambda_3 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_{n-2} & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & \lambda_{n-1} & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & \lambda_n \end{vmatrix} = \lambda_1\lambda_2\lambda_3 \cdot \ldots \cdot \lambda_{n-2}\lambda_{n-1}\lambda_n \,.$$

Da Dreiecks- und Diagonalmatrizen häufig auftreten, sind diese Regeln zur sehr einfachen Berechnung der Determinante tatsächlich **extrem nützlich**.

(5) Analog gilt für obere **Block-Dreiecksmatrizen** die Regel



$$= (\det A_1)(\det A_2) \cdot \ldots \cdot (\det A_{\ell-1})(\det A_\ell)\,,$$

wobei die quadratischen (!) Blöcke $A_1 \in K^{n_1 \times n_1}$, $A_2 \in K^{n_2 \times n_2}$, …, $A_\ell \in K^{n_\ell \times n_\ell}$ mit $\ell, n_1, n_2, \ldots, n_\ell \in \mathbb{N}$ ihre Zentren auf der Hauptdiagonale haben, sich oberhalb der Blöcke beliebige Einträge und unterhalb der Blöcke nur Nullen befinden und die gesamte Blockmatrix $n = n_1 + n_2 + \ldots + n_\ell$ Zeilen und Spalten hat. Zur Herleitung dieser Regel gehen wir nicht ins Detail. Im Wesentlichen ergibt sie sich aus der Überlegung, dass $\prod_{i=1}^{n} a_{i,\pi(i)} \neq 0$ bei dieser Struktur nur dann möglich ist, wenn durch π nur zum selben Block gehörige Indizes untereinander permutiert werden. Eine analoge Regel gilt für *untere* Block-Dreiecksmatrizen, und als Spezialfall ergibt sich für **Block-Diagonalmatrizen**

$$\begin{vmatrix} \boxed{A_1} & & & 0 \\ & \boxed{A_2} & & \\ & & \boxed{A_3} & \\ & & & \ddots \\ & 0 & & & \boxed{A_{\ell-2}} & \\ & & & & & \boxed{A_{\ell-1}} & \\ & & & & & & \boxed{A_\ell} \end{vmatrix} = (\det A_1)(\det A_2) \cdot \ldots \cdot (\det A_{\ell-1})(\det A_\ell)\,.$$

(6) Eine **Permutationsmatrix** $\mathrm{E}_\sigma := (\delta_{\sigma(i),j})_{i,j=1,2,\ldots,n} \in K^{n \times n}$ mit $n \in \mathbb{N}$, $\sigma \in \mathrm{S}_n$ hat nur Einträge 0 und 1, wobei in jeder Zeile und jeder Spalte genau eine 1 steht. Die Matrix E_σ ist die darstellende Matrix der zu σ gehörigen Koordinatenpermutation $K^n \to K^n$ bezüglich der kanonischen Basis von K^n, erfüllt also $\mathrm{E}_\sigma \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_{\sigma(1)} \\ x_{\sigma(2)} \\ \vdots \\ x_{\sigma(n)} \end{pmatrix}$ für alle $\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in K^n$. Für die Determinante von E_σ gilt einfach

$$\det \mathrm{E}_\sigma = \mathrm{sgn}(\sigma) \in \{-1, 1\}\,,$$

denn für $\pi \in \mathrm{S}_n$ mit $\prod_{i=1}^{n} \delta_{\sigma(i),\pi(j)} \neq 0$ muss offensichtlich die Gleichheit $\pi = \sigma$ vorliegen.

Fällt eine Determinantenberechnung unter keinen der gerade diskutierten Punkte, so kann man diese schematisch mit Teil (II) des nächsten Satzes angehen.

Satz. *Seien K ein Körper, $n \in \mathbb{N}$ und $A = (a_{i,j})_{i,j=1,2,\ldots,n} \in K^{n \times n}$.*

(I) *Es gilt*

$$\det A = \det\left(A^{\mathrm{T}}\right).$$

(II) ***Entwicklungssatz von Laplace/Entwickeln nach der i-ten Zeile:*** *Für jedes feste $i \in \{1, 2, \ldots, n\}$ gilt*

$$\det A = \sum_{j=1}^{n} a_{i,j} \widehat{A}_{ij}\,,$$

*wobei sich die sogenannten **Kofaktoren** $\widehat{A}_{ij} \in K$ gemäß*

$$\widehat{A}_{ij} = (-1)^{i+j} \det \begin{pmatrix} a_{1,1} & \cdots & a_{1,j-1} & a_{1,j+1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{i-1,1} & \cdots & a_{i-1,j-1} & a_{i-1,j+1} & \cdots & a_{i-1,n} \\ a_{i+1,1} & \cdots & a_{i+1,j-1} & a_{i+1,j+1} & \cdots & a_{i+1,n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,j-1} & a_{n,j+1} & \cdots & a_{n,n} \end{pmatrix}$$

aus Determinanten von $((n-1)\times(n-1))$-Streichmatrizen[5] *ergeben, bei denen die i-te Zeile und j-te Spalte der ursprünglichen Matrix A wegfallen.*

Mit Teil (II) des Satzes wird also die Berechnung einer allgemeinen $(n\times n)$-Determinante auf die Berechnung von $((n-1)\times(n-1))$-Determinanten zurückgeführt, die dann mit den Einträgen a_{ij} der i-ten Zeile und den schachbrettartig auftretenden Vorzeichen $(-1)^{i+j}$ zu multiplizieren und dann aufzusummieren sind. Wendet man dies iterativ an, so lassen sich im Prinzip beliebige Determinanten schematisch berechnen.

Für praktische Berechnungen mit dem Entwicklungssatz ist es nützlich, zu wissen, dass man wegen Teil (I) des Satzes analog nach einer festen Spalte statt einer festen Zeile entwickeln kann und dass es normalerweise von Vorteil ist, wie im folgenden Beispiel die Entwicklung nach einer Zeile oder Spalte durchzuführen, die möglichst viele Nullen enthält.

Beispiel (zur **Determinantenberechnung mit dem Entwicklungssatz**)**.** Ein Beispiel für die Entwicklung einer (4×4)-Matrix nach ihrer dritten Zeile und anschließende Berechnung der (3×3)-Determinanten mit der Regel von Sarrus ist

$$\begin{vmatrix} 3 & -4 & 0 & 1 \\ 0 & 2 & -5 & 3 \\ -1 & 0 & 0 & 4 \\ -3 & 2 & 4 & 1 \end{vmatrix} = -1 \begin{vmatrix} -4 & 0 & 1 \\ 2 & -5 & 3 \\ 2 & 4 & 1 \end{vmatrix} - 0 + 0 - 4 \begin{vmatrix} 3 & -4 & 0 \\ 0 & 2 & -5 \\ -3 & 2 & 4 \end{vmatrix}$$
$$= -1(20+0+8+10+48-0) - 4(24-60+0-0+30-0) = -62\,.$$

Wir kommen nun zum Beweis der im Satz behaupteten Regeln.

Beweis von Teil (I) *des letzten Satzes.* Wir machen die (teils unten erläuterte) Rechnung

$$\det\left(A^{\mathrm{T}}\right) = \sum_{\pi\in \mathrm{S}_n} \operatorname{sgn}(\pi) a_{\pi(1),1} a_{\pi(2),2} \cdot \ldots \cdot a_{\pi(n),n} \overset{(1)}{=} \sum_{\pi\in \mathrm{S}_n} \operatorname{sgn}(\pi^{-1}) a_{1,\pi^{-1}(1)} a_{2,\pi^{-1}(2)} \cdot \ldots \cdot a_{n,\pi^{-1}(n)}$$
$$\overset{(2)}{=} \sum_{\sigma\in \mathrm{S}_n} \operatorname{sgn}(\sigma) a_{1,\sigma(1)} a_{2,\sigma(2)} \cdot \ldots \cdot a_{n,\sigma(n)} = \det A\,.$$

Dabei basiert der Schritt (1) auf $\operatorname{sgn}(\pi) = \operatorname{sgn}(\pi^{-1})$ und Umsortieren der Faktoren mit Indizes $(\pi(j), j) = (i, \pi^{-1}(i))$ in die durch den vorderen Index $i = \pi(j)$ gegebene Reihenfolge. Im Schritt (2) erfolgt mittels der Bijektion $\mathrm{S}_n \to \mathrm{S}_n\,,\ \pi \mapsto \pi^{-1}$ ein Übergang zum Index $\sigma = \pi^{-1}$. □

Beweis von Teil (II) *des letzten Satzes.* Wir spalten zunächst die Summe in der Leibniz-Formel nach dem zum festen $i \in \{1, 2, \ldots, n\}$ gehörigen Wert $\pi(i) \in \{1, 2, \ldots, n\}$ auf und erhalten so

$$\det A = \sum_{j=1}^{n} \sum_{\substack{\pi\in \mathrm{S}_n \\ \pi(i)=j}} \operatorname{sgn}(\pi) \prod_{k=1}^{n} a_{k,\pi(k)} = \sum_{j=1}^{n} a_{i,j} \sum_{\substack{\pi\in \mathrm{S}_n \\ \pi(i)=j}} \operatorname{sgn}(\pi) \prod_{\substack{k=1 \\ k\neq i}}^{n} a_{k,\pi(k)}\,.$$

Für (erst einmal) festes $(i, j) \in \{1, 2, \ldots, n\}^2$ sei nun $(\overline{a}_{\ell,m})_{\ell,m=1,2,\ldots,n-1} \in K^{(n-1)\times(n-1)}$ die Streichmatrix, in der die i-te Zeile und j-te Spalte von A weggefallen sind. Für die Einträge

[5] Im Fall $n = 1$ legen wir formal $\widehat{A}_{11} := 1$ fest, womit der Entwicklungssatz und weitere folgende Resultate richtig bleiben. Dies kann man sich so erklären, dass man sich in diesem Fall die Streichmatrix als (0×0)-Matrix ohne Einträge und ihre Determinante als leeres Produkt mit Wert 1 vorstellt. Da der Umgang mit (1×1)-Matrizen und -Determinanten trivial ist, ist diese Festlegung aber ziemlich egal.

bedeutet dies $\overline{a}_{\ell,m} = a_{\sigma_i(\ell),\sigma_j(m)}$, wobei $\sigma_i \in \mathrm{S}_n$ den $(n{-}i{+}1)$-Zykel mit $\sigma_i(\ell) = \ell$ für $\ell < i$, mit $\sigma_i(\ell) = \ell{+}1$ für $i \le \ell < n$ und folglich mit $\sigma_i(n) = i$ bezeichnet und $\sigma_j \in \mathrm{S}_n$ analog definiert ist. Mit dieser Notation können wir das obige Produkt gemäß

$$\prod_{\substack{k=1\\k\neq i}}^{n} a_{k,\pi(k)} = \prod_{\ell=1}^{n-1} a_{\sigma_i(\ell),\pi(\sigma_i(\ell))} = \prod_{\ell=1}^{n-1} \overline{a}_{\ell,\sigma_j^{-1}(\pi(\sigma_i(\ell)))}$$

umschreiben. Nun ist $\pi \mapsto \sigma_j^{-1}\circ\pi\circ\sigma_i$ bijektiv von $\{\pi \in \mathrm{S}_n \,|\, \pi(i) = j\}$ auf $\{\gamma \in \mathrm{S}_n \,|\, \gamma(n) = n\}$ und ändert das Vorzeichen gerade um $(-1)^{i+j}$ (denn für $\gamma = \sigma_j^{-1}\circ\pi\circ\sigma_i$ übersetzt sich mit $\sigma_i(n) = i$, $\sigma_j(n) = j$ einerseits $\pi(i) = j$ in $\gamma(n) = n$, und mit σ_i als $(n{-}i{+}1)$-Zykel, σ_j als $(n{-}j{+}1)$-Zykel erhalten wir andererseits $\mathrm{sgn}(\gamma) = (-1)^{n-j+1}\mathrm{sgn}(\pi)(-1)^{n-i+1} = (-1)^{i+j}\mathrm{sgn}(\pi)$). Damit bekommen wir insgesamt

$$\begin{aligned}\sum_{\substack{\pi\in\mathrm{S}_n\\ \pi(i)=j}} \mathrm{sgn}(\pi) \prod_{\substack{k=1\\k\neq i}}^{n} a_{k,\pi(k)} &= (-1)^{i+j} \sum_{\substack{\gamma\in\mathrm{S}_n\\ \gamma(n)=n}} \mathrm{sgn}(\gamma) \prod_{\ell=1}^{n-1} \overline{a}_{\ell,\gamma(\ell)} = (-1)^{i+j} \sum_{\overline{\gamma}\in\mathrm{S}_{n-1}} \mathrm{sgn}(\gamma) \prod_{\ell=1}^{n-1} \overline{a}_{\ell,\overline{\gamma}(\ell)} \\ &= (-1)^{i+j} \det(\overline{a}_{\ell,m})_{\ell,m=1,2,\ldots,n-1} = \widehat{A}_{ij}\,,\end{aligned}$$

wobei wir $\gamma \in \mathrm{S}_n$ mit $\gamma(n) = n$ und $\overline{\gamma} \in \mathrm{S}_{n-1}$ auf naheliegende Weise identifiziert und zuletzt die Definition $\widehat{A}_{ij} = (-1)^{i+j} \det(\overline{a}_{\ell m})_{\ell,m=1,2,\ldots,n-1}$ des Kofaktors $\widehat{A}_{ij}$ benutzt haben. Nun erinnern wir uns, dass $j \in \{1, 2, \ldots, n\}$ beliebig war. Einsetzen der letzten vorausgehenden in die erste Formel des Beweises ergibt dann mit

$$\det A = \sum_{j=1}^{n} a_{i,j}\widehat{A}_{ij}$$

die Behauptung. □

Unser nächstes Ziel ist die **vielleicht nützlichste Anwendung der Determinante bei der Untersuchung der Invertierbarkeit von Matrizen**. Um zugleich auch eine Formel für die Inverse angeben zu können, benötigen wir aber vorweg noch eine Definition.

Definition (**Adjunkte/Kofaktormatrix**). *Seien K ein Körper und $n \in \mathbb{N}$. Die **Adjunkte**, Komplementärmatrix oder **Kofaktormatrix** einer $(n{\times}n)$-Matrix $A \in K^{n\times n}$ ist die $(n{\times}n)$-Matrix*

$$\mathrm{adj}\, A := \mathrm{Cof}\, A := \left(\widehat{A}_{ji}\right)_{i,j=1,2,\ldots,n} \in K^{n\times n}\,,$$

wobei $\widehat{A}_{ji} \in K$ den im Entwicklungssatz eingeführten Kofaktor bezeichnet, also gleich $(-1)^{i+j}$ mal der Determinante der Streichmatrix ist, in der die j-te Zeile und i-te Spalte von A wegfallen. (Man beachte dabei die Reihenfolge der Indizes bei $\widehat{A}_{ji}$, die einem Transponieren entspricht: Der Eintrag in der i-ten Zeile und j-ten Spalte von adj A *ergibt sich aus einer Determinante, bei der die j-te Zeile und i-te Spalte von A wegfallen.)*

Satz (über **Invertierbarkeit von Matrizen**). *Seien K ein Körper und $n \in \mathbb{N}$ und $A \in K^{n\times n}$ eine quadratische Matrix. Dann gelten*

$$\boxed{A \text{ invertierbar} \iff \det A \neq 0}$$

und

$$A(\operatorname{adj} A) = (\det A)\mathbb{I}_n = (\operatorname{adj} A)A\,.$$

Für invertierbares A ergibt sich hieraus die ***Formel für die Inverse***

$$A^{-1} = \frac{1}{\det A}\operatorname{adj} A\,.$$

Außerdem hatten wir als notwendige und hinreichende Kriterien für Invertierbarkeit von $A \in K^{n\times n}$ ja schon $\operatorname{Kern} A = \{0\}$ sowie $\operatorname{Bild} A = K^n$ identifiziert. Diese Kriterien, an die hier noch einmal erinnert sei, sind also äquivalent zu $\det A \neq 0$. Für die rechnerische Überprüfung ist das Determinanten-Kriterium aber tatsächlich oft am günstigsten.

Beweis. Wir zeigen zuerst die Implikation „$\Longrightarrow$“ der behaupteten Äquivalenz, greifen dafür aber auf die Produktformel $\det(AB) = (\det A)(\det B)$ für $A, B \in K^{n\times n}$ vor, die erst in Abschnitt 6.4 bewiesen wird. Ist $A \in K^{n\times n}$ invertierbar, so erhalten wir mit dieser Formel

$$1 = \det \mathbb{I}_n = \det\left(AA^{-1}\right) = (\det A)\left(\det\left(A^{-1}\right)\right).$$

Also ist $\det A$ invers zu $\det(A^{-1})$ im Grundkörper (!) K und insbesondere ungleich Null.

Weiter zeigen wir die Hilfsaussage[6], dass $\det A = 0$ gilt, sobald es für $A = (a_{i,j})_{i,j=1,2,\dots,n} \in K^{n\times n}$ Zeilenindizes $i \neq k$ in $\{1, 2, \dots, n\}$ mit $a_{i,j} = a_{k,j}$ für alle $j \in \{1, 2, \dots, n\}$ gibt, sobald also mit anderen Worten zwei Zeilen von A übereinstimmen. Zur Herleitung der Hilfsaussage zerlegen wir S_n in die Mengen der geraden und ungeraden Permutationen, wobei jede ungerade Permutation $\sigma \in \mathrm{S}_n$ als $\sigma = \pi \circ \tau_{ik}$ mit der geraden Permutation $\pi := \sigma \circ \tau_{ik}^{-1} \in \mathrm{S}_n$ und der festen (!) Transposition $\tau_{ik} \in \mathrm{S}_n$, die i und k vertauscht, geschrieben werden kann. Aus der Leibniz-Formel erhalten wir dann

$$\det A = \sum_{\substack{\pi\in\mathrm{S}_n \\ \pi \text{ gerade}}} \Big(\underbrace{a_{1,\pi(1)}a_{2,\pi(2)}\cdot\ldots\cdot a_{n,\pi(n)} - a_{1,\pi\circ\tau_{ik}(1)}a_{2,\pi\circ\tau_{ik}(2)}\cdot\ldots\cdot a_{n,\pi\circ\tau_{ik}(n)}}_{=:\,P_\pi} \Big)\,.$$

Dabei stimmen im vorderen und hinteren Summand von P_π alle Faktoren außer dem i-ten und dem k-ten überein (denn für $j \in \{1, 2, \dots, n\} \setminus \{i, k\}$ ist $\tau_{ik}(j) = j$), und auch für das Produkt des i-ten und k-ten Faktors erhalten wir mit $a_{i,\pi\circ\tau_{ik}(i)}a_{k,\pi\circ\tau_{ik}(k)} = a_{i,\pi(k)}a_{k,\pi(i)} = a_{k,\pi(k)}a_{i,\pi(i)}$ Übereinstimmung (wobei im letzten Schritt einging, dass i-te und k-te Zeile gleich sind). Also ist $P_\pi = 0$ für alle geraden $\pi \in \mathrm{S}_n$ und damit wie behauptet $\det A = 0$.

Wir kommen nun zum Beweis der Formel $A(\operatorname{adj} A) = (\det A)\mathbb{I}_n$ für $A = (a_{i,j})_{i,j=1,2,\dots,n} \in K^{n\times n}$. Hierfür berechnen wir für $i \in \{1, 2, \dots, n\}$ den (i, i)-Eintrag $(A(\operatorname{adj} A))_{ii}$ von $A(\operatorname{adj} A)$ (auf der Hauptdiagonale von $A(\operatorname{adj} A)$) als

$$(A(\operatorname{adj} A))_{ii} = \sum_{j=1}^{n} a_{i,j}\widehat{A}_{ij} = \det A\,,$$

wobei die erste Gleichheit aus den Definitionen der Adjunkten und der Matrizenmultiplikation folgt und sich die zweite durch Entwicklung nach der i-ten Zeile ergibt. Ähnlich bestimmen wir für $i \neq k$ in $\{1, 2, \dots, k\}$ nun den (i, k)-Eintrag $(A(\operatorname{adj} A))_{ik}$. Wir schreiben dazu $A_{k\leftarrow i}$ für die

[6] Tatsächlich steht im Hintergrund der Hilfsaussage die sogenannte Multilinearität der Determinante, die in Mathematik 3 besprochen wird.

$(n\times n)$-Matrix, die aus A hervorgeht, wenn die k-te Zeile durch eine Kopie der i-ten Zeile ersetzt wird, und die somit in beiden diese Zeilen die gleichen Einträge $a_{i,j}$ enthält. Wir erhalten dann

$$(A(\operatorname{adj} A))_{ik} = \sum_{j=1}^{n} a_{i,j}\widehat{A}_{kj} = \det A_{k\leftarrow i} = 0\,,$$

wobei die zweite Gleichheit auf Entwicklung von $\det A_{k\leftarrow i}$ nach der k-ten Zeile und die dritte Gleichheit auf der Hilfsaussage beruhen. Damit sind die Einträge von $A(\operatorname{adj} A)$ insgesamt als $(A(\operatorname{adj} A))_{ik} = (\det A)\delta_{ik}$ mit $i,k \in \{1,2,\ldots,n\}$ bestimmt, mit anderen Worten gilt also $A(\operatorname{adj} A) = (\det A)\mathbb{I}_n$.

Die Formel $(\operatorname{adj} A)A = (\det A)\mathbb{I}_n$ mit Multiplikation in der umgekehrten Reihenfolge kann man analog herleiten oder auf das Vorige zurückführen. Letzteres gelingt mit der Rechnung $(\operatorname{adj} A)A = \big(A^{\mathrm{T}}(\operatorname{adj} A)^{\mathrm{T}}\big)^{\mathrm{T}} = \big(A^{\mathrm{T}}\operatorname{adj}\big(A^{\mathrm{T}}\big)\big)^{\mathrm{T}} = \big(\det\big(A^{\mathrm{T}}\big)\mathbb{I}_n\big)^{\mathrm{T}} = \big(\det\big(A^{\mathrm{T}}\big)\big)\mathbb{I}_n = (\det A)\mathbb{I}_n$, bei der unter anderem $(\operatorname{adj} A)^{\mathrm{T}} = \operatorname{adj}(A^{\mathrm{T}})$ (direkte Folgerung aus der Definition), das zuvor Gezeigte für A^{T} anstelle von A und $\det(A^{\mathrm{T}}) = \det A$ (Aussage des vorigen Satzes) eingehen.

Insgesamt ist somit $(\operatorname{adj} A)A = (\det A)\mathbb{I}_n = A(\operatorname{adj} A)$ für alle $A \in K^{n\times n}$ gezeigt. Ist nun $\det A \neq 0$, so kann diese Formel durch den Skalar $\det A$ geteilt werden und zeigt, dass $\frac{1}{\det A}\operatorname{adj} A$ invers zu A ist. Damit sind auch die Implikation „$\Longleftarrow$“ der Äquivalenz und die Formel für die Inverse verifiziert, und der Beweis ist komplett. □

Als letztes Thema, das wir zumindest rechnerisch auch über die Determinante angehen werden, beschäftigen wir uns in diesem Kapitel mit speziellen Vektoren, die bei Multiplikation mit einer gegebenen Matrix lediglich vervielfacht werden. (Solche Vektoren lassen sich für viele Matrizen, aber nicht unbedingt immer, finden.)

Definitionen (**Eigenwerte**, **Eigenvektoren**, **Eigenräume**). *Seien K ein Körper, $A \in K^{n\times n}$ mit $n \in \mathbb{N}$ eine $(n\times n)$-Matrix über K und $\varphi \in \operatorname{End}_K(V)$ eine K-lineare Selbstabbildung eines K-Vektorraums V in sich.*

(I) *Wir nennen $x \in K^n \setminus \{0\}$ bzw. $v \in V \setminus \{0\}$ einen **Eigenvektor** von A bzw. φ zu $\lambda \in K$, wenn*

$$Ax = \lambda x \qquad \text{bzw.} \qquad \varphi(v) = \lambda v$$

*gilt. Gibt es einen Eigenvektor (der nach Definition $\neq 0$ sein muss) von A bzw. φ zu $\lambda \in K$, so nennen wir weiterhin λ einen **Eigenwert** von A bzw. φ.*

(II) *Der **Eigenraum** von A bzw. φ zu $\lambda \in K$ ist der Untervektorraum*

$$\mathrm{E}_\lambda(A) := \operatorname{Kern}(A-\lambda\mathbb{I}_n) \subset K^n \qquad \text{bzw.} \qquad \mathrm{E}_\lambda(\varphi) := \operatorname{Kern}(\varphi-\lambda\operatorname{id}_V) \subset V\,,$$

*der genau die Eigenvektoren von A bzw. φ zu λ und den Nullvektor enthält. Als die **geometrische Vielfachheit eines Eigenwerts** λ von A bzw. φ bezeichnet man die Zahl $\dim E_\lambda(A) \in \{1,2,\ldots,n\}$ bzw. $\dim E_\lambda(\varphi) \in \mathbb{N}\,\dot\cup\,\{\infty\}$.*

Bemerkungen (zu **Eigenwerten**, **Eigenvektoren**, **Eigenräumen**). Seien K ein Körper, $n \in \mathbb{N}$ und V ein K-Vektorraum.

(1) Dass $\lambda \in K$ ein Eigenwert von $A \in K^{n\times n}$ bzw. $\varphi \in \operatorname{End}_K(V)$ ist, bedeutet nichts anderes als $\mathrm{E}_\lambda(A) \neq \{0\}$ bzw. $\mathrm{E}_\lambda(\varphi) \neq \{0\}$.

(2) Eigenwerte, -vektoren und -räume einer Matrix hängen direkt mit den Eigenwerten, -vektoren und -räumen eines durch A dargestellten Endomorphismus zusammen, *sofern* man in Definitionsbereich V und Ziel V die gleiche Basis verwendet. Genauer bedeutet dies für $A \in K^{n\times n}$, eine K-Basis $\mathcal{B}$ von V mit $\dim V = n$ und $\lambda \in K$, $x \in K^n$:

$$\begin{aligned} \lambda \text{ Eigenwert von } \mathrm{L}_{\mathcal{BB}}(A) &\iff \lambda \text{ Eigenwert von } A\,, \\ x_{\mathcal{B}} \text{ Eigenvektor von } \mathrm{L}_{\mathcal{BB}}(A) \text{ zu } \lambda &\iff x \text{ Eigenvektor von } A \text{ zu } \lambda\,, \\ \mathrm{E}_\lambda(\mathrm{L}_{\mathcal{BB}}(A)) &= \{x_{\mathcal{B}} \,|\, x \in \mathrm{E}_\lambda(A)\}\,. \end{aligned}$$

Folgerungen & Verfahren (zur **Berechnung von Eigenwerten und Eigenvektoren**)**.** Seien K ein Körper und $n \in \mathbb{N}$.

(1) Die **Eigenwerte** $\lambda \in K$ von $A = (a_{i,j})_{i,j=1,2,\dots,n} \in K^{n\times n}$ sind **genau die Nullstellen** $\lambda \in K$ des **charakteristischen Polynoms**

$$\mathrm{Ch}(A) := \det(\mathrm{X}\mathbb{I}_n - A) = \sum_{\pi\in \mathrm{S}_n} \prod_{i=1}^{n} (\delta_{i,\pi(i)}\mathrm{X} - a_{i,\pi(i)}) \in K[\mathrm{X}]$$

von A in der Unbestimmten X. Da $\mathrm{Ch}(A)$ den Grad n hat, gibt es höchstens n Nullstellen von $\mathrm{Ch}(A)$ und damit höchstens n Eigenwerte von A.

(Begründung: Aus den Definitionen und den verschiedenen Kriterien für Invertierbarkeit von Matrizen entnehmen wir für $A \in K^{n\times n}$ und $\lambda \in K$ die Äquivalenzen

$$\begin{aligned} \lambda \text{ Eigenwert von } A &\iff \mathrm{E}_\lambda(A) \neq \{0\} \iff \mathrm{Kern}(\lambda\mathbb{I}_n - A) \neq \{0\} \iff \lambda\mathbb{I}_n - A \text{ nicht invertierbar} \\ &\iff \det(\lambda\mathbb{I}_n - A) = 0 \iff \lambda \text{ Nullstelle von } \mathrm{Ch}(A)\,, \end{aligned}$$

erhalten also die Behauptung.)

(2) Gemäß (1) kann man die **Eigenwerte** einer Matrix $A \in K^{n\times n}$ **schematisch als Nullstellen** von $\mathrm{Ch}(A)$ **berechnen**. Die **Eigenvektoren** beziehungsweise den **Eigenraum** von A zu den gefundenen Eigenwerten $\lambda \in K$ erhält man im Anschluss **durch Lösen des linearen Gleichungssystems** $(\lambda\mathbb{I}_n - A)v = 0$ in $v \in K^n$.

Beispiel (zur **Berechnung von Eigenwerten und Eigenvektoren**)**.** Wir behandeln das Beispiel der (2×2)-Matrix

$$A := \begin{pmatrix} 1 & -1 \\ 0 & -3 \end{pmatrix} \in \mathbb{R}^{2\times 2}\,,$$

als deren charakteristisches Polynom wir

$$\mathrm{Ch}(A) = \det(\mathrm{X}\mathbb{I}_2 - A) = \begin{vmatrix} \mathrm{X}-1 & 1 \\ 0 & \mathrm{X}+3 \end{vmatrix} = (\mathrm{X}-1)(\mathrm{X}+3)$$

erhalten. Da sich hier das charakteristische Polynom als Produkt von Linearfaktoren ergibt, können wir als dessen Nullstellen die Eigenwerte 1 und -3 von A direkt ablesen. Die Eigenvektoren beziehungsweise Eigenräume von A zu $\lambda = 1$ und $\lambda = -3$ bestimmen wir aus dem Gleichungssystem $(\lambda\mathbb{I}_n - A)v = 0$ wie folgt:

$$\begin{aligned} \begin{pmatrix} 0 & 1 \\ 0 & 4 \end{pmatrix}\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = 0 \quad &\rightsquigarrow \quad v_2 = 0 \quad \rightsquigarrow \quad \mathrm{E}_1(A) = \left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\rangle\,, \\ \begin{pmatrix} -4 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = 0 \quad &\rightsquigarrow \quad v_2 = 4v_1 \quad \rightsquigarrow \quad \mathrm{E}_{-3}(A) = \left\langle \begin{pmatrix} 1 \\ 4 \end{pmatrix} \right\rangle\,. \end{aligned}$$

(Man kann natürlich auch mit $\left(\begin{smallmatrix}1&-1\\0&-3\end{smallmatrix}\right)\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right) = \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$ und $\left(\begin{smallmatrix}1&-1\\0&-3\end{smallmatrix}\right)\left(\begin{smallmatrix}1\\4\end{smallmatrix}\right) = -3\left(\begin{smallmatrix}1\\4\end{smallmatrix}\right)$ die Probe machen, das $\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$ und $\left(\begin{smallmatrix}1\\4\end{smallmatrix}\right)$ in der Tat Eigenvektoren zu den Eigenwerten 1 und -3 sind.) Da beide Eigenräume 1-dimensional sind, haben in diesem Beispiel beide Eigenwerte die geometrische Vielfachheit 1.

Beispiele für die Eigenwert/-vektor-Berechnung bei (etwas) größeren Matrizen, für Eigenwerte höherer Vielfachheiten und für $(n\times n)$-Matrizen mit weniger als n Eigenwerten werden in den Übungen behandelt (und auch in Mathematik 3 noch genauer diskutiert).

Bemerkungen (zur **Berechnung von Eigenwerten und Eigenvektoren**)**.** Seien K ein Körper und $n \in \mathbb{N}$.

(1) ***Bei einer Dreiecks- und Diagonalmatrix*** $A \in K^{n\times n}$ ergibt sich das charakteristische Polynom $\mathrm{Ch}(A) \in K[\mathrm{X}]$ wie im vorigen Beispiel direkt als Produkt von Linearfaktoren, und die **Eigenwerte** sind *bei einer solchen Matrix* **genau die Einträge auf der Hauptdiagonale**. ***Im Allgemeinen*** bekommt man $\mathrm{Ch}(A)$ nicht direkt in dieser günstigen Form, und die Bestimmung der Eigenwerte als Nullstellen erfordert die **Lösung einer polynomialen Gleichung *n*-ten Grades**. Zum Verfahren hierbei vergleiche mit Abschnitt 3.2.

(2) Als **algebraische Vielfachheit eines Eigenwerts** $\lambda \in K$ von $A \in K^{n\times n}$ bezeichnet man die Vielfachheit von λ als Nullstelle des charakteristischen Polynoms $\mathrm{Ch}(A) \in K[\mathrm{X}]$, also die Anzahl der Linearfaktoren $\mathrm{X}-\lambda$, die man von $\mathrm{Ch}(A)$ abspalten kann. In Abschnitt 6.4 werden wir zeigen, dass die algebraische Vielfachheit eines Eigenwerts immer größer oder gleich seiner geometrischen Vielfachheit ist.

(3) Die Eigenwerte eines Endomorphismuses $\varphi \in \mathrm{End}_K(V)$ eines endlich-dimensionalen K-Vektorraums V können nach der früheren Bemerkung (2) als die der darstellenden Matrix $\mathrm{M}_{\mathcal{BB}}(\varphi)$ bezüglich einer beliebigen Basis $\mathcal{B}$ von V berechnet werden. Auch die Eigenvektoren von φ (oder genauer ihre Koeffizienten in $\mathcal{B}$-Basisdarstellung) erhält man aus den Eigenvektoren von $\mathrm{M}_{\mathcal{BB}}(\varphi)$.

6.4 Lineare Gleichungssysteme und Elementaroperationen

In diesem letzten Abschnitt der Mathematik 2 wenden wir die bisher entwickelte lineare Algebra auf lineare Gleichungssysteme an und entwickeln **allgemeine Theorie und Rechenverfahren** zu deren Lösung. Elementaroperationen genannte Umformungen werden sich dabei sowohl fürs Rechnen als auch für die Theorie und den Nachweis einiger in Abschnitt 6.3 zurückgestellter Behauptungen als nützlich erweisen.

Definition (**lineare Gleichungssysteme**)**.** *Seien K ein Körper und $m, n \in \mathbb{N}$. Ein **lineares Gleichungssystem** aus m Gleichungen für n Unbestimmte $x = (x_1, x_2, \ldots, x_n) \in K^n$ hat die Form*

$$\begin{array}{rl} G_1\colon & a_{11}x_1 + a_{12}x_2 + a_{13}x_3 + \ldots + a_{1n}x_n = b_1\,, \\ G_2\colon & a_{21}x_1 + a_{22}x_2 + a_{23}x_3 + \ldots + a_{2n}x_n = b_2\,, \\ \vdots & \quad\vdots \quad\quad \vdots \quad\quad \vdots \quad\quad\quad\quad \vdots \quad\quad \vdots \\ G_m\colon & a_{m1}x_1 + a_{m2}x_2 + a_{m3}x_3 + \ldots + a_{mn}x_n = b_m \end{array} \qquad (*)$$

*mit gegebenen **Koeffizienten** $a_{ij} \in K$ und gegebenen **Inhomogenitäten** $b_i \in K$. Im Fall $b_1 = b_2 = \ldots = b_m = 0$ heißt das Gleichungssystem **homogen**. Die **Lösungsmenge** des Gleichungssystems ist die Menge der $x \in K^n$, für die alle m Gleichungen G_1, G_2, …, G_m zugleich erfüllt sind.*

Bemerkungen (zur **Lösungstheorie linearer Gleichungssysteme**)**.** Seien K, m, n, a_{ij} und b_i wie in der vorausgehenden Definition.

(1) Mit der **Koeffizientenmatrix** $A := (a_{ij})_{\substack{i=1,2,\dots,m\\ j=1,2,\dots,n}} \in K^{m\times n}$ und der **rechten Seite/Inhomogenität** $b := \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$ schreiben wir **das lineare Gleichungssystem (∗) in der kurzen und prägnanten Form**

$$\boxed{Ax = b}\,.$$

(2) Im **homogenen Fall** $b = 0$ ist die **Lösungsmenge** des linearen Gleichungssystems $Ax = 0$ **stets ein K-Untervektorraum** von K^n und genauer gleich dem K-Untervektorraum $\operatorname{Kern} A$ von K^n. Insbesondere ist $x = 0$ (wegen $0 \in \operatorname{Kern} A$) stets eine Lösung von (∗), genannt die **triviale Lösung** oder Nulllösung.

Im allgemeinen, eventuell **inhomogenen Fall** gibt es für die **Lösungsmenge** des linearen Gleichungssystems $Ax = b$ **zwei Alternativen**: Im Fall $b \notin \operatorname{Bild} A$ ist die Lösungsmenge **leer**. Im Fall $b \in \operatorname{Bild} A$ ist die Lösungsmenge **stets ein affiner Unterraum** von K^n und genauer gleich dem affinen Unterraum $x_0 + \operatorname{Kern} A$ von K^n mit irgendeiner Lösung $x_0 \in K^n$ zu $Ax_0 = b$. In letzterem Fall ergibt sich also die **allgemeine Lösung zu $Ax = b$ als Summe aus einer speziellen Lösung x_0 zu $Ax_0 = b$ und der allgemeinen Lösung des zugehörigen homogenen Gleichungssystems $Ax = 0$**.

Aus dem Vorigen und der Dimensionsformel $\dim(\operatorname{Kern} A) = n - \dim(\operatorname{Bild} A)$ des Abschnitts 6.3 lässt sich ablesen: Ist $Ax = b$ für Inhomogenitäten b im k-dimensionalen Raum $\operatorname{Bild} A$ lösbar, so hat für jede einzelne dieser Inhomogenitäten b der Lösungsraum $x_0 + \operatorname{Kern} A$ (mit von b abhängiger spezieller Lösung x_0) stets die Dimension $n-k$.

(3) **Notwendig und hinreichend für Lösbarkeit** von $Ax = b$ ist das **Rangkriterium**

$$\operatorname{Rang}(A \,|\, b) = \operatorname{Rang} A$$

mit der **erweiterten Koeffizientenmatrix** $(A \,|\, b) \in K^{m\times(n+1)}$, die durch Hinzufügen des Vektors $b \in K^m = K^{m\times 1}$ zur Matrix $A \in K^{m\times n}$ in Form einer zusätzlichen Spalte entsteht.

(Begründung: Lösbarkeit von $Ax = b$ bedeutet, dass es $x = (x_1, x_2, \dots, x_n) \in K^n$ mit $Ax = b$ oder äquivalent $\sum_{j=1}^n x_j Ae_j = b$ gibt. Mit anderen Worten heißt dies $b \in \operatorname{Span}\{Ae_1, \dots, Ae_n\}$, äquivalent $\operatorname{Span}\{Ae_1, \dots, Ae_n, b\} = \operatorname{Span}\{Ae_1, \dots, Ae_n\}$ oder, noch anders formuliert, $\operatorname{Bild}(A \,|\, b) = \operatorname{Bild} A$. Schließlich ist auch $\operatorname{Rang}(A \,|\, b) = \operatorname{Rang} A$ äquivalent, denn nach Abschnitt 6.2 tritt für die Vektorräume $\operatorname{Bild} A \subset \operatorname{Bild}(A \,|\, b)$ genau dann Gleichheit ein, wenn $\dim(\operatorname{Bild} A)$ mit $\dim(\operatorname{Bild}(A \,|\, b))$ übereinstimmt.)

(4) **Speziell für $m = n$ und eine invertierbare Koeffizientenmatrix $A \in K^{n\times n}$** hat das lineare Gleichungssystem $Ax = b$ für jede Inhomogenität $b \in K^n$ die **eindeutige Lösung**

$$x = A^{-1}b \in K^n\,.$$

Wegen der Formel für die inverse Matrix bedeutet dies nichts anderes als $x = \frac{1}{\det A}(\operatorname{adj} A)b$. Diese allgemeine Lösungsformel kann man als die sogenannte **Cramersche Regel**

$$x_j = \frac{\det \begin{pmatrix} a_{1,1} \dots a_{1,j-1} & b_1 & a_{1,j+1} \dots a_{1,n} \\ \vdots \ddots \vdots & \vdots & \vdots \ddots \vdots \\ a_{n,1} \dots a_{n,j-1} & b_n & a_{n,j+1} \dots a_{n,n} \end{pmatrix}}{\det \begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \dots & a_{n,n} \end{pmatrix}} \qquad \text{für } j = 1, 2, \dots, n$$

schreiben, wobei man durch Entwicklung nach der j-ten Spalte einsieht, dass die Determinante im Zähler mit $\sum_{i=1}^{n} \widehat{A}_{ij} b_i = ((\operatorname{adj} A)b)_j$ übereinstimmt und die Cramersche Regel eine Umschreibung der zuvor bemerkten Formel ist.

Nun kommen wir zu den bereits angekündigten Elementaroperationen und werden sehen, dass durch diese jedes lineare Gleichungssystem auf eine besonders günstige Form gebracht werden kann, an der sich die Lösung gut ablesen lässt.

Definition (**elementare Zeilenoperationen**). *Seien K ein Körper, seien $m, n \in \mathbb{N}$, und sei ein lineares Gleichungssystem der Form (∗) mit $a_{ij}, b_i \in K$ gegeben. Genau die folgenden drei Typen von Operationen bezeichnen wir als **elementare Zeilenoperationen** mit dem Gleichungssystem (∗) (wobei stets $\lambda \in K$ und $i, k \in \{1, 2, \ldots, m\}$ seien):*

(1) *Ersetzung einer Gleichung G_i durch ihr Vielfaches λG_i mit $\lambda \neq 0$,*

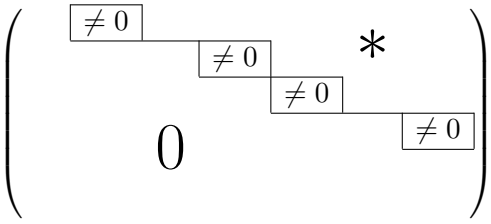
(2) *Ersetzung einer Gleichung G_i durch $G_i + \lambda G_k$ mit $k \neq i$,*

(3) *Vertauschung einer Gleichung G_i mit einer Gleichung G_k.*

Bei (1) werden hier beide *Seiten der Gleichung G_i mit λ multipliziert. Bei (2) werden die beiden linken Seiten von G_i und λG_k zur neuen linken Seite, die beiden rechten Seiten zur neuen rechten Seite addiert. Die Operation (3) schließlich betrifft nur die Reihenfolge, in der die Gleichungen aufgelistet werden.*

Satz (über die **Herstellung der Zeilenstufenform**). *Seien K ein Körper und $m, n \in \mathbb{N}$. Jedes lineare Gleichungssystem $Ax = b$ mit $A \in K^{m \times n}$ und $b \in K^m$ (das ausgeschrieben die Form (∗) hat) kann **durch endlich viele elementare Zeilenoperationen** in ein lineares Gleichungssystem $\widetilde{A}x = \widetilde{b}$ mit $\widetilde{A} = (\widetilde{a}_{ij})_{\substack{i=1,2,\ldots,m \\ j=1,2,\ldots,n}} \in K^{m \times n}$ und $\widetilde{b} \in K^m$ überführt werden, wobei:*

- *$\widetilde{A}x = \widetilde{b}$ die **gleiche Lösungsmenge** wie $Ax = b$ hat und $\operatorname{Kern} \widetilde{A} = \operatorname{Kern} A$ gilt,*
- *$\widetilde{A}$ die nebenstehend angedeutete **Zeilenstufenform** hat, d.h. präzise, es gibt ein $k \in \{0, 1, \ldots, m\}$ und $\ell_1 < \ell_2 < \ldots < \ell_k$ in $\{1, 2, \ldots, n\}$, so dass für $i \in \{1, 2, \ldots, m\}$, $j \in \{1, 2, \ldots, n\}$ gilt: $\widetilde{a}_{i\ell_i} \neq 0$ für $i \leq k$ sowie $\widetilde{a}_{ij} = 0$ für $i \leq k$, $j < \ell_i$ und auch $\widetilde{a}_{ij} = 0$ für $i > k$.*



Tatsächlich kann auch eine speziellere Form erreicht werden, bei der $\widetilde{a}_{i\ell_i} = 1$ für $i \leq k$ (und ansonsten alles wie zuvor) ist. Speziell für $m = n$ und invertierbares $A \in K^{n \times n}$ lässt sich sogar $\widetilde{A} = \mathbb{I}_n$ (und ansonsten alles wie zuvor) erreichen.

Der Beweis des Satzes basiert auf dem wichtigen **Gauß-Verfahren/Gauß-Algorithmus**. Wir geben dazu im Folgenden eine Erläuterung, die sich zwischen einer Beschreibung des Algorithmus, einer Begründung des Vorgehens und einem formalen mathematischen Beweis bewegt:

Beweisskizze. Beim **Gauß-Verfahren** führt man **nacheinander für die Variablen/Spalten** zum Spaltenindex j_0 und jeweils einen zugehörigen Zeilenindex $i_0 \in \{1, 2, \ldots, m\}$ (beginnend mit $i_0 = 1$) elementare Zeilenoperationen mit dem linearen Gleichungssystem (∗) durch. Behandelt und verändert werden dabei in jedem Schritt (und allen danach folgenden) nur noch die Gleichungen $G_{i_0}, G_{i_0+1}, \ldots, G_m$ ab dem aktuellen i_0. Wir **beschreiben** nun das **Vorgehen in den Einzelschritten** und **bezeichnen** dabei **die jeweils *aktuellen* Gleichungen und Koeffizienten mit G_i und a_{ij}:**

- Im trivialen Fall $a_{ij_0} = 0$ für alle $i \in \{i_0, i_0{+}1, \ldots, m\}$ tritt die Variable x_{j_0} in den Gleichungen $G_{i_0}, G_{i_0+1}, \ldots, G_m$ nicht (mehr) auf, und es sind im aktuellen Schritt keine Umformungen erforderlich. Man geht zur nächsten Variable/Spalte (nächsthöheres j_0) und bleibt dabei in der gleichen Zeile (unverändertes i_0).

- Im Fall $a_{ij_0} \neq 0$ für mindestens ein $i \in \{i_0, i_0{+}1, \ldots, m\}$ möchte man $a_{i_0 j_0} \neq 0$ haben, was oft direkt erfüllt ist und ansonsten durch Vertauschung von G_{i_0} mit einer späteren Gleichungen G_i gemäß Operation (3) erreicht werden kann. Ist $a_{i_0 j_0} \neq 0$ erreicht, so ersetzt man mit Anwendungen der Operation (2) für jedes $i \in \{i_0{+}1, i_0{+}2, \ldots, m\}$ die Gleichung G_i durch $G_i - \frac{a_{ij_0}}{a_{i_0 j_0}} G_{i_0}$. Dies ist der **entscheidende Schritt des ganzen Verfahrens**, denn die Vorfaktoren sind gerade so gewählt, dass die **Variable x_{j_0}** in den ersetzenden Gleichungen **ab der Zeile $i_0{+}1$ eliminiert wird**. Man geht nun zur nächsten Variable/Spalte (nächsthöheres j_0) und zugleich zur nächsten Zeile (nächsthöheres i_0) über — außer das nächsthöhere i_0 ist bereits m, so dass nur noch eine Gleichung verbleibt, keine weiteren Operationen nötig sind und das Verfahren an dieser Stelle endet.

Falls nicht vorher mit $i_0 = m$ die Gleichungen ausgehen, endet das Gauß-Verfahren spätestens nach der Behandlung der Variable/Spalte zu $j_0 = n$. Unabhängig vom Kriterium für den Abbruch, **erreicht man bei Abbruch die gewünschte Zeilenstufenform**.

Wir erläutern noch kurz die ergänzenden Behauptungen des Satzes:

Die speziellere Form mit $\widetilde{a}_{i\ell_i} = 1$ erhält man aus der Zeilenstufenform einfach durch Multiplikation der Zeilen mittels Operation (1).

Für $m = n$ und invertierbares A gilt man notwendig $k = n$ (siehe die nach diesem Beweis folgende Bemerkung), und man erhält als Zeilenstufenform eine obere Dreiecksmatrix mit lauter Einträgen 1 auf der Hauptdiagonale. Alle Einträge oberhalb der Hauptdiagonale können nun durch weitere elementare Zeilenoperationen gemäß einer naheliegenden Variante des Gauß-Verfahrens eliminiert werden, um so auf die Einheitsmatrix $\mathbb{I}_n$ zu kommen.

Schließlich bleibt noch zu begründen, dass das neue, durch elementare Zeilenoperationen erreichte Gleichungssystem (in allen Fällen) die gleiche Lösungsmenge und den gleichen Kern der Koeffizientenmatrix hat wie das ursprüngliche Gleichungssystem. Dies folgt aber tatsächlich, da elementare Zeilenoperationen Äquivalenzumformungen des Gleichungssystems und auch des zugehörigen homogenen Gleichungssystems sind und daher Lösungsmenge bzw. Kern nicht ändern. (Man beachte dabei insbesondere, dass die Operationen (1), (2), (3) jeweils durch eine Operation desselben Typs rückgängig gemacht werden können.)

Eine formale Präzisierung der vorausgehenden, auf dem Gauß-Verfahren basierenden Argumente kann durch Induktion nach $n \in \mathbb{N}$ erfolgen. Klarer wird das Vorgehen damit aber nicht unbedingt. □

Bemerkungen und Definitionen (zu **Gauß-Verfahren** und **Elementaroperationen**)**.** Seien K ein Körper und $m, n \in \mathbb{N}$.

(1) Für die Matrizen A und $\widetilde{A}$ des letzten Satzes ist

$$\operatorname{Rang} A = \operatorname{Rang} \widetilde{A} = k$$

(denn zum einen entnimmt man aus der Zeilenstufenform $\operatorname{Bild} \widetilde{A} = \mathbb{R}^k \times \{0\}^{m-k}$ und damit $\operatorname{Rang} \widetilde{A} = k$, zum anderen folgt aus $\operatorname{Kern} \widetilde{A} = \operatorname{Kern} A$ mit der Dimensionsformel für Matrizen, dass $\operatorname{Rang} \widetilde{A} = n - \dim(\operatorname{Kern} \widetilde{A}) = n - \dim(\operatorname{Kern} A) = \operatorname{Rang} A$ ist).

(2) Ist $\widetilde{A}$ wie im letzten Satz auf Zeilenstufenform, so kann man die allgemeine Lösung des linearen Gleichungssystems $\widetilde{A}x = \widetilde{b}$ im Wesentlichen ablesen: Ist $\widetilde{b}_i \neq 0$ für ein $i > k$, so ist wegen der unlösbaren Gleichung $0 = \widetilde{b}_i$ die Lösungsmenge von $\widetilde{A}x = \widetilde{b}$ leer. Ist $b_i = 0$ für alle $i > k$, so kann man die nicht-trivialen Gleichungen in den ersten k Zeilen nacheinander von unten nach oben nach den k Variablen x_{ℓ_k}, $x_{\ell_{k-1}}$, …, x_{ℓ_2}, x_{ℓ_1} auflösen und diese durch die anderen $(n-k)$ Variablen ausdrücken. Für jede Vorgabe der $(n-k)$ „anderen" Variablen erhält man also eine Lösung und insgesamt einen Lösungsraum der Dimension $n-k = n-\operatorname{Rang} A = \dim(\operatorname{Kern} A)$.

Der **Gauß-Algorithmus** ist daher das **Standard-Rechenverfahren zur Herstellung der Zeilenstufenform** und damit **zum Lösen linearer Gleichungssysteme** sowie **zur Bestimmung von Kern oder Rang von Matrizen**.

(3) **Elementare Zeilenoperationen** können auch unabhängig von einem linearen Gleichungssystem **mit (den Zeilen) einer beliebigen Matrix** $A \in K^{m\times n}$ durchgeführt werden. Jede einzelne elementare Zeilenoperation entspricht dabei dem Übergang von $A \in K^{m\times n}$ zu $EA \in K^{m\times n}$ mit einer invertierbaren **Elementarmatrix** $E \in K^{m\times m}$ eines der folgenden **drei Typen** (wobei stets $\lambda \in K$, $i, k \in \{1, 2, \ldots, m\}$ ist und *alle nicht eingetragenen beziehungsweise nicht erwähnten Einträge* 0 *sind*): Der elementaren Zeilenoperation (1) entspricht eine Elementarmatrix

$$\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & \lambda & \\ & & & & 1 \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix},$$

die mit Ausnahme des (i,i)-Eintrags $\lambda \neq 0$ lauter Einträge 1 auf der Hauptdiagonale hat. Der elementaren Zeilenoperation (2) entspricht eine Elementarmatrix

$$\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & \ddots & \lambda \\ & & & \ddots & 1 \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix} \quad \text{oder} \quad \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & \ddots & \\ & & \lambda & & 1 \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix},$$

die den (i,k)-Eintrag λ mit $i \neq k$ und lauter Einträge 1 auf der Hauptdiagonale hat. Der elementaren Zeilenoperation (3) entspricht eine Elementarmatrix

$$\begin{pmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & 0 & & & 1 & \\ & & & & 1 & & & \\ & & & & & \ddots & & \\ & & & & & & 1 & \\ & & & 1 & & & 0 & \\ & & & & & & & 1 \\ & & & & & & & & \ddots \\ & & & & & & & & & 1 \end{pmatrix}$$

mit den (i,k)- und (k,i)-Einträgen 1 für $k \neq i$ sowie mit Ausnahme der (i,i)- und (k,k)-Einträge 0 mit lauter Einträgen 1 auf der Hauptdiagonale. Die letzte Matrix ist dabei nichts anderes als die Permutationsmatrix E_τ zur Transposition $\tau \in \mathrm{S}_m$ von i und k.

Übrigens kann die elementare Zeilenoperation des Typs (3) aus den anderen beiden Operationen zusammengesetzt werden. Dies erkennt man zunächst anhand $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ für (2×2)-Elementarmatrizen. Da

es nur um die Vertauschung von *zwei* Zeilen geht, ist ein analoges Zusammensetzen auch im $(m\times m)$-Fall möglich. Man könnte somit bei der Definition elementarer Zeilenoperationen auf den Typ (3) verzichten. Da dies nicht ganz offensichtlich ist, nimmt man den Typ (3) aber üblicherweise wie oben in die Definition hinein.

(4) **Speziell für** $m = n$ und eine **invertierbare Matrix** $A \in K^{n\times n}$ kann die letzte Aussage des letzten Satzes nach der vorigen Bemerkung (3) so formuliert werden, dass es ein $s \in \mathbb{N}_0$ und Elementarmatrizen $E_1, E_2, \ldots, E_s \in K^{n\times n}$ mit $E_1E_2\cdot\ldots\cdot E_sA = \mathbb{I}_n$ gibt. Dies bedeutet auch $A^{-1} = E_1E_2\cdot\ldots\cdot E_s = E_1E_2\cdot\ldots\cdot E_s\mathbb{I}_n$ und gibt daher ein **Verfahren zur Berechnung der inversen Matrix** an die Hand: Wird nämlich A durch eine Abfolge elementarer Zeilenoperationen (die $E_1, E_2, \ldots, E_s$ entsprechen) in $\mathbb{I}_n$ überführt, so überführt dieselbe Abfolge von Operationen auch $\mathbb{I}_n$ in A^{-1}. Man kann also zwei analoge Rechnungen nebeneinander durchführen. Wenn man dabei einerseits mit dem Gauß-Verfahren von A aus zu $\mathbb{I}_n$ gelangt ist, hat man andererseits von $\mathbb{I}_n$ aus A^{-1} erreicht. Ein Beispiel hierzu ist Thema der Übungen. Bei größeren Matrizen erfordert dieses Vorgehen aber einigen Aufwand und ist nicht unbedingt günstiger als die Berechnung von A^{-1} über die Formel mit der Adjunkten.

Die vorige Aussage kann auch so formuliert werden, dass es für invertierbares $A \in K^{n\times n}$ ein $s \in \mathbb{N}_0$ und Elementarmatrizen $\widetilde{E}_1, \widetilde{E}_2, \ldots, \widetilde{E}_s \in K^{n\times n}$ mit $A = \widetilde{E}_s\cdot\ldots\cdot\widetilde{E}_2\widetilde{E}_1$ gibt. (In der zuvor verwendeten Notation ist einfach $\widetilde{E}_\ell = E_\ell^{-1}$ für $\ell \in \{1, 2, \ldots, s\}$.)

Wir beschließen dieses Kapitel und die Vorlesung Mathematik 2 jetzt mit drei weiteren Sätzen, die jeweils eine schon in Abschnitt 6.3 aufgestellte, aber bisher noch nicht bewiesene Behauptung abhandeln.

Satz (Produktformel für Determinanten). *Seien K ein Körper und $n \in \mathbb{N}$. Für quadratische Matrizen $A, B \in K^{n\times n}$ gilt stets*

$$\boxed{\det(AB) = (\det A)(\det B)}\,.$$

Beweis. Ist A *nicht* invertierbar, so gilt $\det A = 0$ nach[7] einem Satz des Abschnitts 6.3. Zudem ist dann auch $\det(AB) = 0$ (zum Beispiel, weil $\operatorname{Bild} A \subsetneqq K^n$ und wegen $\operatorname{Bild}(AB) \subset \operatorname{Bild} A$ dann auch $\operatorname{Bild}(AB) \subsetneqq K^n$ gelten). Somit ist $\det(AB) = (\det A)(\det B)$ in diesem Fall erfüllt.

Um invertierbare A zu behandeln, betrachten wir zunächst den Fall einer Elementarmatrix A und eines beliebigen $B = (b_{j,\ell})_{j,\ell=1,2,\ldots,n}$. Ist die Elementarmatrix A vom ersten Typ mit $\det A = \lambda$, so erhalten wir mit der Leibniz-Formel

$$\det(AB) = \sum_{\pi\in \mathrm{S}_n} \operatorname{sgn}(\pi)\lambda b_{i,\pi(i)} \prod_{\substack{j=1\\ j\neq i}}^{n} b_{j,\pi(j)} = \lambda(\det B) = (\det A)(\det B)\,.$$

Ist die Elementarmatrix A vom zweiten Typ mit $\det A = 1$, so erhalten wir

$$\det(AB) = \sum_{\pi\in \mathrm{S}_n} \operatorname{sgn}(\pi)(b_{i,\pi(i)}+\lambda b_{k,\pi(i)}) \prod_{\substack{j=1\\ j\neq i}}^{n} b_{j,\pi(j)} = \det B + \lambda \det B_{i\leftarrow k} = (\det A)(\det B)\,,$$

wobei $B_{i\leftarrow k}$ die beim Beweis des Invertierbarkeitssatzes in Abschnitt 6.3 schon betrachtete Matrix mit zwei gleichen Zeilen bezeichnet und, wie dort gezeigt, $\det B_{i\leftarrow k} = 0$ gilt. Ist schließlich

[7] Für *eine* Implikation des früheren Satzes hatten wir tatsächlich die hier noch zu beweisende Produktformel bereits verwendet. Dennoch kommt kein unzulässiger Zirkelschluss zustande, denn wir benutzen hier nur die *andere* Implikation des früheren Satzes, deren Beweis nicht an der Produktformel hing.

$A = \mathrm{E}_\tau$ mit Transposition $\tau \in \mathrm{S}_n$ eine Elementarmatrix vom dritten Typ mit $\det A = -1$, so bekommen wir

$$\begin{aligned}\det(AB) &= \sum_{\pi\in\mathrm{S}_n} \operatorname{sgn}(\pi) b_{k,\pi(i)} b_{i,\pi(k)} \prod_{\substack{j=1\\ i\neq j\neq k}}^{n} b_{j,\pi(j)} \\ &= -\sum_{\pi\in\mathrm{S}_n} \operatorname{sgn}(\pi\circ\tau) \prod_{j=1}^{n} b_{j,\pi\circ\tau(j)} = -\det B = (\det A)(\det B)\,.\end{aligned}$$

Nachdem die Behauptung somit für eine beliebige einzelne Elementarmatrix A gezeigt ist, erhalten wir sie durch vollständige Induktion nach s auch für jede Matrix A, die ein Produkt von $s \in \mathbb{N}_0$ Elementarmatrizen ist. Gemäß der vorausgehenden Bemerkung (4) werden hierdurch alle invertierbaren Matrizen A erfasst, und der Beweis ist komplett. □

Satz („Zeilenrang gleich Spaltenrang“). *Seien K ein Körper und $m, n \in \mathbb{N}$. Für $A \in K^{m\times n}$ gilt stets*

$$\operatorname{Rang}\bigl(A^{\mathrm{T}}\bigr) = \operatorname{Rang} A\,.$$

Beweis. Wie schon bemerkt, verändert sich $\operatorname{Kern} A = \{x \in K^n \mid Ax = 0\}$ durch Anwendung von elementaren Zeilenoperationen auf $A \in K^{m\times n}$ nicht. Analog zu Zeilenoperationen werden elementare Spaltenoperationen mit $A \in K^{m\times n}$ erklärt, und diese lassen tatsächlich $\operatorname{Bild} A = \operatorname{Span}\{Ae_1, Ae_2, \ldots, Ae_n\}$ unverändert. Insgesamt können wir somit festhalten, dass $\operatorname{Rang} A = \dim(\operatorname{Bild} A) = n - \dim(\operatorname{Kern} A)$ *weder* durch elementare Zeilenoperationen *noch* durch elementare Spaltenoperationen mit A verändert wird. Wir können die gegebene Matrix $A \in K^{m\times n}$ nun gemäß dem letzten Satz durch endlich viele elementare Zeilenoperationen auf Zeilenstufenform mit $k := \operatorname{Rang} A$ nicht-trivialen Zeilen bringen, und mit einer Variante des Gauß-Algorithmus können wir von der Zeilenstufenform dann durch endlich viele elementare Spaltenoperationen zur speziellen Form

$$\mathbb{I}_{k,m\times n} := \left(\begin{array}{c|c} \mathbb{I}_k & 0 \\ \hline 0 & 0 \end{array}\right) \in K^{m\times n}$$

(mit der $(k\times k)$-Einheitsmatrix $\mathbb{I}_k$ und drei Null-Blöcken der Formate $k\times(n-k)$, $(m-k)\times k$ und $(m-k)\times(n-k)$) übergehen. Da elementare Zeilenoperationen Links-Multiplikationen mit Elementarmatrizen und elementare Spaltenoperationen Rechts-Multiplikationen mit Elementarmatrizen (genau gleiche Typen erlaubt) entsprechen, bedeutet dies mit anderen Worten

$$ZAS = \mathbb{I}_{k,m\times n}\,,$$

wobei $Z \in K^{m\times m}$ und $S \in K^{n\times n}$ jeweils Produkte endlich vieler Elementarmatrizen sind. Durch Transponieren folgt

$$S^{\mathrm{T}} A^{\mathrm{T}} Z^{\mathrm{T}} = \mathbb{I}_{k,m\times n}^{\mathrm{T}} = \mathbb{I}_{k,n\times m}\,,$$

wobei auch $S^{\mathrm{T}} \in K^{n\times n}$ und $Z^{\mathrm{T}} \in K^{m\times m}$ Produkte endlich vieler Elementarmatrizen sind. Da die zugehörigen Operationen den Rang nicht verändern, lesen wir ab, dass $\operatorname{Rang}\bigl(A^{\mathrm{T}}\bigr)$ mit $\operatorname{Rang}\mathbb{I}_{k,n\times m} = k = \operatorname{Rang} A$ übereinstimmt. □

Satz (über **geometrische und algebraische Vielfachheit von Eigenwerten**). *Seien K ein Körper und $n \in \mathbb{N}$. Für eine quadratische Matrix $A \in K^{n\times n}$ und einen Eigenwert $\lambda \in K$ von A ist die geometrische Vielfachheit des Eigenwerts λ stets kleiner oder gleich der algebraischen Vielfachheit von λ, das heißt, ist $(\mathrm{X}-\lambda)^\ell$ der Teiler von $\mathrm{Ch}(A)$ mit maximalem $\ell \in \mathbb{N}$ (also $\mathrm{Ch}(A) = (\mathrm{X}-\lambda)^\ell p$ für ein $p \in K[\mathrm{X}]$, das λ* nicht *mehr als Nullstelle hat), so gilt*

$$\dim \mathrm{E}_\lambda(A) \leq \ell\,.$$

Beweis. Sei $k := \dim \mathrm{E}_\lambda(A) = \dim(\mathrm{Kern}(\lambda\mathbb{I}_n - A))$ die geometrische Vielfachheit des Eigenwerts λ. Dann ist nach der Dimensionsformel $\mathrm{Rang}(\lambda\mathbb{I}_n - A) = n-k$. Durch elementare Zeilenoperation beziehungsweise Linksmultiplikation mit Elementarmatrizen kann $\lambda\mathbb{I}_n - A$ auf Zeilenstufenform mit $n-k$ nicht-trivialen Zeilen gebracht werden. Insbesondere können wir

$$Z(\lambda\mathbb{I}_n - A) = \left(\frac{B}{0}\right) \in K^{n\times n}$$

mit einem Produkt $Z \in K^{n\times n}$ endlich vieler Elementarmatrizen, einem beliebigen $(n-k)$-zeiligen Block $B \in K^{(n-k)\times n}$ und k Nullzeilen erreichen. Hieraus bekommen wir

$$\mathrm{X}\mathbb{I}_n - A = Z^{-1}[Z(\mathrm{X}-\lambda) + Z(\lambda\mathbb{I}_n - A)] = Z^{-1}\left[(\mathrm{X}-\lambda)Z + \left(\frac{B}{0}\right)\right] = Z^{-1}\left(\frac{(\mathrm{X}-\lambda)Z' + B}{(\mathrm{X}-\lambda)Z''}\right)$$

mit der Zerlegung $Z = \left(\frac{Z'}{Z''}\right)$ von Z in die ersten $n-k$ Zeilen Z' und die letzten k Zeilen Z''. Mit der Produktformel für die Determinante folgt

$$\mathrm{Ch}(A) = \det(\mathrm{X}\mathbb{I}_n - A) = \det\bigl(Z^{-1}\bigr)\det\left(\frac{(\mathrm{X}-\lambda)Z' + B}{(\mathrm{X}-\lambda)Z''}\right)$$

mit $\det\bigl(Z^{-1}\bigr) \neq 0$. Entscheidend ist nun, dass in der Leibniz-Formel für die Determinante rechts jeder Summand mindestens den Faktor $(\mathrm{X}-\lambda)^k$ beinhaltet, weil für jeden Summand der Leibniz-Formel Einträge aus allen Zeilen multipliziert werden und alle Einträge der letzten k Zeilen $(\mathrm{X}-\lambda)Z''$ einen Faktor $\mathrm{X}-\lambda$ beinhalten. (Was in den ersten $n-k$ Zeilen steht, ist für dieses Argument völlig egal.) Insgesamt kann also $(\mathrm{X}-\lambda)^k$ aus $\mathrm{Ch}(A) \in K[\mathrm{X}]$ ausgeklammert werden, und die algebraische Vielfachheit ℓ von λ erfüllt zwingend $\ell \geq k = \dim \mathrm{E}_\lambda(A)$. □

Literaturverzeichnis

Die Themen der Vorlesung werden in einer Vielzahl von Büchern behandelt, von denen hier einige aufgelistet werden. Abgesehen von [2, 5, 12, 6] und den fachdidaktischen Büchern [10, 11] 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] H.-D. Ebbinghaus, H. Hermes, F. Hirzebruch, M. Koecher, K. Lamotke, K. Mainzer, J. Neukirch, A. Prestel, R. Remmert: *Zahlen.* Springer, 1992.

[7] G. Fischer: *Lernbuch Lineare Algebra und Analytische Geometrie.* Springer, 2019.

[8] G. Fischer, B. Springborn: *Lineare Algebra.* Springer, 2020.

[9] O. Forster: *Analysis 1.* Springer, 2015.

[10] G. Greefrath, R. Oldenburg, H.-S. Siller, V. Ulm, H.-G. Weigand: *Didaktik der Analysis.* Springer, 2016.

[11] H.-W. Henn, A. Filler: *Didaktik der Analytischen Geometrie und Linearen Algebra.* Springer, 2015.

[12] P.R. Halmos: *Naive Set Theory.* Springer, 1974.

[13] H. Heuser: *Lehrbuch der Analysis. Teil 1.* Vieweg+Teubner, 2009.

[14] S. Hildebrandt: *Analysis 1.* Springer, 2006.

[15] K. Jänich: *Lineare Algebra.* Springer, 2008.

[16] K. Königsberger: *Analysis 1.* Springer, 2004.

[17] C. Schweigert: *Lineare Algebra.* Vorlesungsskript, Studienjahr 2018/19, Hamburg.

[18] W. Walter: *Analysis 1.* Springer, 2009.