Château de mathématiques

Mathematisches Schloss

Dr. Harald Scherer
Harald@nihilsinecausa.de
www.nihilsinecausa.de

23. August 2020

Inhaltsverzeichnis

1 Einleitung

1.1 Zur Zielsetzung — Mathematik als Dienerin der Physik?

Grundmotiv für die Beschäftigung mit Mathematik ist für mich das Interesse an Physik und am Naturverständnis. Die Mathematik stellt das formale Rückgrat der Physik dar. In dieser Funktion sollte die Mathematik eigentlich Dienerin sein für die Physik. Ich wollte die Mathematik daher auf ihre Rolle reduzieren, die formale Sprache der Physik bereitzustellen und ich wollte die hierzu notwendigen mathematischen Aussagen eigentlich so knapp wie möglich darstellen.

Dieser Versuch ist gescheitert. Je länger ich mich mit Mathematik beschäftige, umso mehr Eigendynamik entwickelt sie in meinem Kopf. Das Verführerische an mathematischen Aussagen ist einerseits, dass es sich um ewige Wahrheiten handelt. Man kann sie elegant formulieren und wunderschön finden. Gerade weil diese Aussagen immer wahr sind, handelt es sich andererseits um bloße Tautologien. Formal sind sie äquivalent zu A oder nicht A. Worin liegt also der Erkenntnisgewinn durch die Mathematik? Offenbar ist die Mathematik eine Beschäftigung des Verstandes mit sich selbst und hat mit der Welt da draußen wenig zu tun, schon gar nicht mit dem Leben.

Das, wovon die Mathematik ausgeht, sind willkürlich erscheinende Setzungen. Je nachdem, welche dieser Setzungen man als gültig annimmt, kann man z.B. euklidische oder nicht euklidische Geometrie betreiben. Was ist nun wahr? Innermathematisch ist diese Frage sinnlos. Beides ist wahr - jede Theorie ist in ihrem eigenen System tautologisch. Und was ist in der Welt? Was davon ist wirklich? Ist die Geometrie der Welt euklidisch oder nicht euklidisch? Wie immer die Antwort lautet, durch die Mathematik allein sind solche Fragen nicht beantwortbar.

Und dennoch scheint es auch innerhalb der Mathematik Grundsätze zu geben, die so etwas wie Glaubensgrundsätze darstellen. Etwas, worauf sich die meisten Mathematiker geeinigt zu haben scheinen. Wie z.B. das „tertium non datur“ in der klassischen Logik: Eine Aussage ist wahr oder falsch, ein Drittes ist nicht gegeben. Dieser Grundsatz und viele ähnliche sind in einem weiten Bereich der Mathematik als gültig akzeptiert. [Wer das „tertium non datur“ nicht akzeptieren möchte, muss sich mit ziemlich exotischen Theorien, wie etwa mit intuistionistischer Mathematik beschäftigen.]

Auf die Frage nach ihren mathematischen Glaubensgrundsätzen werden die meisten Mathematiker mit einem Achselzucken reagieren. Denn solange man

die Mathematik als reines Gedankenspiel betrachtet, ist es gleichgültig, welche Grundsätze „wirklich und wahrhaftig" sind und welche nicht. Das aber ändert sich in dem Augenblick, in dem eine mathematische Theorie zum Bestandteil einer physikalischen Theorie wird, wie z.B. die mathematische Theorie der Analysis im $\mathbb{R}^n$ als Fundament der klassischen Mechanik. Jetzt gelten alle mathematischen Aussagen über den $\mathbb{R}^n$ als „physikalisch wahr", sei es in direkter oder indirekter Form. Und alle vorher vermeintlich austauschbaren Glaubensgrundsätze der Mathematiker sowie alle axiomatischen Grundannahmen werden zu festen Setzungen für die Naturbeschreibung durch die Physik.

So what? Was ist daran schlimm? Nun, es dreht den Spieß um. Aus der Mathematik als Dienerin ist eine Domina geworden, die der Physik vorschreibt, wie die Natur zu beschreiben ist. Moment mal, wird man hier vielleicht einwenden, die Physik ist doch eine empirische Wissenschaft und wird nur Aussagen zu treffen versuchen, die empirisch begründet werden können. Richtig, aber das Problem ist, dass die empirische Methode so ihre Grenzen hat. Insbesondere kann man die Gültigkeit der mathematischen Lehrsätze nur in Ausnahmefällen empirisch untermauern. Um bei dem Beispiel mit dem $\mathbb{R}^n$ zu bleiben: Alle Messergebnisse in der Physik bestehen, aufgrund der endlichen Messgenauigkeit, aus endlichen Dezimalbrüchen. Es würde also der $\mathbb{Q}^n$ oder sogar eine diskretisierte Variante davon ausreichen, um die Ergebnisse aller physikalischen Experimente darzustellen und Eigenschaften des $\mathbb{R}^n$, die über einen diskretisierten $\mathbb{Q}^n$ hinausgehen, können nicht so einfach empirisch begründet werden.

Aus diesem Dilemma gibt es keinen Ausweg und wir müssen das Wechselspiel zwischen Mathematik und Physik akzeptieren. Insbesondere muss ich einer physikalischen Theorie die jeweilige mathematische Theorie als gültig zugrunde legen. Nur möchte ich hierüber im Vorfeld soviel Klarheit wie möglich bekommen, welche mathematischen Glaubensgrundsätze ich mir dabei einhandele. Im Text versuche das mit der Hervorhebung von Paradigmen, die aus meiner Sicht der jeweiligen mathematischen Theorie zugrunde liegen.

Noch ein Hinweis in eigener Sache: Ich bin kein Mathematiker. Vieles von dem, was ich hier schreibe, enthält Fehler. Manche Fehler finde ich mit der Zeit und korrigiere sie, andere nicht. Man möge also keine meiner Aussagen glauben, sondern kritisch nachdenken und/oder in der Literatur nachschlagen. Hier bietet die Mathematik — im Vergleich zu vielen anderen Wissenschaften — den unschlagbaren Vorteil, dass man die sicherste Erkenntnisquelle jederzeit parat hat: den eigenen Verstand!

1.2 Zur Gliederung des Textes

1.2.1 Heuristischer Zirkel bei der Darstellung der Mathematik

In nahezu jedem Lehrbuch wird der Aufbau der Mathematik unterschiedlich dargestellt. Dabei setzt der jeweilige Autor unterschiedliche mathematische (Grund-)Kenntnisse bei seinen Lesern voraus. Das führt häufig zu zirkulären Situationen. Wenn etwa in einem späteren Kapitel die natürlichen Zahlen mit Hilfe der Peano-Axiome eingeführt werden, so waren sie in vorangegangenen Kapiteln schon entsprechend präsent.

Es ist ein alter Traum von mir, mir die Mathematik so systematisch darzustellen, dass alles aufeinander aufbaut und dass nichts als bekannt vorausgesetzt werden muss, was erst auf einer höheren Stufe mathematisch sauber dargestellt werden kann. Hier stoße ich an meine persönlichen Grenzen. Ein wirklich sauber durchformalisierter Zugang zur Mathematik übersteigt meine mathematischen Fähigkeiten und ein solcher Zugang würde vermutlich so überfrachtet von Formalismen sein, dass der Text unlesbar würde. Manchmal beschleicht mich sogar der Verdacht, dass die Struktur der Mathematik zirkulär ist. So etwa wenn beim Aufbau der mathematischen Logik „ganz normale" Beweise geführt werden, die die formale Logik voraussetzen. Wenn wir „Glück" haben ist der Zirkel nicht „bösartig" sondern lediglich hermeneutischer Natur. Aber hier bin ich im Ungewissen und muss noch viel lernen, um den Aufbau der Mathematik wirklich zu verstehen.

Das führt uns zu der Frage nach dem mathematischen Niveau und dem Abstraktionsgrad des vorliegenden Textes. Ich versuche die mathematischen Sachverhalte so darzustellen, wie ich es als (theoretischer) Physiker gewohnt bin und so wie ich persönlich es elegant finde. Das aber hat alles andere als einen Absolutheitsanspruch. Schließlich gibt es ja so fürchterlich viele Monographien und Lehrbücher in der Mathematik, die alle einen leicht unterschiedlichen Abstraktionsgrad bieten. Vielleicht gilt ja auch in der Mathematik der Grundsatz: „Der Weg ist das Ziel"?

Nun interessieren mich — wie in Abschnitt 1.1 ausgeführt — vor allem offensichtliche und versteckte Prämissen, die in die jeweilige mathematische Theorie eingehen. Daher will ich versuchen, bei dem hier gewählten Aufbau so wenig wie möglich vorauszusetzen, was ich später präziser fassen kann. Dabei müsste ich über mehr oder weniger versteckte Prämissen stolpern, vielleicht sogar über einen Zirkel. Und natürlich will ich versuchen, die so gefundenen Prämissen aufzuschreiben, wo immer sie mir auffallen. Wohin mich das führt, weiß ich erst, wenn der Text weiter entwickelt ist. Im derzeitigen Stadium ist es ein Experiment mit ungewissem Ausgang. Zumindest fühlt sich

für mich dieses Vorgehen so als richtig an und ich habe es mir in meinem persönlichen hermeneutischen Zirkel bequem gemacht.

1.2.2 Farbgebung

Wie in jeder mathematischen Darstellung braucht es auch bei unserem Vorhaben Definitionen, Sätze, Beweise, Beispiele, Erläuterungen etc. Ich habe mir angewöhnt, dabei mit verschiedenen Farben zu arbeiten.

Definitionen sind in gelber Farbe gesetzt. Das Gelb erscheint etwas dunkel, weil es sonst auf hellem Hintergrund nicht so gut lesbar wäre.

Theoreme, Sätze, Lemmata, Korollare, etc. tragen die Farbe Blau.

Beweise sind in schwarzer Schrift gesetzt und treten mit etwas verkleinertem Font vornehm in den Hintergrund.

Beispiele erscheinen in grüner Farbe (quasi eine Mischung aus Gelb und Blau = eine Mischung aus Definitionen und Sätzen)

Zusammenfassungen und **Paradigmen** sind in roter Schrift gesetzt.

AXIOME schließlich erscheinen ebenfalls in roter Schrift aber zur besonderen Hervorhebung durchgängig in halbfett.

Allgemeine Einführungen und Erläuterungen erscheinen in schwarzer Normalschrift.

Persönliche Hinweise schreibe ich in kursiv und schwarz.

*Schließlich gibt es noch Hinweise vom **Schlossführer** (er wird im nächsten Abschnitt vorgestellt), diese sind in kursiv und grau gesetzt.*

1.2.3 Das mathematische Schloss

Ich stelle mir die Mathematik seit jeher als ein Gebäude vor. Darin gibt es größere Segmente wie Stockwerke, Flügel, Zentralbereiche aber auch einzelne Zimmer, in denen die jeweiligen Disziplinen und Teildisziplinen der Mathematik untergebracht sind. Die Struktur des Gebäudes ändert sich von Zeit zu Zeit ganz subjektiv, je nachdem mit welchen mathematischen Gebieten ich mich näher befasse und mit welchen nicht.

Das Gebäude ist in sich äußerst stabil. Das liegt in der Natur der Mathematik und eben in ihrer Unumstößlichkeit. Aber das Gebäude ist andererseits aber nicht aus einem festen, irdischen Material. Es bleibt für mich so etwas wie ein Luftschloss, das ständig sich ändert, erweitert und umstrukturiert.

Besonders spannend finde ich es, wenn an den Fundamenten gearbeitet wird (mathematische Logik, Mengenlehre, Metamathematik) und sich dadurch die Struktur des gesamten Gebäudes schlagartig ändern kann.

Indem ich diesen Text schreibe, weiß ich selbst nicht, wie das Schloss am Ende aussehen wird. Auch das ist ein Experiment.

Ich übergebe nun an den Schlossführer, der sich von Zeit zu Zeit zu Wort melden wird. Er erläutert die Struktur des Schlosses, beschreibt die Ausgestaltung der Räume und gibt Hintergrundinformationen aller Art.

Visite guidée: *Die Schlossanlage ist zweigeteilt. Es gibt einen Schlosshof und das eigentliche Schloss. Die verschiedenen mathematischen Disziplinen sind in unterschiedlichen Gebäudeteilen untergebracht, wie sich der folgenden Übersicht entnehmen lässt. Darüber hinaus gibt es ganz hinten am Ende des Schlossparks noch eine Baracke.*

Cour du Château — Schlosshof

Elementare Logik
Konzept der Gleichheit
Elementare Mengenlehre

Salle de Réception — Eingangshalle

Grundlegende Strukturelemente wie: Relationen, Abbildungen, Gruppen, Ringe, Körper, Zahlenmengen
Zugang zu Hilberts Hotel mit Ausblick auf unendliche Mengen

Bel étage — 1. Obergeschoss

Analysis
Lineare Algebra

Toit terrasse — Dachterrasse

. . . mit Wintergärten und einem kleinen Park
Funktionalanalysis
Hilbertraumtheorie

Atelier

Algebra
Zahlentheorie

Loft

Topologie

Souterrain — Keller

. . . mit Grotten und Katakomben
Metamathematik

Mathematische Logik
Axiomatische Megenlehre

Cabane en rondin „Baraque“ — Blockhütte
Intuitionistische Mathematik
Konstruktivismus

2 Cour du Château — Schlosshof

2.1 Elementare Logik

Visite guidée: *Auf dem Schlosshof findet man diejenigen Grundlagen, die man braucht, um überhaupt ins Schloss zu gelangen. In den Boden des Schlosshofs sind Figuren und Tabellen zur elementaren Logik eingelassen. Kleine lachende Figuren stehen für „wahr", böse dreinschauende Teufelfiguren stehen für „falsch". Besucher dürfen diese Figuren anfassen und damit die Aufgaben lösen, die in dem Parcours verteilt sind.*

2.1.1 Aussagen und Junktoren

Definition 2.1. (Aussage): Unter einer **Aussage** wird ein Satz verstanden, von dem sinnvoll angenommen werden kann, dass er wahr oder falsch ist. Vgl. Hilbert-Ackermann [4], S. 3.

Beispiel: Beispiele für Aussagen im Sinne von Definition 2.1:

- „$7 + 5 = 12$", Wahrheitswert: wahr
- „Der Mond ist aus grünem Käse." Wahrheitswert: falsch
- „Jede gerade Zahl, die größer ist als zwei, ist die Summe zweier Primzahlen." Wahrheitswert: unbekannt, Goldbachsche Vermutung

Wir unterstellen Aussagen, dass sie prinzipiell keinen anderen Wahrheitswert besitzen können als „wahr" oder „falsch". Ein drittes ist nicht geben — tertium non datur. Um den Wahrheitswert festzustellen, müsste man den Inhalt der Aussage objektiv prüfen. Am Beispiel der Goldbachschen Vermutung sehen wir, dass wir hier an fundamentale Grenzen stoßen können. Dennoch gilt die Goldbachsche Vermutung gemeinhin als Aussage.

Paradigma 2.1. (tertium non datur): Eine Aussage der klassischen Aussagenlogik ist wahr oder falsch, eine andere Option ist nicht zugelassen.

Aussagen lassen sich durch Junktoren zu neuen Aussagen zusammensetzen. Es handelt sich hierbei um einen rein formalen Vorgang, völlig unabhängig von der inneren Struktur und dem Inhalt der Aussagen.

Definition 2.2. (Aussagenlogische Junktoren): Seien A, B Aussagen.

1. Die **Negation** $\neg A$ (in Worten „nicht A") ist das kontradiktorische Gegenteil von A, genauer: Wenn A wahr ist, ist $\neg A$ falsch und wenn A falsch ist, ist $\neg A$ wahr.

2. Die **Konjunktion** $A \wedge B$ (in Worten „A und B“) ist wahr, wenn A wahr ist und B wahr ist und sie ist falsch, wenn mindestens eine der beiden Aussagen A oder B falsch ist.

3. Die **Disjunktion** $A \vee B$ (in Worten „A oder B“) ist wahr, wenn mindestens eine der Aussagen A oder B wahr ist und sie ist falsch, wenn beide Aussagen A und B falsch sind.

4. Die **Implikation** $A \Rightarrow B$ (in Worten „A impliziert B“) besitzt dieselben Wahrheitswerte wie die zusammengesetzte Aussage $\neg A \vee B$, d.h. sie ist wahr, wenn A falsch ist oder wenn B wahr ist, und sie ist falsch, wenn A wahr ist und B falsch ist.

5. Die **Äquivalenz** $A \Leftrightarrow B$ (in Worten „A äquivalent B“) ist wahr, wenn A und B beide wahr sind oder beide falsch sind, und sie ist falsch wenn A wahr und B falsch oder wenn A falsch und B wahr ist.

Die verschiedenen Wahrheitswerte lassen sich durch Wahrheitswertetafeln anschaulich darstellen.

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$\neg A \vee B$	$A \Leftrightarrow B$
w	w	f	w	w	w	w	w
w	f	f	f	w	f	f	f
f	w	w	f	w	w	w	f
f	f	w	f	f	w	w	w

Durch die Verknüpfung zweier Aussagen über Junktoren entsteht eine neue Aussage. Entgegen der intuitiven Vorstellung müssen die verknüpften Aussagen inhaltlich nichts miteinander zu tun haben. Besonders deutlich wird das bei der Implikation. Nehmen wir ein Beispiel für zwei Aussagen. A : *„Der Mond ist aus grünem Käse.“ und* B : „$7+5 = 13$“ *Da* A *falsch ist, ist* $A \Rightarrow B$ *per definitionem wahr, ungeachtet der Tatsache, dass die Beschaffenheit des Mondes inhaltlich keinen Einfluss auf die Berechnung* $7 + 5 =?$ *haben dürfte. Die Eigenschaft einer für wahr bewerteten Implikation, dass eine falsche Aussage sowohl eine falsche als auch eine wahre Aussage implizieren darf, ist wiederum ein wichtiges Paradigma, das die geheimnisvolle lateinische Bezeichnung „ex falso quodlibet“ bekommen hat.*

Noch merkwürdiger wird die Sache, wenn wir eine wahre Aussage z.B. C : *„Der Mond ist nicht aus grünem Käse.“ zugrunde legen. Dann hängt die Wahrheit oder Falschheit der Implikation* $C \Rightarrow D$ *nur davon ab, ob* D *wahr oder falsch ist. Also im Klartext etwa: „Wenn der Mond nicht aus grünem Käse ist, dann ist* $7 + 5 = 12$“, *ist eine wahre Aussage.*

Die Implikation ist also wenig intuitiv. Jedoch stimmt die folgende Eigen-

schaft, die wir auch von inhaltlichen „wenn ... dann“ Aussagen kennen, mit der Eigenschaft der Implikation überein: Es darf nicht sein, dass der Vordersatz A wahr ist und Nachsatz B falsch. In diesem Fall (und bemerkenswerterweise nur in diesem Fall) ist $A \Rightarrow B$ falsch.

Paradigma 2.2. (ex falso quodlibet): Eine Implikation $A \Rightarrow B$ ist immer wahr, wenn A falsch ist; ex falso quodlibet.

Beim Zusammensetzen von Aussagen durch Junktoren kann es zu beliebig komplexen neuen Aussagen kommen. Um dies eindeutig zu machen, muss man im allgemeinen Klammern verwenden. Um Klammern zu sparen, vereinbaren wir:

Definition 2.3. (Bindungsstärke von Junktoren):
Die Bindungsstärke der folgenden Junktoren ist von links nach rechts abnehmend [links $\widehat{=}$ stark bindend ... rechts $\widehat{=}$ schwach bindend]:

$$\neg \quad \wedge \quad \vee \quad \Rightarrow \quad \Leftrightarrow,$$

also ist insbesondere „und“ stärker als „oder“.
Vgl. Deiser Grundbegriffe [3]. S. 20.

2.1.2 Tautologien

Definition 2.4. (Tautologie): Sei A eine (zusammengesetzte) Aussage. A wird **allgemeingültig** oder **Tautologie** genannt, wenn sie stets wahr ist. D.h. in der Wahrheitstafel müssen alle Zeilen von A mit „w“ belegt sein.
Vgl. Deiser Grundbegriffe [3]. S. 25.

Beispiel: Sei A eine Aussage. Dann ist $A \Rightarrow A$ eine Tautologie:

A	$A \Rightarrow A$
w	w
w	w

Satz 2.1. (Wichtige Tautologien): Seien A, B, C Aussagen. Dann sind folgende Aussagen Tautologien:

$A \vee \neg A$	tertium non datur
$A \Rightarrow B \;\Leftrightarrow\; \neg B \Rightarrow \neg A$	Kontrapositionsgesetz
$\neg B \Rightarrow (C \wedge \neg C) \Leftrightarrow B$	Prinzip des Widerspruchsbeweises
$A \wedge (A \Rightarrow B) \;\Rightarrow\; B$	modus ponens
$\neg B \wedge (A \Rightarrow B) \;\Rightarrow\; \neg A$	modus tollens
$A \;\Leftrightarrow\; (B \Rightarrow A) \wedge (\neg B \Rightarrow A)$	Fallunterscheidung
$\neg(A \wedge B) \;\Leftrightarrow\; \neg A \vee \neg B$	de Morgansches Gesetz
$\neg(A \vee B) \;\Leftrightarrow\; \neg A \wedge \neg B$	de Morgansches Gesetz
$A \vee (B \wedge C) \;\Leftrightarrow\; (A \vee B) \wedge (A \vee C)$	Distributivgesetz
$A \wedge (B \vee C) \;\Leftrightarrow\; (A \wedge B) \vee (A \wedge C)$	Distributivgesetz

Vgl. Deiser Grundbegriffe [3]. S. 33f.

Beweis: Von der Gültigkeit der Tautologien überzeugt man sich leicht via Wahrheitstafel. Hier nur ein Beispiel für die Fallunterscheidung:

A	B	$(B \Rightarrow A)$	$(\neg B \Rightarrow A)$	$(B \Rightarrow A) \wedge (\neg B \Rightarrow A)$	$A \;\Leftrightarrow\; (B \Rightarrow A) \wedge (\neg B \Rightarrow A)$
w	w	w	w	w	w
w	f	w	w	w	w
f	w	f	w	f	w
f	f	w	f	f	w

□

Tautologien sind also immer wahr. Das könnte man für langweilig halten, aber Vorsicht: die Mathematik steckt voller Tautologien. Skizzieren wir ein simples Modell eines mathematischen Satzes innerhalb einer mathematischen Theorie. Hierzu brauchen wir Axiome $A_1, \ldots, A_n$ und Definitionen $D_1, \ldots, D_m$. Dann brauchen wir noch die Prämisse A für unseren Satz und die Folgerung B. Der mathematische Satz hat typischerweise die Form $A \Rightarrow B$. Wenn wir das ausführlicher schreiben, ergibt sich folgende Tautologie:

$$A_1 \wedge \ldots \wedge A_n \;\wedge\; D_1 \wedge \ldots \wedge D_m \;\wedge\; A \;\Longrightarrow\; B$$

Paradigma 2.3. (Tautologisches): Mathematische Sätze sind Tautologien.

2.1.3 Beweisverfahren

Satz 2.2. (Direkter Beweis): Seien A und B Aussagen und sei A wahr. Gelingt es zu zeigen, dass dann auch B wahr ist, so ist $A \Rightarrow B$ wahr.

Beweis: Schauen wir uns die Wahrheitstafel von $A \Rightarrow B$ an

	A	B	$A \Rightarrow B$
1	w	w	w
2	w	f	f
3	f	w	w
4	f	f	w

und betrachten wir die einzelnen Zeilen. Die Annahme ist, dass A wahr und daraus folgte, dass B wahr ist. Zeile 1 ist also wahr. Dass B nicht falsch ist, wurde in dem direkten Beweis auch gezeigt (tertium non datur vorausgesetzt). Also ist der in Zeile 2 dargestellte Fall nicht eingetreten. In Bezug auf den in Zeile 2 dargestellten Fall ist $A \Rightarrow B$ also korrekterweise falsch. Zeile 3 und Zeile 4 betrachten wir beim direkten Beweis nicht. Aber angenommen, A ist falsch, dann ist es gleichgültig ob B wahr oder falsch ist, die Implikation $A \Rightarrow B$ gilt als wahr, so war sie gerade konstruiert. □

Ich stolpere immer wieder darüber, dass bei einem direkten Beweis $A \Rightarrow B$ bewiesen sein soll, obwohl die Zeilen 3 und 4 gar nicht untersucht wurden. Man beachte, dass die Aussage $A \Rightarrow B$ in den Zeilen 1 und 2 dieselben Wahrheitswerte hat, wie die Aussage $A \wedge B$. Ist A falsch, so ist $A \wedge B$ falsch. Warum also können wir uns sicher sein, dass wir beim direkten Beweis keine Konjunktion vor uns haben?

Die Antwort ist: Weil wir das so definiert haben. Die Zeilen 3 und 4 interessieren uns nicht. Ist A falsch, so ist $A \Rightarrow B$ wahr und zwar per definitionem. $A \wedge B$ dagegen ist falsch in Zeile 3 und 4. Wir „setzen" damit, dass wir eine Implikation vor uns haben. Und diese Setzung entspricht genau unserem Paradigma 2.2 (ex falso quodlibet).

Satz 2.3. (Beweis durch Kontraposition): Seien A und B Aussagen und sei $\neg B$ wahr. Gelingt es zu zeigen, dass dann auch $\neg A$ wahr ist, so ist $A \Rightarrow B$ wahr.

Beweis: Ein Beweis durch Kontraposition ist ein direkter Beweis von $\neg B \Rightarrow \neg A$. Dass damit $A \Rightarrow B$ bewiesen ist, ergibt sich aus dem Kontrapositionsgesetz aus unserem Tautologie-Satz 2.1. □

Satz 2.4. (Beweis durch Widerspruch, reductio ad absurdum): Seien A und B Aussagen. Alternative Formulierungen:

1. Angenommen $A \Rightarrow B$ ist falsch. Gelingt es, daraus einen Widerspruch herzuleiten, dann ist $A \Rightarrow B$ wahr.
2. Sei A wahr. Angenommen B ist falsch. Gelingt es, daraus einen Widerspruch herzuleiten, dann ist $A \Rightarrow B$ wahr.

Beweis:

1. Die Annahme war $\neg(A \Rightarrow B)$ wäre wahr. Aufgrund des Widerspruchs folgt das Gegenteil, also ist $\neg\neg(A \Rightarrow B)$ wahr. Wegen tertium non datur folgt daraus, dass $A \Rightarrow B$ wahr ist.

2. Diese Form des Satzes lässt sich analog beweisen. $\neg B$ ist wahr. Daraus folgte ein Widerspruch*, also ist $\neg\neg B$ wahr und damit B wahr. Damit ist $A \Rightarrow B$ wahr.

*Genauer: Formalisieren wir den Widerspruch. Sei C eine beliebige Aussage. Ein Widerspruch ist eine Aussage, die immer falsch ist, also etwa $C \wedge \neg C$. Aus $\neg B$ wahr folgte der Widerspruch, also $\neg B \Rightarrow (C \wedge \neg C)$. Da die Aussage $\neg B \Rightarrow (C \wedge \neg C) \Leftrightarrow B$ eine Tautologie (vgl. Satz 2.1 ist, folgt B ist wahr. □

Definition 2.5. (Beweisschlusszeichen): Das Ende eines Beweises wird mit einem Beweisschlusszeichen angezeigt.

(a) Das Ende eines direkten Beweises sowie das Ende eines Beweises durch Kontraposition wird mit dem folgenden Schlusszeichen beendet: □
Dieses Symbol stellt eine Abkürzung dar von: „was zu beweisen war“, abgekürzt w.z.b.w. oder „quod erat demonstrandum“, abgekürzt q.e.d.

(b) Das Ende eines Beweises durch Widerspruch wird mit folgendem Schlusszeichen angezeigt: $\lightning$.
Dieses Symbol zeigt an, dass

(1) ein „Falsum“ aufgetreten ist, das ist eine Aussage, die immer falsch ist, wie etwa $C \wedge \neg C$ für eine beliebige Aussage C

(2) dass damit der Widerspruchsbeweis beendet ist im Sinne von: „was zu beweisen war“, abgekürzt w.z.b.w. oder „quod erat demonstrandum“, abgekürzt q.e.d.

Bei der hier angewandten „elementaren“ Logik abstrahieren wir von der inneren Struktur von Aussagen. Darauf basierende Beweisverfahren überprüfen insbesondere nicht, ob die Prämisse A und die Folgerung B strukturell etwas miteinander zu tun haben. Es wäre also leicht zu beweisen, dass aus „Wurzel 2 ist eine irrationale Zahl“ folgt, dass „$5 + 7 = 12$“ ist. Welche Aussagekraft hat ein so bewiesener Satz $A \Rightarrow B$? Welche Voraussetzungen müssten erfüllt sein, damit wir von „Erkenntnisgewinn“ sprechen dürfen?

Paradigma 2.4. (Abstraktionsprinzip von der inneren Struktur von Aussagen): Bei den in der „elementaren“ Logik üblichen Beweisverfahren eines mathematischen Satzes der Form $A \Rightarrow B$ wird von der strukturellen Abhängigkeit der Aussagen A und B untereinander abstrahiert.

2.1.4 Quantoren

Definition 2.6. (Variable): Eine **Variable** ist ein sprachliches Zeichen, z.B. x, für das Ausdrücke einer bestimmten Art eingesetzt werden können.
Vgl. Wikipedia Variable (Logik) [10].

Definition 2.7. (Prädikat): Sei x eine Variable. Ein **Prädikat** $A(x)$ mit einem Argument ordnet der Variablen x einen Wahrheitswert zu.
Vgl. Wikipedia Prädikat (Logik) [8]

Definition 2.8. (Quantoren): Sei x eine Variable und sei $A(x)$ ein Prädikat (eine Eigenschaft, die x zukommen kann). Dann gelten folgende Bezeichnungen:

$$\begin{array}{ll} \exists x : A(x) & \text{es existiert ein } x \text{ mit der Eigenschaft } A(x) \\ \forall x : A(x) & \text{für alle } x \text{ gilt die Eigenschaft } A(x) \end{array}$$

Die **Quantoren** $\exists$ und $\forall$ beziehen sich dabei jeweils auf einen **Grundbereich**, der diejenige Ansammlung von Ausdrücken beinhaltet, die für die verwendeten Variablen eingesetzt werden dürfen.
Vgl. Wikipedia Quantifizierung (Logik) [9]

Beispiel: „Es gibt eine Primzahl, die durch 3 teilbar ist“, lässt sich damit wie folgt durch den Quantor $\exists$ ausdrücken: Grundbereich: natürliche Zahlen. Prädikat $T_3(x)$ mit der Bedeutung „3 teilt x“

$$\exists p \text{ Primzahl} : T_3(p)$$

Satz 2.5. (Negation von Quantoren): Gegeben sei ein Grundbereich, eine Variable x aus dem Grundbereich und ein einstelliges Prädikat $A(x)$. Dann gelten folgende Verneinungsregeln

$$\begin{array}{rcl} \neg(\exists x : \ A(x)) & \Leftrightarrow & \forall x : \ \neg A(x) \\ \neg(\forall x : \ A(x)) & \Leftrightarrow & \exists x : \ \neg A(x) \end{array}$$

2.2 Das Konzept der mathematischen Gleichheit

In der Mathematik „sprechen“ wir in einer formalisierten Sprache. Worüber wir sprechen, hängt von dem jeweiligen Zusammenhang ab. Die Formelelemente, in denen wir sprechen, können Terme sein, Aussagen, arithmetische Ausdrücke und dergleichen mehr. In diesem kleinen Abschnitt sprechen wir stellvertretend von Termen.

In jedem mathematischen Zusammenhang haben wir so etwas wie eine Bewertung der betreffenden Terme. Bei Aussagen aus der Aussagenlogik besteht die Bewertung in der Zuordnung von Wahrheitswerten zu dem jeweiligen Term. In der Arithmetik sind es häufig Zahlen, die wir den Termen zuordnen können.

Definition 2.9. (Gleichheit): Seien s und t Terme. Wir sagen s und t sind **gleich**, in Zeichen $s = t$, wenn sich in allen Ausdrücken des jeweiligen mathematischen Sprachbereichs jedes Vorkommen von (s) durch den Term (t) ersetzen lässt sowie jedes Vorkommen von (t) durch den Term (s) ersetzen lässt, ohne dass sich die Bewertung der Ausdrücke durch diese Ersetzung ändert. Die in der Schreibweise (s) und (t) angedeuteten Klammern können bei der Ersetzung ggf. sofort aufgelöst werden.
Vgl. Wikipedia Gleichheit (Mathematik) [7]

Beispiel: Wenn wir in der Arithmetik sagen $7 + 5 = 12$, dann heißt das, dass wir überall dort, wo $(7 + 5)$ steht, die Zahl 12 einsetzen dürfen und überall dort wo 12 steht, den Term $(7 + 5)$ einsetzen dürfen, ohne dass sich die Zahlenwerte in unseren arithmetischen Ausdrücken ändern.

Das Gleichheitszeichen $=$ ist ein vergleichsweise modernes Konzept in der Mathematik. In der Antike und im Mittelalter war es üblich, Gleichheit nur sprachlich auszudrücken. Das Konzept der mathematischen Gleichheit ist sehr mächtig und erlaubt es, komplexe Algorithmen elegant aufzuschreiben.

Allerdings muss man für diese Vorteile auch einen Preis bezahlen. Wenn ich etwa den sprachlichen Ausdruck betrachte „Die Addition der Zahl 7 und der Zahl 5 ergibt die Zahl 12“ so beschreibt man den intellektuellen Vorgang des Rechnens. Setze ich die beiden Terme $7 + 5$ und 12 gleich, dann abstrahiere ich von dem Rechenvorgang.

In der Philosophie Kants wäre die Feststellung $7 + 5 = 12$ ein synthetisches Urteil a priori. Würde man den einen Term durch den anderen ersetzen, also statt $7 + 5 = 12$ schreiben $12 = 12$ so wäre das Ergebnis zwar auch ein synthetisches Urteil a priori aber eben ein anderes als das vorgenannte.

Paradigma 2.5. (Abstraktion durch das Konzept der Gleichheit): Durch das Konzept der Gleichheit $s = t$ zweier Terme s und t abstrahiert man in der Mathematik von denjenigen Vorgängen, mit denen man zur Feststellung der Gleichheit gelangt sein könnte.

Definition 2.10. (Gleichheitszeichen bei Definitionen): Sei s ein [wohldefinierter] Term und sei t ein konstanter Bezeichner für einen Term. Die Fest-

legung

$$t := s$$

definiert t als Abkürzung für den Term s.

2.3 Elementare Mengenlehre

Die folgende Definition stammt von Georg Cantor, vgl. Deiser Mengenlehre [2], S. 17.

Definition 2.11. (Menge): Unter einer **Menge** M verstehen wir eine beliebige Zusammenfassung von bestimmten wohl-unterschiedenen Objekten m — **Elemente** genannt — unserer Anschauung oder unseres Denkens zu einem Ganzen. Formal: $m \in M$, in Worten „m ist Element von M“.

Um auszudrücken, dass eine Menge M all diejenigen Elemente x enthält, die die Eigenschaft $A(x)$ haben, ist folgende Schreibweise gebräuchlich:

$$M := \{x \mid A(x)\}$$

Der Begriff der Menge ist problematisch. So sollte man Mengen ausschließen, die sich selbst als Element enthalten. Anderenfalls können einem schwerwiegende Probleme begegnen, wie man am Beispiel der Russellschen Antinomie sehen kann:

Betrachte dazu die Menge R aller Mengen, die sich selbst nicht als Element enthalten:

$$R := \{x \mid x \notin x\}$$

Nun stellt sich die Frage, ob R Element von R ist, oder nicht. Wäre $R \in R$, dann müsste R per Konstruktion der Menge R die Eigenschaft haben $R \notin R$. Ist nun aber $R \notin R$, dann besitzt R die Eigenschaft, die es zum Element von R macht, also $R \in R$ ↯.

Paradigma 2.6. (Vermeidung von Mengen, die sich selbst als Element enthalten): Um Probleme wie die Russellsche Antinomie zu vermeiden, verbieten wir in der Praxis solche Mengen, die sich selbst als Element enthalten, obwohl es solche Mengen nach unserer Definition 2.11 der Menge gegen kann.

Definition 2.12. (Teilmenge, Gleichheit von Mengen, leere Menge): Seien M, N Mengen

1. N wird **Teilmenge** von M genannt, in Zeichen $N \subseteq M$, wenn jedes Element von N auch Element von M ist. Formal, wenn:

$$\forall x\,(x \in N \Rightarrow x \in M).$$

2. M und N heißen **gleich**, in Zeichen $M = N$, wenn M und N die gleichen Elemente enthalten. Formal, wenn: $M \subseteq N$ und $N \subseteq M$ gilt.

3. Die **leere Menge** ist diejenige Menge, die kein Element besitzt. Sie wird mit $\emptyset$ bezeichnet.

Definition 2.13. (Vereinigung und Durchschnitt von Mengen, Differenzmengen, disjunkte Mengen): Seien M und N Mengen.

1. Folgende Menge wird als **Vereinigung** von M und N bezeichnet:

$$M \cup N := \{x \mid x \in M \text{ oder } x \in N\}$$

2. Folgende Menge wird als **Durchschnitt** von M und N bezeichnet:

$$M \cap N := \{x \mid x \in M \text{ und } x \in N\}$$

3. Folgende Menge wird als **Differenzmenge** von M und N bezeichnet:

$$M \setminus N := \{x \mid x \in M \text{ und } x \notin N\}$$

4. M und N heißen **disjunkt**, falls $M \cap N = \emptyset$.

Mengenbeziehungen wie Vereinigung, Durchschnitt etc. lassen sich recht elegant graphisch darstellen, wie Abbildung 1 verdeutlicht.

Wie steht es mit der Existenz der leeren Menge? Nach unserer Definition 2.11 der Menge wäre die leere Menge eine Zusammenfassung von wohlunterschiedenen Objekten, die weder in unserem Denken noch in unserer Anschauung „sind“. Ist die leere Menge das „Nichts“? Zumindest ist unsere Definition der Menge, ist hier problematisch, denn hier gibt es keine wohlunterschiedenen Objekte, die wir zusammenfassen könnten.

Andererseits ist die leere Menge fürchterlich praktisch und fundamental für die Mathematik. Wir können sie leicht konstruieren. Nehmen wir die Mengen $A := \{1, 3, 5\}$ *und* $B := \{2, 4, 6\}$ *und betrachten wir nun die Schnittmenge* $C := A \cap B$*. Dazu nehmen wir das erste Element von* A*, gehen alle Elemente von* B *durch und prüfen auf Übereinstimmung. Haben wir Übereinstimmung, dann gehört dieses Element in die Schnittmenge. Anderenfalls nicht. Dann nehmen wir das zweite Element von* A *u.s.w. Besonders bei endlichen Mengen — wie in diesem Beispiel — lässt sich die Schnittmenge auf diese Weise sehr anschaulich konstruieren. Nun stellen wir dabei fest, dass es kein Element in* A *gibt, dass auch in* B *ist. Also gibt es kein Element in der Schnittmenge. Wir sagen, die Schnittmenge sei leer. Ist die Schnittmenge überhaupt eine*

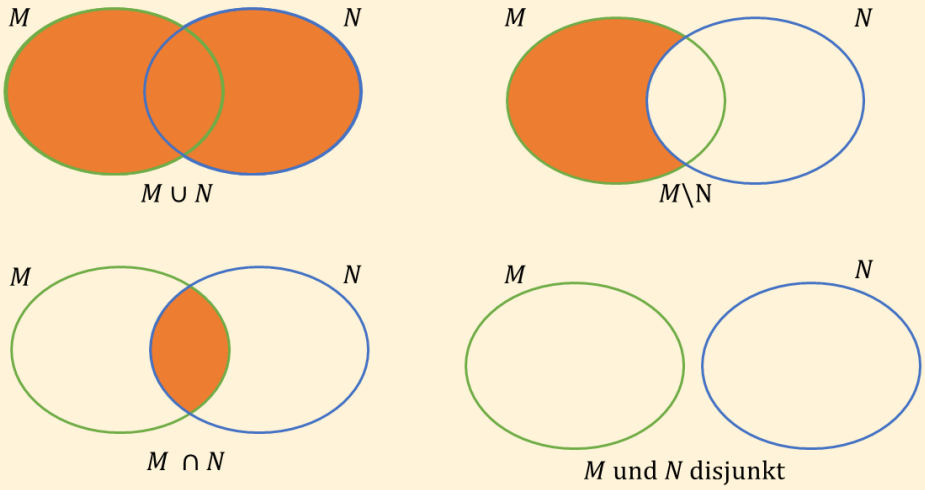

Abbildung 1: Venn-Diagramme — Vereinigung und Durchschnitt, Differenzmenge, disjunkte Mengen

Menge? Ja, denn wir können sie uns denken: als leeres Ergebnis der o.g. Konstruktion unter Verwendung von Elementen aus A und B.

Nun stellt sich die Frage: Gibt es überhaupt nur eine einzige leere Menge? Ist C ***die*** *leere Menge? Eigentlich nicht, denn wir können uns ganz verschiedene leere Mengen denken. So z.B. auch die Menge D, die alle Äpfel enthält, die gleichzeitig Birnen sind. Wobei wir unterstellen wollen, dass sich Äpfel nie gleichzeitig Birnen und Birnen nie gleichzeitig Äpfel sind. Also auch D ist eine leere Menge. Per Konstruktion sind C und D völlig unterschiedlich. Und wenn wir sie uns denken, denken wir ganz offensichtlich Verschiedenes. Aber in der Mathematik machen wir diese Unterscheidung nicht. Eine Menge ist wie die andere, wir betrachten nur die Mengeneigenschaft. Und mit dieser Abstraktion sind alle leeren Mengen gleich* ***der*** *leeren Menge* $\emptyset$.

Paradigma 2.7. (Existenz der leeren Menge): Die leere Menge existiert und ist eindeutig.

Definition 2.14. (Potenzmenge): Sei M eine Menge. Die Menge aller Teilmengen von M wird **Potenzmenge** $\mathcal{P}(M)$ genannt.

3 Salle de Réception — Eingangshalle

Visite guidée: *Die Besucher können nun eintreten in die Eingangshalle des Schlosses. Vorsicht: Die kleinen Figuren für Wahrheit und Falschheit nicht ins Schloss mitnehmen! Berührte man z.B. mit der Falschheit eine Aussage im Schloss, könnte Fürchterliches passieren. Zwar haben wir ein raffiniertes System zur Widerspruchsalarmierung, aber auch das kann nicht immer das Schlimmste verhindern.*

Am Eingang, der großen Drehtür, wird deshalb jeder Besucher daraufhin kontrolliert, ob er etwa noch ein Falsum-Teufelchen bei sich führt. Und noch etwas gilt es zu beachten: Während man die Drehtür durchschreitet, wird man nach den möglichen Wahrheitswerten einer mathematischen Aussage gefragt. Es empfiehlt sich, zu antworten mit „wahr oder falsch — tertium non datur", anderenfalls dreht sich die Drehtür weiter und man landet wieder auf dem Schlosshof.

Besuchern, die nicht an die Zweiwertigkeit der Logik zu glauben, oder die zumindest so tun, ist der Zutritt zum Schloss leider verwehrt. Sie können sich zur Baracke begeben. Die Baracke steht ganz hinten am Ende des Parks. Die Mathematiker dort (sie nennen sich Intuitionisten oder Konstruktivisten) erlauben allen Besuchern den Zutritt.

3.1 Kartesisches Produkt

Definition 3.1. (Kartesisches Produkt): Seien M und N nicht-leere Mengen. Wir definieren die Menge $M \times N$ aller geordneten Paare aus Elementen der Menge M und Elementen der Menge N wie folgt und bezeichnen sie als **kartesisches Produkt** von M und N:

$$M \times N := \{(x, y) \mid x \in M \text{ und } y \in N\}$$

Definition 3.2. (Gleichheit von geordneten Paaren): Sei $M \times N$ ein kartesisches Produkt. Zwei geordnete Paare (x, y), $(x', y') \in M \times N$ heißen gleich, falls $x = x'$ und $y = y'$.

3.2 Relationen

Definition 3.3. (Relation auf einer Menge): Sei M eine [nicht-leere] Menge. Eine beliebige Teilmenge $R \subseteq M \times M$ wird **Relation auf** M genannt.
Schreibweise: Falls $(m, m') \in R$, so schreibt man auch $m \underset{R}{\sim} m'$.

Definition 3.4. (Äquivalenzrelation): Sie M eine [nicht-leere] Menge. Eine Relation R auf M heißt **Äquivalenzrelation**, falls gilt:

(1) $\forall x \ \in M$ gilt: $x \underset{R}{\sim} x$ (Reflexivität)

(2) $\forall x, x' \in M$ gilt: $x \underset{R}{\sim} x' \ \Rightarrow \ x' \underset{R}{\sim} x$ (Symmetrie)

(3) $\forall x, x', x'' \in M$ gilt: $((x \underset{R}{\sim} x') \wedge (x' \underset{R}{\sim} x'')) \ \Rightarrow \ x \underset{R}{\sim} x''$ (Transitivität)

Beispiel 3.1. (Äquivalenzrelation): Die drei Bekannten Clara, Leni und Felix bilden die Menge $M := \{C, L, F\}$, wobei wir die Namen abgekürzt haben. Das kartesische Produkt lautet:

$$M \times M = \{(C,C),(C,L),(C,F),(L,C),(L,L),(L,F),(F,C),(F,L),(F,F)\}$$

Nehmen wir nun an, Clara liebt Felix, Felix liebt Clara, Leni liebt keinen der beiden anderen und wird von ihnen auch nicht geliebt und schließlich alle drei lieben sich jeweils selbst. Dann drückt die folgende Relation diese Liebesbeziehungen aus:

$$R = \{(C,F),(F,C),(C,C),(L,L),(F,F)\}.$$

R ist eine Äquivalenzrelation:

(1) $C \sim C$, $L \sim L$, $F \sim F$ (Reflexivität)

(2) $C \sim F \Rightarrow F \sim C$ und $F \sim C \Rightarrow C \sim F$ (Symmetrie)

(3) $(C \sim F) \wedge (F \sim C) \Rightarrow (C \sim C)$, $(F \sim C) \wedge (C \sim F) \Rightarrow (F \sim F)$ und weitere triviale Fälle wie $(C \sim C) \wedge (C \sim C) \Rightarrow (C \sim C)$ (Transitivität)

Definition 3.5. (Äquivalenzklasse): Sei M eine [nicht-leere] Menge und sei $\underset{R}{\sim}$ eine Äquivalenzrelation auf M. Für ein beliebiges $m \in M$ heißt

$$[m] := \{x \in M \mid x \underset{R}{\sim} m\}$$

die **Äquivalenzklasse** von m.

Lemma 3.1. (Zerlegung einer Menge in Äquivalenzklassen): Sei M eine [nicht-leere] Menge und sei $\underset{R}{\sim}$ eine Äquivalenzrelation auf M. Für beliebige $l, n \in M$ gilt:

$$\text{entweder} \quad [l] = [n] \quad \text{oder} \quad [l] \cap [n] = \emptyset.$$

Beweis: Angenommen $[l] \cap [n] \neq \emptyset$.
Dann existiert ein $m \in [l] \cap [n]$, d.h. $m \underset{R}{\sim} l$ und $m \underset{R}{\sim} n$.

Behauptung: $[l] \subseteq [n]$
Sei dazu $l' \in [l]$, d.h. $l' \underset{R}{\sim} l$.
Wegen $m \underset{R}{\sim} l \underset{\text{Sym.}}{\Rightarrow} l \underset{R}{\sim} m \underset{\text{Tran.}}{\Rightarrow} l' \underset{R}{\sim} m$.
Da $m \underset{R}{\sim} n \underset{\text{Tran.}}{\Rightarrow} l' \underset{R}{\sim} n \Rightarrow l' \in [n]$, also $[l] \subseteq [n]$.

Aus Symmetriegründen gilt auch die Umkehrung $[n] \subseteq [l]$. □

Beispiel 3.2. (Äquivalenzklassen): Kommen wir zurück zu unserem Beispiel zur Äquivalenzrelation 3.1. Die Äquivalenzklassen

$$\begin{aligned} [C] &= \{x \in M \mid x \sim C\} = \{C, F\} = [F] \quad \text{und} \\ [L] &= \{x \in M \mid x \sim L\} = \{L\} \end{aligned}$$

zerlegen unsere Menge M in die Untermengen der wechselseitig Geliebten $\{C, F\}$ und der wechselseitig Ungeliebten $\{L\}$. Insbesondere ist $[C] \cap [L] = \emptyset$ und es gilt $[C] \cup [L] = M$.

Definition 3.6. (Quotientenmenge): Seien M eine [nicht-leere] Menge und $\underset{R}{\sim}$ eine Äquivalenzrelation auf M. Dann heißt

$$\begin{aligned} M/\underset{R}{\sim} &:= \text{Menge aller Äquivalenzklassen bezüglich } \underset{R}{\sim} \\ &= \{[x]_{\underset{R}{\sim}} \mid x \in M\} \end{aligned}$$

die **Quotientenmenge** von M bezüglich der Relation $\underset{R}{\sim}$.

Beispiel: In unserem Beispiel zu Äquivalenzklassen 3.2 können wir die Quotientenmenge direkt hinschreiben:

$$M/\underset{R}{\sim} = \{[C], [L]\} = \{\{C, F\}, \{L\}\}.$$

Definition 3.7. (Ordnungsrelation): Sei M eine [nicht-leere] Menge und sei R eine Relation auf M mit der Schreibweise:

$$\forall x, x' \in M \text{ mit } (x, x') \in R \text{ schreibe } x \leq x'.$$

R heißt **Halbordnung** auf M, falls gilt:

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

(2) $\forall x, x' \in M$ gilt: $((x \leq x') \wedge (x' \leq x)) \Rightarrow x = x'$ (Antisymmetrie)

(3) $\forall x, x', x'' \in M$ gilt: $((x \leq x') \wedge (x' \leq x'')) \Rightarrow x \leq x''$ (Transitivität)

R heißt sogar **Totalordnung**, falls R eine Halbordnung ist und darüber hinaus gilt:

(4) $\forall x, x' \in M$ gilt $(x \leq x') \vee (x' \leq x)$ (Totalität)

Definition 3.8. (Strenge Totalordnung): Sei M eine [nicht-leere] Menge und sei R eine Relation auf M mit der Schreibweise:

$$\forall x, x' \in M \text{ mit } (x, x') \in R \text{ schreibe } x < x'.$$

R heißt **strenge Totalordnung** auf M, falls gilt:

(1) $\forall x, x', x'' \in M$ gilt: $((x < x') \wedge (x' < x'')) \Rightarrow x < x''$ (Transitivität)

(2) $\forall x, x' \in M$ gilt: entweder $x < x'$ oder $x = x'$ oder $x' < x$ (Trichotomie)

Beachte: Eine strenge Totalordnung ist weder eine Halbordnung noch ist sie eine Totalordnung, da sie nicht reflexiv ist.

Beispiel: Nehmen wir an, Clara, Leni und Felix haben eine Klausur geschrieben. Leni erzielt das beste Ergebnis mit 99 von 100 möglichen Punkten. Felix erreicht 75 Punkte und Clara muss mit 50 Punkten zufrieden sein.

Betrachten wir die Relation T „... war schlechter oder gleich gut in der Klausur wie ...“:

$$T = \{(C, C), (C, L), (C, F), (L, L), (F, L), (F, F)\}.$$

T ist reflexiv, antisymmetrisch, transitiv und total. Damit ist T eine Totalordnung von M.

Da alle drei Prüflinge aus M eine unterschiedliche Punktzahl erreicht haben, lässt sich eine strenge Totalordnung wie folgt konstruieren:

$$S = \{(C, L), (C, F), (F, L)\}.$$

S ist transitiv und trichotom, also ist S eine strenge Totalordnung von M. Wir sehen an diesem Beispiel insbesondere, dass S wegen der fehlenden Reflexivität ein anderes Konzept verfolgt als T.

Zusammenfassung: In diesem Kapitel haben wir folgende Relationen auf einer Menge betrachtet:

Relationstyp	Eigenschaften
Äquivalenzrelation	reflexiv, symmetrisch, transitiv
Halbordnung	reflexiv, antisymmetrisch, transitiv
Totalordnung	reflexiv, antisymmetrisch, transitiv, total
Strenge Totalordnung	transitiv, trichotom

3.3 Abbildungen

Definition 3.9. (Relationen zwischen zwei Mengen): Seien M und N nicht-leere Mengen. Eine **Relation** zwischen M und N ist eine Teilmenge $R \subseteq M \times N$.

Beispiel 3.3. (Relation zwischen zwei Mengen): Betrachten wir die Spieler Clara, Leni und Felix, die dreimal ein Brettspiel spielen, bei dem stets genau ein Spieler gewinnen muss (z.B. Mensch ärgere Dich nicht). Sei M die Menge der Spieler $M = \{C, L, F\}$. Sei N die Menge der Spiele S_1, S_2, S_3, also $N = \{S_1, S_2, S_3\}$. Clara gewinnt die Spiele S_1 und S_3, Felix gewinnt das Spiel S_2. Leni gewinnt also kein Spiel.

Das kartesische Produkt aus M und N lautet:
$\{(C, S_1), (C, S_2), (C, S_3), (L, S_1), (L, S_2), (L, S_3), (F, S_1), (F, S_2), (F, S_3)\}$.
In unserem Beispiel drückt das kartesische Produkt alle möglichen Spielausgänge aus.

Die Teilmenge $R \subseteq M \times N$ mit $R = \{(C, S_1), (F, S_2), (C, S_3)\}$ ist ein Beispiel für eine Relation. In diesem Beispiel drückt R aus „Spieler*in ... gewinnt Spiel ...“. Wir prüfen nach: Clara gewinnt Spiel S_1, Felix gewinnt Spiel S_2 und Clara gewinnt Spiel S_3. Stimmt.

Jede andere Teilmenge aus $M \times N$ wäre aber gleichermaßen eine Relation. So ließen sich auch unmögliche Spielausgänge darstellen, wie z.B. $R' = \{(C, S_1), (L, S_1), (F, S_3)\}$, wonach sowohl Clara als auch Leni das Spiel S_1 gewonnen hätten.

Definition 3.10. (Abbildung): Seien M und N nicht-leere Mengen. Eine **Abbildung** — oder synonym **Funktion** — von M nach N ist eine Teilmenge $f \subseteq M \times N$, die folgende Eigenschaften besitzt:

(1) $\forall x \in M\ \exists y \in N$, so dass $(x, y) \in f$

(2) $\forall x \in M\ \forall y, y' \in N$ gilt: wenn $(x, y) \in f$ und $(x, y') \in f$, dann ist $y = y'$.

Schreibweise: Eine so definierte Abbildung wird typischerweise wie folgt no-

tiert:

$$\begin{array}{rccl} f: & M & \longrightarrow & N \\ & x & \longmapsto & f(x) = y. \end{array}$$

Diese Schreibweise ist wohldefiniert, da zu jedem $x \in M$ in eindeutiger Weise ein $y \in N$ zugeordnet werden kann mit $(x, y) \in f$.
M heißt **Defintionsbereich**, N heißt **Wertebereich** von f.

Definition 3.11. (Gleichheit von Abbildungen): Seien $f: M \to N$ und $g: M' \to N'$. f und g heißen gleich, falls $M = M'$, $N = N'$ und $\forall x \in M: f(x) = g(x)$.

Definition 3.12. (Urbild und Bild von Abbildungen): Sei $f: M \to N$ eine Abbildung. Sei $m \in M$ und $f(m) = n \in N$.

(1) m heißt **Urbild** von n unter f.

(2) n heißt **Bild** von m unter f.

(3) Die Menge

$$f(M) := \{y \in N \mid \exists x \in M \text{ mit } f(x) = y\} \subseteq N$$

heißt **Bildbereich** von f.

Beispiel 3.4. (Abbildung): Die Menge $R \subseteq M \times N$ aus dem letzten Beispiel 3.9 ist keine Abbildung, da die Eigenschaft (2) gemäß Definition 3.4 nicht erfüllt ist: Clara hat die Spiele S_1 und S_2 gewonnen. Zum „Urbild“ Clara kann nicht. wie gefordert in eindeutiger Weise, ein „Bild“ zugeordnet werden.

Um das Beispiel zu „retten“ vertauschen wir die beiden Mengen. Wir erhalten die Funktion

$$f: N \to M,\ S_1 \mapsto C,\ S_2 \mapsto F,\ S_3 \mapsto C$$

oder in Mengenschreibweise:

$$N \times M \supseteq f = \{(S_1, C), (S_2, F), (S_3, C)\}$$

Die Abbildung f drückt aus „Das Spiel ... wurde gewonnen von Spieler*in ...“.

Paradigma 3.1. (Abstraktion von der Abbildungsvorschrift): Der mathematische Begriff der Abbildung charakterisiert „lediglich“ die Paare bestehend aus Urbild und Bild. Von der konkreten Vorschrift, mit der die Elemente

des Definitionsbereichs dem Bildbereich zugeordnet werden, wird abstrahiert. Insbesondere muss der „funktionale“ Zusammenhang nicht konstruktiv dargestellt werden, an den man intuitiv beim Begriff einer „Funktion“ denken mag.

Definition 3.13. (Injektivität, Surjektivität, Bijektivität): Sei $f: M \to N$ eine Abbildung.

(a) f heißt **injektiv**, wenn jedes Bild von f genau ein Urbild besitzt. Formal:

$$\forall y \in f(M)\ \forall x, x' \in M\ (f(x) = y \wedge f(x') = y) \ \Rightarrow\ x = x'$$

(b) f heißt **surjektiv**, wenn jedes Element $y \in N$ im Bild von f liegt. Formal:

$$f(M) = N \quad \text{oder anders ausgedrückt} \quad \forall y \in N\ \exists x \in M\ f(x) = y$$

(c) f heißt **bijektiv**, wenn f injektiv und surjektiv ist.

Definition 3.14. (Identische Abbildung): Sei M eine Menge. Die Abbildung

$$\begin{array}{rccl} \mathrm{id}_M: & M & \longrightarrow & M \\ & m & \longmapsto & \mathrm{id}_M(m) := m \end{array}$$

heißt **identische Abbildung** auf M.

Definition 3.15. (Komposition von Abbildungen): Seien L, M, N Mengen und seien $f: L \to M$ und $g: M \to N$ Abbildungen. Die Abbildung

$$\begin{array}{rccl} g \circ f: & L & \longrightarrow & N \\ & l & \longmapsto & (g \circ f)(l) := g(f(l)) \end{array}$$

wird **Komposition** oder **Hintereinanderausführung** der Abbildungen g und f genannt. $g \circ f$ wird gesprochen „g nach f“.

Beispiel: Sei $f: L \to M$ eine Abbildung. Dann gilt

$$\begin{array}{rccl} \forall l \in L & (\mathrm{id}_M \circ f)(l) & = & \mathrm{id}_M(f(l)) = f(l) \\ \forall l \in L & (f \circ \mathrm{id}_L)(l) & = & f(l) \end{array}$$

Also $\mathrm{id}_M \circ f = f \circ \mathrm{id}_L = f$.

Satz 3.1. (Surjektivität, Injektivität und Bijektivität von Kompositionen): Seien L, M, N Mengen und $f: L \to M$ sowie $g: M \to N$ Abbildungen. Dann gilt:

(a) f, g surjektiv $\Rightarrow$ $g \circ f$ surjektiv

(b) f, g injektiv $\Rightarrow$ $g \circ f$ injektiv

(c) f, g bijektiv $\Rightarrow$ $g \circ f$ bijektiv

Beweis:

ad (a): Für alle $n \in N$ gilt folgende Argumentationskette:
g surjektiv: $\exists m \in M$ mit $g(m) = n$.
f surjektiv: $\exists l \in L$ mit $f(l) = m$.
Daher: $(g \circ f)(l) = g(f(l)) = g(m) = n$.
Also: $g \circ f$ surjektiv.

ad (b): Für alle $l_1, l_2 \in L$ mit der Eigenschaft $(g \circ f)(l_1) = (g \circ g)(l_2)$ gilt:

$$\begin{aligned} g(f(l_1)) &= g(f(l_2)) \\ \text{Da } g \text{ injektiv ist, folgt daraus:} \quad f(l_1) &= f(l_2) \\ \text{Da } f \text{ injektiv ist, folgt daraus:} \quad l_1 &= l_2 \end{aligned}$$

Also $(g \circ f)$ injektiv.

ad (c): ergibt sich direkt aus (a) und (b). □

Definition 3.16. (Inverse Abbildung): Seien M, N Mengen und $f : M \to N$ eine Abbildung. f heißt **invertierbar**, falls es eine Abbildung $f^{-1} : N \to M$ gibt mit den Eigenschaften:

$$f^{-1} \circ f = \mathrm{id}_M \quad \text{und} \quad f \circ f^{-1} = \mathrm{id}_N.$$

Dann heißt f^{-1} die zu f **inverse Abbildung**.

Warum fordert man in dieser Definition, dass für die inverse Abbildung sowohl $f^{-1} \circ f = \mathrm{id}_M$ gelten muss als auch $f \circ f^{-1} = \mathrm{id}_N$? Im folgenden Beispiel findet man eine Antwort auf diese Frage.

Beispiel: $M := \{a\}$, $N := \{a, b\}$.
Betrachte zwei wie folgt definierte Abbildungen:
$f : M \to N,\ a \mapsto a$
$g : N \to M,\ a \mapsto a,\ b \mapsto b$
Dann ist $(g \circ f)(a) = g(a) = g$, also $g \circ f = \mathrm{id}_M$
aber $(f \circ g)(b) = f(a) = a$, also $f \circ g \neq \mathrm{id}_N$.

Wie man an $f \circ g \neq g \circ f$ sieht, ist die Komposition i.a. nicht kommutativ.

Satz 3.2. (Invertierbarkeit bijektiver Abbildungen): Seien M, N Mengen und $f: M \to N$ eine Abbildung. Dann sind folgende Aussagen äquivalent:

(a) f ist bijektiv.

(b) f ist invertierbar.

Beweis:

(a)⇒(b) Da f surjektiv ist, gilt $\forall n \in N\ \exists m \in M$ mit $f(m) = n$.
Da f injektiv ist, ist dieses m eindeutig.
Damit ist folgende Abbildung wohldefiniert:

$$\begin{aligned} f^{-1}: \quad N &\longrightarrow M, \\ n = f(m) &\longmapsto m =: f^{-1}(n). \end{aligned}$$

$\forall m \in M$ gilt: $(f^{-1} \circ f)(m) = f^{-1}(f(m)) = m$, also $(f^{-1} \circ f) = \mathrm{id}_M$.
$\forall n \in N$ gilt: $(f \circ f^{-1})(n) = f(f^{-1}(n)) = n$, also $(f \circ f^{-1}) = \mathrm{id}_N$.
Demnach ist f invertierbar.

(b)⇒(a) $\forall m_1, m_2 \in M$ mit der Eigenschaft $f(m_1) = f(m_2)$ gilt:

$$\begin{aligned} & f^{-1}(f(m_1)) = f^{-1}(f(m_2)) \\ \to \quad & (f^{-1} \circ f)(m_1) = m_1 = (f^{-1} \circ f)(m_2) = m_2 \end{aligned}$$

Also ist f injektiv.
Da $(f \circ f^{-1}) = \mathrm{id}_N$ gilt für alle $n \in N$:

$$n = (f \circ f^{-1})(n) = f(\underbrace{f^{-1}(n)}_{\exists m \in M \text{ mit } f^{-1}(n) = m}) = f(m)$$

Also ist f auch surjektiv. □

Satz 3.3. (Assoziativität der Komposition): Seien K, L, M, N Mengen und seien

$$f: K \to L, \quad g: L \to M, \quad h: M \to N$$

Abbildungen. Dann gilt:

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

Kurz: Die Komposition von Abbildungen ist assoziativ.

Beweis: Betrachten wir zunächst die beiden Terme und prüfen sie auf Wohldefiniertheit:

$$\underbrace{(\underbrace{\underbrace{h}_{M \to N} \circ \underbrace{g}_{L \to M}}_{L \to N} \circ \underbrace{f}_{K \to L})}_{K \to N} \qquad \underbrace{\underbrace{h}_{M \to N} \circ (\underbrace{\underbrace{g}_{L \to M} \circ \underbrace{f}_{K \to L}}_{K \to M})}_{K \to N}$$

Also sind die beiden Terme $(h \circ g) \circ f$ und $h \circ (g \circ f)$ wohldefiniert und sie haben denselben Definitionsbereich sowie denselben Wertebereich.
Für alle $k \in K$ gilt:

$$\begin{aligned}((h \circ g) \circ f)(k) &= (h \circ g) \circ f(k) \\ &= h(g(f(k))) \\ &= h((g \circ f)(k)) \\ &= (h \circ (g \circ f))(k) \quad \square\end{aligned}$$

3.4 Gruppen, Ringe, Körper

Definition 3.17. (Verknüpfung): Sei M eine Menge. Eine **Verknüpfung** $\cdot$ **auf** M ist eine Abbildung von $M \times M$ nach M, also

$$\begin{aligned}\cdot : \ M \times M &\longrightarrow M \\ (m, m') &\longmapsto m \cdot m'.\end{aligned}$$

Definition 3.18. (Halbgruppe): Sei G eine Menge mit einer Verknüpfung $\cdot$. $(G, \cdot)$ heißt **Halbgruppe**, falls gilt:

$$\forall x, y, z \in G \quad (x \cdot y) \cdot z = x \cdot (y \cdot z). \quad \text{(Assoziativgesetz)}$$

Definition 3.19. (Abelsche Halbgruppe): Eine Halbgruppe $(G, \cdot)$ heißt **abelsch** oder **kommutativ**, falls gilt:

$$\forall x, y \in G \quad x \cdot y = y \cdot x. \quad \text{(Kommutativgesetz)}$$

Definition 3.20. (Monoid): Eine Halbgruppe $(G, \cdot)$ heißt **Monoid** $(G, \cdot, e)$, falls gilt:

$$\exists e \in G \ \forall x \in G \quad e \cdot x = x \cdot e = e \quad \text{(Existenz des neutralen Elements)}$$

Definition 3.21. (Invertierbare Elemente eines Monoids): Sei $(G, \cdot, e)$ ein Monoid. Ein Element $x \in G$ heißt **invertierbar**, falls gilt:

$$\exists x^{-1} \in G \quad x \cdot x^{-1} = x^{-1} \cdot x = e.$$

Es folgt ein kleiner Satz bei dem wir die natürlichen Zahlen und das Prinzip der vollständigen Induktion brauchen. Wir benutzen diesen Satz aber erst in späteren Abschnitten, wenn die natürlichen Zahlen eingeführt sind.

Satz 3.4. (Eigenschaften invertierbarer Elemente eines Monoids): Sei $(G, \cdot, e)$ ein Monoid und sei $n \in \mathbb{N}$. Dann gilt:

(a) Falls ein invertierbares Elemente $x \in G$ existiert, folgt

$$\forall y, z \in G \quad x\,y = y\,x = 1 \;\wedge\; x\,z = z\,x = 1 \quad \Rightarrow \quad y = z$$

(b) Falls $x_1, \ldots, x_n \in G$ invertierbar sind, so ist ihr Produkt $x := x_1 \cdot \ldots \cdot x_n$ ebenfalls invertierbar und es gilt: $x^{-1} = x_n^{-1} \cdot \ldots \cdot x_1^{-1}$.

Beweis:

ad (a)

$$\begin{aligned} x^{-1} &= x^{-1}\,x\,y = y \\ &= x^{-1}\,x\,z = z \end{aligned}$$

ad (b) Beweis durch vollständige Induktion nach n.
Induktionsanfang: Sei $n = 1$. Dann ist $x = x_1$ invertierbar mit $x^{-1} = x_1^{-1}$.
Induktionsvoraussetzung: Die Behauptung sei wahr für ein $n \leq 1$.
Induktionsschluss: $x = x_1 \cdot \ldots \cdot x_n$ ist invertierbar nach Induktionsvoraussetzung und x_{n+1} ist ebenfalls invertierbar. Es gilt:

$$x\,x_{n+1}\,x_{n+1}^{-1}\,x^{-1} = x\,x^{-1} = e \quad \text{sowie} \quad x_{n+1}^{-1}\,x^{-1}\,x\,x_{n+1} = x_{n+1}^{-1}\,x_{n+1} = e.$$

Also ist auch das Element $x\,x_{n+1}$ invertierbar und sein Inverses lautet $x_{n+1}^{-1}\,x^{-1}$.

□

Definition 3.22. (Gruppe): Ein Monoid $(G, \cdot, e)$ heißt **Gruppe** $(G, \cdot, e, ^{-1})$, falls gilt:

$\forall x \in G\, \exists x^{-1} \in G \quad x \cdot x^{-1} = x^{-1} \cdot x = e$ (Existenz des jeweils inversen Elements)

$(G, \cdot, e, ^{-1})$ heißt abelsche oder kommutative Gruppe, falls $(G, \cdot, e, ^{-1})$ eine Gruppe ist und das Kommutativgesetz gilt.

Konvention: In einer Struktur kann es mehrere Verknüpfungen auf einer Menge geben. So schreibt man beispielsweise Gruppen mit einer multiplikativen Verknüpfung wie oben definiert: $(G, \cdot, e, ^{-1})$. Alternativ dazu schreibt man z.B. bei additiver Verknüpfung: $(G, +, 0, -)$.

Vereinfachung: Bei multiplikativen Gruppen wird das Verknüpfungszeichen $\cdot$ gewöhnlich weggelassen. So schreibt man $x\,y$ statt $x \cdot y$.

Satz 3.5. (Schwache Gruppenaxiome): Sei $(G, \cdot)$ eine Halbgruppe mit folgenden Eigenschaften:

(1) $\exists e \in G\ \forall x \in G \quad e\,a = a$ (Existenz eines linksneutralen Elements)

(2) $\forall x \in G\ \exists x^{-1} \in G \quad x^{-1}\,x = e$ (Existenz des jeweils linksinversen Elements)

Dann ist $(G, \cdot, e, ^{-1})$ eine Gruppe im Sinne der Definition 3.22

Beweis: Sei $x \in G$, sei $x^{-1} \in G$ das zu x linksinverse Element und sei $(x^{-1})^{-1} \in G$ das zu x^{-1} linksinverse Element. Dann gilt:

$$x\,x^{-1} = e\,(x\,x^{-1}) = ((x^{-1})^{-1}\,x^{-1})\,(x\,x^{-1}) = (x^{-1})^{-1}\,(\underbrace{x^{-1}\,x}_{=e}\,x^{-1}) = (x^{-1})^{-1}\,x^{-1} = e.$$

Also ist jedes linksinverse Element x^{-1} gleichzeitig auch ein rechtsinverses Element.

Damit weiter:

$$x\,e = x\,(x^{-1}\,x) = (x\,x^{-1})\,x = e\,x = x.$$

Also ist das linksneutrale Element stets auch rechtsneutral. □

Satz 3.6. (Grundlegende Eigenschaften einer Gruppe): Sei $(G, \cdot, e, ^{-1})$ eine Gruppe. Dann gilt:

(a) Das neutrale Element ist eindeutig. D.h., es existiert genau ein $e \in G$, so dass $\forall x \in G: \quad ex = xe = x$. Dies gilt bereits in einem Monoid $(G, \cdot, e)$.

(b) Das jeweils inverse Element ist eindeutig. D.h. $\forall x \in G$ existiert jeweils genau ein $y \in G$, so dass $xy = yx = e$.

(c) Es gilt die Erweiterungsregel: $\forall x, y, z \quad y = z \ \Rightarrow\ x\,y = x\,z$.

(d) Es gilt die Kürzungsregel:

$$\begin{array}{lll} \forall x, y, z \quad x\,y = x\,z & \Rightarrow & y = z \\ \qquad\qquad\ \ y\,x = z\,x & \Rightarrow & y = z. \end{array}$$

(e) Die Gleichung $y\,x = z$ ist eindeutig lösbar mit der Lösung $x = y^{-1}\,z$.

(f) $e^{-1} = e$ und $\forall x \in G\ (x^{-1})^{-1} = x$.

(g) $\forall x, y \in G \quad (x\,y)^{-1} = y^{-1}\,x^{-1}$.

Beweis:

ad (a) Seien e und e' ggf. verschiedene neutrale Elemente. Also

$$\forall x \in G \quad xe = ex = x \quad \text{und} \quad xe' = e'x = x.$$

Dann gilt:

$$e = ee' = e'.$$

ad (b) Sei $x \in G$ und seien $y, y' \in G$ mit $xy = yx = e$ und $xy' = y'x = e$. Dann gilt einerseits

$$y = ey = y'xy$$

und andererseits

$$y' = y'e = y'xy$$

Also gilt: $y = y'$

ad (c) Diese Behauptung ergibt sich unmittelbar aus der Eigenschaft des Gleichheitszeichens.

ad (d)

$$x\,y = x\,z \quad \Rightarrow \quad \underbrace{x^{-1}\,x}_{=e}\,y = \underbrace{x^{-1}\,x}_{=e}\,z \quad \Rightarrow \quad y = z$$

ad (e)

$$y\,x = z \quad \Rightarrow \quad \underbrace{y^{-1}\,y}_{=e}\,x = y^{-1}\,z \quad \Rightarrow \quad x = y^{-1}\,z$$

ad (f)

$$e^{-1} = e^{-1}\,e = e$$

$$(x^{-1})^{-1}\,x^{-1} = e \quad \Rightarrow \quad (x^{-1})^{-1}\,\underbrace{x^{-1}\,x}_{=e} = x \quad \Rightarrow \quad (x^{-1})^{-1} = x.$$

ad (g) Die Behauptung folgt direkt aus folgender Gleichungskette:

$$x\,y\,(y^{-1}\,x^{-1}) = x\,\underbrace{y\,y^{-1}}_{=e}\,x^{-1} = x\,x^{-1} = e = x\,y\,(x\,y)^{-1}$$

□

Beispiel: Als einfaches Beispiel für eine Gruppe mit drei Elementen betrachte man die Menge $G = \{e, a, b\}$ mit einer Verknüpfung, die über die folgende Tabelle festgelegt ist:

·	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Dann ist $(G, \cdot, e, ^{-1})$ eine kommutative Gruppe.

Definition 3.23. (Ring): Ein **Ring** $(R, +, \cdot)$ ist eine Menge R mit zwei Verknüpfungen, so dass gilt:

(1) $(R, +, 0, -)$ ist eine kommutative Gruppe,

(2) $(R, \cdot, e)$ ist ein Monoid [= eine Halbgruppe mit einem neutralen Element],

(3)

$$\begin{aligned} \forall x, y, z \in R \quad \text{gilt } x(y+z) &= x\,y + x\,z \quad \text{(Links-Distributivgesetz)} \\ \text{und } (y+z)x &= y\,x + z\,x \quad \text{(Rechts-Distributivgesetz).} \end{aligned}$$

$(R, +, \cdot)$ heißt **kommutativer Ring**, falls die dem Monoid $(R, \cdot, e)$ zugrunde liegende Halbgruppe kommutativ ist.

Satz 3.7. (Grundlegende Ring-Eigenschaften): Sei $(R, +, \cdot)$ ein Ring. Dann gilt:

(a) $1 \neq 0$

(b) $\forall x \in R \quad x\,0 = 0$

(c) $\forall a, b \in R \quad ab = 0 \;\Rightarrow\; (a = 0) \vee (b = 0)$

(d) $\forall x, y \in R \quad x\,(-y) = -(xy)$

(e) $\forall x \in R \quad (-1)\,x = -x$

(f) $\forall x \in R \quad x\,(-1) = -x$

(g) $\forall x, y \in R \quad (-x)\,y = x\,(-y) = -x\,y$

(h) $\forall x, y \in R \quad (-x)\,(-y) = x\,y$

Beweis:

ad (a) Sei $x \in R,\ x \neq 0$. Angenommen $1 = 0$. Daraus folgt:

$$x = x\,1 = x\,0 = 0 \lightning$$

ad (b) Die Behauptung folgt direkt aus folgener Gleichungskette:

$$x\,x + 0 = x\,x = x\,(x + 0) = x\,x + x\,0$$

ad (c) Falls $a = 0$ gilt die Behauptung. Sei also $a \neq 0$. Dann gilt:

$$b = a^{-1}\,\underbrace{a\,b}_{=0} = a^{-1}\,0 = 0$$

ad (d)

$$\begin{aligned} x\,y + x\,(-y) &= x\,\underbrace{(y + (-y))}_{=0} = 0 \\ \Rightarrow \quad x\,(-y) &= -(xy) \end{aligned}$$

ad (e) Zu zeigen ist, dass $(-1)\,x$ dem additiv Inversen von x entspricht (das ist dann ja gerade $-x$):

$$(-1)\,x + x = (-1)\,x + 1\,x = (-1+1)\,x = 0\,x = 0.$$

ad (f)

$$x\,(-1) + x = x\,(-1+1) = x\,0 = 0.$$

ad (g) Wir betrachten den ersten und den zweiten Term getrennt:

$$\begin{aligned} (-x)\,y = ((-1)\,x)\,y = (-1)\,x\,y &= -x\,y \\ x\,(-y) = x\,((-1)\,y) = (-x)\,y &= -x\,y \end{aligned}$$

ad (h)

$$(-x)\,(-y) = -(x\,(-y)) = -(-(x\,y)) = x\,y.$$

□

Definition 3.24. (Schiefkörper): Ein Ring $(R, +, \cdot)$ heißt **Schiefkörper**, falls $R\backslash\{0\}$ hinsichtlich der Multiplikation $\cdot$ nicht nur ein Monoid sondern auch eine Gruppe $(R\backslash\{0\}, \cdot, e, ^{-1})$ ist.

Übergang zur Körperdefinition: Handelt es sich bei der Gruppe $(R\backslash\{0\}, \cdot, e, ^{-1})$ sogar um eine abelsche Gruppe, dann heißt $(R, +, \cdot)$ Körper. Wir gönnen uns aber eine etwas ausführlichere Definition:

Definition 3.25. (Körper): Ein **Körper** $(\mathbb{K}, +, \cdot)$ ist eine Menge $\mathbb{K}$ mit zwei Verknüpfungen (Addition $+$ und Multiplikation $\cdot$) genannt, so dass gilt:

(1) $(\mathbb{K}, +, 0, -)$ ist eine abelsche Gruppe,

(2) $(\mathbb{K}\backslash\{0\}, \cdot, 1, ^{-1})$ ist eine abelsche Gruppe,

(3) $\forall x, y, z \in \mathbb{K}$ gilt $x(y+z) = x\,y + x\,z$ (Distributivgesetz).

Wegen $x\,0 = 0$ für alle $x \in \mathbb{K}$ (vgl. Satz 3.7) ist klar, dass $0 \in \mathbb{K}$ kein multiplikativ Inverses haben kann. Das macht verständlich, dass bei der multiplikativen Gruppe, die einem Körper (oder auch einem Schiefkörper) zugrunde liegt, das Element 0 ausgeschlossen werden muss.

Definition 3.26. (Bruchschreibweise): Sei $(\mathbb{K}, +, \cdot)$ ein Körper. Multiplikativ Inverse wie $x^{-1} \in \mathbb{K}\backslash\{0\}$ werden häufig wie folgt geschrieben:

$$x^{-1} =: \frac{1}{x}$$

Damit ergibt sich die **Bruchschreibweise** mit folgender Konvention:

$$\forall x \in \mathbb{K}\ \forall y \in \mathbb{K}\backslash\{0\} \quad x\,\frac{1}{y} =: \frac{x}{y}$$

Die Bruchschreibweise setzt die Körpereigenschaft voraus. In einem Schiefkörper müsste man i.a. zwischen $x\,y^{-1}$ und $y^{-1}\,x$ unterscheiden, wegen der fehlenden Kommutativität der Multiplikation. Bei der Bruchschreibweise $\frac{x}{y}$ dagegen, ist diese Unterscheidung nicht möglich.

Definition 3.27. (Bindungsstärke von Symbolen):
Die Bindungsstärke der folgenden Symbole/Operationen ist von links nach rechts abnehmend [links $\widehat{=}$ stark bindend ... rechts $\widehat{=}$ schwach bindend]:

$$\text{Klammern} \quad \text{Punktrechnung} \quad \text{Strichrechnung} \quad = \quad \Rightarrow \quad \Leftrightarrow$$

Satz 3.8. (Rechenregeln in Körpern): Seien $\mathbb{K}$ ein Körper, $a, b, c, d \in \mathbb{K}$ und $b \neq 0$, $d \neq 0$. Dann gilt:

(a) $\frac{a}{b} \pm \frac{c}{d} = \frac{a\,d \pm b\,c}{b\,d}$ (Hauptnenner-Methode)

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

(c) falls auch $c \neq 0$ $\quad \frac{\frac{a}{b}}{\frac{c}{d}} = \frac{a}{b}\,\frac{d}{c}$ (großer und kleiner Bruchstrich)

Beweis:

ad (a)

$$\begin{aligned}
\frac{a\,d \pm b\,c}{b\,d} &= (a\,d \pm b\,c)\,(b\,d)^{-1} \\
&= a\,d\,(b\,d)^{-1} \pm b\,c\,(b\,d)^{-1} \\
&= a\,\underbrace{d\,d^{-1}}_{=1}\,b^{-1} \pm \underbrace{b\,b^{-1}}_{=1}\,c\,d^{-1} \\
&= \frac{a}{b} \pm \frac{c}{d}
\end{aligned}$$

ad (b)

$$\frac{a}{b}\,\frac{c}{d} = (a\,b^{-1})\,(c\,d^{-1}) = (a\,c)\,(b\,d)^{-1} = \frac{a\,c}{b\,d}$$

ad (c)

$$\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{a}{b}\,\left(\frac{c}{d}\right)^{-1} = \frac{a}{b}\,(c\,d^{-1})^{-1} = \frac{a}{b}\,(c^{-1}\,d) = \frac{a}{b}\,\frac{d}{c}$$

□

Beispiel: Wir betrachten die Menge mit zwei Elementen $\mathbb{F}_2 = \{0, 1\}$. Auf dieser Menge lässt sich eine Addition und eine Multiplikation wie folgt definieren:

Addition $+:\ \mathbb{F}_2 \times \mathbb{F}_2 \to \mathbb{F}_2$ mit folgenden vier Ergebnismöglichkeiten:

$$0 + 0 = 0, \quad 1 + 0 = 0 + 1 = 1, \quad 1 + 1 = 0.$$

Aus dieser Definition lässt sich direkt ablesen: Die Addition besitzt das neutrale Element 0 sowie die inversen Elemente $-1 = 1$ und $-0 = 0$. Sie ist kommutativ. Das Assoziativgesetz lässt sich leicht nachrechnen durch vollständiges „Hinschreiben“. Damit ist $(\mathbb{F}_2, +, 0, -)$ eine abelsche Gruppe.

Multiplikation: $\cdot:\ \mathbb{F}_2 \times \mathbb{F}_2 \to \mathbb{F}_2$ definiert mit folgenden Ergebnismöglichkeiten:

$$0 \cdot 0 = 0 = 1 \cdot 0 = 0 \cdot 1, \quad 1 \cdot 1 = 1.$$

Aus dieser Definition lässt sich direkt ablesen: Die Multiplikation besitzt das neutrale Element 1 sowie ein inverses Element $1^{-1} = 1$. Die Multiplikation ist kommutativ. Auch hier lässt sich das Assoziativgesetz leicht nachrechnen. Demnach ist $(\mathbb{F}_2 \backslash \{0\}, \cdot, 1, ^{-1})$ eine abelsche Gruppe.

Die so definierten Verknüpfungen $+$ und $\cdot$ erfüllen das Distributivgesetz. Auch dies lässt sich leicht nachrechnen. Damit ist $(\mathbb{F}_2, +, \cdot)$ ein Körper.

Zusammenfassung: In diesem Kapitel haben wir folgende Strukturen einer Menge betrachtet:

Strukturtyp	Eigenschaften
(abelsche) Halbgruppe	eine Verknüpfung, assoziativ, (abelsch)
(abelscher) Monoid	(abelsche) Halbgruppe, neutrales Element
(abelsche) Gruppe	(abelscher) Monoid, inverse Elemente
(abelscher) Ring	zwei Verknüpfungen, bzgl. $+$: abelsche Gruppe, bzgl. $\cdot$: (abelscher) Monoid, Distributivgesetze
Schiefkörper	Ring, bzgl. $\cdot$ und ohne 0: Gruppe
Körper	Ring, bzgl. $\cdot$ und ohne 0: abelsche Gruppe
Körper (ausführlicher)	zwei Verknüpfungen, bzgl. $+$: abelsche Gruppe, bzgl. $\cdot$ ohne 0: abelsche Gruppe, Distributivgesetz

3.5 Natürliche und ganze Zahlen

Bisher habe ich versucht, das Abzählen sowie das Rechnen mit Zahlen zu vermeiden. Das erleichtert m.E. das abstrakte Verständnis der oben dargestellten Konstrukte wie Relationen, Abbildungen und Strukturen. Sobald die natürlichen Zahlen und andere fundamentale Zahlenmengen eingeführt werden, ergeben sich vielfältige Verbindungen zu diesen abstrakten Strukturen. Entsprechende Beispiele bringe ich, sobald die jeweilige Zahlenmenge eingeführt ist.

In der folgenden Einführung der Zahlenmengen werden nur wenige Beweise vorgestellt. Als Lektüre sei die „Einführung in die Mathematik“ von Helmut Koch empfohlen [5] sowie die Videos der Vorlesungsreihe „Mathematische Grundlagen“ von Christian Spannagel [6].

Definition 3.28. (Peano-Axiome): Die wie folgt definierte Menge $\mathbb{N}_0$ heißt **Menge der natürlichen Zahlen mit der Null**:

(1) $0 \in \mathbb{N}_0$

(2) $\forall n \in \mathbb{N}_0 \quad \sigma(n) \in \mathbb{N}_0$, dabei heißt $\sigma(n)$ der Nachfolger von n

(3) $\forall n \in \mathbb{N}_0 \quad 0 \neq \sigma(n)$ (0 ist kein Nachfolger)

(4) $\forall m, n \in \mathbb{N}_0 \quad m \neq n \Rightarrow \sigma(m) \neq \sigma(n)$ (die Kette der Nachfolger besitzt keine Verzweigung)

(5) $\forall M \subseteq \mathbb{N}_0 \quad (0 \in M) \wedge (\forall n \in M \text{ gilt } \sigma(n) \in M) \Rightarrow M = \mathbb{N}_0$ (es gibt nur eine solche Kette von Nachfolgern der 0)

Lemma 3.2. (Nachfolger-Darstellung der natürlichen Zahlen): Die natürlichen Zahlen mit der 0 lassen sich wie folgt schreiben:

$$\mathbb{N}_0 = \{0, \sigma(0), \sigma(\sigma(0)), \ldots\}.$$

Definition 3.29. (Addition natürlicher Zahlen): Gegeben seien die natürlichen Zahlen $n, p \in \mathbb{N}_0$. Die Summe $n + p$ wird wie folgt rekursiv definiert:

(a) falls $p = 0$ ist $n + p = n$,

(b) $n + \sigma(p) := \sigma(n + p)$.

Beispiel:

$$\sigma(0) + \sigma(\sigma(0)) = \sigma(\sigma(0) + \sigma(0)) = \sigma(\sigma(\sigma(0) + 0))) = \sigma(\sigma(\sigma(0)))$$

Definition 3.30. (Eins):

$$1 := \sigma(0) \in \mathbb{N}_0$$

Die Menge der natürlichen Zahlen beginnend mit der 1 wird bezeichnet mit

$$\mathbb{N} := \mathbb{N}_0 \backslash \{0\}.$$

Satz 3.9. (Vollständige Induktion ohne Ordnungsrelation): Eine Aussage $A(n)$ ist wahr für alle natürlichen Zahlen $n \in \mathbb{N}_0$, falls gilt:

(a) Induktionsanfang: $A(0)$ ist wahr;

(b) Induktionsschluss: Aus der Induktionsannahme, dass $A(n)$ für ein beliebiges $n \in \mathbb{N}_0$ wahr ist, folgt dass $A(\sigma(n))$ wahr ist.

Satz 3.10. (Struktureigenschaften der natürlichen Zahlen bezüglich der Addition): Die Menge der natürlichen Zahlen $(\mathbb{N}_0, +, 0)$ mit der Addition und der 0 als neutralem Element ist ein abelscher Monoid, d.h. es gilt:

(1) $\forall a, b, c \in \mathbb{N}_0$ gilt $a + (b + c) = (a + b) + c$,

(2) $\forall a, b \in \mathbb{N}_0$ gilt $a + b = b + a$,

(3) $\exists 0 \in \mathbb{N}_0\ \forall n \in \mathbb{N}_0$ gilt $n + 0 = n$.

Beweis: ad (1):
Beweis durch Induktion über $c \in \mathbb{N}_0$.
Induktionsanfang: $a + (b + 0) = a + b = (a + b) + 0$
Induktionsannahme: für ein $c \in \mathbb{N}$ gilt $a + (b + c) = (a + b) + c$
Induktionsschluss:

$$\begin{aligned} a + (b + \sigma(c)) &= a + \sigma(b + c) \\ &= \sigma(a + (b + c)) \\ &\overset{\text{Ind.-Ann.}}{=} \sigma((a + b) + c) \\ &= (a + b) + \sigma(c) \end{aligned}$$

ad (2):
Wir beweisen zunächst zwei Hilfsaussagen jeweils per vollständiger Induktion.
Behauptung 1: $\forall a \in \mathbb{N}$ gilt $a + 0 = 0 + a$.
Induktionsanfang: für $a = 0$ ist die Aussage offensichtlich wahr.
Induktionsvoraussetzung: für ein $a \in \mathbb{N}_0$ gilt $a + 0 = 0 + a$
Induktionsschluss:

$$0 + \sigma(a) = \sigma(0 + a) \overset{\text{Ind.-Ann.}}{=} \sigma(a + 0) = \sigma(a) = \sigma(a) + 0$$

Behauptung 2: $\forall a \in \mathbb{N}_0$ gilt $a + \sigma(0) = \sigma(0) + a$
Induktionsanfang: für $a = 0$ ist die Aussage wahr wegen Behauptung 1.
Induktionsvoraussetzung: für ein $a \in \mathbb{N}_0$ gilt $a + \sigma(0) = \sigma(0) + a$
Induktionsschluss:

$$\sigma(a) + \sigma(0) = (a + \sigma(0)) + \sigma(0) \overset{\text{Ind.-Ann.}}{=} \sigma(0) + (a + \sigma(0)) = \sigma(0) + \sigma(a).$$

Damit beweisen wir nun die Kommutativität ebenfalls per Induktion.
Induktionsanfang: für $b = 0$ gilt $a + 0 = 0 + a$ wegen Behauptung 1.
Induktionsannahme: für ein $b \in \mathbb{N}_0$ sei die Aussage $a + b = b + a$ wahr.
Induktionsschluss:

$$a + \sigma(b) = a + b + \sigma(0) \overset{\text{Ind.-Ann.}}{=} b + a + \sigma(0) \overset{\text{Beh.2}}{=} b + \sigma(0) + a = \sigma(b) + a.$$

ad (3): ergibt sich unmittelbar aus der Definition der Addition. □

Visite guidée: *Von dieser Stelle ab wird es in der Eingangshalle etwas ungenauer, denn nicht alle mathematischen Sätze werden bewiesen. Die Besucher sollen einen gewissen Eindruck bekommen, welche Eigenschaften die verwendeten Zahlenmengen besitzen. Was hier nicht bewiesen wird, wird entweder später nicht gebraucht oder in anderen Disziplinen der Mathematik auf andere Weise hergeleitet.*

Definition 3.31. (Multiplikation natürlicher Zahlen): Die **Multiplikation natürlicher Zahlen** ist eine zweistellige innere Verknüpfung $\cdot$ auf der Menge $\mathbb{N}_0$, die wie folgt rekursiv definiert wird: Für alle $m, n \in \mathbb{N}_0$ gilt:

(a) falls $m = 0$ ist $m \cdot n := 0$

(b) falls $m \neq 0$ ist $\sigma(m) \cdot n := (m \cdot n) + n$

Beispiel:

$$\begin{aligned} \sigma(\sigma(0)) \cdot \sigma(\sigma(0)) &= (\sigma(0) \cdot \sigma(\sigma(0))) + \sigma(\sigma(0)) \\ &= (0 \cdot \sigma(\sigma(0))) + \sigma(\sigma(0)) + \sigma(\sigma(0)) \\ &= \sigma(\sigma(0)) + \sigma(\sigma(0)) \\ &= \sigma(\sigma(\sigma(\sigma(0)))) \end{aligned}$$

Definition 3.32. (Ganze Zahlen): Die Menge der **ganzen Zahlen** $\mathbb{Z}$ lautet:

$$\mathbb{Z} := \mathbb{N} \cup \{-a \,|\, a \in \mathbb{N}_0\}.$$

Dabei ist für ein $a \in \mathbb{N}_0$ die Zahl $-a$ das Inverse von a bezüglich der Addition, also

$$a + (-a) = 0.$$

Satz 3.11. (Ringeigenschaft der ganzen Zahlen): Die Menge $(\mathbb{Z}, +, \cdot)$ ist ein abelscher Ring. Insbesondere ist:

(1) $(\mathbb{Z}, +, 0, -)$ eine abelsche Gruppe,

(2) $(\mathbb{Z}, \cdot, 1)$ ein abelscher Monoid und

(3) $\forall x, y, z \in \mathbb{Z}$ gilt $x(y + z) = xy + xz$.

Definition 3.33. (Kleiner-als-Relation auf den ganzen Zahlen): Seien $a, b \in \mathbb{Z}$. Man sagt

$$\begin{array}{rcl} a \text{ ist kleiner als } b, \text{ in Zeichen} & a & < \; b, \text{ falls gilt:} \\ \exists\, n \in \mathbb{N}, \text{ so dass} & a + n & = \; b. \end{array}$$

Satz 3.12. (Strenge Totalordnung der ganzen Zahlen): Mit der Ordnungsrelation '$<$' besitzt $\mathbb{Z}$ eine strenge Totalordnung. Insbesondere gilt:

(1) $\forall a, b, c \in \mathbb{Z} \quad (a < b) \wedge (b < c) \Rightarrow (a < c)$ Transitivität

(2) $\forall a, b \in \mathbb{Z}\ (a < b) \dot{\vee} (a = b) \dot{\vee} (b < a)$ (Trichotomie)

3.5.1 Summen- und Produktsymbol, Potenzgesetze für ganzzahlige Exponenten

Bei den Ring- und Körpereigenschaften in Abschnitt 3.4 standen die natürlichen und ganzen Zahlen noch nicht zur Verfügung. Daher konnten wir dort Summen- und Produktsymbol sowie die Potenzgesetze nicht darstellen. Das soll nun nachgeholt werden.

Definition 3.34. (Summen- und Produktsymbol): Sei R ein Ring, sei $n \in \mathbb{N}$ und seien $a_i \in R$ für alle $i \in \{1, \ldots, n\} \subset \mathbb{N}$. Dann lassen sich die Summe

(bzw. das Produkt) der a_i wie folgt abgekürzt schreiben:

$$\sum_{i=1}^{n} a_i := a_1 + \ldots + a_n$$
$$\prod_{i=1}^{n} a_i := a_1 \cdot \ldots \cdot a_n.$$

Erlaubt man, dass der Laufindex i von 1 bis 0 läuft, so führt das auf die Definition der **leeren Summe** bwz. des **leeren Produkts**:

$$\sum_{i=1}^{0} a_i \left[= \sum_{i \in \emptyset} a_i\right] := 0$$
$$\prod_{i=1}^{0} a_i \left[= \prod_{i \in \emptyset} a_i\right] := 1.$$

Definition 3.35. (Potenz): Seien $(\mathbb{K}, +, \cdot)$ ein Körper, $a \in \mathbb{K}$ und $n \in \mathbb{N}_0$. Dann heißt

$$a^n := \prod_{i=1}^{n} a = \underbrace{a \cdot \ldots \cdot a}_{n \text{ mal}}.$$

die n-te **Potenz** von a. Insbesondere ist $a^0 = 1$.

Für $b \in \mathbb{K}\backslash\{0\}$ definiere

$$b^{-n} := \frac{1}{b^n}.$$

Satz 3.13. (Potenzgesetze für ganzzahlige Exponenten): Seien $a, b \in \mathbb{K}\backslash\{0\}$ und $m, n \in \mathbb{Z}$. Dann gilt:

(a) $a^m\, a^n = a^{m+n}$

(b) $(a^m)^n = a^{m\,n}$

(c) $a^n\, b^n = (a\, b)^n$

(d) $\frac{a^m}{a^n} = a^{m-n}$

(e) $\frac{a^n}{b^n} = (\frac{a}{b})^n$

3.5.2 Einige Eigenschaften natürlicher und ganzer Zahlen

Da nun die natürlichen und Zahlen eingeführt sind und auch die Ordnungsrelation '$\leq$' zur Verfügung steht, können eine wichtige Eigenschaften natürlicher und ganzer Zahlen aufgeführt werden. Zum Beweis dieser Aussagen

benötigen wir das Prinzip der vollständigen Induktion unter Verwendung der Ordnungsrelation.

Satz 3.14. (Vollständige Induktion): Sei $n_0 \in \mathbb{N}_0$ fest gewählt. Eine Aussage $A(n)$ ist wahr für alle natürlichen Zahlen $n \in \mathbb{N}_0$ mit $n \geq n_0$, falls gilt:

(a) Induktionsanfang: $A(n_0)$ ist wahr

(b) Induktionsschluss: Aus der Induktionsannahme, dass $A(n)$ für ein beliebiges $n \in \mathbb{N}_0$ mit $n \geq n_0$wahr ist, folgt dass $A(n+1)$ wahr ist.

Lemma 3.3. (Spezielle Summen): Für alle $n \in \mathbb{N}_0$ gilt:

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

Beweis: Beweis durch vollständige Induktion.
Induktionsanfang: Für $n = 0$ gilt die Aussage:

$$\sum_{k=0}^{0} k = 0 = \frac{1}{2}\, 0 \cdot 1.$$

Induktionsvoraussetzung: Für $n \in \mathbb{N}_0$ sei die Aussage

$$\sum_{k=0}^{n} k = \frac{1}{2}\, n\,(n+1) \quad \text{wahr.}$$

Induktionsschluss: Dann gilt

$$\begin{aligned} \sum_{k=0}^{n+1} k &= \sum_{k=0}^{n} k + (n+1) \overset{\text{Ind.-vor.}}{=} \frac{1}{2}\, n\,(n+1) + (n+1) \\ &= \frac{1}{2}\, n\,(n+1) + \frac{1}{2}\,(n+1) + \frac{1}{2}\,(n+1) = \frac{1}{2}\,(n+1+1)\,(n+1). \end{aligned}$$

□

Visite guidée: Hier kommen nach und nach noch einige weitere Aussagen über natürliche und ganze Zahlen, die wir in allen Disziplinen der Mathematik brauchen werden.

3.6 Rationale Zahlen

Definition 3.36. (Relation zwischen Paaren ganzer Zahlen): Seien $(x, y), (x', y') \in \mathbb{Z} \times \mathbb{Z}\backslash\{0\}$. Definiere Relation $\underset{A}{\sim}$ wie folgt:

$$(x, y) \underset{A}{\sim} (x', y') \quad :\Longleftrightarrow \quad x\, y' = y\, x'$$

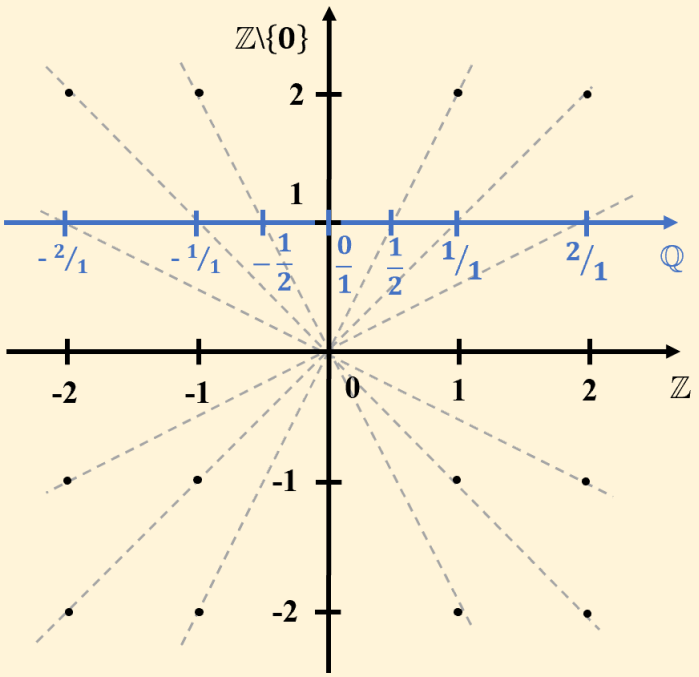

Abbildung 2: Konstruktion der rationalen Zahlen

Lemma 3.4. (Äquivalenzrelation A): $\underset{A}{\sim}$ ist Äquivalenzrelation auf $\mathbb{Z}\times\mathbb{Z}\backslash\{0\}$.

Definition 3.37. (Rationale Zahlen): $\mathbb{Q}$ ist die Menge aller Äquivalenzklassen bezüglich der Relation $\underset{A}{\sim}$ über der Menge $\mathbb{Z}\times\mathbb{Z}\backslash\{0\}$, wobei die Bruchschreibweise verwendet wird. Genauer:

$$\begin{aligned}\mathbb{Q} := (\mathbb{Z}\times\mathbb{Z}\backslash\{0\})\,/_{\underset{A}{\sim}} &= \{\frac{x}{y} := [(x,y)]_{\underset{A}{\sim}} \mid x\in\mathbb{Z}\wedge y\in\mathbb{Z}\backslash\{0\}\},\\ &\quad \text{wobei für } x\in\mathbb{Z} \text{ und } y\in\mathbb{Z}\backslash\{0\}\\ [(x,y)]_{\underset{A}{\sim}} &= \{(x',y')\in\mathbb{Z}\times\mathbb{Z}\backslash\{0\} \mid x\,y' = y\,x'\}.\end{aligned}$$

Zur Veranschaulichung der Konstruktion der rationalen Zahlen gemäß Definition 3.37 stellen wir das kartesische Produkt $\mathbb{Z}\times\mathbb{Z}\backslash\{0\}$ in einem kartesischen Koordinatensystem in Abbildung 2 dar. Den geordneten Zahlenpaaren (x,y) entsprechen die markierten Punkte in der Ebene. Zahlenpaare, die zueinander äquivalent sind im Sinne der Relation $\underset{A}{\sim}$ liegen auf Ursprungsgeraden, die wir gestrichelt dargestellt haben. Dort wo diese Ursprungsgeraden die $(x,1)$-Achse treffen, liegen die „gekürzten“ Repräsentanten der gesuchten Quotientenmenge $\mathbb{Q} := (\mathbb{Z}\times\mathbb{Z}\backslash\{0\})\,/_{\underset{A}{\sim}}$.

Satz 3.15. (Körpereigenschaften der rationalen Zahlen): Die Menge $(\mathbb{Q}, +, \cdot)$ mit den Verknüpfungen Addition $(\mathbb{Q}, +, 0, -)$ und Multiplikation $(\mathbb{Q}\backslash\{0\}, \cdot, 1, ^{-1})$ ist ein Körper.


Visite guidée: *Hier fehlen noch Aussagen zur Teilbarkeit. Erst dann lässt sich ein Stellenwertsystem konstruieren, z.B. mit dem Horner-Schema.*

Definition 3.38. (Stellenwertsystem): Sei $g \in \backslash\{0\}$. Eine natürliche Zahl $n \in \mathbb{N}$ lässt sich in einem **Stellenwertsystem zur Basis** g, oder g-adischen System, wie folgt darstellen:

$$[a_{n-1}a_{n-2}\dots a_1a_0]_g := \sum_{i=1}^{n-1} a_i \cdot g^i = n.$$

Die a_i werden **Ziffern** genannt. Für $g \leq 10$ sind die Ziffern $a_i \in \{0, 1, \dots, g-1\}$. Für $g = 16$ ist der Ziffernvorrat aus $\{0, 1, \dots, 9, A, B, C, D, E, F\}$. Abhängig von dem Wert von G tragen die Stellenwertsysteme folgende Namen: $g = 2$ Dualsystem, $g = 10$ Dezimalsystem, $g = 16$ Hexadezimalsystem.

3.7 Ausblick auf die reellen Zahlen

Visite guidée: *Nun folgt ein Ausblick auf die Analysis. Dieser Bereich ist nur für solche Besucher geeignet, die keine Angst vor Irrationalität und Transzendenz haben.*

In diesem Abschnitt unterstellen wir, dass die reellen Zahlen $\mathbb{R}$ bekannt seien. Es geht hier um einen Ausblick darauf, wodurch sich die reellen und rationalen Zahlen unterscheiden. Vgl. Deiser Analysis 1 [1], S. 15–29.

Definition 3.39. (Wurzel aus 2): Die Lösung der Gleichung

$$d^2 = 2$$

bezeichnen wir mit $\sqrt{2}$, in Worten: **Wurzel aus 2**.

d lässt sich als die Länge der Diagonalen eines Quadrats der Seitenlänge 1 interpretieren. Mit Zirkel und Lineal können wir die Länge d auf unserem Zahlenstrahl abtragen.

Dass die resultierende Zahl $\sqrt{2}$ existiert, werden wir in der Analysis sehen. Im Augenblick wollen wir annehmen, dass diese Zahl existiert und fragen uns, zu welcher Zahlenmenge sie gehört.

Lemma 3.5. (Ganzzahliges Quadrat und seine Teilbarkeit durch 2): Sei $a^2 \in \mathbb{Z}^+\backslash\{0\}$ gerade (d.h. durch 2 ohne Rest teilbar), dann ist auch a eine gerade Zahl.

Beweis: Angenommen a wäre ungerade. Dann existierte ein $k \in \mathbb{N}$ mit

$$\begin{aligned} & a &=& 2\,k+1 \\ \Rightarrow \quad & a^2 &=& 4\,k^2+4\,k+1 \end{aligned}$$

Damit ist a^2 ungerade. $\lightning$

Satz 3.16. (Irrationalität von Wurzel 2):

$$\sqrt{2} \notin \mathbb{Q}.$$

Den folgenden Beweis habe ich in meinem Schulunterricht zum ersten Mal gesehen. Ich bin nach wie vor fasziniert von der eigentümlichen Einfachheit und Tiefe dieses Widerspruchsbeweises.

Beweis: Angenommen, $\sqrt{2} \in \mathbb{Q}$, dann ließe sich $\sqrt{2}$ als gekürzter Bruch aus zwei ganzen Zahlen a und b darstellen:

$$\begin{aligned} & \sqrt{2} &=& \frac{a}{b} \\ \Rightarrow \quad & a^2 &=& 2\,b^2 \end{aligned}$$

$2\,b^2$ ist gerade, also ist auch a^2 gerade. Nach Lemma 3.5 muss auch a gerade sein. Demnach existiert eine Zahl $k \in \mathbb{N}$ mit

$$\begin{aligned} & a &=& 2\,k \\ \Rightarrow \quad & a^2 &=& 4\,k^2 = 2\,b^2 \\ \Rightarrow \quad & 2\,k^2 &=& b^2 \end{aligned}$$

Demnach ist b^2 gerade, wiederum nach Lemma 3.5 muss auch b gerade sein. Da a und b gerade sind, ließe sich der Bruch $\frac{a}{b}$ durch 2 kürzen. $\lightning$

Satz 3.17. (Satz von Gauss): Seien $k \in \mathbb{N}$, $a_0, \ldots, a_{k-1} \in \mathbb{Z}$, $x \in \mathbb{R}$ und es gelte

$$x^k + a_{k-1}\,x^{k-1} + \ldots + a_1\,x + a_0 = 0.$$

Dann ist entweder $x \in \mathbb{Z}$ oder $x \in \mathbb{R}\backslash\mathbb{Q}$ (irrational).

Beweisskizze: Dass x irrational sein kann, sieht schon an dem einfachen Beispiel $x^2 - 2 = 0$. Bleibt also zu zeigen: Falls x eine rationale Zahl der Form $\frac{l}{n}$ ist, dann muss der Nenner $n = 1$ sein. Beim Beweis davon setzt man oBdA voraus, dass l und n teilerfremd sind und führt dies (analog zum Beweis der Irrationalität von $\sqrt{2}$) zum Widerspruch.

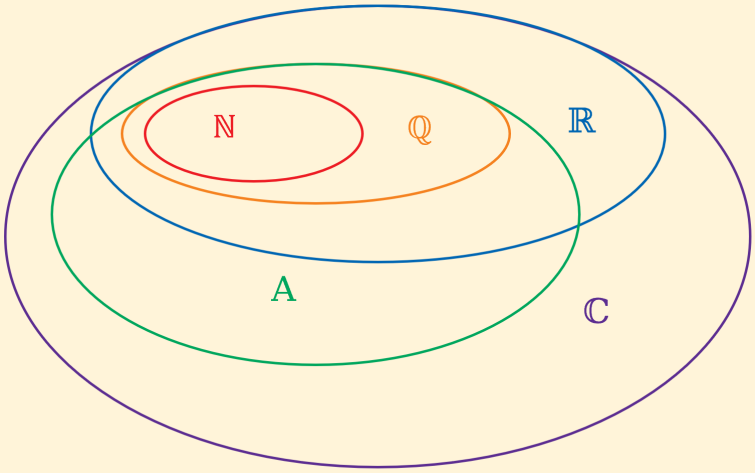

Abbildung 3: Wichtige Teilmengen von $\mathbb{C}$

Definition 3.40. (Algebraische Zahlen): Eine reelle Zahl x heißt **algebraisch**, wenn es $a_0, \ldots, a_k \in \mathbb{Q},\ a_k \neq 0$ gibt, so dass gilt:

$$a_k\, x^k + a_{k-1}\, x^{k-1} + \ldots + a_1\, x + a_0 = 0.$$

Die Menge der so definierten algebraischen Zahlen wird mit $\mathbb{A}$ gekennzeichnet.

Bringt man die rationalen Koeffizienten a_i auf einen Hauptnenner und multipliziert mit diesem das Polynom, so ergibt sich, dass man in der Definition anstelle der rationalen Koeffizienten auch ganzzahlige Koeffizienten hätte fordern können. Die algebraischen Zahlen sind also die Nullstellen der Polynome mit ganzzahligen Koeffizienten und umfassen nicht nur die rationalen Zahlen, sondern eben auch eine gewisse Menge der irrationalen Zahlen. Das sind insbesondere die reellen n-ten Wurzeln und [vermutlich!] die rationalen Linearkombinationen daraus.

In Abbildung 3 sind verschiedene Teilmengenbeziehungen der hier diskutierten Zahlenmengen skizziert. Die dabei zugrunde gelegte Definition der algebraischen Zahlen ist etwas allgemeiner und lässt imaginäre Lösungen der Polynome mit ganzzahligen Koeffizienten zu.

Mit den (reellen) algebraischen Zahlen ist unser Zahlenstrahl aber immer noch nicht „vollständig“. Denn es existieren noch transzendente Zahlen, wie die Zahl π. Das Abrollen des Einheitskreises beginnend am Ursprung des Zahlenstrahls, trifft nach einer Umdrehung auf ein „Loch“ im algebraischen

Zahlenstrahl bei 2π. Die Definition der transzendenten Zahlen ist präzise, aber nicht besonders inspirierend:

Definition 3.41. (Transzendente Zahlen): Eine reelle Zahl heißt **transzendent**, wenn sie nicht algebraisch ist.

Ein sehr mächtiger Satz über transzendente Zahlen, der in den Jahren 1934/35 bewiesen wurde und Hilberts 7. Problem löst, lautet wie folgt:

Satz 3.18. (Gelfond-Schneider): Seien $a \in \mathbb{A}^+ \backslash \{1\}$ und $b \in \mathbb{A}$ irrational. Dann ist a^b transzendent.

Beispiel: $\sqrt{2}^{\sqrt{2}}$ ist eine transzendente Zahl.

3.8 Eigenschaften unendlicher Mengen

Visite guidée: *In diesem Abschnitt geht es um Unendlichkeit, nur etwas für Besucher mit starken Nerven und vor allem großer Ausdauer. Hier ist auch die Rezeption zu Hilberts Hotel. Alle Besucher seien davor gewarnt, in das Hotel einzuchecken. Die Zimmer sind äußerst klein und es herrscht fortwährend Hektik durch ständigen Zimmertausch.*

Definition 3.42. (Mächtigkeit einer Menge): Sei M eine Menge.

1. Besitzt M endlich viele (n) Elemente, so versteht man unter der **Mächtigkeit** oder **Kardinalität** von M die Anzahl ihrer Elemente, in Zeichen $|M| = n$.
2. Besitzt M unendlich viele Elemente, dann ist die Mächtigkeit von M unendlich: $|M| = \infty$. Mengen mit dieser Eigenschaft werden auch **unendliche Mengen** genannt.
3. Die Mächtigkeit der leeren Menge ist Null: $|\emptyset| = 0$.

Gedankenexperiment: das Hilbertsche Hotel

Das Hilbertsche Hotel hat unendlich viele Zimmer mit den Zimmernummern 1, 2, ... Alle Zimmer des Hotels sind belegt. Kommt ein neuer Gast in das Hotel, rücken alle alten Gäste um ein Zimmer weiter, also der Gast aus dem Zimmer n zieht um in das Zimmer $n+1$ für alle n. Dadurch wird Zimmer Nr. 1 frei und der neue Gast kann einziehen. Kommt ein Bus mit unendlich vielen neuen Gästen g_1, g_2, ... an, so ziehen alle alten Gäste jeweils in das Zimmer mit der doppelten Zimmernummer um, also für alle n gilt: Umzug aus dem Zimmer n in das Zimmer $2n$. Dadurch werden die Zimmer 1, 3, 5, ... frei für die neuen Gäste.

Definition 3.43. (Abzählbar unendliche Mengen): Eine Menge M heißt **abzählbar unendlich,** falls es eine bijektive Abbildung $f : \mathbb{N} \to M$ gibt. Schreibweise: $|M| = |\mathbb{N}|$, Sprechweise: die Mächtigkeit der Menge M ist gleich der Mächtigkeit der Menge $\mathbb{N}$.

Beispiel: Beispiele: $|\mathbb{N}_0| = |\mathbb{N}|$, $|\mathbb{Z}| = |\mathbb{N}|$.

Definition 3.44. (abzählbare Mengen): Eine Menge M heißt **abzählbar,** wenn sie endlich ist oder abzählbar unendlich. Schreibweise: $|M| \leq |\mathbb{N}|$.

Satz 3.19. (Abzählbarkeit der rationalen Zahlen): Es gilt: $|\mathbb{Q}| = |\mathbb{N}|$.

Beweisidee (Cantors erstes Diagonalargument, vlg. [11]): Man schreibt sämtliche möglichen Brüche (also die rationalen Zahlen) auf nach folgendem Schema:

$$\begin{array}{cccc} \frac{1}{1} & \frac{1}{2} & \frac{1}{3} & \dots \\ \frac{2}{1} & \frac{2}{2} & \frac{2}{3} & \dots \\ \frac{3}{1} & \frac{3}{2} & \frac{3}{3} & \\ \vdots & \vdots & \vdots & \end{array}$$

und läuft diese Zahlen in diagonalen Streifen ab, wobei man nicht vollständig gekürzte Brüche überspringt: $\frac{1}{1}$, $\frac{1}{2}$, $\frac{2}{1}$, $\frac{3}{1}$, $\frac{1}{3}$, ... Es entsteht eine Folge, die alle rationalen Zahlen enthält und die eine Bijektion $\mathbb{N} \to \mathbb{Q}$ repräsentiert.

Satz 3.20. (Abzählbarkeit der algebraischen Zahlen): Es gilt: $|\mathbb{A}| = |\mathbb{N}|$.

Beweisidee: Die algebraischen Zahlen sind (reelle) Lösungen der Polynome k-ten Grades mit rationalen Koeffizienten. Zu jedem $k \in \mathbb{N}$ findet man eine abzählbare Menge von Polynomen, da die Menge der rationalen Zahlen abzählbar ist. Auf diese Weise kann man alle diese Polynome durchzählen. Macht man sich klar, dass jedes dieser Polynome k-ten Grades maximal k reelle Nullstellen haben kann, wird deutlich, dass alles abzählbar sein muss.

Satz 3.21. (Überabzählbarkeit der reellen Zahlen): Die Menge der reellen Zahlen ist nicht abzählbar.

Beweisidee (Cantors zweites Diagonalargument, vlg. [12], [1] S.26f): Man geht davon aus, dass man jede reelle Zahl in einer (ggf. unendlichen, nicht periodischen) Dezimalbruchdarstellung darstellen kann. Angenommen, $\mathbb{R}$ wäre abzählbar. Dann wäre auch das reelle Intervall $[0, 1[\subset \mathbb{R}$ abzählbar und es gäbe eine abzählbar unendliche Folge x_1, x_2, ... von reellen Zahlen, die alle Zahlen in diesem Intervall enthält.

Nun konstruiert man eine Zahl x in Dezimalbruchdarstellung mit einer 0 vor dem Komma und so, dass ihre erste Stelle nach dem Komma von derjenigen von x_1 abweicht, ihre zweite Stelle nach dem Komma von derjenigen von x_2 abweicht u.s.w. Diese Zahl x ist eine reelle Zahl aus dem Intervall $[0, 1[$, ist jedoch per Konstruktion nicht in der Folge x_1, x_2, ... enthaltenen $\lightning$.

Da die Menge $\mathbb{A}$ abzählbar ist, muss die Menge der transzendenten Zahlen $\mathbb{R} - \mathbb{A}$ überabzählbar groß sein.

Satz 3.22. (Cantor-Bernstein): Seien M und N Mengen mit den Eigenschaften $|M| \leq |N|$ und $|N| \leq |M|$. Dann gilt $|M| = |N|$.

Satz 3.23. (Vergleichbarkeit von Mächtigkeiten): Für alle Mengen M, N gilt: $|M| \leq |N|$ oder $|N| \leq |M|$.

Satz 3.24. (Mächtigkeit der reellen Zahlen): Es gilt: $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$

Beweisidee: Man verwendet Dualbruchdarstellungen und kann so z.B. die reelle Zahl $0,010011\ldots$ durch folgende Menge darstellen: $\{2, 5, 6, \ldots\} \in \mathcal{P}(\mathbb{N})$. Auf diese Weise müsste sich eine Bijektion $[0, 1[\to \mathcal{P}(\mathbb{N})$ konstruieren lassen.

Satz 3.25. (Satz von Cantor): Sei M eine beliebige Menge. Dann gilt $|M| < |\mathcal{P}(M)|$.

Mit diesem Satz lassen sich die Mächtigkeiten wie folgt gruppieren:

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| = |\mathbb{R}| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| = |\mathcal{P}(\mathbb{R})| = \{f | f : \mathbb{R} \to \mathbb{R}\}.$$

Literatur

[1] Oliver Deiser. *Analysis 1*. Oliver Deiser, 22.10.2018 edition, 2018. http://www.aleph1.info/?call=Puc&permalink=analysis1.

[2] Oliver Deiser. *Einführung in die Mengenlehre*. Oliver Deiser, 19.09.2018 edition, 2018. http://www.aleph1.info/?call=Puc&permalink=mengenlehre1.

[3] Oliver Deiser. *Grundbegriffe der Mathematik*. Oliver Deiser, 19.09.2018 edition, 2018. http://www.aleph1.info/?call=Puc&permalink=grundbegriffe.

[4] David Hilbert. *Grundzüge der theoretischen Logik*. Springer-Verlag, Berlin, 6 edition, 1972.

[5] Helmut Koch. *Einführung in die Mathematik*. Springer, Berlin, 2 edition, 2004.

[6] Christian Spannagel. Youttube, mathematische grundlagen, Zugriff 08/2020. https://www.youtube.com/watch?v=73ZxJ_NIXUY&list=PLKEOoDyOnlIp7w4xFSrksET3dBsWZTg_7.

[7] Web Wikipedia. Gleichheit (mathematik), Zugriff 07/2020. https://de.wikipedia.org/wiki/Gleichheit_(Mathematik).

[8] Web Wikipedia. Prädikat (logik), Zugriff 07/2020. https://de.wikipedia.org/wiki/Pr%C3%A4dikat_(Logik).

[9] Web Wikipedia. Quantifizierung (logik), Zugriff 07/2020. https://de.wikipedia.org/wiki/Quantifizierung_(Logik).

[10] Web Wikipedia. Variable (logik), Zugriff 07/2020. https://de.wikipedia.org/wiki/Variable_(Logik).

[11] Web Wikipedia. Cantors erstes diagonalargument, Zugriff 08/2019. https://de.wikipedia.org/wiki/Cantors_erstes_Diagonalargument.

[12] Web Wikipedia. Cantors zweites diagonalargument, Zugriff 08/2019. https://de.wikipedia.org/wiki/Cantors_zweites_Diagonalargument.