VORKURS FÜR MATHEMATIK

MORITZ WEBER

Abstract. Der Vorkurs besteht aus sechs Vorlesungen (jeweils 90 Minuten) plus Übungen (eine Übungssitzung je Vorlesung). Ziel des Vorkurses ist es weniger, konkrete mathematische Inhalte zu vermitteln, als vielmehr an bestimmte Prinzipien des mathematischen Denkens und Arbeitens sowie des Mathematikstudiums heranzuführen und so den Übergang von schulischem Lernen zu universitärem Lernen zu erleichtern.

Contents

Date: October 2, 2024.

Philosophie und Organisation des Vorkurses

Abstract. In diesem Kapitel stellen wir die grundlegenden Ideen vor, die im Vorkurs vermittelt werden sollen. Zudem skizzieren wir die Organisation des Kurses.

Ziele des Vorkurses. Ziel des Vorkurses ist es weniger, konkrete mathematische Inhalte zu vermitteln, als vielmehr an bestimmte Prinzipien des mathematischen Denkens und Arbeitens sowie des Mathematikstudiums heranzuführen und so den Übergang von schulischem Lernen zu universitärem Lernen zu erleichtern. Insbesondere sollen folgende Aspekte anklingen:

(1) Heuristiken bei der Findung von Beweisen:
   (a) vorwärts (von den Annahmen ausgehend schlussfolgern)
   (b) rückwärts (von der finalen Aussage her sich zu den nötigen Annahmen durchhangeln)
   (c) zerlegen (Beweis in grobe Schritte zerlegen und dann verfeinern)
(2) Beweisprinzipien:
   (a) direkter Beweis
   (b) Kontraposition
   (c) Beweis durch Widerspruch
   (d) Unterschied zwischen Gegenbeispiel und Beispiel
   (e) vollständige Induktion
(3) Mathematische Techniken/Charakteristika:
   (a) Unterschied zwischen Implikation und Äquivalenz(umformung)
   (b) axiomatische Methoden (Begriffe axiomatisch definieren)
   (c) Loslösen von der Anschauung/Abstrahieren
   (d) über Analyse von Beispielen zu allgemeiner Aussage kommen
   (e) Verallgemeinern von Resultaten
   (f) relative Aussagen/Theoreme (wenn A dann B)

Themen des Vorkurses. Wie oben erwähnt, stehen die mathematischen Inhalte nicht im Vordergrund bei der Gestaltung des Vorkurses. Vielmehr soll anhand mathematischer Sachverhalte exemplarisch auf obige Aspekte (Heuristik, Beweisprinzipien, mathematische Techniken) eingegangen werden. Folgende Themen werden behandelt:

(1) Vorlesung 1: Logik, Mengenlehre, Beweisprinzipien
(2) Vorlesung 2: Funktionen und Techniken jenseits der Anschauung
(3) Vorlesung 3: Mittelwerte, Funktionen als Objekte, parametrisierte Familien
(4) Vorlesung 4: Zahlen, Irrationalität, Mächtigkeit
(5) Vorlesung 5: Gruppen
(6) Vorlesung 6: Inzidenzgeometrie

Organisation des Vorkurses. Der Vorkurs ist wie folgt organisiert:

- Beginn: Mitte September eines Jahres
- 6 Vorlesungstermine (jeweils 90 Minuten), gestreckt über 3 Wochen
- 6 Übungsgruppentermine (jeweils 90 Minuten), um eine Woche verschoben in Bezug auf die Vorlesungstermine; jedem Vorlesungstermin ist ein Übungsgruppentermin eine Woche später zugeordnet
- die Vorlesungen sind thematisch weitgehend unabhängig voneinander
- Am Ende einer jeden Vorlesungssitzung wird ein Übungsblatt ausgegeben, das dann innerhalb von einer Woche bearbeitet werden soll; es wird in den Übungen besprochen; eine Korrektur und eine Bepunktung durch die Übungsleiter:innen findet nicht statt

1. Logik, Mengenlehre, Beweisprinzipien

Abstract. Wir beginnen mit der Aussagenlogik, der einer Aussage den Wahrheitsgehalt "wahr" oder "falsch" zuordnet. Wir lernen Negation, UND/ODER, Implikation und Äquivalenz kennen. Wir fertigen Wahrheitstafeln an.

Sodann beschäftigen wir uns mit Beweisprinzipien: Direkter Beweis, Kontraposition, Beweis durch Widerspruch, vollständige Induktion. Wir lernen den Unterschied zwischen einem Beispiel und einem Gegenbeispiel kennen. Wir denken auch über relative Aussagen (der Art "wenn A, dann B") nach.

Im dritten Abschnitt (optional) behandeln wir die naive Mengenlehre. Wir definieren Vereinigungen, Durchschnitte, Komplemente und Potenzmengen von Mengen und wir lernen die de Morganschen Regeln kennen. Wir diskutieren wann Abbildungen injektiv, surjektiv oder bijektiv sind.

Einführung. Willkommen an der Uni, willkommen im Mathematikstudium! Auch hier wird gelernt, aber vieles ist anders als an der Schule:

- Es wird mehr Stoff in kürzer Zeit behandelt, meist ohne Wiederholungen.
- Zum Einüben des Stoffes ist der Übungsbetrieb da, nicht die Vorlesung. In den Übungen werden selbstständig Aufgaben bearbeitet. Man hat dafür eine Woche Zeit. Die Abgaben werden dann von den Übungsgruppenleiter:innen korrigiert, bepunktet und zeitversetzt (meistens um 1-2 Wochen) in den Treffen der Übungsgruppe besprochen. Typischerweise müssen 50% der Gesamtpunktzahl erreicht werden, um zur Klausur zugelassen zu werden. Die Übungszettel dürfen in Gruppen bearbeitet und abgegeben werden, typischerweise zu zweit.
- In den Vorlesungen gibt es weniger Interaktion als in der Schule. Sie finden meistens im "Dozierstil" statt.
- Es wird von Ihnen mehr Eigenständigkeit eingefordert, Sie müssen Ihr Lernen mehr und mehr selbst organisieren. Schreiben Sie in den Vorlesungen mit!
- In den Vorlesungen werden oftmals wenige Beispiele und wenige konkrete "Rechnungen" behandelt. Der Fokus liegt mehr auf den Beweisen.
- Man macht viel coolere Mathematik!

Ein wesentlicher Unterschied zwischen der Beschäftigung mit der Mathematik in der Schule einerseits und an der Universität andererseits liegt im Stellenwert der Beweise. Aussagen zu beweisen macht den Großteil der mathematischen Vorlesungen an der Universität aus. Warum spielen Beweise eine so große Rolle? Weil wir an der Uni **nicht nur wissen wollen, *dass* etwas wahr ist, sondern auch *warum***. Wir wollen verstehen, warum ein Sachverhalt aus zwingend logischen Gründen gilt und wir akzeptieren keine empirische Evidenz.

Beispiel 1.1 (Riemannsche Hypothese/Vermutung)**.** Im Jahr 1859 stellte Bernhard Riemann eine berühmte Vermutung zu Primzahlen auf. Dazu betrachtete er die

Riemannsche Zeta-Funktion

$$\zeta(s) := \prod_{p \text{ ist Primzahl}} \frac{1}{1-p^{-s}}, \qquad s \in \mathbb{C}.$$

Seine Vermutung war: Ist $\zeta(s) = 0$, so ist $s \in -2\mathbb{N}$ oder $\mathrm{Re}(s) = \frac{1}{2}$. Mit anderen Worten: "Die nichttrivialen Nullstellen der Zeta-Funktion haben alle Realteil $\frac{1}{2}$."

Jetzt wissen Sie vielleicht noch nicht, was eine Primzahl ist, was eine komplexe Zahl $s \in \mathbb{C}$ ist oder was deren Realteil $\mathrm{Re}(s)$ ist, aber der Punkt in diesem Beispiel ist: Mit Hilfe des Computers konnten unzählige Nullstellen der Zeta-Funktion überprüft werden (Stand 2021: einige Billionen) und die Vermutung wurde nie widerlegt. Aus empirischer Sicht könnte man also einigermaßen zufrieden festhalten, *dass* die Riemannsche Hypothese wahr sein sollte. Doch Mathematiker fragen sich dennoch: *Warum* sollte sie denn wahr sein, wie können wir *beweisen*, dass die Riemannsche Hypothese wahr ist? Zur Lösung des Problems hat das Clay Mathematics Institute ein Preisgeld von einer Million Dollar ausgeschrieben; das Problem ist eines der sieben Milleniumsprobleme, von denen sechs noch immer ungelöst sind.

In diesem Vorkurs werden wir verschiedene Beweisprinzipien kennenlernen sowie andere Charakteristika des Mathestudiums diskutieren.

1.1. **Aussagenlogik.** In der Mathematik beschäftigen wir uns mit Aussagen A, B, C, ... Diese können entweder wahr (w) oder falsch (f) sein, nicht aber beides gleichzeitig. Wir nennen dies den *Wahrheitswert* einer Aussage. Sind eine oder mehrere Aussagen gegeben, können wir diese zu neuen Aussagen verknüpfen, mit Hilfe von *Wahrheitstabellen*.

Definition 1.2. Seien A und B Aussagen. Wir definieren folgende Verknüpfungen mit Hilfe von Wahrheitstabellen, dh. wir weisen den neuen Aussagen einen Wahrheitswert in Abhängigkeit des Wahrheitswerts von A und B zu. Die Verknüpfungen

(a) *Negation* ("nicht A") $\neg A$,
(b) *Konjunktion* (oder *UND-Verknüpfung*, "A und B") $A \wedge B$,
(c) *Disjunktion* (oder *ODER-Verknüpfung*, "A oder B") $A \vee B$,
(d) *Implikation* ("aus A folgt B" oder "A impliziert B") $A \Rightarrow B$,
(e) *Äquivalenz* ("A ist äquivalent zu B" oder "A genau dann, wenn B") $A \Leftrightarrow B$

sind definiert durch die folgenden Wahrheitstabellen:

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \Longrightarrow B$	$A \Longleftrightarrow B$
w	w	f	w	w	w	w
w	f		f	w	f	f
f	w	w	f	w	w	f
f	f		f	f	w	w

Beispiel 1.3. Wir nehmen uns die Aussage $A \Rightarrow B$ vor und argumentieren nun anschaulich (also nicht rein formalistisch-logisch und – ehrlich gesagt auch etwas holprig). Wir nehmen dazu A als die Aussage "es regnet" und für B die Aussage "die Straße ist nass". Gibt es nun einen kausalen Zusammenhang zwischen diesen beiden Aussagen? Die Aussage $A \Rightarrow B$ ist also nun: "Wenn es regnet, ist die Straße nass" und wir interpretieren den Wahrheitswert von $A \Rightarrow B$ im Sinne von: Ist es plausibel, dass wir, gegeben bestimmter Wahrheitswerte von A und B, einen Zusammenhang $A \Rightarrow B$ haben können, oder nicht? Wir weisen $A \Rightarrow B$ also nun (anschaulichen) den Wahrheitswert wahr zu, wenn das gegebene Szenario von A und B einen Zusammenhang "A impliziert B" plausibel scheinen lässt – und den Wahrheitswert falsch andernfalls.

Wir überprüfen die vier Fälle der Wahrheitswerte und formulieren es sprachlich um (und vereinfachen dabei ein wenig: das Gegenteil von nass ist bei uns trocken etc.).

(a) Sind A und B wahr, so wäre die Aussage: Es hat geregnet und die Straße ist nass. Die Aussagen A und B scheinen also durchaus im Sinne von A impliziert B zusammenhängen zu können. Wahrheitswert: wahr.
(b) Ist A wahr und B falsch, so bedeutet dies: Es hat geregnet und die Straße ist trocken. Wenn dem wirklich so ist, kann es keinen kausalen Zusammenhang im Sinne $A \Rightarrow B$ geben, die Aussage $A \Rightarrow B$ bekommt also den Wert falsch.
(c) Ist A falsch, so ist uns der Wert von B egal, denn die Aussagen: "Es hat nicht geregnet, aber die Straße ist nass" lässt die Implikation $A \Rightarrow B$ ebenso zu, wie "Es hat nicht geregnet und die Straße ist trocken". In ersterem Fall könnte ja auch eine Wasserleitung oberhalb der Straße defekt sein und die Straße überfluten – eine nasse Straße kann ja auch andere Ursachen haben, als Regen. In beiden Fällen bekommt $A \Rightarrow B$ also den Wahrheitswert wahr.

Wir schlussfolgern also – in einer vielleicht etwas nicht ganz wasserdichten sprachlichen Anschauung –, dass die Wahrheitswerte von $A \Rightarrow B$ in dessen Definition sinnvoll gewählt sind. Insbesondere erkennen wir, dass aus etwas Falschem alles folgen kann. Dieses logische Phänomen wird mit *Ex falso quodlibet* bezeichnet. Für uns viel entscheidender ist jedoch, dass die in Definition 1.2 gegeben Definition von $A \Rightarrow B$ eine *Definition* ist – wir brauchen sie also nicht zu rechtfertigen oder zu begründen. Es ist eine rein formale Definition und wir bezeichnen diese Verknüpfung der Aussagen A und B eben als $A \Rightarrow B$ (wir hätten sie auch $A \heartsuit B$ oder $A \smile B$ nennen können).

Proposition 1.4 (Regeln für Verknüpfungen von Aussagen)**.** *Es gelten die folgenden Regeln für Verknüpfungen von Aussagen A, B und C.*

(a) *Die Aussage $A \wedge \neg A$ ist immer falsch.*
(b) *Die Aussage $A \vee \neg A$ ist immer wahr.*
(c) *Die Aussage $\neg(\neg A)$ ist äquivalent zur Aussage A, dh. $\neg(\neg A)$ und A haben immer den gleichen Wahrheitswert.*
(d) *Die Aussage $\neg(A \wedge B)$ ist äquivalent zur Aussage $(\neg A) \vee (\neg B)$.*

(e) *Die Aussage* $\neg(A \vee B)$ *ist äquivalent zur Aussage* $(\neg A) \wedge (\neg B)$.
(f) *Die Aussage* $(A \vee B) \wedge C$ *ist äquivalent zur Aussage* $(A \wedge C) \vee (B \wedge C)$.
(g) *Die Aussage* $(A \wedge B) \vee C$ *ist äquivalent zur Aussage* $(A \vee C) \wedge (B \vee C)$.
(h) *Die Aussage* $A \Rightarrow B$ *ist äquivalent zur Aussage* $(\neg A) \vee B$.
(i) *Die Aussage* $A \Rightarrow B$ *ist äquivalent zur Aussage* $(\neg B) \Rightarrow (\neg A)$.
(j) *Die Aussage* $A \Leftrightarrow B$ *ist äquivalent zur Aussage* $(A \Rightarrow B) \wedge (B \Rightarrow A)$.

Beweis. Ein Vergleich der Wahrheitstabellen liefert die Aussagen.

Ist beispielsweise A wahr, so ist $\neg A$ falsch – und also auch $A \wedge \neg A$, nach Definition der Konjunktion. Ist A hingegen falsch, so auch $A \wedge \neg A$. Von daher ist die Aussage $A \wedge \neg A$ immer falsch.

Teil (h) haben wir uns schon in Beispiel 1.3(e) überlegt. Formaler sehen wir, dass $A \Rightarrow B$ und $(\neg A) \vee B$ die gleichen Wahrheitstabellen haben:

A	B	$A \Longrightarrow B$	$(\neg A) \vee B$
w	w	w	w
w	f	f	f
f	w	w	w
f	f	w	w

Für Teil (i) kombinieren wir (h) und (c): Nach (h) ist "$(\neg B) \Rightarrow (\neg A)$" äquivalent zu "$(\neg(\neg B)) \vee (\neg A)$", was nach (c) wiederum zu "$B \vee (\neg A)$" äquivalent ist. Nach (h) ist dies äquivalent zu "$A \Rightarrow B$". (Hier müssten wir uns noch überlegen, dass die Operation $\vee$ kommutativ ist, dass also allgemein $A \vee B$ und $B \vee A$ äquivalent sind – ein Vergleich der Wahrheitstabellen bestätigt es.) □

Wir bemerken, dass wir die obige Proposition rein formal bewiesen haben: Um beispielsweise die Aussage (h) zu beweisen, brauchen wir nicht zu verstehen, was $A \Rightarrow B$ oder $\neg A \vee B$ eigentlich bedeutet – wir brauchen nur mechanisch den Regeln von Definition 1.2 zu folgen und die entsprechenden Wahrheitstafeln zu produzieren und zu vergleichen. Wir haben die Aussage also **formal bewiesen, ohne unsere Anschauung** zu Hilfe nehmen zu müssen.

1.2. **Beweisprinzip: direkter Beweis.** Im vorigen Abschnitt haben wir bereits einen ersten Beweis geführt. Welche Schemata von Beweisen gibt es?

Als erstes lernen wir den *direkten Beweis* ("$A \Rightarrow B$") kennen (auch der Beweis von Proposition 1.4 war ein direkter Beweis): Beweise Aussage B ausgehend von der Aussage A.

Lemma 1.5. *Sei* $n \in \mathbb{Z}$. *Ist* n *eine gerade Zahl, so auch* n^2.

Beweis. Sei n gerade. Es gibt also eine Zahl $k \in \mathbb{Z}$, so dass $n = 2k$. Dann ist

$$n^2 = (2k)^2 = 4k^2 = 2(2k^2)$$

also ebenfalls gerade. □

Gilt eigentlich auch die Umkehrung? Ja.

Lemma 1.6. *Sei $n \in \mathbb{Z}$. Ist n^2 eine gerade Zahl, so auch n.*

Beweis. Sei n^2 gerade. Es gibt also eine Zahl $k \in \mathbb{Z}$, so dass $n^2 = 2k$. Also wird n^2 von 2 geteilt. Da 2 eine Primzahl ist, teilt 2 daher auch n. Hier benutzen wir einen tiefen Satz aus der Zahlentheorie: Ist p eine Primzahl und teilt diese das Produkt ab, so teilt p entweder a oder b (möglicherweise auch beide). Also ist n gerade. □

Wir fassen die beiden Lemmata in eine Aussage zusammen.

Proposition 1.7. *Sei $n \in \mathbb{Z}$. Dann ist n gerade genau dann, wenn n^2 gerade ist.*

Beweis. Sei $n \in Z$. Nach Lemma 1.5 impliziert die Aussage "n ist gerade" die Aussage "n^2 ist gerade". Nach Lemma 1.6 gilt auch die umgekehrte Implikation. Nach Proposition 1.4(i) gilt also die Äquivalenz der beiden Aussagen. □

Wir haben eine **Äquivalenzaussage** "$A \Leftrightarrow B$" nach dem Prinzip "$A \Rightarrow B$ und $B \Rightarrow A$" gezeigt (Proposition 1.4(j)).

Wir beobachten, dass die Aussage "n ist gerade" in Wahrheit "2 teilt n" bedeutet (also: "n ist ein Vielfaches von 2"). Gilt die Aussage aus Lemma 1.5 vielleicht auch allgemeiner? Wir schauen uns zunächst ein paar Beispiele an.

Beispiel 1.8.
(a) Sei $n = 6$. Dann ist $n^2 = 36$. Dann wird n von 3 geteilt und ebenso n^2.
(b) Sei $n = 15$. Dann ist $n^2 = 225$. Dann wird n von 3 geteilt und n^2 ebenso ($225 = 3 \cdot 75$). Genauso wird n von 5 geteilt und n^2 ebenso.

Diese Beispiele bestärken uns darin, dass wir Lemma 1.5 möglicherweise verallgemeinern können. Dennoch geben wir uns nicht mit einer Ansammlung von Beispielen zufrieden, sondern nur mit einem Beweis. Hier ist er.

Lemma 1.9. *Seien a und n aus $\mathbb{Z}$. Wird n von a geteilt, so auch n^2.*

Beweis. Da n von a geteilt wird, gibt es ein $k \in \mathbb{Z}$, so dass $n = ak$. Dann ist

$$n^2 = (ak)^2 = a^2k^2 = a(ak^2).$$

Also ist auch n^2 ein Vielfaches von a und wird somit von a geteilt. □

Wir haben Lemma 1.5 **verallgemeinert**. Dabei wurden wir inspiriert von den Beispielen 1.8 – der formale Beweis stützt sich dann allerdings nicht bloß auf Beispiele.

Begeistert versuchen wir auch Lemma 1.6 zu verallgemeinern, stellen jedoch fest, dass es ein Gegenbeispiel gibt: Ist $n = 6$ und $a = 4$, so wird zwar $n^2 = 36$ von a geteilt, nicht aber n. Dieses Gegenbeispiel liefert den Beweis für folgende Aussage.

Lemma 1.10. *Seien a und n aus $\mathbb{Z}$. Wird n^2 von a geteilt, so nicht notwendigerweise auch n.*

Beweis. Mit $n = 6$ und $a = 4$ haben wir ein Gegenbeispiel für die Aussage A "Wird n^2 von a geteilt, so auch n". Die Aussage A ist daher falsch. □

Wir bemerken, dass es zwar Zahlen n und a gibt, so dass sowohl n^2 als auch n von a geteilt werden (siehe z.B. Lemma 1.5), aber im Allgemeinen ist die Aussage falsch, da es ein Gegenbeispiel ist.

Wir halten fest, dass ein Beispiel niemals einen Beweis für eine allgemeine Aussage liefern kann, die "für alle n" gelten soll (so wie Lemma 1.6), ein Gegenbeispiel aber sehr wohl eine derartige Aussage widerlegen kann. Allgemeiner gesprochen: Für Aussagen wie **"es gibt" kann ein Beispiel als Beleg** gelten, für Aussagen der Art **"für alle" hingegen nie**, hier kann es höchstens als Motivation oder Inspiration dienen.

Übrigens, aufgrund von Lemma 1.10 lässt sich Proposition 1.7 nicht verallgemeinern. Während also für $a = 2$ in Lemma 1.9 sowohl die Aussagen "$A \Rightarrow B$" (Lemma 1.5) als auch "$B \Rightarrow A$" (Lemma 1.6) gelten – und somit "$A \Leftrightarrow B$" (Proposition 1.7) –, ist dies für allgemeine a nicht wahr (Lemma 1.10), allgemein gilt nur "$A \Rightarrow B$" (Lemma 1.9). Man kann sich übrigens überlegen, dass die Äquivalenz "$A \Leftrightarrow B$" für alle Primzahlen a gilt, sogar für alle Zahlen $a \in \mathbb{N}$, die man nicht als $a = b^2c$ schreiben kann, mit $b \neq 1$. Für alle anderen Zahlen $a = b^2c$ findet man ein Gegenbeispiel zu "$B \Rightarrow A$".

Als kleine Anmerkung zu Beispiel 1.1: Das Clay Mathematics Institute hat bestimmt, dass das Preisgeld von einer Million Dollar an denjenigen ausgezahlt werden soll, der entweder einen Beweis für die Riemannsche Hypothese – oder ein Gegenbeispiel liefert. Da die Aussage der Riemannschen Hypothese der Form "für alle s gilt ..." ist, würde also ein Beispiel einer einzigen Zahl s mit $\zeta(s) = 0$ und $s \notin -2\mathbb{N}$ sowie $\mathrm{Re}(s) \neq \frac{1}{2}$ einen Beweis dafür liefern, dass die Riemannsche Hypothese falsch ist. Hier wäre also ein Gegenbeispiel ein Beweis für die gegenteilige Aussage.

1.3. **Beweisprinzip: Kontraposition.** Proposition 1.4(i) liefert uns ein weiteres Beweisschema: den Beweis durch Kontraposition. Anstatt "$A \Rightarrow B$" zu beweisen (direkter Beweis), können wir auch "$(\neg B) \Rightarrow (\neg A)$" zeigen (Kontraposition). Hier ist ein Beispiel für einen solchen Beweis.

Lemma 1.11. *Sei $n \in \mathbb{Z}$. Ist n^2 ungerade, so auch n.*

Beweis. Sei $n \in \mathbb{Z}$. Es ist eine Aussage "$A \Rightarrow B$" zu zeigen, mit $A =$"n^2 ist ungerade" und $B =$"n ist ungerade". Die Kontraposition der Aussage ist "$(\neg B) \Rightarrow (\neg A)$", also die Implikation "ist n gerade, so ist auch n^2 gerade". Genau dies war aber Gegenstand von Lemma 1.5. □

1.4. **Beweisprinzip: Beweis durch Widerspruch.** Beim Beweis durch Widerspruch wollen wir eine Aussage A verifizieren, indem wir zeigen, dass aus $\neg A$ ein Widerspruch folgt – denn dann kann $\neg A$ nicht wahr gewesen sein. Ist aber $\neg A$ falsch, so ist A wahr und wir haben das Gewünschte. Etwas formaler können wir uns folgende Wahrheitstabelle für jenes Beweisprinzip anschauen, wobei wir $\perp$ für "Widerspruch" schreiben (wir könnten auch $\perp := B \wedge (\neg B)$ definieren, eine Aussage, die immer falsch ist, siehe Proposition 1.4(a)).

$\neg A$	$\perp$	$(\neg A) \Longrightarrow \perp$
w	w	w
w	f	f
f	w	w
f	f	w

Da die Aussage $\perp$ immer falsch ist, können Zeilen 1 und 3 der Tabelle nicht eintreten. Zeigen wir nun, dass "$(\neg A) \Longrightarrow \perp$" wahr ist (dass also aus der Aussage $\neg A$ ein Widerspruch folgt), so befinden wir uns zwangsläufig in Zeile 4 der obigen Tabelle – also ist $\neg A$ falsch und demnach A wahr.

Hier ist ein Beispiel eines Beweises durch Widerspruch.

Proposition 1.12. *Die Zahl $\sqrt{2}$ ist irrational.*

Beweis. Wir nehmen an, dass $\sqrt{2}$ rational ist und wollen diese Aussage zu einem Widerspruch führen. Wäre also $\sqrt{2}$ rational, so gäbe es Zahlen $p, q \in \mathbb{Z}$ mit $q \neq 0$ und $\sqrt{2} = \frac{p}{q}$. Wir können annehmen, dass der Bruch gekürzt ist, dass es also keine Zahl a gibt, die sowohl p als auch q teilt. Nun gilt

$$\frac{p^2}{q^2} = \left(\frac{p}{q}\right)^2 = \left(\sqrt{2}\right)^2 = 2$$

und also $p^2 = 2q^2$. Somit ist p^2 gerade und nach Lemma 1.6 also auch p. Das bedeutet, wir können p schreiben als $p = 2m$ für eine Zahl $m \in \mathbb{Z}$. Damit gilt aber

$$4m^2 = (2m)^2 = p^2 = 2q^2$$

und daher auch $q^2 = 2m^2$. Somit ist q^2 gerade und nach Lemma 1.6 also auch q. Wir haben also gezeigt, dass sowohl p als auch q gerade sind (also von 2 geteilt werden), obwohl wir angenommen hatten, dass keine Zahl a gibt, die sowohl p als auch q teilt. Das ist also ein Widerspruch und die Annahme, dass $\sqrt{2}$ rational ist, muss demnach falsch sein. □

Das Prinzip, aus einer Aussage $\neg A$ einen Widerspruch herleiten zu wollen, um zu beweisen, dass A wahr ist, bringt uns zum Prinzip von relativen Aussagen. Das sind Aussagen der Form "$A \Rightarrow B$". Für derartige Aussagen ist es irrelevant, ob A wahr ist oder nicht – es wird lediglich behauptet, dass Aussage B aus Aussage A folgt.

Beispiel 1.13. Ein Beispiel einer solchen relativen Aussage ist ein Resultat von Dudek aus dem Jahr 2014 (aufbauend auf Resultaten von vielen anderen, u.a. von

von Koch aus dem Jahre 1901). Es besagt: Ist die Riemannsche Vermutung wahr, dann gibt es zu jeder reellen Zahl $x \geq 2$ eine Primzahl p im Intervall

$$(x - \frac{4}{\pi}\sqrt{x}\log x, x].$$

Mit anderen Worten, man findet zu jeder Zahl x eine Primzahl "in der Nähe" – die Primzahlen sind also "zufällig" verteilt.

Solche relativen Aussagen sind aus zwei Gründen relevant. Erstens liefern sie sofort Konsequenzen aus Aussage A, sollte es jemandem gelingen diese zu beweisen. Im Fall von Beispiel 1.13 also: Sollte jemand die Riemannsche Vermutung beweisen können, so wissen wir sofort etwas über die zufällige Verteilung der Primzahlen. Zweitens liefern relative Aussagen aber auch Indizien dafür, ob eine Aussage wahr ist – oder führt im besten Fall sogar dazu, A zu widerlegen. Denn wenn eine Aussage "$A \Rightarrow B$" mit einer weiteren Aussage "$B \Rightarrow C$" verknüpft werden kann und diese mit "$C \Rightarrow D$" etc, bis wir schließlich bei einem Widerspruch angelangen, dann kann A nicht wahr gewesen sein.

1.5. **Beweisprinzip: vollständige Induktion.** Kommen wir zu einem weiteren, wichtigen Beweisschema: der vollständigen Induktion. Diese ist ein Prinzip, dass für Aussagen angewandt werden kann, die von natürlichen Zahlen abhängen. Seien dazu $A(n)$ Aussagen, die von $n \in \mathbb{N}$ abhängen. Die Idee ist, dass man zunächst zeigt, dass $A(1)$ wahr ist (der *Induktionsbeginn* oder *Induktionsanfang*) und dann, dass für beliebiges $n \in \mathbb{N}$ die Implikation "$A(n) \Rightarrow A(n+1)$" wahr ist (der *Induktionsschritt*); dabei wird im Induktionsschritt irgendwo verwendet, dass $A(n)$ wahr ist (die *Induktionsannahme* oder *Induktionsvoraussetzung*). Hat man diese beiden Teile gezeigt, den Induktionsbeginn sowie den -schritt, so hat man bewiesen, dass $A(n)$ für alle $n \in \mathbb{N}$ wahr ist, denn es gilt ja dann:

$$A(1) \Longrightarrow A(2) \Longrightarrow A(3) \Longrightarrow A(4) \Longrightarrow \dots$$

Hier ist ein Beispiel.

Proposition 1.14. *Für alle $n \in \mathbb{N}$ gilt die Formel*

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

Beweis. Wir betrachten die Aussage $A(n) =$"es gilt $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

Induktionsbeginn: Sei $n = 1$. Dann ist $\sum_{k=1}^{1} k = 1 = \frac{1(1+1)}{2}$. Die Aussage $A(1)$ ist also wahr.

Induktionsschritt: Sei $n \in \mathbb{N}$ beliebig und sei $A(n)$ wahr. Es gelte also $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$. Wir müssen nun $A(n+1)$ beweisen. Dazu rechnen wir:

$$\sum_{k=1}^{n+1} k = \sum_{k=1}^{n} k + (n+1)$$

Nach der Induktionsvoraussetzung gilt $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$. Wir haben also:

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

Somit ist $A(n+1)$ nachgewiesen und der Induktionsschritt ist bewiesen. □

Die Anekdote hinter dieser Aussage ist, dass dem neun-jährigen Gauß und seinen Klassenkameraden von ihrem Lehre die Aufgabe gestellt wurde, alle Zahlen von 1 bis 100 zu addieren. Der Lehrer versprach sich davon eine kleine Ruhepause, aber Gauß kam schon nach wenigen Minuten zu seinem Pult und überreichte ihm das Ergebnis: 5050. Er hatte nämlich folgenden Trick angewandt, der letztlich hinter obiger Formel steckt:

$$\begin{array}{rcrcrcrcrcr} 1 & + & 2 & + & 3 & + & 4 & + & \dots & + & 50 \\ 100 & + & 99 & + & 98 & + & 97 & + & \dots & + & 51 \\ = & & = & & = & & = & & & & = \\ 101 & + & 101 & + & 101 & + & 101 & + & \dots & + & 101 \end{array}$$

Und er berechnete $101 \cdot 50 = 5050$, also mit $n = 100$ die Rechnung $(n+1) \cdot \frac{n}{2}$.

1.6. **Mengenlehre (optional).** Es ist nicht ganz unproblematisch zu definieren, was überhaupt eine Menge sein soll, aber wir klammern dies hier aus und folgen der sogenannten "naiven" Mengenlehre Cantors vom 1895. Wir bezeichnen demnach eine Menge M mit Elementen x_1, x_2 etc auf folgende Weise:

$$M = \{x_1, x_2, \dots\}$$

Hierbei ist die Reihenfolge, in der wir die Elemente aufschreiben, irrelevant.

Definition 1.15. Wir führen folgende Bezeichnungen für Mengen M, N ein.

(a) Wir schreiben $x \in M$, wenn x ein Element von M ist, und $x \notin M$ andernfalls.
(b) Wir schreiben $N \subseteq M$, wenn N eine *Teilmenge* von M ist, wenn also alle Elemente $x \in N$ auch schon in M liegen.
(c) Wir schreiben $N = M$, wenn $N \subseteq M$ und $M \subseteq N$ gilt.
(d) Mit $|M|$ bezeichnen wir die *Mächtigkeit* von M, also die Anzahl der Elemente von M.
(e) Mit $\emptyset$ bezeichnen wir die *leere Menge*, also die Menge, die kein Element enthält.
(f) Mit $M \cup N$ bezeichnen wir die *Vereinigung* von M und N. Das ist die Menge aller Elemente x, für die $x \in M$ oder $x \in N$ gilt.
(g) Mit $M \cap N$ bezeichnen wir den *Durchschnitt* von M und N. Das ist die Menge aller Elemente x, für die $x \in M$ und $x \in N$ gilt.
(h) Mit $M \backslash N$ bezeichnen wir das *Komplement* von N in M. Das ist die Menge aller Elemente $x \in M$, für die $x \notin N$ gilt.

Proposition 1.16 (Regeln für Mengenoperationen)**.** *Es gelten die folgenden Regeln für Mengen M, N und P.*

(a) $N \cap (M \backslash N) = \emptyset$.
(b) *Sei* $N \subseteq M$. *Dann ist* $N \cup (M \backslash N) = M$.
(c) *Sei* $N \subseteq M$. *Dann ist* $M \backslash (M \backslash N) = N$.
(d) $M \backslash (N \cap P) = (M \backslash N) \cup (M \backslash P)$.
(e) $M \backslash (N \cup P) = (M \backslash N) \cap (M \backslash P)$.
(f) $(M \cup N) \cap P = (M \cap P) \cup (N \cap P)$.
(g) $(M \cap N) \cup P = (M \cup P) \cap (N \cup P)$.

Beweis. Wir überprüfen nur exemplarisch die Aussage (a). Wir nehmen an, dass $N \cap (M \backslash N)$ nicht leer ist. Also gibt es ein $x \in N \cap (M \backslash N)$. Dann ist nach Definition 1.15(g) $x \in N$ und $x \in M \backslash N$. Letzteres bedeutet nach Definition 1.15(h), dass $x \in M$ aber $x \notin N$ ist. Somit ist $x \in N$ und $x \notin N$, was ein Widerspruch ist. Die Aussage $N \cap (M \backslash N) \neq \emptyset$ ist also falsch, dh. $N \cap (M \backslash N) = \emptyset$ ist wahr. □

Wenn wir die Aussagen von Proposition 1.16 mit jenen von Proposition 1.4 vergleichen, stellen wir eine **Analogie** fest.

Tatsächlich ist die Operation $\cup$ für Mengen analog zur ODER-Verknüpfung $\vee$ von Aussagen: Definieren wir die Aussage A durch "x ist in M" und die Aussage B durch "x ist in N", dann gilt $x \in M \cup N$ genau dann, wenn $A \vee B$ wahr ist. Ebenso entsprechen $\cap$ und $\wedge$ einander, genauso wie das Komplement und $\neg$.

Die Regeln von Proposition 1.16(d) und (e) heißen übrigens die *de Morganschen Regeln*.

1.7. **Aufgaben.**

Aufgabe 1.1. Verifizieren Sie die Regeln von Proposition 1.4 mit Hilfe eines Vergleichs von Wahrheitstafeln.

Aufgabe 1.2. Verifizieren Sie die Regeln von Proposition 1.16.

Aufgabe 1.3.
(a) Beweisen Sie: Ist n durch 3 teilbar, so auch n^3.
(b) Gilt auch die Umkehrung? Wenn ja: Beweisen Sie es. Wenn nein: Geben Sie ein Gegenbeispiel an.
(c)* Für welche $a \in \mathbb{N}$ gilt der folgende Satz?
Eine Zahl $n \in \mathbb{N}$ wird genau dann von a geteilt, wenn a auch n^3 teilt.

Aufgabe 1.4. Beweisen Sie mittels vollständiger Induktion:

$$\text{(a)} \quad \sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1}$$

$$\text{(b)} \quad \sum_{k=1}^{n} \frac{k}{2^k} = 2 - \frac{n+2}{2^n}$$

2. Gruppen

Abstract. Wir motivieren, dass der Begriff einer Symmetrie präzise gefasst werden sollte. Dazu führen wir den abstrakten, unanschaulichen Begriff der Gruppen ein. Von einer solchen axiomatischen Definition ausgehend überprüfen wir für eine Reihe von Beispielen, ob sie Gruppen sind oder nicht. Wir lernen dann anhand von Untergruppen und Homomorphismen grundlegende Ideen wie Unterstrukturen, strukturerhaltende Abbildungen sowie Isomorphismen kennen. Zum Schluss betrachten wir noch Gruppenwirkungen und machen den Schulterschluss mit der Motivation: Gruppen als Formalismus für Symmetrien.

2.1. **Motivation.**

Wir betrachten ein gleichseitiges Dreieck. Welche Symmetrien sehen wir?

$$D_3 = \{\mathrm{id}, d_{120}, d_{240}, s_0, s_{60}, s_{120}\}$$

Hierbei ist d_{120} die Drehung im $\mathbb{R}^2$ nach links um 120 Grad, s_{60} die Spiegelung an der Achse, die um den Ursprung geht und einen Winkel von 60 Grad hat. Wir betrachten ein gleichschenkliges aber nicht gleichseitiges Dreieck. Welche Symmetrien sehen wir hier?

$$\mathrm{id}, s_0$$

Und nun ein Dreieck mit drei verschieden langen Seiten. Dessen Symmetrien:

$$\mathrm{id}$$

Wir können also Symmetrien dazu verwenden, Objekte zu unterscheiden. Aber wie fassen wir den Begriff der Symmetrie präzise? Wie formulieren wir ihn für höherdimensionale oder viel abstraktere Objekte?

2.2. **Definition und Beispiele von Gruppen.**

Definition 2.1. Eine *Gruppe* $(G, \circ)$ ist eine nicht leere Menge G mit einer Verknüpfung $\circ : G \times G \times G$, so dass gilt:

(a) *Assoziatitivität* $f \circ (g \circ h) = (f \circ g) \circ h$ für alle $f, g, h \in G$.
(b) *Existenz eines neutralen Elements* Es gibt ein $e \in G$, so dass für alle $g \in G$ gilt: $e \circ g = g = g \circ e$.
(c) *Existenz inverser Elemente* Zu jedem $g \in G$ gibt es ein $g^{-1} \in G$, so dass: $g \circ g^{-1} = e = g^{-1} \circ g$.

Eine Gruppe heißt *abelsch*, falls zusätzlich gilt:

(d) *Kommutativität* $g \circ h = h \circ g$ für alle $g, h \in G$.

Dies ist eine **axiomatische Definition** eines mathematischen Begriffs. Wir können nun für ein paar Beispiele überprüfen, ob sie die Axiome einer Gruppe erfüllen.

Bemerkung 2.2. Man kann nachweisen, dass das neutrale Element immer eindeutig ist (sofern ein solches existiert): Sind $e, e' \in G$, so dass für alle $g \in G$ gilt: $e \circ g = g = g \circ e$ und $e' \circ g = g = g \circ e'$, so gilt $e = e'$, denn $e = e \circ e'$, da e' ein neutrales Element ist (setze $g := e$ in $g = g \circ e'$). Ebenso gilt $e \circ e' = e'$, da e ein neutrales Element ist (setze $g := e'$ in $e \circ g = g$). Also $e = e \circ e' = e'$.

Ebenso ist zu einem gegeben Element $g \in G$ das inverse Element eindeutig.

Beispiel 2.3. (a) Für $n \in \mathbb{N}$ bezeichnet

$$D_n = \{\mathrm{id}, d_{\frac{360}{n}}, d_{2*\frac{360}{n}}, \ldots, d_{(n-1)*\frac{360}{n}}, s_0, s_{\frac{360}{2n}}, s_{2*\frac{360}{2n}}, \ldots, s_{(n-1)*\frac{360}{2n}}\}$$

die *Diedergruppe*. Sie stellt die Symmetrien eines regelmäßigen n-Ecks dar. Mit $g \circ h$ bezeichnen wir hier die Hintereinanderausführung der Operationen (gelesen von rechts nach links) und wir vergewissern uns für $n = 3$:

- Sind $g, h \in D_3$, so auch $g \circ h$. Dies überprüfen wir für alle Elemente $g, h \in D_3$. Zum Beispiel $d_{120} \circ d_{120} = d_{240}$ oder $d_{120} \circ s_{60} = s_0$ oder $s_{60} \circ d_{120} = s_{120}$. Dies zeigt übrigens auch, dass D_3 nicht abelsch ist.
- Wir überprüfen die Assoziativität für alle Elemente $f, g, h \in D_3$. Zum Beispiel

$$d_{120} \circ (s_{60} \circ d_{120}) = d_{120} \circ s_{120} = s_{60} = s_0 \circ d_{120} = (d_{120} \circ s_{60}) \circ d_{120}.$$

- Das Element $\mathrm{id} = d_0$ ist das neutrale Element, denn $g \circ \mathrm{id} = g = \mathrm{id} \circ g$ für alle $g \in D_3$.
- Die inversen Elemente sind gegeben durch $\mathrm{id}^{-1} = \mathrm{id}$, $d_{120}^{-1} = d_{240}$, $d_{240}^{-1} = d_{120}$ sowie $s^{-1} = s$ für $s \in \{s_0, s_{60}, s_{120}\}$, wie direkte Berechnungen zeigen.

Somit sind alle Axiome einer Gruppe erfüllt – D_n ist eine (nicht-abelsche) Gruppe.

(b) Wir verifizieren, dass $(\mathbb{Z}, +)$ eine abelsche Gruppe ist:
- $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ definiert eine Verknüpfung auf $\mathbb{Z}$ (dh. $x + y \in \mathbb{Z}$ für alle $x, y \in \mathbb{Z}$).
- Diese Verknüpfung ist assoziativ, da $x + (y + z) = (x + y) + z$ für alle $x, y, z \in \mathbb{Z}$.
- Das neutrale Element ist $0 \in \mathbb{Z}$, da $x + 0 = x = 0 + x$ für alle $x \in \mathbb{Z}$.
- Zu $x \in \mathbb{Z}$ ist $-x$ das inverse Element, denn $x + (-x) = 0 = (-x) + x$.
- Außerdem gilt $x+y = y+x$ für alle $x, y \in \mathbb{Z}$, die Gruppe ist also abelsch.

(c) Ist $(\mathbb{N}, +)$ eine Gruppe? Nein, denn es gibt keine inversen Elemente, z.B. hat $g = 1$ kein inverses Element – es gibt kein $h \in \mathbb{N}$ mit $g + h = 0$. Allerdings ist $(\mathbb{N}, +)$ eine Halbgruppe (Definition 2.1(a)), sogar ein Monoid (Definition 2.1(a)+(b)), sogar ein abelscher.

(d) Ist $(\mathbb{Z}, \cdot)$ eine Gruppe (mit der Multiplikation)? Nein, denn es gibt keine inversen Elemente. Aber es ist ein abelscher Monoid.

(e) $(\mathbb{R}, +)$ ist eine abelsche Gruppe.

(f) $(\mathbb{R}\backslash\{0\}, \cdot)$ ist eine abelsche Gruppe.

(g) $(\mathbb{R}, \cdot)$ ist keine Gruppe, da 0 kein inverses Element besitzt.

(h) $(\mathbb{Z}_2, +)$ ist eine Gruppe, mit $\mathbb{Z}_2 := \{0, 1\}$ und der Addition definiert durch:

$+$	0	1
0	0	1
1	1	0

Definition 2.4. Seien X, Y Mengen. Eine Abbildung $f : X \to Y$ heißt

(a) *injektiv*, falls für alle $x, y \in X$ gilt: $f(x) = f(y)$ impliziert $x = y$.
(b) *surjektiv*, falls es zu jedem $y \in Y$ ein $x \in X$ gibt mit $f(x) = y$.
(c) *bijektiv*, falls f injektiv und surjektiv ist.

Beispiel 2.5. Typische Bildchen für Injektivität, Surjektivität und Bijektivität.

Bemerkung 2.6. Ist $f : X \to Y$ bijektiv, so existiert eine Umkehrfunktion $f^{-1} : Y \to X$, die für $y \in Y$ definiert ist durch $f^{-1}(y) := x$, für das eindeutig bestimmte $x \in \{1, \dots, n\}$ mit $f(x) = y$. Hierbei existiert das Element x nach der Surjektivität und es ist eindeutig nach der Injektivität. Wir haben $f(f^{-1}(y)) = y$ und $f^{-1}(f(x)) = x$.

Beispiel 2.7. Die *symmetrische Gruppe* S_n ist definiert durch

$$S_n = \{f : \{1, \dots, n\} \to \{1, \dots, n\} \mid f \text{ ist bijektiv}\}$$

zusammen mit der Hintereinanderausführung als Verknüpfung

$$(f \circ g)(x) := f(g(x)), \qquad x \in \{1, \dots, n\}.$$

Wir sehen, dass $\circ$ eine Abbildung von $\{1, \dots, n\} \times \{1, \dots, n\}$ nach $\{1, \dots, n\}$ definiert, die assoziativ ist. Das neutrale Element ist $\mathrm{id} : \{1, \dots, n\} \to \{1, \dots, n\}$ gegeben durch $\mathrm{id}(x) = x$ und das inverse Element von $f \in S_n$ ist die Umkehrfunktion f^{-1}.

Die Gruppe S_n ist nicht abelsch. Man kann sich die Funktionen in S_n bildlich wie folgt vorstellen:

1	2	3	4	5		1	2	3	4	5
2	4	1	3	5		3	4	1	5	2

2.3. **Untergruppen.** Gegeben eine Struktur – wie kann man sinnvoll eine Unterstruktur definieren?

Definition 2.8. Sei $(G, \circ)$ eine Gruppe. Eine nicht leere Teilmenge $U \subseteq G$ heißt *Untergruppe*, falls $(U, \circ_{|U})$ eine Gruppe ist, wobei $\circ_{|U}$ die Einschränkung $\circ_{|U} : U \times U \to U$ bezeichnet.

Bemerkung 2.9. Ist U eine Untergruppe von G und $e \in G$ das neutrale Element von G, so ist $e \in U$ und e ist das neutrale Element von U.

Ist $g \in U$ und $g^{-1} \in G$ das inverse Element von g in G, so ist $g^{-1} \in U$ und g^{-1} ist auch das inverse Element von g in U.

Beispiel 2.10. (a) In U ist $\{e\}$ eine Untergruppe.
(b) In $D_3 = \{\mathrm{id}, d_{120}, d_{240}, s_0, s_{60}, s_{120}\}$ ist $U = \{\mathrm{id}, s_0\}$ eine Untergruppe.

(c) In S_{n+1} ist

$$S'_n := \{f : \{1, \dots, n, n+1\} \to \{1, \dots, n, n+1\} \mid f \text{ ist bijektiv und } f(n+1) = n+1\}$$

eine Untergruppe.

2.4. **Homomorphismen und Isomorphismen.** Was sind strukturerhaltende Abbildungen zwischen Gruppen?

Definition 2.11. Seien $(G, \circ_G)$ und $(H, \circ_H)$ Gruppen. Eine Abbildung $\varphi : G \to H$ heißt *(Gruppen-)Homomorphismus*, falls $\varphi(g \circ_G h) = \varphi(g) \circ_H \varphi(h)$ für alle $g, h \in G$. Ist φ bijektiv, so heißt φ ein *(Gruppen-)Isomorphismus*.

Homomorphismen sind also Abbildungen, die die Struktur einer Gruppe erhalten. Gibt es sogar einen Isomorphismus zwischen zwei Gruppen, so können wir in gewissem Sinne sagen, dass die beiden Gruppen "gleich" sind.

Der Isomorphismus ist einer der wichtigsten Begriffe in der Mathematik und er wird in jeder einzelnen Disziplin der Mathematik entsprechend definiert. Die Idee ist immer die gleiche: Ein Isomorphismus ist eine Abbildung zwischen den Objekten, die die Struktur vollständig erhält und es uns erlaubt, diese beiden Objekte in gewissem Sinne zu identifizieren. Der Isomorphismus ist die **Abstraktion des Begriffs von "gleich sein"**.

Bemerkung 2.12. Sei $\varphi : G \to H$ ein Homomorphismus zwischen zwei Gruppen.

(a) Es gilt $\varphi(e_G) = e_H$ für die neutralen Elemente $e_G \in G$ bzw. $e_H \in H$.

(b) Der *Kern* von φ

$$\ker \varphi := \{g \in G \mid \varphi(g) = e_H\}$$

ist eine Untergruppe von G. Es gilt immer $\{e_G\} \subseteq \ker \varphi$, nach (a).

(c) φ ist injektiv genau dann, wenn $\ker \varphi = \{e_G\}$.

Beispiel 2.13. (a) Die Gruppe $\mathbb{Z}_2$ ist isomorph zu D_2 (nachrechnen).

(b) Die Untergruppe $S'_n \subseteq S_{n+1}$ aus Beispiel 2.10(c) ist isomorph zu S_n. Es gibt nämlich einen Isomorphismus

$$\varphi : S_n \to S'_n \subseteq S_{n+1}$$

definiert durch $\varphi(f) := \tilde{f}$, wobei

$$\tilde{f}(x) := \begin{cases} f(x) & \text{falls } x \leq n \\ n+1 & \text{falls } x = n+1 \end{cases}, \qquad \text{für } x \in \{1, \dots, n, n+1\}.$$

Wir überprüfen, dass $\varphi(f \circ g) = \varphi(f) \circ \varphi(g)$ gilt: Für $x \leq n$ gilt

$$\widetilde{f \circ g}(x) = (f \circ g)(x) = f(g(x)) = f(\tilde{g}(x)) = \tilde{f}(\tilde{g}(x)) = (\tilde{f} \circ \tilde{g})(x)$$

und außerdem

$$\widetilde{f \circ g}(n+1) = n+1 = \tilde{f}(n+1) = \tilde{f}(\tilde{g}(n+1)) = (\tilde{f} \circ \tilde{g})(n+1).$$

Also gilt $\varphi(f \circ g) = \widetilde{f \circ g} = \tilde{f} \circ \tilde{g} = \varphi(f \circ g)$.

Des Weiteren ist φ injektiv: Ist $\tilde{f} = \varphi(f) = \varphi(g) = \tilde{g}$, so ist $f = g$. Und φ ist surjektiv: Zu $g \in S'_n$ ist $g(n+1) = n+1$. Also ist

$$f : \{1, \dots, n\} \to \{1, \dots, n\}$$

definiert durch $f(x) := g(x)$ bijektiv und somit in S_n. Es gilt dann $\varphi(f) = g$, also ist φ surjektiv.

Damit ist φ ein bijektiver Homomorphismus, also ein Isomorphismus.

(c) Die Gruppe D_4 ist isomorph zu $D'_4 := \{\mathrm{id}, d_{90}, d_{180}, d_{270}, s_0, s_{45}, s_{90}, s_{135}\} \subseteq D_8$. Beachten Sie, dass in D_8 noch viel mehr Drehungen und Spiegelungen enthalten sind.

2.5. **Gruppenwirkungen und Symmetrien.** Kommen wir zurück zum Symmetriebegriff. Warum fassen Gruppen diesen Begriff in einem sinnvollen Maße?

Definition 2.14. Sei $(G, \circ)$ eine Gruppe und X eine Menge. Wir sagen, dass G auf X *wirkt* (oder: *operiert*), falls es eine Abbildung $\alpha : G \times X \to X$ gibt, mit

(a) $\alpha(e, x) = x$ für alle $x \in X$,
(b) $\alpha(g, \alpha(h, x)) = \alpha(g \circ h, x)$ für alle $g, h \in G$ und $x \in X$.

Beispiel 2.15. Die symmetrische Gruppe S_n wirkt auf der Menge $\{1, \dots, n\}$ via

$$\alpha : S_n \times \{1, \dots, n\} \to \{1, \dots, n\}$$

wobei $\alpha(f, x) := f(x)$ für $f \in S_n$ und $x \in \{1, \dots, n\}$. Das neutrale Element von S_n ist $e = \mathrm{id}$ und wir haben $\alpha(e, x) = \mathrm{id}(x) = x$. Außerdem gilt

$$\alpha(g, \alpha(h, x)) = \alpha(g, h(x)) = g(h(x)) = (g \circ h)(x) = \alpha(g \circ h, x).$$

Beispiel 2.16. Die Diedergruppe D_n wirkt auf dem regelmäßigen n-Eck. Hierzu parametrisieren wir das n-Eck durch Nummerierung seiner Eckpunkte. Dann wirkt

$$D_n = \{\mathrm{id}, d_{\frac{360}{n}}, d_{2*\frac{360}{n}}, \dots, d_{(n-1)*\frac{360}{n}}, s_0, s_{\frac{360}{2n}}, s_{2*\frac{360}{2n}}, \dots, s_{(n-1)*\frac{360}{2n}}\}$$

im kanonischen Sinne auf dem n-Eck. Für $n = 3$ schreiben wir

$$X = \{\{1,2,3\}, \{1,2,3\}, \{2,1,3\}, \{3,1,2\}, \{2,3,1\}, \{3,2,1\}\}$$

Wir beobachten, dass D_4 nicht auf dem gleichseitigen Dreieck E_3 wirkt, da beispielsweise eine Drehung d_{90} von E_3 um 90 Grad das Dreieck nicht wieder in sich selbst überführt. Daraus lesen wir, dass das gleichseitige Dreieck E_3 andere Symmetrien hat als das Quadrat E_4.

Wir haben den Begriff einer Symmetrie **abstrahiert** und **von unserer Anschauung losgelöst** mathematisch präzise gefasst. Dadurch können wir mit diesem Begriff rein formal arbeiten und wasserdichte Aussagen beweisen.

2.6. **Aufgaben.**

Aufgabe 2.1. Fertigen Sie eine Tabelle aller Verknüpfungen $g \circ h$ für $g, h \in D_4$ an. Lesen Sie daran das neutrale Element und die inversen Elemente ab und überzeugen Sie sich, dass D_4 eine nicht-abelsche Gruppe ist.

Aufgabe 2.2. Überprüfen Sie, ob die folgenden Objekte Gruppen sind. Welche sind abelsch?

(a) $(\mathbb{Z}, \cdot)$, wobei $\cdot$ die Multiplikation auf $\mathbb{Z}$ ist.
(b) $(\mathbb{Q}, +)$.
(c) $(\mathbb{Q}\backslash\{0\}, \cdot)$.
(d) $\mathbb{Z}^2$ versehen mit $(x_1, y_1) \circ (x_2, y_2) := (x_1 + x_2, y_1 + y_2)$, für $x_1, x_2, y_1, y_2 \in \mathbb{Z}$.

Aufgabe 2.3. Es seien

$$X_1 := \{1, 2, 3\}, \qquad X_2 := \{1, 2, 3, 4\}, \qquad X_3 := \mathbb{R}.$$

Finden Sie – wenn möglich – für jedes $i, j \in \{1, 2, 3\}$ jeweils Abbildungen $f_1, f_2, f_3, f_4 : X_i \to X_j$, so dass

(a) f_1 weder injektiv, noch surjektiv,
(b) f_2 injektiv, aber nicht surjektiv,
(c) f_3 nicht injektiv, aber surjektiv,
(d) f_4 bijektiv ist.

Saarland University, Fachbereich Mathematik, Postfach 151150, 66041 Saarbrücken, Germany
Email address: weber@math.uni-sb.de